

**UNIVERSIDADE PAULISTA - UNIP**

**JOÃO LEONARDO VIEGAS**

**COMPARATIVO E ANÁLISE DE DESEMPENHO ENTRE OS PROTOCOLOS  
IPv4 E IPv6: um estudo de caso em um servidor Samba**

**LIMEIRA**

**2017**

**JOÃO LEONARDO VIEGAS**

**COMPARATIVO E ANÁLISE DE DESEMPENHO ENTRE OS PROTOCOLOS  
IPv4 E IPv6: um estudo de caso em um servidor Samba**

Trabalho de conclusão de curso para obtenção do título de Bacharel em Ciências da Computação apresentado à Universidade Paulista - UNIP.

Professores Orientadores: Prof. Ms. Sergio Nunes  
Prof. Ms. Antônio Mateus Locci  
Prof. Ms. Marcos Vinícius Gialdi

**LIMEIRA**

**2017**

**JOÃO LEONARDO VIEGAS**

**COMPARATIVO E ANÁLISE DE DESEMPENHO ENTRE OS PROTOCOLOS  
IPv4 E IPv6: um estudo de caso em um servidor Samba**

Trabalho de conclusão de curso para obtenção  
do título de Bacharel em Ciências da  
Computação apresentado à Universidade  
Paulista - UNIP.

Aprovada em \_\_\_ de \_\_\_\_\_ de 2017.

**BANCA EXAMINADORA**

---

Prof. Dr. Nome completo

---

Prof. Me. Nome completo

---

Prof. Esp. Nome completo

## **DEDICATÓRIA**

Dedico este trabalho primeiramente a Deus, que me deu forças para seguir em frente em todos os momentos, à minha família, que me incentivou desde o início, minha namorada Patrícia, que esteve comigo desde o início e sabe todos os momentos difíceis enfrentados e a todos os professores que fizeram parte durante todos esses anos de curso e puderam cada um contribuir com suas experiências. Sem os mesmos, nada disso seria possível.

## EPÍGRAFE

*“Não confunda derrotas com fracasso nem vitórias com sucesso. Na vida de um campeão sempre haverá algumas derrotas, assim como na vida de um perdedor sempre haverá vitórias. A diferença é que, enquanto os campeões crescem nas derrotas, os perdedores se acomodam nas vitórias.”*

**(Roberto Shinyashiki)**

## RESUMO

Devido ao seu uso comercial no início dos anos 1990, a Internet teve um crescimento significativo, muito além do imaginado por especialistas de protocolos de IP da época, causando assim um grande impacto na indústria de redes. Soluções foram buscadas, a fim de amenizar este impacto, corrigir e melhorar sua infraestrutura. O protocolo de IPv4 deveria ser modernizado, fazendo surgir um novo protocolo, o IPv6, capaz de corrigir e estruturar da melhor maneira o uso da Internet a população. Neste estudo, foi realizado um estudo de caso, mostrando o desempenho dos protocolos IPv4 e IPv6 em uma rede real, focada em um servidor de transferência de arquivos, chamado Samba. Foram utilizados três computadores para o estudo, um sendo o servidor, com *Linux Ubuntu* e outras duas máquinas sendo os *clients*, uma com *Windows 7*, onde ocorreu a transferência dos arquivos e outra com *Linux Ubuntu*, para realizar as medições. As medidas que foram levadas em consideração durante a transferência destes arquivos foram as seguintes: Vazão (*Throughput*), Latência e Perda de pacotes, em dois ambientes diferentes, IPv4 puro e IPv6 puro. Os dados obtidos nesse estudo podem ser de fundamental importância para administradores de redes escolherem o melhor cenário para sua rede, caso ela possua um servidor para transferência de arquivos.

**Palavras chaves:** Redes de computadores, protocolos, desempenho, Linux, Samba.

## ABSTRACT

Due to its commercial use in the beginning of 1990, the Internet has experienced significant growth, far beyond the imagined by networking administrators and experts of IP protocols of the time, causing a major impact on the networking industry. Solutions were sought in order to mitigate this impact, correct and improve its infrastructure. The IPv4 protocol should be modernized, giving rise to a new protocol, the IPv6, able to fix and structure the best way to use the Internet to population. In this study, was made a study of case, showing the performance between IPv4 and IPv6 protocols, in a real network, where the focus was a server for files transferring, called Samba. Three computers were used for this study, one being the server, with Linux Ubuntu, and another two computers, one with Windows 7 as operational system, and another one with Linux Ubuntu, to do the measurements. The measures that was focused were: Throughput, latency and Package loss, in two different environments, pure IPv4 and pure IPv6. The data obtained in this study can be very important for a network administrator to choose the best scenario for his network, if this one has a server for files transferring.

**Keywords.** Network, protocols, performance, Linux, Samba.

## LISTA DE FIGURAS

Figura 01 - Exemplo de Conexão direta Ponto a Ponto. ....	17
Figura 02 - Exemplo de arquitetura multiponto.....	18
Figura 03 - Exemplo de Topologia Estrela. ....	18
Figura 04 - Topologia de rede em anel.....	19
Figura 05 - Exemplo de uma rede barramento.....	20
Figura 06 - Endereços no TCP/IP.....	25
Figura 07 - Relação das camadas e endereços TCP/IP.....	25
Figura 08 - Topologia de rede utilizada para os testes.....	34
Figura 09 - Configuração do servidor Samba.....	37
Figura 10 - Arquivos contidos no servidor Samba.....	38
Figura 11 - Servidor Samba IPv4 mapeado no sistema. ....	39
Figura 12 - Servidor Samba IPv6 mapeado no sistema. ....	39
Figura 13 - Conteúdo do arquivo .bat.....	40
Figura 14 - Exemplo de saída após transferências de arquivos (IPv4). ....	40
Figura 15 - Exemplo de Saída em modo Gráfico. ....	41

## **LISTA DE QUADROS**

Quadro 01 - Comparativo entre os Protocolos IPv4 e IPv6.....	30
Quadro 02 - Configurações dos Dispositivos Utilizados.....	35

## LISTA DE GRÁFICOS

Gráfico 01 - Representação da perda de pacotes.....	46
Gráfico 02 - Representação da latência. ....	46
Gráfico 03 - Representação da vazão média. ....	47

