UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDE

LUIS HENRIQUE BOGADO DE CARVALHO

IMPLEMENTAÇÃO DE IPV6 EM UMA REDE LOCAL VIRTUALIZADA

MONOGRAFIA

CURITIBA
2015

LUIS HENRIQUE BOGADO DE CARVALHO

IMPLEMENTAÇÃO DE IPV6 EM UMA REDE LOCAL VIRTUALIZADA

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Configuração e Gerenciamento de servidores e equipamentos de rede, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná – UTFPR
Orientador: Prof. MSc. Julliano de Mello Pedroso

CURITIBA
2015

RESUMO

CARVALHO, Luís Henrique. **Implementação de Ipv6 em uma rede virtualizada.** 2015. 55d f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

Esta monografia foi elaborada atravez de uma pesquisa bibliográfica em artigos, livros, monografias já publicadas e no estudo de caso da implantação do Ipv6 em uma rede virtualizada no GNS3. Essa atividade pratica consiste no passo a passo para emulação de duas lans remotas interconectadas através de seus roteadores, formando assim uma WAN com Ipv4. Após isso, é apresentado o passo a passo para configurar a comunicação Ipv6, com roteamento dinâmico através do protocolo RIPng da CISCO.

Palavras-chave: GNS3, Ipv6, Ipv4, RIPNg, Emulação.

ABSTRACT

CARVALHO, Luis Henrique. **IPV6 implementation in a virtualized network.** 2015. 55 p. Monograph (Specialization in Configuration and Network Server Management) - Graduate Program in Technology, Federal Technological University of Paraná. Curitiba, 2015.

This monograph was developed through a literature research for articles, books, monographs already published and in the case study of the implementation of IPv6 in a virtualized network in GNS3. This activity is practiced in the walkthrough for emulation two remote lans interconnected through their routers, thus forming a WAN with IPv4. After that, step by step appears to configure the IPv6 communication with dynamic routing via CISCO RIPng protocol.

LISTA DE ILUSTRAÇÕES

Índice de ilustrações

SUMÁRIO

1. INTRODUÇÃO

Neste capítulo serão tratados os elementos introdutórios relacionados ao estudo e implementação de endereçamento Ipv6, Escopo da pesquisa, Problemas e premissas, objetivo geral, objetivos específicos, Justificativa, Metodologia de pesquisa, Embasamento teórico e a estrutura do trabalho.

1.1 TEMA

Desde o final de 2011 não há mais nenhum bloco de Ipv4 em estoque na entidade internacional responsável pela distribuição de Ipv4 IANA *(Internet Assigned Numbers Authority),* essa distribuição afeta hierarquivamente até o usuário final e será explicado no capítulo 2 dessa monografia. Desde então a preocupação e os projetos para implementação do Ipv4 tem se intensificado. Entretanto, por motivos que serão apontados no capítulo 1.3 dessa monografia, muitas empresas tem adiado o uso do Ipv6. A partir dessa pesquisa, bem como de pesquisas em fóruns sobre o tema, é possíivel identificar que as alternativas para dar sobrevida ao Ipv4 podem atrapalhar a velocidade de comunicação na internet. E que ainda é necessário difundir o conhecimento a respeito do Ipv6 em todos os níveis hirárquicos da rede mundial, desde o usuário residencial, grandes provedores, grandes instituições, etc.

1.2 ESCOPO DA PESQUISA

Esta monografia compreende o levantamento teórico básico para conhecimento do tema, motivos que levaram ao atraso na implementação do Ipv6 e a atividade prática para configuração do Ipv6 em uma rede LAN emulada.

1.3 PROBLEMAS E PREMISSAS

O Ipv6 já possui compatibilidade com quase a totalidade dos S.O.s (Sistemas Operacionais). No entanto, para alguns hardwares é necessário efetuar atualizações de

firmware ou até mesmo a troca e muitas vezes há um receio por parte do usuário em alterar um dispositivo que está funcionando, principalmente quando se trata de segurança e custos.

Para difundir a utilização do Ipv6 é necessário incentivo do Governo Federal, Grandes Provedores de Internet (ISPs) e de grandes empresas provedoras de conteúdo, como Google, Facebook, etc.

Tendo isso, é necessário compartilhar o conhecimento sobre o Protocolo através de trabalhos, artigos, tutoriais etc.

1.4 OBJETIVO

1.4.2 Objetivo Geral

Disseminar e incentivar o uso do Ipv6, através de um passo à passo para configuração do protocolo em hosts e roteadores bem como a configuração do roteamento dinâmico com o protocolo RIPng.

1.4.3 Objetivos Específicos

- Estudar o funcionamento básico do protocolo Ipv6;
- Implementar em uma topologia em pleno funcionamento com o Ipv4 o protocolo Ipv6;
- Testar a comunicação com ambos os protocolos.

1.5 JUSTIFICATIVA

Neste capítulo é apresentado a justificativa e a importância para o estudo e implantação do Ipv6.

1.5.1 Crescimento Da Rede Mundial De Computadores

A RFC 791 definia em 1981 a ideia básica do endereçamento IP, com os seus 32 bits, podemos dizer que em teoria existem 2^{32} possibilidades de e dereços Ipv4, iniciando em 0.0.0.0 e terminando em 255.255.255.255. No entanto, boa parte desses Ips não são endereçaveis na internet. Algumas faixas de Ips são rezervadas, conforme mostrado na Ilustração 2.

O gráfico 1 demonstra que até o inícios dos anos 2000 os usuários de internet, no Brasil, estavam concentrados em duas classes da população (A e B). Nos anos seguintes houve um crescimento exponencial com o surgimento das redes sociais, mas somente a partir de 2007 é que a CLASSE C passou a participar em peso da rede mundial de computadores.

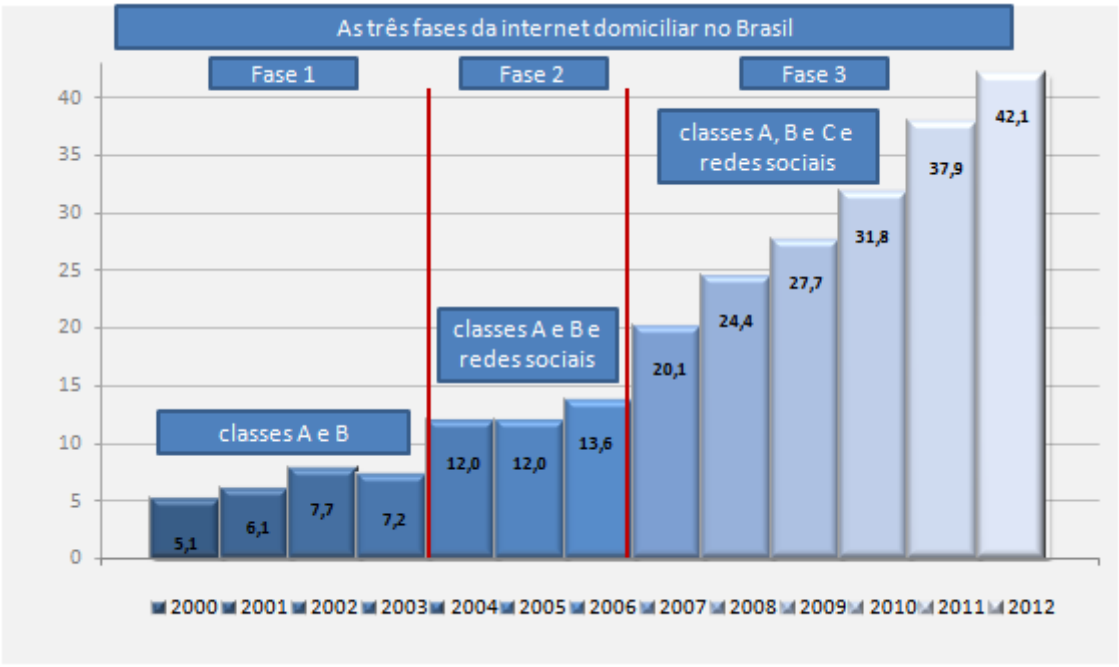

Gráfico 1: Gráfico das três fases de utilização da internet no Brasil - Fonte: IBOPE 2012

1.5.2 Redes Convergentes e Internet de Todas as Coisas

O analista José Calanz do IBOPE (Responsável pela pesquisa do gráfico 1) acredita que estamos entrando em uma quarta fase da utilização da internet com a utilização de equipamentos móveis, como tablets e celulares. Mas assim como a Ericsson, quando inventou o primeiro Telefone Móvel em 1956 (Utilizado em carros) não imaginava a utilização de aparelhos de telefonia móvel para comunicação via textos, imagens e vídeos, não podemos imaginar todas as aplicações possíveis a serem desenvolvidas na internet.

Ilustração 1: Ericsson MTA 1956 - Considerado o primeiro telefone móvel - Fonte: Erocsson

Diariamente surgem novas implementações e soluções para o dia-a-dia. Já estamos ambientados aos serviços convergentes, como serviços de Internet, Telefone e Televisão em um único meio físico. Implementações tecnológicas, como geladeiras inteligentes com o controle de estoque por exemplo, são projetos que visam um conforto, comodidade e uma melhor qualidade de vida. Entretanto, cada aplicação dessas necessita de comunicação com a rede mundial, para isso é necessário um endereço IP.

1.5.3 Escassez de endereços IPv4

O IP foi descrito pela RFC 791 no início dos anos 80 e dava um total , em teoria, de mais de 4 bilhões de endereços. Inicialmente não era imaginado a utilização comercial do mesmo nos níveis de hoje. Os endereços foram divididos em 3 classes de endereçamento (A,B e C), além do rápido crescimento, essa divisão dos endereços colaboraram muito para escasses dos endereços. Segundo o IPV6.BR os endereços de classe A davam poucas redes (128) com muitos endereços de HOST (15 milhões) para cada uma das redes de classe A, para os endereços de Classe B eram 16 mil redes com 65 mil endereços cada uma e a classe C possuia 2 milhõess de redes com 256 endereços cada uma. Caso um administrador de rede necessitasse de uma rede com 500 hosts, necessitaria usar uma

classe B e desperdissaria 15.500 endereços. Segue abaixo a representação das 3 classes principais e as duas classes de endereços reservados.

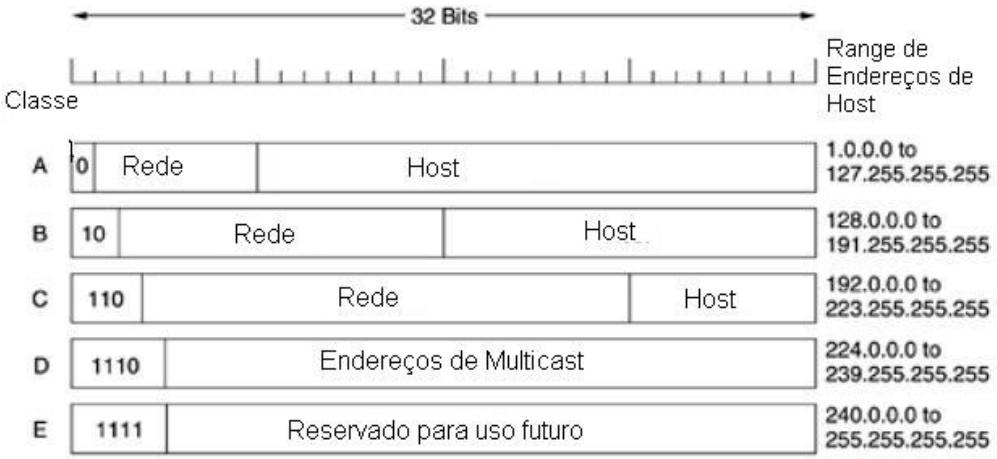

Ilustração 2: CLASSES DE IP – Fonte: Livro Rede de Computadores, Andrew S. Tanenbaum, pg. 337

No entanto, além das três classes de endereçamento, há mais duas classes (D e E) para uso de Multicast e Experimental.

Algumas empresas, à essa época, receberam blocos de classe A de ip, o que dispõe mais de 16 milhões de endereços IP.

Esse mal dimensionamento da utilização levou à necessidade de criar soluções paliativas para manter a utilização da versão 4 do IP.

Com a abertura da comercialização da internet, no início dos anos 90 identificou-se a necessidade de melhorar o dimensionamento de IP's. No caso da classe A, haviam poucas redes mas com muitos endereços de hosts sobrando. Um desperdício de Ips, sendo que na classe C, há várias redes com poucos hosts. Em 1991 foi criado pela IETF (Internet Engineering Task Force) um grupo de trabalho com a missão de melhorar o endereçamento e o problema com o aumento das tabelas de roteamento (deviddo a rápida expansão da internet), esse grupo era o ROAD(ROating and Addressing). Os resultados foram a

elaboração das técnicas de CDIR (Classless Inter-domain Routing), DHCP (Dynamic Host Configuration Protocol) e NAT (Network Address Translation), sendo respectivamente suas funções dimensionar melhor o endereçamento (host x rede), alocar dinamicamente um ip a cada host em uma determinada rede e diminuir o esgotamento de IP através do compartilhamento de IP público com vários hosts em uma rede interna. Esse último dificulta a comunicação fim a fim pois não há como fazer uma comunicação ponto a ponto de um host com IP público diretamente à um host com IP privado.

Abaixo segue a imagem que ilustra a diminuição do consumo de Ips com a implementação do Nat e o CDIR.

