UNIVERSIDADE EDUARDO MONDLANE
FACULDADE DE ENGENHARIA
CURSO DE ENGENHARIA ELECTRÓNICA

Trabalho de Licenciatura

Tema: Proposta de Migração do Protocolo IPv4 Para o Protocolo IPv6 em Redes de Computadores Em Moçambique

Autor:
Denilson Rafael Langa

Supervisora:
Engª Ivone Cipriano

Coordenador:
Eng˚ Julian Garzon

Maputo, Junho de 2022

UNIVERSIDADE EDUARDO MONDLANE
FACULDADE DE ENGENHARIA
CURSO DE ENGENHARIA ELECTRÓNICA

Trabalho de Licenciatura

Tema: Proposta de Migração do Protocolo IPv4 Para o Protocolo IPv6 em Redes de Computadores Em Moçambique

Autor:

Denilson Rafael Langa

Trabalho de Conclusão de Curso apresentado à Faculdade de Engenharia da Universidade Eduardo Mondlane, como parte dos requesítos para obtenção do título de Licenciatura em Engenharia Electrónica.

Supervisora: Engª Ivone Cipriano

Coordenador:

Eng˚ Julian Garzon

Maputo, Junho de 2022

Agradecimentos

A Deus em primeiro lugar por sempre me abençoar e permitir que as dificuldades viessem para que pudesse crescer e enxergar a vida por outras perspectivas. Em especial a minha supervisora, Engenheira Ivone Cipriano por ter contribuído com o seu importantíssimo subsídio no desenvolvimento do estudo em questão e por ter acreditado na minha vontade de realizar a pesquisa.

A minha família, em especial àqueles que sempre estiveram me apoiando moral e financeiramente. A minha mãe Beatriz Tembe pelo amor incondicional, ao meu avô Henrique Filipe por cuidar e me amar como filho, a minha avó Adelina Massango por se sacrificar e me apoiar incondicionalmente. A minha tia e mãe Dânia Simione pelo carinho e apoio, aos meus irmãos Henrique Langa e Júlia Langa pelo suporte.

Aos meus amigos e colegas: Edson Nhamtumbo, Chelsea Malauene, Albino Mahumana, Nilza Cossa, Enoque Muchanga, Calvin Maposse, Makumene Mpiuka e Bejamin Matsinhe pelas palavras de encorajamento e partilha de bons momentos.

Um profundo agradecimento a todos que fizeram parte da minha jornada acadêmica directa ou indirectamente.

RESUMO

Tendo em vista que diversas áreas de negócios como industrias, empresas e instituições acadêmicas adoptaram serviços assentados nas tecnologias de informação mas que por outro lado a condição atual do protocolo fundamental da *Internet* apresentar alguns obstáculos para fazer face a condição presente da rede mundial, pesquisa-se sobre técnicas de transição do protocolo IPv4 para o protocolo IPv6 em redes de computadores, a fim de propor um modelo de migração do protocolo IPv4 para o protocolo IPv6. Para tanto, é necessário incialmente, apresentar a arquitetura de rede baseada no protocolo Ipv4, identificar os constragimentos do protocolo IPv4 e descrever as caracteristicas do funcionamento do protocolo IPv6. Portanto, realiza-se o trabalho baseando-se numa pesquisa de finalidade básica estratégica, objectivo descritivo, sob o método hipotético-dedutivo, com abordagem qualitativa com realização de procedimentos bibliográficos e documentais. Diante disso, verifica-se que as técnicas de transição oferecem um meio para que os dois protocolos possam interoperar por um bom período de tempo até que o IPv6 seja maioritariamente implantado e por fim o IPv4 substituído. Verifica-se ainda, que as diferentes técnicas de migração para além de oferecerem suporte para a interoperabilidade dos protocolos podem também funcionar numa mesma rede oferecendo serviços diversificados para dificuldades específicas.

Palavras-chave: Transição para o IPv6. Migração do IPv4 para o IPv6. Pilha dupla, Tunelamento. Protocolos.

Abstract

Considering that several business areas such as industries, companies and academic institutions adopted services based on information technologies, but on the other hand, the current condition of the fundamental Internet protocol presents some obstacles to face the present condition of the global network, transition techniques from IPv4 protocol to IPv6 are researched, in order to propose a migration model from the IPv4 protocol to the IPv6 protocol in computer networks. To do so, it is necessary initially to present the network architecture based on the IPv4 protocol, identify the constraints of the IPv4 protocol and describe the characteristics of the operation of the IPv6 protocol. Therefore, the work is carried out based on a research of basic strategic purpose, descriptive objective, under the hypothetical-deductive method, with a qualitative approach with bibliographic and documentary procedures. In view of this, it appears that the transition techniques offer a means for the two protocols to interoperate for a good period of time until IPv6 is mostly implemented and finally IPv4 is replaced. It is also verified that the different migration techniques, in addition to offering support for the interoperability of protocols, can also work in the same network, offering diversified services for specific difficulties.

Keywords: Transition to IPv6. Migration from IPv4 to IPv6. Double stack, Tunneling. protocols.

Sumário

Lista de Siglas

ARP	Address Resolution Protocol
ARPANET	Advanced Research Projects Agency Network
BGP	Border Gateway Protocol
CGNAT	Carrier Grade NAT
CGI.BR	Comitê Gestor da Internet no Brasil
CIDR	Classless Interdomain Routing
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain name System
EUI-64	Extended Unique Identifier 64
FTP	File Transfer Protocol
GTA	Grupo de Teleinformática e Automação
GUA	Global Unicast Address
HTTP	Hypertext Transfer Protocol
IoT	Internet of Things
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
INTIC	Instituto Nacional de Tecnologias de Informação e Comunicação
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
LAN	Local Area Network
LLA	Link Local Address
MAC	Media Access Control Address
MPLS	Multi - Protocol Label Switching
NAT	Network Address Translation
NIC.BR	Núcleo de Informações e Coordenação do Ponto BR

OSI	Open System Interconnection
OSPF	Open Shortest Path First
PDU	Packet Data Unit
POP3	Post Office Protocol 3
RA	Router Advertisement
RFC	Request For Comments
RIP	Routing Information Protocol
RS	Router Solicitation
SLAAC	Stateless Auto Configuration
SSI	Sistema de Segurança Interna
TIC	Tecnologia de Informação E Comunicação
TCP	Transmission Control Protocol
TTL	Time To Live
UDP	User Datagram Protocol
UFRJ	Universidade Federal do Rio de Janeiro
ULA	Unique Local Address
WAN	Wide Area Network
WWW	World Wide Web

Lista de Figuras

Capítulo 1 – Introdução

1.1 Contextualização

Nas últimas duas décadas, o mundo vem vivenciando uma evolução a larga escala em vários ramos, sobretudo no que diz respeito as tecnologias computacionais. Diante deste contexto, as tecnologias impulsionaram os ramos de produção, contribuindo para o surgimento da indústria 4.0**.** Sabe-se que no período da primeira revolução, a produção manual era praticamente dominante nas industrias, entretanto, com o avanço tecnológico, verifica-se a predominância das tecnologias proporcionando serviços diversificados com enfoque em sistemas automatizados, sistemas ciber-físicos, *Internet* das coisas (IoT), entre outros.

Consequentemente, estas tecnologias proporcionam vantagens incontestáveis, nomeadamente a redução de custos, produção mais eficiente com serviços de alta qualidade. Por outro lado, no ramo de negócios são hoje destacadas de forma recorrente as tecnologias de informação e comunicação (TICs), pois, o modelo de funcionamento das organizações da actualidade alicerçam os seus serviços e produtos em redes de computadores, ou seja, serviços em rede. Com vários outros serviços alicerçados em TICs, o seu crescimento experimenta o pico na *Internet* das coisas. Neste último, a demanda por recursos e serviços baseados em redes de computadores segue sem precedentes e segundo dados levantados pela Statista (2021), estima-se que dispositivos envolvendo IoT, alcancem a marca dos 75 bilhões de dispositivos em 2025 contra os atuais 5.17 bilhões.

O denominador comum que torna as tecnologias de informação tão fulcrais para o funcionamento e contínuo avanço das diversas áreas em que atua, são as formas como os diferentes serviços se interligam. No que diz respeito as redes de computadores, os protocolos usados nesses sistemas, são responsáveis por gerir as comunicações de todos os dispositivos e regras entre os mesmos. No decorrer do tempo, várias soluções e serviços surgiram, tornando se necessário a criação de diferentes protocolos para atender a situações específicas. Entre eles, o Protocolo da Internet (IP), é provavelmente o mais importante por ser o mais abragente em redes de computadores.

O IP apresenta duas versões atualmente em uso no mercado, o IPv4 e IPv6. O IPv4 é o mais antigo e atualmente o mais utilizado compondo 64% das redes implantadas em todo mundo segundo dados do *Google* (2022). Embora o IP tenha sido criado sem a previsão de que a *Internet* se tornaria no que ela é hoje, várias funções foram integradas

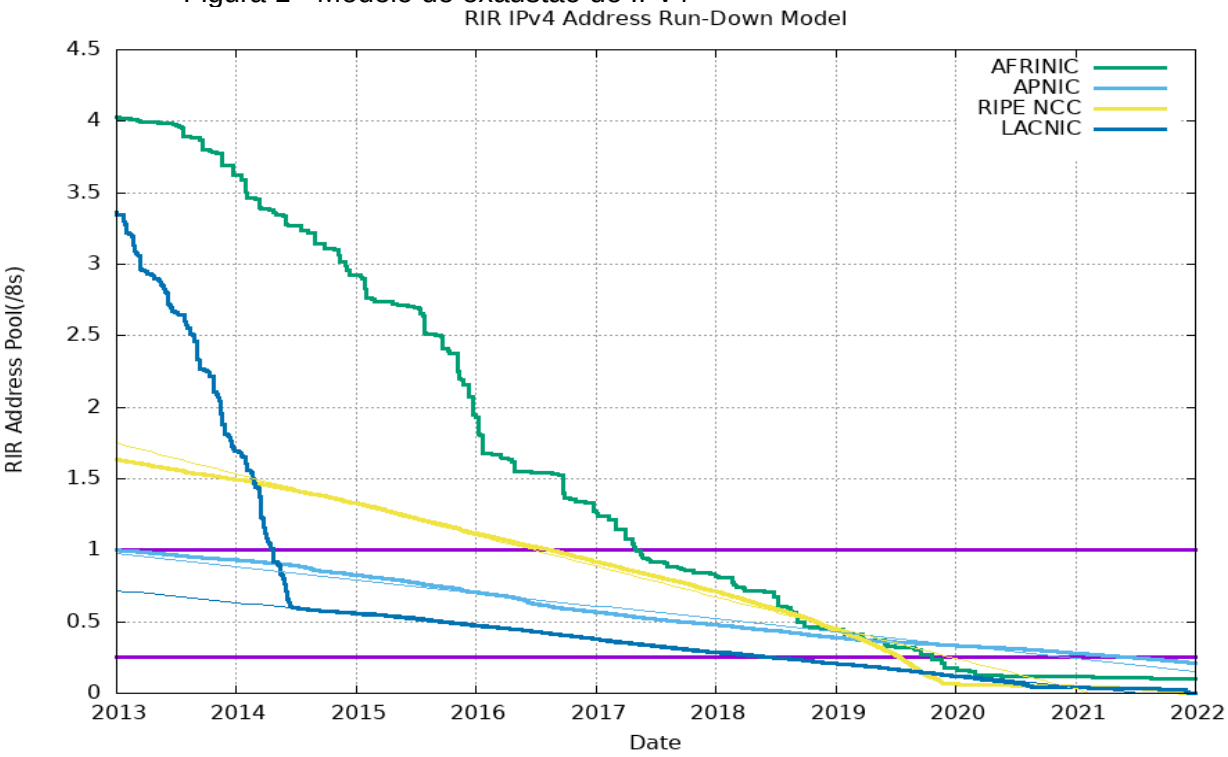
a ele para que pudesse dar suporte as demandas de serviços que foram surgindo, em muitos casos funcionando perfeitamente. Porém, varios outros obstáculos foram surgindo, alguns dos quais o IPv4 mostra-se ineficiente para dar suporte. Desta forma, a *Internet Engeneering Task Force* (IETF), propôs em 1994 a versão 6 do IP (IPv6), dentre as várias aplicações deste protocolo, surge também como forma de auxiliar em certas limitações encontradas no IPv4.

1.2 Formulação do problema

Acontece que, como observa Torres (2001), cada máquina ligada a uma rede de computadores, deve possuir um número único e que não pode ser duplicado, esse número é o IP. Neste sentido, ele torna-se a base fundamental para comunicação nas redes de computadores, sendo o IPv4 atualmente o mais usado. No entanto, o crescimento das redes de computadores interligadas a *Internet* traz como consequência a escassez de endereços IPs em vigor, pois este, possui 32 bits em sua estrutura o que possibilita um pouco mais 4 bilhões de endereços, número consideravelmente alto, mas não se comparado com a realidade atual das máquinas conectadas a *Internet.*

Em vista disso, vislumbra-se num futuro breve, o esgotamento dos endereços IPv4, não havendo mais endereços IP para conectar os novos entrantes e serviços às redes de computadores. Segundo dados levantados pela, *Internet Live Stats* (2021), estima-se existir atualmente, 1.88 bilhões de *websites* disponíveis na rede mundial, comumente conhecida como *Internet*. Ocorre que, se a quantidade de IPs disponíveis forem comparados com a quantidade de servidores, roteadores, computadores e outros dispositivos interligados, esse número aproxima-se dos 4 bilhões de endereços disponíveis, e segundo a Autoridade para Atribuição de Números da *Internet* (IANA, 2014), a rede mundial está sofrendo a exaustão de endereços IPv4. A figura 1 ilustra essa escassez nos registradores dos quatro continentes.

Figura 1 - Modelo de exaustão do IPv4



Fonte: Labs – Repositório Digital da APNIC[1] (2022)

Com o objetivo de colmatar a fragilidade que este protocolo apresenta, vários mecanismos entre eles o *Network Address Translation* (NAT), foram incorporados nas redes de computadores de modo a tornar mais racional e cuidadoso a alocação de endereços IPs. No entanto, mesmo com as várias soluções paliativas adoptadas, a demanda pelo uso da *Internet* segue crescendo expressivamente, com a iminência do esgotamento total dos últimos blocos de endereços IPv4, demostrando ser um obstáculo para a interligação de novos dispositivos ou redes de computadores, opondo-se igualmente ao desenvolvimento e aplicabilidade da *IoT*. Para além dos aspectos descritos acima, o IPv4 apresenta outras fragilidades, como o facto de não ter sido projetado inicialmente para suportar serviços móveis e por não apresentar mecanismos de segurança, tornando-se um desafio para serviços financeiros disponibilizados na *Internet.*

Portanto, com o propósito de trazer soluções em virtude das limitações que o IPv4 apresenta, o presente trabalho ira guiar-se por meio da seguinte pergunta de pesquisa: Que mecanismos podem ser implementados nas redes de computadores de modo a fazer face a situação atual de escassez de endereços IPv4?

[1] https://labs.apnic.net/ipv4/report.html acesso em 05 de janeiro de 2022

1.3 Justificativa

O tema que se apresenta neste trabalho “Proposta de Migração do IPv4 para o IPv6 em redes de computadores”, teve como fundamento vários factores. Primeiramente, pelo facto de redes baseadas no IPv4 rumarem para o seu desfecho com a exaustão de endereços Ips, tornando-se urgente dessa forma, encontrar outras medidas para o contínuo uso e crescimento das redes de computadores e da *Internet* evitando a paralisação destes serviços. O estudo de IPv6 como proposta torna-se crucial então, por apresentar uma solução de continuidade dos serviços computacionais, sendo uma delas os seus 340 decilhões de endereços IP.

Partindo do princípio de que grande parte das industrias, organizações e diferentes instituições, edificam a sua estrutura de funcionamento alicerçadas nas redes de computadores ou *Internet,* a implementação de mecanismos apropriados torna-se oportuna e fundamental para o contínuo funcionamento da rede mundial e para oferecer suporte as novas tecnologias que demandam o uso massivo de IPs.

Por outro lado, o baixo índice de estudos do género em Moçambique demostra ser uma lacuna, para o futuro de redes de computadores no país. Nesta perspectiva, o estudo mostra-se relevante pois pesquisas com enfoque no tema proposto irão permitir técnicos de TI mais preparados para responder aos problemas enumerados e mais qualificados para as condições da *Internet* futura.

Por último, porém não menos importante, para o autor deste trabalho, esta pesquisa irá contribuir de forma significativa no seu aprendizado, dotando-lhe de competências para responder aos desafios no tocante as redes de computadores.

Como um dos primeiros trabalhos de pesquisa em relação ao tema na faculdade de engenharia, espera-se que o pioneirismo possa incentivar empresas e futuros alunos a se interessarem pelo estudo. Espera-se também, atrair a atenção ao assunto e contribuir para a pesquisa de implementação de novas soluções de redes de computadores em Moçambique.

1.4 Objectivo geral

Apresentar uma proposta de migração do protocolo IPv4 para o protocolo IPv6 em redes de computadores.

1.5 Objectivos específicos

- Identificar os principais componentes passíveis de transição do protocolo Ipv4 para o protocolo Ipv6 em redes de computadores;

- Desenvolver redes experimentais usando técnicas de migração;
- Descrever e analisar as experiências realizadas para validar o funcionamento das técnicas de migração em ambientes reais e virtuais de redes de computadores.

1.6 Metodologia

Metodologia científica corresponde a um conjunto de técnicas usadas em trabalhos de pesquisa com a finalidade de responder a um problema proposto de forma detalhada e meticulosa.

Todo o projecto de estudo precisa responder e descrever o processo de pesquisa do trabalho, respondendo de forma clara e concisa os caminhos usados para chegar a uma determinada conclusão sobre o problema proposto..

Portanto, importa relatar sobre a metodologia usada para o desenvolvimento deste trabalho. Quanto a metodologia, um trabalho pode ser classificado de 4 formas:

- Quanto ao objectivo;
- Quando a abordagem;
- Quanto aos Procedimentos;
- Quanto a Natureza.

