UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO

DEPARTAMENTO ACADÊMICO DE ELETRÔNICA

CURSO DE ESPECIALIZAÇÃO EM REDES DE COMPUTADORES E TELEINFORMÁTICA

RICARDO HEY NETTO

PROTOCOLO DE INTERNET VERSÃO 6 (IPV6)

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA

2018

RICARDO HEY NETTO

PROTOCOLO DE INTERNET VERSÃO 6 (IPV6)

Monografia de Especialização, apresentada ao Curso de Especialização em Redes de Computadores e Teleinformática, do Departamento Acadêmico de Eletrônica – DAELN, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Dr. Kleber Kendy Horikawa Nabas

CURITIBA

2018

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Câmpus Curitiba

Diretoria de Pesquisa e Pós-Graduação
Departamento Acadêmico de Eletrônica
Curso de Especialização em Redes de Computadores e Teleinformática

TERMO DE APROVAÇÃO

PROTOCOLO DE INTERNET VERSÃO 6 (IPV6)

por

RICARDO HEY NETTO

Esta monografia foi apresentada em 23 de Julho de 2018 como requisito parcial para a obtenção do título de Especialista em Redes de Computadores e Teleinformática. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Dr. Kleber Kendy Horikawa Nabas
Orientador

_____
Prof. Dr. Edenilson José da Silva
Membro titular

_____
Prof. M.Sc. Omero Francisco Bertol
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

RESUMO

HEY NETTO, Ricardo. **Protocolo de internet versão 6 (IPv6)**. 2018. 53 f. Monografia de Especialização em Redes de Computadores e Teleinformática, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

A internet tornou-se imprescindível praticamente em todas as atividades humanas, uma vez que os dispositivos móveis possibilitam estar conectado em qualquer lugar, à qualquer hora. Com o constante avanço, como ocorre nas demais áreas, a evolução faz com que cada vez mais equipamentos se conectem, transformando a forma de interação com esses objetos. A pilha de protocolos TCP/IP é responsável pela conexão desses milhões e milhões de dispositivos. Com o esgotamento dos endereços IPv4, tornou-se necessário e urgente a utilização do protocolo IPv6. Este trabalho aborda as principais características do protocolo IPv6, assim como algumas das técnicas de transição, além da simulação da técnica pilha-dupla, a qual consiste em utilizar os protocolos IPv4 e IPv6 na mesma rede.

Palavras-chave: IPv6. Técnicas de transição. Pilha-dupla.

ABSTRACT

HEY NETTO, Ricardo. **Internet protocol version 6 (IPv6)**. 2018. 53 f. Monografia de Especialização em Redes de Computadores e Teleinformática, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

The internet has become a must in virtually every human activity, since mobile devices make it possible to be connected anywhere, anytime. With constant progress, as in other areas, evolution causes more and more equipment to connect, transforming the form of interaction with these objects. The TCP / IP protocol stack is responsible for connecting these millions and millions of devices. With the exhaustion of IPv4 addresses, it became necessary and urgent to use the IPv6 protocol. This work addresses the main characteristics of the IPv6 protocol, as well as some of the transition techniques, as well as the simulation of the dual stack technique, which consists of using the IPv4 and IPv6 protocols in the same network.

Keywords: IPv6. Transition techniques. Dual stack.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

AH	*Authentication Header* (ou cabeçalho de autenticação)
ARP	*Address Resolution Protocol* (ou protocolo de resolução de endereços)
CATNIP	*Common Architecture for the Internet*
CIDR	*Classless Inter-Domain Routing*
CoA	*Care-of-Address*
DAD	*Duplicate Address Detection* (ou detecção de endereços duplicados)
DARPA	*Defense Advanced Research Projects Agency*
DHCP	*Dynamic Host Configuration Protocol* (ou protocolo de configuração dinâmica de *host*)
DHCPv6	*Dynamic Host Configuration Protocol version 6*
DNS	*Domain Name System* (ou sistema de nomes de domínio)
ESP	*Encapsulatoing Security Payload*
EUA	Estados Unidos da América
EUI-64	*Extended Unique Identifier*
HoA	*Home-of-Address*
HTML	*Hyper-Text Markup Language* (ou linguagem de marcação de hipertexto)
HTTP	*Hypertext Transfer Protocol* (ou protocolo de transferência de hipertexto)
ICMPv6	*Internet Control Message Protocol version 6* (ou protocolo de mensagens de controle de internet versão 6)
IANA	*Internet Assigned Numbers Authority* (ou autoridade para atribuição de números da internet)
IETF	*Internet Engineering Task Force*
IHL	*Internet Header Length* (ou comprimento do cabeçalho da internet)
IoT	*Internet of Things* (ou internet das coisas)
IP	*Internet Protocol* (ou protocolo de internet)
IPng	*IP next generation* (ou protocolo de internet nova geração)
IPSec	*Internet Protocol Security* (ou protocolo de segurança IP)
IPv4	*Internet Protocol version 4* (ou protocolo de internet versão 4)
IPv6	*Internet Protocol version 6* (ou protocolo de internet versão 6)
ISP	*Internet Service Provider* (ou provedor de serviço internet)
LACNIC	*Latin America and Caribbean Network Information Centre*
MAC	*Media Access Control*

MIPv6	*Mobile IPv6* (ou *protocolo* para a gestão da *mobilidade* IP)
NA	*Neighbor Advertisement*
NAT	*Network Address Translation* (ou tradução de endereços de rede)
NDP	*Neighbor Discovery Protocol*
NIC.br	Núcleo de Informação e Coordenação do Ponto BR
NRO	*Number Resources Organization*
NS	*Neighbor Solicitation*
NTP	*Network Time Protocol* (ou *protocolo* de tempo para redes)
P2P	*Peer-to-peer* (ou par-a-par, ou ainda, ponto-a-ponto)
QoS	*Quality of Service* (ou qualidade de serviço)
RA	*Router Advertisement*
RFC	*Request for Comments* (ou pedido de comentários)
ROAD	*ROuting and ADdressing*
RS	*Router Solicitation*
SIPP	*Simple Internet Protocol Plus*
SLAAC	*StateLess Address AutoConfiguration*
TCP	*Transmission Control Protocol* (ou protocolo de controle de transmissão)
TCP/IP	*Transmission Control Protocol / Internet Protocol* (ou protocolo de controle de transmissão / protocolo de internet)
TFTP	*Trivial File Transfer Protocol* (ou protocolo de transferência de arquivo)
ToS	*Type of Service* (ou tempo de serviço)
TTL	*Time to Live* (ou tempo de vida)
TUBA	*TCP and UDP with Bigger Addresses*
ULA	*Unique-Local Address*
URSS	União das Repúblicas Socialistas Soviéticas
VoIP	*Voice over Internet Protocol* (voz sobre protocolo de internet)
VPN	*Virtual Private Network* (ou rede particular virtual)
www	*word wide web* (ou rede mundial de computadores)

SUMÁRIO

1 INTRODUÇÃO

A internet foi um marco na história da humanidade, mudando completamente a forma de se relacionar, estudar, obter qualquer tipo de informação, das mais banais, como buscar um simples endereço de um restaurante, a fazer pesquisas científicas de alto grau de complexidade.

A Rede Mundial de Computadores (ou *word wide web* - www), como é comumente chamada, é fundamental nas atividades diárias de pessoas, governos e empresas das mais diversas áreas de atuação, os quais a utilizam para efetuar de uma simples chamada de voz, a transferências de capital entre instituições financeiras de diferentes nações.

Projetados inicialmente para fins militares, os protocolos *Transmission Control Protocol* (TCP, ou protocolo de controle de transmissão) e *Internet Protocol* (IP, ou protocolo de internet), foram desenvolvidos pelo Departamento de Defesa dos Estados Unidos da América na década de 70.

O *Internet Protocol version 4* (IPv4, ou protocolo de internet versão 4) possui o espaço de endereçamento baseado em valor inteiro de 32 bits, representado por quatro octetos em decimal. Com a explosão da internet, se tornou inadequado para acompanhar a evolução, sendo necessário a utilização de recursos como o *Network Address Translation* (NAT, ou tradução de endereços de rede) e o *Classless Inter-Domain Routing* (CIDR) como soluções paliativas para a falta de endereços disponíveis.

Com o objetivo de suprir a falta de endereçamento e outras necessidades em relação ao IPv4, na década de 90 foi desenvolvido por um grupo de pesquisadores do *Internet Engineering Task Force* (IETF) a nova geração do protocolo IP, a *next generation*, ou *Internet Protocol version 6* (IPv6, ou protocolo de internet versão 6), o qual possui espaço de endereçamento de 128 bits, suporte a roteamento e segmentação de pacotes na estação de origem, mecanismos de segurança, entre outros avanços.

Em função da necessidade de recursos demandados pelo rápido avanço tecnológico e a utilização de redes convergentes, como *stream* de video em alta definição e a Internet das Coisas (ou *Internet of Things* - IoT), a especificação do protocolo IPv6 tem sido revisada continuamente.

Com a utilização predominantemente com dispositivos IPv4, se faz necessária a transição para o protocolo IPv6, utilizando recursos como tunelamento e pilha-dupla (*dual stack)*.

Este trabalho tem como objetivo descrever algumas das deficiências do protocolo IPv4 e as principais características do protocolo IPv6, além de abordar o recurso Pilha-dupla na transição de redes IPv4 e IPv6.

2 O SURGIMENTO DA INTERNET E O PROTOCOLO IPV4

Em 1966, a *Defense Advanced Research Projects Agency* (DARPA), uma agência do Departamento de Defesa dos Estados Unidos da América, desenvolveu uma rede experimental, cujo principal objetivo era ser resistente a falhas. O projeto consistia no desenvolvimento de uma rede descentralizada, de tal forma que ocorrendo uma falha em um determinado ponto, os demais não fossem afetados e a rede permanecesse operando.

Nessa época, ocorria a “Guerra Fria” entre Estados Unidos da América (EUA) e União das Repúblicas Socialistas Soviéticas (URSS), de modo que havia um medo de que os meios de comunicação pudessem ser atacados, e dessa forma, uma grande indisponibilidade dos recursos de telecomunicação, os quais predominantemente, eram centralizados. Por esse motivo o projeto foi financiado pelo Departamento de Defesa dos EUA.

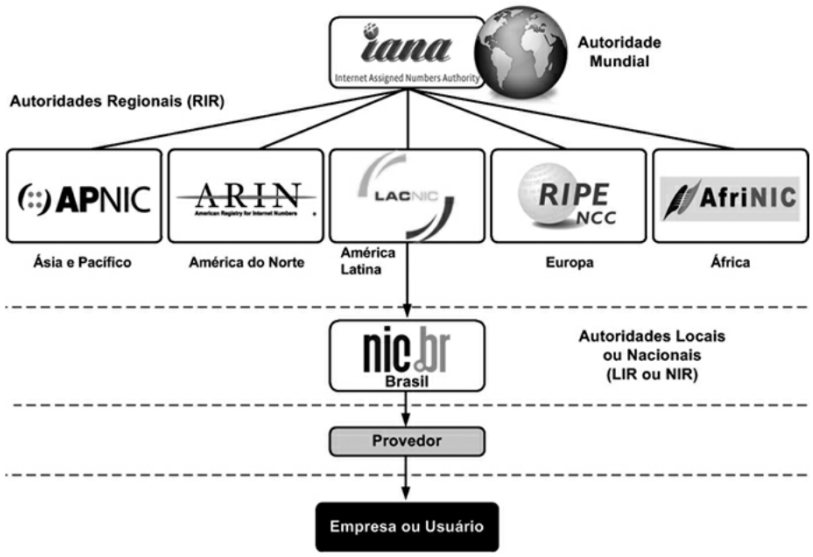
Os quatros primeiros nós da rede que passou a ser denominada de ARPANET, foram instalados em meados de 1969, interligando universidades dos EUA, são elas: Universidade da Califórnia em Los Angeles; Universidade da Califórnia em Santa Barbara; Universidade de Utah; e Universidade de Stanford.

Após alguns anos depois, em 1983, com mais de 500 *hosts*, surgiu a internet como conhece-se hoje, do ponto de vista estrutural, baseada nos protocolos *Transmission Control Protocol / Internet Protocol* (TCP / IP). O TCP é responsável pelo transporte e o IP pelo endereçamento.

Um protocolo é um conjunto de regras e padrões, de forma semelhante a um idioma, uma linguagem própria, possibilitando a comunicação entre dois ou mais *hosts*, ou seja, dois ou mais dispositivos em uma rede.

A internet, regulamentada pelas autoridades apresentadas na Figura 1, é uma rede baseada em padrões abertos e toda a documentação é publicada pela *Internet Engineering Task Force* (IETF), disponível através de *Request for Comments* (RFC, ou pedido de comentários), acessível por qualquer pessoa, como por exemplo a RFC 791 (BRITO, 2013).

Figura 1. Autoridades na governança da internet no mundo



Fonte: Brito (2013).