## LISTA DE ABREVIATURA E SIGLAS

ARPA	<i>Advanced Research Project Agency</i>
WWW	<i>World Wide Web</i>
UIT	<i>União Internacional de Telecomunicações</i>
BITNET	<i>Because It's Time to Network</i>
LAN	<i>Local Area Networks</i>
WAN	<i>Wide Area Networks</i>
MAN	<i>Metropolitan Area Networks</i>
TCP	<i>Transmission Control Protocol</i>
IP	<i>Internet Protocol</i>
UDP	<i>User Datagram Protocol</i>
RPC	<i>Remote Procedure Call</i>
RTTP	<i>Real Time Transport Protocol</i>
IPv4	<i>Internet Protocol version 4</i>
IPv6	<i>Internet Protocol version 6</i>
RFC	<i>Request for Comments</i>
IETF	<i>Internet Assigned Numbers Authority</i>
NLANR	<i>National Laboratory for Applied Network Research</i>
DAST	<i>Distributed Applications Support Team</i>
DHPC	<i>Dynamic Host Configuration Protocol</i>

## SUMÁRIO

<b>1. INTRODUÇÃO</b> .....	<b>13</b>
1.1 Objetivo .....	13
<b>2. CONCEITO DE REDES DE COMPUTADORES</b> .....	<b>15</b>
2.1 Classificação de Redes.....	15
2.2 Arquitetura de Redes .....	16
2.2.1 Ponto a Ponto .....	17
2.2.2 Multiponto ou Ponto-Multiponto.....	18
2.2.3 Estrela .....	18
2.2.4 Anel.....	19
2.2.5 Barramento .....	20
<b>3. PROTOCOLOS</b> .....	<b>21</b>
3.1 Funções dos protocolos de rede .....	21
3.2 Protocolo TCP/IP .....	21
3.2.1 Protocolo IP.....	23
3.2.2 Funcionamento do TCP/IP .....	24
3.2.3 Endereçamento .....	24
3.3 Convergência e interoperabilidade em redes .....	26
3.4 Os Protocolos IPv4 e IPv6 .....	28
3.4.1 NAT ( <i>Network Address Resolution</i> ) .....	28
3.4.2 Comparativo entre os protocolos IPv4 e IPv6 .....	30
3.4.3 Estratégia de Migração entre os protocolos IPv4 para o IPv6 .....	31
3.4.4 Pilha Dupla.....	31
3.4.5 Tunelamento ( <i>Tunelling</i> ) .....	32
<b>4. MATERIAIS E MÉTODOS</b> .....	<b>34</b>
4.1 Topologia e Equipamentos Utilizados .....	34
4.2 Cenários Utilizados Para as Análises .....	35
<b>5. ESTUDO DE CASO</b> .....	<b>36</b>
5.1 Teste de Desempenho e Métricas .....	40
5.1.1 Perda de Pacotes.....	41
5.1.2 Latência.....	42
5.1.3 Vazão ( <i>Throughput</i> ) .....	43
<b>6. RESULTADOS EXPERIMENTAIS</b> .....	<b>45</b>
6.1 Análises dos Resultados.....	45
6.2 Discussões dos Experimentos .....	47
<b>7. CONCLUSÃO E TRABALHOS FUTUROS</b> .....	<b>49</b>
<b>8. REFERÊNCIAS</b> .....	<b>51</b>

## 1. INTRODUÇÃO

Com a globalização digital e a crescente demanda de informações, causando conseqüentemente o aumento de redes conectadas a Internet, foi se necessário a modernização dos protocolos de gerenciamento e infraestrutura da indústria de redes.

Protocolos de IPv4, são nada mais que combinações numéricas que estabelecem a conexão entre os computadores, ou seja, protocolo este que permite o uso da Internet em qualquer lugar. Porém, com o aumento significativo nos últimos tempos do uso de conexão banda larga, prevê-se a substituição do protocolo de IPv4 para outro mais moderno, mas que a mantivessem com sua estrutura global preservada, contudo solucionando suas deficiências, entre elas, as exigências por mais espaço de endereçamento, maior segurança, entre outros, foram fatores que contribuíram para o desenvolvimento do protocolo de IPv6.

Segundo Domingos (2011), o IPv6 veio para resolver vários problemas do IPv4, trazendo melhorias em diversos aspectos, como a autoconfiguração do roteamento e de redes e o problema da escassez de números de IP.

Mas para que essas informações sejam trocadas na rede utilizando os dois protocolos, é necessário a utilização de um dispositivo que possa permitir a transição e convivência entre os mesmos, julgando que ambos os protocolos são incompatíveis. Atualmente, existem roteadores capazes de permitir uma conexão entre os dois. (IPV6.BR, 2012)

Com o intuito de avaliar o desempenho destes dois protocolos, o *software Jperf* foi utilizado, com ele foi possível avaliar e analisar o desempenho destes dois protocolos na prática. O *Jperf* é um *software* que realiza várias análises de desempenho dentro de uma rede. Também foi utilizado o comando *ping* para realizar uma parte dos testes.

### 1.1 OBJETIVO

O principal objetivo deste trabalho, foi implementar uma análise de desempenho entre os protocolos IPv4 e IPv6 em uma rede real, a fim de

fornecer dados quantitativos para um administrador de rede poder projetar a estrutura correta na utilização desse protocolo, que apesar de não ser tão novo, muitas empresas ainda não pensam nessa migração e nem possuem profissionais totalmente capacitados para trabalhar com esse protocolo.

Os administradores de rede devem projetar como será a estrutura de sua rede com muita precisão, onde para cada finalidade, uma estrutura diferente pode ser utilizada.

Foram gerados dados quantitativos baseados em uma rede que contém um servidor para transferência de arquivos, que é o Samba. O estudo foi realizado em uma rede real, onde foi montada uma pequena estrutura, de um servidor e dois *clients*, onde foram realizados os testes e obtido os dados.

Para a coleta dos dados entre esses dois protocolos, foram realizados testes de latência, perda de pacotes e vazão (*Throughput*). Estes testes foram realizados utilizando o comando *ping*, através do terminal do Linux Ubuntu e a ferramenta *Jperf* (*iPerf* com interface gráfica).

Todos os logs, imagens obtidas neste estudo, script utilizado para a transferência dos arquivos, estão disponíveis em um DVD anexo ao trabalho.