O objectivo ou finalidade de um trabalho pode ser classificado de três formas, exploratório, descritivo e explicativo. Este trabalho faz o uso do tipo descritivo pois, pretende caracterizar o objecto de estudo em relação as variáveis que se relacionam com ela através de levantamento e registro de caracteristicas dos mesmos. Em outras palavras, todos os artigos analisados não sofrem influência ou modificações pelo autor desde trabalho. (COELHO,2017)

A abordagem de pesquisa refere-se à forma que se faz a análise de dados coletados e pode ser classificada como abordagem qualitativa, quantitativa e quali-quantitativa. O presente trabalho foi explorado através da abordagem qualitativa porque este tipo de abordagem permite compreender em profundidade, fenómenos a partir de explicações e motivos sem dados mensuráveis. (COELHO,2017)

As técnicas ou procedimentos, correspodem aos métodos usados para a coleta de dados para o trabalho de pesquisa. Eles podem ser classificados em pesquisas

bibliográficas, documentais, experimentais, estudo de campo, entre outros. (COELHO,2017)

O presente trabalho apoiou-se nos procedimentos de pesquisa bibliográfica e documental. A pesquisa bibliográfica consiste no uso de material previamente elaborado e por se tratar de fontes secundárias, esta é composta por livros, artigos cientificos, trabalhos de conclusão de curso e outros textos divulgados electronicamente que procuram explicar o problema do tema e que constituem base para desenvolvimento da monografia. (COELHO,2017)

Quanto a natureza, o projecto de pesquisa pode ser classificado como, básica e aplicada. Este trabalho é classificado como pesquisa básica estratégica pois pretende aprofundar os conhecimentos da matéria mas com o foco de aplicar esses conhecimentos para solucionar um problema específico. (COELHO,2017)

1.7 Estrutura do trabalho

O presente trabalho de pesquisa, é dividido em quatro capítulos. Introdução, revisão bibliográfica, proposta de implementação e conclusão.

O capítulo 1 aborda assuntos introdutórios, apresentando a contextualização da pesquisa, formulação do problema, a justificativa do tema, objectivos geral e específicos, e culmina com a metodologia de pesquisa usada.

O capítulo 2, apresenta o referencial bibliográfico usado na elaboração da pesquisa. Ele apresenta três secções: apresentação da arquitetura das redes IPv4, síntese dos constrangimentos das redes IPv4 e por último, aspéctos relacionados as redes IPv6.

O capítulo 3 apresenta a implementação de topologia de redes usando as técnicas de migração, discussão e análise dos resultados de simulações de redes usando o cisco packet tracer.

O capítulo 4, apresenta as conclusões de pesquisa as limitações e as recomendações para trabalhos futuros que pretendam explorar este tema.

Capítulo 2 - Revisão da Literatura

2 Arquitetura de redes IPv4

2.1 Rede de computadores

Segundo Kurose e Ross (2014), redes de computadores, designa-se ao conjunto de dispositivos electrónicos interligados por um meio de transmissão que, com base em regras de comunicação podem compartilhar, informações, dados, serviços, entre outros recursos lógicos. Estas são projectadas com o objectivo principal de partilhar recursos, serviços e prover comunicação. Em relação ao modo de partilha recursos, podem ser destacadas dois tipos de redes: Redes ponto a ponto e redes cliente servidor. A figura abaixo ilustra uma rede de computadores.

Figura 2 - Esquema de uma rede de computadores

Fonte: Site oficial de Gabriel Borba[2]

2.2 Classificação de redes

Uma rede é um aglomerado de computadores que disponibilizam e podem prover serviços uns aos outros. Esta pode ser interligada com várias outras, formando uma estrutura de *internet* (redes interconectadas), surgindo assim, várias classificações para os diferentes tipos de ligações. Entre as diversas classificações, as que mais se destacam são: quanto a abrangência, quanto a topologia, quanto ao método de transmissão e quanto ao modelo computacional.(TORRES, 2001)

A abrangência de uma rede, relaciona-se ao tamanho da área geográfica que ela ocupa e para essa classificação, as redes podem ser: LANs, WLAN, MANs e WAN. A Quadro abaixo, sintetiza os principais tipos e suas características.

[2] https://www.gabrielborba.com.br acesso em 01 de novembro de 2021

Quadro 1 - Classificação das redes quanto a abrangência

Redes quanto a abrangência	Característica
LAN – Local Area Network	Redes pequenas de tamanho de uma sala, casa ou um único prédio.
WLAN – Wireless Local Area Network	Uma LAN com meio de transmissão sem fios.
MAN – Metropolitan Area Network	Abrangência maior, bairros ou cidades inteiras.
WAN – Wide Area Network	Redes de interligação de países ou continentes. A Internet é o maior exemplo de redes WAN

Fonte: Quadro do Autor

A topologia de rede descreve como os despositivos estão organizados nela e as formas mais comuns de organização são descritas no Quadro 2.

Quadro 2 - Classificação das redes quanto a topologia

Topologia	Características
Barramento	Nesta, todos dispositivos compartilham um mesmo cabo disposto verticalmente ou horizontalmente, cujos extremos são bloqueados com um terminador.
Estrela	A topologia do tipo estrela funciona a base da tecnologia mestre-escravo. O dispositivo central é o mestre e os restantes, escravos. Geralmente o mestre é um Switch ou um Hub.
Anel	Na topologia do tipo anel os dispositivos são ligados num mesmo cabo e a sua interligação lembra um círculo.
Híbrida	Topologia usada em grandes redes. É uma espécie de junção de topologia, isto é, uma rede hibrida, pode empregar uma rede do tipo anel e outra do tipo estrela.

Fonte: Quadro do Autor

O método de transmissão está relacionado a arquitetura utilizada para transmissão de dados e assim como em outras classificações, existem vários métodos de transmissão e os mais comuns são:

Quadro 3 - Classificação das redes quando ao método de transmissão

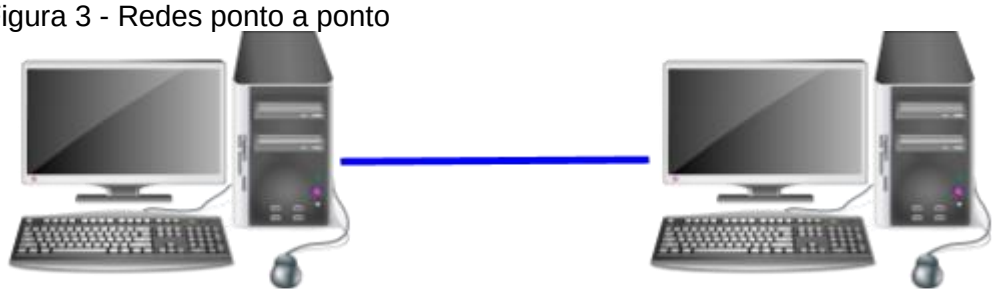
Método	Características
Ethernet (802.3)	É o tipo da arquitetura usado para transmissão de dados em redes locais via cabo.
Wi-fi (802.11)	A semelhança do Ethernet, o Wi-fi oferece suporte para transmissão de dados, mas usando como meio de transmissão o ar.

Fonte: Quadro do Autor

Quanto ao Modelo computacional, existem basicamente duas classificações: Redes ponto-a-ponto e cliente-servidor.

Muitas vezes a necessidade é a de simplesmente interligar um número reduzido de dispositivos como computadores e impressoras, este cenário verificam-se em redes de pequeno porte, como escritórios ou redes caseiras. Quando se conectam computadores com essa finalidade, de modo que um computador funciona, ora como cliente ora como servidor, chama-se a esse estrutura de organização, redes ponto a ponto. Citado por Torres (2014), a figura 3 apresenta essa topologia de rede.

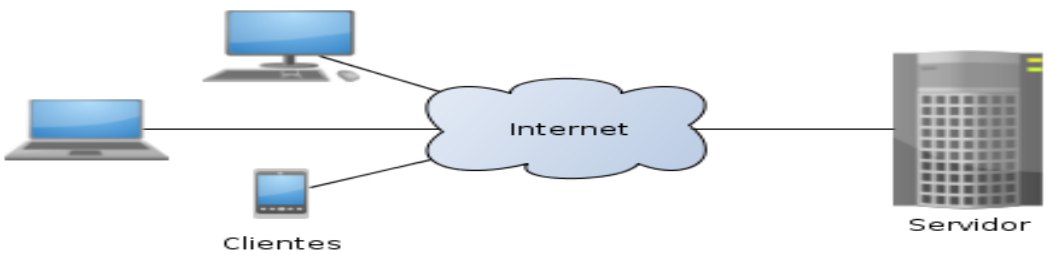
Figura 3 - Redes ponto a ponto



Fonte: Site oficial da Alura[3] (2021)

Por outro lado, redes Cliente/Servidor são o tipo de interconexão de computadores usados em ambientes corporativos mais robustos em que a praticidade e a segurança são requeridas ao mais alto nível. Neste tipo de rede existe um servidor que pode ser um computador de mesa (*desktop)* ou um outro dispositivo projectado com a finalidade de oferecer serviços para as demais estações de trabalho (clientes), esse cenário é visto na figura 4. Dentre as várias vantagens possíveis, o que torna essa arquitetura ideal para serviços em rede, é o facto de que o servidor é simplesmente dedicado ao fornecimento de serviços para os clientes o que possibilita a resposta rápida aos pedidos, o que não acontece na rede ponto a ponto pois a mesma estação que funcionaria como servidor pode estar usando o seu processador para executar outras tarefas, o que afectava o desempenho da rede. Torres(2014)

Figura 4 - Rede Cliente-Servidor



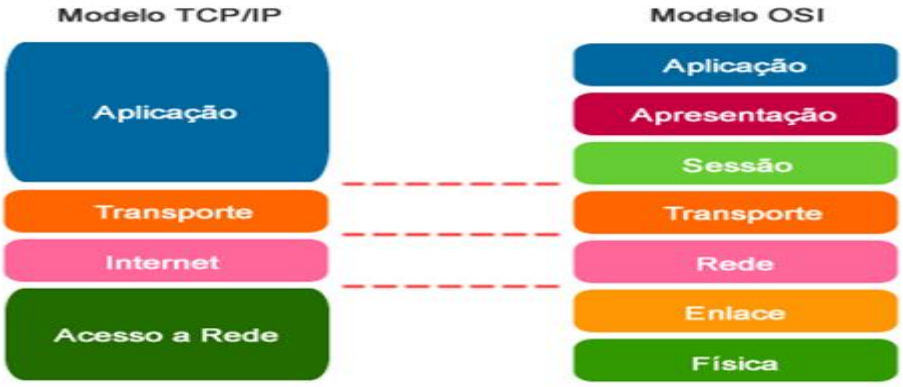
Fonte : Site oficial da wikiwand[4] (2021)

2.3 Modelo OSI e TCP/IP

O modelo OSI (*Open System Interconnection)* é um modelo de referência de sete camadas. Ele foi criado pela ISO e é usado por fabricantes na construção de protocolos e arquitetura de redes. A arquitetura mais conhecida e adoptada pela *Internet* é arquitetura TCP/IP (*Transmission Control Protocol and Internet Protocol*). Ele é um modelo de 4 camadas com funções equivalentes as camadas do modelo OSI. Torres (2001). Essa relação é apresentada na figura 5

[3] https://www.alura.com.br/artigos/conhecendo-algumas-topologias acesso em 01 de novembro de 2021
[4] https://www.wikiwand.com/pt/Modelo-cliente%e2%80%93sevidor acesso em 01 de novembro de 2021

Figura 5 - TCP/IP e Modelo OSI



Fonte: Site oficial do dataRain[5] (2020)

> Nos primeiros anos do surgimento das redes de computadores as soluções (dispositivos de rede) eram proprietárias, isto é, a tecnologia de um fabricante não tinha suporte de comunicação com a tecnologia de outro. Não havia a possibilidade de misturar soluções de diferentes fabricantes. Assim, cada fabricante era responsável por construir todos os dispositivos de uma rede. Com o intuíto de permitir que houvesse o suporte de comunicação entre os diversos fabricantes, a ISO criou o modelo OSI (TORRES, 2001, p. 39).

De Torres (2001), Percebe-se que criação do modelo OSI efectuou um grande salto para o crescimento e discentralização das redes de computadores. Tal avanço, abriu espaço para a competitividade e possibilitou serviços muito mais completos pois desenvolvedores de software e hardware podem se especializar numa única linha de produção. Mas como aponta Forouzan (2007), o modelo OSI não é um protocolo e nem uma arquitetura de rede, ele é uma referência que especifica as regras a serem seguidas por fabricantes de protocolos e arquiteturas de redes. Esse modelo é universalmente usado por possibilitar a interconexão de sistemas distintos.

2.3.1 Descrição das camadas do modelo OSI

A camada de aplicação é a primeira camada do modelo OSI e é a camada mais próxima do usuário, servindo de interface entre o protocolo de rede e aplicação que fez a requesição do serviço.

A camada de apresentação é a camada responsável pela tradução ou conversão dos formatos dos dados recebidos pela camada de aplicação no formato que será usado por todos outros protocolos. Também é responsável pelo processo de codificação e compressão de dados.

A camada de sessão compõe os protocolos que têm a função de estabelecer, gerenciar e finalizar conexões entre aplicações.

[5] https://www.datarain.com.br acesso em novembro de 2021

A camada de transporte é a camada que contém os protocolos que servem de veículos para o transporte dos dados pela rede. Ela faz o uso de porta que permite que diversas aplicações acessem a rede de forma simultânea. Os protocolos mais conhecidos desta camada são o TCP e o UDP.

A camada de rede tem a função de fazer o endereçamento dos pacotes e gerenciamento de rotas de modo a determinar o melhor percurso dos pacotes baseada nas condições de tráfego e prioridade dos percursos

A camada de enlace de dados é uma camada dividida em duas subcamadas LLC (*Logical link control*) e MAC (*Medium access control*) que tratam da realização de endereçamento físico, detecção e correção de erros e controle de fluxo de dados.

LLC – Identifica e encapsula dados provenientes da camada de rede, e controla a verificação de erros e sincronismo.

MAC – Controla como os dispositivos da rede obtém acesso ao meio de transmissão, monitora o uso do cabo (Colisões), trata dos endereços MAC, etc.

A camada física é responsável pela gerência e manipulação do meio físico em que são transmitidos os dados, codificação e decodificação. É também responsável transformar os quadros recebidos da camada de enlace em sinais electricos, sinais luminosos ou electromagnéticos, consoante ao meio de transmissão em uso.

2.4 Protocolos

“Para que os dispositivos que constituem uma rede consigam efectivamente se comunicar e trocar dados entre si, eles precisam de uma liguagem que os permite ”falar”, essa liguaguem em tecnologia de informação é chamada de protocolo”. (Torres, 2001, p.34).

Na Electrónica e na computação, protocolos são regras que permitem a comunicação dos diversos dispositivos de rede. Eles podem ser implementados no hardware ou software. Estes podem ser dos mais variados tipos e apresentarem diversas funções, dentre elas:

Possibilitar a divisão dos dados em pacotes – A divisão de dados em inúmeros pacotes permite que sejam adicionadas informações em cada um deles e por consequência identifiquer-se o destinatário dos dados numa rede complexa.

Optimizar a transmissão – A divisão de dados em pacotes permite com que o meio seja utilizado por mais de um transmissor ao mesmo tempo o que é conhecido como TDM (Time Division Multiplexing).

Propriedades mais específicas, podem ser: detectar conexão física de dispositivos adjacentes, estabelecer ligações, formatar mensagens, detectar perda inesperada de conexão ou terminar uma conexão. Devido a existência de várias propriedades, torna-se difícil generalizar sobre protocolos pois variam no propósito de implementação, uma maneira de agrupá-los, seria através de suas funções nas camadas do modelo TCP/IP.

2.4.1 Protocolos da camada de aplicação

O modelo TCP/IP que é a principal arquitetura da *Internet*, divide-se em quatro camadas justamemte para fazer separação entre os protocolos que oferecem serviços diferentes. Protocolos como HTTP(*Hypertext Transfer Protocol*), FTP(*File Transfer Protocol*), TELNET(*Teletype Network*) e DNS(*Domain Name System*), são exemplos de alguns protocolos que operam na camada de aplicação. Os protocolos que atuam nesta camada, têm a função primordial de oferecer serviços para as aplicações existentes nas máquinas.

2.4.2 Protocolos da camada de transporte

A camada de transporte possui protocolos de funções diversas, como as de negociação da garantia de entrega dos pacotes entre os comunicantes. Os protocolos da camada de transporte mais comuns são o UDP e o TCP. Eles são responsáveis por fragmentar os dados vindos da camada de aplicação em pequenos pacotes e oferecer um meio para que os mesmos possam ser transferidos, com ou sem garantia de chegada ao destino. Também fazem parte dessa camada, alguns protocolos de roteamento e os mais conhecidos são: o RIP (*Routing Information Protocol*), OSPF(*Open shortest Path first*) e BGP (*Border Gateway Protocol*) classificados como protocolos de roteamento interior e exterior.

A divisão dos protocolos de roteamento em protocolos de roteamento interno e externo, deve-se aos interesses envolvidos no roteamento de pacotes. Protocolos de roteamento interno precisam especificar o melhor caminho para os dados, mas os externos para além de melhor caminho precisam de especificar o caminho de menor custo e lidar com politicas de segurança pois operam em redes estrangeiras.

2.4.3 Protocolos da camada de rede

A camada de rede ou camada de Internet, é composta de protocolos que efectuam controle da rede como o *Internet Control Message Protocol* (ICMP) e os protocolos IPv4 e IPv6.

O protocolo IP oferece a capacidade rotear pacotes, identificar o destinatário do pacote dentro de uma rede e identificar a máquinas em uma rede complexa. As duas versões, o IPv4 e IPv6 são o caso de estudo dessa pesquisa e serão abordadas com mais profundidade nas outras secções.

ICMP– é um protocolo da camada de rede responsável por, detectar eventos inesperados, testar redes e outros tipos de gerência da *Internet.* Existem vários tipos de mensagens ICMP e os mais importantes são mostrado na Quadro abaixo.

Quadro 4 - Tipos de mensagens ICMP

Tipo de mensagem	Descrição
Destination Unreachable	Enviado quando o pacote não acha o destino
Time exceeded	Enviado quando TTL=0, representa um loop na rede
Parameter problem	Um campo no cabeçalho possui um valor inválido
Echo Resquest and Reply	Verificam se uma máquina está ativa ou não na rede
Redirect	Usado para informar ao host que teve mudar de rota
Router advertisement/solic	Encontra um roteador próximo

Fonte: Quadro do Autor

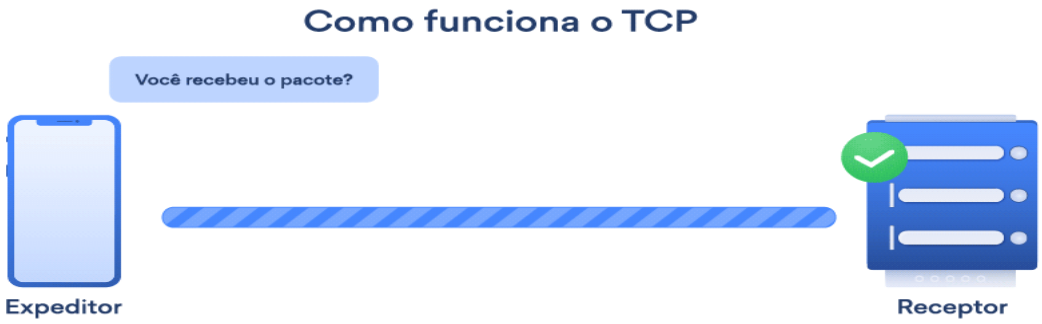
2.4.4 Protocolos da camada física

Todo o computador possui uma placa de rede para que possa se comunicar efectivamente com o restante dos dispositivos. Essas placas possuem características diferentes para cada tipo de meio de transmissão. Os meios de transmissão existentes, são baseados em arquiteturas de redes que usam protocolos capazes de estabelecer, manter e gerenciar os pacotes que trafegam na rede, esses são os protocolos da camada física. Os protocolos mais difundidos dessa camada são: ATM (*Ansynchronous Transfer Mode*), Frame Relay, FDDI(*Fiber Distributed Data Interface*), Token ring e outros, mas dentre estes, os mais usados são o ethernet (IEEE 802.3) e wi-fi (IEEE 802.11).