No começo da década de 1990, a internet passou a ser comercial através da *word wide web* (www), surgindo então os primeiros servidores de páginas web e seus clientes, os *browsers*. A partir daí, o *Hyper-Text Markup Language* (HTML, ou linguagem de marcação de hipertexto) foi definida como padrão para a comunicação entre os servidores *web* e os *browsers*. A medida que a internet se tornava mais conhecida e utilizada, o volume de conteúdo e os serviços disponíveis ficavam cada vez mais complexos, surgindo os buscadores (sites de pesquisa), o *e-commerce* (comércio eletrônico), o *bankline* (bancos online), *e-governament* (serviços públicos governamentais), entre outros recursos.

Com a popularização da internet, ainda na década de 1990, começou a ficar evidente os problemas estruturais do protocolo IPv4, com o comprometimento da escalabilidade, em função do número de endereçamento limitado, além da falta de segurança nas aplicações que necessitavam manter em completo sigilo e restrito o acesso às informações que trafegavam pela *web* (BRITO, 2013).

2.1 O ESGOTAMENTO DOS ENDEREÇOS IPV4

De acordo com as especificações do protocolo IPv4, 32 bits são reservados para o endereçamento, possibilitando gerar mais de 4 bilhões de endereços, os quais foram divididos em três classes de tamanhos fixos (IPV6.BR, 2012b), apresentadas na Tabela 1.

rTabela 1. Classes de endereçamento IPv4

Classe	Formato	Redes	Hosts
A	7 bits rede, 24 bits host	128	16.777.216
B	14 bits rede, 16 bits host	16.384	65.536
C	21 bits rede, 8 bits host	2.097.152	256

Fonte: Ipv6.br (2012b).

As classes: “Classe A”, “Classe B”, e “Classe C”, apresentadas ainda na Tabela1, são assim descritas (IPV6.BR, 2012b):

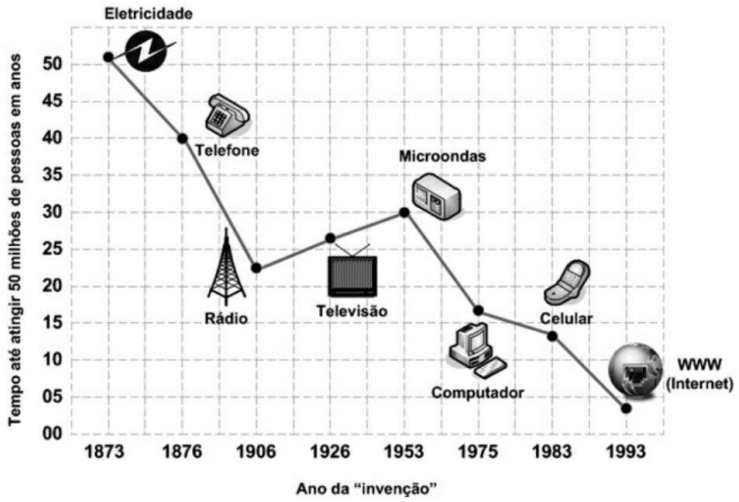
- Classe A: definia o bit mais significativo como 0, utilizava os 7 bits restantes do primeiro octeto para identificar a rede, e os 24 bits restantes para identificar o host. Esses endereços utilizavam a faixa de “1.0.0.0” até “126.0.0.0”;
- Classe B: definia os 2 bits mais significativo como 10, utilizava os 14 bits seguintes para identificar a rede, e os 16 bits restantes para identificar o host. Esses endereços utilizavam a faixa de “128.1.0.0” até “191.254.0.0”;
- Classe C: definia os 3 bits mais significativo como 110, utilizava os 21 bits seguintes para identificar a rede, e os 8 bits restantes para identificar o host. Esses endereços utilizavam a faixa de “192.0.1.0” até “223.255.254.0”.

Essa divisão das classes, apresentada novamente na Tabela 1, tinha por objetivo tornar a distribuição de endereços mais flexível, de modo a abranger redes de vários tamanhos, essa classificação se mostrou ineficiente. A “Classe A” atendia um número muito pequeno de redes, ocupando a metade de todos os endereços disponíveis, enquanto a “Classe C” permitia criar muitas redes, mas com poucos endereços disponíveis.

As faixas “Classe A”, foram atribuídas a grandes instituições como IBM, AT&T, Xerox, HP, Apple, MIT, Ford, Departamento de Defesa dos EUA, entre outros, totalizando para cada uma 16.777.216 milhões de endereços, os quais dificilmente seriam utilizados, contribuindo desta forma para um desperdício de endereços, ocasionando a sua escassez.

Com a criação do *Hypertext Transfer Protocol* (HTTP, ou protocolo de transferência de hipertexto) e a disponibilização pelo Governo Americano para o uso comercial da internet, houve um salto ainda maior no crescimento da rede, que passou de 2 milhões em 1993 (ano da invenção da internet - Figura 2), para mais de 26 milhões de *hosts* em 1997 (BRITO, 2013).

Figura 2. Ano da invenção da internet



Fonte: Brito (2013).

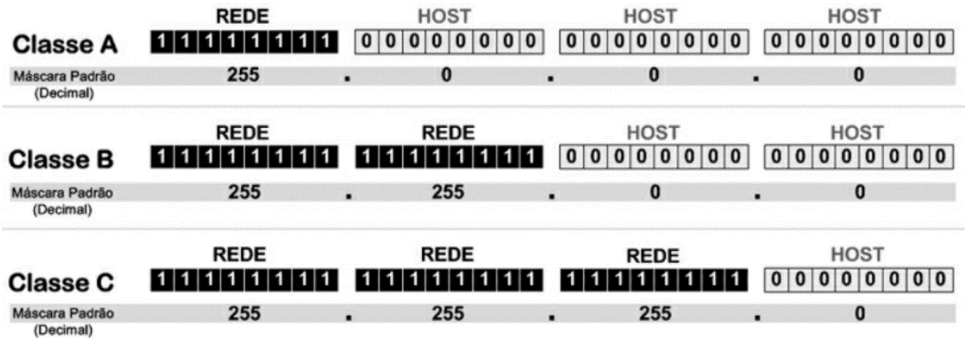
Diante desta situação, o IETF passou a discutir formas para solucionar a questão do esgotamento dos endereços IP e do aumento da tabela de roteamento. Em 1991 é formado o grupo *ROuting and ADdressing* (ROAD), o qual apresenta como soluções a utilização do *Classless Inter-Domain Routing* (CIDR) (IPV6.BR, 2012b).

O CIDR, assim como o *Dynamic Host Configuration Protocol* (DHCP) e o *Network Address Translation* (NAT), foram utilizados como medidas paliativas a falta de endereços no IPv4 (BRITO, 2013).

2.1.1 Cidr

Definido na RFC 4632, tornando obsoleta a RFC 1519 de 1993, o *Classless Inter-Domain Routing* (CIDR) tem como objetivo a alocação de blocos de tamanho apropriado, de acordo com a necessidade de cada rede, extinguindo o uso das classes de endereços. Os blocos são referenciados como prefixo de redes, surgindo então a máscaras de rede, apresentadas na Figura 3 (IPV6.BR, 2012b).

Figura 3. Máscaras de rede das classes padrões



Fonte: Brito (2013).

A máscara pode ser escrita de maneira simplificada, apontando a quantidade de bits do prefixo da rede precedido por uma barra, como nos próximos exemplos:

- Classe A: 255.0.0.0 (/8)
- Classe B: 255.255.0.0 (/16)
- Classe C: 255.255.255.0 (/24)

Como exemplo, uma determinada empresa com 400 *hosts* não podia solicitar um bloco “Classe C”, pois com apenas 8 bits, seria possível endereçar somente 254 hosts, sendo necessário enquadrar esta empresa na “Classe B”, com 16 bits para identificação dos *hosts*, sendo possível endereçar 65.534 *hosts*, uma quantidade muito acima do que o necessário, ocorrendo então o desperdício de mais de 65.000 endereços.

O CIDR otimiza significativamente a alocação de endereços e evita o desperdício. Para endereçar 400 *hosts*, são necessários 9 bits, 2^9 permite endereçar até 510 *hosts*, utilizando 23 bits para o prefixo de rede, dessa forma otimizando o uso dos endereços (BRITO, 2013).

2.1.2 Dhcp

Especificado em 1993 e atualizado em 1997 na RFC 2131, o *Dynamic Host Configuration Protocol* (DHCP) tem por objetivo distribuir automaticamente os endereços para os hosts internos de uma rede, diminuindo assim substancialmente os esforços na configuração dos nós, uma vez que o DHCP provê além do IP, a máscara de rede, o gateway e o *Domain Name System* (DNS) local (BRITO, 2013).

O servidor DHCP possui uma lista de endereços IP disponíveis (*range*), e toda vez que um novo cliente se conectar à rede, é designado um desses endereços de forma arbitrária e, no momento que o cliente se desconecta, o endereço é liberado e pode ser alocado a outro cliente, possibilitando aos provedores de acesso, também chamados de *Internet Service Provider* (ISP) realocar os endereços sem necessidade de fornecer um IP fixo para cada cliente (IPV6.BR, 2012b).

2.1.3 Nat

O *Network Address Translation* (NAT) foi o maior responsável pela sobrevivência do IPv4, o qual através de um processo de compartilhamento de um ou

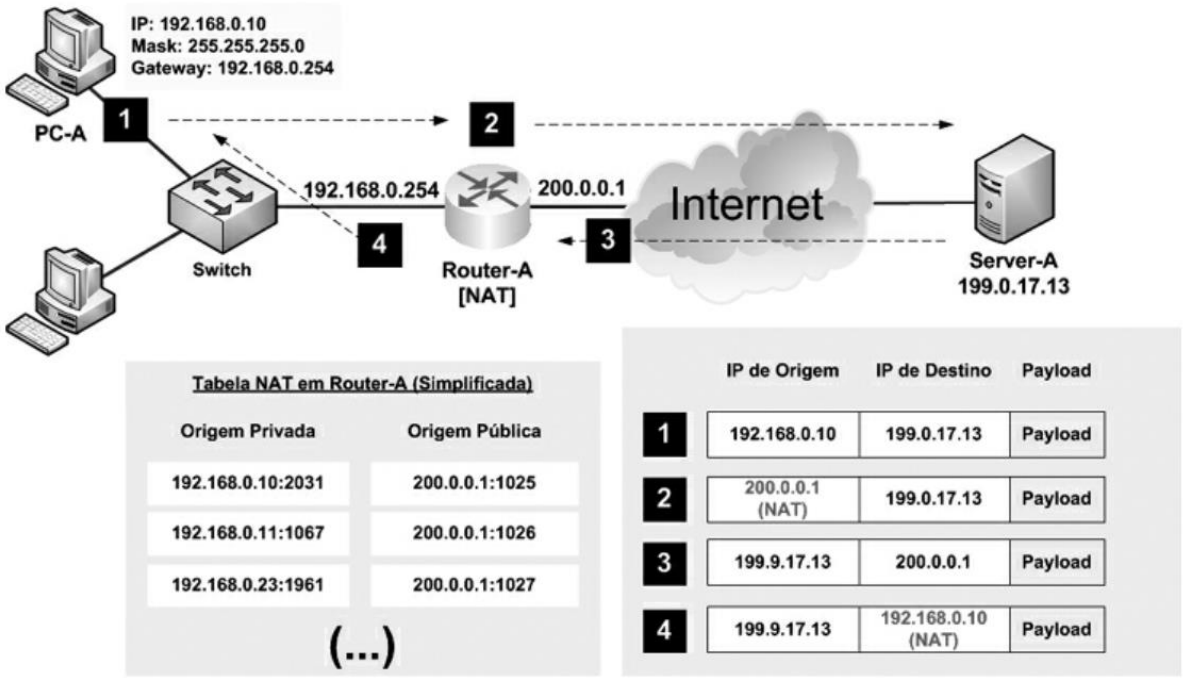
poucos endereços públicos roteáveis na internet, mantém a conectividade com vários endereços privados não roteáveis, especificado através da RFC 2663 de 1999.

Na RFC 1918 de 1996, foram reservadas algumas faixas de endereços de cada uma das classes padrões para uso local, sem comunicação com a internet. São elas:

- 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)

Esta também foi uma medida com o objetivo de economizar endereços IPv4 roteáveis (Figura 4), uma vez que em função desses endereços privados, pode ser utilizado apenas um IP válido para manter a conexão da rede interna com a internet (BRITO, 2013).

Figura 4. Mecanismo de tradução do NAT



Fonte: Brito (2013).

Outra questão importante, é que o NAT quebra o modelo fim-a-fim da internet, não permitindo conexões diretas entre dois hosts, o que dificulta o funcionamento de uma série de aplicações, como *Peer-to-peer* (P2P, ou par-a-par, ou ainda, ponto-a-ponto), *Voice over Internet Protocol* (VoIP, ou voz sobre protocolo de internet) e *Virtual Private Network* (VPN, ou rede particular virtual). Outro problema é a baixa escalabilidade, pois o número de conexões simultâneas é limitado, além de exigir um grande poder de processamento do dispositivo tradutor. O uso da NAT também

impossibilita rastrear o caminho de pacote, através de ferramentas como *traceroute*, por exemplo, e dificulta a utilização de algumas técnicas de segurança como o *Internet Protocol Security* (IPSec, ou protocolo de segurança IP). Além disso, seu uso passa uma falsa sensação de segurança, pois, apesar de não permitir a entrada de pacotes não autorizados, a NAT não realiza nenhum tipo de filtragem ou verificação nos pacotes que passa por ela (IPV6.BR, 2012b).

