FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Superior em Segurança da Informação

Maria Victoria Trecco de Arruda Leme

Vulnerabilidade no NDP: Ataque *Denial of Service* através da função de *Duplicate Address Detection*

Americana, SP
2016

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior em Segurança da Informação

Maria Victoria Trecco de Arruda Leme

Vulnerabilidade no NDP: Ataque *Denial of Service* através da função de *Duplicate Address Detection*

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superio em Segurança da Informação, sob a orientação da Prof.(a) Esp. Daniele Junqueira Frosoni.

Área de concentração: Segurança da Informação

Americana, SP

2016

L568v LEME, Maria Victoria Trecco de Arruda

Vulnerabilidade no NDP: ataque *denial of service* através da função de *duplicate address detection*. / Maria Victoria Trecco de Arruda Leme. – Americana: 2016.

109f..

Monografia (Curso de Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.

Orientador: Profa. Daniele Junqueira Frosoni

1. Comunicação de dados 2.Segurança em sistemas de informação I. FROSONI, Daniele Junqueira II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.519

Maria Victoria Trecco de Arruda Leme

Vulnerabilidade no NDP: Ataque *Denial of Service* através da função de *Duplicate Address Detection*

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 10 de Dezembro de 2016.

Banca Examinadora:

Daniele Junqueira Frosoni
Especialista
Faculdade de Tecnologia de Americana

Edson Roberto Gaseta
Especialista
Faculdade de Tecnologia de Americana

Jeferson Willian de Godoy Stenico
Doutor
Faculdade de Tecnologia de Americana

AGRADECIMENTOS

Agradeço meus pais e meus irmãos por me apoiarem sempre, as minhas amigas Cris, Sill e Stephanie que iniciaram essa jornada comigo e sempre me ajudaram quando precisei, aos meninos Paulo, Tarcisio, Marcelo e Jucilei que me proporcionaram muitas risadas e chocolate. E a Professora Daniele, minha orientadora, que ajudou no desenvolvimento desse trabalho e durante todo o curso, obrigada pela atenção.

DEDICATÓRIA

Aos meus pais que não se importaram com as dificuldades encontradas e me ajudaram a chegar até aqui.

“O tormento acompanha todas as grandes mudanças. E nós já passamos por mais tormentos do que deveria nos caber, pois somos agentes dessa própria mudança.”

(Christopher Paolini)

RESUMO

O modelo de arquitetura de comunicação com a Internet usado mundialmente é o TCP/IP (Protocolo de Controle de Transmissão/ Protocolo da Internet), esse modelo possue diversos protocolos. O IPv4 é um destes protocolos e o mais importante quando trata-se da troca de dados com a Internet e endereço de rede. A expansão do acesso a informação nos últimos anos fez com que o número de endereços disponíveis tornasse insuficiente, sendo necessária a definição da versão mais atual desse protocolo, o IPv6. Com essa mudança, outros protocolos também precisaram ser modificados, como o ICMPv6 e o NDP, que trabalham juntos no TCP/IP. No entanto, tais alterações trouxeram vulnerabilidades ao protocolo NDP, quando realiza a função de detecção de endereços duplicados, que é um procedimento realizado toda vez que um endereço IP é atribuído a um *host,* sendo possível realizar um ataque de negação de serviço a rede.

Palavras Chave: IPv6; ICMPv6; NDP; Vulnerabilidade.

ABSTRACT

The model of Internet communication architecture used worldwide is TCP / IP (Transmission Control Protocol / Internet Protocol), this model has several protocols. IPv4 is one of these protocols and most important when it comes to data exchange with the Internet and network address. The expansion of access to information in recent years has made the number of available addresses insufficient, and it is necessary to define the most current version of this protocol, IPv6. With this change, other protocols also needed to be modified, such as ICMPv6 and NDP, which work together on TCP / IP. However, such changes have brought vulnerabilities to the NDP protocol, when performing the function of detecting duplicate addresses, which is a procedure performed every time an IP address is assigned to a host, it being possible to perform a denial of service attack on the network.

Keywords: *IPv6; ICMPv6; NDP; vulnerability*.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AFRINIC: *African Network Information Centre*

APNIC: *Asia Pacific Network Information Centre*

ARIN: *American Registry for Internet*

ARP: *Addres Resulation Protocol*

CERT:Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.

CGA: *Cryptographically Generated Addresses*

DAD: *Duplicate Address Detection*

DDoS: *Distributed Denial of Service*

DHCP: *Dynamic Host Configuration Protocol*

DoS: *Denial of Service*

IANA: *Internet Assigned Numbers Authority*

ICMP: *Internet Control Message Protocol*

ICMPv4: *Internet Control Message Protoco version 4*

ICMPv6: *Internet Control Message Protoco version 6*

IGMP: *Internet Group Management Protocol*

IP: *Internet Protocol*

IPSec: *Internet Protocol Security*

IPv4: *Internet Protocol Version 4*

IPv6: *Internet Protocol Version 6*

LACNIC: *Latin America & Caribbean Network Information Centre*

MLD: *Multicast Listener Discovery*

MTU: *Maximum Transfer Unit*

NAT: *Network Address Translation*

NA: *Neighbor Advertisement*

NDP: *Neighbor Discovery Protocol*

NS: *Neighbor Solicitation*

OSI: *Open Systems Interconection*

P2P: *Peer-to-Peer*

PING: *Packet InterNet Grouper*

PRKI: *Resource Public Key Infrastructure*

RA: *Router Advertisement*

RARP: *Reverse Address Resolution Protocol*

RFC: *Request for Comments*

RIPE: *Réseaux IP Européens*

RSVP: *Répondez S'il Vous Plaît*

SLAAC: *Stateless Address Autoconfiguration*

SEND: *Secure Neighbor Discovery*

TCP/IP: *Transmission Control Protoco/Internet Protocol*

THC-IPV6: *The Hackers Choice - Internet Protocol Version 6*

UIT: União Internacional de Telecomunicações

VOIP: *Voice over Internet Protocol*

VPNs: *Virtual Private Network*

SUMÁRIO

1 INTRODUÇÃO

Com a expansão do acesso à Internet na última década foi necessária que ocorresse uma mudança no protocolo de comunicação com a Internet, a *Internet Protocol*. Atualmente ocorre uma transição entre o IPv4 (*Internet Protocol version 4*) e o IPv6 (*Internet Protocol version 6*), a nova versão do protocolo, mas essa alteração fez com que diversos protocolos mudassem, como é o caso do ICMP (*Internet Control Message Protocol*) e do NDP (*Neighbor Discovery Protocol*).

Uma das funções do NDP é a detecção de endereços duplicados. O objetivo desse trabalho é explorar e detectar a vulnerabilidade do NDP quando realiza-se a detecção de endereços duplicados, através da apresentação de um ataque DoS (*Denial of Service*).

Para isso foi necessário pesquisar sobre os protocolos IP nas suas versões quatro (IPv4) e seis (IPv6) e como fazer a transição desse protocolo e quais as dificuldades de implementação do IPv6 em toda a internet. Aprofundar os conhecimentos sobre o protocolo ICMP nas suas versões quatro (ICMPv4) e seis (ICMPv6), suas novas funções e estudar o protocolo NDP que utiliza mensagens do ICMP para realizar suas funções. Por fim, este trabalho visou descrever as vulnerabilidades e os problemas de segurança encontrados nesses protocolos com foco no DAD (*Duplicate Address Detection*).

A justificativa para a escolha desse trabalho é desmistificar que o IPv6 é um protocolo seguro. O IPv6 corrigiu problemas de segurança do IPv4, porém as mudanças dos protocolos fizeram com que surgissem novos problemas de segurança e vulnerabilidades, e o profissional de Tecnologia da Informação precisa conhecer essas mudanças.

O trabalho foi escrito em quatro capítulos: o primeiro capítulo, é uma introdução ao assunto; no segundo, o resultado da pesquisa bibliográfica sobre o modelo TCP/IP (*Transmission Control Protoco/Internet Protocol*) e os protocolos IP, ICMP e NDP; no terceiro, contém um ataque de negação de serviço através da função de detecção de duplicação de endereços, uma função do protocolo NDP; e por último a conclusão desse projeto. Além dos quatro capítulos, o trabalho contém também nos apêndices os tutoriais para a

realização da parte prática apresentado no capítulo três.

A metodologia para Minayo (2007, p. 44) é “a apresentação adequada e justificada dos métodos, técnicas e dos instrumentos operativos que devem ser utilizados para as buscas relativas às indagações da investigação”.

Para desenvolver esse trabalho foi utilizada a metodologia que busca o conhecimento científico, que é descrito por Tartuce (2006, p. 8):

> o conhecimento científico exige demonstrações, submete-se à comprovação, ao teste. O senso comum representa a pedra fundamental do conhecimento humano e estrutura a captação do mundo empírico imediato, para se transformar posteriormente em um conteúdo elaborado que, por intermédio do bom senso, poderá conduzir às soluções de problemas mais complexos e comuns até as formas de solução metodicamente elaboradas e que compõe o proceder científico.

A ferramenta utilizada foi o bibliográfico que segundo Marconi e Lakatos (1992) é o levantamento e leitura de bibliografias já publicada, nesse caso em livros, artigos, teses e dissertações.

E o conhecimento científico permite a utilização do método do estudo de caso que segundo Machado (2016) “define estudo de caso como uma categoria de pesquisa cujo objetivo é uma unidade que se analisa profundamente. Tendo como objetivo aprofundar a descrição de determinada realidade”.

2 MODELO TCP / IP

De acordo com Tanenbaum (2003), Rede de Computadores é um “conjunto de computadores autônomos interconectados por uma única tecnologia”. Para Mendes (2015), “Redes de computadores estabelecem a forma-padrão de interligar computadores para o compartilhamento de recursos físicos ou lógicos”.

Internet para Kurose (2006) “é uma rede de computadores mundial, isto é, uma rede que interconecta milhões de equipamentos de computação em todo o mundo”.

O modelo de arquitetura TCP/IP (*Transmission Control Protoco/Internet Protocol*) permite a comunicação em uma rede de computadores, neste caso a Internet, o modelo de cinco camadas utilizado por Tanenbaum (2003) é composta por: Aplicação, Transporte, Rede, Enlace e Física. sendo que cada camada é responsável por um processo e há diversos protocolos responsáveis por cada uma delas.

Outro modelo apresentado para comunicação de redes é a arquitetura OSI (*Open Systems Interconection*), dividida em sete camadas: Aplicação, Apresentação, Sessão, Transporte, Rede, Enlace e Física. Mais utilizado para estudos acadêmicos. O modelo TCP/IP engloba algumas camadas do modelo OSI.

O modelo de quatro camadas é conhecido como Modelo Internet utilizado por Kurose e Ross (2010), contém as camadas de Aplicação, Transporte, Internet e Acesso à Rede. As diferenças de cada modelo estão descritas na Tabela 1:

Tabela 1: Diferença de Arquiteturas

Modelo OSI	**Modelo Cinco Camadas**	**Modelo Internet**
Aplicação	Aplicação	Aplicação
Apresentação		
Sessão		
Transporte	Transporte	Transporte
Rede	Rede	Internet
Enlace	Enlace	Acesso à rede
Física	Física	

Fonte: Próprio Autor.

Os protocolos são utilizados para que ocorra a comunicação entre os computadores, e são empregados para unificar a linguagem na comunicação global.

E o que acontece quando alteramos um protocolo nesse modelo de comunicação? É o caso do protocolo IP (*Internet Protocol*) da camada de Rede, que está na versão IPv4 (*Internet Protocol Version 4*) e sofre uma transição para a versão IPv6 (*Internet Protocol Version 6*).

Os protocolos mais importantes de cada camada estão apresentados na Tabela 2.

Tabela 2: Protocolos

Camadas	**Protocolos**
Aplicação	FTP, SMTP, TELNET, HTTP, DNS.
Transporte	TCP e UDP
Rede	IP
Enlace	Ethernet, PPP
Física	

Fonte: Próprio Autor.

Cada camada tem sua função e é responsável pela comunicação com a camada de baixo.

A aplicação é responsável pelos programas, criptografia dos dados, e identificar a qual aplicativo o pacote pertence, *web*, transferências de arquivos e serviços de nomes.

A camada de transporte faz o trabalho de garantir que o pacote tenha chegado ao seu destino, início e término de conexões lógicas, controle de fluxo.

A camada de rede é responsável pela identificação da origem e do destino, endereço, roteamento, fragmentação, qualidade de serviço e controle de congestionamento.

A camada de enlace é o meio pelo qual os dados vão passar enquadramento, detecção de erros e tratamento dos mesmos, controle de fluxo e acesso ao meio.

E a camada de física sinalização, interface com o meio de transmissão,

início e término de conexões, sincronização e multiplexação.

2.1 PROTOCOLOS DA CAMADA DE REDE

Os protocolos objetos de estudo deste trabalho estão na camada de Rede, o IP e o ICMP (*Internet Control Message Protocol*) que serão abordados nas versões quatro e seis, e o NDP (*Neighbor Discovery Protocol*).

De acordo com o Tanenbaum (2003), a camada de rede tem como função principal o roteamento de pacotes, ou seja, é responsável por escolher o melhor caminho para o pacote trafegar na rede, controlar o fluxo e congestionamento do canal. A camada de rede é importante, pois conecta as camadas mais próximas da aplicação com as camadas mais próximas do hardware do computador.

2.1.1 Protocolo IPv4

O IPv4 foi criado na década de 70, localizado na camada de rede, tem como objetivo conectar redes. Tem como função o endereçamento lógico, a segmentação, a priorização e descartes dos pacotes após serem identificados problemas com o roteamento.

Após ocorrer um grande avanço no mundo da tecnologia, o acesso à rede se tornou essencial, e com isso o IPv4 tem se mostrado inadequado para uso.

O endereço IP é utilizado para identificar um *host* na Internet de maneira única. Segundo Kurose e Ross (2005), a forma de endereçamento do IP na versão quatro é composto por 32 *bits*, ou seja, 4 bytes. Cada *byte* é separado por um ponto e normalmente é representado por números decimais.

Ex: 11111111.11111111.11111111.11111111 = 255.255.255.255

Sendo assim a quantidade de endereços que o IPv4 suporta é resultado do cálculo 2^{32}, ou seja, 4.294.967.296 bilhões de endereços possíveis.

Cerca de 4 bilhões de endereços pode parecer muito, mas de acordo com a União Internacional de Telecomunicações (UIT, 2015) no ano de 2000 a Internet tinha cerca de 400 milhões de usuários e em 2015 esse número atingiu

cerca de 43% da população mundial, isso equivale a 3,2 bilhões de pessoas.

Ponderando que essas pessoas possuem *desktops, notebooks, tablets*, *smartphones*, *smart TV* e até geladeira com acesso à Internet, e levando em consideração que cada um desses *hosts* utilizam um endereço, o número de quatro bilhões de endereços disponíveis pelo IPv4 se esgotou.

2.1.1.1 Endereçamento

De acordo com a RFC 1466 os endereços IPv4 são divididos em classes de endereços. De acordo com Tanenbaum (2003), a classe A reserva os 8 primeiros bits para identificar a rede e os outros 24 bits para identificar o host; a classe B reserva os 16 primeiros bits para identificar a rede e os 16 últimos bits para identificar o *host*; e a classe C usa os 24 primeiros bits para identificar a rede e os últimos 8 bits para identificar o host; a classe D é reservada para *Multicast*; e a classe E é reservada para teste.

Essa divisão em classes faz com que dos 4 bilhões de endereços possíveis somente 2,5 bilhões são disponíveis para uso, conforme observado na .

Tabela 3.

Tabela 3: Classes e Respectivas Faixas

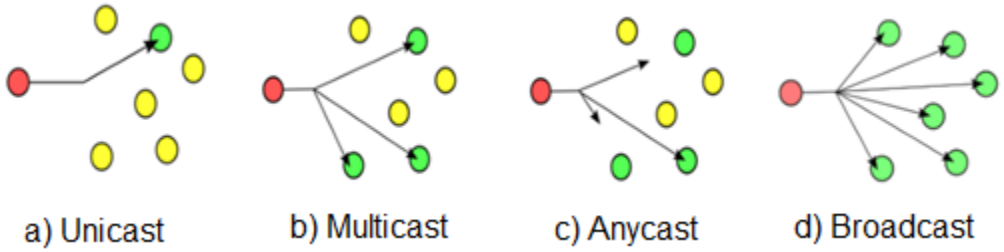
Classe	**Faixa IP**	**Máscara**	**Funcionalidade**
A	1.0.0.1 – 126.255.255.254	255.0.0.0	--
B	128.0.0.1 – 191.255.255.254	255.255.0.0	--
C	192.0.0.1 – 223.255.255.254	255.255.255.0	--
D	224.0.0.0 – 239.255.255.255	--	Multicast
E	240.0.0.0 – 247.155.255.255	--	Teste

Fonte: Kurose, 2010.

A função do *Multicast*, endereços reservadas da classe D, faz parte da comutação de redes ou transferência de pacotes, essas comutações de redes podem ser feitas de quatro tipos (Figura 1):

- *Unicast*: um remetente para um receptor.
- *Multicast*: um remetente para um grupo de receptores.
- *Anycast*: realiza cálculos e descobre o menor caminho para enviar o pacote do remetente até o receptor.
- *Broadcast*: um remetente para todos os receptores.

Figura 1: Comutação de Pacotes



Fonte: Brito, 2013.

2.1.1.2 Network Address Translation

Para driblar o problema de esgotamento do número de endereços do IPv4, utiliza-se o IP Privado, que não tem acesso direto a internet por não ser um IP válido na rede externa. De acordo com Kurose e Roos (2003), para solucionar o problema do acesso de um IP Privado a rede Internet criou-se o NAT (*Network Address Translation*), é um protocolo definido pela RFC (*Request for Comments*) 3022, que traduz esses endereços privados em endereços públicos no roteador, para que seja possível um pacote trafegar na internet.

De acordo com Tanenbaum (2003), o IP público é o endereço IP que tem acesso à Internet, e o IP privado é utilizado para comunicação na rede local. Quando algum dispositivo da rede local precisar acessar a rede externa (Internet) ela usa o NAT, para encapsular esse IP privado em um IP público. Isso ocorre, pois, os endereços com acesso direto a Internet, ou seja, os IP's público da versão IPv4 já se esgotaram, sendo assim impossível destinar um IP público para cada *host.*

A RFC 1918 definiu que as faixas de IP consideradas privadas são:

- 10.0.0.0 a 10.255.255.255/8 (16.777.216 hosts);

- 172.16.0.0 a 172.31.255.255/12 (1.048.576 hosts);
- 192.168.0.0 a 192.168.255.255//16 (65.536 hosts).

De acordo com BRAGA (2011), as vantagens de usar NAT são:

> • Reduz a necessidade de endereços públicos, contribuindo para diminuir a escassez deste tipo de endereço;
> • Facilita a numeração interna das redes;
> • Oculta a topologia das redes e;
> • Permite apenas a entrada de pacotes gerados em resposta a um pedido de rede.

Ainda de acordo com o autor, as desvantagens são:

> • Quebra do modelo fim-a-fim da Internet, já que não permite a conexão direta entre dois hosts;
> • Dificulta o funcionamento de uma série de aplicações, como VPNs (*Virtual Private Network*), VOIP (*Voice over Internet Protocol*) e P2P (*Peer-to-Peer*);
> • Baixa escalabilidade devido ao baixo número de conexões simultâneas;
> • Exige grande poder de processamento do dispositivo tradutor;
> • Passa uma falsa sensação de segurança porque não permite a entrada de pacotes não autorizados, mas não realiza nenhum filtro nos pacotes que passam por ele;
> • Não permite o rastreamento do caminho do pacote através de ferramentas como *traceroute*;
> • Dificulta a utilização de técnicas de segurança como o IPSec (*Internet Protocol Security*)

2.1.1.3 Datagrama

A RFC 1594 define que datagrama é "uma entidade de dados completa e independente que contém informações suficientes para ser roteada da origem ao destino sem precisar confiar em trocas anteriores entre essa fonte, a máquina de destino e a rede de transporte", ou seja, é um pacote de dados transferido através da comutação por pacotes, sem levar em consideração em que hora ou em que ordem a entrega é efetuada.

O cabeçalho do IPv4 (Figura 2), de acordo com a RFC 791, possuem os seguintes campos:

- Versão: É o primeiro campo do cabeçalho e contém a versão do protocolo IP que é usado na rede em que o *host* está conectado. Isso permite o roteador ler o restando do datagrama.
- Comprimento do Cabeçalho: determina o tamanho do cabeçalho já

que os campos não têm tamanho fixo.

- Tipo de serviço: determina o tipo de percurso do roteamento.
- Comprimento do datagrama: é o comprimento do datagrama e não somente do cabeçalho.
- Identificação: indica o fragmento do IP original.
- *Flags*: é usado para identificar se mais fragmentos chegarão
- Deslocamento de fragmentação: indica a qual posição do datagrama atual o fragmento pertence.
- Tempo de vida: é o tempo que o datagrama pode permanecer na rede, ou seja, o tempo de vida útil dele antes de ser descartado e outro igual ser mandando.
- Protocolo: Indica qual protocolo da camada de transporte esse datagrama está ligado.
- Bits para a verificação da Integridade do cabeçalho: é o *checksum*, verifica a integridade do pacote.
- Endereço IP da fonte: indica o IP do *host* de origem.
- Endereço IP do destino: indica o IP do *host* que vai receber o pacote.
- Opções: informa a rota, o tempo que o pacote demorou para atravessar os roteadores, é um campo opcional.

Nem todos os campos do cabeçalho estão sempre completos, caso o dado transmitido não possuir aquela informação o valor é vazio.

Figura 2 : Cabeçalho IPv4

Versão	**Comprimento do Cabeçalho**	**Tipo de Serviço**	**Comprimento do Datagrama**
Identificador	Flags	Deslocamento de Fragmentação	
Tempo de Vida	Protocolo	Bits para verificação da Integridade do Cabeçalho	
Endereço IP da Fonte			
Endereço IP do Destino			
Opções			

Fonte: Gupta; Lasalle; Parihar; Scringer, 2002.

2.1.2 Protocolo IPv6

O IPv6 é definido pela RFC 2460 de 1998. Sendo a nova versão do

protocolo IP, desenvolvido com o objetivo de solucionar o problema do esgotamento de endereços do IPv4 de forma definitiva. Foi desenvolvida principalmente por Allison Marken e Scott Bradner em 1994 na RFC 1752.

A distribuição de endereços IP's é realizada pela IANA (*Internet Assigned Numbers Authority*), que delega sua atividade e distribui os endereços IP's para cinco autoridades regionais, são elas:

- ARIN (*American Registry for Internet*);
- RIPE (*Réseaux IP Européens*);
- LACNIC (*Latin America & Caribbean Network Information Centre*);
- AFRINIC (*African Network Information Centre*);
- APNIC (*Asia Pacific Network Information Centre)*.

Cada autoridade aborda uma região do mundo conforme visto na Figura 3.

Figura 3: Autoridades Regionais da Internet

Fonte: IANA

O IPv6 foi oficializado em 6 de junho de 2012, após a APNIC anunciar o esgotamento do IPv4 na sua região de domínio.