2.5 Protocolo TCP

Todo o pacote que trafega numa rede, precisa de um protocolo de transporte para que chegue ao seu destino. Os protocolos da camada de transporte são responsáveis por fornecer o serviço de transporte desses pacotes do host origem até o destino. Para além de servirem como veículo para datagramas da *Internet,* os protocolos de transporte são responsáveis por especificar os serviços a serem acessados no servidor. O caso prático dessa funcionalidade verifica-se quando um servidor possui vários serviços como os de *e-mail*, serviços de HTTP e serviços de FTP. Assim, quando um processo é iniciado no host origem, esse processo tem de especificar com que serviço deseja se comunicar dos disponíveis no servidor. Os protocolos com essa finalidade são: *User Datagram Protocol* (UDP) e o *Transmission control Protocol* (TCP)

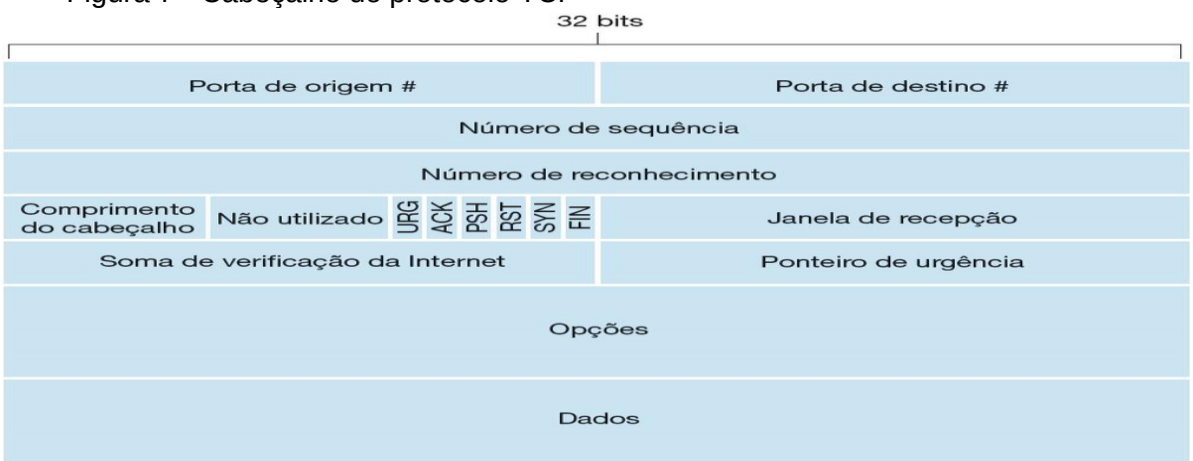
Figura 6 - Funcionamento do protocolo TCP



Fonte: site oficial da NordVPN[6] (2020)

O TCP tem a função de transmitir dados e garantir que eles sejam recebidos e verificar se foram enviados na sequência correcta. No processo de envio usando esse protocolo, o host origem espera mensagens de confirmação de recebimento dos pacotes, esse processo pode ser visto na figura 6. No caso de não confirmação dos pacotes, eles são retransmitidos, garantindo que nada se perca. No início da troca de dados entre os nós, o protocolo TCP estabelece uma conexão entre os comunicantes, por este motivo, diz-se que o protocolo TCP é orientado a conexão pois TCP garante uma comunicação fiável uma vez que todos os pacotes recebidos são confirmados ao remitente.

Figura 7 - Cabeçalho do protocolo TCP



Fonte: Fábio dos Reis[7] (2015)

Os campos *porta de origem e porta de destino* da figura 7, especificam os processos envolvidos numa comunição entre dois hosts. Algumas portas mais conhecidas são 80 [HTTP], 21 [FTP]. Os campos *número de sequência* e *número de*

[6] https://www.nordvpn.com/ acesso em novembro de 2021
[7] https://www.bosontreinamentos.com/ acesso em novembro de 2021

reconhecimento, juntos servem para indentificar uma sequência contígua de pacotes. O número de sequência identifica um conjuto de bytes por um único valor e o número de reconhecimento representa a quantidade de bytes recebidos pelo destinatário. *Comprimento do cabeçalho* representa o tamanho do cabeçalho TCP em palavras de 32bits. *O Campo reservado* é para o uso futuro. Consiste atualmente na sequência 000. O *tamanho da Janela* indica o número de bytes que o transmissor do segmento quer enviar ao host de destino, em cada transmissão. O campo *Checksum* é usado para verificação de erros do cabeçalho e dos dados transmitidos. O campo *Opções* representa informações não cobertas pelos demais campos do cabeçalho TCP.

2.6 Protocolo UDP

Quando no processo de transmissão de dados a ordem e a garantia de que os dados chegarão ao host destino não é fundamental, usa-se o protocolo UDP.

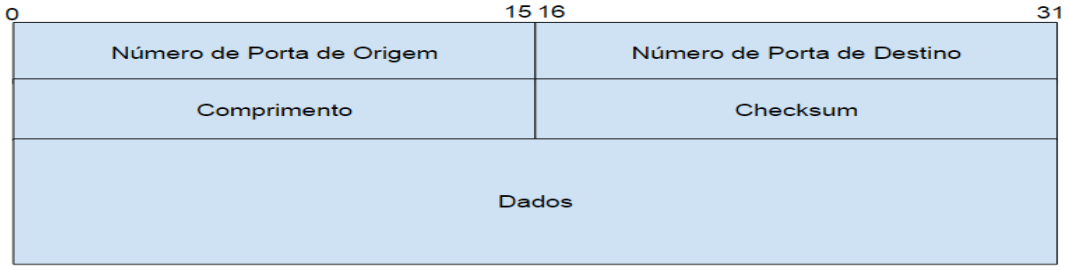
Figura 8 - Funcionamento do protocolo UDP

Fonte: site oficial da NordVPN (2020)

No envio de dados entre estações da *Internet*, o UDP não garante que os dados serão recebidos, nem se estão em ordem correcta. Ao enviar dados na rede, o UDP não estabelece nenhuma conexão, os dados são enviados sem se estabelecer um acordo entre os nós. Diz-se que o protocolo UDP não é orientado a conexão.

Por não estabelecer uma coneção no início e por não garantir a integridade dos pacotes, o UDP é tido como não confiável mas em contra-partida ele apresenta um cabeçalho mais leve o que o torna muito mais rápido que o TCP. O cabeçalho UDP pode ser visto na figura 9.

Figura 9 - Cabeçalho do UDP



Fonte: Fábio dos Reis (2015)

Número de porta de origem – Porta lógica que identifica o protocolo de aplicação que envia os dados. As portas usadas por uma aplicação em UDP, são diferentes das usadas pelas mesmas aplicações em TCP.

Número de porta de destino – Porta lógica que identifica a aplicação que recebe os dados.

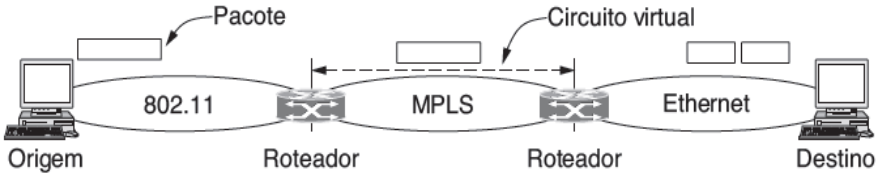
Comprimento – Especifica em bytes o comprimento do cabeçalho mais o dados carregados. O comprimento mínimo é de 8bytes que é o comprimento do cabeçalho com a área de dados vazia e o máximo é de 65 535bytes.

Checksum **–** Usado para verificação de erros do cabeçalho e dos dados transmitidos.

2.7 Protocolo IP

A figura 10 apresenta um problema típico da *Internet,* chamado **heterogeneidade de redes.** As redes mudiais que formam a estrutura da *Internet* são muitas vezes diferentes entre si **(**redes wi-fi, ethernet, ATM e outros**).** Nesta figura, um pacote enviado da rede origem (802.11 - Wifi) pretende alcançar a rede *ethernet* mas deve passar pela rede MPLS (Multi Protocol Label Switching) primeiramente. A dificuldade do encaminhamento de um pacote da rede 1 para a rede 3 observa-se ao nível da camada física porque cada tipo de rede oferece um tipo de acesso ao meio e por consequência quadros de diferentes estruturas. Isso causa incompatibilidade e pode originar perda de dados porque uma rede MPLS não pode transportar tráfego de redes *ethernet* e mesmo que seja possível, por exemplo, especificar o endereço de destino de um host da rede 802.11 no cabeçalho *ethernet*, os quadros passariam de uma rede orientada a conexões a uma rede não orientada a conexões, isso causaria a necessidade de se configurar uma nova conexão sem aviso prêvio mas o fim último seria a perda de pacotes. Tenenbaum e Wetherall (2017)

Figura 10 - cenário de heterogeinidade de redes

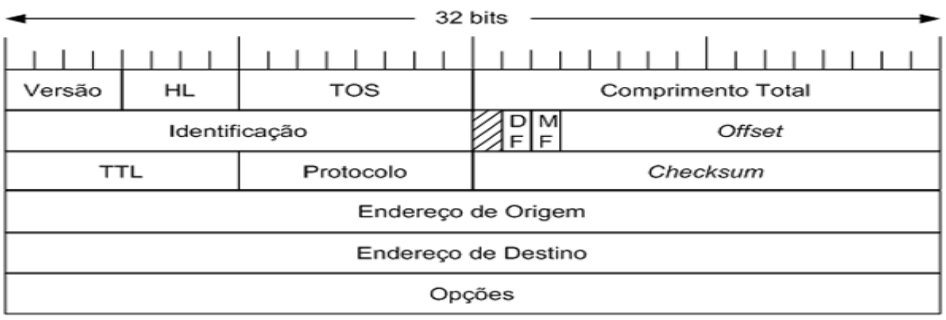


Fonte: Tenenbaum e Wetherall (2017)

Para Tenenbaum e Wetherall (2017), a heterogeneidade das redes de computadores é um mal necessário. Segundo eles, o valor de uma rede torna-se muito mais cara a medida em que ela se expande. Assim, redes gigantes são muito mais valiosas que redes pequenas e portanto, a combinação delas torna-se fulcral. Porque as redes heterogênias devem co-existir, torna-se necessário uma solução para que as diversas redes seja interconectadas. Essa solução é provida através do IP**.**

O IP – É um protocolo de comunicação da camada de *Internet* do modelo TCP/IP, usado por todas as máquinas em redes de computadores para efeitos de encaminhamento de dados. O IP oferece um formato de pacote universal que todos os dispositivos de redes reconhecem. O pacote IP tem uma parte fixa de 20 bytes e uma parte opcional que pode ter até 40 bytes. A figura 16 mostra o formato do cabeçalho IP

Figura 11 - Cabeçalho do protocolo IP



Fonte: site oficial da Techtudo[8] (2021)

O campo versão possui 4 bits e é designado para indicar a versão do protocolo que está em uso, versão 4 ou 6. Por ter um formato variável, o datagrama IP possui o campo HL (*Header Lenght*) que especifica o tamanho atual do cabeçalho em palavras de 32 bits. Quando nenhuma opção é usada, o HL recebe o valor de 5 que simbolizam as 5 linhas restantes no cabeçalho IP. O campo TOS (*Type of Service*) é utilizado para distiguir entre diferentes classes de serviço (serviços com menos ou mais prioridade). O comprimento total especifica o tamanho total de todo o pacote IP incluindo os dados

[8] https://www.techtudo.com.br acesso em novembro de 2021

e o cabeçalho e tem como tamanho máximo, 65 536 bytes. O campo identificação é necessário para os casos em que um datagrama sofre diversas fragmentações para que possa chegar ao seu destino, esse campo oferece uma identificação que permite o destino identificar fragmentos pertecentes ao mesmo pacote. O bit a tracejado não tem utlidade nenhuma em IPv4. Os bits DF(*Don't fragment*) e MF *(more fragment)*, quando activos, indicam a existência ou não de mais fragmentos a caminho para serem remontados com os outros já recebidos. O campo *offset* (deslocamento em português) é usado em conjunto com as flags e o ID para a remontagem do datagrama. Por possuir 13 bits, ela permite 8192 fragmentos todos de 8 bytes e 8192*8=65 536 bytes. No caso de *ethernet* cada deslocamento deve ser múltiplo de 185, excepto o último, sendo que o primeiro fragmento é sempre 0. O campo TTL representa um contador que decrementa o seu valor a cada salto que dá. Ao atingir o valor 0, ele envia uma mensagem ICMP (*Internet Control Message Protocol*) ao remetente. Esse campo é importante porque evita que pacotes entrem num loop infinito na rede e a congestionem. O campo protocolo especifica qual processo de nível superior requesitou o serviço. Os endereços de origem e de destino comportam os endereços do remitente e do destinatário respectivamente. Tenenbaum e Wetherall (2017)

2.7.1 Endereçamento Ipv4

Endereço IP

O endereço IPv4 é um endereço de 32 bits, composto por uma parte de rede e outra de máquina, ambos de tamanho variáveis chamadas de classes de endereço IP. As classes IPs podem ser vistos na figura 12 . A parte da rede é sempre fixa para todos os hosts de uma mesma rede e ela é chamada de **prefixo.** O endereço IP é dividido em quatro octetos e cada parte é escrita na forma decimal e separada por um ponto do outro. Os valores de cada octeto podem variar de 0 a 255. O endereço 192.168.145.68 representa um endereço aleatório que pode identificar uma máquina na rede.

Figura 12 - Classes IP

Fonte: Repositório Docplayer[9] (2021)

O tamanho do prefixo de rede quando escrito na forma de 1's é dita **máscara de sub-rede.** A máscara de sub-rede ao ser submetida a AND lógico com um endereço IP de host, retorna o endereço de rede. Essa operação pode ser vista na equação 1.

Dado o endereço IP: 217.114.22.150 (Classe C)

Máscara de sub-rede: 255.255.255.0

	11011001.01110010.00010110.10010110	= (217.114.22.150)	
AND	11111111.11111111.11111111.00000000	= (255.255.255.0)	(1)
=	11011001.01110010.00010110.00000000	= (217.114.22.0)	

O resultado de uma operação AND entre endereço de host e a máscara de sub-rede, sempre resulta no endereço de rede e este nunca deve ser atribuído a nenhuma máquina pois é usado para efeitos de roteamento.

O endereçamento em classes tem vantagens e desvantagens. A maior vantagem é que ela possibilita aos roteadores encaminhar pacotes só com base no prefixo de um endereço IP a outra que permite uma melhor racionalização dos endereços, para redes de pequeno e grande porte. Isso ajuda a reduzir o esforço dos roteadores uma vez que não há a necessidade de armazenar todos o endereços da *Internet*, simplesmente os endereços das interfaces dos roteadores, isso ajuda a reduzir o tamanho das Quadros do roteamento. Porém, a facto dos endereços de rede serem fixos, inviabiliza o suporte a mobilidade, pois ao se deslocar de uma rede, um host perde a seu IP e consequentimente a sua conexão. Ao ser introduzido em uma nova rede, o host precisa iniciar todo o processo de aquisição de endereço na sua nova casa mas com todos os serviços em andamento perdidos. Outro ponto fraco do endereçamento por classes é o disperdício de endereços quando se precisa de uma rede pequena como uma rede doméstica de 15 computadores, por exmplo. A Quadro 3 mostra o disperdício existente em cada classe para esse cenário. A solução para esse problema é a divisão de redes maiores em redes menores chamadas de **sub-redes**.

Quadro 5 - Disperdício por classe de IP

Classes	Quantidade de endereços	Endereços disperdiçados
A	$\mathbf{2^{24} - 2 = 16.777.214}$	$\mathbf{16.777.214 - 15 = 16.777.199}$
B	$\mathbf{2^{16} - 2 = 65.534}$	$\mathbf{65.534 - 15 = 65.519}$
C	$\mathbf{2^{8} - 2 = 254}$	$\mathbf{254 - 15 = 239}$

[9] https://www.docplayer.com.br acesso em novembro de 2021

Fonte: Quadro do Autor

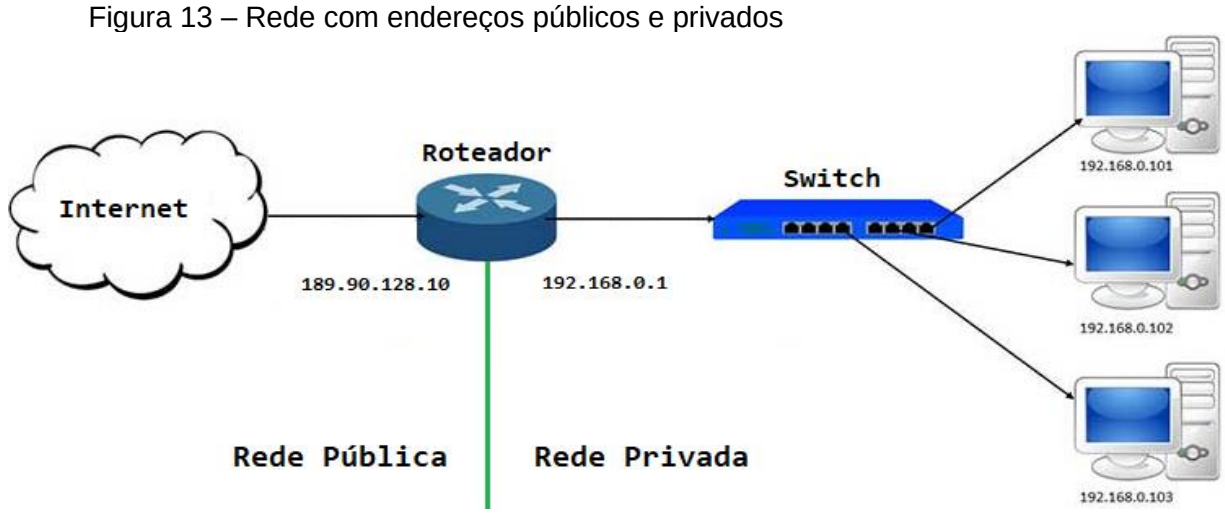
2.7.2 Sub-redes

As classes A,B,C,D e E são sub-redes padrão do endereçamento IP. Quando se deseja criar uma rede diferente de até no máximo 25 hosts, por exemplo, torna-se inviável usar umas das classes padronizadas devido a quantidade de endereços desperdiçados nela. A razão principal para se criar sub-redes é o da possibilidade de criar uma rede de dimensões variadas de modo a evitar o disperdício de endereços IPs. Uma sub-rede é uma subdivisão lógica de uma rede IP em várias outras menores. Realizar essa subdivisão permite diminuir o tráfego da rede, simplificar a administração e aumentar a performace da mesma.