3 O PROTOCOLO IPV6

No final de 1993, a IETF formalizou através da RFC 1550, pesquisas sobre a nova versão do protocolo IP. Um grupo de pesquisa foi formado e vários projetos foram desenvolvidos, levando em conta questões como:

- Escalabilidade;
- Segurança;
- Configuração e administração de rede;
- Suporte a *Quality of Service* (QoS);
- Mobilidade;
- Políticas de roteamento;
- Transição.

Em janeiro de 1995, através da RFC 1752, foram apresentadas um resumo das avaliações das três principais propostas (IPV6.BR, 2012b). São elas:

a. *Common Architecture for the Internet* (CATNIP): foi concebido como um protocolo de convergência, para permitir a qualquer protocolo da camada de transporte ser executado sobre qualquer protocolo de camada de rede, criando um ambiente comum entre os protocolos da internet, OSI e Novell;
b. *TCP and UDP with Bigger Addresses* (TUBA): sua proposta era de aumentar o espaço para endereçamento do IPv4 e torná-lo mais hierárquico, buscando evitar a necessidade de se alterar os protocolos da camada de transporte e aplicação. Pretendia uma migração simples e em longo prazo, baseada na atualização dos host e servidores DNS, entretanto, sem a necessidade de encapsulamento ou tradução de pacotes, ou mapeamento de endereços;
c. *Simple Internet Protocol Plus* (SIPP): concebido para ser uma etapa evolutiva do IPv4, sem mudanças radicais e mantendo a interoperabilidade com a versão 4 do protocolo IP, fornecia uma plataforma para novas funcionalidades da internet, aumentava o espaço para endereçamento de 32 bits para 64 bits, apresentava um nível maior de hierarquia e era composto por um mecanismo que permitia “alargar o endereço” chamado *cluster addresses*. Já possuía cabeçalhos de extensão e um campo *flow* para identificar o tipo de fluxo de cada pacote.

Entretanto, as três propostas apresentavam problemas significativos, de modo que a recomendação final para o novo protocolo internet baseou-se em uma versão revisada do SIPP, que passou a incorporar endereços de 128 bits, juntamente com os elementos de transição e autoconfiguração do TUBA, o endereçamento baseado no CIDR e os cabeçalhos de extensão. O CATNIP, por ser considerado muito incompleto, foi descartado. A partir de então, a nova versão do protocolo internet passou a ser chamado oficialmente de IPv6 (IPV6.BR, 2012b).

A cronologia da internet pode ser classificada basicamente em três fases, em função das mudanças no decorrer do seu processo de evolução. São elas:

1. Internet das Máquinas;
2. Internet das Pessoas;
3. Internet das Coisas.

Como abordado anteriormente, originalmente a internet foi concebida para conectar máquinas, dispositivos fixos instalados em prédios (*sites*). Evidentemente, nessa primeira fase, não havia nenhum suporte à mobilidade.

Com a popularização comercial da internet na década de 1990, aliada a maciça disseminação dos dispositivos móveis no inicio dos anos 2000, o foco inicial se altera, dando origem a uma nova era, cujo elemento principal passa a ser as pessoas, ou seja, o próprio usuário passa a estar conectado à internet, fazendo uso desse recurso em qualquer lugar, através de vários dispositivos, como computadores, *smartphones*, *tablets* e outros aparelhos.

Pode-se dizer agora, que nos encontramos em uma fase de transição para uma nova fase, um novo ciclo de evolução para “’A Internet das Coisas”. Em função do avanço tecnológico da eletrônica embarcada, viabilizada pela construção de chips cada vez menores em tamanho, mas com poder de processamento computacional cada vez maior, qualquer aparelho poderá ser conectado à internet, de carros à geladeiras, estarão conectados, possibilitando um nível de interação e automatização nunca vistos.

Com o esgotamento de endereços IPV4, uma vez que os 4,3 bilhões de endereços não comportam um aumento significativo de dispositivos e aplicações, somente com o IPv6 efetivamente operando na internet, será viável o avanço para esta nova fase.

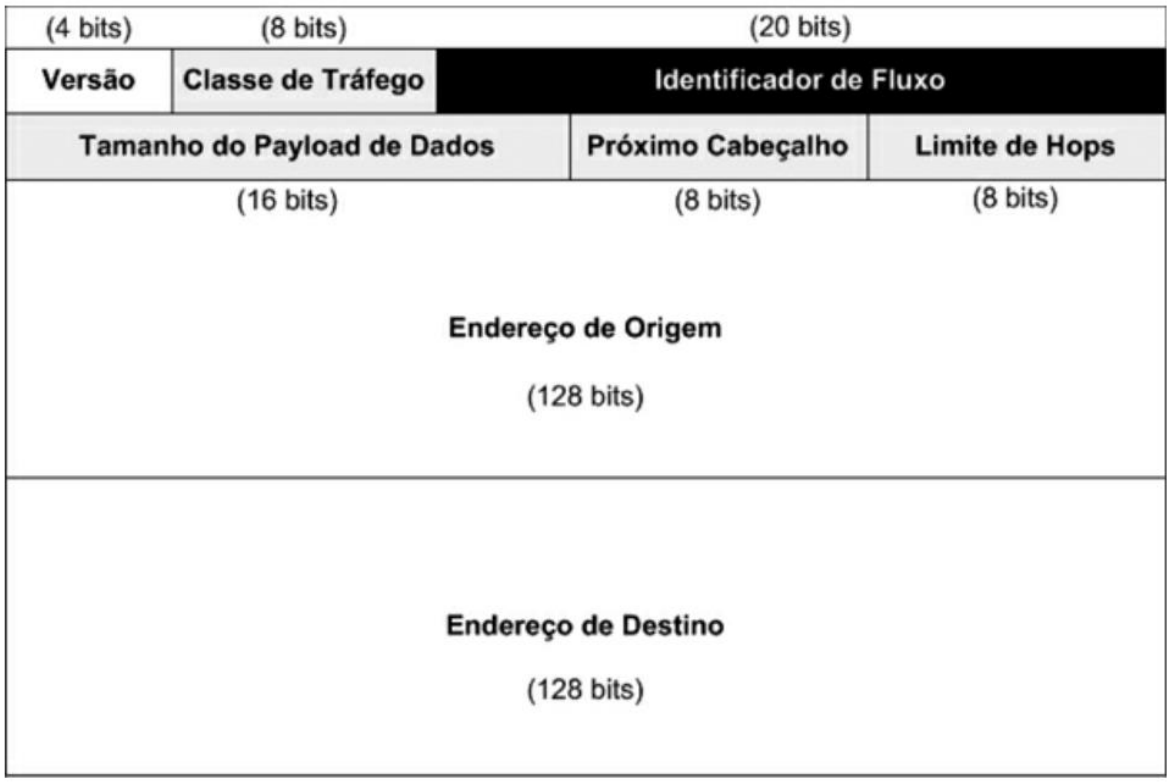
Além do aumento significativo de endereços, o IPv6 possui outras vantagens em relação ao IPv4 (BRITO, 2013), tais como:

- Espaço quase ilimitado de endereços;
- Cabeçalho simplificado e de tamanho fixo;
- Processamento simplificado nos roteadores;
- Recomendações internacionais de agregação de prefixos;
- Dispensa de adoção de NAT, preservando o modelo fim-a-fim;
- Segurança embutida (*Internet Protocol Security* - IPSec);
- Suporte à mobilidade (*Mobile Ipv6* - MIPv6).

3.1 O CABEÇALHO DO IPV6

O cabeçalho do IPv6, apresentado na Figura 5, possui oito campos: “Versão”; “Classe de Tráfego”; “Identificador de Fluxo”; “Tamanho do Playload de Dados”; “Próximo Cabeçalho”; “Limite de Hops”; “Endereço de Origem” e “Endereço de Destino”.

Figura 5. Cabeçalho do protocolo IPv6



Fonte: Brito (2013).

Os campos do cabeçalho do protocolo IPv6, apresentados ainda na Figura 5, são assim descritos:

1. Versão: identifica a versão do protocolo utilizado, 0110 (6 em decimal).
2. Classe de Tráfego: identifica os pacotes por classes de serviços ou prioridade. Ele provê as mesmas funcionalidades e definições do campo “Tipo de Serviço” do IPv4.
3. Identificador de Fluxo: identifica pacotes do mesmo fluxo de comunicação. Esse campo é configurado pelo endereço de destino para separar os fluxos de cada uma das aplicações e os nós intermediários de rede, os quais podem utilizá-lo de forma agregada com os endereços de origem e destino para realização de tratamento específico dos pacotes, possibilitando a aplicação de *Quality of Service* (QoS), por exemplo.
4. Tamanho do Payload de Dados: indica o tamanho, em bytes, apenas dos dados enviados junto ao cabeçalho IPv6. Substituiu o campo “Tamanho Total” do IPv4, que indicava o tamanho do cabeçalho mais o tamanho dos dados transmitidos. Contudo, os tamanhos dos cabeçalhos de extensão também são somados nesse novo campo (mostrado com fundo preto na Figura 5).
5. Próximo Cabeçalho: identifica o cabeçalho de extensão que segue o atual. Ele foi renomeado (no IPv4 chamava-se “Protocolo”) para refletir a nova organização dos pacotes IPv6, uma vez que ele deixou de conter os valores referentes a outros protocolos, para indicar os tipos dos cabeçalhos de extensão.
6. Limite de Hops: esse campo é decrementado a cada salto de roteamento e indica o número máximo de roteadores pelos quais o pacote pode passar antes de ser descartado. Ele padronizou o modo como o campo “Tempo de Vida” (ou *Time to Live* - TTL) do IPv4 vinha sendo utilizado, o qual diferia significativamente da descrição original que o definia como o tempo, em segundos, para o pacote ser descartado caso não chegasse ao seu destino.
7. Endereço de origem (128 bits): indica o endereço de origem do pacote.
8. Endereço de Destino (128 bits): indica o endereço de destino do pacote.

Uma característica importante é que o cabeçalho possui tamanho fixo de 40 bytes, impactando assim no desempenho dos roteadores, uma vez que essa abordagem simplifica o processamento dos equipamentos, pois não precisam mais

analisar o *Internet Header Length* (IHL, ou comprimento do cabeçalho da internet) para determinar o tamanho do cabeçalho, antes de analisar o restante das informações de controle (BRITO, 2013).

Os quatro campos, destacados em cinza novamente na Figura 5, foram renomeados apenas para melhor representar suas atribuições no contexto do IPv6, mais facilmente compreendidos na Tabela 2.

Tabela 2. Campos renomeados no IPv6

Nome do Campo	
Protocolo IPv4	**Protocolo IPv6**
Tipo de serviço (ou *Type of Service* - ToS)	Classe de tráfego (TC)
Tamanho total	Tamanho do *Payload* de dados
Protocolo	Próximo cabeçalho
Tempo de vida (ou *Time to Live* - TTL)	Limite de *hops*

Fonte: Brito (2013).

No IPv4 o campo Protocolo apontava para o protocolo de camada superior, o que não ocorre com o IPv6, o qual aponta para um cabeçalho de extensão.

3.1.1 Cabeçalhos de Extensão

O cabeçalho IPv6 foi desenhado para possuir menos campos e com tamanho fixo de 40 bytes, não possui portanto, um campo de opções (*options* + *padding*) para contemplar as informações complementares, as quais, se existissem, seriam inseridas neste campo do cabeçalho do IPv4. No IPv6, as funcionalidades que anteriormente eram utilizadas no campo de opções, estão a cargo de cabeçalhos adicionais, chamados de cabeçalhos de extensão, de modo que esses cabeçalhos não precisam ser verificados pelos roteadores intermediários na comunicação entre dois nós, resultando em melhor performance na rede em decorrência de um menor esforço computacional no processo de roteamento. Desta forma, o cabeçalho IPv6 agrega apenas as funcionalidades que são realmente necessárias, adicionando novas funcionalidades separadas do cabeçalho principal.

Um ou mais cabeçalhos de extensão são anexados ao cabeçalho IPv6, de maneira encadeada através dos seus códigos de próximo cabeçalho, promovendo flexibilidade para que sejam implementadas diferentes funcionalidades. Na RFC 2460, é recomendado que os cabeçalhos de extensão sigam a sequência de encadeamento detalhada na Tabela 3.

Tabela 3. Encadeamento de cabeçalhos de extensão no IPv6

Ordem	Nome do cabeçalho	Código do campo "Next Header"
01	Cabeçalho IPv6 convencional	-
02	*Hop-by-Hop*	0
03	*Destination Options*	60
04	*Routing Header*	43
05	*Fragment Header*	44
06	*Authentication Header* (AH)	51
07	*Encapsulation Security Payload* (ESP)	50
08	*Destination Options*	60
09	*Mobility*	135
-	Ausência de próximo cabeçalho	59
Camada superior	ICMPv6	58
Camada superior	UDP	17
Camada superior	TCP	6

Fonte: Brito (2013).