A transição do Ipv4 para o Ipv6 deve acontecer de forma gradativa para que não haja problemas de indisponibilidade ou de incompatibilidade nos sistemas.

> Para que ocorra uma transição sem muitos problemas a melhor forma de difundir IPv6 é o método da coexistência IPv4-IPv6, assim as funcionalidades presentes no IPv4 continuaram funcionando sem a necessidade de interoperabilidade e somados com as novas

funcionalidades presentes no IPv6. (CAVALHIERI, 2006)

De acordo com Kurose e Roos (2003), os dois principais mecanismos de transição são:

- Pilha dupla: quando as duas versões do protocolo IP coexistem nos equipamentos. Isso permite que o equipamento trabalhe com ambos os protocolos, baseando seu comportamento de acordo com o protocolo.
- Tunelamento: O túnel é utilizado quando as duas versões não coexistem dentro do equipamento, permitindo assim que uma rede IPv6 se comunique com uma rede IPv4 através do encapsulamento do pacote IPv6 dentro de um datagrama IPv4.

Apesar das técnicas de transição, há problemas na implementação do IPv6, de acordo com Brito (2013) os maiores responsáveis pela lenta implementação são a escassez de profissionais qualificados para trabalhar com o IPv6 e a falta de investimento em novos equipamentos.

2.1.2.1 Endereçamento

O endereço do IPv6 é constituído por 128 bits, , ou seja, o IPv6 é constituído por $2^{128.}$ Isso permite que tenha 340.282.366.920.938.463.463.374.607.431.768.
211.456, ou seja, aproximadamente 340 onzilhões de endereços. Para que se torne mais quantitativo esse número equivale de acordo com a Brito (2013), “79 trilhões de trilhões de vezes a quantidade atual do IPv4”.

A representação é feita por hexadecimais separado por “:” a cada 16 bits. Já que a representação por binários é inviável.

Exemplo: 2000:0DB6:AB25:236F:0000:0000:0000:00B4

Esse tipo de endereçamento vai permitir utilizar maiúsculo e minúsculo, além das regras de abreviação, em que os “::” (dois pontos) representam os zeros contínuos, e onde é possível omitir os zeros as esquerda.

Exemplo:

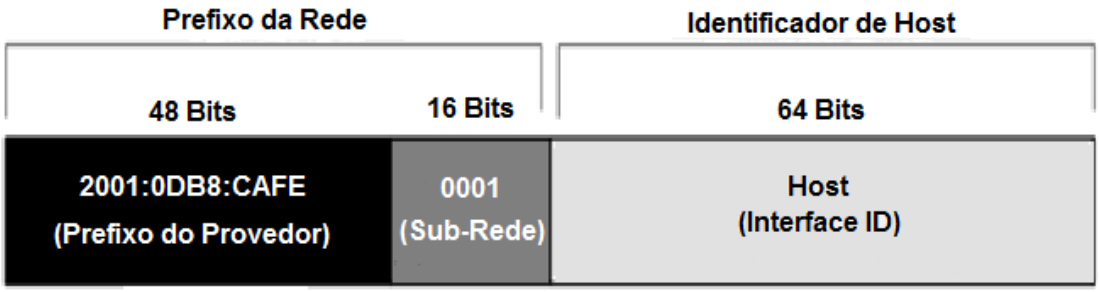
2000:0DB6:AB25:236F:0000:0000:0000:00B4 (Endereço Completo)

2000:0DB6:AB25:236F:0:0:0:B4 (Primeiro Passo)

2000:0DB6:AB25:236F::B4 (Representação Fiscal)

Os 64 bits da direita identificam o host e os 64 bits da esquerda representa a rede, sendo que 16 bits desses 64 bits da rede são pra sub-rede (conceito de sub-rede) e 48 bits do provedor, conforme descrito na Figura 4.

Figura 4: Estrutura do Endereço IPv6



Fonte: Brito, 2013.

Como visto na sessão ***2.1.1.1 Endereçamento***, hoje existem quatro tipos de comunicação, são eles: *unicast, multicast, anycast, broadcast.*

No IPv6 o *broadcast* não existe mais, quem vai exercer sua função é um grupo do *multicast*, em que todos os nós fazem parte, o *multicast-all-nodes*, que de acordo com Gorito (2014):

> Seu funcionamento é similar ao Broadcast, a única diferença é que na transmissão broadcast todos os dispositivos da rede sem exceção recebem o pacote, e na transmissão multicast apenas os dispositivos que pertencem a um grupo recebem o pacote.

Outro tipo de endereço é o *multicast solicited-node* que de acordo com o IPv6.br:

> identifica um grupo *multicast* que todos os nós passam a fazer parte assim que um endereço *unicast* ou *anycast* lhes é atribuído. Um endereço *solicited-node* é formado agregando-se ao prefixo **FF02::1:FF00:0000/104** os 24 bits mais a direita do identificador da interface, e para cada endereço *unicast* ou *anycast* do nó, existe um endereço *multicast solicited-node* correspondente.

E o endereço *unicast* possui três categorias:

- *Link Local*: são endereços reservados para comunicação local. E são automaticamente distribuídos para garantir o funcionamento.
- *Unique Local*: são endereços privados, ou seja, não são válidos na internet.
- *Global Unicast*: são os endereços públicos, que podem ser utilizados

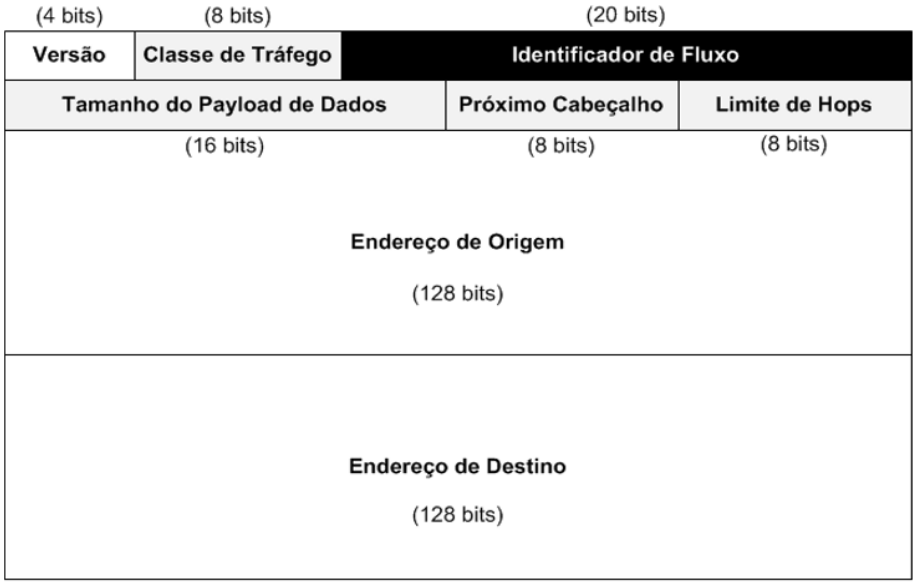
por um único equipamento.

2.1.2.2 Datagrama

O cabeçalho do IPv6 (Figura 5) tem tamanho fixo (40 *bytes*), isso permite uma velocidade maior no processamento do pacote. Os campos do cabeçalho IPv6 de acordo com o NIC.br (Núcleo de Informação e Coordenação de Pontos do Brasil) são:

- Versão: Onde identifica a versão do protocolo utilizado. Que nesse caso é o valor 6.
- Classe de Tráfego: Identifica os pacotes por classes de serviços ou prioridade.
- Identificador de Fluxo: Identifica pacotes do mesmo fluxo de comunicação.
- Tamanho do Dados: Indica o tamanho total dos dados, soma também o tamanho dos cabeçalhos de extensão.
- Próximo Cabeçalho: Identifica o próximo cabeçalho de extensão.
- Limite de Encaminhamento: Contém o número máximo de saltos permitido entre o roteamento. Ele é decrementado a cada salto e pode se descartado caso chegue a 0 e o pacote não chegue no destino.
- Endereço de origem: Indica o endereço de origem.
- Endereço de Destino: Indica o endereço de destino.

Figura 5: Cabeçalho do IPv6



Fonte: Brito, 2013.

De acordo com o IPv6.br o cabeçalho do IPv4 inclui todas as informações opcionais, diferente do IPv6, que trata essas informações nos cabeçalhos de extensão, que se encontra entre o cabeçalho base do IPv6 e o cabeçalho da camada de cima, e não tem tamanho fixo.

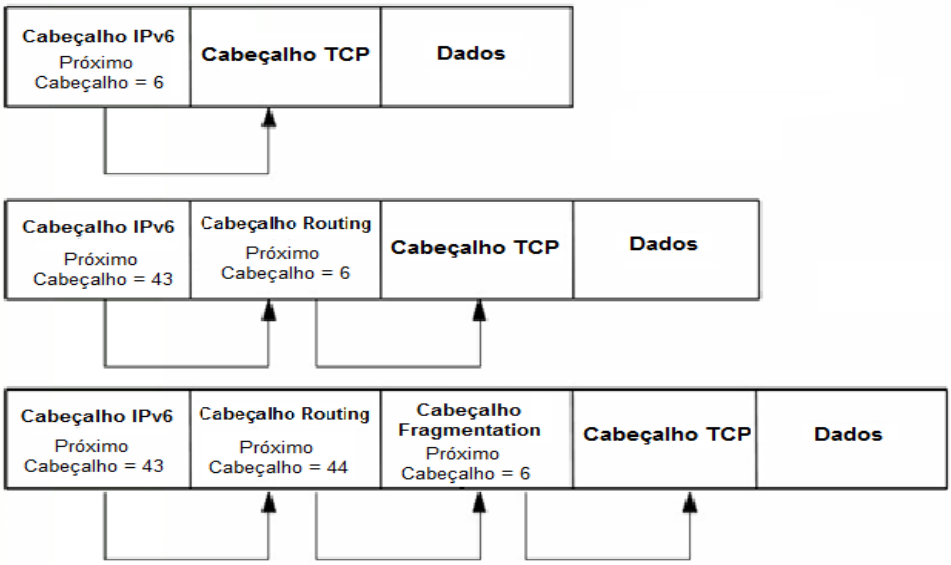
Esses cabeçalhos servem para aumentar a velocidade de processamento dos roteadores. O único a ser processado pelo roteador é o *Hop-by-Hop*. Os outros somente são tratados no nó de destino. E uma das vantagens desse uso é que podem ser criados novos cabeçalhos sem a necessidade de alterar o cabeçalho base, seu número é colocado no campo Próximo Cabeçalho.

Ainda de acordo com o IPv6.br, no IPv6 existem seis cabeçalhos de extensão:

- *Hop-by-Hop Options*: Tem o valor 00 no campo de próximo cabeçalho, possui dois tipos. O Router Alert que é utilizado para informar aos nós que a mensagem precisa de um tratamento específico. Muito utilizada pelos protocolos MLD (*Multicast Listener Discovery*) e RSVP (*Répondez S'il Vous Plaît*). E o Jumbogram informa que o tamanho do pacote IPv6 é maior do que 64KB:
- *Routing*: Tem o valor 43 e serve para carregar o endereço de origem do nó móvel em pacotes enviados pelos nós correspondentes;
- *Fragmentation*: Tem o valor 44 e é utilizado quando o pacote IPv6 é maior que o Path MTU (*Maximum Transfer Unit*);
- *Authentication Header*: tem valor 51 e é o cabeçalho responsável pela integridade e autenticação;
- *Encapsulating Security Payload*: tem o valor 52, semelhante ao cabeçalho anterior e é usado dentro do serviço do IPSec (é uma suíte de protocolos que visa serviços de segurança, integridade, autenticidade, e confidencialidade);
- *Destination Options*: Tem o valor 60 e deve ser processado apenas pelo nó do destino, ele é utilizado no suporte de mobilidade do IPv6, que contém o Endereço de Origem do Nó Móvel quando está no transito.

Caso um cabeçalho base possua muitos cabeçalhos de extensão, eles formam uma cadeia de cabeçalhos conforme a Figura 6.

Figura 6 : Cabeçalho de Extensão do IPv6



Fonte: NIC.br

2.1.3 Comparações entre IPv4 e IPv6

O cabeçalho das versões 4 e 6 do protocolo IP possuem diferenças, conforme visto na

Figura 7.

A diferença entre os cabeçalhos do IPv4 e do Ipv6 são:

- O IPv4 não contem um tamanho fixo (tamanho variável entre 20 e 60 *bytes*), enquanto o IPv6 possui um tamanho fixo de 40 *bytes* o que facilita o processamento dessas dados, tornando um protocolo mais ágil.
- De 12 campos a nova versão apresenta 8 deles. E o cabeçalho de extensão o torna mais flexível e eficiente.

Quatro campos foram renomeados, conforme a

- Tabela 4:

Tabela 4 : Renomeação dos Campo IPv4 x IPv6

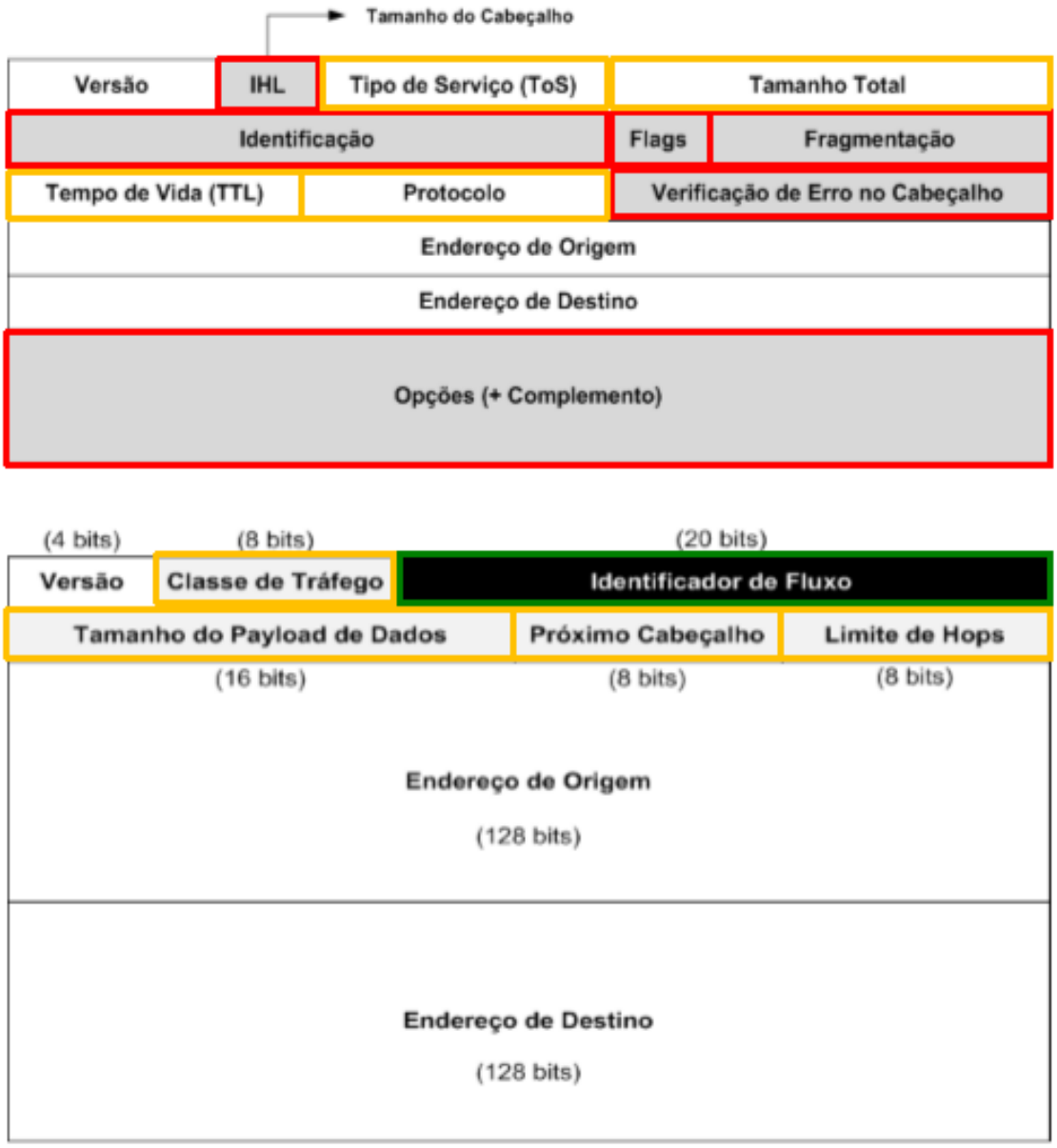
IPv4	IPv6
Tipo de Serviço	Classe de Serviço
Tamanho Total	Tamanho dos Dados
Tempo de Vida (TTL)	Limite de encaminhamento
Protocolo	Próximo Cabeçalho

Fonte: NIC.br

De acordo com o IPv6.br o campo Tamanho do Cabeçalho foi retirado, pois se tornou desnecessário apresentar a quantidade de *bytes* que o cabeçalho tem já que ele possui tamanho fixo. Outros campos como Identificação, *Flags*, Deslocamento do Fragmento e Opções e Complementos foram removidos também e essas informações quando apresentadas aparecem nos cabeçalhos de extensão. E o campo Soma de Verificação foi removido, pois outros protocolos das camadas superiores já fazem uma verificação e validação dos dados.

O campo Identificador de Fluxo foi adicionado na nova versão para melhorar o serviço de qualidade.

Figura 7: Cabeçalho IPv4 x IPv6



Fonte: Brito, 2013.

Além do cabeçalho IP outras mudanças aconteceram, conforme descrito na Tabela 5.

Tabela 5: Principais Diferenças entre o IPv4 e o IPv6

Itens de Comparação	IPv4	IPv6
Endereços IP	● Tamanho do campo de endeços igual a 32 bits. ● Definição de cinco classes de endereços (A, B, C, D e F)	● Tamanho máximo do campo de endereços igual a 128 bits. ● Defenição de três tipos de endereços: *unicast, anycast e multicast.*

Cabeçalho	● Existência de *checksum* do cabeçalho. ● Existência de um campo de opções, limitando em 40 bytes. ● Inexistência de mecanismo de definição de fluxo de tráfego.	● Inexistência de *checksum* do cabeçalho. ● Existência de cabeçalhos de extensão, com tamano arbitrários. ● Possibilidades de vincular vários datagramas ao mesmo fluxo de tráfego.
Frangmentação	● Realização de fragmentação em qualquer roteador, usado na interconexão de sub-redes destintas.	● Realização de fragmentação apenas no nó origem.
Roteamento	● Suporte aos protocolos básicos de roteamento. ● Função de roteamento na fonte por exercida por um protocolo de camada superio.	● Suporte aos protocolos básicos de roteamento. ● Função de roteamento na fonte implementada utilizando-se o cabeçalho de extensão de roteamento.
Segurança	● Inesxistência de mecanismos de segurança.	● Suporte a mecanismos de segurança usados na implementação de serviços de autenticação, não-repudiação, integridade e confidencialidade.
Controle de Erros e Resolução de Endereços	● Controle de erros é efetuado pelo protocolo ICMP, a resolução de endereços IP e físicos realizada pelos protocolos ARP e RARP respectivamente e o controle de membros de endereços multicast efetuado pelo protocolo IGMP.	●As funções de controle de erro, resolução de endereços e controle de membros de endereços *multicast* é realizada dentro do âmbito de um único protocolo, o ICMP.

Fonte: Carvalho, 1997.

2.1.4 Protocolo ICMPv4

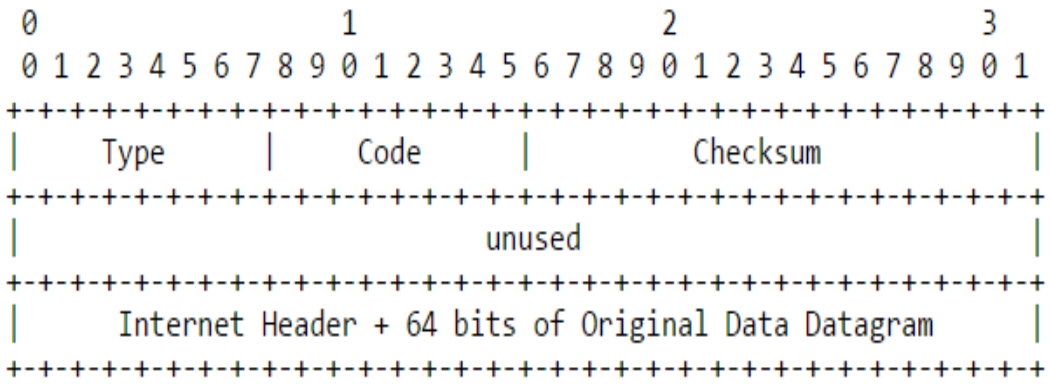
De acordo com Dantas (2002), “o ICMP (*Internet Control Message Protocol*) tem por objetivo prover mensagens na comunicação entre nós num ambiente de rede TCP/IP”. Ou seja, o ICMP é o protocolo que permite a troca de mensagens, de erro e de controle entre o roteador e o host, além de realizar diagnósticos e enviar mensagens sobre as características da rede. É definido pela RFC 792.

O ICMP é um protocolo de aviso de erros e é encapsulado no datagrama IP.

E o pacote ICMPv4 (*Internet Control Message Protoco version 4*) (Figura 8) possui os seguintes campos:

- *Type*: identifica a mensagem;
- *Code*: contém o número do tipo de mensagem;
- *Cheksum*: soma de verificação para cálculo de perda de pacotes;
- Unused: não usado;
- Internet Header + 64 bits of Original Data Datagram: Contém os dados específicos do datagrama.

Figura 8 : Pacote ICMPv4



Fonte: RFC 792.

No campo “tipo” é possível receber diversas mensagens, como demonstrado abaixo na Tabela 6.

Tabela 6: Mensagens do campo "tipo" no ICMPv4

Tipo de mensagem	Descrição
Destination unreachable	Não foi possível entregar o pacote
Time exceeded	O campo Time to live chegou a 0
Parameter problem	Campo de cabeçalho inválido
Source quench	Pacote regulador9 Redirect Ensina geografia a um roteador
Echo	Pergunta a uma máquina se ela está ativa
Echo reply	Sim, estou ativa
Timestamp request	Igual a Echo, mas com timbre de hora
Timestamp reply	Igual a Echo reply, mas com o timbre de hora

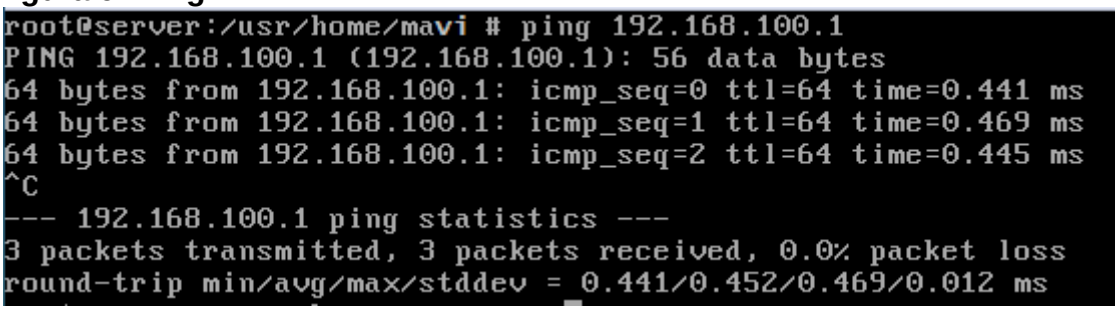
Fonte: Tanenbaum, 2003.