## 2. CONCEITO DE REDE DE COMPUTADORES

Uma rede de computadores é constituída por um conjunto de módulos processadores, capazes de realizar a troca de informações e compartilhar recursos, através de celulares, *tablets*, arquivos online, impressoras, etc. (NASCIMENTO, 2011)

As redes de computadores existem para atender a demanda de aplicações comerciais, aplicações domésticas e dos usuários móveis. (AMARAL, 2012)

Segundo Pinheiro (2003), no início as redes de computadores eram pequenas, possuindo poucos computadores, sendo estas comercialmente usada em 1964, nos Estados Unidos, pelas companhias aéreas.

Pinheiro (2003), ainda cita que na década de 1970 houve um movimento para a padronização das redes, por meio de fabricantes diferentes, dando direção a construção de protocolos abertos que poderiam servir à várias soluções; já na década de 1980, as empresas DEC, Intel e Xerox se uniram para criar o que conhecemos hoje como o padrão *Ethernet*.

Uma rede de computadores vai muito além de uma simples conexão de cabos e placas. Existem também a necessidade de uma série de protocolos para regular a comunicação entre todos os níveis, desde o programa que está sendo utilizado até o tipo de cabo instalado. (AMARAL, 2012)

De acordo com Dantas (2002), uma das características mais utilizadas para a classificação de redes é a sua abrangência geográfica. Assim, é convencional a classificação das redes locais - LANs (*Local Area Networks*), metropolitanas - MANs (*Metropolitan Area Networks*), geograficamente distribuídas WANs (*Wide Area Networks*), dentre outras.

### 2.1 Classificação das redes

Uma rede de computadores pode ser classificada de diversas formas, sendo alguma delas: LAN, WAN E PAN.

Uma rede LAN, é capaz de alcançar uma distância de algumas centenas

de metros, ocupando instalações em escritórios, residências, prédios comerciais e industriais. (AMARAL,2012)

“Rede local é uma rede para comunicação de informações na forma de bits entre dispositivos independentes e interconectados, estando completamente sobre o controle do usuário e limitada a existir dentro das premissas do usuário”. (SOUSA, p.292)

Chamamos de rede local (Lan-local área network) um conjunto de computadores interligados numa área dentro de um edifício ou campus de uma empresa. (SOUSA, 2005)

Esse tipo de rede geralmente é composto por computadores conectados entre si, através de dispositivos tecnológicos (placas de rede, switch, hub, etc), podendo facilitar assim a troca de informações. (PERLIN et. al., 2014)

Já uma rede WAN, é considerada uma rede de longa distância, capaz de operar e compartilhar recursos especializados por uma maior população de usuários dispersos geograficamente (Figura 3). Estas redes possuem um custo considerado elevado, portanto a maioria desta são mantidas, operadas, gerenciadas e de propriedade pública. (MAZZOLA, 2000)

Uma Rede de Área Pessoal ou PAN, nada mais é que uma rede formada por dispositivos muito próximos uns dos outros. Podemos dar um exemplo desse tipo de rede, dispositivos bluetooth compartilhando informações entre si ou dois notebooks em uma mesma sala. (PERLIN, et. al. 2014)

## **2.2 Arquiteturas de Redes**

De acordo com Guerber (2009), a forma como os equipamentos de uma rede é interligada definem a arquitetura da mesma.

Sousa (2005, p. 38) define que “uma rede de computadores é composta por diversos equipamentos, como roteadores, computadores tipo PC, computadores de grande porte (mainframes ou hosts), switches computadores, gateways, hubs, cabos, conectores e outros equipamentos e softwares”.

Uma parte lógica da rede, desenvolvida para executar uma determinada

tarefa que pode ser um cálculo, elaboração de dados ou impressão de um relatório a partir de dados armazenados em discos, por exemplo, são chamados de “softwares”. Já os “hardwares”, são equipamentos que fazem parte da rede, ou seja, a parte física da rede. (SOUSA, 2005)

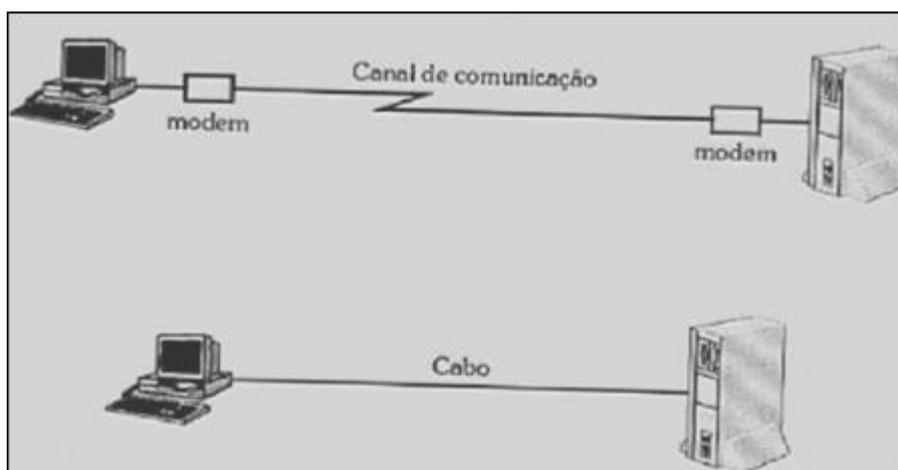
A interação desses equipamentos, a forma como são interligados entre si, são chamados de arquitetura de rede, que podem ser definidas pela forma de conexão física de equipamentos, ou pelos componentes de software ou programas que utilizam. (SOUSA, 2005)

Em nível de conexão física, temos definições de arquiteturas como: ponto a ponto, multiponto ou Ponto-Multiponto, estrela, anel e barramento.

### 2.2.1 Ponto a Ponto

Podemos definir como arquitetura de rede ponto a ponto a forma mais comum de conexão, onde temos receptor e transmissor (dois pontos) interligados e trocando informações diretamente. Neste caso, não há compartilhamento entre vários usuários, somente dois pontos falando entre si. (SOUSA, 2005)

Figura 01 - Exemplo de Conexão direta Ponto a Ponto.