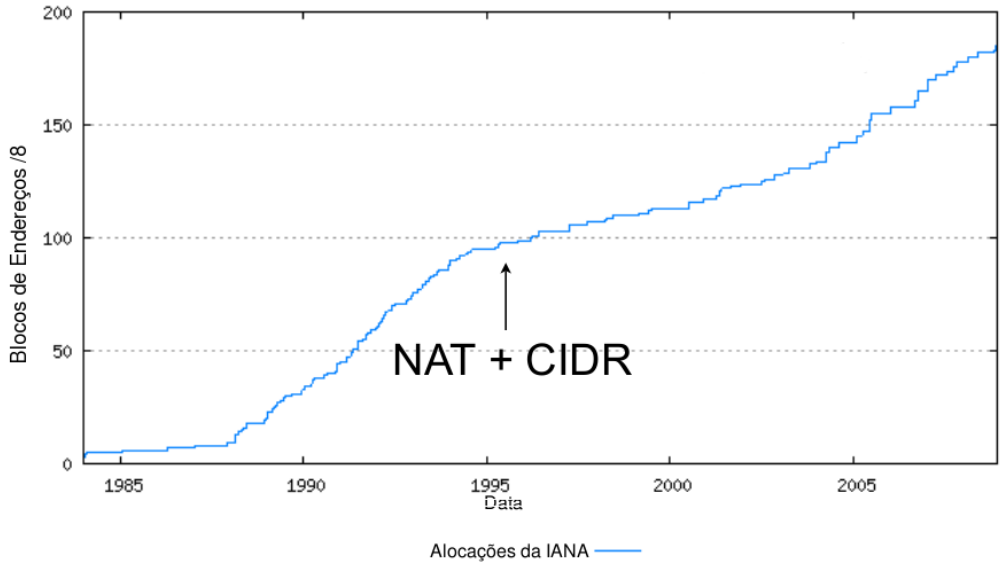

Gráfico 2: Gráfico de alocações de endereços Ipv4. Fonte IPV6.BR

Essas medidas foram efetivas no propósito de dar sobrevida à quantidade de Ips disponíveis mas a rede continuava crescendo.

1.5.4 Cenário Atual

Os diversos recursos, que aumentaram a sobrevida do IPV4, acabam por atrapalhar, algumas vezes, a comunicação ponto a ponto, velocidade de comunicação, latência, etc. De encontro à isso vem a necessidade de cada vez mais a crescente busca por alta velocidade e qualidade de conexão. É necessário que a implementação do IPv6 se dê o quanto antes para atender à essas demandas bem como possibilitar ainda mais o crescimento da rede mundial.
Ao mesmo tempo em que há necessidade de migração para o IPV6, vemos uma resistência a essa implantação, tanto por parte do usuário como por parte dos provedores de serviços na internet. O documento do Plano de Disseminação do IPV6 do Governo Federal relata em sua introdução que mesmo o protocolo IPV6 garantindo uma enorme quantidade de endereços, maior segurança e um maior desempenho mas que por outro lado, em muitos casos, é necessário custos com capacitação e com atuallizações de software e hardware. Na maior parte, para o usuário final, a escassez do Ipv4 está fora de sua realidade e a migração para o Ipv6 desnecessária.

Essa realidade está mudando. Alguns provedores estão implementando uma nova técnica, conhecida como CGNAT, atribuindo faixas de portas lógicas â vários usuários. Usuários que necessitam do recurso de Port Forwarding (Redirecionamento de portas) como DMZ, Firewalls, etc, não são compatíveis com essa solução. Outros serviços que são incompatíveis, são os que necessitam de conexão ponto à ponto, como cameras IP.

Uma empresa provedora de internet do Paraná, está fornecendo o serviço aos seus usuários o IPV6 e Ipv4 com CGNAT através de um recurso conhecido como pilha dupla, uma técnica para fornecer ao usuário a possibilidade de acessar recursos disponíveis na WEB independente da versão do Protocolo.

Este ainda não é o cenário ideal. Pois o cliente que necessita acessar a um serviço com Ipv4, essa conexão será limitada à um número de portas disponíveis a esse usuário. Se o servidor necessita de redirecionamento de portas ou de uma conexão ponto à ponto via IPV4, a conexão não ocorrerá.

1.5.5 Cenário Futuro

Com o IPv6 em pleno funcionamento, haverá recursos de sobra para novas implementações e soluções. Como a Internet de todas as coisas como controle de ambientes residenciais à distância. Será possível o desenvolvimento de novos recursos e facilidades para o dia-a-dia.

1.6 METODOLOGIA DE PESQUISA

Para o estudo do tema, será utilizado a pesquisa bibliográfica em artigos científicos, publicações oficiais de projeto de implantação do Ipv6 no Governo Federal, Request For Comments – Requisições Para Comentários (RFC), documentos técnicos de implantação e configuração de endereçamento e roteamento Ipv6. A partir disso é possível iniciar o teste prático, para o qual será utilizado um programa de emulação com roteadores CISCO e algumas máquinas virtuais com pleno funcionamento da comunicação entre duas redes distintas pelo protocolo de versão 4. Após os testes de comunicação via IPV4, será configurado o endereçamento IPV6, habilitado o RIPng para roteamento dinâmico e finalizado com testes de comunicação.

1.7 Embasamento Teórico

Para descrever sobre o conhecimento sobre internet e seu histórico destacam-se as obras Redes de Computadores de Andrew S. Tanenbaum, Guia do TCP/IP – Entendendo o IPV4 e IPV6 de Daniel Donda, Registro.BR e a Revista Pesquisa da FAPESP. Sobre os conceitos de Ipv6, destaca-se o material produzido pela IETF com as RFCs bem como pela NIC.BR.

2. REFERENCIAL TEÓRICO

Este capítulo apresenta o conteúdo que visa dar base para que o leitor possa se interar sobre um tema de característica técnica.

2.1 Encapsulamento

Em redes de computadores a comunicação entre dois hosts distintos ocorre através do encapsulamento dos dados a serem enviados em pilhas de protocolos. Essa pilha de protocolos vai desde o bit trafegando através de um pulso elétrico em um cabo de rede até a aplicação que usuário roda em um computador. Atualmente há dois modelos de Pilhas de Protocolos que são utilizados para estudo desse conceito, são eles os Modelos TCP/IP (Transfer Control ProtocoL / Internet Protocol) e o modelo OSI (Open Systems Interconnection).

A imagem abaixo dá um exêmplo básico dos protocolos em cada camada, dando a idéia de pilha no modelo de referência TCP/IP.

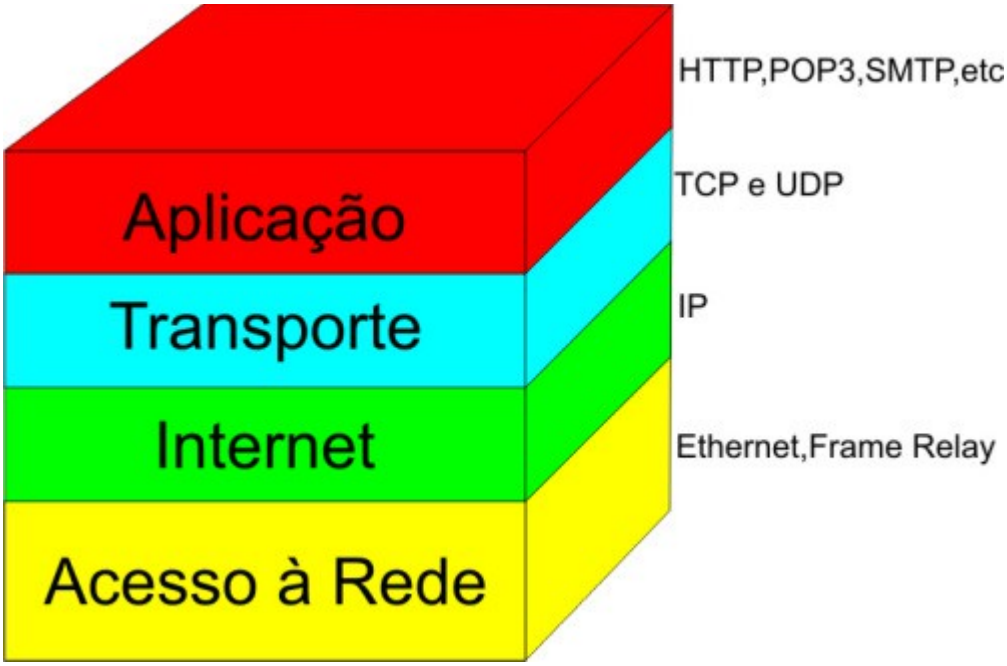

Ilustração 3: Pilha TCP/IP e seus protocolos - Fonte Andrew S. Tanenbaum (2010) adapatado.

2.1.1 Modelo de Referencial OSI

Em meados de 1980 a ISO (International Standard Organization) publicou a proposta desenvolvida na década anterior para padronizar os diversos protocolos usados nas diversas camadas das redes de computadores. Andrew S. Tanenbaum publicou em seu livro Redes de Computadres demonstre como é o modelo OSI e que possui sete camadas conforme a imagem abaixo.

- Camada física – É a primeira camada do modelo OSI e trata os padrões fisicos de quantos pinos possui um conector ethernet e a função de cada um, qual o tipo de interface mecânica, elétricos, padrões de transmissão pelo meio físico para que um bit “1” chegue ao destino sem interferências como o mesmo bit “1” e não “0”, se esse meio físico comporta uma transmissão em dois sentidos ao mesmo tempo (Full e half duplex);

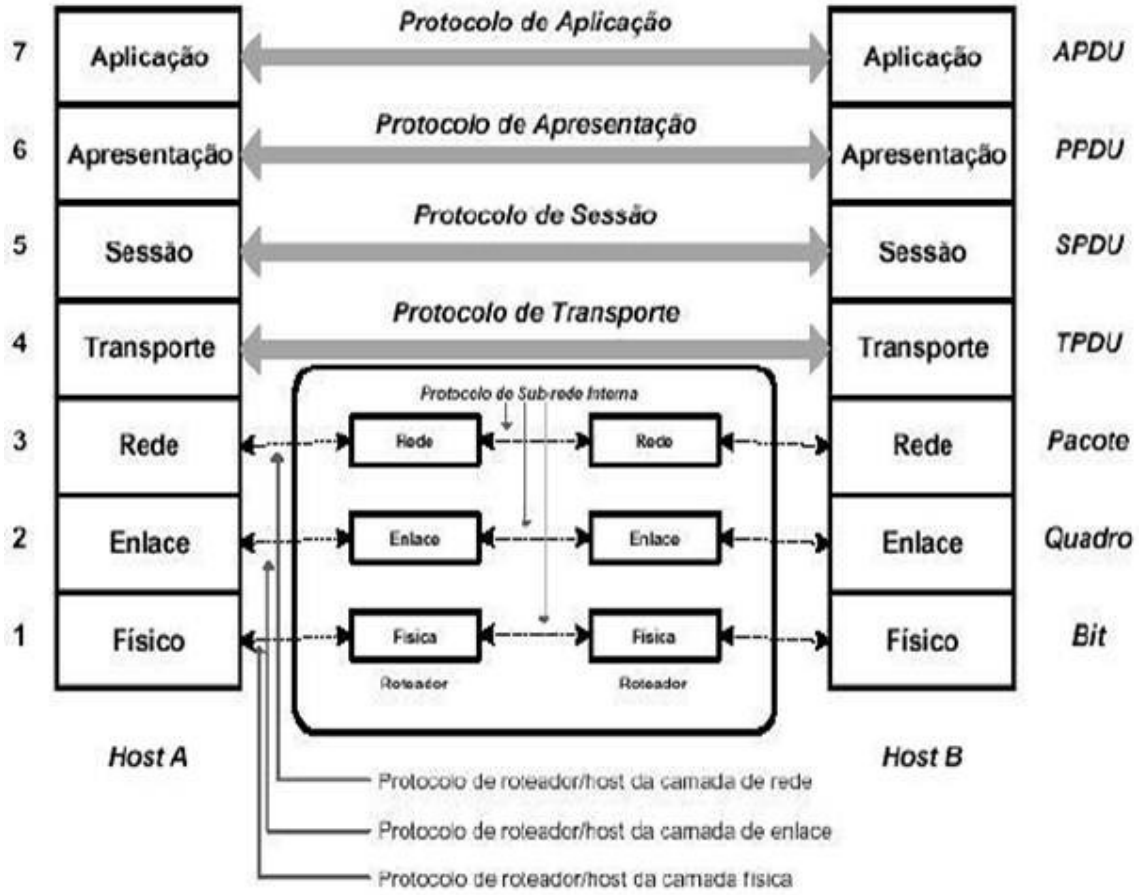

Ilustração 4: Pilha modelo OSI - Fonte Andrew S Tanenbaum (2010) adaptado.

- Camada de Enlace – A principal função da camada de enlace é fazer com que os bits brutos da camada anterior sejam transmitidos para a próxima camada, sem erros em formato de quadros, enviando ao remetente uma confirmação para cada quadro recebido. Ela também é responsável por fazer com que emissor e receptor se comuniquem à mesma velocidade, ou seja, se em uma rede wireless, por exêmplo, existe um notebook com placa wireless com padrão IEE 802.11n comunicando com um roteador IEEE 802.11 ebgn e ao mesmo tempo na rede existe um equipamento com configurações inferiores no padrão 802.11g, toda a rede terá de coomunicar no padrão inferior. É onde atua o endereçamento físico (MAC Address);

- Camada de rede – É onde atua o protocolo IP, controla a operação das sub-redes, endereçamento lógico (endereço IP), e por meio desse trata do roteamento, que por sua vez ajuda no controle congestionamento (gargalo) em algumas , definindo rotas melhores através de roteamento dinâmico;
- Camada de transporte – Tem como principal função receber os dados da camada superior (sessão) e dividí-los em pacotes menores, se necessário, e repassá-los às camadas inferiores, assegurando-se que todos os pacotes cheguem ao destino correto na ordem correta. É a camada onde atua o protocolo TCP (Transmission Control Protocol – Protocolo de Controle de Transmissão). É a camada onde inicia a conexão fim a fim, ou seja, o host de origem conversa com o host final. Nas camadas inferiores a comunicação é feita entre os vizinhos (próximo salto);
- Camada de sessão – Uma de suas fufnções é fazer com que os diversos serviços rodando em um host não sejam misturados. Por exêmplo, um bit de uma página web rodando em um browser não se misture com um bit de uma conexão Telnet que estejam ocorrendo simultaneamente;
- Camada de apresentação – Ao contrário das primeiras camadas que focam na transmissão de bits, a camada 6 é responsável pela sintaxe e semântica das informações transmitidas. Também é responsável pela compressão de dados e pela criptografia;
- Camada de aplicação – É a camada de interação com o usuário, como os protocolos HTTP (HyperText Transfer Protocol).