As sub-redes utilizam o conceito de máscaras para efectuar essa divisão. Uma máscara tem função de distiguir a porção de rede e de host em um endereço IP. Ela é semelhante em sua estrutura ao IPv4. A parte dos bits constituídos pelo valor “1” representam as parcelas do endereço IP que serão vistos como endereço de rede e os bits “0” representam as parcelas do endereço do host. Assim, chama-se máscara de sub-rede, qualquer endereço que quando aplicada uma operação lógica AND em relação a um endereço IP de host, retorna o endereço de rede (Prefixo de roteamento).

2.7.3 Tipos de endereços

Figura 13 – Rede com endereços públicos e privados



Fonte: Rennan Cockles[10] (2021)

A ideia de uma rede de computadores acenta-se na base de que não podem existir dois ou mais computadores com o mesmo endereço IP. Quando dois dispositivos por algum motivo recebem o mesmo endereço, eles entram em um conflito, designado

[10] https://www.r3ck0.medium.com/ acesso em dezembro de 2021

conflito de IP. Embora esse modelo seja fundamental para o conceito de conectividade ponto a ponto, na *Internet* esse princípio não se verifica. Devido ao IP disponibilizar um pouco mais de 4 bilhões de endereços, essa quantidade torna-se insuficiente para dar suporte a realidade atual da *Internet* que comporta um pouco mais de 5 bilhões de dispositivos. sendo assim, os endereços devem ser reutilizados. A reutilização de endereços é feita através de uma técnica de conversão de endereços designada NAT. Esta possibilita com que uma rede inteira seja identificada externamente por um único endereço IP, implicando a existência de dois tipos de IPs, os internos(privados) e externos(públicos). Esse cenário pode ser visto na figura 13.

Endereço privado

Os endereços privados são endereços usados dentro de redes locais, sendo que os hosts que as usam são separados da *Internet* por roteadores ou outros dispositivos que efetuem o NAT. Os dispositivos de redes locais não podem ser atribuídos qualquer endereço uma vez que os endereços privados não são roteáveis nem visíveis na rede pública, isso permite que diferentes redes locais usem os mesmos endereços IPs. Os endereços abaixo são reservados pela IANA(*Internet Assigned Numbers Authority*) para desempenharem essa função.

- 10.0.0.0 até 10.255.255.255 (Classe A)
- 172.16.0.0 até 172.31.255.255 (Classe B)
- 192.168.0.0 até 192.168.255.255 (Classe C)

Endereços públicos

Os dispositivos locais não podem acessar a *Internet* com seus IPs privados pois esses não são reconhecidos na *Internet* mas podem comunicar-se entre si dentro da rede. Para um dispositivo terminal ser capaz de aceder a *Internet* ele precisa do auxilio de um IP público, isso sugere que ele tenha dois endereços. Um privado que o identifica na rede privada e outro público que o identifica na *Internet* (Este último é o que identifica o roteador da rede privada em causa). Para que seja possível essa camuflagem é necessário um dispositivo de rede que implemente o NAT.

2.8 Constrangimentos do IPv4

2.8.1 Limitações no desenvolvimento da Internet

> Na época do nascimento da Internet, ela era apenas uma rede de pesquisa conectando Universidades, algumas empresas e bases militares. Ninguém percebeu que a Internet se tornava um sistema de

> comunicação de mercado em massa, competindo com a rede telefônica. Na época, alguém sem dúvida disse: “Os Estados Unidos têm cerca de 2 mil faculdades e universidades. Mesmo que todas elas se conectem à Internet e muitas outras universidades em outros países também se juntem, nunca chegaremos aos 16 mil, pois não existem tantas universidades no mundo inteiro.
> (TENENBAUM et WETHERALL, 2017, p. 283).

Para Moreiras e al (2015) uma das deficiências mais apontadas do IPv4 foi o espaço de endereçamento baseado num valor inteiro de 32 bits, que é tipicamente representado por quatro octetos em decimal. Para contornar essa deficiência, inúmeras soluções paliativas foram propostas e adotadas, como por exemplo o NAT e o *Classless InterDomain Routing* (CIDR).

Como nota Torres (2014), essa escassez não é nova para as autoridades da *Internet* e já desde 1995, técnicas para atrasar o esgotamento definitivo, foram adoptados. Entre essas técnicas estava o NAT. O problema é que mesmo tais soluções, viriam a apresentar problemas futuros. Embora o NAT, seja referido muitas vezes como uma solução, pois foi criado para adiar a escassez dos endereços IPv4, ele fere o modelo de conectividade ponto a ponto da *Internet*.

Para Moreiras e al (2015) o modelo de conectividade ponto a ponto impõem que um host deva ser capaz de enviar pacotes para qualquer outro a qualquer momento. Esse problema acontece porque o NAT é configurado por pacotes de saída. Na prática isso significa que um cliente pode acessar um servidor remotamente, mas um host remoto teria dificuldades para acessar um servidor numa rede caseira. Para contornar esse tipo de problemas é necessário o uso de técnicas especiais ou de travessia do NAT. O uso dessas técnicas, muitas vezes leva a problemas de segurança, expondo o cliente a ataques na *Internet*.

Por outro lado, (TENENBAUM e Wetherall, 2017) afirmam que, quando o NAT apresenta falhas de conectividade, todas as conexões TCP em andamento são destruídas, mas isso não acontece no caso de uso simples de roteadores sem a sua implementação. No caso de um pane nos roteadores, eles entram em *timeout* para que dentro de segundos as transmissões sejam reiníciadas para os pacotes não confirmados.

Um outro obstáculo oferecido pelo NAT, mais precisamente pela sua variante *carrier grande* NAT (CGNAT – NAT usado nas provedoras de Internet), encontra-se no campo de resolução de crimes cibernéticos. Há ainda, outros problemas como os

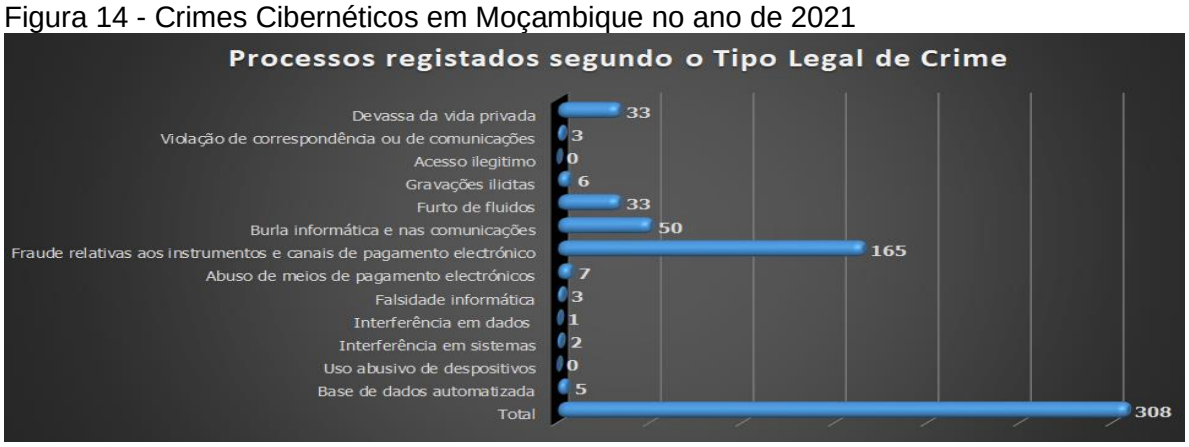
apontados por Morais e al (2015), que mostram que o CGNAT aumenta o custo de uma rede, pois acrescenta equipamentos caros e complexos e que um servidor que esteja operando sob uma rede que incorpora o CGNAT, terá todos seus serviços paralisados a menos que encontre mecanismos de burlar o sistema de sigurança do CGNAT. Isso inviabiliza o IoT (*Internet of Things*) por exemplo, pois nenhum dispositivo que funciona como um servidor pode operar dentro de um NAT, uma vez que, os servidores que implementem os mesmos serviços não podem utilizar diferentes números de porta.

.No lado de resoluções de crimes cibernéticos, o relatório anual de segurança interna de Portugal (2020) apontou dificuldades nas investigações criminais devido ao CGNAT como um dos maiores problemas para investigação de crimes cibernéticos.

> A legislação referente à retenção de dados é um obstáculo à preservação da prova, neste tipo de investigações. A disseminação pelos *Internet Service Provider* (ISP) nacionais da tecnologia Carrier Grade Network Address Translation (CGNAT), criou um relevante constragimento no processo de indentificação de autores de crimes em território nacional e tem sido um obstáculo às investigações. (SSI, 2020, p. 67)

O crime cibernético é uma realidade que preocupa os governos. No atual contexto da pandemia da Covid-19, por exemplo, a concentração de serviços na *Internet* tem aumentado e infelizmente esse crescimento é proporcional ao crime no ciberespaço, só no ano de 2021 o Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC) apresentou 308 casos de crime cibernéticos de vários tipos como mostrado na figura abaixo.

Figura 14 - Crimes Cibernéticos em Moçambique no ano de 2021



Fonte: site oficial do Intituto nacional de Tecnologias de informação e comunicação[11] (2021)

Para além dos crimes direcionados, existem ainda os não direcionados como os *phishings, spams e* outros tipos de *malwares.* Segundo dados levantados pelo Instituto

[11] https://www.Intic.gov.mz/?p=1106 acesso em dezembro de 2021

nacional do governo electrónico (INAGE) de Moçambique (Apud Cepik e Marcelino, 2021), só no ano de 2018 Moçambique registrou mais de 1.5 milhões de ataques por mês. No entanto esses ataques não são simplesmente direcionados a pessoas individuais, afectam também á empresas e instituições de ensino pois muitas vezes sofrem ataques DDoS (*distributed denial-of-service*), oque causa prejuizos de bilhões de dólares a várias delas. Segundo Cepik e Marcelino (2021).

Muitos dos problemas apresentados, relacionam-se a segurança no IPv4, este não possui nenhum mecanismo de autenticação para efeitos de segurança o que o torna vulnerável a ataques perpetuados por agentes de ameaça na *Internet*.

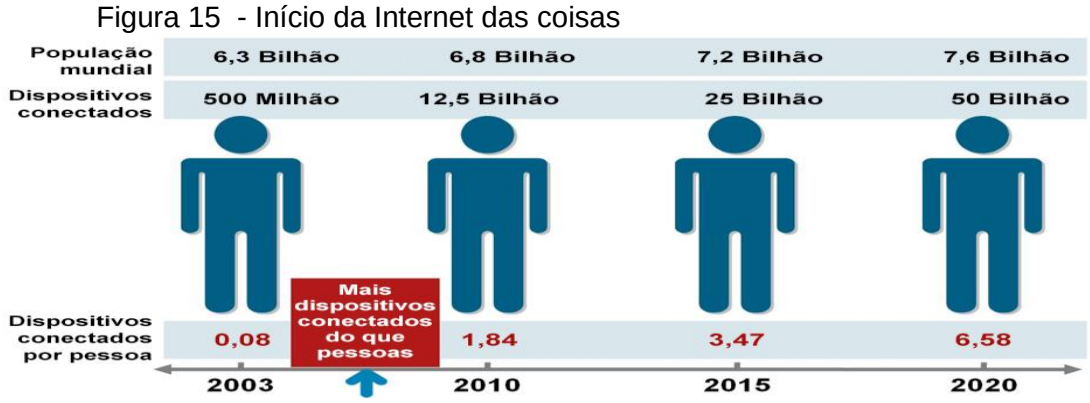
2.8.2 IPv4 e a Internet das coisas (IoT)

Segundo Pimparel (2017, p. 1), "O termo "*Internet* das Coisas" foi proposto em 1999 por Kevin Ashton do *Massachussets Institute of Technology* (MIT) juntamente com sua equipe, tendo escrito 10 anos depois, um artigo para o RFID Journal, denominado " *Internet* das coisas"".

Para Rocha et al (2017, p. 10) "*Internet* das Coisas, é um advento da tecnologia e da própria *Internet* que, através da conexão de dispositivos físicos, torna possível acessar dados de sensores e controlar o mundo físico à distância, a qualquer hora e lugar".

De acordo com a Cisco (2011), a *Internet* das coisas iniciou-se no momento em que mais "Coisas" foram conectados a *Internet* do que pessoas. Esse evento aconteceu entre o ano de 2009 à 2010 como mostra a figura abaixo.

Figura 15 - Início da Internet das coisas



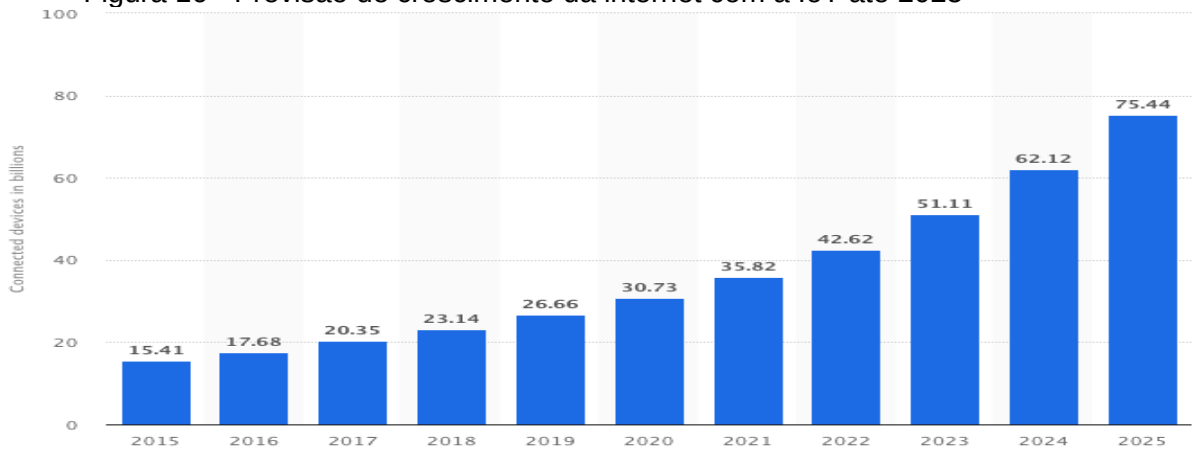
Fonte: EVANS (2011, p. 3)

O mundo caminha a passos largos para mais uma evolução tecnológica na área de tecnologias de informação. Por muito tempo a *Internet* foi a base de serviços de coorporações e áreas acadêmicas. Porém, com a *Internet* das coisas, vários dispositivos

serão interconectados a ela, possibilitando com que outros ramos como os da medicina, industria e automação residencial façam parte.

O objectivo é permitir que todos os ramos sejam ligados a *Internet.* O crescimento nessas dimensões demandará por parte da *Internet,* vários recursos, entre eles a quantidade de endereços IP. O gráfico abaixo prevê que até 2025 existirão próximo de 75 bilhões de dispositivos conectados a *Internet*.

Figura 16 - Previsão de crescimento da internet com a IoT até 2025



Fonte: Página oficial da Statista[12] (2021)

Para Rocha et al (2017), o IPv4 é incapaz de dar suporte ao desenvolvimento da *Internet* das coisas pelo facto de que para este é crucial que os dispositivos funcionem como servidores, implicando o uso endereços públicos o que não acontece com o IPv4 por utilizar o NAT.

O uso do NAT limita o desenvolvimento da *Internet* das coisas, pois nele, os endereços não são exclusivos e há necessidade de auxiliar os pacotes através do encaminhamento de portas. Basicamente um usuário residencial deveria configurar seu roteador para contornar o NAT, fazendo encaminhamento de porta para cada dispositivo que esteja na *De-militarized zone* (DMZ). O problema dessas configurações é que servidores com mesmas funções precisam de mesmo número de porta o que dificulta o encaminhamento do pacote uma vez que usam o mesmo endereço IP exterior. Assim, dois servidores que implemetem o mesmo serviço numa rede, não podem ser distiguidos se estiverem usando endereços privados.

Para Moreiras e al (2015) a consequência de não adoptar o IPv6 o mais rápido possível, resultará numa rede ramificada, em que algumas empresas e instituições

[12] https://www.statista.com/ acesso em dezembro de 2021

estejam a utilizar o IPv6 e outras a utilizar técnicas de CGNAT, uma vez que todos os serviços e dispositivos aplicados recentemente vem com o IPv6 como o protocolo padrão.

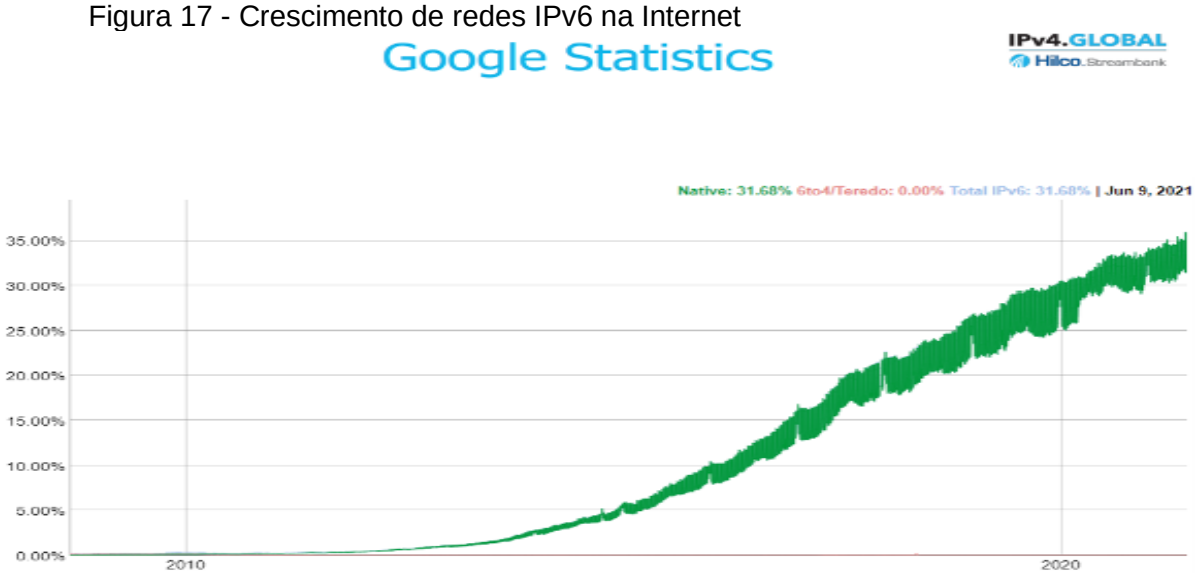
Como faz menção (BARRETO, 2015), para ultrapassar esta diferença, os computadores podem utilizar técnicas que combinem os dois tipos de endereços IP, técnica conhecida como pilha dupla (*dual stack*). O uso da pilha dupla não resolve o problema de esgotamento de endereços mas permite evitar que a *Internet* seja ramificada enquanto não se implementa o IPv6 por completo..