Fonte: SOUSA, 2005, p.39

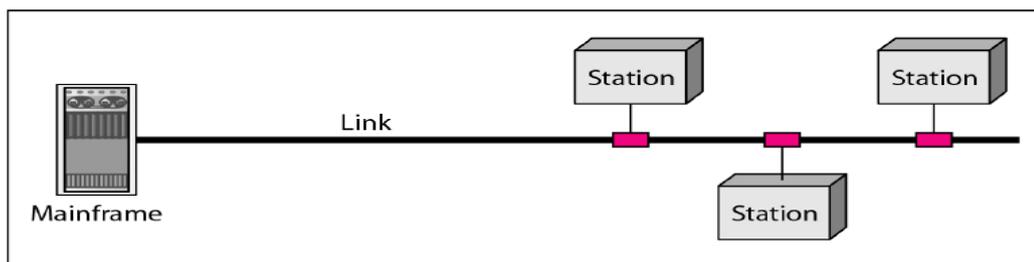
### 2.2.2 Multiponto ou Ponto-Multiponto

De acordo com Sousa (2005), nesta arquitetura um ponto central pode

estar enviando informações para vários pontos, utilizando um mesmo meio e fazendo derivações ao longo do meio.

Este tipo de ligação pode ser utilizado em redes conectadas a grandes distâncias entre si (Figura 02), onde a informação passada por um computador central parte por um único meio de transmissão, sendo distribuída para vários pontos por meio de endereços diferentes. (SOUSA, 2005)

Figura 02 - Exemplo de arquitetura multiponto.



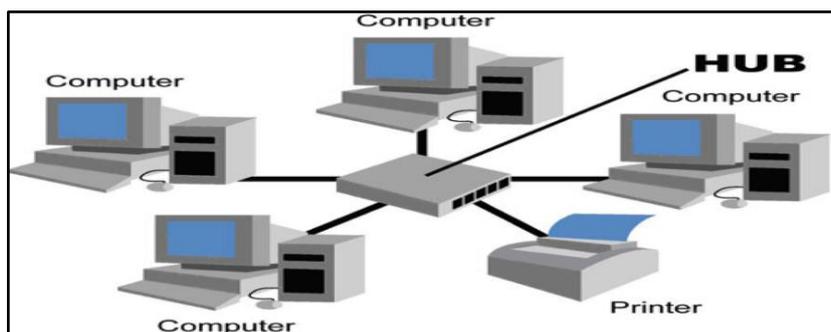
Fonte: NUNES, 2013.

### 2.2.3 Estrela

A arquitetura estrela (Figura 03) é aquela em que todos os pontos e equipamentos de rede convergem para um ponto central, ou seja, todos os meios de comunicação convergem para um nó central. Podemos citar como exemplo, uma rede corporativa, onde o centro pode ser um computador de grande porte chamado host central ou mainframe. (SOUSA, 2005)

Esta topologia era utilizada antigamente somente em redes mainframe, sendo o centro da rede. Hoje esta estrutura voltou a ser utilizada em redes locais com a implementação de hubs, visando facilitar principalmente a detecção e correção de falhas de conexão. (SOUSA, 2005)

Figura 03 - Exemplo de Topologia Estrela.



Fonte: ESIJMJG, 2017

“Os terminais conectados a mainframes são chamados de ‘*terminais burros*’, pois não processam nem armazenam dados, apenas consultam e enviam dados para as aplicações e arquivos do computador central”. (SOUSA, p. 41, 2005)

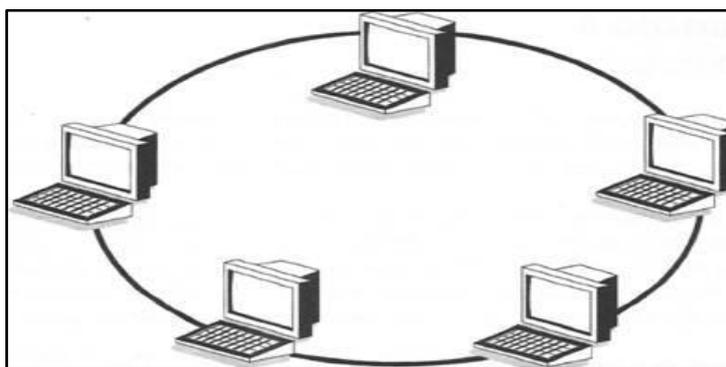
#### 2.2.4 Anel

Segundo Sousa (2005), nesta topologia os dados circulam em dispositivos conectados na rede em circuito fechado até formar um anel. Os dados percorrem por todos os nós da rede, até encontrar o nó com o endereço destino dos dados. Os fluxos dos dados percorrem seu caminho em apenas um sentido (unidirecional). (SOUSA, 2005)

Na arquitetura de rede em anel, caso um nó pare de funcionar, sua transmissão é interrompida, afetando toda rede. Este problema pode ser evitado se um hub concentrador for conectado nas estações, simulando internamente o anel de conexão e sua unidirecionalidade. Vale frisar que nesta topologia todos os nós estão interconectados, ou seja, não existe um nó central. (SOUSA, 2005)

A figura 04, mostra um exemplo da topologia de rede em anel:

Figura 04 - Topologia de rede em anel.



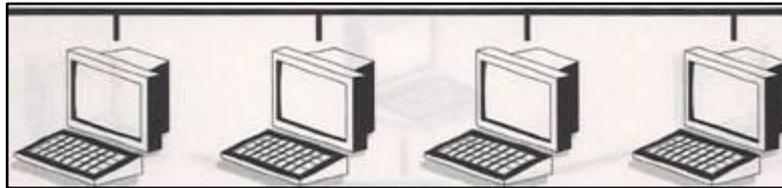
Fonte: FAZER FÁCIL, 2017

#### 2.2.5 Barramento

Pode ser caracterizada como uma linha única de dados (Figura 05), uma forma de conexão de baixo custo em redes locais, tendo como vantagem a

rapidez com que se consegue ligar novos nós ao barramento. A desvantagem é que se o cabo partir em algum ponto, toda rede para de funcionar. (SOUSA, 2005)

Figura 05 - Exemplo de uma rede barramento.



Fonte: FAZER FÁCIL, 2017

### 3. PROTOCOLOS

Segundo Reisswitz (2012, p. 70) na computação, um protocolo é uma convenção que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais.