2.1.2 Modelo de Referência TCP/IP

Assim como o modelo OSI o modelo TCP/IP também foi desenvolvido para padronização da comunicação nas redes. Seus primórdios iniciaram ainda na ARPANET nos anos 70, mas definida nos anos 80. A principal diferença entre ambos os modelos é que

o segundo possui apenas 4 camadas, sendo que as camadas Sessão e Apresentação foram englobadas pela camada aplicação e as camadas física e delace foram compactadas em uma nova camada “acesso à rede”.

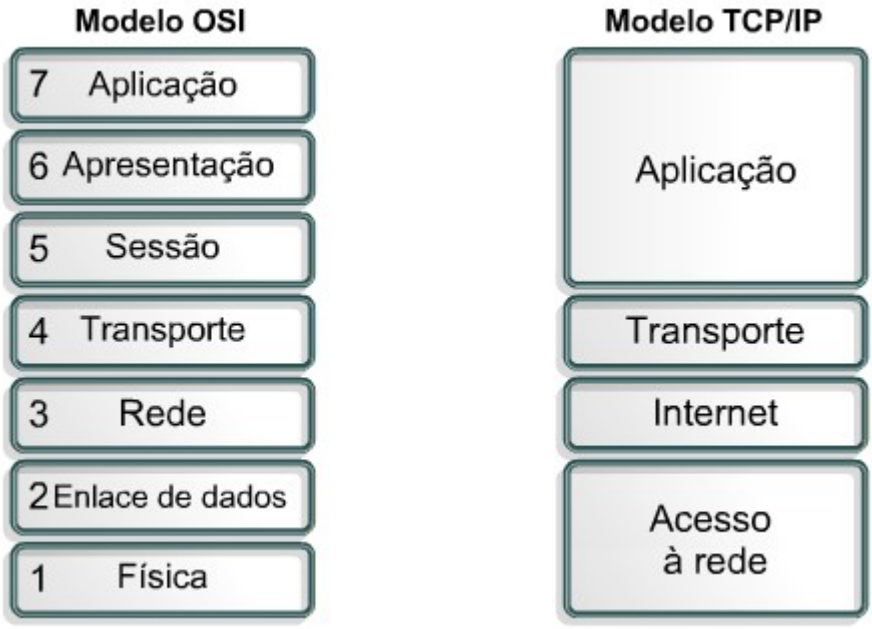

Ilustração 5: Comparativo OSI x TCP/IP - Fonte - CISCO CCNA5.0

- Camada de Aplicação – É a camada de nível mais alto, que está mais próxima do nível de usuário. Ao contrário do que se pensa, essa camada não comporta as aplicações (S.O, Web Browser, etc), mas os protocolos que auxiliam a utilziação do mesmo, como no caso do HTTP para o Browser;
- Camada de transporte – Correlata à camada 4 do modelo de referência OSI. Tem a responsabilidade escolher a forma de controle de fluxo (UDP ou TCP);
- Camdaa de Internet – É equivale à camada 3 do modelo OSI, essa camada comporta o protocolo da Internet (IP), com responsabilidade de interconexão, roteamento etc;

- Camada de acesso a rede – É a camada maixa baixa do modelo TCP/IP e faz o controle de acesso ao meio físico, tipo de protocolo, etc.

2.1.3 A pilha de protocolos e a atividade prática

Para a atividade proposta nesta monografia, a análise da pilha de protocolos será concentrada até a camada 3 do modelo OSI/ISO, na qual será implementado o Ipv6, com roteamento dinâmico, onde o primeiro host irá encapsular o endereço de origem e destino IP, para encaminhar esse pacote para a camada 2 (Enlace), onde será anexado o endereço físico (MAC ADDRESS), o qual o protocolo de enlace irá encaminhar para a camada abaixo (FÍSICA), transformando todo o dado em bits até chegar ou host destino que efetuará o caminho inverso.

2.2 O QUE É O IP

Como na sociedade, na comunicação digital, para que haja comunicação é necessário ter um padrão para que ambos os lados (emissor e receptor) utilizem a mesma linguagem, os mesmos códigos e as mesmas regras de comunicação. No início da internet, como conta o coordenador da Ansp (Academic Network São Paulo), Luiz Fernandez Lopez, em entrevista à revista Pesquisa da FAPESP, haviam diversas redes proprietárias, diversos fabricantes de equipamentos cada um com seu padrão e diversos protocolos de endereçamento e encapsulamento de dados. Certamente o que faltava para o crescimento da Internet era a padronização, sem interesses particulares, com um protocolo aberto.

O IP como conhecemos hoje é o responsável pelo endereçamento (origem e destino) e, em conjunto com o TCP (Transfer Control Protocol), pela fragmentação de um dado maior em pacotes menores (comutação de pacotes), correção de erros (solicitação de envio do pacote em caso de perda), possibilitando a utilização do meio físico de acordo com sua capacidade (largura de banda), escolhendo se for o caso caminhos alternativos para cada pacote, conforme descrito no IPV6.BR.

Segundo TANENBAUM, Andrew S. 2010, a internet é formada por um conjunto de sub-redes ou sistemas autônomos conectados entre si. Onde não existe uma interligação única, mas vários conjuntos de backbones e roteadores interconectados. O IP pode ser entendido como o agente responsável por interligar todas as redes no mundo fornecendo a melhor forma possível (não garantido) de transportar os dados ao destino, independente de os hosts estarem na mesma rede ou de haver outras redes entre eles.

Para que cada computador possa acessar à internet é necessário ter um endereço. Esse endereço deve ser único (não repetido). Para que cada computador no mundo tenha um endereço não repetido é necessário que essa distribuição seja controlada de forma estruturada e hierárquica. A IANA (Internet Assigned Numbers Authority) é a entidade que detem os endereços IP'S a nível mundial. Ela repassa blocos de Ips aos registros regionais da Internet como a LACNIC (Registro Regional para a América Latina e Caribe), que por sua vez são responsáveis pela distribuição de seus endereços aos Registros Nacionais de Internet, como no Brasil a NIC.br (Núcleo de Informação e Cordenação do Ponto BR). Por fim há ainda os Registros locais de Internet (LIRs – Local Internet Registries) que podem ser os Provedores.

Ilustração 6: Mapa internnacional da IANA - Fonte LACNIC

Com a expansão da utilização do endereçamento Ipv4, hierarquicamente, foram acabando os endereços disponíveis. Em 03 de Fevereiro de 2011 foram alocados os últimos blocos de Ipv4 /8 da IANA para a os cinco Registros Regionais. Atualmente a LACNIC possui uma quantidade de Ips com uma política de esgotamento, a qual foi dividida em três fases (conforme disponível em sua página web:

- Quando for atingido o equivalente ao último bloco /9, incluindo os dois /11 reservados para o esgotamento gradativo do IPv4 e para novos entrantes;

– Quando for atingido o último bloco /10 (Fase atual);

– Quando se esgotar o bloco /11 de terminação gradativa.

Conforme demonstrado no gráfico de disponibilidade de Ips disponibilizado pelo LACNIC, em 10 de Junho de 2014, foi atingido o número de Ips no LACNIC considerado o limite nessa entidade e no Brasil, por meio do Núcleo de Informação e Comunicação do Ponto BR (NIC.br).

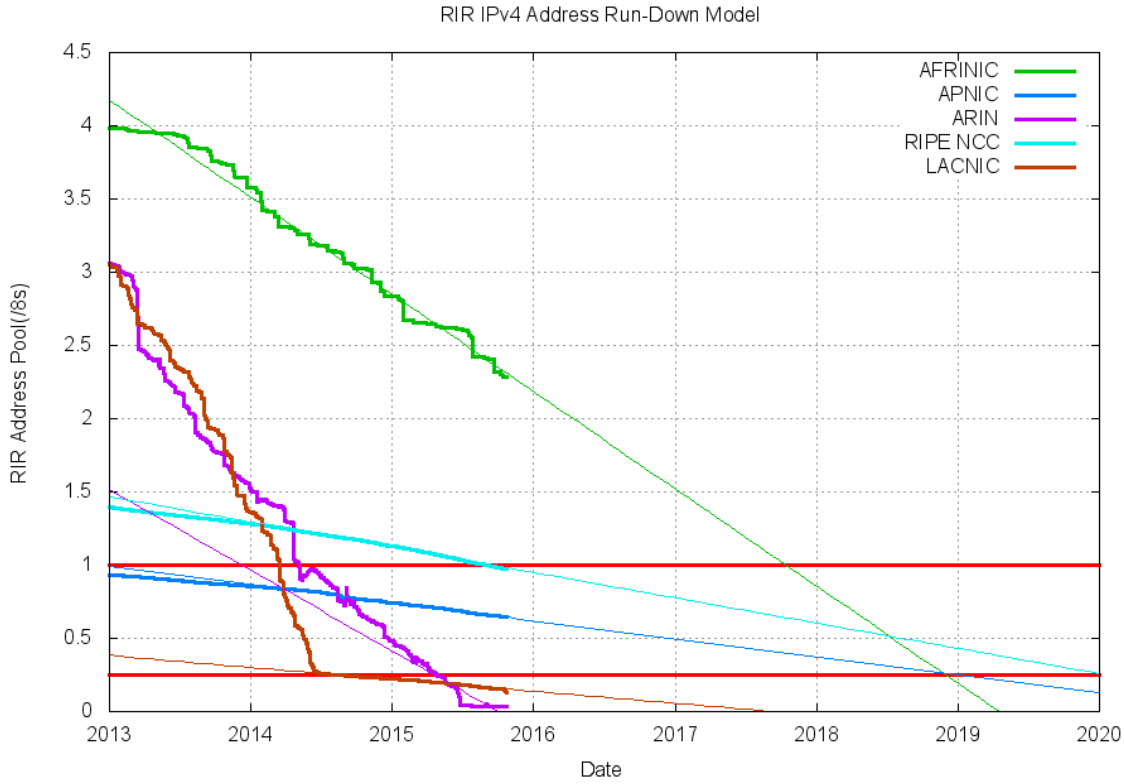

Gráfico 3: Gráfico de queda de disponibilidade de /8 - Fonte NIC.br

2.2.1 O IPv4

O IPv4 é um endereço binário, formado por quatro octetos (Conjunto de oito bits), cada casa pode ser 0 ou 1(para linguagem das máquinas) de tamanho fixo em 32 bits (32 zeros ou uns), mas para adequar a representação desses endereços usamos a notação decimal (0,1,2....9) formados por quatro conjuntos, representando os quatro octetos. Esses conjuntos na notação binária compoem 8 bits, dando o nome de octeto. Ou seja, na linguagem binária, um endereço Ipv4 possui 4 octetos de 8 bits, somando no total 32 bits.

Exemplo de Ipv4 representação decimal: 192.168.0.1

A representação decimal acima, demonstra que há quatro grupos de números separados por pontos, cada um desses conjuntos possui 8 bits. O primeiro octeto “192” é formado pelos bits “1100000000”. Essa sequência de dois números 1 seguida por uma sequência de 6 zeros é a representação binária do primeiro octeto “192”. Cada um dos

octetos é formado por oito bits e cada bit é uma unidade binária (0 ou 1). Cada uma das quatro seções pode compor um número de 0 à 255. Isso resulta um número total de 4.294.967.296 (2^{32}) de endereços Ipv4.

2.2.1.1 Cáculo para transformar um endereço binário em decimal

Asseguir a tranformação do exêmplo acima (192.168.0.1), transformando um número decimal em binário:

potência	7	6	5	4	3	2	1	0
base	2	2	2	2	2	2	2	2
Resultado	128	64	32	16	8	4	2	1

Essa é a formula padrão para descobrir um número binário. Queremos descobrir a representação do número decimal “192”. Para isso, basta somarmos (da esquerda para a direita) todos os números necessários da linha resultado, até alcançarmos o número desejado. Nesse caso, deve-se somar apenas os dois primeiros (128+64). Para cada número da linha resultado usado na soma, representamos a utilização desse bit ou em outras palavras, ligamos esse bit na linha binária:

potência	7	6	5	4	3	2	1	0
base	2	2	2	2	2	2	2	2
Resultado	128	64	32	16	8	4	2	1
Binário	1	1	0	0	0	0	0	0

O mesmo processo deve ser executado para os outros três octetos.

Ao final teremos o resultado:

11000000.10101000.00000000.00000001

2.2.1 Cabeçalho IPv4

Como já citado, e como descrito por Andrew S. Tanenbaum (2010), a comunicação na internet ocorre através de encapsulamento de dados em pacotes. No caso de um pacote IP ou Datagrama é composto por uma parte de seu cabeçalho e a outra parte de texto (dados a serem enviadospropriamente dito). Conforme IPV6.BR, o cabeçalho é divido em 12 campos, conforme a imagem abaixo:

<table>
<tr><td>Versão
(Version)</td><td>Tamanho do Cabeçalho
(IHL)</td><td>Tipo de Serviço
(ToS)</td><td colspan="2">Tamanho Total
(Total Length)</td></tr>
<tr><td colspan="3">Identificação
(Identification)</td><td>Flags</td><td>Deslocamento do Fragmento
(Fragment Offset)</td></tr>
<tr><td colspan="2">Tempo de Vida
(TTL)</td><td>Protocolo
(Protocol)</td><td colspan="2">Soma de verificação do Cabeçalho
(Checksum)</td></tr>
<tr><td colspan="5">Endereço de Origem (Source Address)</td></tr>
<tr><td colspan="5">Endereço de Destino (Destination Address)</td></tr>
<tr><td colspan="5">Opções + Complemento
(Options + Padding)</td></tr>
</table>

Ilustração 7: Cabeçalho IPV4 - Fonte Andrew S. Tanenbaum (2010) adaptado

A função desses campos é, conforme a sequência da imagem acima, transmitir a versão do protocolo, o tamanho do datagrama (cabeçalho + dados), a fragmentação dos pacotes, o tipo dos dados enviados, o tempo de vida do pacote, o protocolo da próxima camada, a soma do cabeçalho como forma de garantir a integridade dos dados e por fim a origem e destino do pacote.