2.9 Endereçamento IPv6

> O problema de esgotar os endereços IP não é um problema teórico que poderia ocorrer em algum momento no futuro distante. Ele está acontecendo aqui e agora. A solução a longo prazo é a Internet inteira migrar para o IPv6, que tem endereços de 128 bits. Essa transição está ocorrendo com lentidão e a conclusão do processo demorará muitos anos (TENENBAUM et WETHERALL, 2017, p. 283).

O reduzido tamanho de seu predecessor, IPv4, fez a transição para o IPv6 inevitável. Os números do *Google* revelam uma taxa de adoção do IPv6 de forma exponencial ou dobrando a cada nove meses como mostra a figura 17.

Figura 17 - Crescimento de redes IPv6 na Internet



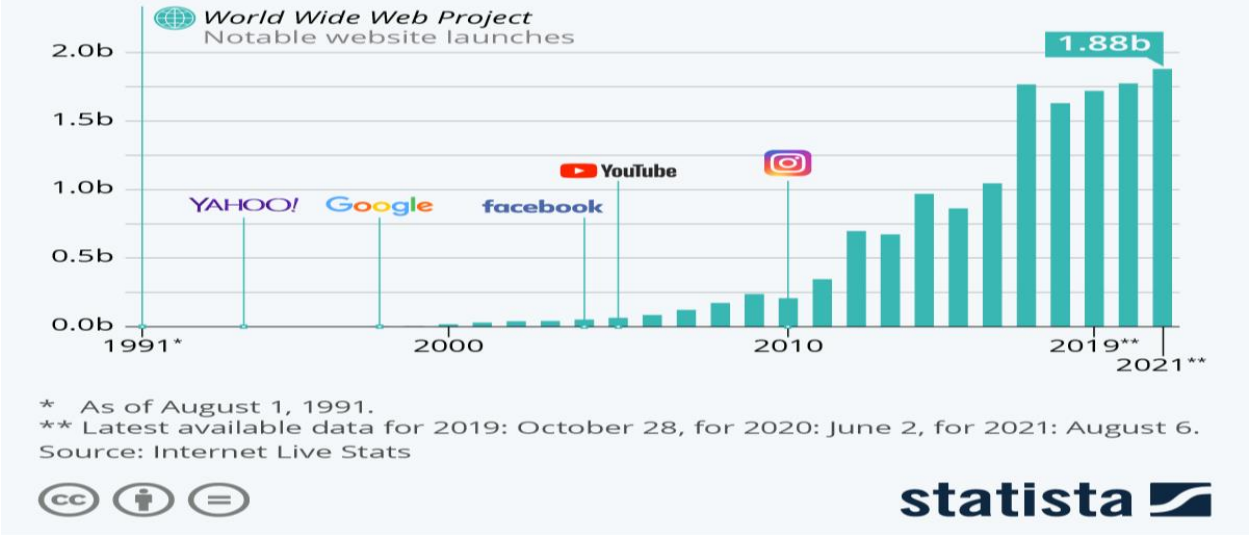
Fonte: Página de estatística de implantação do IPv6 da Google[13] (2021)

Segundo (STATISTA, 2021) até 06 de agosto de 2021, a *Internet* comportava um pouco mais de 1.88 bilhões de sites como aponta a figura 18. Dados mais recentes

[13] https://www.google.com/intl/pt-br/ipv6/statistics.html acesso em dezembro de 2021

revelam o marco de 1.92 Bilhões de websites em 29 de Dezembro segundo a *Internet Live Stats*.

Figura 18 – Número de websites na *Internet* até 2021



Fonte: Página oficial da Statista[14] (2021)

O IPv4 por ter 32 bits oferece um pouco mais de 4 bilhões de endereços, mas essa quantidade de endereços embora pareça gigante, não é. Com objectivo evitar uma eventual escassez de endereços IPs a IETF criou o IPv6. O IPv6 não é um desejo nem o endereço do futuro, ele já está em funcionamento e é usado em conjunto com o IPv4, aos poucos ela vai substituindo a versão antiga. O IPv6 é uma boa opção porque dificilmente se esgotaria o número de IP's ofereridos por este. Diferente do IPv4 que na sua constituição apresenta 32 bits, o IPv6 possui 128 bits consequentemente terá $2^{128} = 340282366920938463463374607431768211456 \approx 340x\ 10^{36}\ undecilhão$ endereços.

2.9.1 Estrutura do Endereço IPv6

Um endereço aleatório Ipv6 tem a seguinte estrutura: "2001:0db8:0000:1111:0000:0000:0000:0200", este integra números e letras com numeração hexadecimal contendo 8 blocos. Cada bloco de separação apresenta 4 caracteres, sendo separados por dois pontos (:). Diferente do IPv4, o IPv6 possui outras maneiras de representação dos seus endereços, por omissão de zeros a esquerda ou representação de dois pontos duplos. No primeiro, um bloco "0020" é equivalente a "20" e um "000a" à "a". A outra forma, consiste em suprimir as cadeias consecutivas de zeros. Essa supressão, deve ser usada uma vez em cada endereço, de modo a evitar possíveis

[14] https://www.statista.com/chart/number-of-websites-online/ acesso em dezembro de 2021

ambiguidades pois supressões consecutivas podem tornar a recuperação do endereço real impossível.

O endereço aleatório descrito acima, por exemplo, teria o seguinte aspecto: “2001:0db8:0000:1111::0200”, reduzindo significativamente o tamanho da representação do endereço.

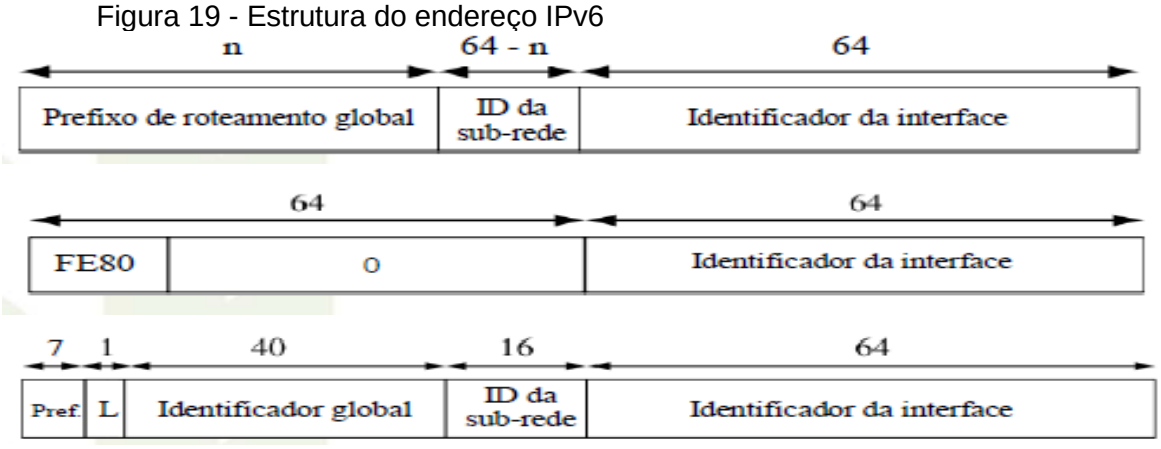
2.9.2 Tipos de endereço Ipv6

Em IPv6 existem três tipos de endereços principais, relativos ao modo de comunicação entre os hosts. Esses endereços são: Unicast, *Multicast* e Anycast.

a) Endereços Unicast

São responsáveis por identificar exclusivamente uma interface em um dispositivo habilitado para Ipv6. Diferente do IPv4, o IPv6 possibilita que cada interface tenha um ou mais endereços por máquina. Por possuirem endereços globalmente roteáveis na *Internet*, viabilizam a conexão ponto a ponto que foi quebrado pelo NAT. Santos et al (2010). Os endereços *Unicast* são divididos em três tipos, descritos abaixo e as suas estruturas apresentadas na figura 19.

Figura 19 - Estrutura do endereço IPv6



Fonte: Santos et al (2010)

- **Endereço Unicast Global (GUA) –** Endereço unicast é equivalente a um endereço Ipv4 público. São globalemente roteáveis e exclusivos na *Internet*. Atualmente todos os endereços atribuídos dessa familia têm o prefixo 2000::/3 (valores em binário que iniciam com 001), esse prefixo equivale à faixa de “2000::” até “3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff”. Santos et al (2010)
- **Endereço de Link Local (LLA) –** Endereço Unicast obrigatório para todos os dispositivos habilitados para Ipv6, é usado para se comunicar com outros

dispositivos no mesmo link local. Os LLAs não são roteáveis e estão confinados a um único link. Esses endereços têm o prefixo FE80::/10. Santos et al (2010)

- **Endereço Único Local (ULA) –** Similares aos endereços privados Ipv4. São usados dentro de uma rede privada e não são roteáveis na *Internet*. Esses endereços têm o prefixos que variam de Fc00::/7 a fdff::/7. O bloco Fc00::/7 foi mais tarde dividido “fc00::/8” e “fd00::/8”. Assim, se o bit “L” da sua estrutura for 1 (“fd00::/8), os endereços podem ser atribuídos localmente, mas se o “L” tiver seu valor setado para 0 (“fc00::/8”) então eles são atribuídos pelas autoridades da *Internet*. Santos et al (2010)

Para além dos endereços usados para comunicação host para host, existem também os endereços especiais, usados para situações especificas. Existem dois tipos de endereços especiais e são descritos abaixo:

- **Endereço loopback –** Tem a mesma função do endereço Loopback do Ipv4 e para Ipv6 o endereço é: 0::1/128. Santos et al (2010)
- **Endereço IPv4 – Mapeado –** são endereços Ipv6 com a possibilidade de camuflagem para endereços Ipv4, esses endereços são usados para fazer a tradução de endereços ipv4 para ipv6 e vice-versa. São representados por “0:0:0:0:0:FFFF<IPv4>. Santos et al (2010)

b) Endereços *Multicast*

Um endereço Ipv6 *multicast* é usado para enviar um único pacote Ipv6 para vários destinos. São usados em aplicações de comunicação de natureza “um para muitos”, como por exemplo serviços de teleconferência, serviços de monitoramento distribuído, entre outros. Os principais endereços *multicast* são descritos na Quadro 7. Eles iniciam em “FF00::/8”, e não podem ser usados como endereço de origem, justamente porque representam um grupo de máquinas que irá receber o pacote *multicast*. Em IPv6, o broadcast é substituído pelo *multicast* de todos os nós (”FF02::1”). Quando um host utiliza esse endereço, somente os dispositivos terminais(PCs) têm a capacidade de “escutar” esse tipo de mensagem, isto é, servidores e roteadores não podem. Para o grupo de roteadores por exemplo, é usado o endereço de todos os roteadores (“FF02::2”). O uso típico do endereço “FF02::2” acontece quando os hosts fazem o pedido do **anúncio do roteador (RA)** através de uma mensagem de **solicitação do roteador (RS)** na tentativa de adquirir prefixos de rede, endereços DNS e muito mais. Santos et al (2010)

Quadro 6 - Tipos de endereço de *multicast*

Endereços	Descrição
FF02::1	Todos os hosts
FF02::2	Todos os roteadores do link
FF01::5	Protocolo OSPFv3 (roteadores)
FF01::1:2	Sevidores DHCP

Fonte: Quadro do Autor

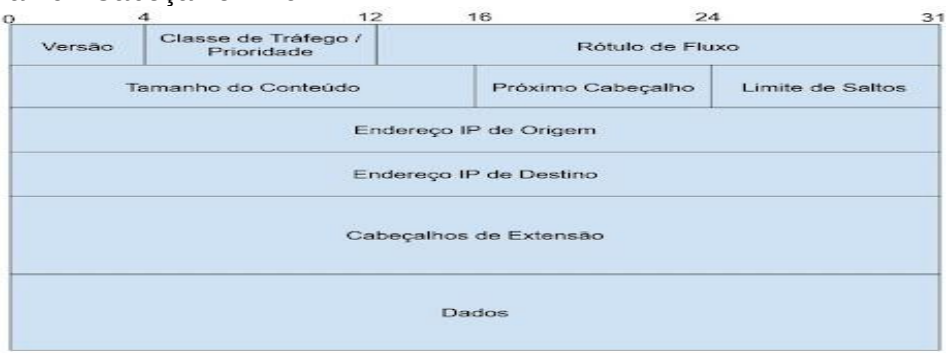
c) Anycast

Um endereço *anycast* é qualquer endereço Ipv6 *unicast* que possa ser atribuido a vários dispositivos que tenham o mesmo fim. Um pacote enviado a um endereço *anycast* é roteado para o dispositivo mais próximo que tenha esse endereço. Um exemplo dessa aplicação, é o cenário em que vários servidores de DNS estão disponíveis numa rede, que é uma situação comum na *Internet*.

2.9.3 Estrurura do cabeçalho Ipv6

Um pacote Ipv6 é composto por um cabeçalho e um payload (conteúdo), o payload consiste no Packet Data Unit (PDU) da camada superior mais os cabeçalhos de extensão opcionais, a figura abaixo apresenta a estrutura do cabeçalho IPv6.

Figura 20 - Cabeçalho IPv6



Fonte: Fábio dos Reis (2020)

O campo *versão* especifica a versão IP do pacote em questão e para o IPv6, esse valor é 6 em binário. O campo de *classe de tráfego* é usado para distinguir a classe de serviço para pacotes com diferentes requisítos de entrega em tempo real. Ele é usado com a arquitetura de serviço diferenciado para qualidade de serviço da mesma maneira que o campo de mesmo nome em IPv4. O campo *rótulo de fluxo*, permite marcar pacotes de uma mesma origem direcionados para um mesmo processo no dispositivo destino. Esse campo, facilita com que pacotes de um mesmo processo possam ser reestruturados no destino. O campo tamanho de *carga útil* determina o número de bytes carregados no payload correspondentes somente aos dados. O campo *próximo cabeçalho* permite a simplificação do cabeçalho principal pois nele podem ser encapsulados várias opções

que outrora eram parte do cabeçalho IPv4, sendo um deles o campo de autenticação para questões de segurança. O *limite de hops* equivale ao campo TTL do IPv4 e impede que pacotes entrem em loops infinitos nas redes. Os *campos endereço de origem e endereço de destino* especificam os endereços de 128 bits do remitente e destinatário de um processo. Fábio dos Reis (2020)

2.9.4 Configuração de endereços IPv6 unicast

Em IPv6, os dispositivos obtêm endereços ou prefixo de rede dinamicamente através de mensagens *Internet control Message Protocol version* 6 (ICMPv6). O processo de aquisição de recursos IPv6 é feito através de mensagens RS e RA trocadas por hosts, servidores e roteadores que implementem o o serviço *Dynamic Host Configuration* (DHCP). As mensagens de RS são enviadas por dispositivos da rede para descobrir roteadores Ipv6 e as mensagens de RA são enviadas por roteadores para informar os hosts sobre como obter um GUA Ipv6 e fornecer informações úteis de rede, como: Prefixo de rede e comprimento do prefixo, endereço de gateway padrão e endereço DNS. As configurações requeridas, podem ser alcançadas usando três técnicas de configuração de endereços, Stateless Address Auto-Configuration (SLAAC), SLAAC com servidor DHCPv6 Stateless e DHCPv6 stateful. Santos et al (2010)

a) Atribuição de endereço SLAAC

A atribuição de endereços (SLAAC) é o método mais comum de atribuição de endereços para clientes IPv6. O SLAAC fornece conectividade simples *plug-and-play,* na qual os clientes se auto-atribuem endereços com base no prefixo Ipv6. Esse processo é realizado quando o roteador Ipv6 envia mensagens periódicas de anúncio do roteador que informam o cliente sobre o prefixo em uso (os primeiros 64 bits) e do gateway padrão. A partir desse ponto, os clientes podem gerar os 64 bits restantes de seu endereço Ipv6 com base em dois algoritmos: EUI-64, que é baseado no endereço MAC da interface, ou endereços privados que são gerados aleatóriamente. A escolha do algoritmo depende do cliente e geralmente é configurável. Santos et al (2010)

O EUI – 64, foi definido pela IEEE e consiste no seguinte processo: Um valor de 16bits de FFFE é inserido no meio do endereço MAC Ethernet de 48bits do cliente. O 7º bit do endereço MAC do cliente é revertido do binário 0 para 1. A Quadro abaixo mostra esse processo.

Quadro 7 - Mecanismo de autoconfiguração por slaac

MAC de 48 bits	**fc:99:47:75:ce:e0**

ID da interface EUI-64	Fe99:47ff:fe75:cee0

Fonte: Quadro do Autor

b) Atribuição de endereço através DHCPv6

O uso do DHCPv6 não é necessário para a conectividade do cliente Ipv6 se o SLAAC já estiver implementado. Há dois modos de operação para DHCPv6 chamados: **Stateless e Stateful.**

O modo DHCPv6 Stateless é usado para fornecer aos clientes informações de rede adicionais não disponíveis no anúncio do roteador, mas não um endereço Ipv6, pois isso já é autoconfigurado no SLAAC. Essas informações podem incluir o nome de domínio DNS, os servidores DNS e outras opções específicas do fornecedor de DHCP.

A opção Stateful DHCPv6, também conhecida como modo gerenciado, opera de forma semelhante ao DHCPv4, na medida que atribui endereços exclusivos a cada cliente, em vez do cliente gerá-las por si próprio como acontece em SLAAC. Santos et al (2010)

2.10 Técnicas de Migração IPv4 para IPv6

Moreiras e al. (2015) afirmam que o momento ideal para a implementação do IPv6 já passou, e que por conta disso, arranjou-se um grande complicador para a migração para a nova versão. O problema é que muitos relutam à aderência da nova tecnologia. A África, por exemplo, é o continente que menos adoptou o IPv6 e Moçambique conta somente com 0,02% de redes IPv6, o que é preocupante. A figura abaixo mostra dados colectados pela *google statistics*.