Uma das funções do ICMPv4 é o PING (*Packet InterNet Grouper*), comando utilizado para diagnóstico de redes, verificando a conectividade entre dois dispositivos.

O *ping* é um comando utilizado que mede a quantidade de tempo em milissegundos (ms) que um pacote de informações leva para ir e voltar, do remente até o destinatário. Ou seja, quanto menor o valor, mais rápido é a conexão.

Em um ambiente com sistema operacional Linux o comando é utilizado do seguinte modo (Figura 9: Ping): **ping e número do endereço IP que deseja testar a conexão.**

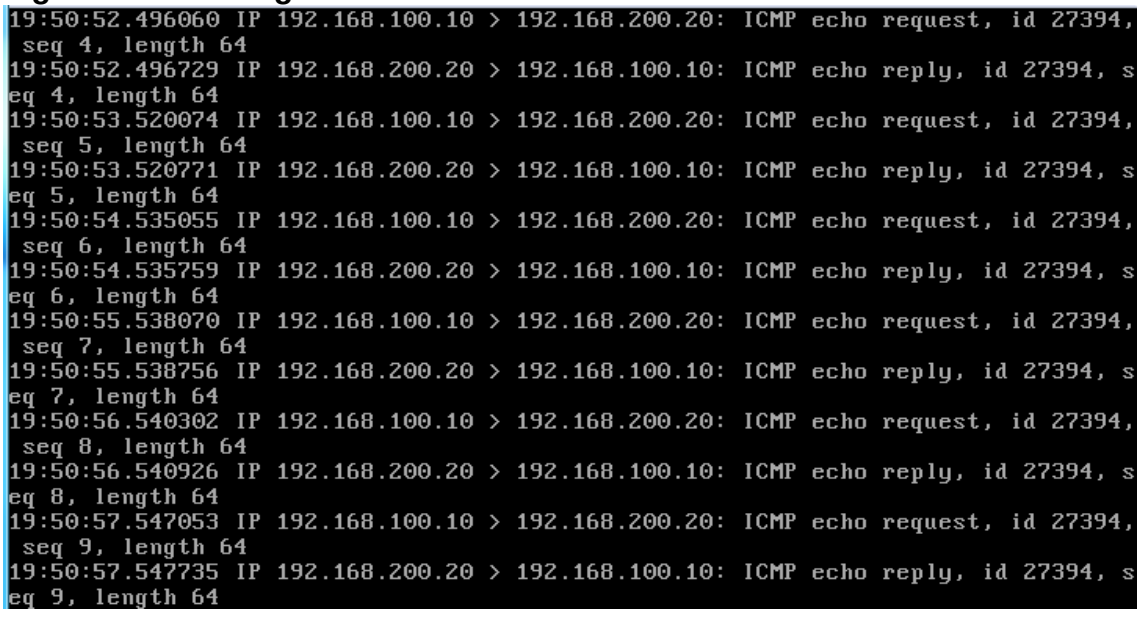
Figura 9: Ping



Fonte: Próprio Autor

Após o comando **ping** ser utilizado, o ICMP envia as mensagens, conforme pode ser visto na Figura 10.

Figura 10 : Mensagem ICMP



Fonte: Próprio Autor

2.1.5 Protocolo ICMPv6

O protocolo ICMPv6 (*Internet Control Message Protoco version 6*) é definido pela RFC 4443 e sua implementação é obrigatória nas redes que utilizam o IPv6 para se comunicar. Continua realizando as mesmas funções que a versão anterior, porém assume muitas outras funções. Isso acontece, pois o ICMPv6 assume funções de outros protocolos que existem no IPv4, para que se reduza a quantidade de protocolos.

Os protocolos que foram agregados ao ICMPv6 são:

- ARP (*Addres Resulation Protocol*): “tem por função o mapeamento de endereços IP para endereços físicos de rede, ou seja, podemos dizer que o ARP tem por função a resolução de endereços físicos, uma vez fornecidos endereços IPs”. (CAVALHIERE, 2006)
- RARP (*Reverse Address Resolution Protocol*): Dantas (2002) afirma que “O paradigma de resolução do protocolo RARP é o inverso do ARP.” Ou seja, na comunicação dos processos existe a informação do endereço físico e o protocolo pode pedir a informação do endereço lógico através dele.
- IGMP (*Internet Group Management Protocol*): atua como gerenciamento dos membros do grupo multcast.

Segundo o IPv6.br além de substituir esses protocolos descritos acima, o ICMPv6 é utilizado por outros protocolos, são eles:

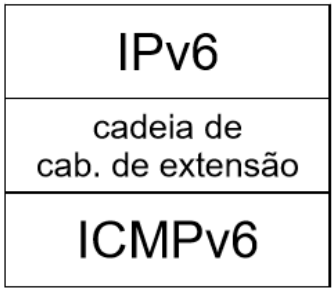
- MLD (*Multicast Listener Discovery*): opera com o gerenciamento de grupos multicast.
- NDP (*Neighbor Discovery Protocol):* é responsável por identificar e conhecer características da vizinhança.
- Path MTU Discovery: tem como objetivo descobrir o menor caminho entre dois nós.
- *Mobility Support*: responsável por gerenciar os endereços de origem do host dinamicamente.
- Autoconfiguração *Stateless*: Permite a aquisição de endereços IP’s sem o uso do protocolo DHCP (*Dynamic Host Configuration Protocol*).

O ICMPv6 localiza-se no campo Next Header do cabeçalho IPv6 com o

valor 58.

Para Santos, Moreiras, Reis e Rocha (2010), “em um pacote IPv6, o ICMPv6 posiciona-se logo após o cabeçalho base do IPv6, e dos cabeçalhos de extensão, se houver”. A Figura 11 retrata o posicionamento do cabeçalho ICMPv6 em um cabeçalho IPv6.

Figura 11 : Localização do ICMPv6 no cabeçalho IPv6

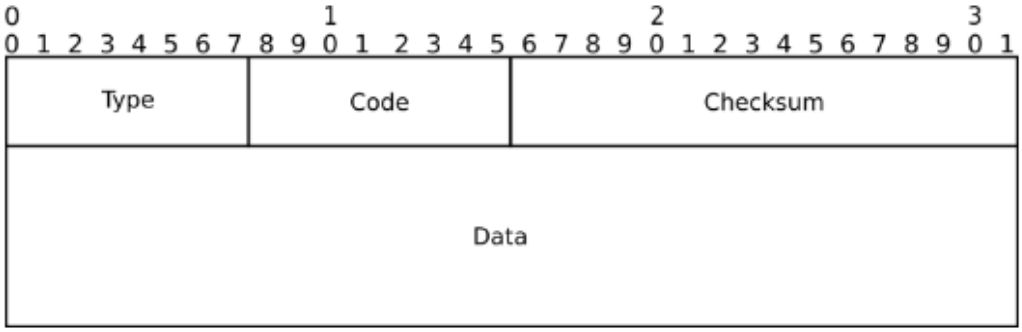


Fonte: IPv6.br

O cabeçalho do ICMPv6, conforme pode ser visto na Figura 12, possui os seguintes campos:

- *Type*: Campo com 8 bits, identifica a mensagem.
- *Code*: Campo com 8 bits, contém o número do tipo de mensagem (0 a 7), isso fornece informações adicionais sobre a mensagem.
- *Checksum*: campo com 16 bits, faz a soma de verificação para cálculo de perda de pacotes, ou seja, determina se há dados corrompidos no cabeçalho ICMPv6 e em parte do cabeçalho IPv6.
- Data: o campo não tem tamanho fixo, ele varia de acordo com o tipo da mensagem, mas tem valor máximo e 1280 bits. Ele mostra as informações ligadas ao tipo da mensagem.

Figura 12: Cabeçalho ICMPv6



Fonte: IPv6.br

O ICMPv6 possui duas classes de mensagens, as mensagens de erro (Tabela 7) e as mensagens de informação (Figura 8), conforme pode ser visto abaixo:

Tabela 7: Mensagem de Erro ICMPv6

Tipo	Nome	Descrição
1	Destination Unreachable	Indica falhas na entrega de pacote como endereço ou porta desconhecida ou problemas na comunicação.
2	Packet Too Big	Indica que o tamanho do pacote é maior que a Unidade Máxima de Transito (MTU) de um enlace.
3	Time Exceeded	Indica que o limite de Encaminhamento ou o tempo de remontagem do pacote foi excedido.
4	Parameter Problem	Indica erro em algum campo do cabeçalho IPv6 ou que o tipo indicado no Próximo Cabeçalho não foi reconhecido.
100-101		Uso experimental
102-126		Não utilizado
127		Reservado para expansão das mensagens de erro ICMPv6

Fonte: Santos, Moreiras, Reis, Rocha, 2010.

Tabela 8: Mensagem de Informação do ICMPv6

Tipo	Nome	Descrição
128 129	Echo Request Echo Replay	Utilizadas pelo comando *ping*.
130 131 132	Multicast Listener Query Multicast Listener Report Multicast Listener Done	Utilizadas no gerenciamento de grupos *multicast.*
133 134	Router Solicitation Router advertisement	Utilizadas com o protocolo Descoberta de Vizinhança

135 136 137	Neighbor Solicitation Neighbor Advertisement redirect Message	
138	Router Renumbering	Utilizada no mecanismo de Re-endereçamento (R*enumbering*) de roteadores.
139 140	Router Node Information Querry Router Node Information Response	Utilizadas para descobrir informações sobre nomes e endereços, são atualmente limitadas a ferramentas de diagnóstico, depuração e gestão de redes.
141 142	Inverse ND Solicitation Message Inverse ND Advertisement Message	Utilizadas em uma extensão do protocolo de Descoberta de Vizinhança.
143	Version 2 Multicast Listener Report	Utilizada no gerenciamento de grupos *multcast*.
144 145 146 147	HA Address Discovery Req. Message HA Address Discovery Reply. Message Mobili Prefiz Solicitation Mobili Prefiz Advertisement	Utilizadas no mecanismo de Mobilidade IPv6
148 149	Certification Path Solicitation Message Certification Path Advertisement Message	Utilizadas pelo protocolo SEND
150		Utilizadas experimentalmente com protocolos de mobilidade como o *Seamoby*.
151 152 153	Multicast Router Advertisement Multicast Router Solicitation Multicast Router Termination	Utilizadas pelo mecanismo *Multicast Router Discovery.*
154	FMIPv6 Messages	Utilizada pelo protocolo de mobilidade *Fast Handovers.*
200-2001		Uso experimental
255		Reservado para expansão das mensagens de erro ICMPv6.

Fonte: Santos, Moreiras, Reis, Rocha, 2010.

2.1.6 Protocolo NDP

O protocolo NDP (*Neighbor Discovery Protocol*) é definido pela RFC 4861 e assume as funções dos protocolos ARP, ICMP *Router Discovery* e ICMP *Redirec*.

O NDP não é um protocolo que funciona sozinho. Brito (2013) afirma que, “ele funciona a partir do ICMPv6 e, por isso, possui alguns tipos de mensagens reservadas para sua operação. Além das mensagens de erros e

das mensagens de informações". Com essa dependência do ICMP, o NDP utiliza cinco mensagens do ICMPv6, são elas:

- *Router Solicitation* (mensagem 133): é utilizada pelos hosts para requisitar aos roteadores a mensagem *Router Advertisements*.
- *Router Advertisement* (mensagem 134): é enviada em resposta da *Router Solicitation*, onde o roteador anuncia sua presença no enlace.
- *Neighbor Solicitation* (mensagem 135): é uma mensagem *multicast* enviada para determinar o MAC (*Media Access Control*), a acessibilidade de um vizinho, e detectar endereços duplicados.
- *Neighbor Advertisement* (mensagem 136): Enviada em resposta ao *Neighbor Solicitation,* e anuncia a mudança de algum endereço no enlace.
- *Redirect* (mensagem 137): enviada pelo roteador com o objetivo de informar ao *host* o melhor caminho.

E as mensagens descritas a cima podem trazer algumas opções, que são definidas pela RFC 4861:

- *Source Link-layer Address:* contém o endereço MAC do remetente;
- *Target Link-layer Address:* contém o endereço MAC do destino;
- *Prefix Information:* envia para o *host* o prefixos dos enlaces e da autoconfiguração do endereço;
- *Redirected Header:* contém o pacote (parcial ou total) que está sendo redirecionado;
- *Maximum Transfer Unit:* Indica o MTU (a quantidade dos dados que podem ser transmitidos em um único quadro) do enlace.

De acordo com Brito (2013), o NDP possui outras funções como a Descoberta de Endereços da Camada de Enlace que tem a função de determinar o endereço MAC dos vizinhos no mesmo enlace. Para isso o host envia uma mensagem *Neighbor Solicitation* para o endereço *multicast solicited* node informando seu MAC, e quando o destinatário recebe a mensagem ele envia uma mensagem *Neighbor Advertisement* informando seu endereço MAC.

De acordo com Brito (2013) a função de Descoberta de Roteadores e Prefixos que serve para localizar roteadores vizinhos dentro do mesmo enlace, e determina prefixos e parâmetros relacionados a autoconfiguração de endereços. Os dados são enviados por um roteador local através de uma

mensagem *Router Advertisement* enviada ao *multicast solicited node*.

A Detecção de Endereços Duplicados, que é utilizado na hora de atribuir um endereço IP, é necessário verificar se aquele endereço já não está sendo usado. Para isso o NDP implementa o DAD (*Duplicate Address Detection*).

Outra função é a Detecção de Atividade no Vizinho, procedimento utilizado para verificar se há algum roteador inacessível na rede, caso tenha, é procurado outro caminho para o pacote.

O Redirecionamento de Rotas que utiliza a mensagem *Redirect* para descobrir se há outro roteador na rede para que possa encaminhar o pacote por um caminho menor.

E por último a função de Autoconfiguração *Stateles que é realizado* pelo protocolo SLAAC (*Stateless Address Autoconfiguration)*, permite que a rede possa se autoconfigurar sem o serviço do DHCP.

2.2 SEGURANÇA NOS PROTOCOLOS DE REDE

Para Santiago e Lisboa (2011, apud. Ramos, 2006), “segurança é um estado onde se está livre de perigos e incertezas”.

E quando tratamos de Tecnologia da Informação, segurança possui uma definição mais ampla, para Rocha (2008 apud. Sêmola, 2003) segurança da informação é “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”. Segundo Fontes (2006), o princípio de Disponibilidade é a informação estar acessível.

De acordo com Silveira (2004), o IPv6 corrige alguns problemas de segurança do IPv4, sendo os mais graves, o IP Spoofing, “que são ataques que utilizam de pacotes IP com endereços falsos”; o Eavesdropping que é a “análise não autorizada dos pacotes que trafegam na rede”; e Packet Sniffing, “ataque no qual um intruso pode diretamente ler as informações transmitidas e conteúdo de base de dados.”

Porém segundo Brito (2013), isso não o torna completamente seguro, o IPv6 somente tem potencial de ser mais seguro que o antecessor IPv4, ressaltando que o IPv6 é novo operacionalmente, mas academicamente não,

pois foi desenvolvido na década de 90.

O protocolo IPSec foi criado para trabalhar de forma nativa com o IPv6 visando sua segurança, ou seja, os equipamentos que possuem suporte para o IPv6 também possuem suporte para IPSec.

Vulnerabilidade segundo Prado e Souza (2014) é “uma falha ou uma brecha da Segurança da Informação, pode ser explorada por ameaças. Quando uma ameaça encontra uma vulnerabilidade, dá-se uma violação da segurança.”

Algumas vulnerabilidades na rede IPv6 já foram encontradas, a maior parte delas é no ICMPv6 que explora as opções de descoberta de vizinhança. Na seção 2.2.1, estão apresentadas algunas falhas de segurança no ICMPv6. As falhas de segurança no IPv6 são conhecidas publicamente, e foram lançadas soluções para mitigar o risco.

2.2.1 Falhas de Segurança no ICMPv6

O IPSec não protege as mensagens ICMPv6 que são utilizadas pelo NDP, tornando-o mais vulnerável.

No IPv4 é comum configurar no firewall o bloqueio do ICMPv4 como medida de segurança com o objetivo de evitar ataques que incapacitem o sistema por causa do soprecarregamento da memória, como um ataque através do PING, mas no IPv6 o ICMPv6 incorpora os protocolo ARP e DHCP, sendo assim impossível bloqueá-lo totalmente, e caso isso acontecesse seria impossível trafegar na rede.

Alguns dos ataques conhecidos, descritos pelo Brito (2013), são:

- Ataque à detecção de endereços duplicados: o atacante gera sucessivas mensagens NA (*Neighbor Advertisement)* em resposta a toda mensagens NS (*Neighbor Solicitation)*, impossibilitando o host se conectar a rede.
- Envenenamento na tabela de vizinhança: o atacante envia sucessivas mensagens *Neighbor Advertisement*, ao fazer adiciona muitas entradas falsas na tabela de vizinhança, fazendo com que o desempenho diminua e até estourar o limite de entradas nas tabelas.
- Falsificadores de roteadores e prefixos: uma das funções do NDP é

anunciar os roteadores do enlace. Um atacante pode gerar uma mensagem RA (*Router Advertisement)* passando-se por roteador, podendo intermediar as comunicações.

- Varredura de endereços e privacidade: O *scanning* é utilizado para fazer a leitura dos endereços válidos e para encontrar vulnerabilidades, no IPv4 era possível varrer os endereços de uma máscara /24 que possuem 254 endereços, em 5 minutos. No IPv6 a prática ainda é utilizada, porém é necessário que os *scans* sejam mais direcionados, pois uma faixa de endereço IPv6 padrão possui máscara /64, tornando possível 18.446.744.073.709.551.616 endereços, isso demoraria 5 bilhões de anos para fazer a varredura completa. Tornando esse tipo de ataque inviável.

3 ATAQUE *DENIAL OF SERVICE* (DoS)

Há um ataque DoS (*Denial of Service*), ou seja, negação de serviço, que utiliza o NDP no ICMPv6.

De acordo com o CERT (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) para um ataque DoS é necessário que o atacante utilize um *host* na rede e esteja conectado a internet. Quando o ataque ocorre por mais de um indivíduo e de forma coordenada recebe o nome de Ataque Distribuído de Negação de Serviço, mais conhecido como DDoS (Distributed Denial of Service).

Sobre os ataques DDoS, o CERT diz que “Apesar de não ser possível impedir que eles ocorram, com um planejamento adequado, é possível torná-los menos eficazes e danosos”.

O ataque DoS tem o objetivo de incapacitar o alvo, afetando o princípio de Disponibilidade da Segurança da Informação.

Com a indisponibilidade do serviço o usuário é afetado, pois não consegue acessar ou realizar as ações desejadas, já que o serviço está sobrecarregado tratando das requisições recebidas.

Para se proteger desse tipo de ataque há algumas técnicas para mitigar esses problemas, como:

- Implementação da RFC 4890 que faz recomendações de filtragem das mensagens ICMPv6.
- Implementação do protocolo SEND (Secure Neighbor Discovery) que é uma extensão do NDP, descrito pela RFC 3971 e agora pela RFC 4861 prevê formas de proteger o protocolo NDP, por meio de criptografia e autenticidade, usa criptigrafua CGA (Cryptographically Generated Addresses) e PRKI (Resource Public Key Infrastructure), que são recursos de chaves públicas, providenciando assim mais segurança ao NDP com método criptografado independente do IPSec.
- Implementação de um Firewall, que de acordo com a equipe IPv6.br (2015) “Firewalls são equipamentos de rede ou programas de computador que por meio do bloqueio seletivo de conexões, baseados em uma política de segurança, buscam proteger redes de computadores”.

• Ou a implementação da ferramenta NDPmon que gera logs, ou seja, registros de comportamentos suspeitos no enlace, podendo gerar até alertas por e-mail, e identificando as máquinas suspeitas.

3.1 COMO FUNCIONA A DETECÇÃO DE DUPLICAÇÃO DE ENDEREÇO

De acordo com a Equipe IPv6.br a detecção de endereços duplicados *(Duplicate Address Detection – DAD),* é o procedimento realizado toda vez que um endereço IP é atribuído a um *host*, pode ser por autoconfiguração ou manualmente ou até mesmo quando o dispositivo é ligado.

Isso é realizado através do protocolo NDP que envia uma mensagem NS (*Neighbor Solicitation*) com a origem do endereço **::**, ou seja, não especificado.

Caso um host responda com NA (*Neighbor Advertisement*), o IP está sendo utilizado e o problema precisa ser resolvido manualmente.

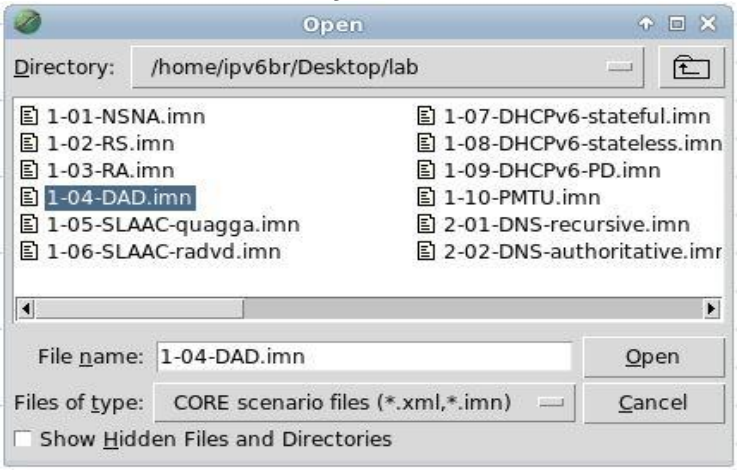
Mas caso o host não receba uma NA, terminará sua configuração. Sendo de um segundo o tempo de espera pela NA.

A seguir será realizada uma simulação onde atribuiremos um endereço duplicado a um *host*, para demonstrar na prática como a função DAD funciona.

3.1.1 Prática

Para a realização dessa etapa é necessário fazer a instalação da máquina virtual conforme o Apêndice A. Após a instalação e iniciação da máquina, abre-se o CORE e inicia a simulação 1-04-DAD.imn **(**
) conforme o Apêndice B e realizar o tutorial disponível no Apêndice C.