De maneira simples, um protocolo pode ser definido como “As regras”, a sintaxe, semântica e sincronização da comunicação. Os protocolos podem ser implementados pelo hardware, software, ou por ambos. (REISSWITZ, 2012, p. 70)

#### 3.1 Funções dos protocolos de rede

Para que haja comunicação entre redes são necessários alguns requisitos para fornecer conectividade e seleção de caminho entre transmissor e receptor. Em uma camada de enlace, a comunicação só é possível pois transmissor e receptor estão numa mesma rede. Mas em uma camada de rede, a comunicação entre ambos é realizada host a host, numa rede com diversos roteadores a comunicação é realizada através de seus pares. (BEZERRA, 2008)

Existem diversas pilhas ou famílias de protocolos, dentre as abordadas neste trabalho são:

- Protocolo TCP/IP;
- Protocolos de IPv4 e IPv6.

#### 3.2 Protocolo TCP/IP

O protocolo TCP/IP surgiu devido à necessidade de comunicação do exército americano com outros setores do governo, no período da Guerra Fria, com os trabalhos realizado pelo que atualmente é conhecido como Internet. (BURGESS, 2006)

O nome TCP/IP, refere-se aos dois protocolos de rede mais utilizados atualmente, sendo eles, *Transmission Control Protocol* ou Protocolo de Transmissão e *Internet Protocol* ou Protocolo de Internet, mais conhecido como

IP. (RIOS, 2012)

O modelo TCP/IP é formado por 4 (quatro) camadas e sua tarefa é realizar a entrega de pacotes IP, onde se faz necessário. O roteamento e a entrega de pacotes são uma questão ARPA dos Estados Unidos. O protocolo TCP/IP permitiu que pequenas redes do exército americano fossem interligadas. Com o tempo, o número de redes interligadas foi aumentando, gerando de grande importância nessa camada, assim como a necessidade de evitar o congestionamento. (TANENBAUM, 2003)

- Aplicação: o programa de aplicação passa os dados no formato necessário para a camada de transporte para que a entrega possa ser feita, ou seja, uma aplicação é capaz de interagir com a camada de transporte para que possa enviar ou receber dados. (COMER, 2015)
- Camada de transporte: essa parte controla a comunicação *host-a-host*, sendo responsável pelo envio de uma mensagem de um processo para outro. (REISSWITZ, 2012)
- Inter-redes: esta camada é capaz de realizar o envio de um pacote, da origem ao destino, passando por várias redes (links). A camada de rede garante que cada pacote vá do seu ponto de origem até seu destino. (FOROUZAN, 2010)
- Host/Rede: Esta é a camada responsável por detectar e corrigir erros no nível físico e controlar o fluxo entre transmissão e recepção de quadros em tecnologias de rede. (RIOS, 2012, p. 28)

As principais características deste protocolo, de acordo com Scrimger et. al. (2002), são sua transferência de dados, robustez, controle de fluxo, multiplex, conexões lógicas e o fato de ser *Full duplex*. Os termos estão descritos abaixo:

- Transferência de fluxo de dados: uma aplicação pode confirmar se todos os dados transferidos obtiveram sucesso na entrega no local de destino previsto e obter o retorno do sucesso da aplicação;
- Robustez: o TCP do receptor agrupa os segmentos caso eles cheguem fora de ordem;

- Controle de fluxo: o receptor, à medida que recebe os segmentos, envia uma mensagem confirmando a recepção;
- Multiplex: uso paralelo das portas de comunicação;
- Conexões lógicas: são identificadas pelo processo transmissor e receptor, pela combinação dos mecanismos TCP;
- *Full duplex*: a transferência de dados pode ser simultânea em ambas as direções.

O processo de encaminhamento de pacotes TCP é mais lento que o UDP, porém, quando se necessita de garantia e ordenação na entrega dos segmentos, a melhor opção é o TCP. (RIOS, 2012)

São definidos três protocolos na camada de transporte, no caso: TCP, UDP e SCTP. Já na camada de rede, o protocolo principal definido pelo TCP/IP é o IP. (FOROUZAN, 2008)

### **3.2.1 Protocolo IP**

O protocolo IP é responsável por rotular cada pacote de endereço informações máquina de origem e destino apropriado. Cada computador conectado à Internet tem um endereço Internet (endereço IP) que é única e exclusiva e que o distingue de qualquer outro computador pertencente à Internet. (BARCELL, 2014)

Qualquer programa de internet ou aplicativo precisa saber o número IP do computador com que você quer se comunicar. No entanto, como será visto a seguir, o usuário não precisa saber essa informação, porque não há um sistema mais simples para se referir a um nome de endereço. (BARCELL, 2014)

O protocolo IP lida com pacotes TCP, contendo as peças de informação, e a informação adicional para reordenar e detectar erros de destino e adiciona os endereços IP das máquinas de origem e destino, criando um novo pacote IP podendo ser transmitida através da rede. (BARCELL, 2012)

O IP tornou-se o protocolo oficial da internet, à medida que a internet

evoluiu o IP também desenvolveu. Existem três versões mais recentes, de acordo com Forouzan (2008):

- **Versão 4:** é a mais usada na rede atualmente, porém, possui falhas significativas. Seu principal problema é que o endereço de Internet possui apenas 32 bits, divididos em diferentes classes. Com a alta demanda da Internet, esse esquema de endereçamento não consegue manipular o número projetado de usuários. (FOROUZAN, 2008)
- **Versão 5:** de acordo com Forouzan (2008) explica, está versão foi uma proposta como modelo base o OSI. Essa versão ficou somente como proposta, devido às grandes mudanças de camada e às despesas projetadas.
- **Versão 6:** projetada para manipular transmissões como de áudio e vídeo em tempo real, como também possibilitar o transporte de dados de outros protocolos. (FOROUZAN, 2008)

### 3.2.2 Funcionamento do TCP/IP

Uma rede TCP/IP transfere dados mediante a montagem de blocos de dados em pacotes contendo: (BARCELL, 2014)

- A informação a ser transmitida;
- A informação do IP de destino;
- A informação do IP remetente;
- Outros dados de controle.