Figura 21 - Implantação do IPv6 em Moçambique

Fonte: Página de estatística de implantação do IPv6 da Google (2021)

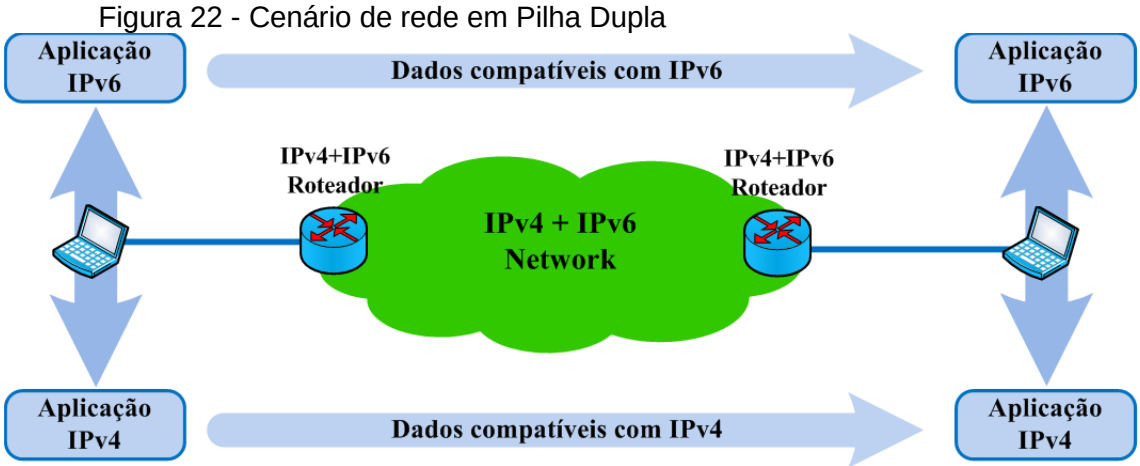
O IPv6 não foi projetado para ser uma extensão ou complemento do IPv4, mas, um substituto que resolve o problema do esgotamento de endereços. Embora não interoperem, ambos podem funcionar em paralelo nos mesmos equipamentos, possibilitando realizar a transição de forma gradual. Desse modo, sua implantação começa aos poucos, com o IPv4 ainda funcionando. Esse cenário é chamado de pilha dupla ou *dualstack*. Quando o IPv6 estiver implantado em todos os dispositivos, o IPv4 pode ser abandonado. Isso implica que, tanto o IPv4 como o IPv6 co-existirão no futuro próximo e a transição levará mais algum tempo, por este motivo a IETF criou vários protocolos e ferramentas para ajudar os administradores de redes a migrarem para o IPv6. Santos et al (2010)

As técnicas de migração podem ser divididas em três categorias: Pilha dupla, Tunelamento e Tradução

2.10.1 PILHA DUPLA - *DUAL STACK*

A técnica de transição pilha dupla, é o método de migração mais simples e não requer muito esforço técnico. Consiste no uso das duas versões do IP disponíveis, visto que muitos serviços e dispositivos na *Internet* ainda operam com IPv4. Manter o IPv4 já existente funcionando de forma estável e implantar o IPv6, para que coexistam nos mesmos equipamentos, é a forma básica escolhida para a transição na *Internet*. A utilização deste método permite que dispositivos e roteadores estejam equipados com pilhas para ambos os protocolos, tendo a capacidade de enviar e receber os dois tipos de pacotes, IPv4 e IPv6. Com isso, um nó Pilha Dupla, ou nó IPv6/IPv4, se comportará como um nó IPv6 na comunicação com outro nó IPv6 e se comportará como um nó IPv4 na comunicação com outro nó IPv4 (NIC.br 2012). Esse cenário é visto na figura 22.

Figura 22 - Cenário de rede em Pilha Dupla



Fonte: BARRETO (2017 p. 38)

Na implementação de uma infra-estrutura que use o método de transição de pilha dupla, devem ser observadas algumas configurações no DNS, nos protocolos de roteamento e de *firewalls*. Em relação ao DNS, é necessário configurar os novos endereços IPv6, usando registros do tipo AAAA (quad-A), que armazenam seus endereços. Ao receber endereços IPv6 e IPv4 como resposta a uma consulta no DNS a aplicação decide qual protocolo usar. Normalmente a preferência é pelo protocolo IPv6 e, em caso de falha, tenta-se o IPv4.

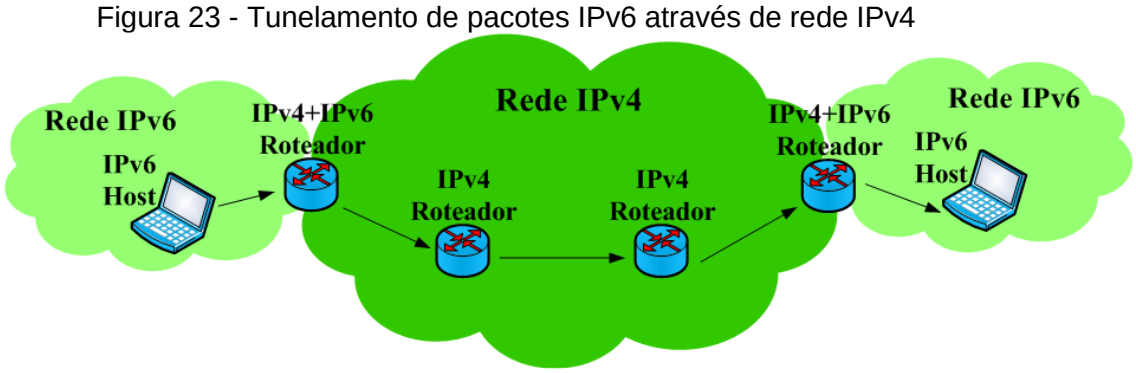
Em uma rede com pilha dupla, a configuração do roteamento IPv6 normalmente é independente da configuração do roteamento IPv4. Neste caso, os gestores de rede podem optar por protocolos que suportem as duas tecnologias ou forçar aqui dois protocolos diferentes trabalhem paralelamente.

Embora essa técnica seja o método padrão de migração de redes IPv4 para IPv6, ela apresenta limitações no sentido de que, não oferece suporte algum no caso de falta de endereços IPs por parte da provedora. Nos casos em que não existam endereços IPs v4 para dar suporte a essa técnica de transição, os provedores devem optar por outros métodos como as de tunelamento e de tradução.

2.10.2 TUNELAMENTO – *TUNNELING*

Tunelamento é o tipo de técnica de transição que permite que uma rede inteiramente IPv4 transporte tráfego IPv6 e vice-versa. Assim, se duas extremidades precisam se comunicar mas a provedora possui uma rede inteiramente IPv4, a técnica usada é o tunelamento. A figura abaixo ilustra uma rede desse tipo.

Figura 23 - Tunelamento de pacotes IPv6 através de rede IPv4



Fonte: BARRETO (2017 p. 34)

As técnicas de tunelamento fazem o encapsulamento de pacotes IPv6 em pacotes IPv4. Este encapsulamento é conhecido como 6in4 ou IPv6-in-IPv4. Ele consiste em colocar o pacote IPv6 dentro de um pacote IPv4, adequar os endereços de origem e destino para o IPv4 e colocar no campo protocolo do cabeçalho IPv4 o tipo 41 (29 em

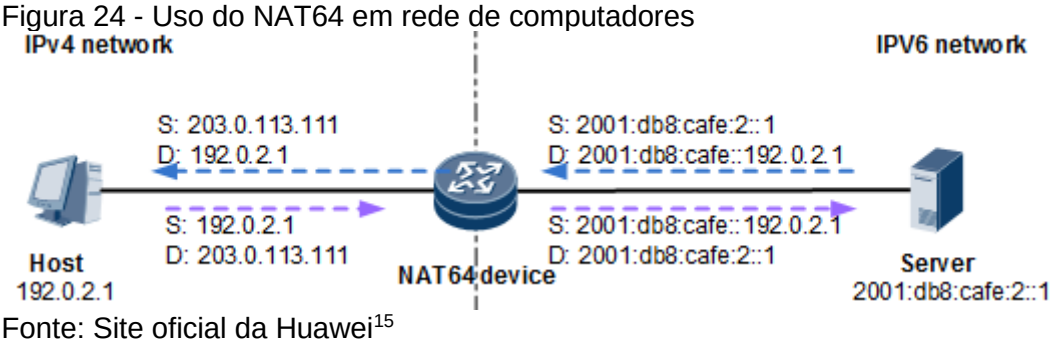
hexadecimal). Esse tipo de encapsulamento é conhecido por 6in4, ou como “protocolo 41”. Quando o destino receber o pacote com tipo 41 ele irá remover o cabeçalho IPv4 e tratar o pacote como IPv6. Também é possível, de forma análoga, encapsular pacotes IPv4 em pacotes IPv6, técnica conhecida como 4in6. (NIC.br 2012).

Uma das formas de utilizar-se túneis é criando-os manualmente. A técnica 6over4 explicada no Request For Comment (RFC 4213) utiliza um túnel manual estabelecido entre dois nós IPv4 para enviar o tráfego IPv6. Todo o tráfego IPv6 a ser enviado é encapsulado em IPv4 usando 6in4, explicado anteriormente. A configuração manual consiste em definir quais serão os IPs v4 de origem e destino que serão utilizados em cada ponta do túnel. Ao ser recebido pelo nó destino, o pacote IPv6 é desencapsulado e tratado adequadamente. Esse tipo de túnel pode ser utilizado para contornar um equipamento ou enlace sem suporte a IPv6 numa rede, ou para criar túneis estáticos entre duas redes IPv6 através da Internet IPv4. O túnel 6over4 é um caminho estabelecido manualmente que tem o objetivo de permitir conexão IPv6 entre dois nós de rede conectados por uma rede via IPv4. Ele usa o encapsulamento 6in4. O encapsulamento 6in4, com a utilização do tipo 41, pode ser utilizado também em outras técnicas de transição que transportam pacotes IPv6 em redes IPv4. (NIC.br 2012)

2.10.3 TRADUÇÃO – *TRANSLATION*

Técnicas de tradução consistem basicamente na conversão de cabeçalhos dos pacotes que trafegam numa rede. Essa conversão é feita com o auxílio do protocolo *unicast* especial (Endereço IPv4-Mapeado) e a técnica de tradução NAT64 (*Network Address Translation* IPv6 to IPv4) como mostra a figura abaixo.

Figura 24 - Uso do NAT64 em rede de computadores



Fonte: Site oficial da Huawei[15]

O NAT64 necessita da técnica auxiliar DNS64 para fazer a conversão dos DNS requisitados por um host, isto significa que todo o servidor capacitado ao IPv6, deve ter um endereço IPv4 equivalente. O lado negativo é que este possui as mesmas

[15] https://support.huawei.com/enterprise/en/doc/EDOC1100125492 acesso em 11 de Junho de 2022

desvantagens que o NAT normal, por este motivo, é desaconselhável seu uso na rede. Embora essas técnicas devam ser evitadas ao máximo, Barreto destaca o seu importante papel para a transição:

> O fato é que a técnica de tradução, apresenta-se como uma importante tecnologia para auxiliar na transição do IPv4 para o IPv6, como suporte à administração do acelerado crescimento da Internet. Mesmo que novos usuários da Internet só obtenham endereços IPv6, eles não são capazes de acessar conteúdos sobre as predominantes redes IPv4, excepto, se existir um elemento com papel de Tradução. Citado por Barreto (2015, p. 35)

NAT64 e DNS64

No processo de comunicação entre um host puramente IPv6 e uma rede IPv4, os endereços precisam ser convertidos para que a comunicação tenha sucesso. Ao tentar acessar um servidor IPv4 na *Internet*, a máquina IPv6 só poderá efectuar um pedido de resolução DNS para registros AAAA que correspondem ao IPv6, esse registro é encaminhado para o servidor DNS64 que converte para o registro de IPv4 (A), assim, o pedido de resolução de DNS é encaminhado ao servidor DNS normal que responde com um endereço IPv4. No envio da resolução por parte do DNS, a resposta é capitada pelo DNS64 que atribui um endereço IPv6 equivalente. Neste momento a máquina é capaz de fazer um requisito de serviço para o endereço adquirido. Após este processo, os endereços IPv6 de origem e destino são convertidos novamente pelo NAT64 para que possam ser interpretados pelo servidor IPv4. (NIC.br 2012)

Capítulo 3 – Implementação

Este capítulo tem como objetivo, demostrar as técnicas de migração do protocolo IPv4 para IPv6 em uma rede virtual e real usando dois computadores. Para este fim, serão testadas as seguintes técnicas

1. Pilha dupla
2. Tunelamento

No caso do experimento virtual, far-se-á o uso do simulador Cisco Packet Tracer**.** A proposta de teste através de um simulador, deve-se ao facto de este permitir uma visão realística de uma rede em todos os seus moldes e permitir efectuar testes mais robustos que outrora não seriam viáveis sem grandes investimentos. Os dispositivos usados nas redes virtuais são: Roteadores, *Switches*, computadores, servidores, cabos seriais e par

trançado. Para a rede real serão usados dois laptops de marca HP 250 G4 e cabo ethernet de 100Mbps.

3.1 Especificações dos Equipamentos com capacidade de migração

As técnicas usadas aqui, não influênciam no desempenho dos serviços que correm na rede. Isso significa que todos os serviços que já tenham sido previamente usados na rede antes da migração não precisarão sofrer nenhum impacto na troca do IPv4 para o IPv6, não há necessidade de paralisar os serviços enquanto a implementação do IPv6 ocorre, isso permite continuidade dos serviços sem influênciar na experiência do usuário final.

O IPv6 não é uma tecnologia recente e portanto a maioria dos equipamentos, mesmos os mais antigos suportam este tipo de tecnologia. Isso significa que não há necessidade de mudança de equipamentos de rede para efectuar a transição, a menos que os equipamentos sejam tão antigos que não suportem o IPv6. Abaixo seguem as especificações de dispositivos com suporte a migração IPv4-IPv6:

Tabela 8 - Requisítos de dispositivos com capacidade de migração

Dispositivo	Requesitos para migração
Computadores	Todos os computadores com suporte à entrada ethernet ou wi-fi fabricados após o ano 2000
Switches	Os switches da camada 2 não lidam com endereços de IP e por este motivo qualquer switch pode ser implementado numa rede em transição
Roteadores	Os roteadores são os mais afectados pela transição pois para funcionarem sob o conceito de túnel terão de possuir um CPU multi-core que o permite funcionar com roteador multi-protocolo, outras especificações são: portas FastEthernet de no mínimo 100Mpbs, Entradas Wan e Lan.
Servidor	Servidores com versão Apache acima de 2.0.16
Cabo Rj45	Qualquer tipo de cabo FastEthernet e GigabitEthernet

Fonte: Quadro do Autor

Nos casos em que um computador não tenha a interface de configuração do IPv6 mas tenha suporte ao mesmo via software, pode ser usado o seguinte código no prompt de comando para efectuar a sua instalação:

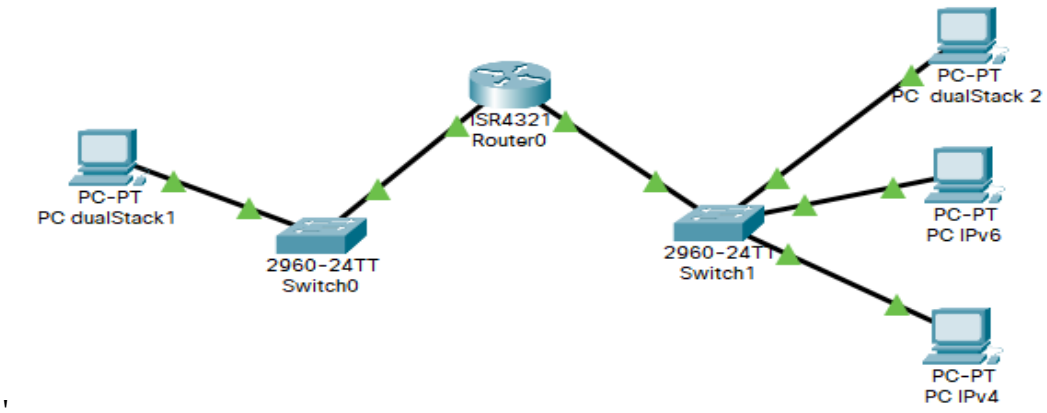
```
> Netsh interface ipv6 install
```

3.2 Configuração da técnica Pilha dupla

A técnica de migração de pilha dupla é o método mais recomendado para a transição gradual do IPv4 para o IPv6. Este tipo de técnica, em especial, concentra-se na migração dos dispositivos finais como, computadores, laptops e servidores. A figura 25 mostra um experimento de transição usando esta técnica.

A figura abaixo, mostra duas redes que se comunicam sob o conceito de protocolos em pilha dupla. Dois dos computadoes foram configurados com a pilha dupla e outros dois possuem um único tipo de protocolo. Esta topologia tem um propósito experimental, pois pretende verificar o funcionamento da pilha dupla. As configurações necessárias para a atribuição do IP podem ser feitas de duas formas: de forma estática ou dinâmica. O presente experimento optou por usar os dois métodos de atribuição, o método estático para a rede a esquerda e o método dinâmico para a rede a direita, as configurações feitas para atribuição dos endereços IP encontram-se no APÊNDICE A e os resultados na secção 3.4.1.

Figura 25 – Topologia física da rede



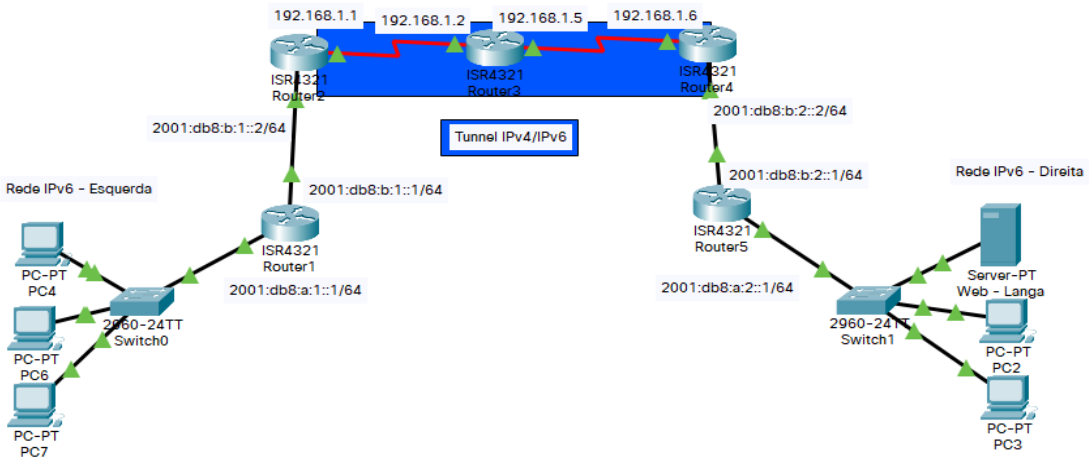
Fonte: Figura do Autor

3.3 Configuração da técnica de Tunelamento

A figura 26 ilustra a rede implementada no simulador da Cisco**.** Esta é dividida em 2 sub-redes nomeadamente, rede somente IPv6 - Esquerda e IPv6 - Direita. O laboratório pretende analisar o comportamento existente entre as sub-redes usando a técnica de migração do tipo tunelamento, para tal, foram usados 5 roteadores, nomeadamente *router* 1, *router* 2, *router* 3, *router* 4, *router* 5. Destes, os roteadores 2 e 4, desempenham o papel de roteadores **Multiprotocolos,** pois implementam o conceito de túnel que os permite encapsular protocolos IPv6 em IPv4. Esta e as diversas outras configurações, podem ser vistas no APÊNDICE B. Para além destes, foram usados 3 switches com vista a comutar os diversos dispositivos existentes na mesma rede. 1 servidor que implementa serviços de DNS, DHCP e HTTP. 5 hosts dos quais 3 pertecem a rede IPv6 a esquerda e 2 a rede IPv6 a direita. A redes locais utlizam a arquitetura ethernet e por este motivo utilizam os cabos par trançado e para comunicações remotas foram usados os cabos serial que oferem meios de transmissão para redes WAN. Nos meios de comunicação, os cabos *fastethernet* que possuem taxas nominais de 100Mbps, interligam

computadores e *switches* e os *gigabitethernet* de até 1gbps são usados para interligar equipamentos de maior tráfego como os roteadores.