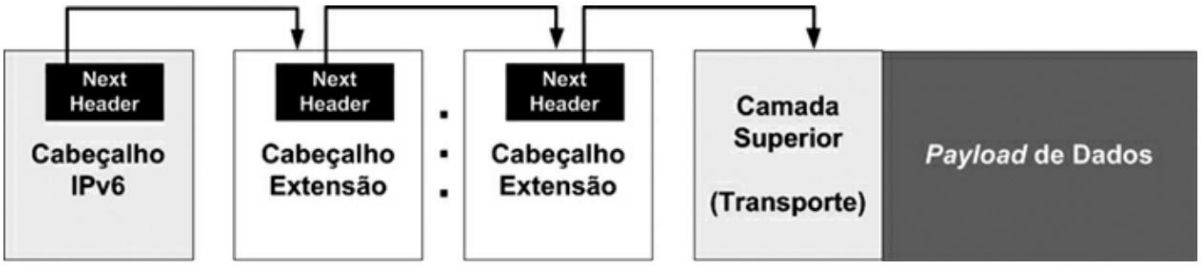
Descrevendo os cabeçalhos apresentados, ainda da Tabela 3, “Hop-by-Hop”; “Destination Options”; “Routing Header”; “Fragment Header”; “Authentication Header”; “Encapsulation Security Payload” e “Destination Options”; com suas respectivas finalidades descritas a seguir:

- *Hop-by-Hop options*: informações gerais para os roteadores. Deve vir logo após o cabeçalho base IPv6, já que ele é o único cabeçalho a ser examinado por cada nó intermediário.
- *Destination options*: informação adicional para o destinatário. Pode aparecer duas vezes na cadeia de cabeçalhos, sendo uma antes da extensão de roteamento e outra antes do protocolo da camada superior.
- *Routing*: originalmente desenvolvido para carregar informações para determinar a rota. Por esse motivo trazia campos adicionais para armazenar mais endereços representando os roteadores intermediários, tornando-se obsoleto na RFC 5095, sendo definido um novo cabeçalho "*Routing Type* 2", como parte da solução de mobilidade, utilizado por outro cabeçalho de extensão, responsável pelas funcionalidades de mobilidade do protocolo MIPv6.
- *Fragmentation*: responsável pelo gerenciamento da fragmentação dos pacotes.
- *Authentication Header* e *Encapsulatoing Security Payload*: viabiliza as soluções de autenticação, integridade e confidencialidade (criptografia).
- *Destination options*: informação adicional sobre o destinatário.

Desses cabeçalhos, apresentados ainda na Tabela 3, o único que é interpretado por todos os roteadores é o “Hop-by-Hop” e em função disso, é obrigatório

que ele seja o primeiro cabeçalho de extensão (Figura 6), sendo que todos os demais, serão analisados pelo destinatário informado no campo “Endereço de Destino”.

Figura 6. Encadeamento de cabeçalhos de extensão no IPv6



Fonte: Brito (2013).

3.2 ESTRUTURA DO ENDEREÇO IPV6

O IPv6 foi desenvolvido, entre outras finalidades, para solucionar o problema da escassez de endereços disponíveis no IPv4, passando de 32 bits de seu antecessor, para 128 bits, o que permite o endereçamento de 340 undecilhões de endereços públicos na internet.

Em Ipv6.br (2012c), o endereço IPv6 é escrito no formato hexadecimal (base 16), composto de 8 grupos de 16 bits, separados pelo caractere ":", como por exemplo o endereço: “2001:0b8:cafe:0000:5097:0000:0000:7518”.

Na representação de um endereço IPv6 é permitido utilizar caracteres maiúsculos e minúsculos (IPV6.BR, 2012c), em qualquer combinação entre eles, como “CaFe", “CAFe", “cafe", “CAFÉ”, entre outras.

O endereço pode ser simplificado de duas formas, sendo que a primeira permite que todos os zeros à esquerda sejam omitidos, de modo que “00b1” e “b1” são equivalentes, da mesma forma que “0000” e “0” também se equivalem. A outra forma, consiste em suprimir as cadeias consecutivas de zeros. Essa supressão, pode ser utilizada no endereço apenas uma vez, evitando possíveis ambiguidades. Sendo assim, o endereço “2001:0db9:0000:0000:0000:0000:00b1”, poderia ser representado como “2001:db9:0:0:0:0:b1”, ou ainda “2001:db9::b1”, reduzindo significativamente o tamanho da representação do endereço.

No IPv6, foi mantido o princípio hierárquico do IPv4, cuja primeira parte do endereço identifica a rede (prefixo), e a segunda parte, identifica um host dentro desta rede (sulfixo). A rede, deve ser referenciada através da notação CIDR, uma vez que no IPv6 não existe mais a máscara de rede.

As redes locais devem ser “/64”, de acordo com a RFC 4291, independentemente da quantidade de *hosts*.

Para referenciar IPv6 na URL dos navegadores, embora pouco usual em função da utilização da resolução de nomes de domínio através de servidores DNS, o endereço deve ser colocado entre colchetes ([ ]), dessa forma não há conflitos com a representação das portas (*socket*), como por exemplo: <http://[201:db8:0ca7::1]:8080/index.htm>.

3.3 TIPOS DE ENDEREÇOS

Há vários tipos de endereços associados ao modo de comunicação das redes. No protocolo IPv4 os endereços eram classificados em três tipos: *unicast*, *multicast* e *broadcast* (IPV6.BR, 2012c). Já no protocolo IPv6 os tipos de endereços existentes são: *unicast*, *multcast* e *anycast* (IPV6.BR, 2012c).

3.3.1 Endereços Unicast

São responsáveis por identificar um host de maneira única, por meio de uma interface específica. No IPv6 existem endereços suficientes para cada que cada host na internet tenha seu endereço *unicast* público, viabilizando o modelo fim-a-fim.

Os endereços *unicast* podem ser do tipo: a) “link-local”; b) “unique-local address”; e c) “global unicast".

3.3.1.1 Link-local

Reservados exclusivamente para comunicação local em nível de enlace. Os endereços são iniciados em “FE80::/10”. Os dez primeiros bits do endereço, compreende o seguinte intervalo possível “FE80::/10”, “FE90::/10”, “FEA0::/10” e “FEB0::/10”, sendo complementado os 54 bits restantes com “0”, formando um prefixo “/64”. O sulfixo de 64 bits que identifica o *host* é gerado automaticamente a partir do endereço “mac address” da interface de rede.

3.3.1.2 Unique-local address

Os endereços *Unique-Local Address* (ULA) são equivalentes ao endereços privados no IPv4 e só podem ser atribuídos no contexto local, de modo que não devem ser roteados para internet.

No projeto IPv6 (IPV6.BR, 2012c), foi reservado um bloco “FC00::/7” para endereços privados, entretanto após algumas divergências, os endereços ULA sofreram algumas mudanças. De acordo com a RFC 4193, o bloco “FC00::/7” foi dividido em dois blocos “/8”: a) “FC00::/8”; e b) “FD00::/8”.

Os endereços “FC00::/8” devem ser alocados por uma autoridade da internet responsável por atribuir um identificador global aleatório, de forma parecida com os endereços públicos. Entretanto os endereços ULA não devem ser visíveis/roteados na internet, assim como acontece com os endereços privados IPv4. Existem endereços ULA iniciados em “FD00::/8”, os quais poderão ser definidos localmente pela própria empresa, como era com os endereços privados IPv4. Contudo, existe a recomendação de que esses identificadores não sejam óbvios, como por exemplo: “FD00:0:0:1::/64”, “FD00:0:0:2::/64”, entre outros; conforme a recomendação da RFC 4193, um algoritmo pseudoaleatório deve ser utilizado na geração do identificador global, o qual geraria algo como “FD0B:AB3E:4C2B::/48”, de modo que poderiam ser derivadas sub-redes /64, cabendo ao quarto quarteto a identificação da sub-rede que pode ser sequencial (IPV6.BR, 2012c).

3.3.1.3 Global unicast

Os “Global Unicast”, São endereços públicos e roteáveis, de responsabilidade das autoridades da internet a distribuição de maneira coerente. A *Internet Assigned Numbers Authority* (IANA, ou autoridade para atribuição de números da internet) separou uma pequena quantidade de endereços IPv6 disponíveis na internet iniciados em “2000::/3”. O prefixo “2000::/3” equivale à faixa de endereços entre “2000:0:0:0:0:0:0:0” até “3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF”, sendo todos os demais endereços disponíveis para uso futuro (IPV6.BR, 2012c).

3.3.2 Endereços Multcast

São endereços utilizados em aplicações de comunicação de natureza “um para muitos”, como por exemplo serviços de teleconferência, serviços de

monitoramento distribuído, entre outros. Os endereços *multcast* (Tabela 4) são iniciados em “FF00::/8”, conforme RFC 3306, os quais não podem ser utilizados na origem de uma comunicação, pois representa um grupo composto de múltiplos nós. Todas as interfaces dos computadores de uma rede local fazem parte de um grupo *multcast-all-nodes* (FF02::1). Em função desse grupo *multcast* que o endereço de broadcast pôde ser eliminado no IPv6. Outro grupo fundamental para o IPv6 é o *multcast-all-routers* (FF02::2), em que todas as interfaces dos roteadores são associadas.

Tabela 4. Endereços multicast do IPv6

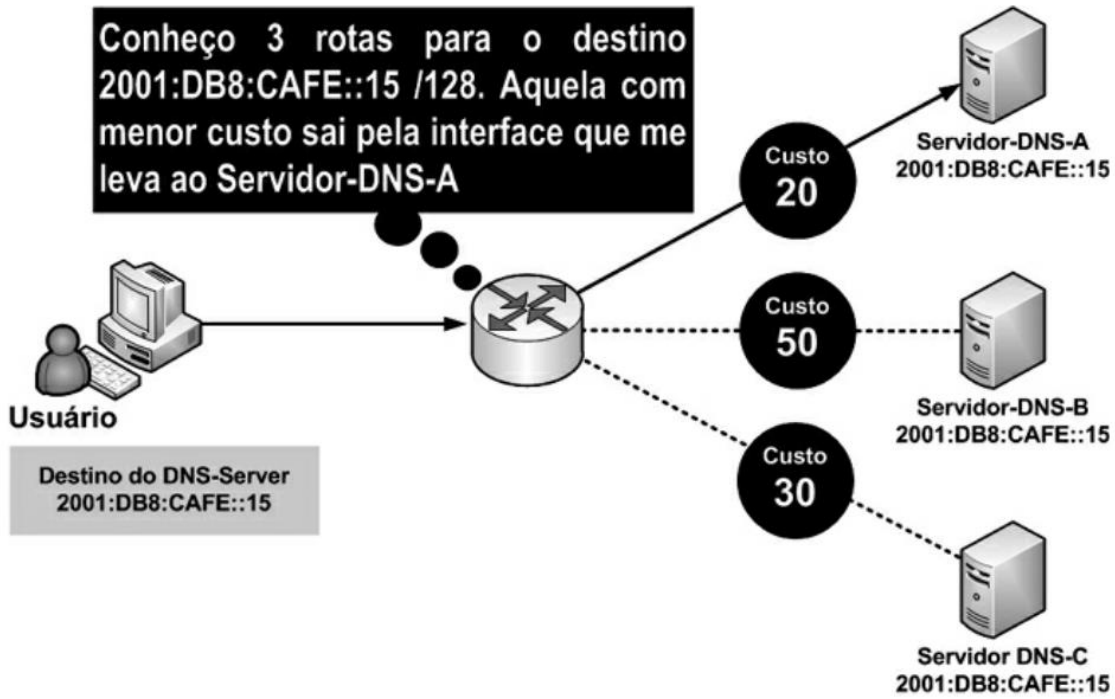
Endereço	Escopo	Descrição
FF01::1	Interface	Todas as interfaces
FF02::1	Enlace	Todos os *hosts* do link
FF02::2	Enlace	Todos os roteadores no link
FF02::5	Enlace	Protocolo OSPFv3 (roteadores)
FF02::6	Enlace	Protocolo OSPFv3 (roteadores designados)
FF02::9	Enlace	Protocolo RIPng
FF02::A	Enlace	Protocolo Cisco EIGRP
FF02::1:FFXX:XXXX	Enlace	*Solicited-Node*
FF02::1:2	Enlace	Todos os servidores DHCP e *relay-agents*
FF05::1:3	Site	Todos os servidores DHCP
FF0X::101	Variável	Todos os servidores NTP

Fonte: Brito (2013).

3.3.3 Endereços Anycast

Os endereços *anycast*, com exemplo de comunicação apresentado na Figura 7, consiste em uma comunicação destinada para o nó mais próximo de um grupo de nós (um para um de muitos ou um para mais próximo). Esse modelo de comunicação possibilita a atribuição de um mesmo endereço “*unicast*” para múltiplos computadores, desde que na sua configuração, seja explicitamente informada a palavra *anycast*. Desta forma, a inteligência de encaminhamento dos pacotes para o nó mais próximo, é responsabilidade dos roteadores intermediários, de modo que os mesmos devem ter configurada uma entrada separada /128 que equivale ao host. Um exemplo dessa aplicação é um cenário em que existem vários servidores DNS pelo ambiente, situação comum na internet, de forma a garantir que às maquinas clientes, que o processo de resolução de nomes sempre será direcionado para o servidor mais próximo, otimizando o desempenho da rede (BRITO, 2013).

Figura 7. Exemplo de comunicação *anycast*



Fonte: Brito (2013).