2.3 IPv6

O IPv6 foi idealizado para atender as necessidades de escalabilidade,e permitir a comunicação ponto a ponto que o endereçamento IPv4 começava a ter problemas na década de 1990 e garantir a continuidade de novas implementações.

2.3.1 O endereço IPv6

É um endereço hexadecimal (0,1...9, A, B, C, D, E, F), separados por **dois** pontos (:) em oito grupos de 16 bits, totalizando um total de 128 bits, possibilitando um total de 2^128 = 340,282,366,920,938,463,463,374,607,431,768,211,456 endereços. Segue abaixo a representação Exadecimal do ipv6.

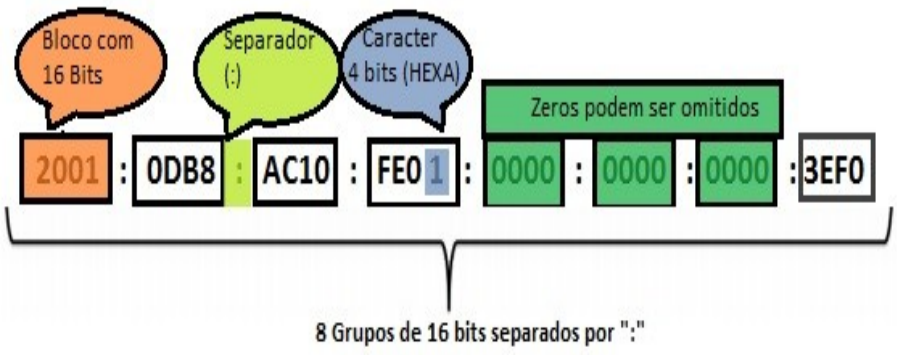

Ilustração 8: Fonte: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/3591/1/CT_GESER_V_2014_4.pdf - Adaptado

Por se tratar de uma representação extença, criou-se algumas regras de abreviação. Assim como na matemática, o zero (0) a esquerda pode ser omitido. Uma sequência de 4 zeros pode substituida pela representação de apenas um zero apenas ou ainda duas sequências de 4 zeros podem ser omitidas conforme imagem abaixo.

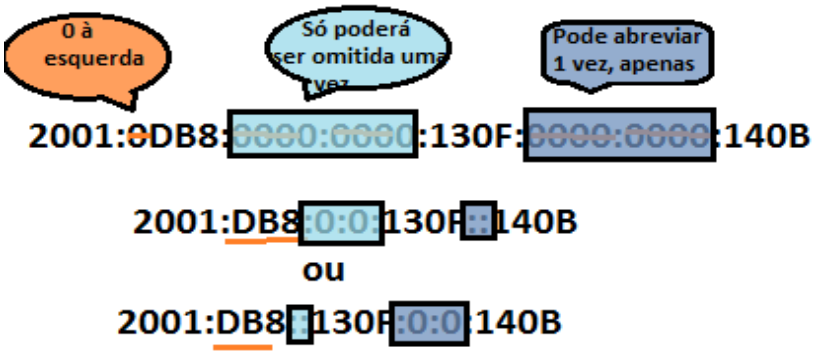

Ilustração 9: Fonte: https://reaipv6.wordpress.com/abreviacao/ - Adaptado

Assim como o IPV4, o ipv6 também possui Classless Inter Domain Routing (CIDR), o que define o endereçamento atribuido como host ou rede. Ele é representado pela forma "IPV6/tamanho do prefixo", sendo que o prefixo é a quantidade de bits (à esquerda do endereço) utilizados para identificar a sub-rede. Segue abaixo o exemplo da Ilustração 5:

- Prefixo 2001:DB8::130F:0:0/64;
- Prefixo global 2001:0DB8::/32;
- Id da sub-rede 0:0:130F.

2.3.1.1 Tipos de endereços IPv6

O NIC.br efetua alguns encontros para difundir o conhecimento do novo protocolo, um desses encontros é chamado de "Ipv6 no Café da Manhã", e estão disponíveis na página do Ipv6.br. No segundo encontro, é apresentado que Também como o Ipv4, o Ipv6 possui alguns tipos de endereços, sendo os relacionados abaixo:

- Unicast – São os endereços que representam um único host ou interface. Os endereços unicast podem ser de três categorias:
  - ➔ Global Unicast – São os endereços globalmente roteáveis e podem ser comparado aos endereços válidos do IPV4. A IANA, reservou a faixa 2000::/3 para endereçamento global. Isso representa aproximadamente 13% de todos os

endereços IPV6 possíveis (340 undecilhões), o prefixo “/3” significa que os três primeiros BITS do endereço número 2 (0010 em binário) serão fixos, ou representam o endereço de sub rede. Com isso o range de IPV6 varia de 2000:0000:0000:0000:0000:0000:0000:0000 até 3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

- ➔ Link-Local – É o endereço Unicast atribuido automaticamente pelo sistema operacional, quando em uma rede local, o host não conseguiu receber um endereço IP. Pode ser comparado ao APIPA, recurso utilizado pelo Windows para alocar um Ipv4, quando a máquina não recebe um IP via DHCP ou manualmente. É importante ressaltar que esse é um endereço não roteável, ou seja, não sairá pela interface WAN do roteador para outras redes. Para que não haja problemas de alguém tentar configurar um endereço de link-local como como endereço de roteador, foi reservado o range FE80::/10 (rfc4291).
- ➔ Unique-Local – Também conhecidos como ULA (Unique local) e pode ser comparado ao endereço privado o Ipv4. Os endereços ULA tem o prefixo FC00::/7, o que resulta em um range de FC00:0000:0000:0000:0000:0000:0000:0000 até FDFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

- Multicast – No ipv4, o que mais se aproxima desse tipo de endereço é o Broadcast. No entanto, no IPV6 ele é segregado por subrede através do prefixo FF00::/8, com isso todos os hosts de uma subrede irão receber a mensagem.
- Localhost – É equivalente ao 12.0.0.1 do IPV4 e é apresentado pelo seguinte endereço “::1”.

- Não especificado – é utilizado, por exemplo, em regras de firewall para dizer que qualquer endereço com qualquer prefixo deve seguir essa regra. É equivalente ao “0/0” do ipv4 e representado no IPV6 pelo endereço ::0.

2.3.3 O cabeçalho IPv6

Como um dos objetivos do projeto inicial do IPNg era diminuir o tamanho dos pacotes sendo roteados na rede, o cabeçalho do Ipv6 tornou-se mais simples que a versão anterior. O cabeçalho passou a ter oito campos (diferente do IPV4 que possui 12) e um tamanho fixo de 40 Bytes.

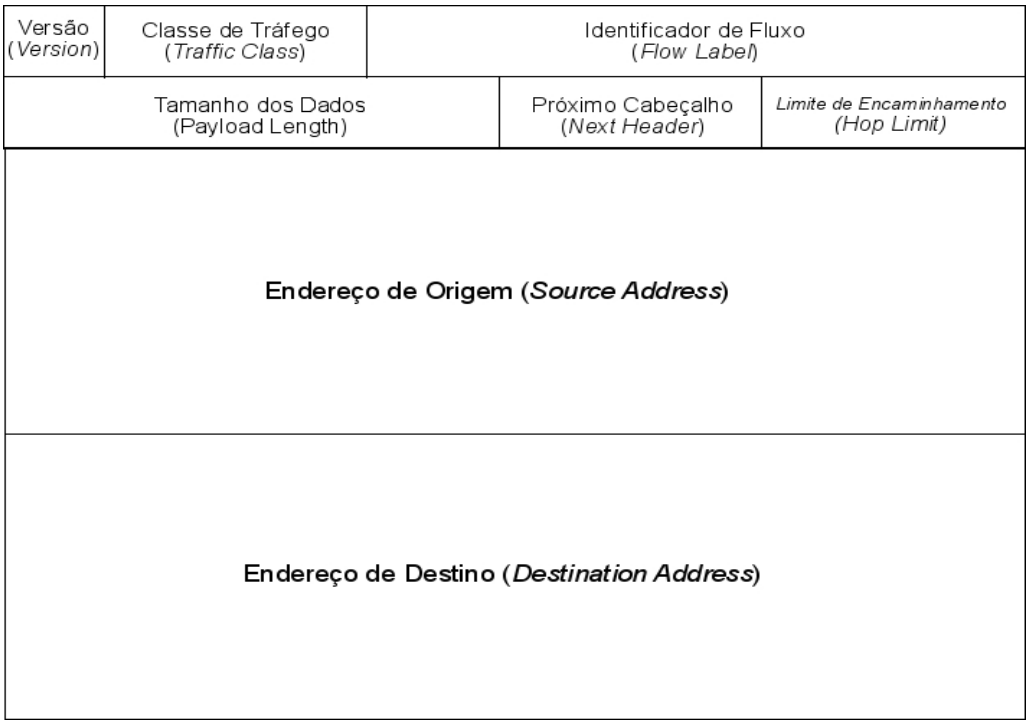

Ilustração 10: Cabeçalho IPV6 - Fonte Andrew S. Tanenbaum 2010 - Adaptado

De acordo com o IPV6.BR, as mudanças no cabeçalho do protocolo IP além de torná-lo mais simples e de tamanho inferior ao IPV4(de 20 à 60 bytes) mesmo com um endereço quatro vezes maior.

A imagem abaixo destaca os campos que não foram incluídos na versão 6.

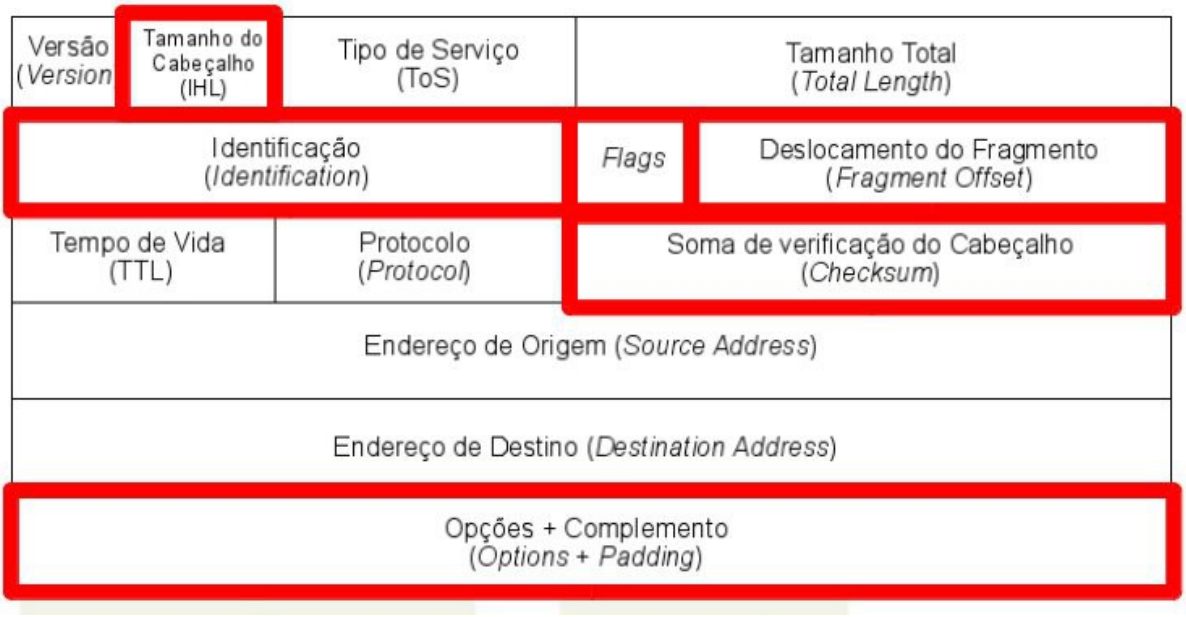

Ilustração 11: Campos não incluídos no ipv6 - Fonte CCNA 5.0

Esses campos foram retirados pois o tamanho do cabeçalho agora é fixo em 40 bytes, e a soma de verificação foi retirada visto que outros controles são feitos pelas camadas superiores, com isso há um ganho no processamento dos pacotes. Os demais campos não incluídos na versão seis possuem cabeçalhos de extensão próprios. Outra alteraçao que beneficiou o processamento é a renomeação e o reposicionamento dos campos, conforme tabela abaixo:

IPV4	IPV6
Tipo de Serviço	Classe de Serviço
Tamanho Total	Tamanho de Dados
Tempo de Vida (TTL)	Limite de Encaminhamento
Protocolo	Próximo Cabeçalho

Ilustração 12: Quadro comparativo entre IPV6 e IPV4 - Fonte: autoria própria

Os campos versão, Endereço de Origem e Endereço de Destino foram mantidos, porem com o tamanho alterados. Segue abaixo a descrição e o tamanho dos campos do cabeçalho IPV6:

- Versão (4bits): Tanto na versão quatro quanto na versão seis, esse campo tem a mesma função. Identifica a versão do protocolo. No caso do Ipv6 esse campo traz o número “6”;
- Classe de tráfego (8bits): Identifica a classe de serviço e a prioridade;
- Identificador de fluxo (20 bits): Segundo Andrew S. Tanenbaum (2010) os fluxos são uma tentativa de se ter a flexibilidade de uma sub-rede de datagramas juntamente com as garantias de uma subrede de circuitos virtuais;
- Tamanho do Dados (16bits): Mostra em Bytes o tamanho dos dados enviados no datagrama, excetuando-se o tamanho do cabeçalho (40bytes);
- Próximo cabeçalho (8 bits): Indica qual o próximo cabeçalho (cabeçalho de extensão do ipv6);
- Limite de encaminhamento (8bits): É o campo que limita o número máximo de saltos de um host até o seu destino, afim de evitar-se o loop infinito;
- Endeço de origem: Indica o endereço de origem do pacote;
- Endereço de destino (128 bits): Indica o endereço de destino do pacote.