Os dois protocolos básicos de TCP/IP são TCP e IP para transporte e transmissão de dados, respectivamente. Neste caso:

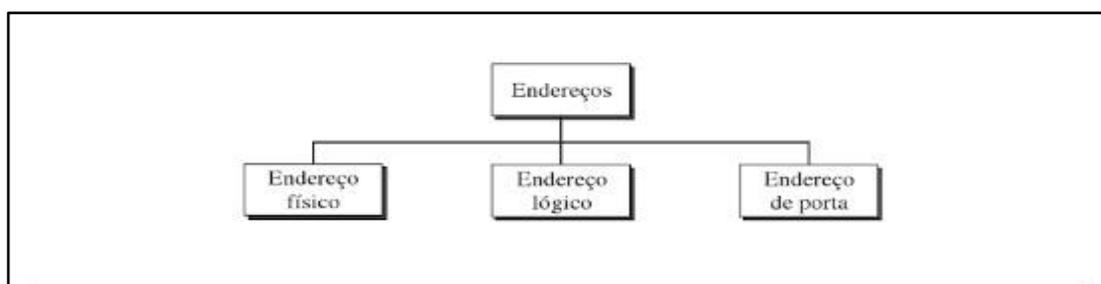
- **TCP:** coordena o movimento de dados entre computadores, dividindo os dados em pacotes.
- **IP:** Move os dados de um computador a outro, os pacotes podem percorrer por caminhos distintos, o receptor os reordena, se um pacote chega errado ele é somente transmitido novamente. (BARCELL, 2014)

### 3.2.3 Endereçamento

Em uma Internet onde o protocolo TCP/IP é utilizado existem três níveis de endereço diferentes, sendo eles: (FOROUZAN, 2008)

- Endereço físico (link);
- Endereço lógico (IP);
- Endereço de porta (Figura 06).

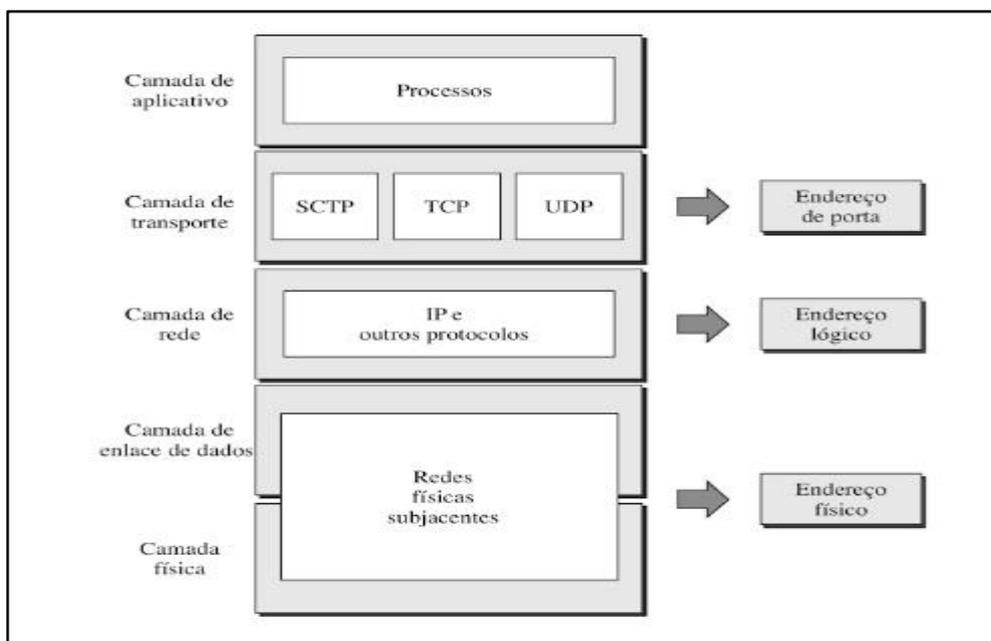
Figura 06 - Endereços no TCP/IP.



Fonte: FOROUZAN, 2008, p.45

Ainda conforme Forouzan (2008) explica, cada endereço pertence a uma camada específica na arquitetura TCP/IP, como mostra na figura 07a seguir:

Figura 07 - Relação das camadas e endereços TCP/IP.



Fonte: FOROUZAN, 2008, p.46

### 3.3 CONVERGÊNCIA E INTEROPERABILIDADE EM REDES

Nassif e Soares (2005) explica que uma rede convergente pode ser considerada como uma associação de redes autônomas operadas por autoridades diferentes, cada qual com sua própria forma de disponibilizar o serviço (fixo, acesso móvel, óptica, etc.)

Esta técnica veio com uma nova visão das redes de comunicações e aplicações multimídias. Podendo assim se concretizar uma plataforma de transporte comum para vídeo, voz e dados, permitindo dessa maneira aplicações do tipo telefonia IP, acesso à web através de telefones móveis e o *streaming* em vídeo se tornará uma realidade. (NASSIF e SOARES, 2005)

No caso da rede voz, podemos destacar dois grupos distintos, sendo eles:

- Telefonia fixa;
- Telefonia móvel. (BRAGA, 2011)

Para serviços de vídeo, outros conceitos foram desenvolvidos e empregados:

- TV a cabo;
- TV via satélite. (BRAGA, 2011)

Já para oferecimento de serviço de dados, eis que surge a criação de rede de computadores, dentre os protocolos mais utilizados o TCP/IP. (BRAGA, 2011)

Em redes convergentes, as arquiteturas da mesma são divididas em três camadas básicas por seus provedores, sendo:

- Infraestrutura de transporte e acesso: unidade de acessos à assinantes, como telefones IP, comutadores e roteadores;
- Camada de controle: responsável pelo encaminhamento, supervisão e liberação das ligações que trafegam pela rede IP;
- Serviços: formada pelos softwares que permitem às operadoras

fornecerem novos serviços aos seus usuários. (NASSIF e SOARES, 2005)

Esta nova arquitetura deveria oferecer QoS (*Quality of Service*) e transparência fim a fim, uma vez que muito dos serviços como voz necessitam de um alto padrão de segurança e qualidade de entrega. (BRAGA, 2011)

A interoperabilidade é outro fator importante desse novo conceito em redes já com outras existentes no mercado, com suas interfaces já abertas, uma vez que seria impossível sua substituição toda de uma só vez. Dessa maneira, uma interconexão seria criada, permitindo a utilização de ambas as redes, para que seus produtos fossem oferecidos. (BRAGA, 2011)

Segundo Braga (2011), outras características são fundamentais para a implantação dessa nova arquitetura:

- Mobilidade na rede de usuários;
- Suporte para terminais já existentes, como para os novos;
- Maior flexibilidade em sua configuração;
- Mecanismos de serviços que pudessem oferecer segurança a fim de proteger a troca de informações.
- Garantir a convergência de redes fixas e móveis;
- Integração de redes fio a fio.