3.3.4 Endereços Especiais

Além dos tipos de endereços citados anteriormente, existem ainda alguns endereços especiais no IPv6 que são reservados para algumas finalidades específicas.

O prefixo “2001:DB8::/32” é reservado para ser utilizado em textos e documentações, de modo a não expor nenhum endereço público nos documentos técnicos.

No IPv4 o bloco “127.0.0.0/8” é reservado para *loopback*, ou seja, para teste de conectividade local, totalizando 16 milhões de endereços disperdiçados. No IPv6, se utiliza apenas um endereço de *loopback*, o “0:0:0:0:0:0:0:1/128” (ou apenas “::1” no seu formato abreviado).

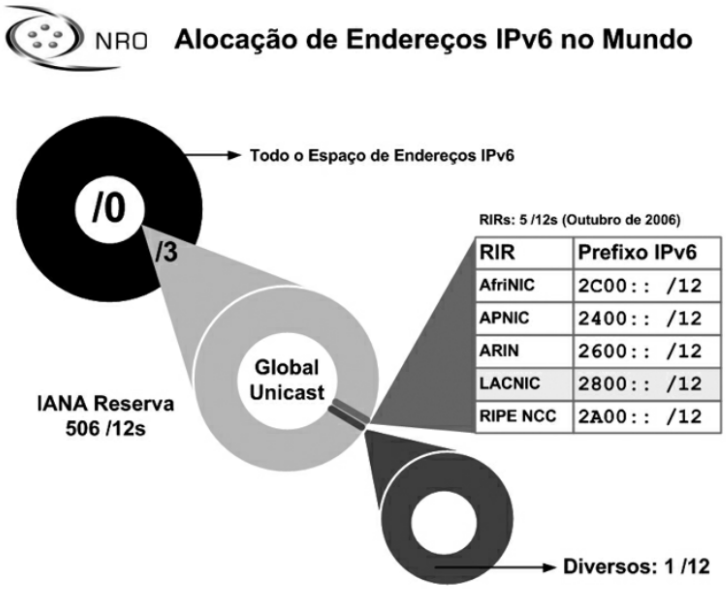
Outro endereço especial é o “endereço não especificado”, o qual é escrito no formato “::/128”. Ele indica a ausência de um endereço e ocorre na inicialização da interface. Do mesmo modo, o endereço de rota padrão no IPv6 é escrito no formato “::/0”, utilizado nos roteadores para uma saída quando não houver rota mais específica.

O endereço IPv4-Mapeado, é representado por “0:0:0:0:FFFF:<IPv4>” e é utilizado para criar um mapeamento entre um endereço IPv4 e um endereço IPv6. Os primeiros cinco quartetos representam uma sequência de zeros, o sexto é uma sequência de Fs, restando dois quartetos (32 bits), a quantidade de bits do IPv4, sendo permitido representar o sétimo e o oitavo quartetos no formato decimal pontuado como se representa o IPv4. Por exemplo o endereço: “0:0:0:0:0:FFFF:203.0.113.1”, comumente utilizado para dispositivos de rede como *access-point*, *firewalls*, *appliances*, entre outros.

3.4 ALOCAÇÃO DE ENDEREÇOS GLOBAIS

Todos os prefixos IPv6 (Figura 8), além dos demais recursos, como nomes de domínio, ASN e IPv4, estão sob gestão e coordenação da autoridade mundial da internet (IANA), a qual distribuiu um prefixo “/12” para cada uma das cinco RIR (autoridades regionais) administrarem. Um prefixo “/12” representa uma quantidade considerável de endereços, aos quais estão sub responsabilidade de cada RIR, como por exemplo o *Latin America and Caribbean Network Information Centre* (LACNIC), autoridade da América Latina e Caribe, que possui o prefixo “2800::/12”.

Figura 8. Prefixos IPv6 alocados às cinco autoridades regionais



Fonte: Brito (2013).

De acordo com Brito (2013), os prefixos da figura 8 foram retirados do relatório oficial publicado pela *Number Resources Organization* (NRO) referente à utilização

dos recursos da internet no mundo, a qual é uma organização composta por todas as cinco autoridades regionais da internet. Ainda em relação a figura 8, mostra que a IANA reservou 506 prefixos /12 para atribuição mundial, no entanto, apenas cindo desses prefixos foram oficialmente distribuídos.

No Brasil, o NIC.br, autoridade nacional da internet, recebeu do LACNIC um prefixo /16 (2801:: /16) para coordenar e distribuir no país.O NIC.br, através do grupo de trabalho IPv6.br, recomenda que as operadoras de telecomunicações recebem um prefixo /32, as empresas recebam um prefixo /48, os usuários residenciais recebam um prefixo /56, os usuários de tecnologias móveis recebam um prefixo /64, de modo que a operadora reserve um prefixo /56 para esses usuários.

Segundo a recomendações da RFC 4291, os prefixos IPv6 não devem ultrapassar prefixos de 64 bits, de modo a assegurar o correto funcionamento utilizado na identificação dos hosts.

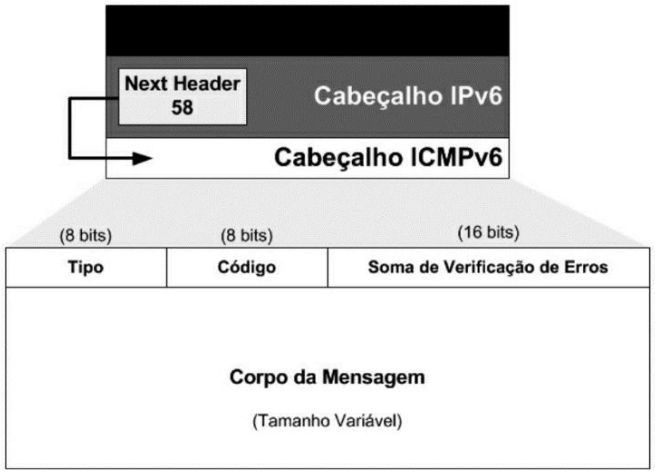
3.5 ICMPV6 E CONFIGURAÇÃO DE ENDEREÇOS

O *Internet Control Message Protocol Version 6* (ICMPv6), especificado na RFC 4443, é extremamente importante na operacionalização do IPv6, assim como no IPv4, é a base de operação por trás do “ping”, o software mais comum utilizado para testar se existe conectividade entre dois hosts. Entretanto, sua importância no IPv6 vai muito além do que em seu antecessor. O ICMPv6 possui funcionalidades necessárias para o bom funcionamento da rede, de modo que não pode mais ser simplesmente bloqueado pelos firewalls, como era comum com o ICMPv4, uma vez que não estão restritas apenas ao diagnóstico da rede. O ICMPv6 assume novas funções importantes para o funcionamento da rede, funções estas que no IPv4 eram de responsabilidade de outros protocolos, tais como ARP, RARP e IGMP.

O protocolo NDP, especificado na RFC 4861, atua sobre o ICMPv6. Os hosts conectados no mesmo enlace, utilizam este protocolo para a descoberta de vizinhança, para descobrir as presenças uns dos outros e determinar os endereços físicos (ou *Media Access Control* - MAC) dos vizinhos, para encontrar roteadores, descobrir prefixos de rede e manter a informação de alcançabilidade dos vizinhos ativos.

O ICMPv6 é integrado ao IPv6 através da sinalização do código 58 no campo “Próximo Cabeçalho (*Next Header*)”, do cabeçalho convencional do IPv6, inserindo assim um novo cabeçalho do ICMPv6 com suas funcionalidades adicionais, como mostra a Figura 9.

Figura 9. Cabeçalho do ICMPv6



Fonte: Brito (2013).

O cabeçalho ICMPv6 possui dois campos de tipo/código para representar o formato das mensagens de controle, um campo de verificação de erros para checar a integridade das mensagens de controle e um campo de tamanho variável para a mensagem propriamente dita. As mensagens podem ser agrupadas em duas categorias:

a. Mensagens de erro: identificadas pelo bit mais representativo à esquerda igual a 0 no campo “Tipo”, variando entre 0 e 127 (Tabela 5).

Tabela 5. Principais mensagens de erro do ICMPv6

Tipo	Grupo	Código	Descrição
1	Destino inalcançável	0	Sem rota para o destino
		1	Comunicação com o destino administrativamente proibida
		2	Além do escopo do endereço da origem
		3	Endereço inalcançável
		4	Porta inalcançável
		5	Falha na política de ingresso/egresso
		6	Destino rejeitado
2	Pacote muito grande	0	Pacote ultrapassou o MTU
3	Tempo excedido	0	Limite de saltos excedido
		1	Limite de remontagem de fragmentação excedido
4	Problema de parâmetro	0	Campo inválido no cabeçalho IPv6
		1	Próximo cabeçalho inválido
		2	Opções inválidas
127	-	-	Reservado para novas mensagens de erro

Fonte: Brito (2013).

b. Mensagens de informação: identificadas pelo bit 1 no campo “Tipo”, variando entre 128 e 255 (Tabela 6).

Tabela 6. Principais mensagens de informaçao do ICMPv6

Tipo	Grupo	Código	Descrição
128	*Echo Request*	0	Utilizado no ping
129	*Echo Reply*	0	Utilizado no ping
255	-	-	Reservado para novas mensagens de informação

Fonte: Brito (2013).

3.5.1 Protocolo NDP na Descoberta da Vizinhança

O *Neighbor Discovery Protocol* (NDP) funciona a partir do ICMPv6, de modo que raramente necessita de configuração explicita, entretanto, está presente nas máquinas e roteadores, executando tarefas como (IPV6.BR, 2012c):

- Descoberta de parâmetros de enlace;
- Autoconfiguraçao de endereços (ou *StateLess Address AutoConfiguration* - SLAAC);
- Descoberta de roteadores e prefixos;
- Resolução de endereços físicos (ou *Media Access Control* - MAC);
- Detecção de endereços duplicados (ou *Duplicate Address Detection* - DAD);
- Detecção de atividade no vizinho;
- Redirecionamento de roteadores.

Além das mensagens de erro e mensagens de informação abordadas anteriormente na Tabelas 5 e na Tabela 6, o NDP possui tipos de mensagens para fins de descoberta de vizinhança (Tabela 7).

Tabela 7. Mensagens ICMPv6 do protocolo NDP

Tipo	Mensagem	Descrição
133	*RS - Router Solicitation*	Enviada pelos hosts para encontrar roteadores
134	*RA - Router Advertisement*	Enviada periodicamente pelos roteadores
135	*NS - Neighbor Solicitation*	Enviado para obter informações de vizinhança
136	*NA - Neighbor Advertisement*	Enviada por um host como resposta à solicitação
137	*Redirect*	Enviado por roteadores para redirecionar rota

Fonte: Brito (2013).

As mensagens RS são utilizadas por máquinas que necessitam localizar roteadores em sua rede local para identificar o prefixo que deve ser utilizado no processo de autoconfiguração de seu endereço global. Por outro lado, os roteadores da rede, periodicamente enviam mensagens RA para anunciá-los ou em resposta às

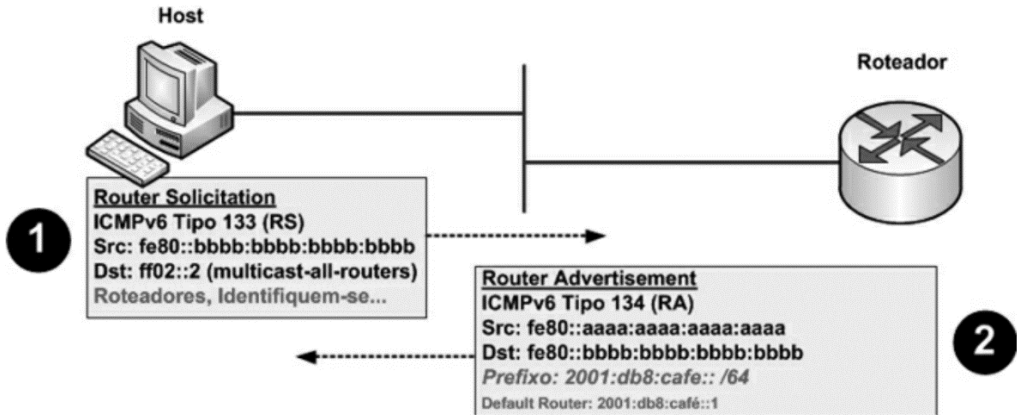
mensagens RS. De maneira objetiva, a mensagem Neighbor Solicitation (NS) é originada por algum host na rede que necessita obter informações sobre outro vizinho, o qual responde através de uma mensagem *Neighbor Advertisement* (NA). Mensagens entre NS/NA podem ser trocadas entre hosts quando precisam realizar três tarefas. São elas:

a. Resolução de endereços físicos;
b. Detecção de endereços duplicados;
c. Detecção de atividade no vizinho.

3.5.1.1 Descoberta de roteadores e prefixos

Quando entra na rede, uma estação de trabalho envia uma mensagem RS para localizar um ou mais roteadores na rede local. Essa máquina então, origina um pacote ICMPv6 RS (Tipo 133) com destino ao endereço FF02::2 (*multcast-all-routers*), de modo que os roteadores respondem com uma mensagem ICMPv6 RA (Tipo 134) destinado ao endereço *unicast link-local* da máquina solicitante. O importante das mensagens RA é que nelas, o roteador passa informações sobre o prefixo da rede e o endereço do *gateway*. A Figura 10, ilustra a troca de mensagems RS e RA.