Além desses campos o cabeçalho Ipv6 pode conter cabeçalhos de extensão, diferente do Ipv4 que trazia os bits referente às informações opcionais existindo elas ou não o Ipv6 somente traz esses bits quando necessário. Esses cabeçalhos adicionais aparecem entre o cabeçalho base e o cabeçalho da camada acima. Caso existam vários cabeçalhos adicionais eles são apresentados em série, conforme imagem abaixo:

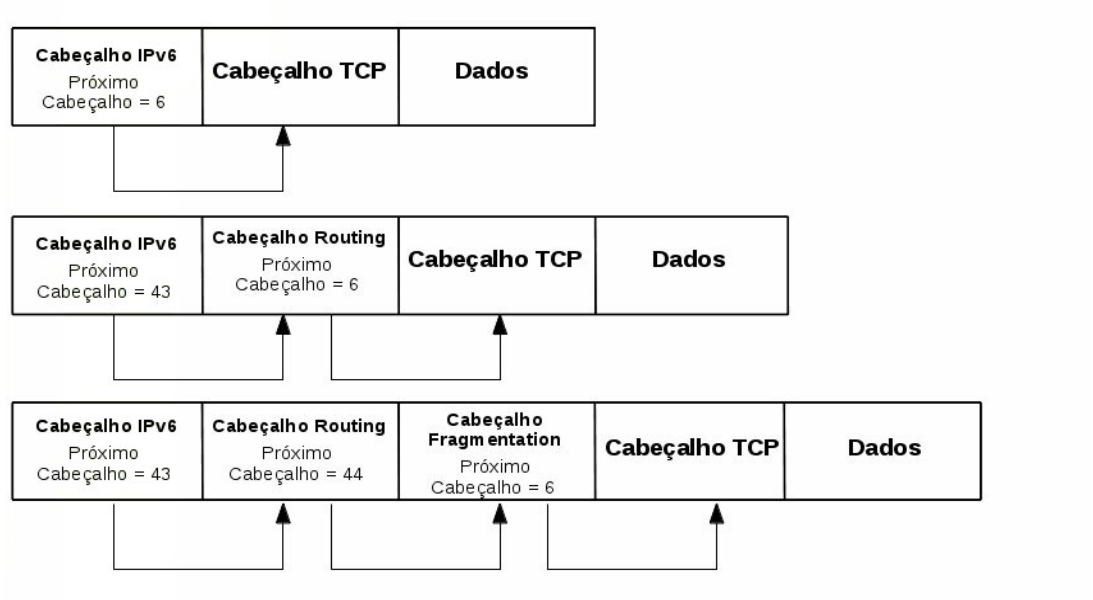

Ilustração 13: Cabeçalho do IPV6 - Fonte - CCNA 5.0

Abaixo seguem os cabeçalhos de extensão e suas funções:

- Hop-by-hop – deve estar presente logo após o cabeçalho base. Deve ser examinado por todos os nós intermediários do caminho da origem ao desrtino. Caso não exista um cabeçalho hop-by-hop, os roteadores não necessitam ler nada além do cabeçalho base. Contem os campos Próximo Cabeçalho, Tamanho do cabeçalho e Opções;
- Destination Options – Como o nome diz, é um cabeçalho usado apenas no destino. É utilizado como suporte ao mecanismo de mobilidade do IPV6;

- Routing – Também auxilia no mecanismo de mobilidade do Ipv6. Possui os campos Próximo cabeçalho, Tamanho do cabeçalho, Routing Type (identifica o tipo de cabeçalho routing, atualmente apenas o Type 2 está especificado), Saltos restantes (indica por decremento quantos saltos há até o destino final) e endereço de origem (mostra o endereço de origem do nó móvel);
- Fragmentation – Como o nome diz, é relacionado à fragmentação de um pacote a ser enviado quando o mesmo é maior que o MTU Path. Esse cabeçalho possui os campos Próximo cabeçalho, Deslocamento do fragmento (indica a posição dos dados do fragmento atual em relação ao início do pacote original, Flag M (se estiver com o valor binário 1, significa que há mais fragmentos, caso esteja com o valor 0, esse será o fragmento final) e identificação (traz um valor único cujo objetivo é identificar o pacote original, onde esse número deverá constar em todos os fragmentos desse pacote);
- Authentication – assim como cabeçalho seguinte (Encapsulating Security Payload) faz parte do protocolo IPSec. Sua função, segundo Andrew S. Tanenbaum (2010) é de verificação da identidade do emissor;
- Encapsulating Security Payload – sua função é fazer com que os dados dentro dos pacotes sejam criptografados e somente o destino tenha acesso à chave para decriptografar e ler a mensagem.

2.4 Roteamento

O roteamento dos dados na Internet ocorre na camada 3 do modelo OSI e pode passar por diversos hops (saltos) até o seu destino final. Pode passar por vários nós, sendo dentro de uma mesma instituição, entre matriz e filial ou pode sair do usuário final, acessar seu provedor de acesso, um roteador de um ptt, roteador de um provedor de serviço até o

seu servidor. Ou de forma simples, em um escritório ou em uma residência a comunicação entre um host e uma impressora através da rede.

Esse roteamento pode ser fixo, definido pelo administrador da rede, com uma rota (Endereço IP darede destino através de uma interface do roteador ou através do ip do próximo salto) fixa para todos os hosts ou pode ser dinâmico. É pelo roteamento que os roteadores conhecem e aprendem a chegar às redes remotas.

Os roteamentos fixos são são configurados através de rotas estáticas e tem a vantagem de consumir menos processamento dos roteadores, no entanto em uma rede de grandes e médias proporções a sua configuração torna-se difícil e até inviável ou quando a topologia muda logicamente ou fisicamente. Pois será necessário alterar todas as rotas estáticas. As rotas dinâmicas são aprendidas pelos roteadores que usam o mesmo protocolo de roteamento. Normalmente os protocolos de roteamento dinâmiico enviam quais são as redes conectadas diretamente a eles mesmos aos seus vizinhos. Esse tipo de roteamento é escalável e aconselhável para redes de médio e grande porte. No entanto, é importante ressaltar, que a utilização dos dois roteamentos em conjunto traz benefícios, como por exemplo, garantir que um tráfego específico tenha uma saída diferente através do roteamento estático. Caso um pacote tenha as duas opções de saída do roteador (estática e dinâmica) a opção escolhida pelo roteador será o roteamento estático, pois por padrão, tem a AD (Distância administrativa) é 1 (maior preferência).

De acordo com a CISCO (CCNA 5.0) podemos elencar as finalidades dos protocolos de roteamento dinâmico para:

- Descoberta de redes remotas – Cada roteador envia aos seus vizinhos suas redes conectadas diretamente e após a primeira troca de tabela de roteamento, recebe novas redes conhecidas por seus vizinhos e repassará para os próximos também essas novas redes aprendidas;

- Manutenção das informações de roteamento atualizadas – Em caso de queda de um link, o protocolo de roteamento dinâmico enviará um pacote contendo a informação na próxima troca de mensagens. Essa atualização é conhecida como convergência;
- Escolher melhor caminho para as redes destino – através de métricas que podem ser Largura de banda do link, número de saltos, e AD (Distância Administrativa);

Pode-se dizer que essas são, também, as vantagens do roteamento dinâmico em relação ao roteamento estático, visto que em caso de mudança da topologia, o protocolo automaticamente irá escolher a melhor rota. Entretanto o problema do roteamento dinâmico é utilizar os recursos de largura de banda e processamento para envio de mensagens de roteamento bem como processar os algoritmos de roteamento.

Pode-se dizer que os protecolos de roteamento dinâmico podem ser de dois tipos:

• Protocolos Internos de Gateway (IGPs) – são os protocolos de roteamento entre uma mesma rede de propriedade de uma empresa. Os protocolos IGPs podem ser separados entre:

➔ Vetor distância – são os protocolos que escolhem o melhor caminho considerando a quantidade de saltos para chegar ao destino. A contagem de saltos incremental é feita a cada vez que um roteador recebe de seu vizinho a mensagem da descoberta de uma nova rede. Esse tipo de divulgação de rotas poderia causar um problema de loop infinito se os protocolos desse gênero não utilizassem o recurso conhecido como *SPLIT HORIZON* que impede que um roteador envie atualizações sobre uma rede aprendida pela mesma interface da qual aprendeu essa nova rede. Caso isso não existisse, em uma rede com dois roteadores, ambos enviariam de um a outro a incrementação de salto + 1;

➔ Link-State – utiliza como métrica a largura de banda entre os roteadores para determinar qual é o melhor caminho.

• Protocolos Externos de Gateway – São os protoclos de roteamento de borda entre AS (Autonomous System).

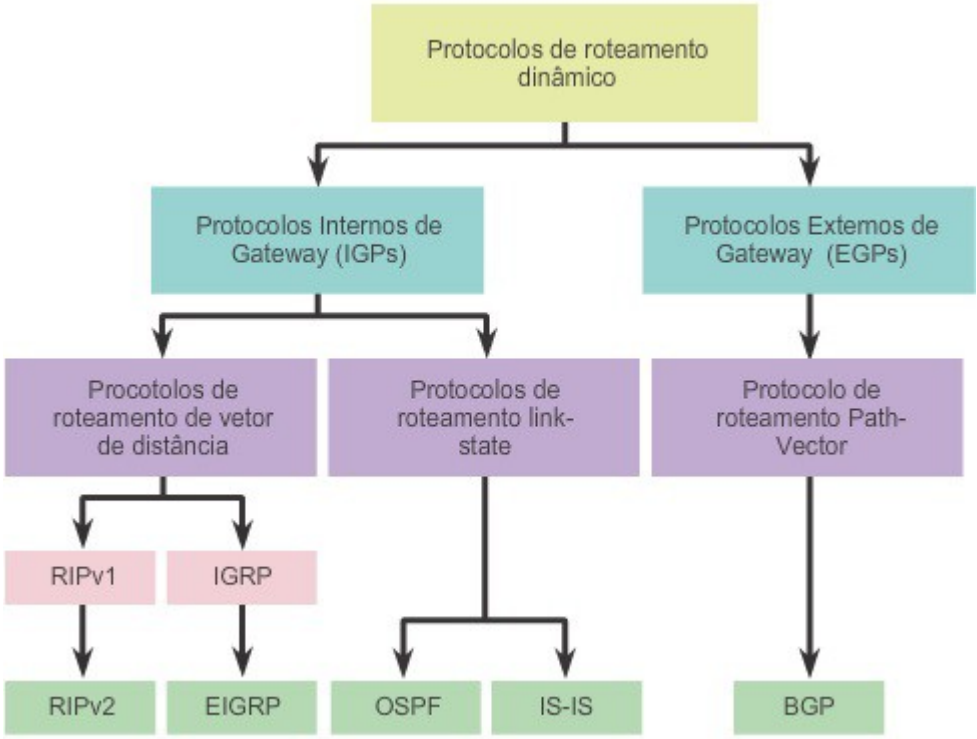

Ilustração 14: Tipos de protocolos de Roteamento Dinâmico - Fonte CCNA 5.0

Abaixo segue a ilustração da classificação dos protocolos de roteamento.

2.4.1 Protcolos de Vetor de Distância

Os protocolos de Vetor de Distância são mais simples porém tornam-se não recomendáveis para redes de grande porte, devido ao limite de saltos e ao maior nível de processamento. E é por esse motivo que foi escolhido o protocolo RIP para o roteamento do tráfego Ipv4 e o RIPNg para Ipv6.

2.4.2 Protocolo de roteamento dinamico RIPNG

O RIPNg (Rip Next Generation) é a versão do protocolo de Roteamento dinâmico RIP para o Ipv6. Na realidade o RIPNg é baseado no RIP versão 2, onde o mesmo possui a

mesma distância administrativa de no máximo 15 saltos e atualizações a cada 30 segundos. Para a configuração do Ipv4 com subrede é necessário ativar a versão 2 do protocolo RIP, que conforme já citado, permitirá a divisão de uma determinada em sub-rerdes.

O RIP V2 envia as atualizações de roteamento para todas as interfaces, inclusive para as interfaces que não possuem roteadores com RIP ativado. É necessário habilitar o comando “Passive interface” na interfaces LAN por exemplo.

A principal diferença entre o RIP V2 e o RIP Ng é a forma de implementação do protocolo. Enquanto que no RIP V2 o protocolo é habilitado na tela de configuração global, no RIP Ng o protocolo é habilitado em cada interface, criando o mesmo domínio para todas as interfaces.

2.4.3 Divulgando Rota Estática RIPNg

Para que o RIPNg divulgue uma rota estática IPV6, é necessário aplicar – no modo de configuração global - a rota estática 0::/0 apontando para o Ipv6 da interface de saída (ex.: 2001:db8:cafe:1::1), acessar o modo de configuração da interface e aplicar o comando “*ipv6 rip domain-name default-information originate”*. Isso fará com que esse roteador seja a origem das informações de rota estática e propagará essa rota aos vizinnhos nas trocas de mensagens.