A grande motivação das empresas prestadoras de serviços para buscar o processo da convergência era a redução de custos de operação e manutenção do sistema, além de poder oferecer aos clientes maior quantidade de opções para oferecimento de serviços. (BRAGA, 2011)

Redes convergentes com ambiente IP, permitem que suas operadoras ofereçam serviços novos, aplicações e comodidade a seus novos usuários de maneira eficiente e de custo menor. (NASSIF e SOARES, 2005)

Uma rede convergente com ambiente QoS, poderá gerar soluções mais competitivas as operadoras de serviços de telecomunicações, gerando maior eficiência de sua utilização e com sua infraestrutura orientada à demanda de

tráfego e conjuntos completos e amplos de novos serviços multimídia e banda, larga. (NASSIF e SOARES, 2005)

### **3.4. Os protocolos IPv4 e IPv6**

O protocolo de IP primordialmente criado foi o IPv4 (Internet Protocol version 4). Cada endereço de IPv4 é composto por um número de 32 bits, gerando virtualmente uma quantidade limitada de endereços de IP, logo não havendo mais endereços disponíveis para a criação de novas redes. (SILVEIRA, 2012)

Representado pelos 4 bytes, o endereço IPv4 são separados por “.” (ponto) e representados por números decimais. Desta maneira, o endereço IP 11000001 00100000 11011000 00001001 é representado por 193.32.216.9, por exemplo. (MIOTELLI e CASAGRANDE, 2013)

As principais modificações foram o aumento de endereços, a simplificação do cabeçalho, melhor suporte para as opções oferecidas e seu avanço na questão de segurança. Este protocolo (o IPv6), atende todos os objetivos propostos, preservando os bons recursos do IP, descartando ou reduzindo a importância das características ruins e criando outras quando necessário. (TANENBAUM, 2003)

Nesta nova versão, o IPv6 (Internet Protocol version 6) são compostos por 128 bits (conforme citado anteriormente), gerando assim, uma quantidade ilimitada de endereços de IP. Além disso, revisar completamente o formato do datagrama, substituindo o campo de opções de tamanho variável por uma série de cabeçalhos fixos. (COMER, 2006)

Podemos dizer que o protocolo IPv6 é uma nova versão do protocolo IPv4, desenvolvido para solucionar definitivamente o problema da escassez de endereços disponíveis na Internet, permitindo assim a inserção de novos usuários. (BRITO, 2013, p. 157)

#### **3.4.1 NAT (*Network Address Resolution*)**

O NAT é uma técnica desenvolvida de maneira paliativa, a fim de

solucionar o problema de esgotamento de endereços IPv4. Basicamente tem como ideia permitir que, com um único endereço IP ou um número pequeno deles, vários hosts possam trafegar na internet. (SANTOS, 2009)

Esta técnica utilizada na versão 4 continua sendo a solução para o problema relacionado ao uso limitado de endereços IP, como também traz outros benefícios para seus usuários em termos de segurança: traz privacidade. Usuários que se conectam à rede através de NAT se tornam invisíveis pelo fato de seu endereço IP não estar aberto diretamente a Internet. (FREITAS e TERENCE, 2016)

Segundo Braga (2011) a utilização de NAT, possui às seguintes vantagens:

- Reduz a necessidade de endereços públicos;
- Facilita a numeração interna das redes;
- Oculta a topologia das redes;
- Permite apenas a entrada de pacotes gerados em resposta a um pedido de rede.

Como também possui desvantagens:

- Quebra do modelo fim-a-fim da Internet, já que não é permitido a conexão direta entre dois hosts;
- Aplicações como VPNs, VOIP e P2P terá seu funcionamento dificultado;
- Permite a passagem de pacotes não autorizados, não fazendo um filtro dos mesmos, ou seja, não há segurança.

De qualquer forma, mesmo com todas as soluções paliativas, o problema de esgotamento IP não foi totalmente solucionado com esta técnica, desta forma, a implementação de IPv6 seria a única solução capaz de sustentar a Internet e seu uso em sociedade. (BRAGA, 2011)

Um ponto considerável como argumentação para a não utilização de NAT em IPv6 é o fato que a Internet foi desenvolvida como modelo fim-a-fim e NAT

quebra esse modelo. Em IPv4, NAT continua sendo um excelente mecanismo para assegurar sua vida útil, porém com a nova versão 6 disponível no mercado, esta técnica não terá mais sua função principal, pois não haverá mais necessidade de ser feita a tradução de endereços de uma rede para a outra. (FREITAS e TERENCE, 2016)

### 3.4.2 Comparativo entre os protocolos IPv4 e IPv6

Nunes (2013) explica, que ao comparar os dois protocolos, pode-se observar que, sua estrutura veio para amenizar deficiências da sua versão antiga.

Podemos ver no quadro a seguir (Quadro 01) um comparativo de características entre os protocolos IPv4 e IPv6.

Quadro 01 - Comparativo entre os Protocolos IPv4 e IPv6.

Itens	IPv4	IPv6
Endereços	Endereço IP com tamanho igual a 32 bits.	Endereço IP com tamanho igual a 128 bits.
	Classes de endereços (A, B, C),	Possui três tipos de endereços unicast, anycast e multicast.
Cabeçalho	Existência de <i>checksum</i> do cabeçalho.	Inexistência de <i>checksum</i> do cabeçalho.
	Possui um campo de opções, limitado em 40 bytes.	Possui vários cabeçalhos de extensão com tamanhos variados.
Fragmentação	Pode realizar a fragmentação em qualquer <i>gateway</i> da rede.	Realiza a fragmentação somente na máquina origem.
Roteamento	Suporta aos protocolos básicos de roteamento.	Suporta aos protocolos básicos de roteamento.
	Função de roteamento na fonte exercida por um protocolo de camada superior.	Roteamento é feito através de um cabeçalho de extensão.
Segurança	Não existe mecanismos de segurança.	Suporta mecanismos de segurança, como integridade, autenticação entre outros.
ICMP	Controle de erros.	O protocolo ICMP exerce as funções de controle de membros e controle de erros.

Fonte: MARTINI E BOGO, 2003, p.05

Conforme Brito (2013, p.156) cita, uma das evoluções mais significativas do protocolo IPv6 em relação ao seu antecessor seria a disposição dos campos presentes nos cabeçalhos da camada de rede.