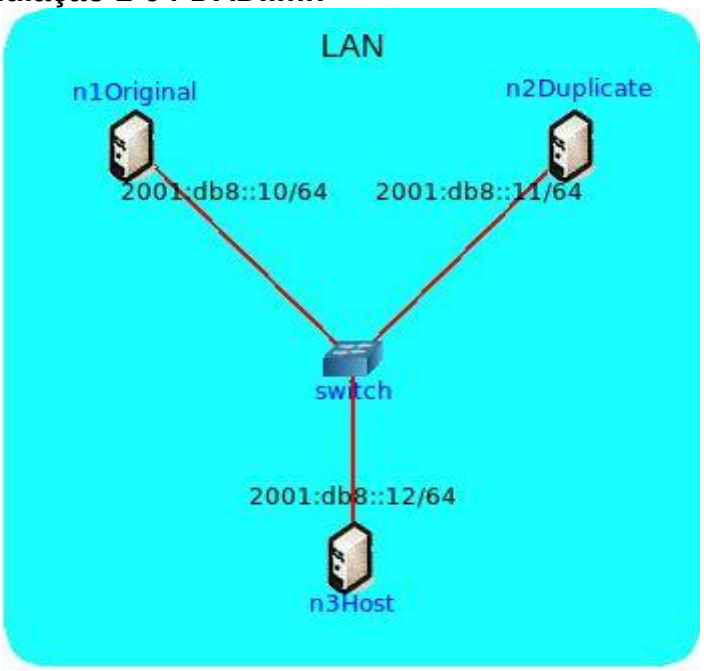
Figura 13: Abrir Cenário da Simulação



Fonte: Próprio Autor.

O cenário da simulação, conforme pode ser visto na Figura 14, contém os itens mínimos necessários para o experimento. Três computadores e um switch.

Figura 14: Simulação 1-04-DAD.imn



Fonte: Próprio Autor.

Configuração de rede:

- N1Original: 2001:db8::10/64
- N2Duplicate: 2001:db8::11/64
- N3Host: 2001:db8::12/64

Abrir o Wireshark no n1Original, n2Duplicate e n3Host e realizar o teste de conexão com todas as máquinas com o comando ping6, conforme descrito a seguir.

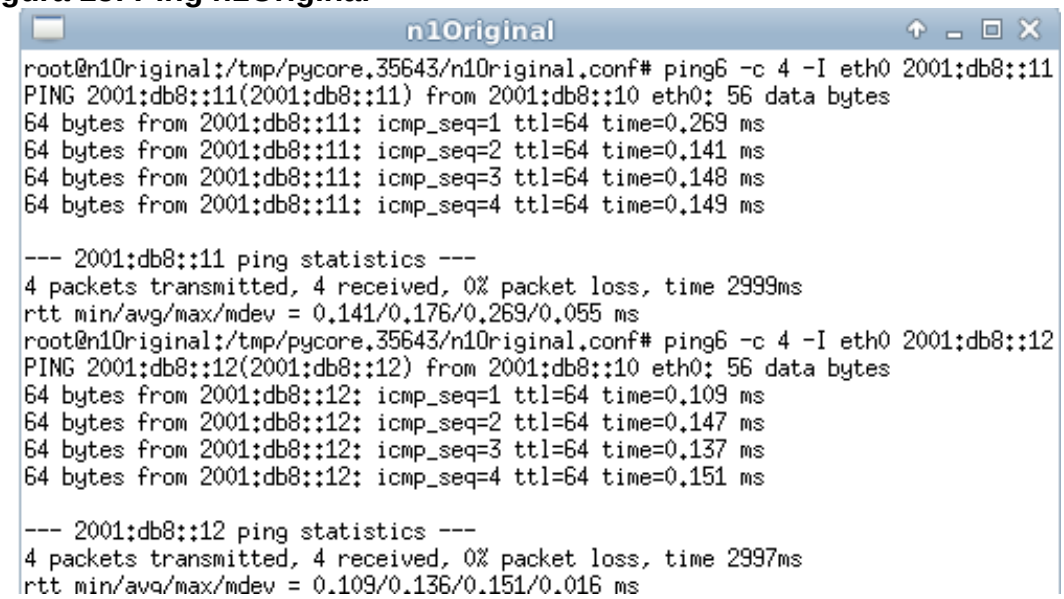
No terminal n1Original, executar os comandos:

```
#ping6 -c 4 -I eth0 2001:db8::11
#ping6 -c 4 -I eth0 2001:db8::12
```

Esses comandos testam a conexão do n1Original com o n2Duplicate e

n3Host.O resultado obtido é a conexão ativa, conforme visto na Figura 15:

Figura 15: Ping n1Original



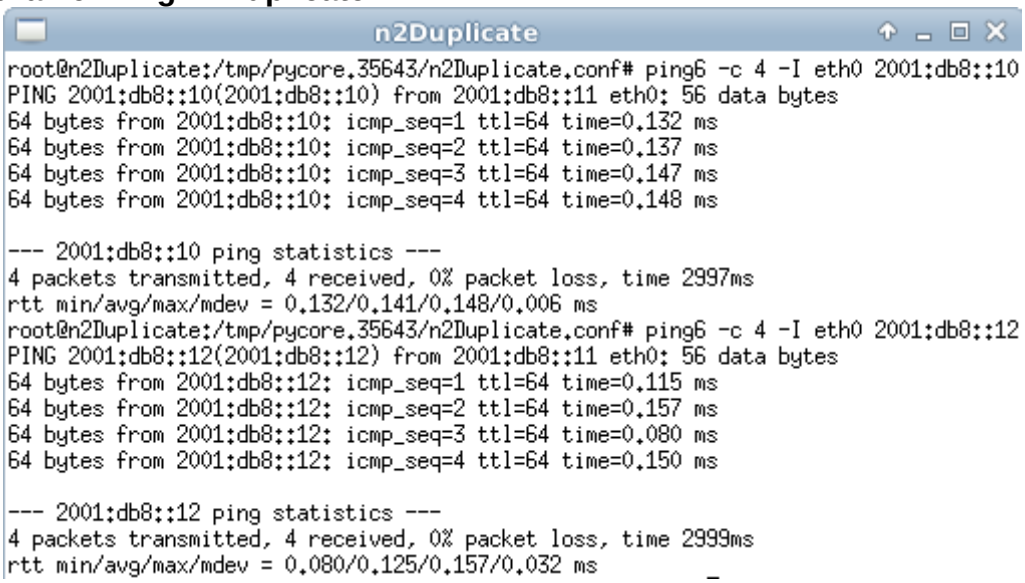
Fonte: Próprio Autor.

No terminal n2Duplicate, executar os comandos:

```
#ping6 -c 4 -I eth0 2001:db8::10
#ping6 -c 4 -I eth0 2001:db8::12
```

Esses comandos testam a conexão do n2Duplicate com o n1Original e n3Host. O resultado obtido é a conexão ativa, conforme visto na Figura 16:

Figura 16: Ping n2Duplicate



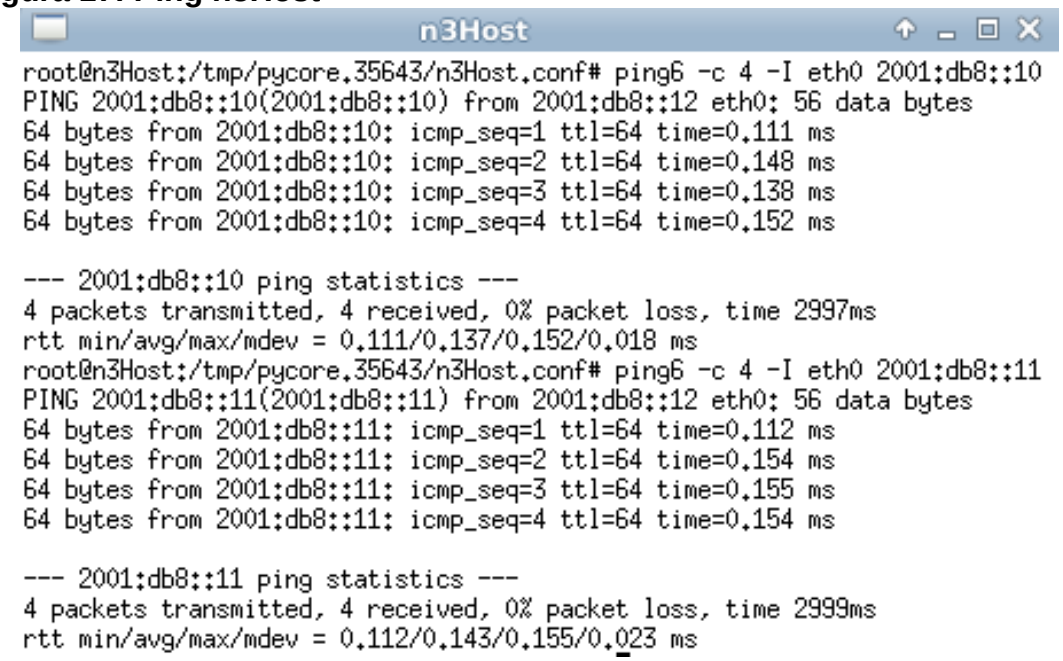
Fonte: Próprio Autor.

No terminal n3Host, executar os comandos:

```
#ping6 -c 4 -I eth0 2001:db8::10
#ping6 -c 4 -I eth0 2001:db8::11
```

Esses comandos testam a conexão do n3Host com o n2Duplicate e n1Original. .O resultado obtido é a conexão ativa, conforme visto na Figura 17:

Figura 17: Ping n3Host



Fonte: Próprio Autor.

Pausar e salvar as mensagens capturadas pelo Wireshark em todos os hosts, salvos com os nomes de Pingn1, Pingn2, Pingn3, conforme o Apêndices F, G e H respectivamente, os arquivos gerados contêm:

- *Neighbor Solicitation:* Quando o comando *ping* é realizado, o *host* de origem envia uma mensagem NS para o vizinho pedindo o endereço dele.
- *Neighbor Advertisement:* Quando a mensagem NS chega no destino, o host responde com uma mensagem NA avisando seu endereço. Assim as próximas mensagens são trocadas sem a necessidade do multicast. Criando uma conexão entre si.
- *Echo (ping) request:* Após a mensagem NS obter a resposta NA a conexão é estabelecida, e o E*cho Request* é um comando de requisição

enviado pelo *host* de origem no comando ping que pergunta se o host de destino está ativo.

- *Echo (ping) reply:* é o comando de resposta do *ping,* que responde positivamente que ele está ativo.

Caso não seja recebido um *Echo Reply* a conexão do host de destino não está ativa.

Após a análise das mensagens é necessário abrir novamente o Wireshark na n1Original e n2Duplicate.

- Abrir o terminal n2Duplicate, executar os comandos:

```
#ip addr del 2001:db8::11/64 dev eth0
#ip addr add 2001:db8::10/64 dev eth0
#ifconfig eth0
#ip addr show dev eth0
```

O resultado será igual ao da Figura 18:

Figura 18: Duplicação

Fonte: Próprio Autor.

O comando **#ip addr del 2001:db8::11/64 dev eth0** deleta o endereço indicado da placa de rede.

O comando **#ip addr add 2001:db8::10/64 dev eth0** atribui o endereço

indicado na placa de rede.

Nesse caso, é deletado o próprio endereço da n2Duplicate e é atribuído o endereço da n1Original, gerando assim propositalmente uma duplicação de endereço na rede.

O comando **#ifconfig eth0** mostra a nova configuração da rede.

E o comando **#ip addr show dev eth0** verifica o endereço atribuído e mostra que a tentativa de atribuição de endereço foi falha.

- No terminal do n3Host:

```
#ping6 –c 4 –I eth0 2001:db8::10
```

Pausar o Wireshark das máquinas n1Original e n2Duplicate e salvar o arquivo.

No host n1Original é gerado o arquivo do Apêndice I, onde é possível verificar na mensagem nº 5 “Neighbor Solicitation for 2001:db8::10” ocorre na atribuição do novo endereço na n2Duplicate, que manda uma NS que verifica a solicitação do novo endereço. Como o endereço é duplicado, o n1Original recebe a NS e envia uma NA.

E na mensagem nº 6 “Neighbor Advertisement 2001:db8::10 (ovr) is at 00:00:00:aa:00:00” ocorre quando o IP 2001:db8::10 responde a NS com uma NA avisando que o IP está sendo utilizado.

As mensagens nº 7 a nº 16 estão relacionadas ao ping que o n3Host realizou.

E no host n2Duplicate é gerado o arquivo do Apêndice J, onde é possível verificar na mensagem nº 5 “Neighbor Solicitation for 2001:db8::10”, a solicitação do endereço 2001:db8::10.

Na mensagem nº 6 “Neighbor Advertisement 2001:db8::10 (ovr) is at 00:00:00:aa:00:00”, o recebimento da NA avisando que o endereço já esta em uso.

E na mensagem nº 7 Neighbor Solicitation for 2001:db8::10 from 00:00:00:aa:00:02”, o recebimento da notificação do n3Host para pedir o endereço para o *ping*, mas ele não envia uma resposta, pois o endereço dele é

invalido.

O objetivo dessa simulação é tornar mais claro o entendimento da função de Detecção de Endereços Duplicados na rede IPv6.

3.2 ATAQUE DOS ATRAVÉS DO DAD

Nesse trabalho será realizado um ataque de Negação de Serviço através do NDP no ICMPv6, utilizando a função DAD. Para isso será utilizado o sistema operacional Linux em uma máquina virtual.

De acordo com Laureano (2006), “uma máquina virtual (Virtual Machine – VM) pode ser definida como uma duplicata eficiente e isolada de uma máquina real”, essa máquina virtual é utilizada em um emulador, que segundo Péricas e Raitz (2005), “é um software que simula um computador real” como é o caso do Virtual Box.

Para desenvolver o ataque será utilizado o CORE, um software que emula reder. Para a equipe do IPv6.br (2015), CORE é “um ambiente gráfico, que permitirá a você experimentar diversas topologias e configurações de redes diferentes”.

E a coleta de pacotes será realizada pela ferramenta Wireshark, que é um analisador de protocolos, pois permite ver o que acontece na rede em um nível microscópico.

Para a detecção de atividade maliciosa será utilizado o NDPmon que de acordo com a equipe do IPv6.br (2015) é “uma ferramenta para a geração de logs e registros de comportamentos suspeitos no enlace, será utilizada para auxiliar na detecção de ataques e na identificação de máquinas atacantes”.

THC-IPv6 é uma ferramenta criada pelo The Hackers Choice em 2006, e desde então sofre *updates* e melhorias no serviço oferecido. Essa ferramenta traz um série de instrumentos de invasão através do IPv6 e do ICMPv6.

Na rede IPv6 O NDP utiliza o *multicast solicited-node* para resolver endereços MAC e IP de um host. Assim somente as interfaces do grupo pode examinar o pacote.

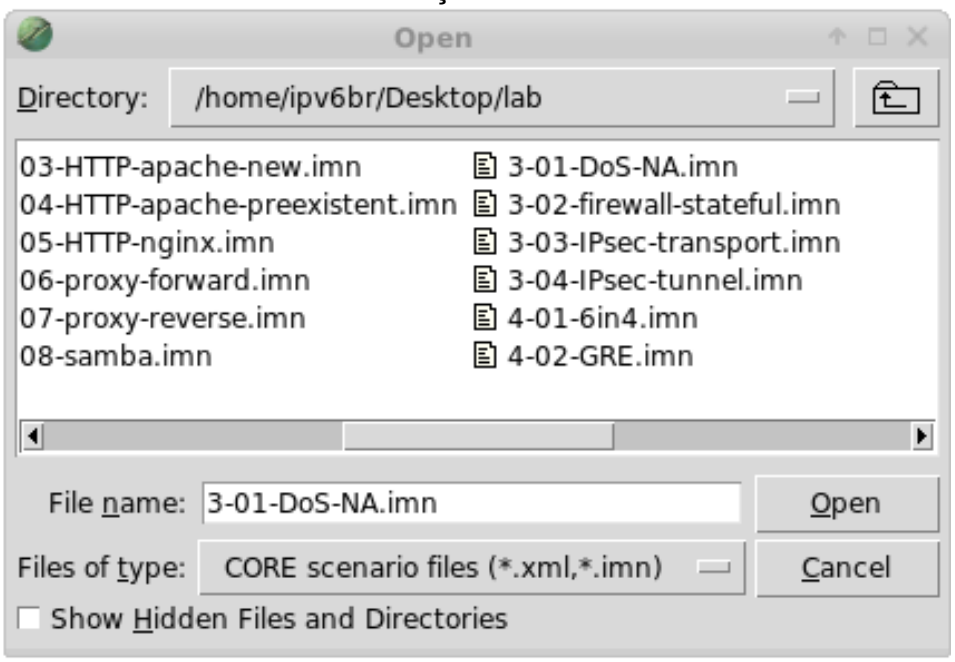
O ataque DoS utilizando o NDP na funcionalidade de DAD (*Duplicate Address Detection*), que verifica a duplicação de endereços é realizado da

seguinte forma: quando um *host* se conecta a rede ele envia um mensagem *multicast* do tipo NS (*Neighbor Solicitation*) para confirmar se o endereço IP atribuído não está duplicado na rede, se o endereço já estiver em uso é enviado uma mensagem NA (*Neighbor Advertisement)* informando que aquele endereço já está sendo utilizado no nó, portanto ele não pode se conectar a rede, sendo assim necessário pedir outro endereço IP e confirmar se o endereço recebido não está duplicado com uma mensagem NS. O ataque acontece quando um *host* intercepta e reponde todas as mensagens NS com uma NA, impossibilitando os *hosts* de obterem um endereço válido para se comunicar com a rede.

3.1.2 Prática Ataque

Para o ataque Dos ao DAD, foi utilizada a topologia **3-01-Dos-NA.imn** (**Erro! Fonte de referência não encontrada.**).

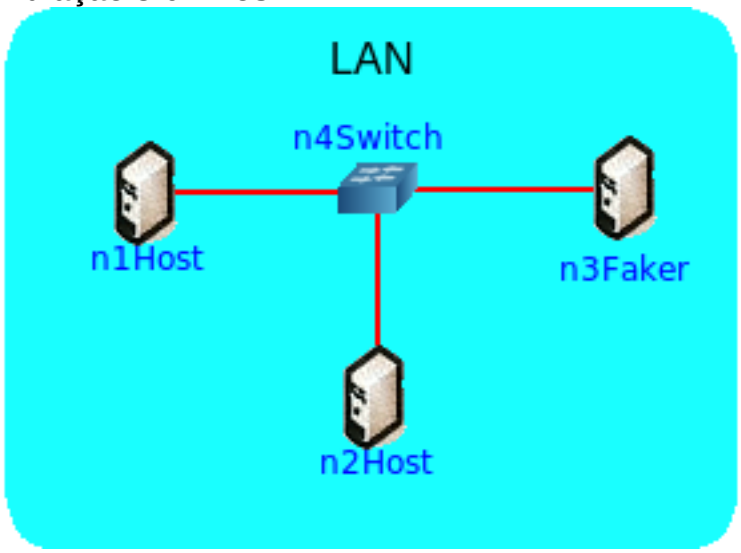
Figura 19: Abrir Cenário da Simulação



Fonte: Próprio Autor.

A simulação que pode ser vista na Figura 20, contém o mínimo necessário para a realização do ataque

Figura 20: Simulação 3-01-Dos-NA.imn



Fonte: Próprio Autor.

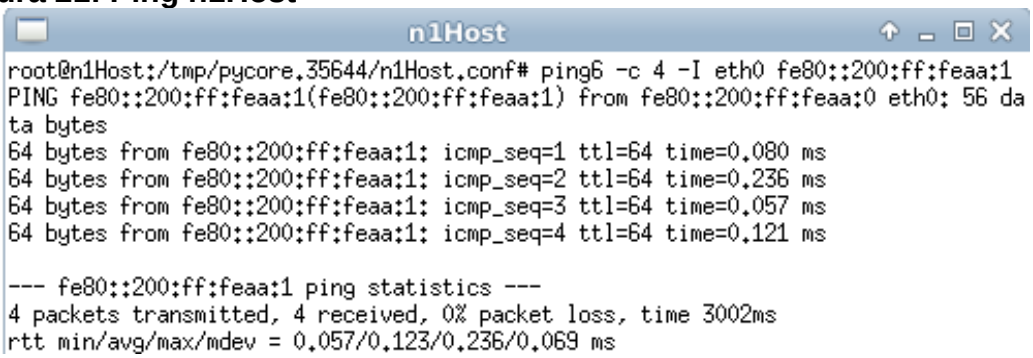
Configuração de rede:

- n1Host: fe80::200:fe:feaa:0
- n2Host: fe80::200:fe:feaa:1
- n3Faker: fe80::200:fe:feaa:2
- No terminal do n1Host é executado o comando:

```
#ping6 – c 4 –I eth0 fe80::200:ff:feaa:1
```

E o resultado do teste de conexão com o n2Host pode ser observado a seguir na Figura 21, o resultado obtido é a conexão ativa.

Figura 21: Ping n1Host



Fonte: Próprio Autor.

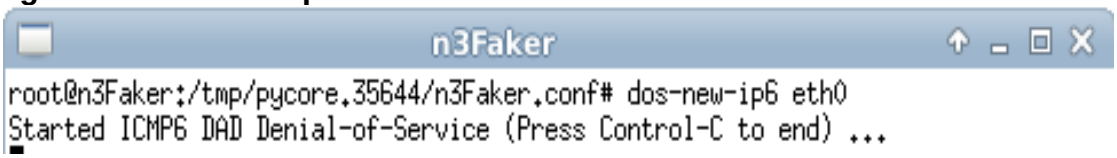
- No terminal do n3Faker é necessário abrir o Wireshark e após isso é necessário executar o comando:

```
#dos-new-ip6  eth0
```

Esse comando faz parte da aplicação THC-IPv6, que executa ataques ao IPv6, nesse caso o n3Faker vai emitir o comando com o objetivo de se passar pelo roteador e interceptar todas as NS e responder com uma NA, fazendo assim com que os hosts não consiga terminar suas configurações de rede, pois acusará duplicidade no endereço em todas as tentativas.

A Figura 22 demonstra a execução do comando.

Figura 22: dos-new-ip6 eth0



Fonte: Próprio Autor.

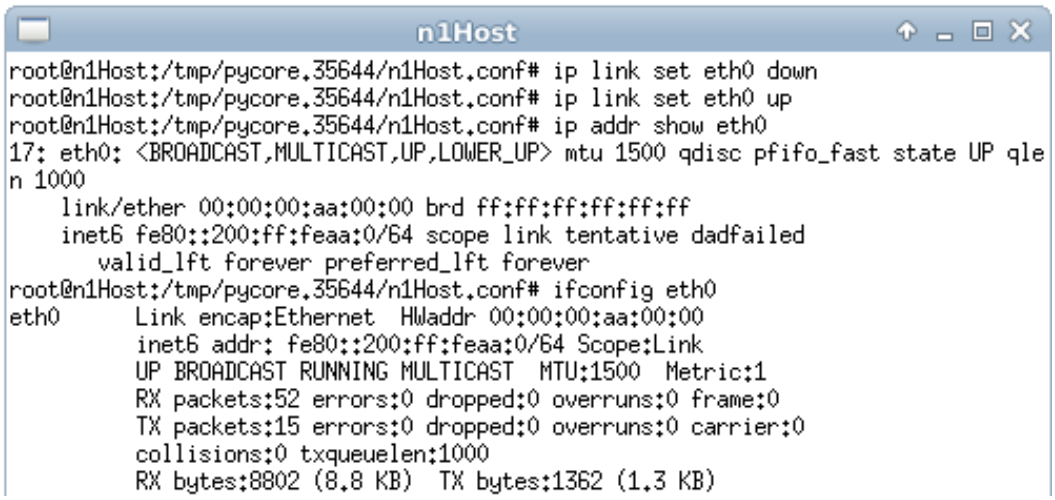
Após a execução do ataque, efetuaremos os seguintes comandos.