3. ATIVIDADE PRÁTICA

Esse capítulo consiste no passo-a-passo para configuração do IPV6 em uma rede emulado através do GNS3 e Virtual Box.

3.1 Instalação do GNS3

O GNS3 é uma ferramenta de software livre totalmente free, disponível no site do desenvolvedor www.gns3.com na área de download.

Após o download, basta executar o arquivo de instalação.

Um dos primeiros passos é selecionar os componentes de instalação, pois o GNS3 além de ter o softwara para emular os ativos de rede, o mesmo vem com um pacote para instalar o software emulador de máquinas virtuais (virtual box), WireSharl, Putty entre outros. É importante que todos os itens estejam selecionados.

3.2 Configuração do GNS3

Ao abrir o GNS3 é apresentada uma tela solicitando que o usuário insira o nome do arquivo (Projeto) e o local em que será salvo. É importante que o usuário crie o projeto, para que depois de criar as imagens de máquinas virtuais e roteadores, fiquem todas salvas na mesma pasta, evitando que erros possam ocorrer no momento de salvar o projeto.

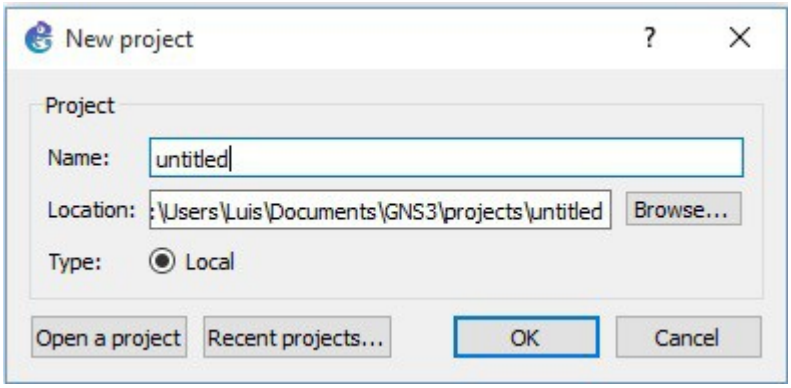

Ilustração 15: Configurando o GNS3 - Fonte: Autoria própria

Criado o arquivo, agora é necessário configurar os emuladores do GNS3. Basicamente é utilizado o Dynamips para emular um IOS (Internetwork Operating Sistem) – sistema operacional dos roteadores Cisco – entre outros e o QEMU, segundo a IBM, é um emulador para sistemas de Computadores. É uma máqiuina dentro de uma máquina.

Antes de iniciar a construção da rede no GNS3, é necessário testar a funcionalidade do Dynamips com a imagem do IOS. O IOS é um software de propriedade da CISCO, por isso é necessário ter um roteador verdadeiro para poder copiar a imagem. Esse processo é explicado no site da própria CISCO através do documento PDF “Copyimage”.

Partindo do princípio que exista a imagem legal do do roteador é necessário acessar o menu “edit” e em seguida a opção “Preferences” quando será apresentada a tela abaixo:

Basta localizar a imagem e avançar para as configurações de nome e plataforma desse roteador (nome do modelo do roteador), avançar novamente quando ele perguntará quanto de memória será alocada para esse roteador (Por padrão 128 MB).

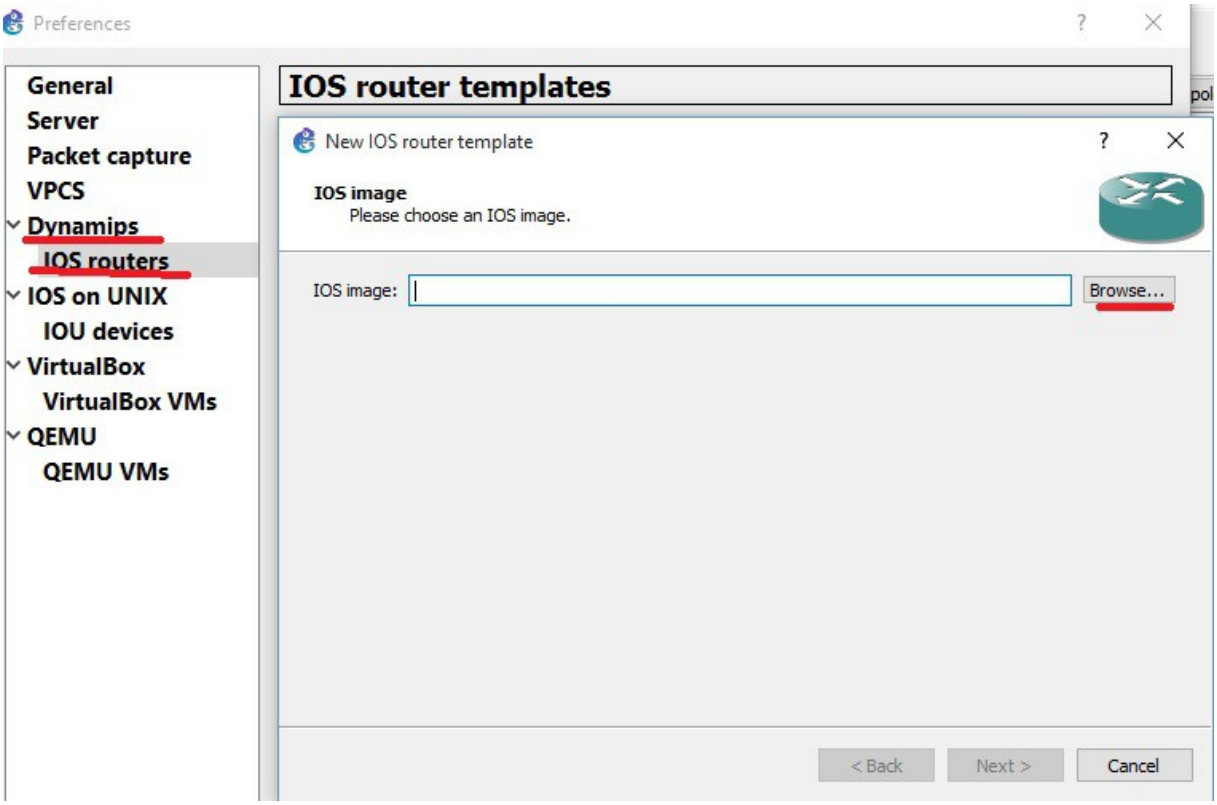

Ilustração 16: Configurando o GNS3 - FONTE autoria própria

Em seguida será apresentado a tela para escolher quantos e quais slots de interfaces será aplicado a esse roteador.

Nesse exemplo, foi escolhido um módulo Ethernet 1/0.

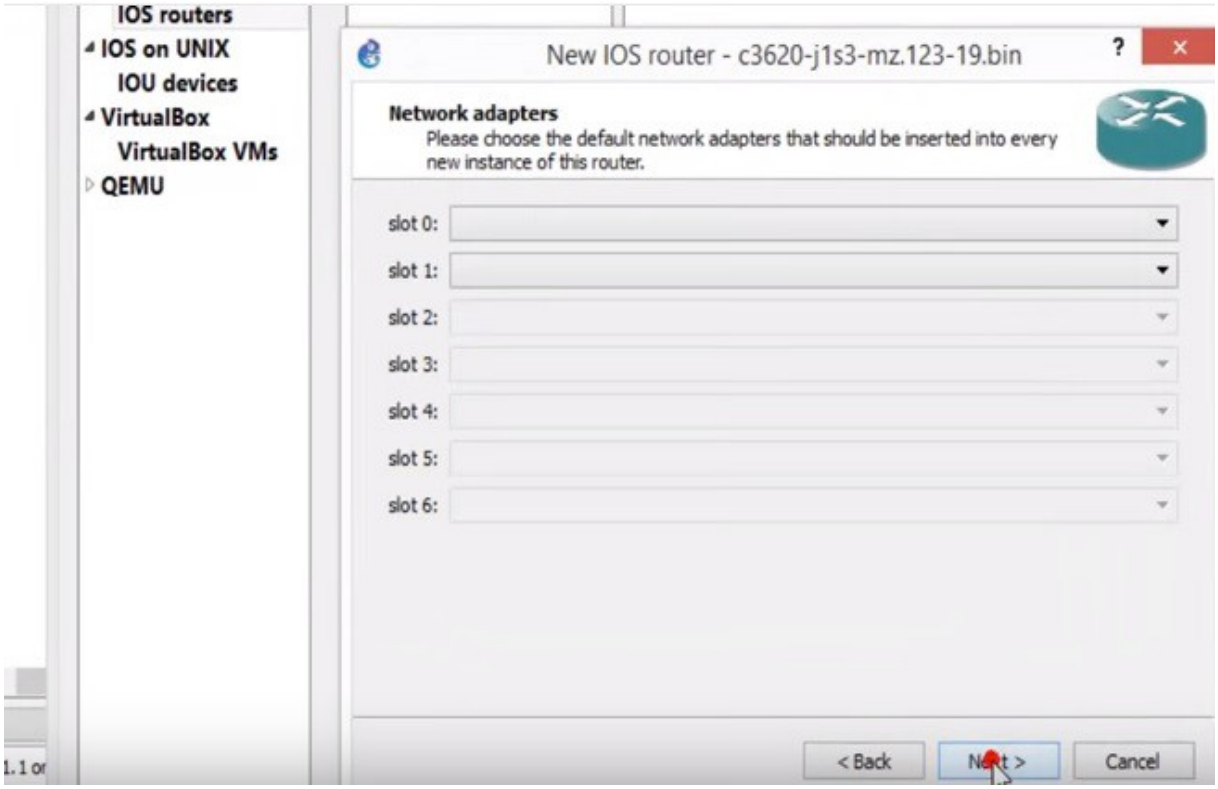

Ilustração 18: Configurando o GNS3 - Fonte autoria própria

Por último é importante clicar em Idle-Pc finder. Isso auxilia no controle de processamento. Ao final deve aparecer a tela com os detalhes do roteador criado.

Agora que o emulador do roteador foi configurado é necessário configurar o emulador de PC, que nesse caso é o VIRTUALBOX. Para isso, ainda na mesma janela (Preferences), é preciso selecionar a opção “VIRTUAL BOX” e adicionar uma máquina virtual, a qual já deve ter sido criado anteriormente. Para fins de teste de emulação de um ambiente real, é importante que seja a mesma ISO dos sistemas operacionais utilizados atualmente, garantindo o ambiente mais próximo do real. Por questões de processamento, optou-se por criar uma máquina virtual com Debian em modo texto.

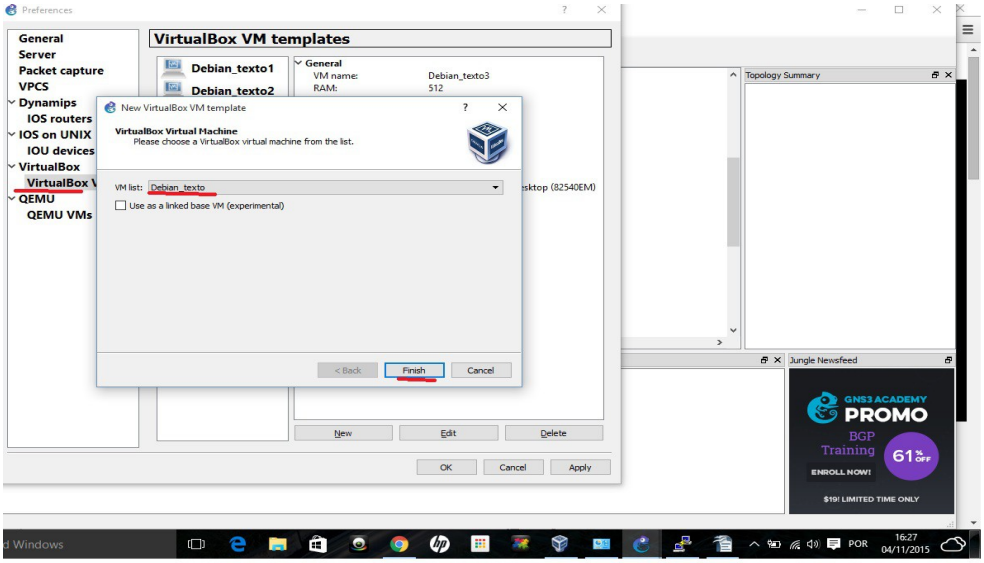

Ilustração 19: Configurando o GNS3 - Fonte autoria própria

3.3 Desenhando a topologia

O próximo passo é desenhar a topologia, o mais próximo da topologia real, se essa é baseada em uma rede real.

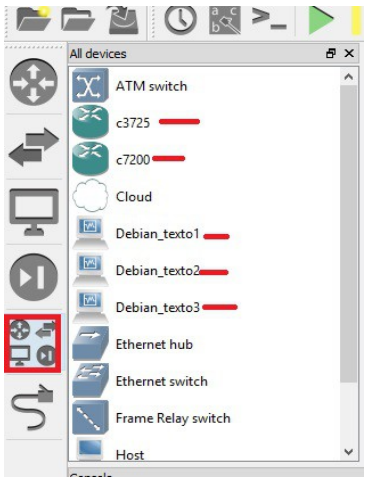

Ilustração 20: Menu- Fonte autoria própria

O menu do lada esquerdo do GNS3 possui todos os elementos (ativos de rede, cabos, etc) que podem ser usados na rede. Basta clicar na opção *"Browse all devices"* para mostrar as máquinas virtuais adicionadas ao GNS3 bem como os roteadores.

Então, é necessário conectar esses equipamento com os cabos disponíveis no mesmo menu, no botão logo abaixo *"Add a link"*. É importante, para fins de documentação e facilidade na configuração da rede, estrruturar essa topologia, demonstrando qual o IP da rede, host, etc.