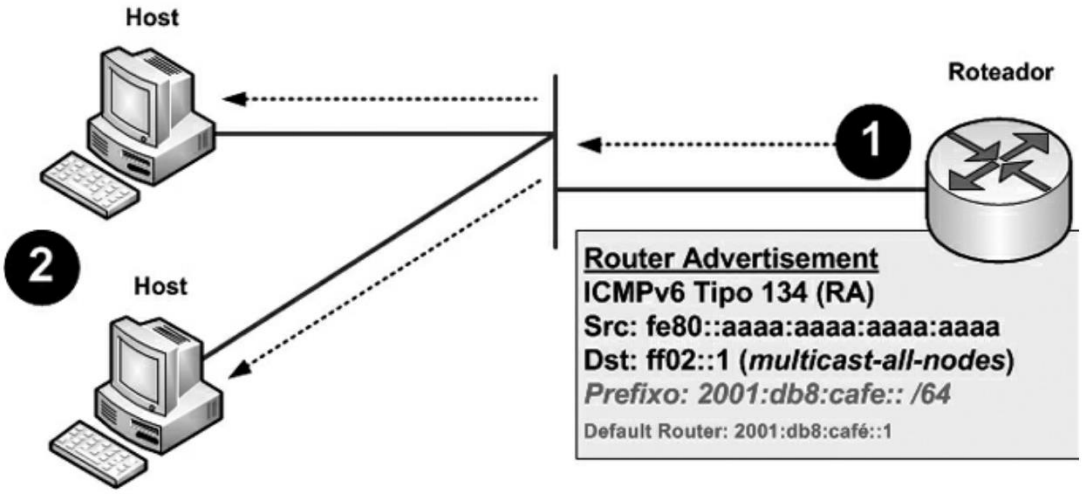
Figura 10. Troca de mensagens RS e RA



Fonte: Brito (2013).

Uma mensagem RA (Figura 11) não é apenas enviada em resposta a uma mensagem RS, de modo que é uma característica de roteadores do tipo *appliance* (“caixas” projetada para uma finalidade específica), que regularmente enviam mensagens ICMPv6 RA (Tipo 134) para o endereço FF02::1 (*multcast-all-nodes*).

Figura 11. Envio periódico de mensagens RA



Fonte: Brito (2013).

3.5.1.2 Resolução de endereços físicos em IPv6

O IP é um endereço lógico atribuído às interfaces de rede através do sistema operacional, para identificar as máquinas em uma rede. Entretanto, a comunicação ocorre com base no endereço físico, o qual é definido eletronicamente, ainda no processo de fabricação do equipamento, o endereço MAC.

No IPv6 a resolução de endereços lógicos em endereços físicos e de responsabilidade do NDP, por meio das mensagens ICMPv6 NS (Tipo 135) e NA (Tipo 136). É de responsabilidade dos sistemas operacionais manterem uma tabela de vizinhança contendo o IPV6 e o MAC dos hosts, a tabela de vizinhança.

Esse processo, definido na RFC 4861, consiste em um envio de mensagem a um “grupo” de nós para descobrir o endereço físico da interface com esse IPv6, dessa forma, a mensagem é destinada ao respectivo endereço *multicast-solicited-node*.

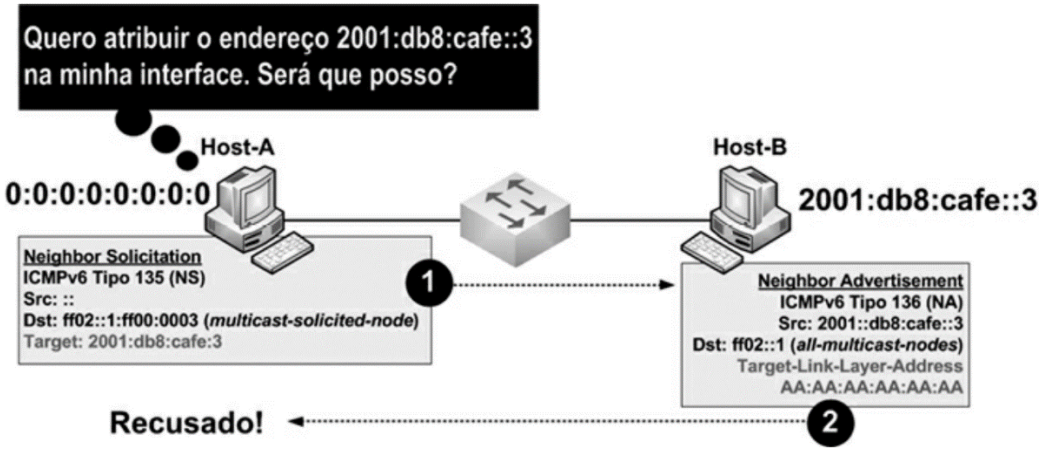
O campo *target* do cabeçalho é preenchido com o endereço IPv6 a ser resolvido, evitando assim que dois ou mais hosts tenham os mesmos 24 bits finais no seu endereço. Além disso, o campo *source-link-layer-address* que é preenchido com o endereço MAC da origem para evitar que o destino, ao receber a mensagem, tenha que refazer este processo de resolução de endereços, para obter o MAC do vizinho antes de responde-lo. Na segunda etapa, o outro host B recebe uma mensagem NS com o seu endereço IPv6 no campo *target*, o host B envia uma mensagem NA com o seu endereço MAC no campo *target-link-layer-address*, destinada ao Host A. Quando

o NA é recebido pelo Host A, é capaz de criar uma nova associação na sua tabela de vizinhança (BRITO, 2013).

3.5.1.3 Detecção de endereços duplicados

Não podem haver endereços IPs repetidos, a detecção de endereços duplicados é mostrada na Figura 12, uma vez que pela forma de sua implementação, não permite endereços duplicados na rede. A duplicidade de endereços acabaria com a inteligência do roteamento, uma vez que não seria possível definir um destino único para estabelecer essa comunicação.

Figura 12. Detecção de endereços duplicados



Fonte: Brito (2013).

Para evitar que isso ocorra, o NDP utiliza uma funcionalidade denominada *Duplicate Address Detection* (DAD, ou detecção de endereços duplicados) antes de atribuir um endereço IPv6 para uma interface, independentemente da configuração utilizada, como autoconfiguração, dinâmico ou estático. O host gera uma mensagem NS com o endereço de destino *multicast-solicited-node* gerado a partir do endereço que está prestes a ser atribuído a interface. A principal diferença é que o endereço de origem da mensagem é preenchido com o endereço especial não especificado (::), pois ainda não possui endereço. O IPv6 a ser checado é inserido no campo *target* da mensagem, de modo que se algum host responder à NS através de uma mensagem NA, o endereço já se encontra em uso e assim, o mesmo é recusado. Não havendo resposta, após a ocorrência de *timeout*, o endereço pode ser atribuído (BRITO, 2013).

3.5.1.4 Detecção de atividade no vizinho

Consiste em detectar se um determinado roteador se tornou inacessível na rede. Caso isso ocorra, o objetivo é manter a comunicação através de outra rota, desde que haja outro roteador na rede no mesmo enlace.

Essa operação consiste em detectar se há atividade depois de detectada a falha, enviando-se três novas mensagens NS para o endereço *unicast* do roteador vizinho. Se depois de um *timeout* houver uma resposta NA, o roteador vizinho continua ativo e a comunicação é normalizada. Isso não ocorrendo, o host de origem exclui a associação APv6-MAC daquele vizinho em sua tabela de vizinhança, e parte para busca de outro roteador no mesmo enlace.

3.5.1.5 Redirecionamento de rotas

Existe ainda, uma mensagem ICMPv6 do Tipo 137 denominada *Redirect*, a qual e utilizada por roteadores, com o objetivo de informar os hosts da existência de outro roteador na rede, o qual pode encaminhar os pacotes para um determinado destino através de um melhor caminho. Como os roteadores se comunicam para trocar informações de roteamento, para estes dispositivos é normal conhecer o melhor caminho para um determinado destino.

Quando um host tenta acessar algum destino fora de sua rede local, a comunicação é direcionada a seu *gateway*, no caso um roteador, de modo que este pode saber o destino desejado pode ser alcançado com o menor custo através de outro roteador existente no mesmo enlace. Uma mensagem *redirect* é enviada ao *host*, informando que os pacotes para aquele destino devem ser encaminhadas por outro roteador que oferece melhor desempenho.

3.5.2 Configuração do IPv6 nas Interfaces

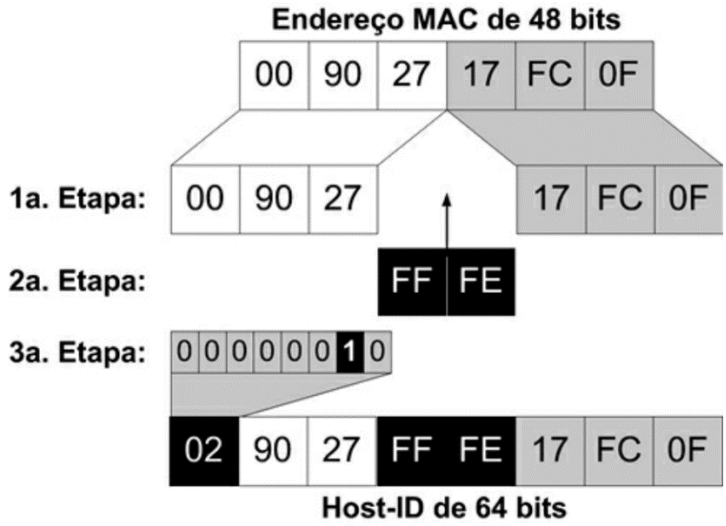
Os endereços podem ser atribuídos através de diversas formas, seja por autoconfiguração, configuração manual, configuração manual com função de expansão (denominada IEEE EUI-64: *Extended Unique Identifier*), DHCPv6 *stateless* ou DHCPv6 *stateful*.

3.5.2.1 Autoconfiguração stateless (slaac)

O processo de autoconfiguração de endereços IPv6 é determinado basicamente em duas etapas, configuração do prefixo e do sulfixo do host.

Os hosts obtém o prefixo da rede através de mensagem ICMPv6 Tipo 134 (RA) anunciadas pelos roteadores, conforme já mencionado anteriormente. Vale ressaltar que em redes IPv6, os roteadores são responsáveis por esta funcionalidade. Após a obtenção do prefixo, o sulfixo do host é gerado automaticamente a partir do endereço físico da placa de rede (MAC), o qual possui 48 bits. Em função disso, é aplicada a função de expansão denominada IEEE EUI-64 (*Extended Unique Identifier*) no endereço físico que preenche os demais 16 bits, utilizando um algoritmo padronizado, mostrado na Figura 13.

Figura 13. Aplicação da função EUI-64 na identificação do *host*



Fonte: Brito (2013).

A pós a aplicação da função de expansão, o prefixo é anexado ao identificador do host, uma vez que já existe um endereço *global unicast* automaticamente atribuído à interface.

Importante mencionar que os sistemas operacionais Microsoft Windows não utilizam a função EUI-64 a partir do MAC das interfaces. O sulfixo nesses sistemas operacionais são gerados aleatoriamente, por entender ser um risco de segurança, de acordo com a RFC 4941 (BRITO, 2013).

3.5.2.2 Dhcpv6

O *Dynamic Host Configuration Protocol version 6* (DHCPv6) foi definido na RFC 3315 e a comunicação entre o servidor e as estações de trabalho ocorre nas portas UDP 546 e 547, podendo ser utilizado através de duas modalidades: *stateless* e *stateful*.

A stateless permite aproveitar as funcionalidades do *StateLess Address AutoConfiguration* (SLAAC), de modo que cabe ao servidor DHCPv6 atribuir apenas as informações complementares importantes para a rede, como o servidor DNS, servidor de tempo (*Network Time Protocol* - NTP), servidor de arquivo (*Trivial File Transfer Protocol* - TFTP, utilizado em algumas soluções VoIP e wireless).

A modalidade *stateful* provê todas as informações de endereçamento, com o escopo explicitamente configurado e com registro das informações relacionadas aos endereços, normalmente empregado em servidores Linux e Windows, sendo possível executa-lo em alguns roteadores que possuem suporte e este recurso.

Em redes com apenas um servidor DHCP, é possível utilizar a opção *rapid-commit* em que o diálogo entre cliente e servidor ocorre com apenas duas mensagens, entretanto esse recurso necessita de uma configuração adicional no servidor e nos clientes.

Ainda existe um recurso totalmente novo no DHCPv6, o qual é denominado como delegação de prefixos, de modo que através desse recurso, um roteador que recebe um prefixo 2001:DB8:café::/56 de algum servidor DHCP da rede ou mesmo adicionado localmente é capaz de gerar automaticamente subprefixos /64 e entrega-los às sub-redes diretamente conectadas a ele, recurso interessante para provedores (BRITO, 2013).