Figura 26 - Experimento de Tunelamento



Fonte: Figura do Autor

Os hosts da rede recebem configurações especiais para que possam adquirir automaticamente registros de domínio, endereços IP, gateway-padrão e vários outros serviços. As configurações feitas nos roteadores, permitem aprendizagem de rotas automáticas através de protocolos de roteamento, para além disso, configurações para permitir tráfego IPv6 em redes IPv4 foram necessárias. Neste experimento, as interfaces que endereçam IPv6 utilizam o protocolo de roteamento RIP e as rotas IPv4, o protocolo OSPF. A razão disso reside no facto de que atualmente a maioria das redes é IPv4 e podem existir inúmeras rotas para o seu tráfego. Por outro lado, a rota IPv6 é específica para caminhos que implementam túneis e deve ser corretamente ajustada.

No roteador 1 são definidos os IPs de gateway-padrão de 2001:db8:a:1::1 para IPv6 e 192.168.2.1 para IPv4 na interface *GigabitEthernet* 0/0/0 e para a interface *GigabitEthernet* 0/0/1 do mesmo roteador, 2001:db8:b:1::1 para IPv6 e 192.168.1.9 para IPv4. No roteador 2, o *GigabitEthernet* 0/0/1 tem os gateways-padrões de 2001:db8:b:1::2 e 192.168.1.10 para IPv6 e IPv4 respectivamente. A interface serial 0/1/0 recebe o endereço 192.68.1.1. O roteador 3 possui somente interfaces seriais. A interface serial 0/1/0 recebe 192.168.1.2 para questões de gateway a serial 0/1/1. 192.168.1.5. O roteador 4 a semelhança do roteador 2, representa um dispositivo entre as redes IPv4 e IPv6. A interface serial 0/1/1 possui o gateway 192.168.1.6 e a interface g0/0/0 recebe 2001:db8:b:2::2. Por fim, o roteador 5, recebe os endereços 2001:db8:b:2::1 e 2001:db8:a:2::1 nas interfaces g0/0/0 e g0/0/1 respectivamente.

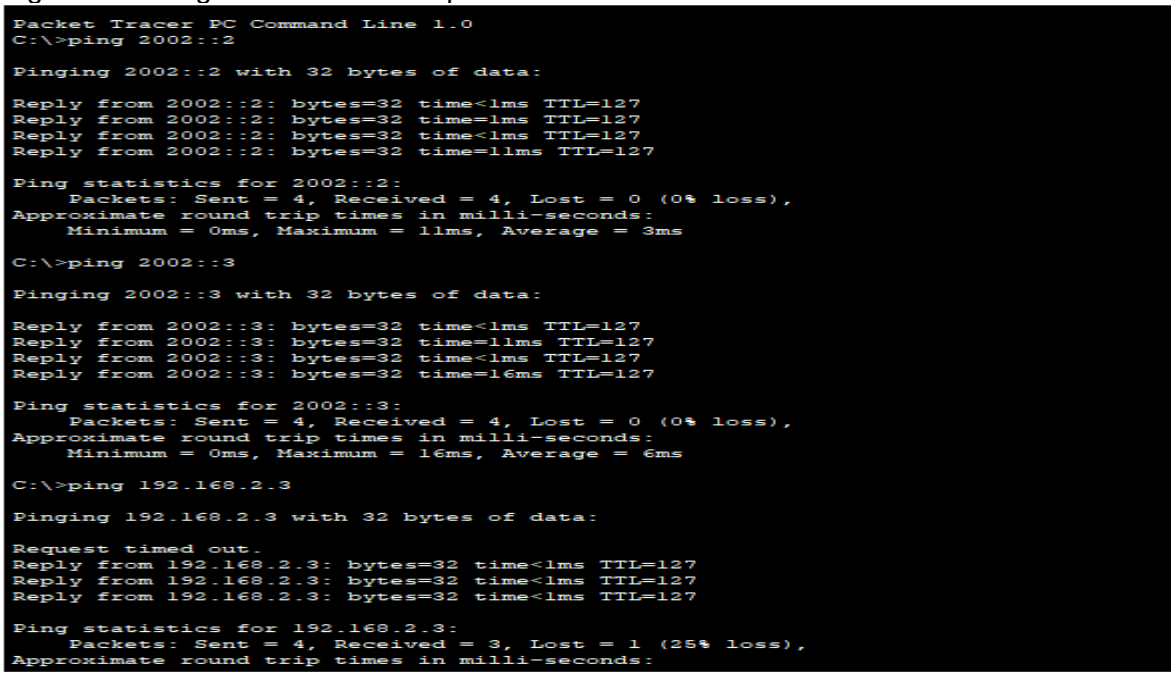
Os roteadores 2 e 4 diferente dos roteadores 1, 3 e 5, precisam de configurações adicionais para permitir o tunelamento de pacotes. No APÊNDICE B, as configurações dos dispositivos são apresentadas de forma detalhada.

3.4 Resultados obtidos

Nesta secção serão apresentados os resultados obtidos dos experimentos das técnicas de pilha dupla (Ambiente real e virtual) e tunelamento.

3.4.1 Resultados da experiência virtual usando pilha dupla

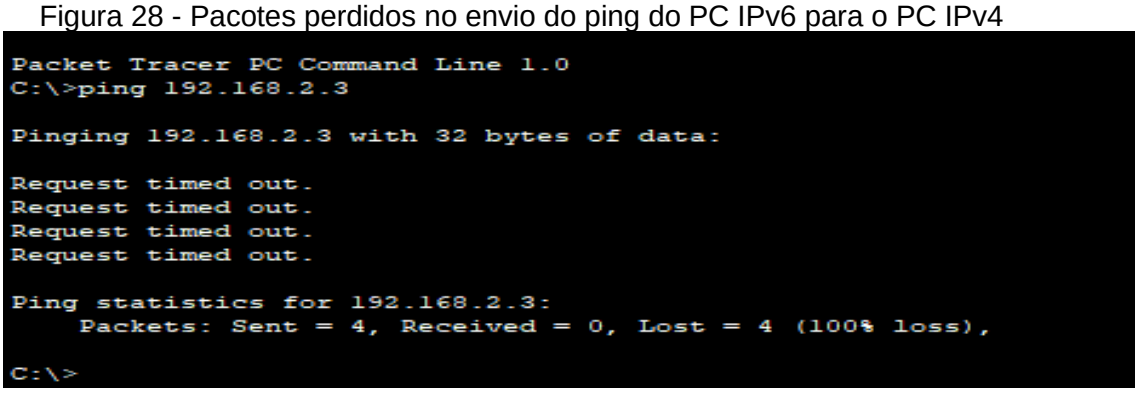
Figura 27 - Ping do PC dualStack para todos PC da rede a direita



Fonte: Figura do Autor

A figura acima apresenta o cenário em que o host PC *dualStack* 1, de endereço 2001::2/64, envia uma mensagem ICMP no formato de Ping para os PC *dualStack* 2, PC IPv6 e PC IPv4. No envio dos quatro pacotes, todos foram recebidos no destino, isso acontece porque o PC *dualStack* 1 possui uma pilha dupla e pode acessar redes com os dois tipos de serviço. No cenário da figura 28 por exemplo, todos os pacotes enviados do PC IPv6 para o PC IPv4 são perdidos. A perda de pacotes é devido a não implementação da pilha dupla pois nós puramente IPv6 não possuem capacidade para se comunicar com nós puramente IPv4.

Figura 28 - Pacotes perdidos no envio do ping do PC IPv6 para o PC IPv4



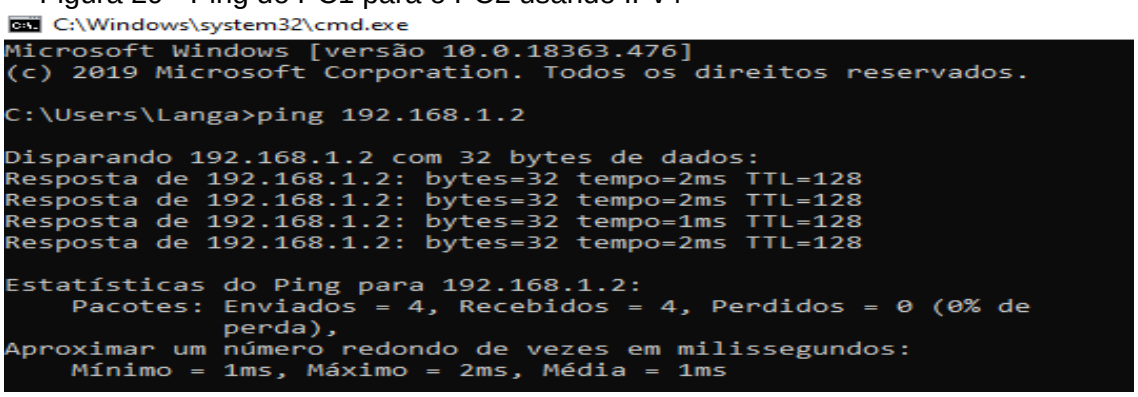
Fonte: Figura do Autor

3.4.2 Resultados do experiência real usando pilha dupla

O seguinte experimento tem a mesma finalidade que o anterior, o objectivo é demostrar o funcionamento da pilha dupla usando uma rede com componentes reais e averiguar o funcionamento da pilha dupla nestas condições, porém, não será possível validar o funcionamento do túnil, por este ser implementado em roteadores e não dispositivos terminais como um computador. As configurações dos computadores envolvidos são encontradas no APÊNDICE C.

No laboratório, a máquina de nome Langa foi configurada para suportar a pilha dupla e os IPs atribuídos são 192.168.1.1 e 2001:1::1/64 para IPv4 e IPv6 respectivamente. A máquina de de nome Dembele recebe um único IP, o IPv4. Na figura 29, é efectuado um ping da máquina Langa para Dembele, o resultado são todos os pacotes recebidos, isto porque a máquina 2001:1::1/64 pode se comunicar tanto com IPv4 como com IPv6.

Figura 29 - Ping do PC1 para o PC2 usando IPv4

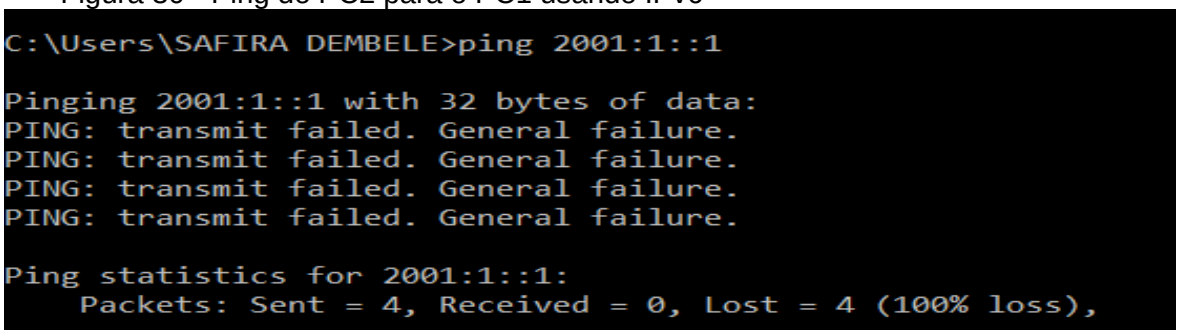


Fonte: Figura do Autor

Nesta experimento, o objectivo é demostrar que na ausência da pilha dupla, a tentativa de conectar redes IPv4 e IPv6, fracassa. Para tal, desactivou-se a pilha dupla do host 1, somente o endereço 2001:1::1/64 ficou ativo nesta máquina, como mostra a

figura abaixo, na tentativa de testar a conectividade entre os pc1 usando o endereço 2001:1::1/64 e o pc2 de endereço 192.168.1.2, todos os pacotes são perdidos.

Figura 30 - Ping do PC2 para o PC1 usando IPv6



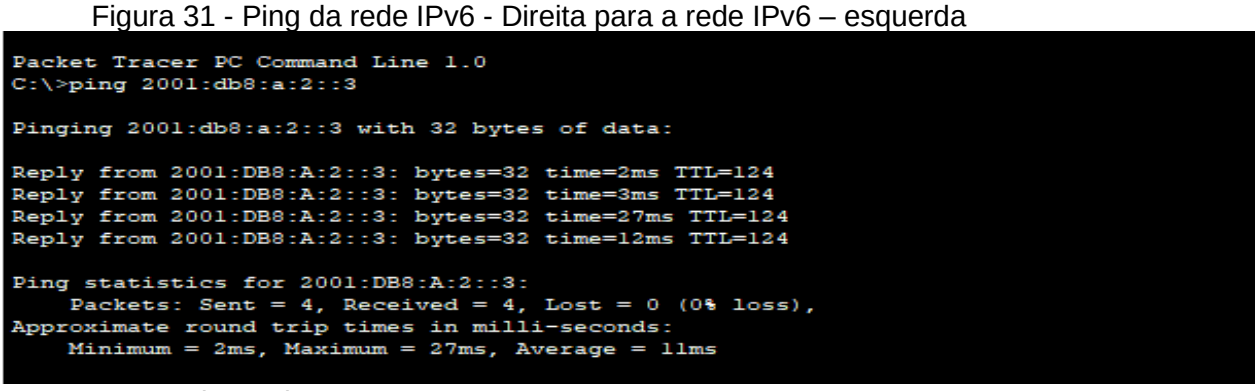
Fonte: Figura do Autor

3.4.3 Resultados do experiência de tunelamento

No experimento, os roteadores na barra azul no topo da figura 26, representam arquiteturas somente IPv4, porém, os roteadores 2 e 4 implementam o conceito de tunelamento, ao efectuar um *ping* para uma máquina da rede IPv6 todos os pacotes são entregues ao host destino conforme a figura 31, isso comprova o funcionamento do túnel e portando a possibilidade de se trafegar pacotes IPv6 através redes puramente IPv4.

Para comprovar a existência de um túnel, foi efectuado um ping da máquina PC4 para o host 2001:db8:a:2::3 (PC3) . O resultado é que todos os pacotes são recebidos, como mostra a figura 31. No percurso do tunelamento, os pacotes IPv6 que saiem das máquinas da rede IPv6 são encapsulados em pacotes IPv4 pelo roteador 2, para que possam trafegar nas redes puramente IPv4. No fim, são interceptados pelo roteador 4 que o desencapsula, os entregando a outra extremidade da rede puramente IPv6.

Figura 31 - Ping da rede IPv6 - Direita para a rede IPv6 – esquerda



Fonte: Figura do Autor

4 Conclusão

Quando se iniciou o presente trabalho de pesquisa, constatou-se que devido a diversas áreas de negócios como industrias, empresas e instituições acadêmicas adoptarem serviços assentados nas tecnologias de informação, a condição atual do protocolo fundamental da *Internet* apresentava alguns obstáculos para fazer face ao cenário atual da rede mundial. Essas objeções tornaram importante o estudo do tema sobre a migração do protocolo IPv4 para o Protocolo IPv6 em redes de computadores.

A pesquisa partiu do problema de se encontrar técnicas que possibilitassem a interoperabilidade dos protocolos IPv4 e IPv6 pois existe uma incompatibilidade entre os dois. Durante o trabalho, verificou-se a existência de mecanismos que possibilitam essa comunicação entre os diferentes protocolos e então foram feitos os testes das possibilidades. Conforme descrito na secção 3, as hipóteses foram comprovadas através de testes onde foram verificados os seguintes achados:

Pois verificou-se que o utilitário *Ping* usando as técnicas de migração comprova a existência de conectividade entre as redes que utilizam protocolos diferentes. Com isso verificou-se que o problema de pesquisa foi completamente respondido.

No decorrer do projecto, foram identificadas 3 técnicas de migração de redes IPv4 para IPv6 nomeadamente, pilha dupla, tunelamento e tradução. Das 3, somente duas foram usadas para fins de teste, pilha dupla e tunelamento. A técnica de tradução é em muitos casos desaconselhado pois prolonga o tempo de vida do protocolo IPv4 na rede, o que é totalmente indesejável. Conclui-se que das duas aprovadas, a que mais se adequa a situação de migração atual é o método de tunelamento, uma vez que este não necessita que os dispositivos terminais tenham de adquirir o IPv4. Assim, dispositivos que estejam em uma rede que implemente o tunelamento, podem acessar todos os tipos de serviços (sejam eles baseados em IPv4 ou IPv6) adquirindo simplesmente endereços IPv6 o que o torna ideal pois atualmente existem poucos endereços IPv4 disponíveis, porém muitos dos serviços ainda funcionam com base no protocolo antigo.

Da pesquisa conclui-se também, que os dois métodos de transição (pilha dupla e tunelamento), podem ser usados para resolver problemas diferentes de esgotamento IPv4. A técnica de pilha dupla é o método virado a transição de dispositivos finais, por este motivo ele resolve o problema de ramificação de redes devido a incompatibilidade dos protocolos IPv4 e IPv6. Por outro lado, a técnica de tunelamento oferece maior suporte ao cenário de escassez do protocolo antigo.

Por fim, verificou-se que, resultado do experimento real e do virtual foi o mesmo, isso permitiu concluir que os métodos são funcionais e que podem ser implementados em ambientes reais de trabalho sem afectar os serviços que correm nela.

4.1 Limitações

O presente projecto de pesquisa não pôde ser testado em condições específicas de trabalho, o que apresenta-se como uma limitação na recolha e análise de dados pois somente nestas condições é possível tirar conclusões mais acuradas da aplicação destes métodos. Por outro lado, a falta de entrevistas o limitou na recolha de dados sobre situações mais recentes e reais sobre os problemas apresentados pelo protocolo. Por fim, a limitação encontrada por falta de um laboratório real foi o da ausência de testes de desempenho e segurança entre os dois protocolos. Portanto, diante da metodologia proposta, percebe-se que o trabalho poderia ter sido realizado com uma pesquisa mais ampla na bibliografia para realizar a coleta de situações reais enfrentas por instituições e provedoras da *Internet* sobre a situação atual e real do IPv4.