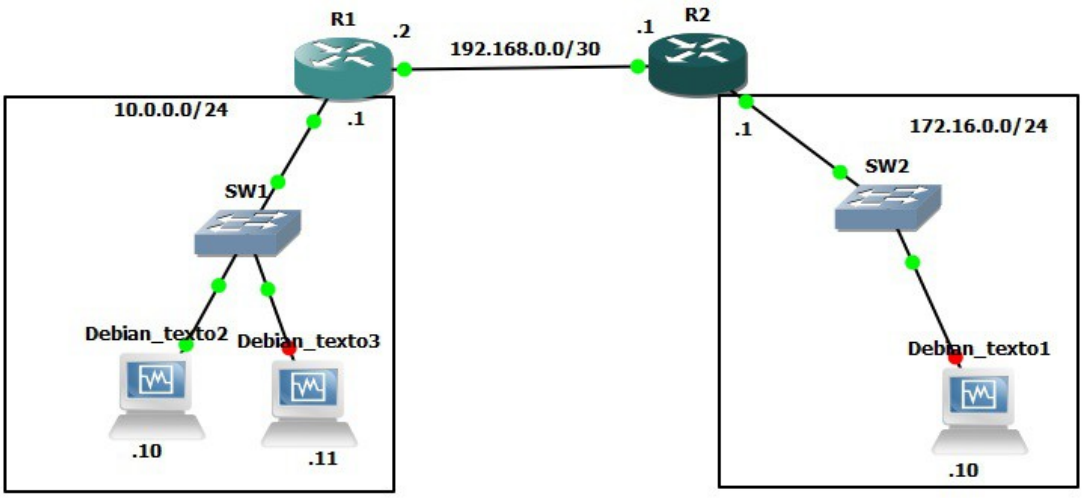

Ilustração 21: Topologia IPV4 - Fonte autoria própria

Para simular uma conexão entre matriz e filial com através de um provedor, optou-se por criar duas LANs (Local Area Network) 10.0.0.0/24 e 172.16.0.0/24 iterligadas através de uma WAN, ponto à ponto. Normalmente, em uma situação real, a WAN é composta por diversos roteadores para sair de um ponto até chegar à filial de um cliente. Para economizar recursos de Ipv4 e aumentar a segurança da conexão entre R1 e R2, foi configurado a rede 192.168.0.0/30, a qual possui apenas 4 endereços IP's, sendo o primeiro (192.168.0.0) o endereço de rede, o último (192.168.0.3) o endereço de broadcast dessa sub-rede e apenas dois endereços de host (finais .1 e .2), sendo um para cada roteador. Optou-se também por definir para os hosts clientes de cada uma da LANs os endereços Ips com final acima de 9, sendo o gateway de cada rede o primeiro IP endereçável (final .1).

Tendo isso definido, basta configurar as interfaces de cada roteador, configurar o ip fixo em cada máquina e habilitar o roteamento dinâmico.

3.4 Configurando Interfaces

Antes de ligar todos os equipamentos, é importante ligar e configurar um equipamento de cada vez, afim de manter os níveis de uso do processador da máquina onde roda o GNS3. Portanto ao escolher o primeiro equipamento a ser configurado, basta clicar com o botão direito do mouse sobre esse equipamento e clicar na oção "*start"* e dar um duplo clique sobre o equipamento para abrí-lo. Nesse momento o Dynamips irá emular a conexão via console com o roteador, conforme tela abaixo.

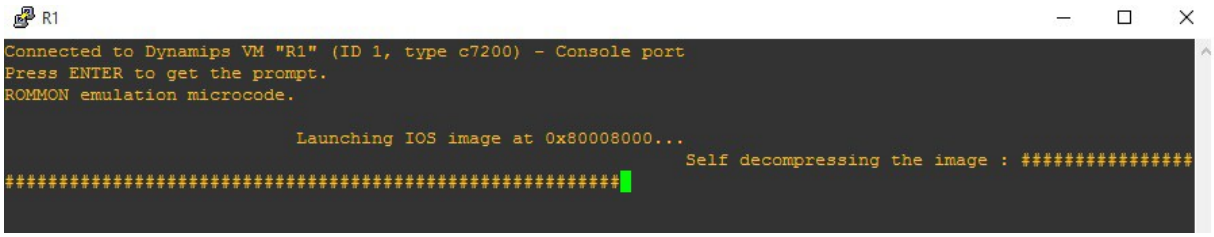

Ilustração 22: Inicando o roteador - Fonte autoria própria

Assim que finalizar o carregamento da memória do roteador, que deverá estar vazia, é necessário acessar o modo de configuração Global pelo comando "*conf term",* acessar a interface a ser configurada *"interface eth 1/0"* e adicionar o IP versão 4 nessa interface pelo comando "*ip address 172.16.0.1 255.255.255.0"* que significa que o endereço IP dessa interface é o primeiro (de 254) host da rede 172.16.0.0/24, ou seja, o *gateway*. Por fim é necessário ligar essa interface através do comando "*no shutdown"*. Agora é necessário fazer o mesmo para a outra interface do mesmo roteador, com base no desenho da topologia.

Para tal, é necessário sair da interface Ethernet 1/0 através do comando "*exit"* e acessar a interface WAN de R1 através do comando "*interface fastethernet 0/0",* adicionar o ip dessa interface pelo comando "*ip address 192.168.0.1 255.255.255.252"* e habilitar a mesma pelo comando "*no shutdown"*.

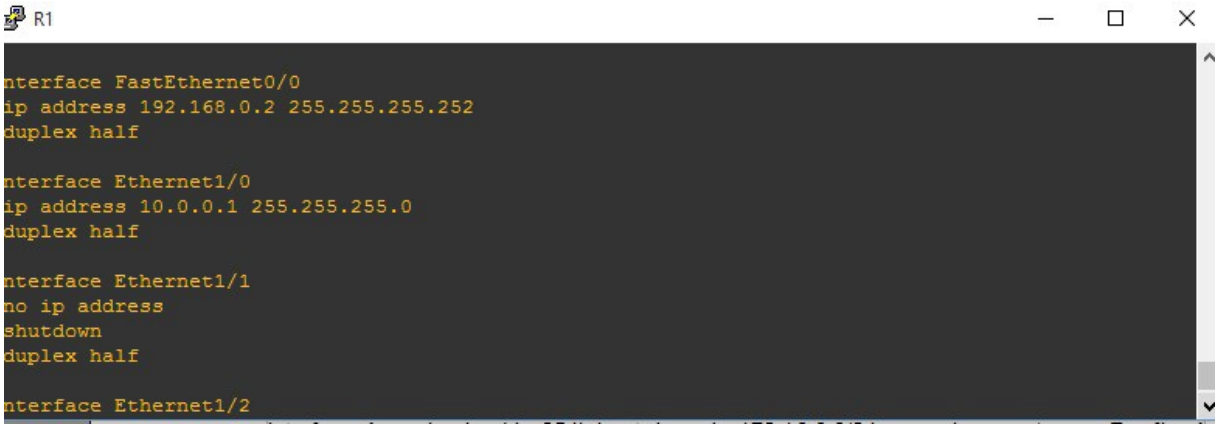

Ilustração 23: Configurando a interface - Fonte autoria própria

Agora basta repetir o mesmo processo para o R2.

3.5 Configurando endereçamento IP no linux

Para verificar quais são as configurações de IP já aplicadas no linux, basta digitar o comando "*ifconfig"* e serão apresentados os resultados como endereço Ipv4 da placa de rede, broadcast e a máscara de rede. Essa linha é identificada pelo nome "*inet end.:",* conforme tela abaixo.

Pelo comando também é possível identificar se o Ipv6 já está habilitado nessa placa de rede. Ele é observado na linha "*endereço inet6:"*. Nesse caso, como não foi definido nenhum IP via servidor ou manualmente, o S.O. Aplicou um endereço de Link-Local, que é identificado pelo prefixo FE80:: misturado ao endereço físico da placa de rede (Mac adress) como já explicado no capítulo 2. Para alterar essas configurações é necessário editar o arquivo que contém essas opções através de algum editor do linux. Nesse exemplo foi usado o "VIM /ETC/NETWORKS" e alterar as linhas de configuração de IP estático.

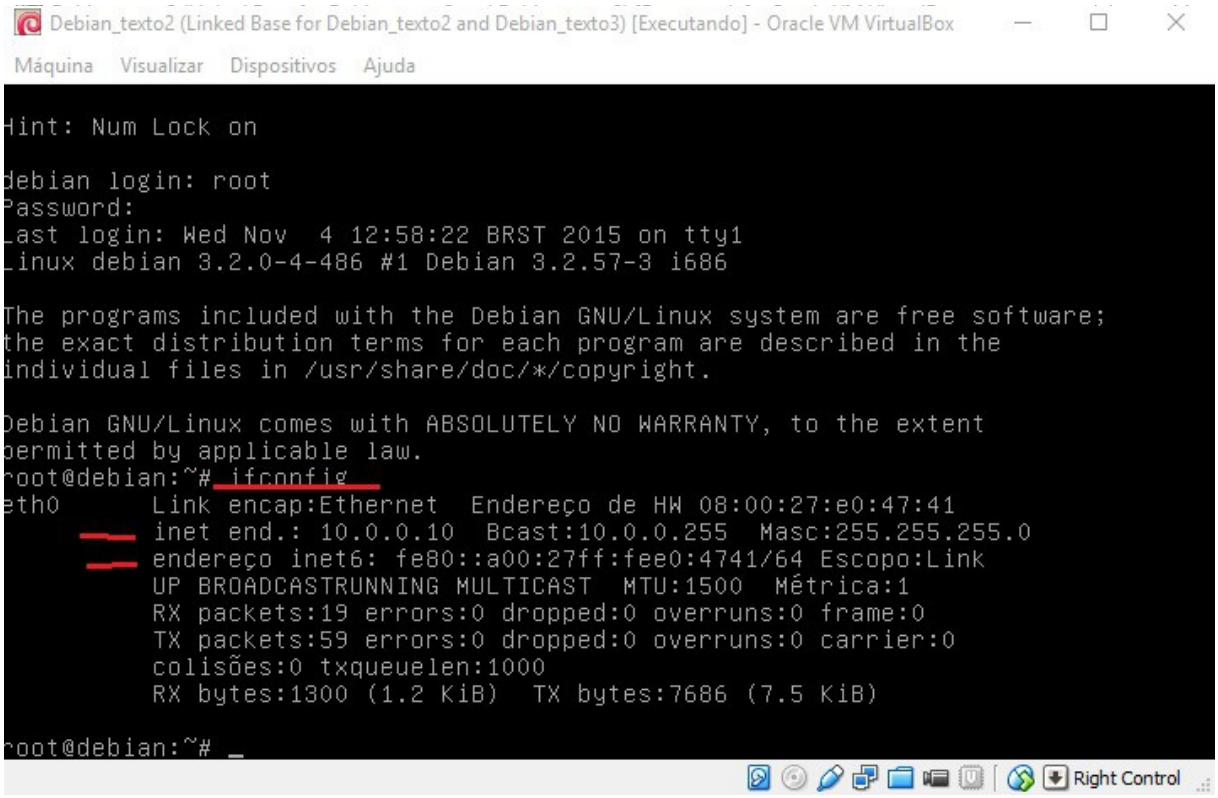

Ilustração 24: Verificar configurações de ip linux - Fonte autoria própria

Agora basta repetir o mesmo processo para as outras máquinas.

3.6 Configurando o Roteamento dinâmico para Ipv4

Apesar dessa topologia ser uma rede pequena, optou-se por configurar o roteamento dinâmico, assim tornando essa rede escalável sem a necessidade de reconfigurar rotas manualmente. O protocolo escolhido foi o RIP Versão 2 para o IP de versão 4, pois essa versão possiblita o uso de VLSM (sub-redes). Para configurar o RIP é necessário acessar o modo de configuração global de cada roteador e cadastrar as redes diretamente conectadas.

No caso do R1, as redes diretamente conectadas são as redes 10.0.0.0 e 192.168.0.0. A configuração é feita através do comando "*Router RIP*" e em seguida, após pressionar enter habilitar a versão dois pelo comando "*version 2*" e o cadastro das redes pelas linhas de comando "Network 10.0.0.0" e "Network 192.168.0.0".

Ilustração 25: Configurando RIP V2 - Fonte autoria própria

E então é só repetir o mesmo processo em R2 com as redes diretamente conectadas a esse roteador.

Ilustração 26: Configurando o RIP V2 - Fonte autoria própria

3.8 Testando a comunicação IPV4 entre as duas LANS

Há diversas maneiras de testar a comunicação entre as duas pontas. A forma mais simples é mandando um teste de PING (Protocolo ICMP). Para isso, pode-se abrir o prompt da máquina 10.0.0.10 e digitar o comando "*ping 172.16.0.10"* que enviará pacotes ICMP para o host destino e esse deverá devolver outros pacotes com confirmação.