3.6 SEGURANÇA

O IPv6, por ser um projeto mais recente, foi possível a correção de algumas vulnerabilidades em relação ao seu antecessor, entretanto, não se pode afirmar ser mais seguro, até porque, um protocolo que teve seu desenvolvimento até certo ponto muito recente, de modo que podem surgir novas vulnerabilidades e novas modalidades de ataque.

De qualquer forma, do ponto de vista arquitetural, o IPv6 é mais robusto em relação ao IPv4, uma vez que segurança foi um dos critérios mais relevantes na escolha da proposta que daria origem ao *IP next generation* (IPng). E neste contexto foi criado o *Internet Protocol Security* (IPSec), o qual veio a ser aproveitado para suprir uma necessidade urgente na versão 4.

Entretanto, a firmação de que o IPv6 é um protocolo mais seguro em função do IPSec ser um recurso nativo, não é verdadeira, embora o IPSec faça parte da suíte de protocolos da arquitetura TCP/IPv6, não está ativo por padrão, sendo necessário que o administrador realize as configurações adequadas para que seja de fato ativado.

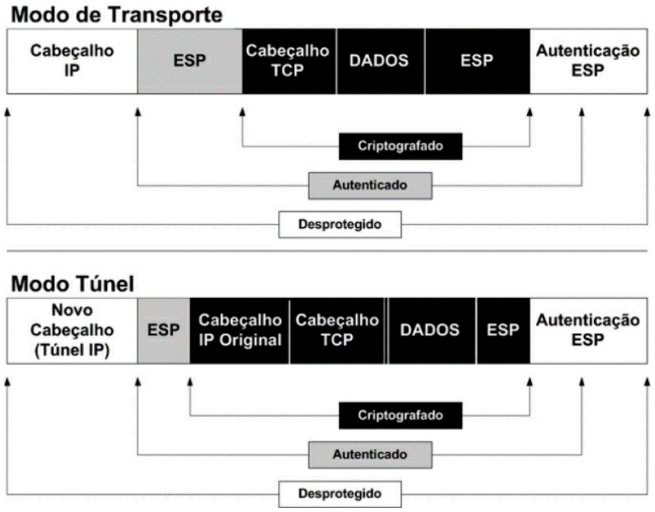
Outra questão de alta importância, é que a implantação do IPv6 deve ser planejada, pois existem muitas mensagens IPv6 decorrentes das operações ICMPv6, que implicam em tráfego desnecessário na rede, além cuidados na configuração dos firewalls, pois os sistemas operacionais modernos implementam túneis automáticos, tornando a rede IPv4 totalmente alcançável a partir da internet IPv6.

3.6.1 Ipsec

Especificado através da RFC 4301, o IPSec consiste em uma solução de segurança em nível da camada de rede, com o objetivo de proteger o tráfego na internet, o qual pode ser utilizado diretamente nos hosts ou nos roteadores e firewalls.

O IPSec, com os modos de operação apresentados na Figura 14, é comeposto por diversas tecnologias, as quais possui dois subprotocolos principais: AH e ESP.

Figura 14. Modos de operação do IPSec



Fonte: Brito (2013).

O IPSec, possui os seguintes modos de operação:

- Modo de Transporte: somente os dados (*payload*) são criptografados. Não há nenhuma alteração no cabeçalho da camada de rede, permitindo o roteamento normal dos pacotes pela internet, normalmente utilizado entre comunicações *host-to-host*.
- Modo Túnel: todo o pacote é criptografado, de modo que o pacote é encapsulado e recebe um novo cabeçalho (túnel). Normalmente utilizado em VPN *site-to-site* (entre roteadores/*firewalls* de borda).

A utilização do IPSec em VPNs para comunicação entre unidades remotas de uma empresa (*site-to-site*), proporciona um menor custo em relação a um link privativo (MPLS ou Ponto a Ponto, por exemplo), entretanto a empresa precisa fazer a gestão do acesso e da configuração dos roteadores/firewall das pontas.

O suporte nativo ao IPSec no IPv6 permite a simplificação de várias funcionalidades de segurança, como por exemplo em relação aos protocolos de roteamento dinâmico, os quais utilizavam soluções independentes de segurança. Com o IPv6/IPSec, são utilizados os cabeçalhos de extensão AH e ESP para fins de autenticação e criptografia.

3.7 DNSV6

O DNS é um dos mais importantes serviços de rede, sendo ele responsável por traduzir os nomes de domínio (*websites*), em endereço IP. Utilizado não só na internet, mas também em redes internas, atua de forma totalmente transparente para os usuários.

Seu funcionamento é muito similar ao do IPv4, cujo registro é do tipo A (32 bits). Para o IPv6 o registro passou a ser do tipo AAAA ou quad-A, de 128 bits. Como o servidor não tem forma de saber qual o protocolo utilizado pelo cliente que solicita a tradução do nome, serão providenciados ao cliente os registos tipo A e AAAA, sendo a versão 6 preferencial em relação a versão 4.

O endereço v6 reverso não pode ser abreviado, cada caractere é separado por “.”, e seu domínio raiz é IP6.ARPA (RFC 3596). Por exemplo, o nome do domínio de pesquisa inversa correspondente ao endereço: “4321:0:1:2:3:4:567:89ab”; seria: “b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.ARPA”.

Como o serviço é o mesmo e houve apenas a adição de um novo registro (AAAA), as buscas DNS funcionam para ambos os protocolos, independente da origem ser IPv4 ou IPv6.

3.7 MOBILIDADE

Uma das maiores deficiências do IPv4 era a ausência de suporte à mobilidade, uma vez que esse protocolo foi concebido em uma época em que não existiam dispositivos móveis conectados à internet. Para solucionar este problema, foi desenvolvida uma solução de mobilidade chamada MIP (*Mobile IP*).

Apesar do MIP viabilizar a mobilidade, estava baseada em um mecanismo de triangulação com arquitetura complexa e que tinha o desempenho comprometido.

No IPv6 passou a ser nativa, através de novos cabeçalhos de extensão, ao invés de necessitar do reencapsulamento dos pacotes, como ocorria no IPv4. O *Mobile IPv6* (MIPv6) opera de modo que cada nó móvel passa a ter dois endereços IP, um fixo de sua rede nativa e outro dinâmico que muda, conforme o dispositivo ingressa em outras redes no decorrer de seu deslocamento. O endereço fixo da rede nativa é chamado de *Home-of-Address* (HoA), enquanto o endereço dinâmico possui um prefixo na rede em que o nó móvel está se conectando, chamado de *Care-of-Address* (CoA). Na rede nativa, o dispositivo utiliza um agente nativo (*home agent*) que executa a solução de mobilidasde e fica responsável por manter uma tabela associando HoA - CoA, de modo que as conexões com a internet sempre se comunicam com o nó móvel através do seu HoA que não se altera.

O roteador nativo recebe os pacotes e os redireciona para a posição atual do nó móvel, por meio do seu CoA, uma vez que quando ocorre alguma alteração de rede, uma mensagem (*binding update*) é enviada para o roteador nativo para atualizar sua associação HoA - CoA. Através dos cabeçalhos de extensão do IPv6, e possível carregar os endereços CoA e HoA nos pacotes, de modo que o nó móvel encaminha os pacotes diretamente para o seu destino na internet, tendo como referência o seu endereço CoA como origem, obtendo como grande benefício em relação ao MIPv4, que o envio é direto do nó móvel para o destino do roteador nativo, conforme RFC 3775.

3.8 TÉCNICAS DE TRANSIÇÃO

É fato que a mudança de toda estrutura IPv4 na internet, não será alterada para IPv6 de forma automática, tão pouco ocorrerá de uma forma rápida e sem esforços.

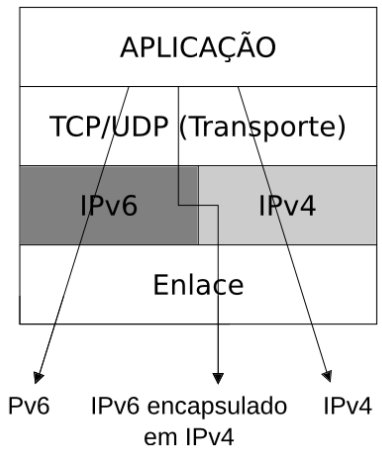
As técnicas de transição tem como objetivo, viabilizar a interoperabilidade entre as versões do protocolo IP, de modo que redes baseadas no IPv4 se comuniquem com redes IPv6, e vice versa.

Existem diversas técnicas de transição possíveis, entretanto, optar por uma ou outra, depende das particularidades de cada ambiente, em relação à facilidade de implementação e o resultado esperado (IPV6.BR, 2012c).

3.8.1 Pilha-dupla

O método da “Pilha-dupla” (Figura 15), consiste em instalar e configurar as duas versões, IPv4 e IPv6, nas máquinas e dispositivos de infraestrutura, implicando na existência das duas redes em paralelo. Essa técnica facilita no processo de transição, permitindo que a rede IPv4 seja desativada gradativamente, à medida que a rede IPv6 seja implementada (BRITO, 2013).

Figura 15. Funcionamento do método pilha-dupla



Fonte: Ipv6.br (2012c)

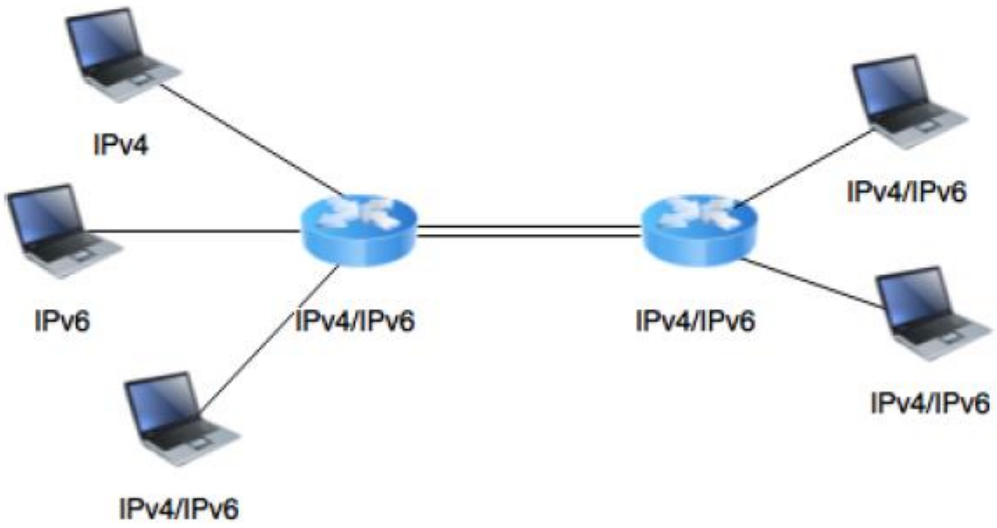
Segundo IPv6.BR, algumas questões referente à infraestrutura de rede devem ser consideradas ao se implementar a técnica de pilha dupla, tais como:

- Serviço de DNS deve possuir os endereços IPv6 (registros do tipo AAAA);
- Protocolo de roteamento com suporte IPv6 e IPv4;

- Regras de firewall adequadas ao IPv6.

Manter as duas pilhas IPv4 e IPv6 operando simultaneamente (Figura 16), aumenta a complexidade da tarefa de gestão da rede, pois com duas redes em paralelo, cada uma possui um plano de endereçamento, tabelas de roteamento, regras de *firewall*, configurações e estratégias de resoluções de nomes, entre outras questões que devem ser observadas, inclusive quanto a performance da rede (BRITO, 2013).

Figura 16. Representação de uma rede pilha-dupla

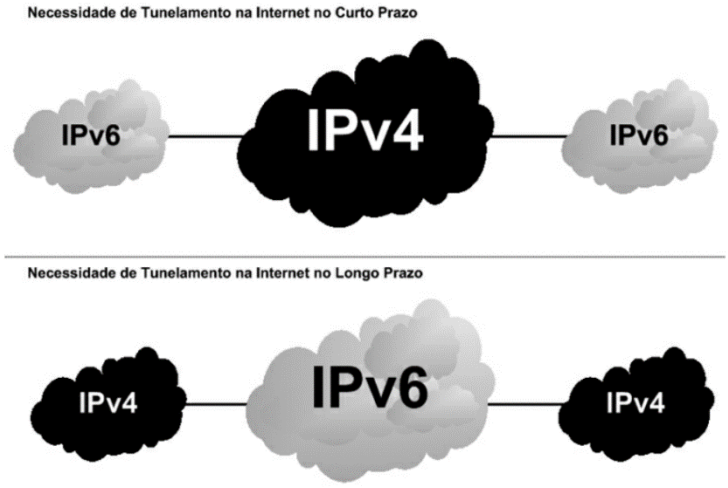


Fonte: Ribeiro (2015).

3.8.2 Tunelamento

As técnicas de tunelamento (Figura 17) consistem em encapsular um protocolo em outro, tornando possível que o tráfego baseado em um protocolo, possa ser transportado por outro, muito interessante quando o método de pilha-dupla não pode ser utilizado. A técnica de tunelamento e comum em cenários em que há um trânsito do protocolo IPv4 entre redes IPv6, contudo, é esperado que essa situação se inverta com a ampliação do protocolo v6.

Figura 17. Tendência de tunelamento a curto e longo prazos



Fonte: Brito (2013).