- No terminal n1Host:

```
#ip link set eth0 down
#ip link set eth0 up
#ip addr show eth0
#ifconfig eth0
#ping6 – c 4 –I eth0 fe80::200:ff:feaa:1
```

E o resultado pode ser observado na Figura 23:

Figura 23: Configuração Placa de Rede



Fonte: Próprio Autor.

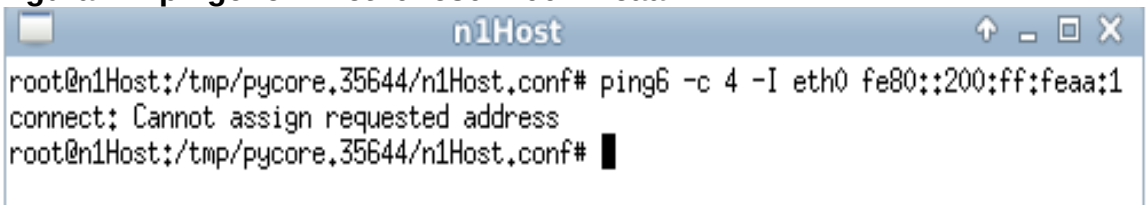
O comando **ip link set eth0 down** vai retirar as configurações da placa de rede, e logo em seguida o comando **ip link set eth0 up** vai obrigar a placa de rede a buscar novas configurações, forçando assim a atribuição de um novo endereço IP para a mesma, quando isso acontece ele vai mandar uma mensagem em *multicast solicited-node* para os nós da rede para verificar se o endereço não está duplicado.

Com o comando **ip addr show eth0** vai mostrar o seguinte erro **link tentative dadfailed** mostrando que foi impossível atribuir um endereço IP válido para a placa de rede.

E o comando **ifconfig eth0** demonstra que a placa de rede foi configurada com aquele endereço e as configurações de rede, e por isso é mais confiável utilizar o comando ip para verificar as configurações da placa de rede.

E para confirmar que a máquina não conseguiu terminar suas configurações de rede é executado o comando **ping6 –c 4 –I eth0 fe80::200:ff:feaa:1** para testar sua conectividade com o n2Host, conforme a Figura 24.

Figura 24: ping6 -c 4 -I eth0 fe80::200:ff:feaa:1

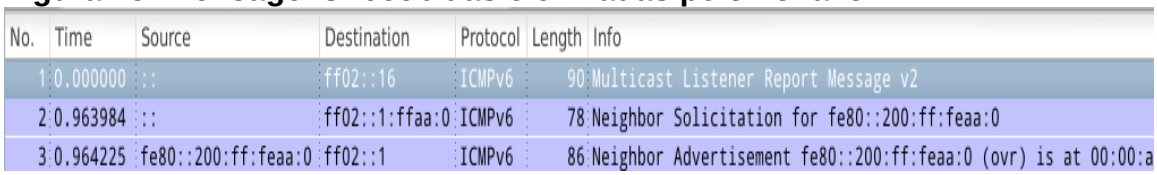


Fonte: Próprio Autor.

Após essas etapas no terminal do n3Faker que está rodando a aplicação do ataque, é executado o comando **Ctrl + C** para parar a aplicação.

Encerrar os terminais e salvar o arquivo gerado pelo wireshark conforme o Apêndice K para analisar as mensagens recebidas e enviadas pelo n3Faker, o atacante da rede e encerrar a simulação conforme o Apêndice B.

Figura 25: Mensagens recebidas e enviadas pelo n3Faker



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
2	0.963984	::	ff02::1:ffaa:0	ICMPv6	78	Neighbor Solicitation for fe80::200:ff:feaa:0
3	0.964225	fe80::200:ff:feaa:0	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::200:ff:feaa:0 (ovr) is at 00:00:a

Fonte: Próprio Autor.

Como pode ser visto na Figura 25, a mensagem nº 2 “Neighbor Advertisement” é recebida pelo n3Faker, através da mensagem multicast. E na mensagem nº 3 o n3Faker responde a NS com uma NA, impedindo o n1Host de encerrar suas configurações de rede, tornando-o inacessível.

3.2.2 Prática Detecção

Após o ataque DoS apresentaremos uma forma de detecção do ataque na rede. Para isso utilizaremos o mesmo cenário utilizado para o ataque DoS.

No terminar do n2Host executar o comando que abre o programa NDP Mon conforme a

- Figura 26:

```
#ndpmon –i eth0 -v
```

Figura 26: Inicialização NDP Mon

Fonte: Próprio Autor.

- No terminal do n3Faker é executado o comando do ataque que iniciará conforme a Figura 27 :

```
#dos-new-ip6 eth0
```

Figura 27: Iniciar Ataque

Fonte: Próprio Autor.

O comando **ndpmon –i eth0 -v** faz com que inicie a aplicação NDP Mon. Após a execução da ferramenta ela passa a ouvir toda a rede.

- No terminar do n1Host vão ser executados os comandos para derrubar e subir a rede novamente:

```
#ip link set eth0 down
#ip link set eth0 up
#ip addr show eth0
```

Gerando o erro **link tentative dadfailed** conforme pode ser visto na Figura 28.

Figura 28: Erro

Fonte: Próprio Autor.

Com o ataque efetuado é possível voltar no n2Host e verificar que a ferramenta identificou o ataque.

A ferramenta identifica uma mensagem NS na rede, e logo após identifica uma mensagem NA gerando assim o alerta de ataque DAD DoS.

Nas configurações do NDP Mon é possível mandar o alerta para o email do administrador da rede.

A Figura 29, mostra a ferramenta NDP Mon detectando o ataque DoS efetuado pelo n3Faker.

Figura 29: Detecção do Ataque

Fonte: Próprio Autor.

4 CONSIDERAÇÕES FINAIS

A mudança de versão do IP foi necessária por causa do esgotamento de endereços IPv4. A nova versão trás como principais diferenças o tamanho fixo e a diminuição na quantidade de campos do datagrama, a inutilização do NAT e o suporte a mecanismos de segurança na implementação do protocolo.

As funções de controle de erro, resolução de endeço, mapeamento de endereços físicos e lógicos, e gerenciamento do grupo *multicast* é realizado pelo ICMPv6, em conjunto com outros protocolos como é o caso do NDP, que tem como objetivo identificar e conhecer características da vizinhança, e utiliza cinco tipos de mensagens do ICMPv6 para exercer suas funções. Ou seja, com a mudança do IPv4 para o IPv6, os outros protocolos de comunicação da internet também mudaram e foram otimizados, como é o caso do ICMPv6 e do NDP, que trabalham juntos para diminuir a quantidade de protocolos existentes no IPv4.

O IPv6 é um protocolo mais seguro em relação ao IPv4, pois as mudanças corrigiram as vulnerabilidades já conhecidas da versão quatro, e criaram o IPSec com o objetivo de aumentar a segurança na rede, porém o IPSec só provê segurança para o protocolo IPv6, os outros protocolos não são abordados em seus critérios de segurança, fazendo com que novas vulnerabilidades fossem criadas e descobertas.

Tendo como o principal foco de vulnerabilidades o ICMPv6 e os protocolos que utilizam suas mensagens. No ICMPv4 era possível bloquear o protocolo direto no *firewall*, pois a sua função era realizar o diagnostico na rede, porém na nova versão ele aborda diversas função, sendo assim impossível bloqueá-lo totalmente.

O NDP possui quatro vulnerabilidades amplamente conhecidas, envenenamento na tabela de vizinhança, falsificadores de roteadores e prefixos, varredura de endereços e o ataque à detecção de endereços duplicados.

O ataque de negação de serviço, tem o objetivo atingir o princípio de disponibilidade da informação, um dos pilares da segurança da informação, no caso do ataque DoS através da função de detecção de endereços duplicados,

o objetivo do ataque é impossibilitar os *hosts* se conectarem na rede, tornando necessário a correção manual das configurações da placa de rede após a identificação do ataque a rede, a ferramenta NDP Mon ajuda na identificação desse e de outros ataques ligados ao protocolo NDP.

Portanto, apesar do IPv6 ser amplamente conhecido como um protocolo mais seguro, não o isenta de vulnerabilidades que possam ser exploradas. Com isso a escolha do presente trabalho teve como objetivo explorar uma das vulnerabilidades do NDP, por meio da demonstração de um ataque de negação de serviço através da função de detecção de endereços duplicados e a apresentação de uma ferramenta que detecta o ataque gerando um alerta na rede para o administrador da mesma.

O fato é que o uso do IPv6 é necessário por causa do esgotamento de endereços disponíveis na sua versão anterior. Contudo ainda há poucos profissionais que possuem o conhecimento adequado para implementar o protocolo e as consequências dessa mudança na rede de forma segura.

Este trabalho não só apresentou o resultado de um levantamento bibliográfico sobre possíveis vulnerabilidades no IPv6, como demonstrou o ataque DoS utilizando o NDP, como forma de incrementar o conhecimento dos profissionais de T.I., e apresentar a importância do estudo e prática de laboratórios de redes IPv6 para identificar vulnerabilidade e implementar detecções e correções, tornando as redes mais seguras.

Espera-se que este trabalho possa contribuir na realização de futuros trabalhos, tendo como principais temas a implementação da RFC 4890, que faz recomendações de filtragens dos pacotes ICMPv6, no firewall, e do protocolo SEND, uma extensão mais segura do NDP, descrito pela RFC 4861 que usa recursos criptográficos para prover mais segurança.

REFERÊNCIAS BIBLIOGRÁFICAS

BEZERRA, Romildo. **A Camada de Transporte.** Bahia: CEFET, 2008, p. 05. Disponível em: < http://www2.ufba.br/~romildo/downloads/ifba/transporte.pdf > Acesso em: 22 maio 2016.

BRITO, Samuel Henrique Bucke. **Webinar:** IPv6. Cisco Networking Academy: 2013.

BRITO, Samuel Henrique Bucke. IPv6: O Novo Protocolo da Internet. São Paulo: Editora Novatec, 2013, p. 208. ISNB 978857522374.

BUGALLO, Angela; BARROS, Márcio; TORRES, Waldeck. **Introdução ao DHCP.** Rede Nacional de Ensino e Pesquisa, 1999. Disponível em: < https://memoria.rnp.br/newsgen/9911/dhcp.html > Acesso em: 28 maio 2016.

CAVALHIERI, Luis Fernando. **Estudo do padrão IPv6 e sua Comparação com o IPv4.** Marília, 2006, p. 63. Disponível em: < http://aberto.univem.edu.br/bitstream/handle/11077/421/Estudo%20do%20Padr%C3%A3o%20IPv6%20e%20sua%20compara%C3%A7%C3%A3o%20com%20o%20IPv4.pdf?sequence=1 > Acesso em: 14 abr. 2016.

CANTÚ, Evandro. **Redes de Computadores e a Internet**. Santa Catarina: IFSP, 2010, p. 87. Disponível em: < http://wiki.sj.ifsc.edu.br/wiki/images/2/2d/ApostilaRedes2010.pdf > Acesso em: 30 mar. 2016.

DANTAS, M. **Tecnologias de Redes Comunicação e Computadores**. 1ª Ed. Rio de Janeiro: Editora Axcel Books, 2002, p. 344. ISBN 8573231696..

CARVALHO, T. C. M. B. **Arquitetura de redes de computadores OSI e TCP/IP.** 2ª Ed. Rev. Ampl. São Paulo: Editora Makron Books, 1997. Volume 1. ISBN 9788534606943.

Equipe IPv6.br. **Laborátorio de IPv6.** 1º Ed. São Paulo: Editora Novatec, 2015, p. ISBN 9788575224182.

FERAZ, Tatiana Lopes; ALBUQUERQUE, Marcelo Portes; ALBUQUERQUE, Márcio Portes. **Introdução ao Ping e Traceroute**. Centro Brasileiro de Pesquisas Físicas. Acervo de Notas Técnicas nº CBPF-NT/02, publicado em: 26 de novembro de 2002. Disponível em: < http://www.rederio.br/downloads/pdf/nt01002.pdf > Acesso em: 21 ago. 2016.

FONTES, Edison. **Segurança da Informação: o usuário faz a diferença.** 1ª Ed, São Paulo: Editora Saraiva, 2006. ISBN 8502054422.

GORITO, Europe Moraes. **Endereçamento no IPv6.** URFJ (Universidade Federal do Rio de Janeiro), 2014. Disponível em: < http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2014_2/europe/ > Acesso em: 14 out. 2016.

GUPTA, M.; LASALLE, P.; PARIHAR, M; SCRINGER. R. **TCP/IP A Bíblia.** Tradução: Furmankiewiez, Doweware Traduções. Editora Campus, 2002, p. 664. ISBN 8535209220.

IANA. **Internet Assigned Numbers Authority.** Disponível em: < http://www.iana.org/ > Acesso em 15 jun. 2016.

IPV6. **Internet Protocol versão 6 Brasil**. Disponível em: < http://www.ipv6.br > Acesso em 20 ago. 2016

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet**: uma abordagem top-down. 3. Ed. São Paulo: Editora Person Addison Wesley, 2005, p. 680. ISNB 8588639181.

KUROSE, James F.; ROSS, Keith W**. Redes de Computadores e a Internet:**

uma abordagem top-down. 5. ed. São Paulo: Person Addison Wesley, Brasil, 2010, p. 576. ISNB 9788588639973.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. 5º Ed. São Paulo: Editora Atlas, 2003, p. 320. ISBN 8522433976.

LAUREANO, Marcos. **Máquinas Virtuais e Emuladores: Conceito Técnicas e Aplicações**. 1ª Ed. São Paulo: Editora Novatec, 2006, p.184. ISBN 857522098-5

LISBOA, Gilvânia dos Santos; SANTIAGO, Hewerton Luis P., **Segurança de Sistemas de Informação: O Contexto da Segurança dos Sistemas de Informação.** Faculdade Atenas, Núcleo de Iniciação Científica 2011. Disponível em: < http://www.atenas.edu.br/faculdade/arquivos/NucleoIniciacaoCiencia/REVISTAS/REVIST2011/6.pdf> Acesso em 24 set. 2016.

MACHADO, Weily Toro. **O Estudo de Caso como Método de Pesquisa Científica**. Revista Online Portal da Classe Contábil, publicado em 09 de fevereiro de 2006. Disponível em: < http://www.classecontabil.com.br/artigos/o-estudo-de-caso-como-metodo-de-pesquisa-cientifica > Acesso em 27 set. 2016.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Metodologia do trabalho científico**. 4ª Ed. São Paulo: Editora Atlas, 1992, p. 214. ISBN 8522408599.

MENDES, Douglas Rocha. **Redes de Computadores: Teoria e Prática.** 2ª Ed. São Paulo: Editora Novatec, 2015, p. 528. ISBN 8575223682.

MINAYO, M.C.S. **O desafio do conhecimento**: pesquisa qualitativa em saúde. 3ª Ed. São Paulo: Editora Hucitec, 2007, p. 406. ISBN 8527101815.

NIC. **Núcleo de Informação e Coordenação do Ponto BR.** Disponível em: < http://www.nic.br > Acesso em 20 ago. 2016.

PÉRICAS, Francisco Adell; RAITZ, Luciano. **Utilização de Máquinas Virtuais para Implantar um Mecanismo Transparente de Detecção de Intrusão em Servidor Web.** Universidade Regional de Blumenau, 2005. Disponível em: < http://www.inf.furb.br/~pericas/publicacoes/VMIDS.pdf > Acesso em 26 set. 2016.

PRADO, Edmir; SOUZA, Cesar Alexandre. **Fundamentos de sistemas de informação**. 1ª Ed. São Paulo: Editora Elsevier, 2014, p. 312. ISBN 9788535274356.

RFC. **Request for Comments.** Internet Society e Association Management Solutions. Disponível em: < https://www.ietf.org/rfc.html Acesso em: 30 fev. 2016.

ROCHA, Paulo Cesar Cardoso. **Segurança da Informação: Uma questão não apenas tecnológica.** Universidade de Brasília, 2008. Disponível em: < http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/paulo_cesar.pdf > Acesso em 24 set. 2016.

SANTOS, Rodrigo Regis; MOREIRAS, Antonio; REIS, Eduardo Ascenço; ROCHA, Ailton Soares. **Curso IPv6 Básico**. Núcleo de Informação e Coordenação do ponto BR, São Paulo, 2010, p. 314.

SILVEIRA, Cláudio Discacciati. **Protocolo IPV6: a nova geração do protocolo IP.** UNIPAC (Universidade Presidente Antônio Carlos Faculdade de Ciência da Computação e Comunicação Social de Barbacena), 2004. Disponível em: < http://www.unipac.br/site/bb/tcc/tcc-1c5e688351d676d58d5660e66cca7f7f.pdf > Acesso em: 14 out. 2016.

TANENBAUM, Andrew S**. Redes de Computadores**. Tradução da 4rd. Ed. em inglês. Editora Elsevier. 2003, p. 632. ISBN 8535211853.

TARTUCE, T. J. A. **Métodos de pesquisa.** Fortaleza: UNICE – Ensino Superior, 2006. Apostila.

THC-IPV6. **Versão v3.0**, atualizado em 22 de janeiro de 2016. Disponível em: < https://www.thc.org/thc-ipv6/ > Acesso em 27 set. 2016

UIT. **União Internacional de Telecomunicações.** Nações Unidas no Brasil. Disponível em: < https://nacoesunidas.org/agencia/uit/ > Acesso em 27 set. 2016.

APÊNDICE A – Instalação e Iniciação da Máquina Virtual

1. Download do Virtual Box:

Fazer o download do Vitural Box no site: https://www.virtualbox.org/wiki/Downloads.

Clicar em **VirtualBox 5.1.6 for Windows hosts -> x86/amd64** conforme a **Erro! Fonte de referência não encontrada.**.

Figura 30: Download Virtual Box

Fonte: Próprio Autor.

Após o download terminar clicar no aplicativo, após abrir, clicar em **executar**.

2. Instalação:

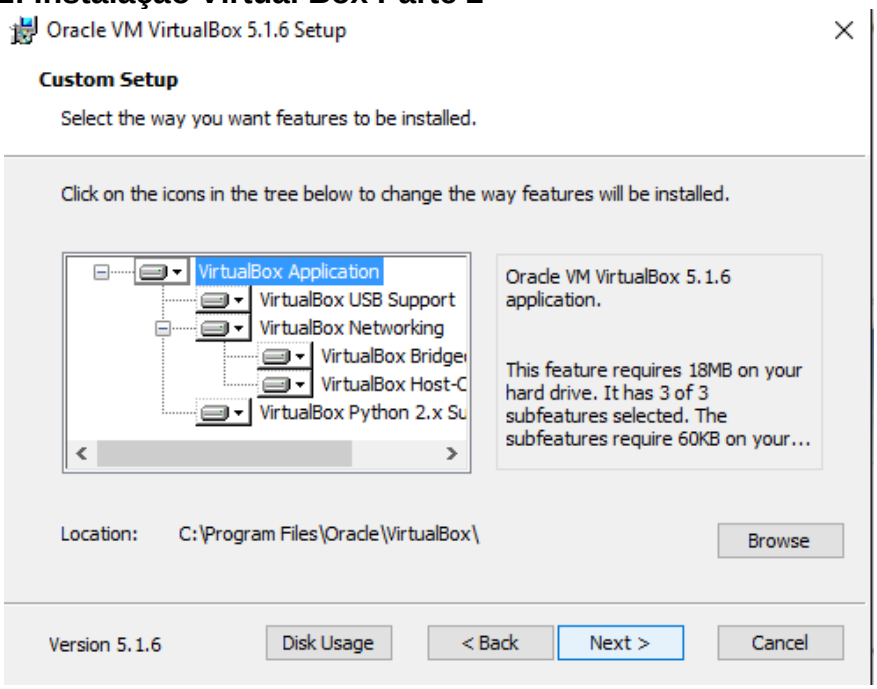
Após executar o arquivo baixado, abrirá uma tela conforme a Figura 31. Clicar em **next.**

Figura 31: Instalação Virtual Box Parte 1

Fonte: Próprio Autor.

Na próxima tela (Figura 32) clicar em **next**.

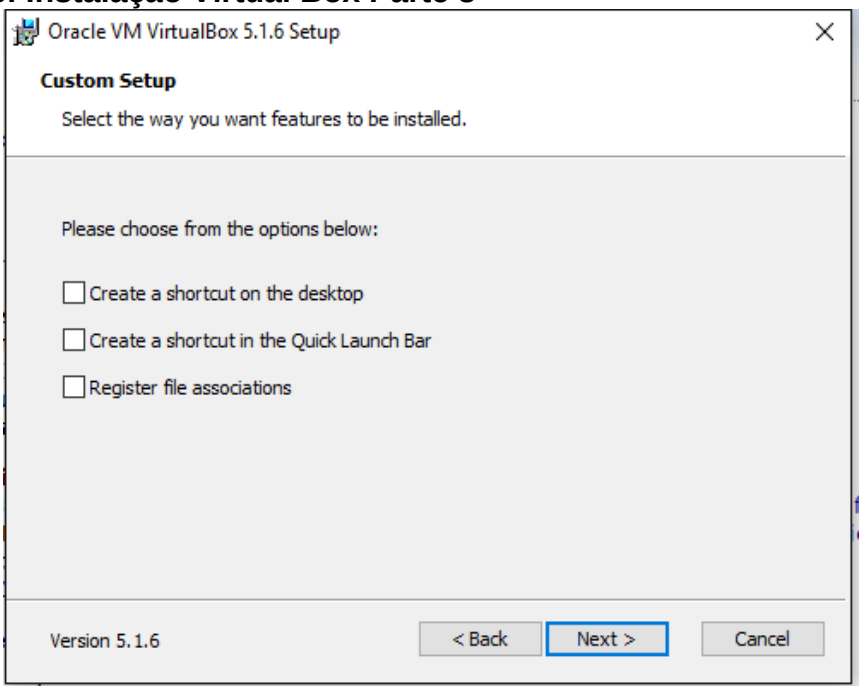
Figura 32: Instalação Virtual Box Parte 2



Fonte: Próprio Autor.

Na tela seguinte desmarcar as opções das três caixas e clicar em **next**, conforme a Figura 33.