4.2 Recomendações

Tendo em vista que os experimentos representam de certo modo uma simulação ideal, o presente trabalho abre espaço para que empresas ou outras entidades com interesse no tema possam realizar estudos mais apurados em ambientes reais, recolhendo ferramentas de análise e de planejamento estratégico para situações mais específicas.

Portanto, em vista das limitações encontradas e devido a indisponibilidade de algumas informações e de tempo, recomenda-se para trabalhos futuros a incorporação ao presente modelo de proposta de migração, o levantamento de dados exploratórios como as entrevistas para averiguar as reais condições proporcionadas pelo protocolo IPv4 nas instituições. Recomenda-se também a realização de experimentos em ambientes reais para que se possam comparar alguns parâmetros de desempenho entre os dois protocolos.

Por fim, sugere-se o uso do seguinte trabalho para análise de desempenho para redes de grande dimensão como os de grandes operadoras ou provedoras *Internet* para que se possa analisar os impactos da migração IPv4/Ipv6 nessas dimensões.

Referências Bibliográficas

Forouzan, B. 2007 – Data Communications and Networking, 4th ed., McGraw-Hill, New York

Kurose e Ross. 2014 – Redes de Computadores e a Internet, 6th ed., Pearson Education, São Paulo

Moreiras e al. 2015 – Laboratório de IPv6, Novatec, São Paulo

Moreiras e al. 2012 – IPv6 Básico, São Paulo

Tenenbaum e Wetherall, 2017 – Redes de Computadores, 5th ed., Pearson Education, Rio de Janeiro

Torres, G. 2001 – Redes de Computadores Curso Completo, 1st edition, Axcel Books do Brasil, Rio de Janeiro

Torres, G. 2014 – Redes de Computadores Curso Completo, 2nd edition, SF Editorial, rio de Janeiro

Cordeiro, E. Comparação de Técnicas de Transição do IPv4 para o IPv6. Dissertação de mestrado – Instituto de Pesquisas Tecnológica do Estado de são Paulo, 2014

Barreto, J. Um Modelo de Migração de Ambiente IPv4 para IPv6 em uma Rede Acadêmica Heterogênea. Dissertação de Mestrado – Instituto de ciências exatas do departamento de Ciências da Computação da Universidade de Brasília, Brasília, 2015

Pimparel P. Internet das coisas e a Integração de Sistemas Domóticos Residenciais. Dissertação de Mestrado – Universidade da Beira Interior, 2017

Evans D. 2011 – A Internet das Coisas, Cisco Internet Business Solutions Group

Rocha A. Internet of Things – Aplicações na Área da Saúde. Artigo concebido a disciplina de gestão de produção – Universidade de Brasília, Brasília, 2017

Netto R. Protocolo de Internet versão 6. Monografia de especialização – Universidade Tecnológica Federal do Paraná, Curitiba, 2018

Cepik e Marcelino, 2021 – Segurança Cibernética em Moçambique, *Carta Internacional*, vol.16, n.3

Lopes e al. 2015 – As camadas do Modelo OSI, *Revista Interdisciplinar do pensamento Científico,* vol.1, n 19

Nordmark e Gilligan. Request For Comments 4213. Basic Transition Mechanisms for IPv6 Hosts and Routers. https://datatracker.ietf.org/doc/html/rfc4213 05 de Janeiro de 2022

Bafalluy e al. 2012 - IP Mobility. http://cba.upc.edu 23 de dezembro 2021

Sistema de segurança Interna – Relatório anual, 2020. https://www.portugal.gov.pt 02 de dezembro de 2021

Rennan Cockles. 2019 – IPs públicos e privados disponível em https://r3ck0.medium.com/analogia-sobre-ips-e0c20a8c05c7 26 de Janeiro de 2022

Sacks Anelise 2016 – Redes de Computadores I https://www.gta.ufrj.br/grad/02_2/MIPv6/ 07 de novembro de 2021

https://labs.apnic.net/ipv4/report.html 05 de Janeiro de 2022

https://www.gabrielborba.com.br acesso em 01 de novembro de 2021

https://www.clubedohardware.com.br/artigos/redes/como-o-protocolo-tcp-ip-funciona-parte-1-r34823/?nbcpage=6 19 de outubro de 2021

https://www.dltec.com.br/blog/redes/Quadro-de-enderecos-mac/ 18 de outubro de 2021

Fábio dos Reis. 2016 - Cabeçalho UDP https://www.bosontreinamentos.com.br visto 13 de dezembro de 2021

https://www.google.com/a mp/s/docplayer.com.br/am/65888008-Instituto-federal-de-educacao-ciencia-e-tecnologia-rio-grande-do-norte-ifrn.html 22 de dezembro de 2021

https://www.google.com/amp/s/docplayer.com.br/amp/7527844-Redes-de-computadores-endereco-ip.html 22 de dezembro de 2021

https://www.google.com/amp/s/www.techtudo.com.br/google/amp/noticias/2018/04/cloudflare-lanca-dns-1111-e-promete-mais-velocidade-e-privacidade.ghtml 24 de dezembro de 2021

https://revistasegurancaeletronica.com.br/o-que-e-snmp-e-sua-utilizacao-em-seguranca-eletronica/ 23 de dezembro de 2021

COELHO, Beatriz. **Blog da Mettzer,** 2017. Página inicial. Disponível em: https://blog.mettzer.com/metodologia-cientifica . Acesso em: 21 de dezembro de 2021

https://www.google.com/intl/pt-BR/ipv6/statistics.html 20 de dezembro de 2021

APÊNDICES

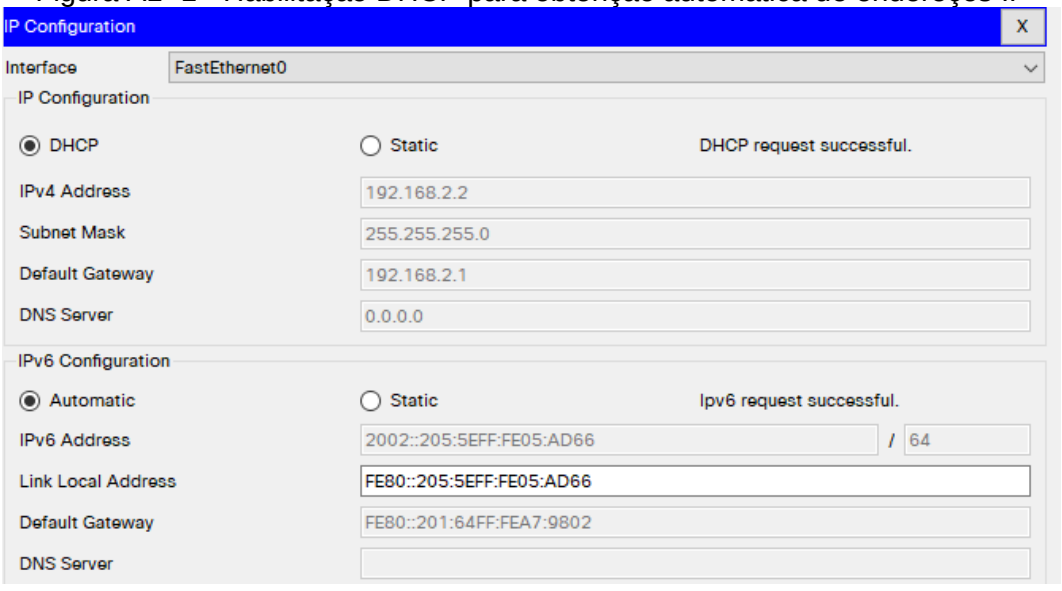
APÊNDICE A

Configuração dinâmica dos dispositvos do laboratório pilha dupla da rede a direita

```
Router> enable
Router# Configure terminal
Router(config-if)#ip dhcp pool denny
Router(dhcp-config)#network 192.168.2.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#exi
Router(config)#int g0/0/1
Router(config-if)#ipv6 dhcp pool denny
Router(config-dhcpv6)#network 2002/64
```

Para habilitar a atribuição automática dos endereços IPs via DHCP, é necessário usar a interface gráfica dos computadores e habilitar o DHCP, como mostra a figura abaixo

Figura A1- 1 - Habilitação DHCP para obtenção automática de endereços IP



Fonte: Autor

Para atribuir os endereços de forma estática, isto é, através do próprio administrador da rede, é necessário habilitar a parte *static* da figura A.1 acima e escrever os endereços de IPv4 do computador, a máscara de sub-rede, o gateway padrão e o endereço de DNS manualmente

APÊNDICE B

Configuração de roteadores sem Tunelamento

```
Configuração do router1

Router> enable

Router# Configure terminal

Router (Config)# ipv6 unicast-routing

Router (Config)# ipv6 router rip redev6

Router (Config-rtr)# exit

Router (Config)# interface gigabitethernet0/0/0

Router (Config-if)# ipv6 address 2001:db8:a:1::1/64

Router (Config-if)# ip address 192.168.2.1 255.255.255.0

Router (Config-if)# ipv6 rip redev6 enable

Router (Config-if)# no shutdown

Router (Config-if)# exit

Router (Config)# interface gigabitethernet0/0/1

Router (Config-if)# ipv6 address 2001:db8:b:1::1/64

Router (Config-if)# ip address 192.168.2.9 255.255.255.252

Router (Config-if)# ipv6 rip redev6 enable

Router (Config-if)# no shutdown

Router (Config-if)# exit

Router (Config)# router ospf 1

Router (Config-router)# router-id 4.4.4.4

Router (Config-router)# log-adjacency-changes

Router (Config-router)# network 192.168.2.0 0.0.0.255 area 0

Router (Config-router)# network 192.168.1.8 0.0.0.3 area 0

Router (Config-router)# exit

Router (config)# ip dhcp pool denny
```

```
Router (config-dhcp)# network 192.168.2.0 255.255.255.0

Router (config-dhcp)# default-router 192.168.2.1

Router (config-dhcp)# dns 200.200.200.2


Configuração do router 3

Router> enable

Router# Configure terminal

Router (Config)# interface serial 0/1/0

Router (Config-if)# ip address 192.168.2 255.255.255.252

Router (Config-if)# no shutdown

Router (Config)# exit

Router (Config)# interface serialt0/1/1

Router (Config-if)# ip address 192.168.1.5 255.255.255.252

Router (Config-if)# no shutdown

Router (Config-if)# exit

Router (Config)# router ospf 1

Router (Config-router)# router-id 2.2.2.2

Router (Config-router)# log adjacency-changes

Router (Config-router)# network 192.168.1.0 0.0.0.3 area 0

Router (Config-router)# network 192.168.1.4 0.0.0.3 area 0

Router (Config-router)# exit
```

APÊNDICE B – Configuração de roteadores com Tunelamento

Configuração do router 2

```
Router> enable

Router# Configure terminal

Router (Config)# ipv6 unicast-routing

Router (Config)# ipv6 router rip redev6

Router (Config-rtr)# exit

Router (Config)# interface gigabitethernet0/0/1

Router (Config-if)# ipv6 address 2001:db8:b:1::2/64

Router (Config-if)# ip address 192.168.1.10 255.255.255.252

Router (Config-if)# ipv6 rip redev6 enable

Router (Config-if)# no shutdown

Router (Config-if)# exit

Router (Config)# interface serial0/1/0

Router (Config-if)# ip address 192.168.1.1 255.255.255.252

Router (Config-if)# no shutdown

Router (Config-if)# exit

Router (Config)# router ospf 1

Router (Config-router)# router-id 1.1.1.1

Router (Config-router)# log-adjacency-changes

Router (Config-router)# network 192.168.1.0 0.0.0.255 area 0

Router (Config-router)# network 192.168.1.8 0.0.0.3 area 0

Router (Config-router)# exit

Router (Config)# interface tunnel 0

Router (Config-if)# ipv6 address 3000::1/112

Router (Config-if)# router rip redev6 enable

Router (Config-if)# tunnel source serial 0/1/0

Router (Config-if)# tunnel destination 192.168.1.6
```

```
Router (Config-if)# tunnel mode ipv6ip

Configuração do router 4

Router> enable

Router# Configure terminal

Router (Config)# ipv6 unicast-routing

Router (Config)# ipv6 router rip redev6

Router (Config-rtr)# exit

Router (Config)# interface gigabitethernet0/0/0

Router (Config-if)# ipv6 address 2001:db8:b:2::2/64

Router (Config-if)# ip address 192.168.1.10 255.255.255.252

Router (Config-if)# ipv6 rip redev6 enable

Router (Config-if)# no shutdown

Router (Config-if)# exit

Router (Config)# interface serial0/1/1

Router (Config-if)# ip address 192.168.1.6 255.255.255.252

Router (Config-if)# no shutdown

Router (Config-if)# exit

Router (Config)# router ospf 1

Router (Config-router)# router-id 3.3.3.3

Router (Config-router)# log-adjacency-changes

Router (Config-router)# network 192.168.1.4 0.0.0.3 area 0

Router (Config-router)# exit

Router (Config)# interface tunnel 0

Router (Config-if)# ipv6 address 3000::2/112

Router (Config-if)# router rip redev6 enable

Router (Config-if)# tunnel source serial 0/1/1

Router (Config-if)# tunnel destination 192.168.1.1

Router (Config-if)# tunnel mode ipv6ip
```

APÊNDICE C – Configuração do PC1 e PC2

Figura A3- 1 - Configuração dos endereços IPv4 do PC1

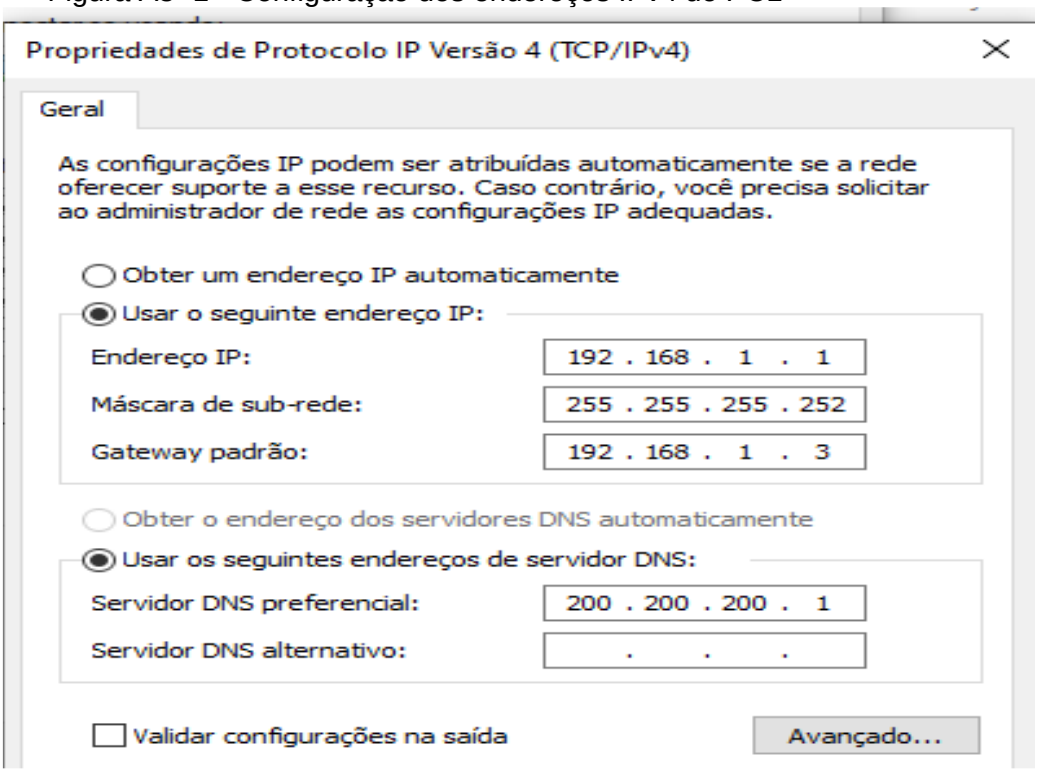


Figura A3- 2 - Configuração dos endereços IPv6 do PC1

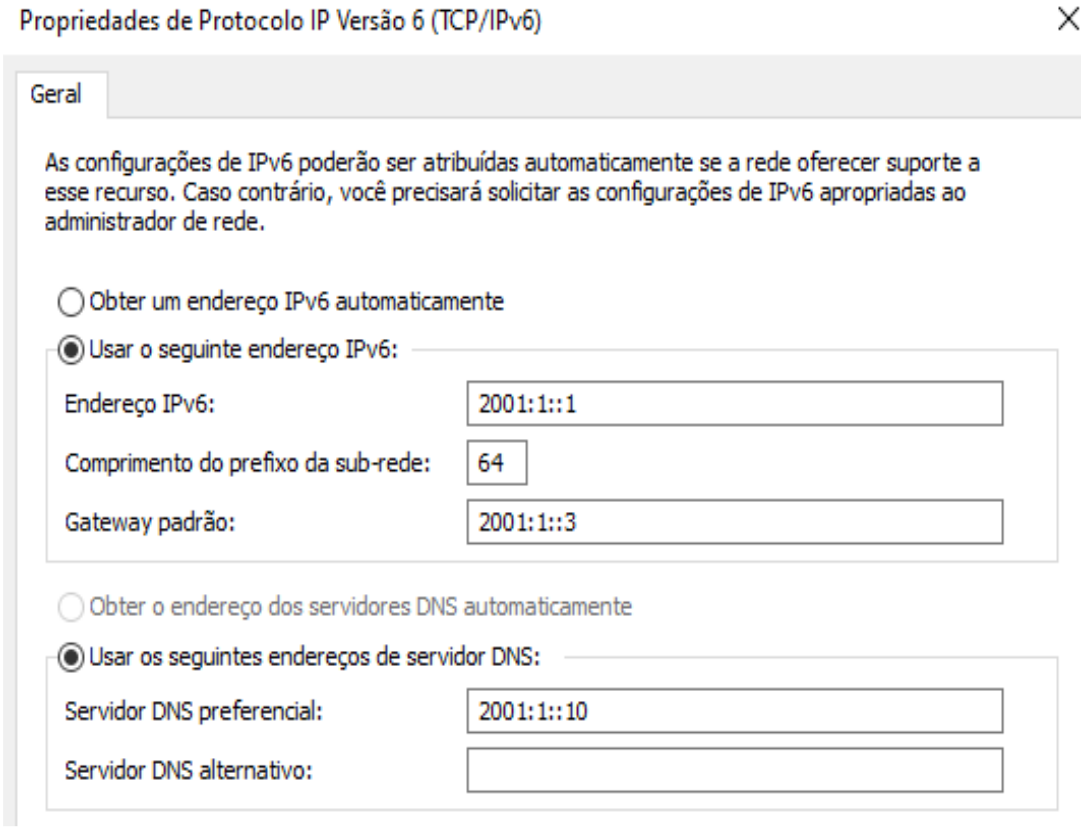


Figura A3- 3 - Configuração dos endereços IPv4 do PC2