Apesar das técnicas de tunelamento serem atrativas, por serem de rápida implementação, apresentam um pior desempenho e contribuem para a manutenção do protocolo IPv4, de modo que supostamente podem contribuir para o atraso na disseminação do IPv6 (BRITO, 2013).

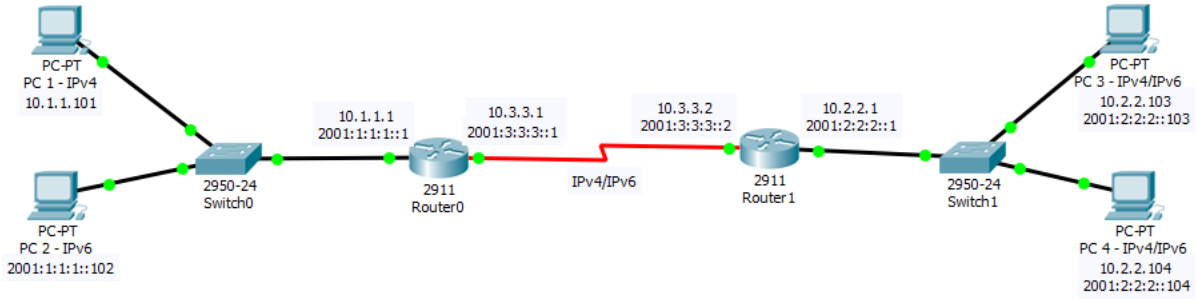
Existem várias técnicas de tunelamento, entre elas pode-se citar:

- Serviço de *Tunnel Broker*;
- Túnel Manual *6over4* (*6in4*);
- Túnel *6to4*;
- Túnel 6rd;
- Túnel Teredo;
- Túnel ISATAP;
- Túnel DS-Lite;
- Túnel L2TP.

3.9 IMPLEMENTAÇÃO PILHA-DUPLA

Como exemplo prático, apresentado na Figura 18, foi elaborado através do software Cisco Packet Tracer, versão 7.1, a implementação da técnica de transição Pilha-Dupla, a qual consiste em utilizar os protocolos IPv4 e IPv6 simultaneamente, nos mesmos dispositivos de rede.

Figura 18. Topologia exemplo do método pilha-dupla



Fonte: Autoria própria.

A Tabela 8, apresenta os endereçamentos dos dispositivos implementados no exemplo ainda da Figura 18.

Tabela 8. Endereçamentos dos dispositivos

Dispositivo	Interface	Endereço IP	CIDR
PC 1	FastEthernet 0	10.1.1.101	/24
PC 2	FastEthernet 0	2001:1:1:1::102	/64
Router0	GigabitEthernet 0/0	10.1.1.1	/24
		2001:1:1:1::1	/64
	Serial 0/3/0	10.3.3.1	/24
		2001:3:3:3::1	/64
Router1	GigabitEthernet 0/0	10.2.2.1	/24
		2001:2:2:2::1	/64
	Serial 0/3/0	10.3.3.2	/24
		2001:3:3:3::2	/64
PC 3	FastEthernet 0	10.2.2.103	/24
		2001:2:2:2::103	/64
PC 4	FastEthernet 0	10.2.2.104	/24
		2001:2:2:2::103	/64

Fonte: Autoria própria.

3.9.1 Configuração dos Roteadores

A configuração dos roteadores, “Router0” e “Router1” novamente implementados na Figura 18, apresenta:

- “Router0”:

  Router>enable

  Router#

  Router#configure terminal

  Router(config)#hostname R0

  - Configuração do protocolo IPv4 nas interfaces:

    R0(config)#interface g0/0

R0(config-if)#ip address 10.1.1.1 255.255.255.0
R0(config-if)#no shutdown
R0(config-if)#exit
R0(config)#
R0(config)#interface s0/3/0
R0(config-if)#ip address 10.3.3.1 255.255.255.0
R0(config-if)#no shutdown
R0(config-if)#^Z

- Configuração do protocolo IPv6 nas interfaces:

R0(config)#ipv6 unicast-routing
R0(config)#interface g0/0
R0(config-if)# ipv6 enable
R0(config-if)#ip address 2001:1:1:1::1/64
R0(config-if)#no shutdown
R0(config-if)#exit
R0(config)#
R0(config)#interface s0/3/0
R0(config-if)# ipv6 enable
R0(config-if)#ip address 2001:3:3:3::1/64
R0(config-if)#no shutdown
R0(config-if)#^Z

- Configuração do protocolo de roteamento RIP no IPv4:

R0(config)#router rip
R0(config-router)#version 2
R0(config-router)#no auto-summary
R0(config-router)#network 10.1.1.0
R0(config-router)#network 10.3.3.0
R0(config-router)#^Z

- Configuração do protocolo de roteamento RIP no IPv6:

R0(config)#ipv6 router rip TCC
R0(config-rtr)#exit

R0(config)#interface g0/0
R0(config-if)#ipv6 rip TCC
R0(config-if)#ipv6 rip TCC enable
R0(config-if)#exit
R0(config)#interface s0/3/0
R0(config-if)#ipv6 rip TCC enable
R0(config-if)#^Z
R0#wr

- “Router1”:
  Router>enable
  Router#
  Router#configure terminal
  Router(config)#hostname R1
  - Configuração do protocolo IPv4 nas interfaces:
    R1(config)#interface g0/0
    R1(config-if)#ip address 10.2.2.1 255.255.255.0
    R1(config-if)#no shutdown
    R1(config-if)#exit
    R1(config)#
    R1(config)#interface s0/3/0
    R1(config-if)#ip address 10.3.3.2 255.255.255.0
    R1(config-if)#no shutdown
    R1(config-if)#^Z

  - Configuração do protocolo IPv6 nas interfaces:
    R1(config)#ipv6 unicast-routing
    R1(config)#interface g0/0
    R1(config-if)# ipv6 enable
    R1(config-if)#ip address 2001:2:2:2::1/64
    R1(config-if)#no shutdown
    R1(config-if)#exit
    R1(config)#
    R1(config)#interface s0/3/0

```
R1(config-if)# ipv6 enable
R1(config-if)#ip address 2001:3:3:3::2/64
R1(config-if)#no shutdown
R1(config-if)#^Z
```

- Configuração do protocolo de roteamento RIP no IPv4

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#no auto-summary
R1(config-router)#network 10.2.2.0
R1(config-router)#network 10.3.3.0
R1(config-router)#^Z
```

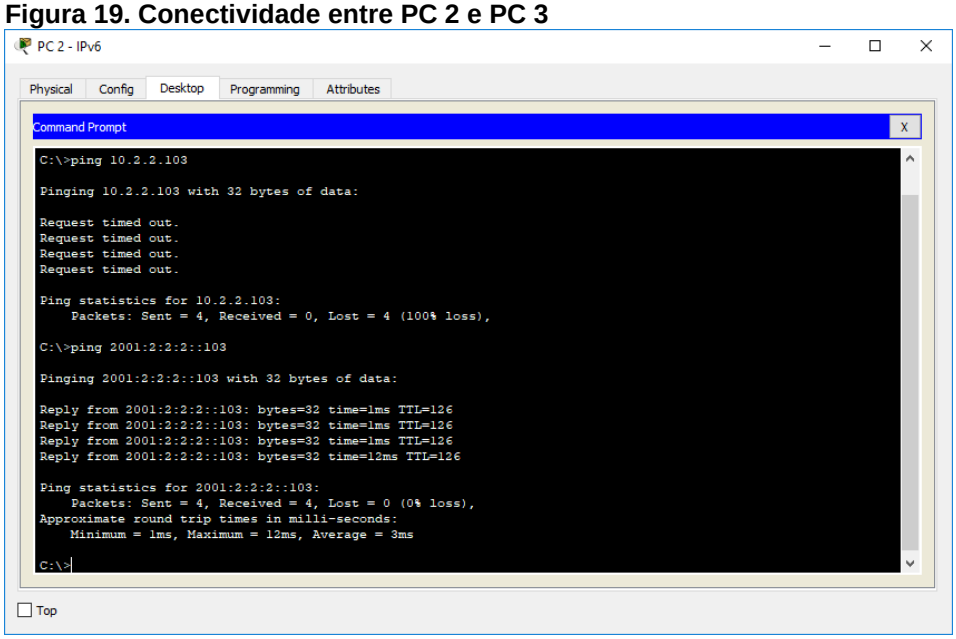
- Configuração do protocolo de roteamento RIP no IPv6

```
R1(config)#ipv6 router rip TCC
R1(config-rtr)#exit
R1(config)#interface g0/0
R1(config-if)#ipv6 rip TCC
R1(config-if)#ipv6 rip TCC enable
R1(config-if)#exit
R1(config)#interface s0/3/0
R1(config-if)#ipv6 rip TCC enable
R1(config-if)#^Z
R1#wr
```

3.9.2 Testes de Conectividade

O dispositivo “PC 2” com o dispositivo “PC 3” (Figura 19), conectividade apenas através do IPv6, uma vez que o PC 2 não foi configurado com o IPv4.

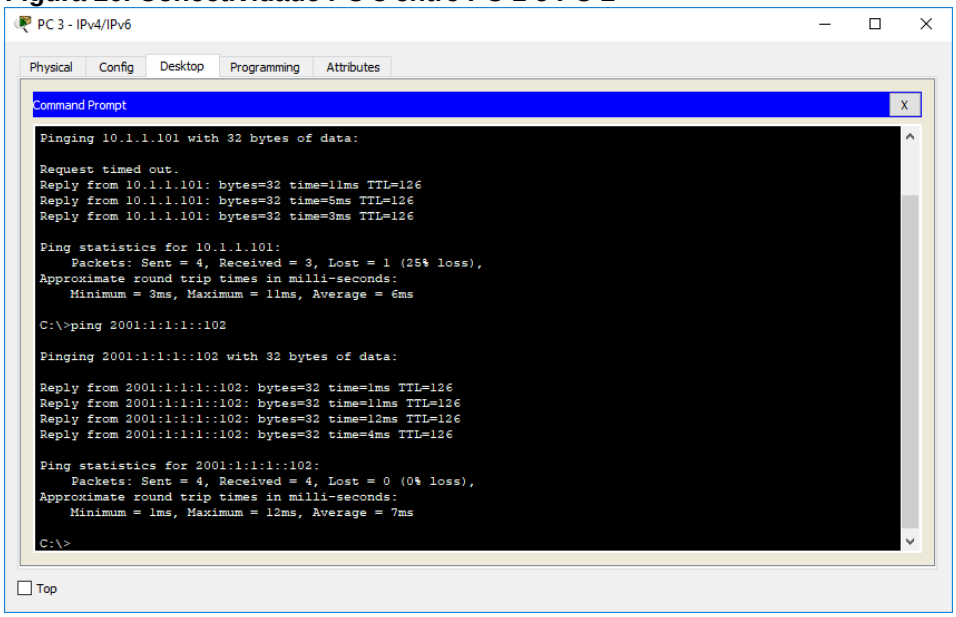
Figura 19. Conectividade entre PC 2 e PC 3



Fonte: Autoria própria.

O dispositivo PC 3 com PC 1 e PC 2 (Figura 20), conectividade com PC 1 através IPv4, e com PC 2 através do IPv6.

Figura 20. Conectividade PC 3 entre PC 1 e PC 2



Fonte: Autoria própria.

4. CONCLUSÃO

A implantação do IPv6 é importante para a evolução da internet, pois o esgotamento dos endereços IPv4 dificulta ou até mesmo inviabiliza a adoção de novos recursos e tecnologias.

As técnicas de transição facilitam implantação. Tem como principais pré-requisitos a compatibilidade dos dispositivos com o IPv6 e a análise do ambiente para definição da técnica mais adequada a ser utilizada. Possibilitando assim a implantação gradual do IPv6, uma vez que permite a utilização dos dois protocolos em paralelo.

A técnica Pilha-dupla simulada neste trabalho, se mostrou eficiente e de fácil implementação.

REFERÊNCIAS

BRITO, Samuel Henrique Bucke. **Ipv6 - O novo protocolo da internet**. São Paulo: Editora Novatec Ltda, 2013. p. 208.

IPV6.BR. **IPv6: transição**. Copyrigth by nic.br (Núcleo de Informação e Coordenação do Ponto BR), publicado em: 15 abr. 2012a. Disponível em: <http://ipv6.br/post/transicao/>. Acesso em: 19 set. 2018.

IPV6.BR. **IPv6: introdução**. Copyrigth by nic.br (Núcleo de Informação e Coordenação do Ponto BR), publicado em: 15 mai. 2012b. Disponível em: <http://ipv6.br/post/introducao/>. Acesso em: 19 set. 2018.

IPV6.BR. **IPv6: endereçamento**. Copyrigth by nic.br (Núcleo de Informação e Coordenação do Ponto BR), publicado em: 15 mai. 2012c. Disponível em: <http://ipv6.br/post/enderecamento/>. Acesso em: 19 set. 2018.

RIBEIRO, André Filipe Costa. **IPv6 - integração, transição e segurança**. Porto, Portugal: ISEP, 2015. Originalmente apresentada como dissertação de mestrado, Instituro Superior de Engenharia do Porto, área de Engenharia Informática, 2015. Disponível em: <http://recipp.ipp.pt/handle/10400.22/7093>. Acesso em: 10 jun. 2018.