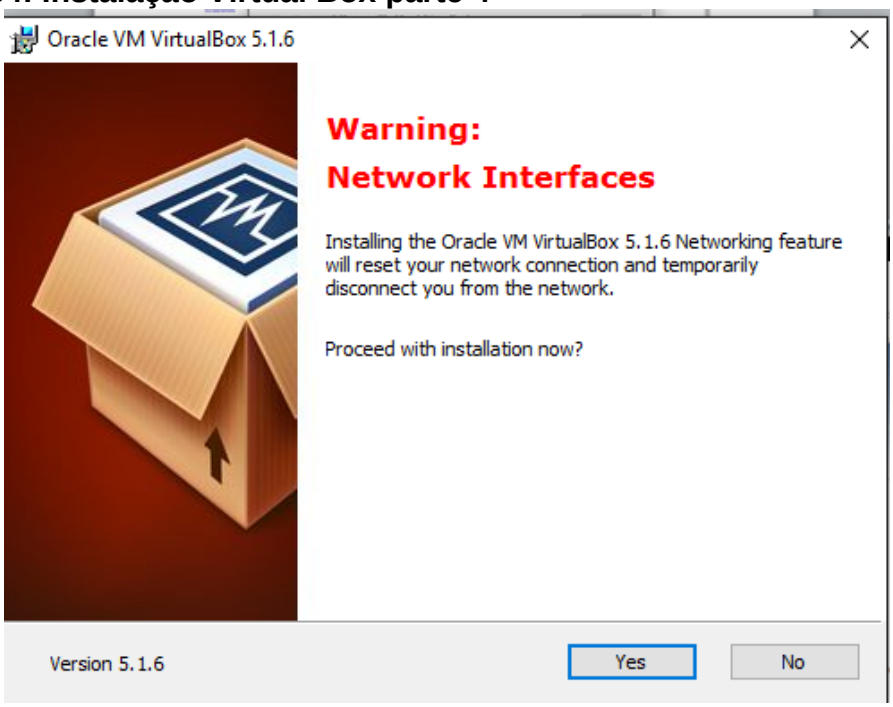
Figura 33: Instalação Virtual Box Parte 3



Fonte: Próprio Autor.

Clicar em **Yes** para aceitar o aviso, conforme a Figura 34.

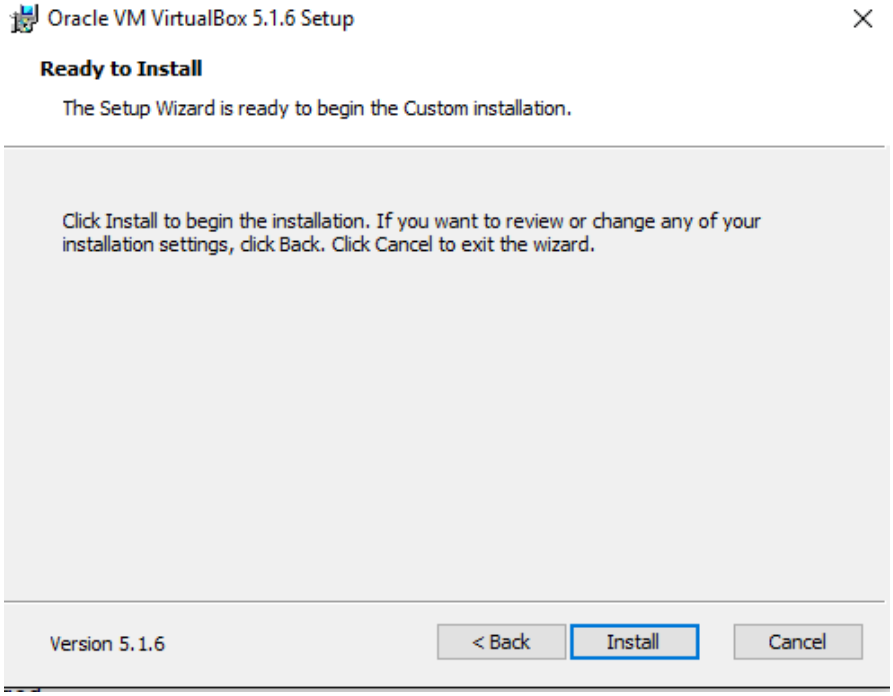
Figura 34: Instalação Virtual Box parte 4



Fonte: Próprio Autor.

E por último clicar em **Install** para completar a instalação do Virtual Box (Figura 35).

Figura 35: Instalação Virtual Box parte 5



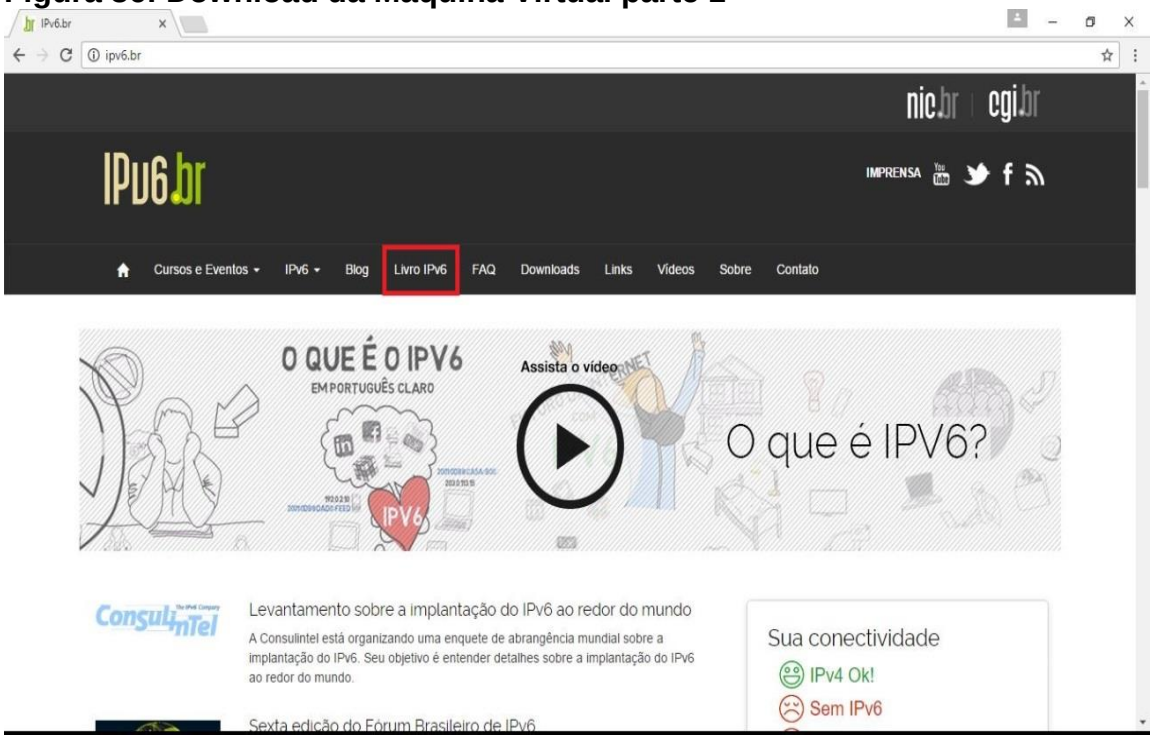
Fonte: Próprio Autor.

3. Download Máquina Virtual do IPv6.br.

Para o download é necessário acessar o site ipv6.br e seguir os passos a seguir, na Figura 36 clicar em **Livro IPv6** destacado em vermelho. E na Figura 37 clicar em **Download VM (.ova)** destacado em vermelho.

O arquivo do download aparecerá no canto inferior esquerdo, após o termino clicar na seta na lateral do arquivo e selecionar a opção **Mostrar na Pasta.** E copiar o arquivo para dentro da pasta que deseja.

Figura 36: Download da Máquina Virtual parte 1



Fonte: Próprio Autor.

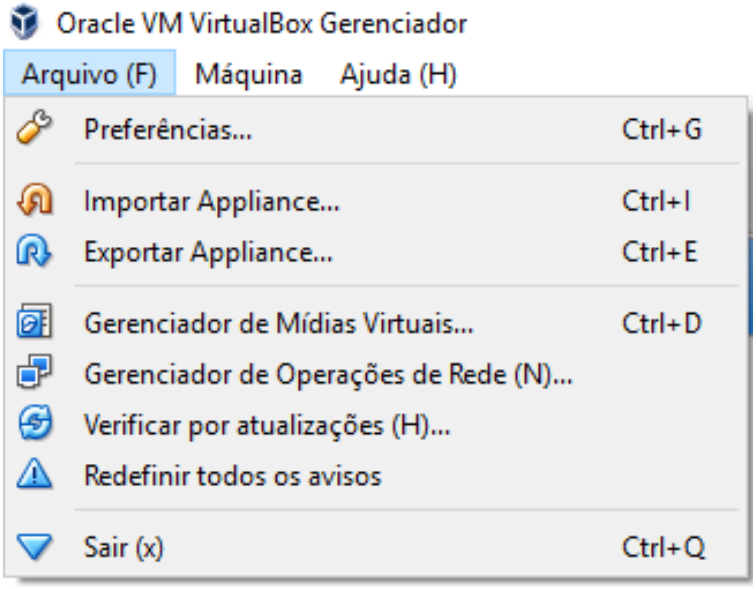
Figura 37: Download Máquina Virtual parte 2

Fonte: Próprio Autor.

4. Inclução da Máquina Virtual no Virtual Box.

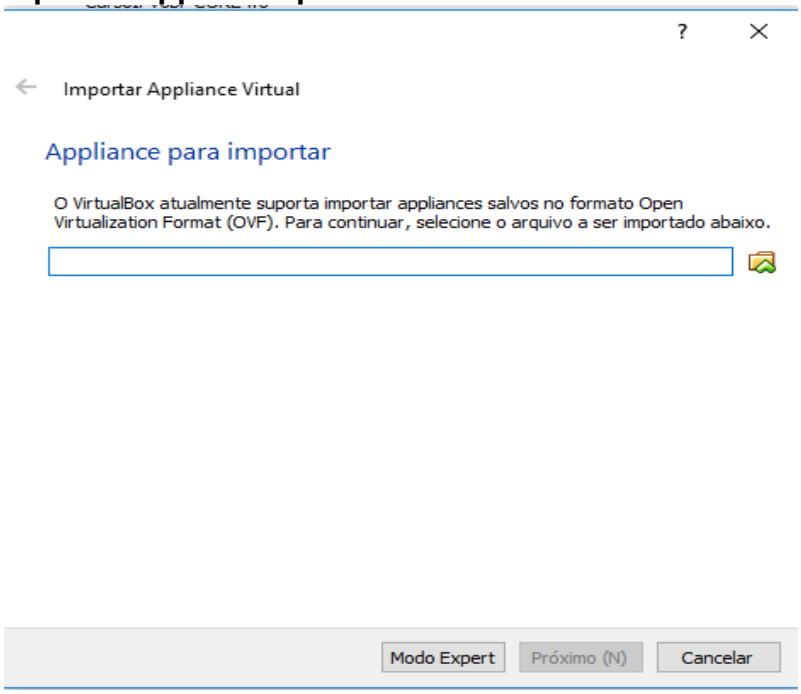
Abrir o Virtual Boc com duplo clique, e clicar em Arquivo e Importar Appliance, conforme a Figura 38.

Figura 38: Importar Appliance parte 1



Fonte: Próprio Autor.

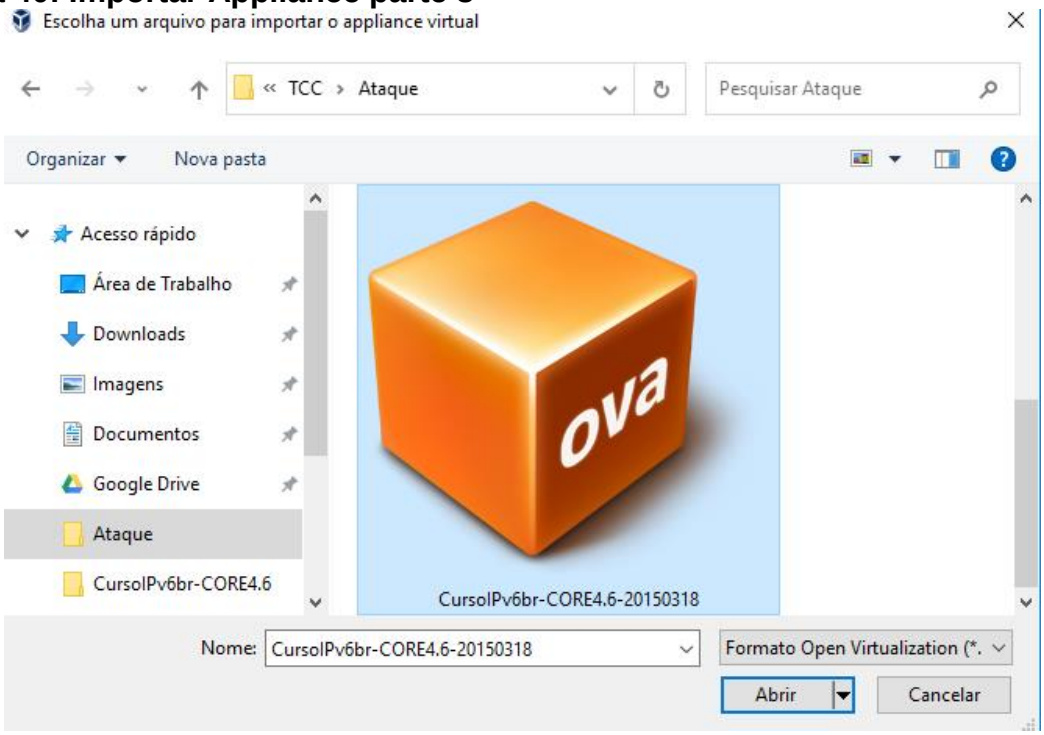
Figura 39: Importar Appliance parte 2



Fonte: Próprio Autor.

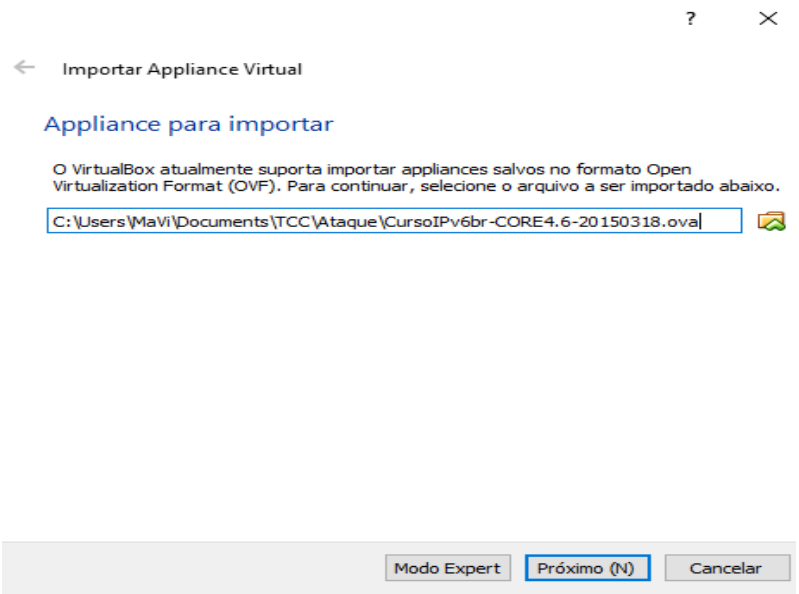
Clicar na pasta amarela igual ao que aparece na Figura 39 e escolher a máquina virtual que foi baixada **CursoIPv6br-CORE4.6-20150318** e clicar em **Abrir**, conforme a Figura 40. Após a seleção do arquivo é só clicar em **Próximo**, igual a Figura 41.

Figura 40: Importar Appliance parte 3



Fonte: Próprio Autor.

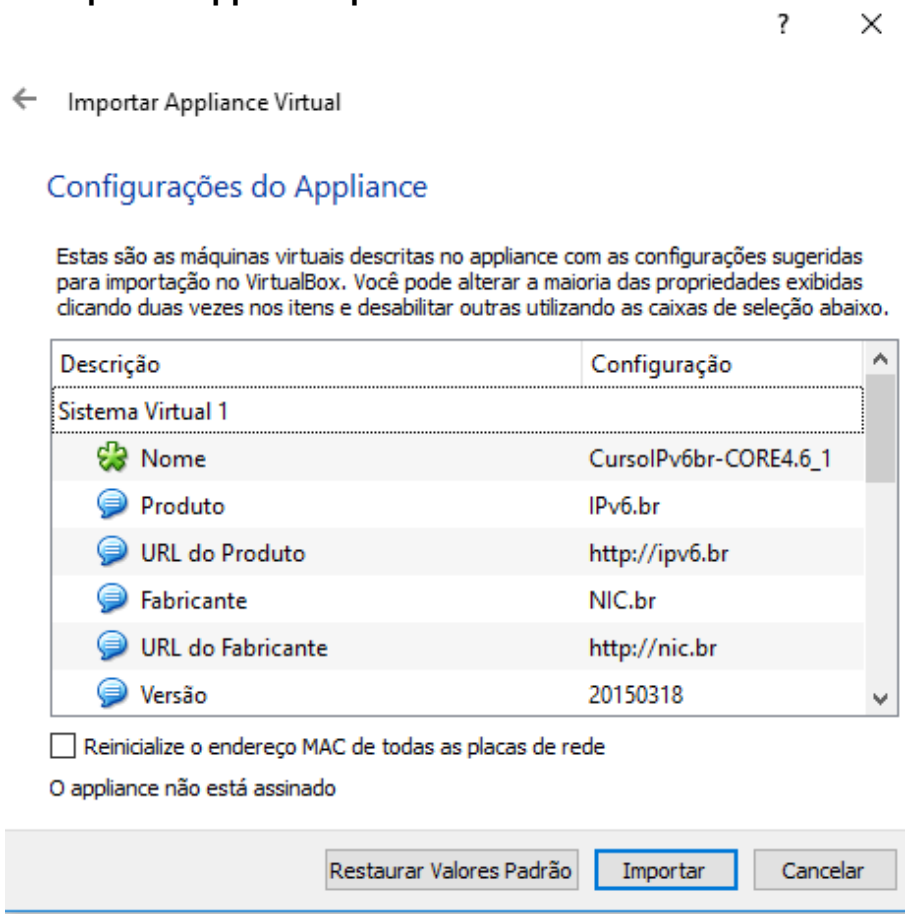
Figura 41: Importar Appliance parte 4



Fonte: Próprio Autor.

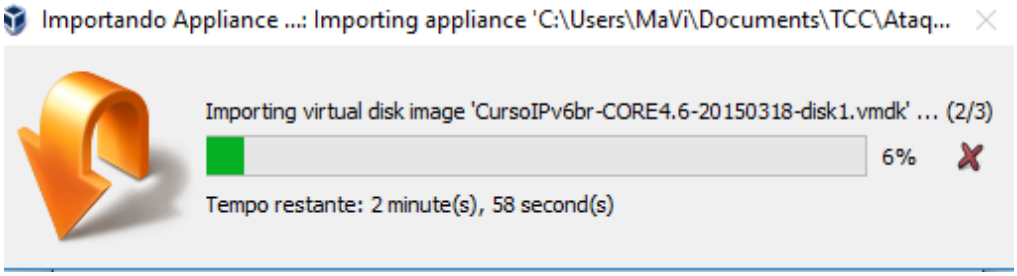
Para finalizar a importação é só seguir os passos descritos na Figura 42 e Figura 43.

Figura 42: Importar Appliance parte 5



Fonte: Próprio Autor.

Figura 43: Importar Appliance parte 6



Fonte: Próprio Autor.

Esperar carregar a Appliance, no virtual box ela aparece na parte esquerda da tela, selecionar a máquina que deseja e Iniciar, Igual a Figura 44.

Figura 44: Importar Appliance parte 7

Fonte: Próprio Autor.

APÊNDICE B – Comandos Básicos dos Softwares Utilizados

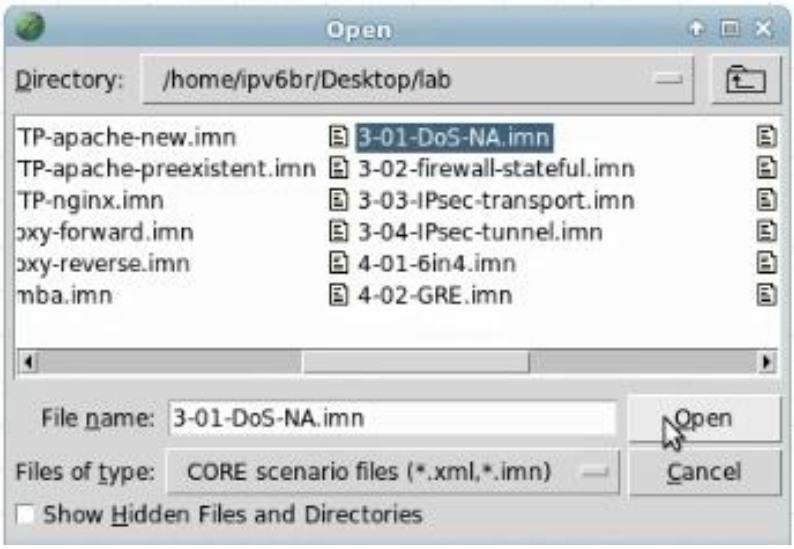
1. Comando Básico Terminar

Abrir: Dois clique em cima do CORE no host.

2. Comando Básicos CORE:

Abrir Simulação - Clicar em **File.** Escolher a simulação que deseja e clicar em **Open** conforme a Figura 45.

Figura 45: CORE parte 1



Fonte: Próprio Autor.

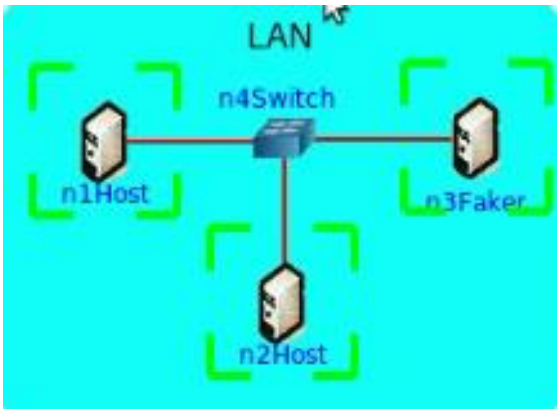
Iniciar Simulação: Clicar no Start, igual a Figura 46.

Figura 46: CORE parte 2

Fonte: Próprio Autor.

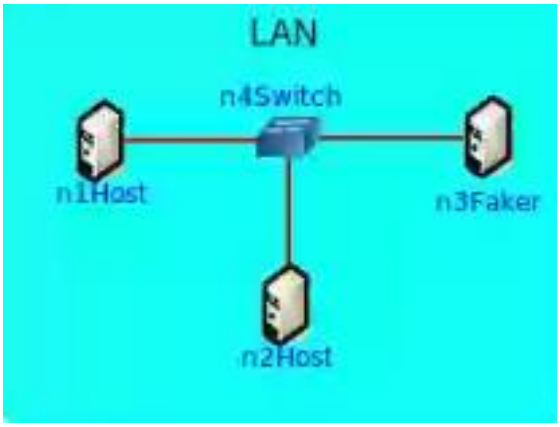
A simulação poderá ser utilizada quando sumir os quadros da volta dos hosts igual a Figura 47 e Figura 48.

Figura 47: CORE parte 3



Fonte: Próprio Autor.

Figura 48: CORE parte 4



Fonte: Próprio Autor.

Encerrar Simulação: para encerrar a simulação é só clicar no Stop, demonstrado pela Figura 49.

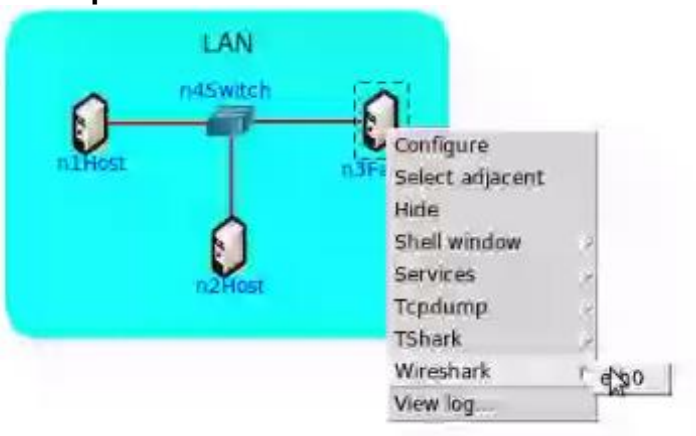
Figura 49: CORE parte 5

Fonte: Próprio Autor.