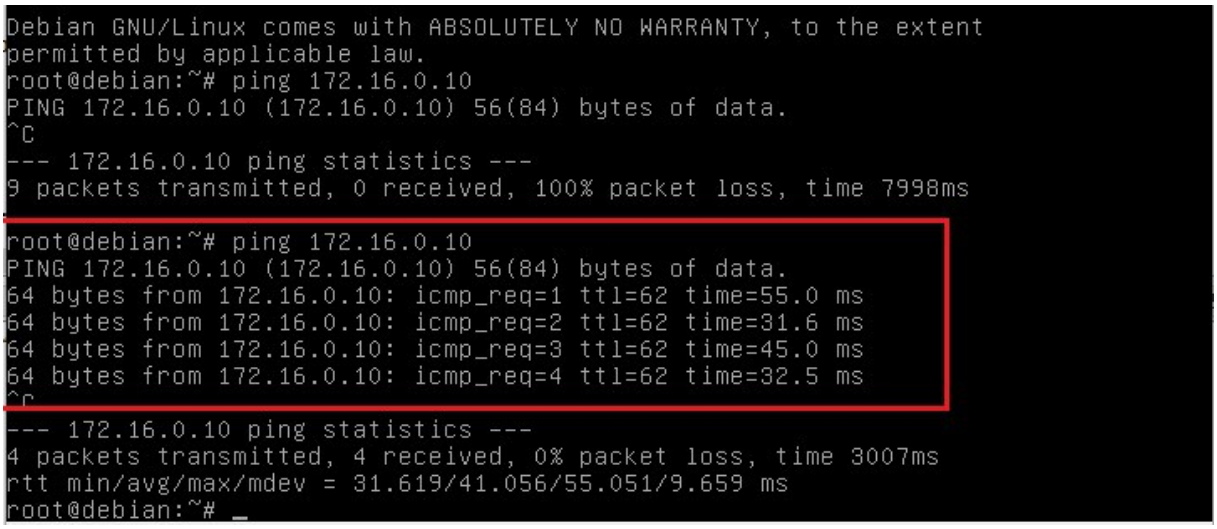

Ilustração 27: Teste de ping - Fonte autoria própria

Também é possível verificar nos roteadores se as redes remotas foram anunciadas pelo protocolo de roteamento dinâmico. Para isso, em dos Roteadores é necessário digitar o comando "*Show ip route*" no modo de usuário privilegiado (Após o comando "*enable"*).

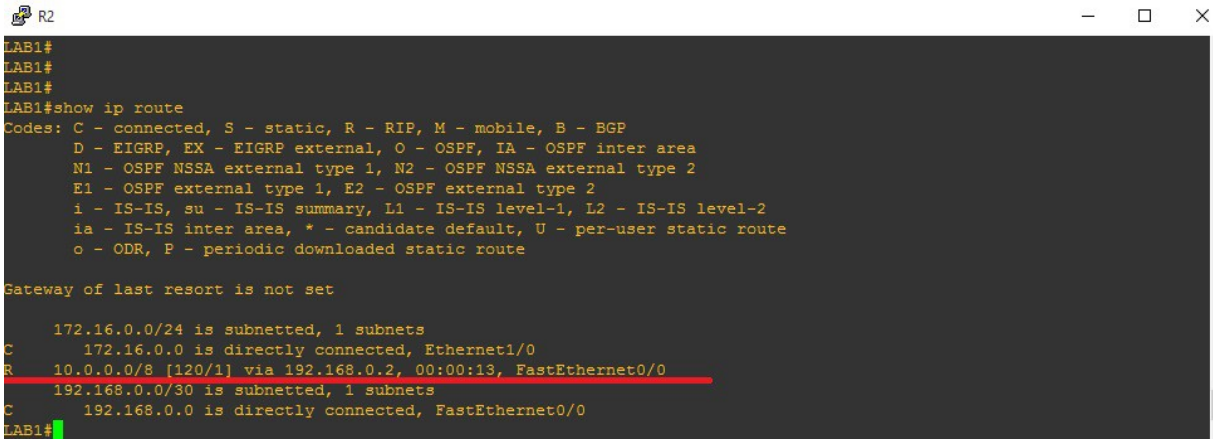

Ilustração 28: Comando show ip route - Fonte autoria própria

Conforme a imagem acima, há duas redes conectadas diretamente ao R2, sendo elas a 172.16.0.0 pela interface Ethernet1/0 e a rede 192.168.0.0 conectada via interface Fastethernet 0/0. Foi identificada na tabela de roteamento de R2 a rede 10.0.0.0 via host 192.168.0.2 (ip da interface do roteador R1) pela interface FasEthernet 0/0 do próprio R2.

3.10 Implementado o IPV6

Da mesma forma que na topologia do Ipv4, é importante planejar primeiro a estrutura da rede, para depois configurar as interfaces e as rotas dinâmicas. Então o primeiro passo é definir as redes IPV6.

Diferente do IPV4, mesmo na rede local, usa-se um endereço global. E como já visto no capítulo 2, os endereçsos globais são 2000::/3. Vale lembrar que os endereços das máquinas serão definidos automaticamente pelo S.O. Assim que o gateway tiver com endereço IPV6 definido.

Segue abaixo a imagem da proposta da estrutura de rede IPV6.

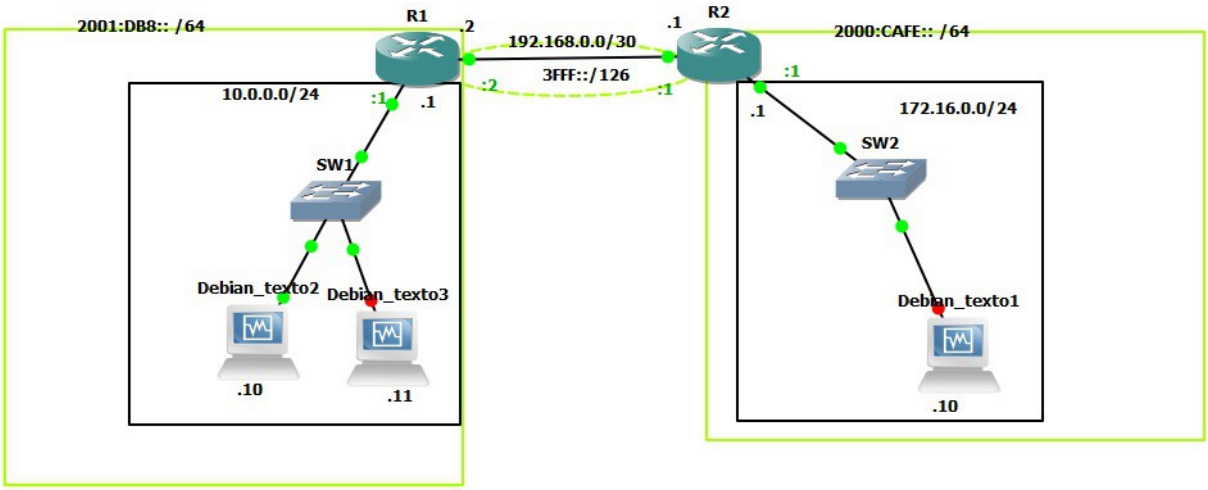

Ilustração 29: Topologia IPV6 - Fonte autoria própria

Pela imagem é possível verificar que o protocolo IPV4 continua funcionando sem nenhuma alteração. Apenas foi adicionado a versão 6 em paralelo (marcado em verde). Para as redes locais foi definido uma rede /64, que é foi definido o padrão a ser entregue ao usuário fina pela RFC. Já para a rede WAN, optou-se por limitar o número de Ips nessa rede, visto que trata-se de um ponto a ponto.

Definido a topologia, agora é necessário adicionar o Ipv6 em ambos os roteadores, habilitando o tráfego ipv6 e adicionando endereços ipv6 às suas interfaces.

3.11 Habilitando e Configurando o Tráfego Ipv6 nos Roteadores

Primeiramente é necessário permitir que o roteador roteie os pacotes IPV6, pelo comando "*ipv6 unicast-routing"* na área de configuração global. Depois é necessário entrar em cada uma das interfaces e adicionar junto ao endereço IPV4 o endereço IPV6, pela sequência de comandos *"interface NOMEDAINTERFACE", "ipv6 add ENDEREÇOIP/MASCARA"*

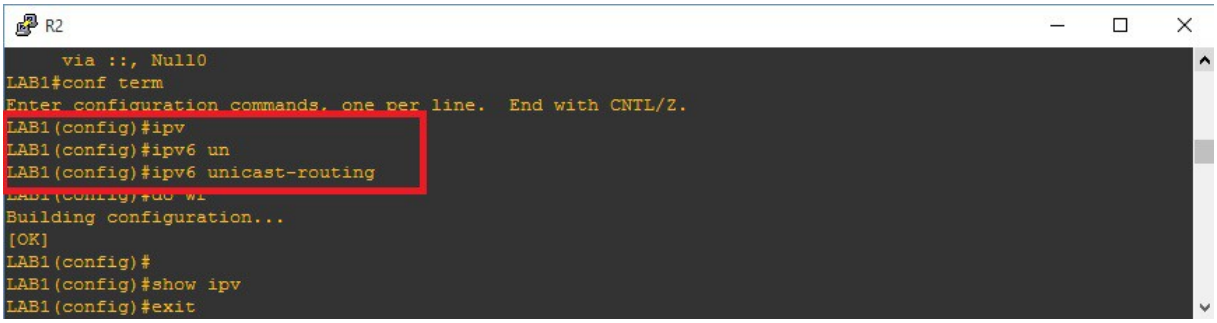

Ilustração 30: Adicionar IPV6 - Fonte autoria própria

Após aplicar os endereços às interfaces, é necessário configurar o roteamento dinâmico. Para habilitar o RIPNg, diferentemente do IPV4 com RIP v2, não é necessário dizer quais são as redes conectadas para divulgálas dinamicamente. É necessário apenas criar um nome de domínio RIP dentro das interfaces envolvidas, através do comando "ipv6 rip NOMEDOMINIO enable", conforme imagem abaixo.

Ilustração 31: Aplicar o RIPNg - Fonte autoria própria

Para que os roteadores comecem a trocar informações de roteamento dinâmico é necessário repetir o mesmo processo para o R1. Após isso é possível verificar a as redes anunciadas via protocolo pelo comando *"Show Ipv6 route".*

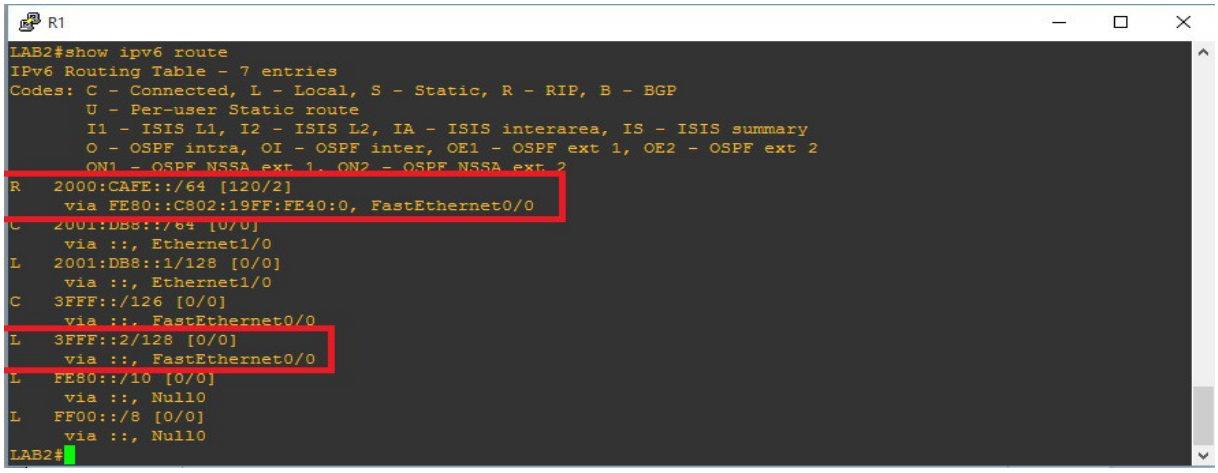

Ilustração 32: Mostrar rotas - Fonte autoria própria

3.12 Testando a Conexão Remota

Para executar o teste de comunicação do IPV6, pode ser utilizado o mesmo teste realizado para o IPV4. Através do protocolo ICMP, "PING6".

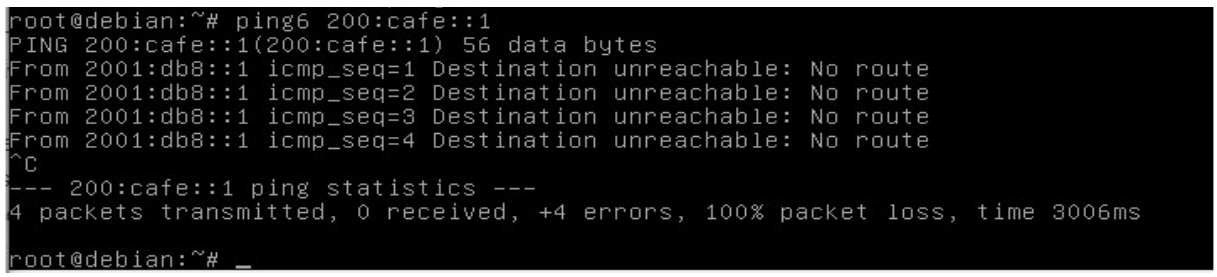

Ilustração 33: Teste de comunicação IPV6 - Fonte autoria própria

4. CONCLUSÃO

O protocolo IPV6 traz diversas vantagens a todos usuários da rede mundial. No entanto ainda é necessário incentivar a utilização deste protocolo demonstrando seus benefícios. A implantação da nova versão foi efetuada através do emulador GNS3 com sucesso, sem alterações no protocolo antigo, sendo que a utilização de ambos poderá ser realizada ao mesmo tempo, dependendo do serviço acessado no destino, tendo assim atingido assim o onjetivo inicial dessa monografia.

REFERÊNCIAS

IPV6.BR, *Endereçamento IPv6*. Disponível em < http://ipv6.br/entenda/enderecamento/> Acesso em 08/06/15

IPV6.BR, *Endereçamento IPv4*. Disponível em < http://ipv6.br/entenda/enderecamento/> Acesso em 08/06/15

IPV6.BR, f*ragmentação IPv4*. Disponível em < ipv6.br/entenda/introdução/ /> Acesso em 08/06/15

IBOPE, Pesquisa da utilização de internet entre as classes no Brasil 2012. Disponível em < Gráfico de utilização de internet domiciliar no Brasil
Fonte: IBOPE - http://imguol.com/2012/11/01/grafico-ibope-1351803347198_563x333.png> Acesso em 07/06/2015,

FARREL, Adrian, A Internet e Seus Protocolos, Capitulo 2, Endereçamento IPv4