3. Wireshark

Abrir: Para abrir o wireshark na simulação é só clicar com o botão esquerdo do mouse em cima do host, escolher o Wireshark e clicar em **eth0**.

Figura 50: Wireshark parte 1



Fonte: Próprio Autor.

O software começa a capturar pacotes automaticamente.

Pausar: para pausar a captura de pacotes e só clicar na imagem igual a Figura 51.

Figura 51: Wireshark parte 2

Fonte: Próprio Autor.

Salvar: para salvar os arquivos clicar em **File**; **Save as**; **Name**: (dar um nome para os arquivos gerados); Escolher diretório e clicar em **Save**.

APÊNDICE C - Tutorial DAD (*Duplicate Address Detection*)

1. Ligar a máquina Virtual;
2. Abrir o CORE e carregar a Topologia 1-04-DAD.imn (diretório lab dentro do Desktop) e inicial;
3. Abrir o Wireshark nos *hosts* n1Original; n2Duplicate; n3Host;
4. Abrir o terminal das máquinas n1Original; n2Duplicate; n3Host;
5. No terminal n1Original:
   #ping6 –c 4 –I eth0 2001:db8::11
   #ping6 –c 4 –I eth0 2001:db8::12
6. No terminal n2Duplicate:
   ```
   #ping6 –c 4 –I eth0 2001:db8::10
   #ping6 –c 4 –I eth0 2001:db8::12
   ```
7. No terminal n3Host:
   ```
   #ping6 –c 4 –I eth0 2001:db8::10
   #ping6 –c 4 –I eth0 2001:db8::11
   ```
8. Fechar os terminais de todas as máquinas.
9. Abrir cada tela do Wireshark, pausar a captura e salvar o arquivo.
10. Abrir o Wireshark na n1Original e n2Duplicate novamente;
11. Abrir o terminal n2Duplicate:
    ```
    #ip addr del 2001:db8::11/64 dev eth0
    #ip addr add 2001:db8::10/64 dev eth0
    #ifconfig eth0
    #ip addr show dev eth0
    ```
12. No terminal do n3Host:
    ```
    # #ping6 –c 4 –I eth0 2001:db8::10
    ```
13. Pausar o Wireshark das máquinas n1Original e n2Duplicate e salvar o arquivo.

APÊNDICE D - Tutorial Ataque ao DAD

1. Iniciar o CORE e abrir o arquivo 3-01-DOS-NA.imn (diretório lab dentro do Desktop)
2. Inicial a simulação e verificar as configurações dos endereços IPv6 nos hosts

   ```
   #ifconfig eth0
   ```
3. Abrir no terminal do n1Host e executar o comando para verificar a conexão:

   ```
   #ping6 –c 4 –I eth0 fe80::200:ff:feaa:1
   ```
4. No n3Faker abrir o Wireshark;
5. No n3Faker abrir um terminal com duplo clique em cima da máquina e executar o comando:

   ```
   #dos-new-ip6 eth0
   ```
6. No terminal do n1Host:

   ```
   #ip link set eth0 down
   #ip link set eth0 up
   #ip addr show eth0
   #ifconfig eth0
   ```
7. No n1Host:

   ```
   #ping6 –c 4 –I eth0 fe80::200:ff:feaa:1
   ```
8. No Terminal n3Faker encerrar o dos-new-ip6 com Ctrl+C.
9. Analisar no Wireshark as mensagens icmpv6 (NS e NA) e salvar o arquivo.
10. Encerrar simulação.

APÊNDICE E - Tutorial Detecção NDPmon

1. Iniciar o CORE e abrir o arquivo 3-01-DOS-NA.imn (diretório **lab** dentro do **Desktop**)
2. Inicial a simulação.
3. No n2Host iniciar o NDPmon

   ```
   #ndpmon –i eth0
   ```
4. No n3Faker executar:

   ```
   #dos-new-ip6 eth0
   ```
5. No n1Host executar:

   ```
   #ip link set eth0 down
   #ip link set eth0 up
   #ip addr show eth0
   ```
6. No n2Host analisar o log gerado.

APÊNDICE F - Mensagens Capturadas pelo Wireshark na Demonstração do DAD (ping n1Original)

```
No.     Time           Source                Destination           Protocol Length Info
      1 0.000000       2001:db8::10          ff02::1:ff00:11       ICMPv6   86
Neighbor Solicitation for 2001:db8::11 from 00:00:00:aa:00:00

Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: IPv6mcast_ff:00:00:11
(33:33:ff:00:00:11)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: ff02::1:ff00:11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      2 0.000066       2001:db8::11          2001:db8::10          ICMPv6   86
Neighbor Advertisement 2001:db8::11 (sol, ovr) is at 00:00:00:aa:00:01

Frame 2: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      3 0.000071       2001:db8::10          2001:db8::11          ICMPv6   118    Echo
(ping) request id=0x0026, seq=1, hop limit=64 (reply in 4)

Frame 3: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      4 0.000086       2001:db8::11          2001:db8::10          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=1, hop limit=64 (request in 3)

Frame 4: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      5 0.999014       2001:db8::10          2001:db8::11          ICMPv6   118    Echo
(ping) request id=0x0026, seq=2, hop limit=64 (reply in 6)

Frame 5: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      6 0.999067       2001:db8::11          2001:db8::10          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=2, hop limit=64 (request in 5)

Frame 6: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      7 1.998008       2001:db8::10          2001:db8::11          ICMPv6   118    Echo
(ping) request id=0x0026, seq=3, hop limit=64 (reply in 8)

Frame 7: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::11
Internet Control Message Protocol v6
```

```
No.     Time           Source                Destination           Protocol Length Info
      8 1.998046       2001:db8::11          2001:db8::10          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=3, hop limit=64 (request in 7)

Frame 8: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      9 2.997009       2001:db8::10          2001:db8::11          ICMPv6   118    Echo
(ping) request id=0x0026, seq=4, hop limit=64 (reply in 10)

Frame 9: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     10 2.997045       2001:db8::11          2001:db8::10          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=4, hop limit=64 (request in 9)

Frame 10: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     11 5.008557       fe80::200:ff:feaa:1   2001:db8::10          ICMPv6   86
Neighbor Solicitation for 2001:db8::10 from 00:00:00:aa:00:01

Frame 11: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:1, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     12 5.008588       2001:db8::10          fe80::200:ff:feaa:1   ICMPv6   78
Neighbor Advertisement 2001:db8::10 (sol)

Frame 12: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: fe80::200:ff:feaa:1
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     13 7.154539       2001:db8::10          ff02::1:ff00:12       ICMPv6   86
Neighbor Solicitation for 2001:db8::12 from 00:00:00:aa:00:00

Frame 13: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: IPv6mcast_ff:00:00:12
(33:33:ff:00:00:12)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: ff02::1:ff00:12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     14 7.154609       2001:db8::12          2001:db8::10          ICMPv6   86
Neighbor Advertisement 2001:db8::12 (sol, ovr) is at 00:00:00:aa:00:02

Frame 14: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     15 7.154614       2001:db8::10          2001:db8::12          ICMPv6   118    Echo
(ping) request id=0x0027, seq=1, hop limit=64 (reply in 16)

Frame 15: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
```

```
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     16 7.154630       2001:db8::12          2001:db8::10          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=1, hop limit=64 (request in 15)

Frame 16: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     17 8.153549       2001:db8::10          2001:db8::12          ICMPv6   118    Echo
(ping) request id=0x0027, seq=2, hop limit=64 (reply in 18)

Frame 17: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     18 8.153594       2001:db8::12          2001:db8::10          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=2, hop limit=64 (request in 17)

Frame 18: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     19 9.152547       2001:db8::10          2001:db8::12          ICMPv6   118    Echo
(ping) request id=0x0027, seq=3, hop limit=64 (reply in 20)

Frame 19: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     20 9.152583       2001:db8::12          2001:db8::10          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=3, hop limit=64 (request in 19)

Frame 20: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     21 10.017258      fe80::200:ff:feaa:0   fe80::200:ff:feaa:1   ICMPv6   86
Neighbor Solicitation for fe80::200:ff:feaa:1 from 00:00:00:aa:00:00

Frame 21: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:0, Dst: fe80::200:ff:feaa:1
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     22 10.017342      fe80::200:ff:feaa:1   fe80::200:ff:feaa:0   ICMPv6   78
Neighbor Advertisement fe80::200:ff:feaa:1 (sol)

Frame 22: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:1, Dst: fe80::200:ff:feaa:0
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
```

```
     23 10.152447      2001:db8::10          2001:db8::12          ICMPv6   118    Echo
(ping) request id=0x0027, seq=4, hop limit=64 (reply in 24)

Frame 23: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     24 10.152482      2001:db8::12          2001:db8::10          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=4, hop limit=64 (request in 23)

Frame 24: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     25 12.160461      fe80::200:ff:feaa:2   2001:db8::10          ICMPv6   86
Neighbor Solicitation for 2001:db8::10 from 00:00:00:aa:00:02

Frame 25: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:2, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     26 12.160488      2001:db8::10          fe80::200:ff:feaa:2   ICMPv6   78
Neighbor Advertisement 2001:db8::10 (sol)

Frame 26: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: fe80::200:ff:feaa:2
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     27 15.024489      fe80::200:ff:feaa:1   fe80::200:ff:feaa:0   ICMPv6   86
Neighbor Solicitation for fe80::200:ff:feaa:0 from 00:00:00:aa:00:01

Frame 27: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:1, Dst: fe80::200:ff:feaa:0
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     28 15.024507      fe80::200:ff:feaa:0   fe80::200:ff:feaa:1   ICMPv6   78
Neighbor Advertisement fe80::200:ff:feaa:0 (sol)

Frame 28: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:0, Dst: fe80::200:ff:feaa:1
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     29 17.169741      fe80::200:ff:feaa:0   fe80::200:ff:feaa:2   ICMPv6   86
Neighbor Solicitation for fe80::200:ff:feaa:2 from 00:00:00:aa:00:00

Frame 29: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:0, Dst: fe80::200:ff:feaa:2
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     30 17.169790      fe80::200:ff:feaa:2   fe80::200:ff:feaa:0   ICMPv6   78
Neighbor Advertisement fe80::200:ff:feaa:2 (sol)

Frame 30: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
```

```
Internet Protocol Version 6, Src: fe80::200:ff:feaa:2, Dst: fe80::200:ff:feaa:0
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     31 22.176490      fe80::200:ff:feaa:2   fe80::200:ff:feaa:0   ICMPv6   86
Neighbor Solicitation for fe80::200:ff:feaa:0 from 00:00:00:aa:00:02

Frame 31: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:2, Dst: fe80::200:ff:feaa:0
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     32 22.176511      fe80::200:ff:feaa:0   fe80::200:ff:feaa:2   ICMPv6   78
Neighbor Advertisement fe80::200:ff:feaa:0 (sol)

Frame 32: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:0, Dst: fe80::200:ff:feaa:2
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     33 41.219201      2001:db8::11          2001:db8::10          ICMPv6   118    Echo
(ping) request id=0x0026, seq=1, hop limit=64 (reply in 34)

Frame 33: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     34 41.219215      2001:db8::10          2001:db8::11          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=1, hop limit=64 (request in 33)

Frame 34: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     35 42.218279      2001:db8::11          2001:db8::10          ICMPv6   118    Echo
(ping) request id=0x0026, seq=2, hop limit=64 (reply in 36)

Frame 35: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     36 42.218299      2001:db8::10          2001:db8::11          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=2, hop limit=64 (request in 35)

Frame 36: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     37 43.217584      2001:db8::11          2001:db8::10          ICMPv6   118    Echo
(ping) request id=0x0026, seq=3, hop limit=64 (reply in 38)

Frame 37: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     38 43.217614      2001:db8::10          2001:db8::11          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=3, hop limit=64 (request in 37)
```

```
Frame 38: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     39 44.216547      2001:db8::11          2001:db8::10          ICMPv6   118    Echo
(ping) request id=0x0026, seq=4, hop limit=64 (reply in 40)

Frame 39: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     40 44.216563      2001:db8::10          2001:db8::11          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=4, hop limit=64 (request in 39)

Frame 40: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     41 46.225316      fe80::200:ff:feaa:0   2001:db8::11          ICMPv6   86
Neighbor Solicitation for 2001:db8::11 from 00:00:00:aa:00:00

Frame 41: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:0, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     42 46.225360      2001:db8::11          fe80::200:ff:feaa:0   ICMPv6   78
Neighbor Advertisement 2001:db8::11 (sol)

Frame 42: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: fe80::200:ff:feaa:0
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     43 48.257238      2001:db8::11          ff02::1:ff00:12       ICMPv6   86
Neighbor Solicitation for 2001:db8::12 from 00:00:00:aa:00:01

Frame 43: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: IPv6mcast_ff:00:00:12
(33:33:ff:00:00:12)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: ff02::1:ff00:12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     44 82.941651      2001:db8::12          2001:db8::10          ICMPv6   118    Echo
(ping) request id=0x0026, seq=1, hop limit=64 (reply in 47)

Frame 44: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     45 82.941675      2001:db8::10          ff02::1:ff00:12       ICMPv6   86
Neighbor Solicitation for 2001:db8::12 from 00:00:00:aa:00:00

Frame 45: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: IPv6mcast_ff:00:00:12
(33:33:ff:00:00:12)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: ff02::1:ff00:12
Internet Control Message Protocol v6
```

```
No.     Time           Source                Destination           Protocol Length Info
     46 82.941706      2001:db8::12          2001:db8::10          ICMPv6   86
Neighbor Advertisement 2001:db8::12 (sol, ovr) is at 00:00:00:aa:00:02

Frame 46: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     47 82.941711      2001:db8::10          2001:db8::12          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=1, hop limit=64 (request in 44)

Frame 47: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     48 83.940668      2001:db8::12          2001:db8::10          ICMPv6   118    Echo
(ping) request id=0x0026, seq=2, hop limit=64 (reply in 49)

Frame 48: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     49 83.940683      2001:db8::10          2001:db8::12          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=2, hop limit=64 (request in 48)

Frame 49: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     50 84.940605      2001:db8::12          2001:db8::10          ICMPv6   118    Echo
(ping) request id=0x0026, seq=3, hop limit=64 (reply in 51)

Frame 50: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     51 84.940621      2001:db8::10          2001:db8::12          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=3, hop limit=64 (request in 50)

Frame 51: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     52 85.940682      2001:db8::12          2001:db8::10          ICMPv6   118    Echo
(ping) request id=0x0026, seq=4, hop limit=64 (reply in 53)

Frame 52: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     53 85.940719      2001:db8::10          2001:db8::12          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=4, hop limit=64 (request in 52)

Frame 53: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
```

```
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::12
Internet Control Message Protocol v6
```

APÊNDICE G - Mensagens Capturadas pelo Wireshark na Demonstração do DAD (ping n2Duplicate)

```
No.     Time           Source                Destination           Protocol Length Info
      1 0.000000       2001:db8::10          ff02::1:ff00:11       ICMPv6   86
Neighbor Solicitation for 2001:db8::11 from 00:00:00:aa:00:00

Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: IPv6mcast_ff:00:00:11
(33:33:ff:00:00:11)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: ff02::1:ff00:11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      2 0.000039       2001:db8::11          2001:db8::10          ICMPv6   86
Neighbor Advertisement 2001:db8::11 (sol, ovr) is at 00:00:00:aa:00:01

Frame 2: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      3 0.000052       2001:db8::10          2001:db8::11          ICMPv6   118    Echo
(ping) request id=0x0026, seq=1, hop limit=64 (reply in 4)

Frame 3: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      4 0.000061       2001:db8::11          2001:db8::10          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=1, hop limit=64 (request in 3)

Frame 4: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      5 0.999015       2001:db8::10          2001:db8::11          ICMPv6   118    Echo
(ping) request id=0x0026, seq=2, hop limit=64 (reply in 6)

Frame 5: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      6 0.999038       2001:db8::11          2001:db8::10          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=2, hop limit=64 (request in 5)

Frame 6: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      7 1.998005       2001:db8::10          2001:db8::11          ICMPv6   118    Echo
(ping) request id=0x0026, seq=3, hop limit=64 (reply in 8)

Frame 7: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::11
Internet Control Message Protocol v6
```

```
No.     Time           Source                Destination           Protocol Length Info
      8 1.998020       2001:db8::11          2001:db8::10          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=3, hop limit=64 (request in 7)

Frame 8: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      9 2.997004       2001:db8::10          2001:db8::11          ICMPv6   118    Echo
(ping) request id=0x0026, seq=4, hop limit=64 (reply in 10)

Frame 9: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     10 2.997020       2001:db8::11          2001:db8::10          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=4, hop limit=64 (request in 9)

Frame 10: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     11 5.008509       fe80::200:ff:feaa:1   2001:db8::10          ICMPv6   86
Neighbor Solicitation for 2001:db8::10 from 00:00:00:aa:00:01

Frame 11: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:1, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     12 5.008570       2001:db8::10          fe80::200:ff:feaa:1   ICMPv6   78
Neighbor Advertisement 2001:db8::10 (sol)

Frame 12: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: fe80::200:ff:feaa:1
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     13 7.154542       2001:db8::10          ff02::1:ff00:12       ICMPv6   86
Neighbor Solicitation for 2001:db8::12 from 00:00:00:aa:00:00

Frame 13: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: IPv6mcast_ff:00:00:12
(33:33:ff:00:00:12)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: ff02::1:ff00:12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     14 10.017282      fe80::200:ff:feaa:0   fe80::200:ff:feaa:1   ICMPv6   86
Neighbor Solicitation for fe80::200:ff:feaa:1 from 00:00:00:aa:00:00

Frame 14: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:0, Dst: fe80::200:ff:feaa:1
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     15 10.017315      fe80::200:ff:feaa:1   fe80::200:ff:feaa:0   ICMPv6   78
Neighbor Advertisement fe80::200:ff:feaa:1 (sol)

Frame 15: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
```

```
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:1, Dst: fe80::200:ff:feaa:0
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     16 15.024444      fe80::200:ff:feaa:1   fe80::200:ff:feaa:0   ICMPv6   86
Neighbor Solicitation for fe80::200:ff:feaa:0 from 00:00:00:aa:00:01

Frame 16: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:1, Dst: fe80::200:ff:feaa:0
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     17 15.024488      fe80::200:ff:feaa:0   fe80::200:ff:feaa:1   ICMPv6   78
Neighbor Advertisement fe80::200:ff:feaa:0 (sol)

Frame 17: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:0, Dst: fe80::200:ff:feaa:1
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     18 41.219161      2001:db8::11          2001:db8::10          ICMPv6   118    Echo
(ping) request id=0x0026, seq=1, hop limit=64 (reply in 19)

Frame 18: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     19 41.219197      2001:db8::10          2001:db8::11          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=1, hop limit=64 (request in 18)

Frame 19: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     20 42.218237      2001:db8::11          2001:db8::10          ICMPv6   118    Echo
(ping) request id=0x0026, seq=2, hop limit=64 (reply in 21)

Frame 20: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     21 42.218282      2001:db8::10          2001:db8::11          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=2, hop limit=64 (request in 20)

Frame 21: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     22 43.217531      2001:db8::11          2001:db8::10          ICMPv6   118    Echo
(ping) request id=0x0026, seq=3, hop limit=64 (reply in 23)

Frame 22: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
```

```
     23 43.217600      2001:db8::10          2001:db8::11          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=3, hop limit=64 (request in 22)

Frame 23: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     24 44.216508      2001:db8::11          2001:db8::10          ICMPv6   118    Echo
(ping) request id=0x0026, seq=4, hop limit=64 (reply in 25)

Frame 24: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     25 44.216545      2001:db8::10          2001:db8::11          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=4, hop limit=64 (request in 24)

Frame 25: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     26 46.225316      fe80::200:ff:feaa:0   2001:db8::11          ICMPv6   86
Neighbor Solicitation for 2001:db8::11 from 00:00:00:aa:00:00

Frame 26: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:0, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     27 46.225334      2001:db8::11          fe80::200:ff:feaa:0   ICMPv6   78
Neighbor Advertisement 2001:db8::11 (sol)

Frame 27: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: fe80::200:ff:feaa:0
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     28 48.257193      2001:db8::11          ff02::1:ff00:12       ICMPv6   86
Neighbor Solicitation for 2001:db8::12 from 00:00:00:aa:00:01

Frame 28: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: IPv6mcast_ff:00:00:12
(33:33:ff:00:00:12)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: ff02::1:ff00:12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     29 48.257247      2001:db8::12          2001:db8::11          ICMPv6   86
Neighbor Advertisement 2001:db8::12 (sol, ovr) is at 00:00:00:aa:00:02

Frame 29: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     30 48.257251      2001:db8::11          2001:db8::12          ICMPv6   118    Echo
(ping) request id=0x0027, seq=1, hop limit=64 (reply in 31)

Frame 30: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
```

```
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     31 48.257299      2001:db8::12          2001:db8::11          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=1, hop limit=64 (request in 30)

Frame 31: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     32 49.256471      2001:db8::11          2001:db8::12          ICMPv6   118    Echo
(ping) request id=0x0027, seq=2, hop limit=64 (reply in 33)

Frame 32: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     33 49.256522      2001:db8::12          2001:db8::11          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=2, hop limit=64 (request in 32)

Frame 33: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     34 50.256622      2001:db8::11          2001:db8::12          ICMPv6   118    Echo
(ping) request id=0x0027, seq=3, hop limit=64 (reply in 35)

Frame 34: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     35 50.256656      2001:db8::12          2001:db8::11          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=3, hop limit=64 (request in 34)

Frame 35: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     36 51.256396      2001:db8::11          2001:db8::12          ICMPv6   118    Echo
(ping) request id=0x0027, seq=4, hop limit=64 (reply in 37)

Frame 36: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     37 51.256430      2001:db8::12          2001:db8::11          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=4, hop limit=64 (request in 36)

Frame 37: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     38 53.265116      fe80::200:ff:feaa:2   2001:db8::11          ICMPv6   86
Neighbor Solicitation for 2001:db8::11 from 00:00:00:aa:00:02
```

```
Frame 38: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:2, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     39 53.265176      2001:db8::11          fe80::200:ff:feaa:2   ICMPv6   78
Neighbor Advertisement 2001:db8::11 (sol)

Frame 39: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: fe80::200:ff:feaa:2
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     40 58.273156      fe80::200:ff:feaa:1   fe80::200:ff:feaa:2   ICMPv6   86
Neighbor Solicitation for fe80::200:ff:feaa:2 from 00:00:00:aa:00:01

Frame 40: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:1, Dst: fe80::200:ff:feaa:2
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     41 58.273201      fe80::200:ff:feaa:2   fe80::200:ff:feaa:1   ICMPv6   78
Neighbor Advertisement fe80::200:ff:feaa:2 (sol)

Frame 41: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:2, Dst: fe80::200:ff:feaa:1
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     42 63.280435      fe80::200:ff:feaa:2   fe80::200:ff:feaa:1   ICMPv6   86
Neighbor Solicitation for fe80::200:ff:feaa:1 from 00:00:00:aa:00:02

Frame 42: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:2, Dst: fe80::200:ff:feaa:1
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     43 63.280451      fe80::200:ff:feaa:1   fe80::200:ff:feaa:2   ICMPv6   78
Neighbor Advertisement fe80::200:ff:feaa:1 (sol)

Frame 43: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:1, Dst: fe80::200:ff:feaa:2
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     44 82.941662      2001:db8::10          ff02::1:ff00:12       ICMPv6   86
Neighbor Solicitation for 2001:db8::12 from 00:00:00:aa:00:00

Frame 44: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: IPv6mcast_ff:00:00:12
(33:33:ff:00:00:12)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: ff02::1:ff00:12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     45 88.520469      2001:db8::12          2001:db8::11          ICMPv6   118    Echo
(ping) request id=0x0027, seq=1, hop limit=64 (reply in 46)

Frame 45: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::11
Internet Control Message Protocol v6
```

```
No.     Time           Source                Destination           Protocol Length Info
     46 88.520485      2001:db8::11          2001:db8::12          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=1, hop limit=64 (request in 45)

Frame 46: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     47 89.519493      2001:db8::12          2001:db8::11          ICMPv6   118    Echo
(ping) request id=0x0027, seq=2, hop limit=64 (reply in 48)

Frame 47: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     48 89.519515      2001:db8::11          2001:db8::12          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=2, hop limit=64 (request in 47)

Frame 48: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     49 90.518492      2001:db8::12          2001:db8::11          ICMPv6   118    Echo
(ping) request id=0x0027, seq=3, hop limit=64 (reply in 50)

Frame 49: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     50 90.518516      2001:db8::11          2001:db8::12          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=3, hop limit=64 (request in 49)

Frame 50: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     51 91.517493      2001:db8::12          2001:db8::11          ICMPv6   118    Echo
(ping) request id=0x0027, seq=4, hop limit=64 (reply in 52)

Frame 51: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     52 91.517510      2001:db8::11          2001:db8::12          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=4, hop limit=64 (request in 51)

Frame 52: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     53 93.520465      fe80::200:ff:feaa:1   2001:db8::12          ICMPv6   86
Neighbor Solicitation for 2001:db8::12 from 00:00:00:aa:00:01

Frame 53: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
```

```
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:1, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     54 93.520509      2001:db8::12          fe80::200:ff:feaa:1   ICMPv6   78
Neighbor Advertisement 2001:db8::12 (sol)

Frame 54: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: fe80::200:ff:feaa:1
Internet Control Message Protocol v6
```

APÊNDICE H - Mensagens Capturadas pelo Wireshark na Demonstração do DAD (ping n3Host)

```
No.     Time           Source                Destination           Protocol Length Info
      1 0.000000       2001:db8::10          ff02::1:ff00:11       ICMPv6   86
Neighbor Solicitation for 2001:db8::11 from 00:00:00:aa:00:00

Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: IPv6mcast_ff:00:00:11
(33:33:ff:00:00:11)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: ff02::1:ff00:11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      2 7.154541       2001:db8::10          ff02::1:ff00:12       ICMPv6   86
Neighbor Solicitation for 2001:db8::12 from 00:00:00:aa:00:00

Frame 2: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: IPv6mcast_ff:00:00:12
(33:33:ff:00:00:12)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: ff02::1:ff00:12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      3 7.154582       2001:db8::12          2001:db8::10          ICMPv6   86
Neighbor Advertisement 2001:db8::12 (sol, ovr) is at 00:00:00:aa:00:02

Frame 3: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      4 7.154601       2001:db8::10          2001:db8::12          ICMPv6   118    Echo
(ping) request id=0x0027, seq=1, hop limit=64 (reply in 5)

Frame 4: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      5 7.154610       2001:db8::12          2001:db8::10          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=1, hop limit=64 (request in 4)

Frame 5: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      6 8.153552       2001:db8::10          2001:db8::12          ICMPv6   118    Echo
(ping) request id=0x0027, seq=2, hop limit=64 (reply in 7)

Frame 6: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      7 8.153571       2001:db8::12          2001:db8::10          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=2, hop limit=64 (request in 6)

Frame 7: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6
```

```
No.     Time           Source                Destination           Protocol Length Info
      8 9.152546       2001:db8::10          2001:db8::12          ICMPv6   118    Echo
(ping) request id=0x0027, seq=3, hop limit=64 (reply in 9)

Frame 8: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      9 9.152562       2001:db8::12          2001:db8::10          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=3, hop limit=64 (request in 8)

Frame 9: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     10 10.152446      2001:db8::10          2001:db8::12          ICMPv6   118    Echo
(ping) request id=0x0027, seq=4, hop limit=64 (reply in 11)

Frame 10: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     11 10.152462      2001:db8::12          2001:db8::10          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=4, hop limit=64 (request in 10)

Frame 11: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     12 12.160421      fe80::200:ff:feaa:2   2001:db8::10          ICMPv6   86
Neighbor Solicitation for 2001:db8::10 from 00:00:00:aa:00:02

Frame 12: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:2, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     13 12.160475      2001:db8::10          fe80::200:ff:feaa:2   ICMPv6   78
Neighbor Advertisement 2001:db8::10 (sol)

Frame 13: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: fe80::200:ff:feaa:2
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     14 17.169745      fe80::200:ff:feaa:0   fe80::200:ff:feaa:2   ICMPv6   86
Neighbor Solicitation for fe80::200:ff:feaa:2 from 00:00:00:aa:00:00

Frame 14: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:0, Dst: fe80::200:ff:feaa:2
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     15 17.169769      fe80::200:ff:feaa:2   fe80::200:ff:feaa:0   ICMPv6   78
Neighbor Advertisement fe80::200:ff:feaa:2 (sol)

Frame 15: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
```

```
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:2, Dst: fe80::200:ff:feaa:0
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     16 22.176449      fe80::200:ff:feaa:2   fe80::200:ff:feaa:0   ICMPv6   86
Neighbor Solicitation for fe80::200:ff:feaa:0 from 00:00:00:aa:00:02

Frame 16: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:2, Dst: fe80::200:ff:feaa:0
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     17 22.176500      fe80::200:ff:feaa:0   fe80::200:ff:feaa:2   ICMPv6   78
Neighbor Advertisement fe80::200:ff:feaa:0 (sol)

Frame 17: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:0, Dst: fe80::200:ff:feaa:2
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     18 48.257216      2001:db8::11          ff02::1:ff00:12       ICMPv6   86
Neighbor Solicitation for 2001:db8::12 from 00:00:00:aa:00:01

Frame 18: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: IPv6mcast_ff:00:00:12
(33:33:ff:00:00:12)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: ff02::1:ff00:12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     19 48.257241      2001:db8::12          2001:db8::11          ICMPv6   86
Neighbor Advertisement 2001:db8::12 (sol, ovr) is at 00:00:00:aa:00:02

Frame 19: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     20 48.257260      2001:db8::11          2001:db8::12          ICMPv6   118    Echo
(ping) request id=0x0027, seq=1, hop limit=64 (reply in 21)

Frame 20: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     21 48.257299      2001:db8::12          2001:db8::11          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=1, hop limit=64 (request in 20)

Frame 21: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     22 49.256498      2001:db8::11          2001:db8::12          ICMPv6   118    Echo
(ping) request id=0x0027, seq=2, hop limit=64 (reply in 23)

Frame 22: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
```

```
     23 49.256520      2001:db8::12          2001:db8::11          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=2, hop limit=64 (request in 22)

Frame 23: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     24 50.256642      2001:db8::11          2001:db8::12          ICMPv6   118    Echo
(ping) request id=0x0027, seq=3, hop limit=64 (reply in 25)

Frame 24: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     25 50.256658      2001:db8::12          2001:db8::11          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=3, hop limit=64 (request in 24)

Frame 25: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     26 51.256416      2001:db8::11          2001:db8::12          ICMPv6   118    Echo
(ping) request id=0x0027, seq=4, hop limit=64 (reply in 27)

Frame 26: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     27 51.256431      2001:db8::12          2001:db8::11          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=4, hop limit=64 (request in 26)

Frame 27: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     28 53.265072      fe80::200:ff:feaa:2   2001:db8::11          ICMPv6   86
Neighbor Solicitation for 2001:db8::11 from 00:00:00:aa:00:02

Frame 28: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:2, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     29 53.265195      2001:db8::11          fe80::200:ff:feaa:2   ICMPv6   78
Neighbor Advertisement 2001:db8::11 (sol)

Frame 29: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: fe80::200:ff:feaa:2
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     30 58.273178      fe80::200:ff:feaa:1   fe80::200:ff:feaa:2   ICMPv6   86
Neighbor Solicitation for fe80::200:ff:feaa:2 from 00:00:00:aa:00:01

Frame 30: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
```

```
Internet Protocol Version 6, Src: fe80::200:ff:feaa:1, Dst: fe80::200:ff:feaa:2
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     31 58.273203      fe80::200:ff:feaa:2   fe80::200:ff:feaa:1   ICMPv6   78
Neighbor Advertisement fe80::200:ff:feaa:2 (sol)

Frame 31: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:2, Dst: fe80::200:ff:feaa:1
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     32 63.280417      fe80::200:ff:feaa:2   fe80::200:ff:feaa:1   ICMPv6   86
Neighbor Solicitation for fe80::200:ff:feaa:1 from 00:00:00:aa:00:02

Frame 32: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:2, Dst: fe80::200:ff:feaa:1
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     33 63.280460      fe80::200:ff:feaa:1   fe80::200:ff:feaa:2   ICMPv6   78
Neighbor Advertisement fe80::200:ff:feaa:1 (sol)

Frame 33: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:1, Dst: fe80::200:ff:feaa:2
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     34 82.941617      2001:db8::12          2001:db8::10          ICMPv6   118    Echo
(ping) request id=0x0026, seq=1, hop limit=64 (reply in 37)

Frame 34: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     35 82.941665      2001:db8::10          ff02::1:ff00:12       ICMPv6   86
Neighbor Solicitation for 2001:db8::12 from 00:00:00:aa:00:00

Frame 35: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: IPv6mcast_ff:00:00:12
(33:33:ff:00:00:12)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: ff02::1:ff00:12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     36 82.941681      2001:db8::12          2001:db8::10          ICMPv6   86
Neighbor Advertisement 2001:db8::12 (sol, ovr) is at 00:00:00:aa:00:02

Frame 36: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     37 82.941697      2001:db8::10          2001:db8::12          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=1, hop limit=64 (request in 34)

Frame 37: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     38 83.940633      2001:db8::12          2001:db8::10          ICMPv6   118    Echo
(ping) request id=0x0026, seq=2, hop limit=64 (reply in 39)
```

```
Frame 38: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     39 83.940670      2001:db8::10          2001:db8::12          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=2, hop limit=64 (request in 38)

Frame 39: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     40 84.940573      2001:db8::12          2001:db8::10          ICMPv6   118    Echo
(ping) request id=0x0026, seq=3, hop limit=64 (reply in 41)

Frame 40: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     41 84.940608      2001:db8::10          2001:db8::12          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=3, hop limit=64 (request in 40)

Frame 41: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     42 85.940629      2001:db8::12          2001:db8::10          ICMPv6   118    Echo
(ping) request id=0x0026, seq=4, hop limit=64 (reply in 43)

Frame 42: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     43 85.940712      2001:db8::10          2001:db8::12          ICMPv6   118    Echo
(ping) reply id=0x0026, seq=4, hop limit=64 (request in 42)

Frame 43: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     44 88.520455      2001:db8::12          2001:db8::11          ICMPv6   118    Echo
(ping) request id=0x0027, seq=1, hop limit=64 (reply in 45)

Frame 44: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     45 88.520493      2001:db8::11          2001:db8::12          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=1, hop limit=64 (request in 44)

Frame 45: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::12
Internet Control Message Protocol v6
```

```
No.     Time           Source                Destination           Protocol Length Info
     46 89.519474      2001:db8::12          2001:db8::11          ICMPv6   118    Echo
(ping) request id=0x0027, seq=2, hop limit=64 (reply in 47)

Frame 46: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     47 89.519526      2001:db8::11          2001:db8::12          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=2, hop limit=64 (request in 46)

Frame 47: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     48 90.518476      2001:db8::12          2001:db8::11          ICMPv6   118    Echo
(ping) request id=0x0027, seq=3, hop limit=64 (reply in 49)

Frame 48: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     49 90.518528      2001:db8::11          2001:db8::12          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=3, hop limit=64 (request in 48)

Frame 49: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     50 91.517478      2001:db8::12          2001:db8::11          ICMPv6   118    Echo
(ping) request id=0x0027, seq=4, hop limit=64 (reply in 51)

Frame 50: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::11
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     51 91.517520      2001:db8::11          2001:db8::12          ICMPv6   118    Echo
(ping) reply id=0x0027, seq=4, hop limit=64 (request in 50)

Frame 51: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::11, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     52 93.520492      fe80::200:ff:feaa:1   2001:db8::12          ICMPv6   86
Neighbor Solicitation for 2001:db8::12 from 00:00:00:aa:00:01

Frame 52: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:1, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     53 93.520510      2001:db8::12          fe80::200:ff:feaa:1   ICMPv6   78
Neighbor Advertisement 2001:db8::12 (sol)

Frame 53: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
```

```
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01
(00:00:00:aa:00:01)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: fe80::200:ff:feaa:1
Internet Control Message Protocol v6
```

APÊNDICE I - Mensagens Capturadas pelo Wireshark na Demonstração do DAD (atribuição do endereço duplicado n1Original)

```
No.     Time           Source                Destination           Protocol Length Info
      1 0.000000       fe80::200:ff:feaa:1   ff02::16              ICMPv6   90
Multicast Listener Report Message v2

Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: IPv6mcast_16
(33:33:00:00:00:16)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:1, Dst: ff02::16
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      2 2.616128       fe80::200:ff:feaa:1   ff02::16              ICMPv6   90
Multicast Listener Report Message v2

Frame 2: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: IPv6mcast_16
(33:33:00:00:00:16)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:1, Dst: ff02::16
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      3 38.172742      fe80::200:ff:feaa:1   ff02::16              ICMPv6   110
Multicast Listener Report Message v2

Frame 3: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: IPv6mcast_16
(33:33:00:00:00:16)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:1, Dst: ff02::16
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      4 38.780010      fe80::200:ff:feaa:1   ff02::16              ICMPv6   110
Multicast Listener Report Message v2

Frame 4: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: IPv6mcast_16
(33:33:00:00:00:16)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:1, Dst: ff02::16
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      5 38.920036      ::                    ff02::1:ff00:10       ICMPv6   78
Neighbor Solicitation for 2001:db8::10

Frame 5: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: IPv6mcast_ff:00:00:10
(33:33:ff:00:00:10)
Internet Protocol Version 6, Src: ::, Dst: ff02::1:ff00:10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      6 38.920082      2001:db8::10          ff02::1               ICMPv6   86
Neighbor Advertisement 2001:db8::10 (ovr) is at 00:00:00:aa:00:00

Frame 6: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: IPv6mcast_01
(33:33:00:00:00:01)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: ff02::1
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      7 148.786298     2001:db8::12          ff02::1:ff00:10       ICMPv6   86
Neighbor Solicitation for 2001:db8::10 from 00:00:00:aa:00:02

Frame 7: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: IPv6mcast_ff:00:00:10
(33:33:ff:00:00:10)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: ff02::1:ff00:10
Internet Control Message Protocol v6
```

```
No.     Time           Source                Destination           Protocol Length Info
      8 148.786338     2001:db8::10          2001:db8::12          ICMPv6   86
Neighbor Advertisement 2001:db8::10 (sol, ovr) is at 00:00:00:aa:00:00

Frame 8: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      9 148.786349     2001:db8::12          2001:db8::10          ICMPv6   118    Echo
(ping) request id=0x0033, seq=1, hop limit=64 (reply in 10)

Frame 9: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     10 148.786359     2001:db8::10          2001:db8::12          ICMPv6   118    Echo
(ping) reply id=0x0033, seq=1, hop limit=64 (request in 9)

Frame 10: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     11 149.785289     2001:db8::12          2001:db8::10          ICMPv6   118    Echo
(ping) request id=0x0033, seq=2, hop limit=64 (reply in 12)

Frame 11: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     12 149.785310     2001:db8::10          2001:db8::12          ICMPv6   118    Echo
(ping) reply id=0x0033, seq=2, hop limit=64 (request in 11)

Frame 12: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     13 150.784296     2001:db8::12          2001:db8::10          ICMPv6   118    Echo
(ping) request id=0x0033, seq=3, hop limit=64 (reply in 14)

Frame 13: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     14 150.784315     2001:db8::10          2001:db8::12          ICMPv6   118    Echo
(ping) reply id=0x0033, seq=3, hop limit=64 (request in 13)

Frame 14: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     15 151.784263     2001:db8::12          2001:db8::10          ICMPv6   118    Echo
(ping) request id=0x0033, seq=4, hop limit=64 (reply in 16)

Frame 15: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
```

```
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: 2001:db8::10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     16 151.784317     2001:db8::10          2001:db8::12          ICMPv6   118    Echo
(ping) reply id=0x0033, seq=4, hop limit=64 (request in 15)

Frame 16: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     17 153.800550     fe80::200:ff:feaa:0   2001:db8::12          ICMPv6   86
Neighbor Solicitation for 2001:db8::12 from 00:00:00:aa:00:00

Frame 17: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:0, Dst: 2001:db8::12
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     18 153.800593     2001:db8::12          fe80::200:ff:feaa:0   ICMPv6   78
Neighbor Advertisement 2001:db8::12 (sol)

Frame 18: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: fe80::200:ff:feaa:0
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     19 158.808010     fe80::200:ff:feaa:2   fe80::200:ff:feaa:0   ICMPv6   86
Neighbor Solicitation for fe80::200:ff:feaa:0 from 00:00:00:aa:00:02

Frame 19: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00
(00:00:00:aa:00:00)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:2, Dst: fe80::200:ff:feaa:0
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
     20 158.808043     fe80::200:ff:feaa:0   fe80::200:ff:feaa:2   ICMPv6   78
Neighbor Advertisement fe80::200:ff:feaa:0 (sol)

Frame 20: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02
(00:00:00:aa:00:02)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:0, Dst: fe80::200:ff:feaa:2
Internet Control Message Protocol v6
```

APÊNDICE J - Mensagens Capturadas pelo Wireshark na Demonstração do DAD (atribuição do endereço duplicado n2Duplicate)

```
No.     Time           Source                Destination           Protocol Length Info
      1 0.000000       fe80::200:ff:feaa:1   ff02::16              ICMPv6   90
Multicast Listener Report Message v2

Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: IPv6mcast_16
(33:33:00:00:00:16)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:1, Dst: ff02::16
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      2 2.616110       fe80::200:ff:feaa:1   ff02::16              ICMPv6   90
Multicast Listener Report Message v2

Frame 2: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: IPv6mcast_16
(33:33:00:00:00:16)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:1, Dst: ff02::16
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      3 38.172635      fe80::200:ff:feaa:1   ff02::16              ICMPv6   110
Multicast Listener Report Message v2

Frame 3: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: IPv6mcast_16
(33:33:00:00:00:16)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:1, Dst: ff02::16
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      4 38.780009      fe80::200:ff:feaa:1   ff02::16              ICMPv6   110
Multicast Listener Report Message v2

Frame 4: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: IPv6mcast_16
(33:33:00:00:00:16)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:1, Dst: ff02::16
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      5 38.920039      ::                    ff02::1:ff00:10       ICMPv6   78
Neighbor Solicitation for 2001:db8::10

Frame 5: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: IPv6mcast_ff:00:00:10
(33:33:ff:00:00:10)
Internet Protocol Version 6, Src: ::, Dst: ff02::1:ff00:10
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      6 38.920114      2001:db8::10          ff02::1               ICMPv6   86
Neighbor Advertisement 2001:db8::10 (ovr) is at 00:00:00:aa:00:00

Frame 6: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: IPv6mcast_01
(33:33:00:00:00:01)
Internet Protocol Version 6, Src: 2001:db8::10, Dst: ff02::1
Internet Control Message Protocol v6

No.     Time           Source                Destination           Protocol Length Info
      7 148.786312     2001:db8::12          ff02::1:ff00:10       ICMPv6   86
Neighbor Solicitation for 2001:db8::10 from 00:00:00:aa:00:02

Frame 7: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: IPv6mcast_ff:00:00:10
(33:33:ff:00:00:10)
Internet Protocol Version 6, Src: 2001:db8::12, Dst: ff02::1:ff00:10
Internet Control Message Protocol v6
```

APÊNDICE K - Mensagens Capturadas pelo Wireshark no Ataque DoS (n3Faker)

```
No.     Time        Source                Destination           Protocol Length Info
      1 0.000000    ::                    ff02::16              ICMPv6   90
Multicast Listener Report Message v2

Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: IPv6mcast_00:00:00:16
(33:33:00:00:00:16)
Internet Protocol Version 6, Src: :: (::), Dst: ff02::16 (ff02::16)
Internet Control Message Protocol v6

No.     Time        Source                Destination           Protocol Length Info
      2 0.235966    ::                    ff02::1:ffaa:0        ICMPv6   78     Neighbor
Solicitation for fe80::200:ff:feaa:0

Frame 2: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: IPv6mcast_ff:aa:00:00
(33:33:ff:aa:00:00)
Internet Protocol Version 6, Src: :: (::), Dst: ff02::1:ffaa:0 (ff02::1:ffaa:0)
Internet Control Message Protocol v6

No.     Time        Source                Destination           Protocol Length Info
      3 0.240161    fe80::200:ff:feaa:0   ff02::1               ICMPv6   86     Neighbor
Advertisement fe80::200:ff:feaa:0 (ovr) is at 00:00:09:1a:1e:54

Frame 3: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: Xerox_1a:1e:54 (00:00:09:1a:1e:54), Dst: IPv6mcast_00:00:00:01
(33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:0 (fe80::200:ff:feaa:0), Dst:
ff02::1 (ff02::1)
Internet Control Message Protocol v6

No.     Time        Source                Destination           Protocol Length Info
      4 0.240909    fe80::200:ff:feaa:0   ff02::1               ICMPv6   86     Neighbor
Advertisement fe80::200:ff:feaa:0 (ovr) is at 00:00:09:1a:1e:54

Frame 4: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: Xerox_1a:1e:54 (00:00:09:1a:1e:54), Dst: IPv6mcast_00:00:00:01
(33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::200:ff:feaa:0 (fe80::200:ff:feaa:0), Dst:
ff02::1 (ff02::1)
Internet Control Message Protocol v6

No.     Time        Source                Destination           Protocol Length Info
      5 7.463960    ::                    ff02::16              ICMPv6   90
Multicast Listener Report Message v2

Frame 5: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: IPv6mcast_00:00:00:16
(33:33:00:00:00:16)
Internet Protocol Version 6, Src: :: (::), Dst: ff02::16 (ff02::16)
Internet Control Message Protocol v6
```