### 3.4.3 Estratégia de Migração entre os protocolos IPv4 para o IPv6

De acordo com Nunes (2013), a migração para o protocolo IPv6, deveria ser feita de forma cautelosa, para que os usuários não sentissem o impacto, mantendo assim a qualidade do serviço. Para que isso fosse feito, todos os

computadores devem migrar para o novo protocolo, porém, este não seria um processo rápido.

As técnicas de mecanismo de transição, que permitem a interoperabilidade entre os protocolos estão divididas em duas categorias:

- RFC 1933, onde são definidos os mecanismos de transição de pilha dupla e tunelamento. (GILLIGAN e NORDMARK, 1996)
- RFC 2766, com as definições dos mecanismos de tradução. (TSIRTISIS, 2000)

Dessa forma as duas técnicas permitem a coexistência dos dois protocolos. Mas na RFC 2766 a infraestrutura da rede pode conter as seguintes características físicas:

- Nó IPv4: comunicação suportada apenas pelo IPv4, onde a maioria dos nós ainda possui essa característica. O IPv4 *only node*;
- Nó IPv6: comunicação suportada pelo IPv6. O IPv6 *only node*;
- Nó IPv4 e IPv6: suporta os dois tipos de protocolo, fazendo assim a comunicação sem a necessidade de transição.

#### **3.4.4 Pilha Dupla**

Como Nunes (2013) explica, a técnica de pilha dupla permite que haja comunicação entre os dois protocolos simultaneamente, ou seja, sistemas de rede que possuem pilha dupla habilitada terão dois endereços de rede, sendo um IPv4 e um IPv6, permitindo dessa maneira que o datagrama seja processado da maneira correta, de acordo com o protocolo.

Roteadores e demais nós quem permitem sua função de tráfego e que possuam a função de Pilha Dupla em sua configuração poderão operar de três maneiras: (NUNES, 2013)

- Pilha IPv4 habilitada e pilha IPv6 desabilitada;
- Pilha IPv6 habilitada e pilha IPv4 desabilitada;
- Ambas as pilhas habilitadas.

Essas configurações podem ser modificadas de acordo com a topologia, a tecnologia dos aparelhos que compõem a rede, ou por alguma questão estratégica e/ou administrativa.

“Utilizar Pilha Dupla pode não ser possível em todas as ocasiões. Por exemplo, quando não há mais IPv4 disponíveis e o provedor precisa atender a novos usuários com IPv6 e IPv4. Outra situação que dificulta a implantação do IPv6 usando pilha dupla é a existência de equipamentos que não o suportam e que não podem ser facilmente substituídos.” (IPv6.BR, 2012)

Para que esta situação seja contornada, existem diversas técnicas disponíveis, que serão descritas brevemente neste trabalho.

### 3.4.5 Tunelamento (*Tunneling*)

O método de tunelamento é conhecido pela capacidade de integração, onde um pacote IPv6 é encapsulado dentro de outro protocolo, como o IPv4. Dessa maneira é possível que haja conexão das ilhas IPv6 sem que haja necessidade de conversão intermediárias para IPv6. Já quando houver o uso do protocolo IPv4 para encapsular o IPv6, o pacote incluirá um cabeçalho de IPv4 de 20 bytes sem opções, um cabeçalho de IPv6 e um *payload*. (PAMPLONA e TOKUNAGA, 2014)

Esta técnica permite que a transmissão de pacotes IPv6 aconteça por uma estrutura IPv4, sem que haja a necessidade de realizar qualquer mudança em seus mecanismos de roteamento. Para isso existem várias técnicas que permitem que isso aconteça, incluindo: (PAMPLONA e TOKUNAGA, 2014)

- Tunelamento manual (Configurado): onde pacotes IPv6 são encapsulados em IPv4, sobre uma infraestrutura IPv4. Esses túneis são ponto a ponto que necessitam serem configurados manualmente. (HAGEN, 2002)
- Tunelamento automático: funciona somente em tunelamento de IPv6 para IPv4, pois, são utilizados em endereços privados. Este método permite a comunicação de pacotes e a passagem de IPv6 por uma estrutura IPv4. (MUN e LEE, 2005)

Segundo Nunes (2013), diversas técnicas de tunelamento, algumas já em desuso foram adotadas pela IETF (*Internet Assigned Numbers Authority*). As técnicas mais utilizadas em redes que requerem interoperabilidade são:

- Túnel Broker;
- 6to4;
- Teredo;
- ISATAP.

## 4. MATERIAIS E MÉTODOS

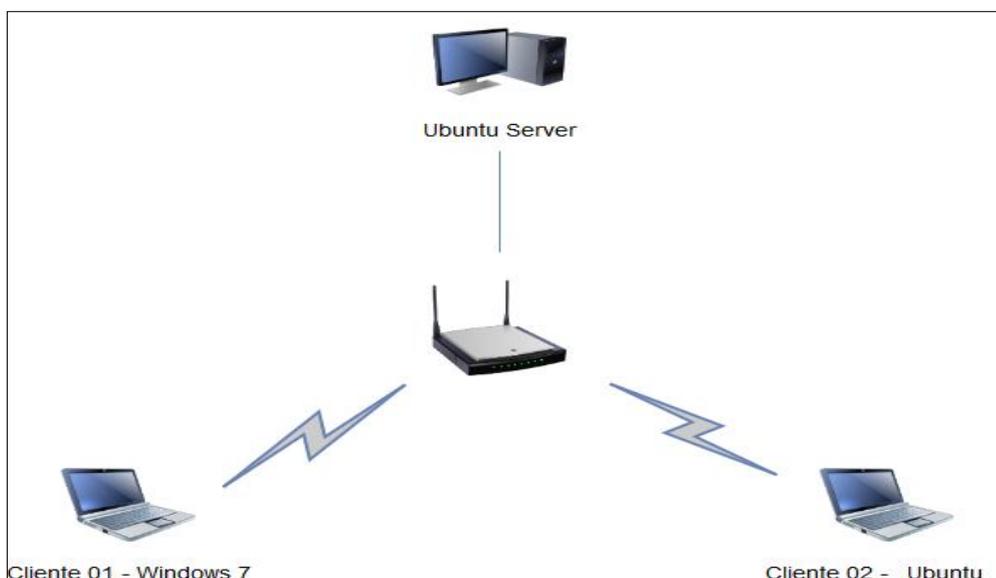
Esse capítulo apresenta a topologia usada para as análises, os dispositivos que compõem as redes e também os cenários utilizados para o estudo, detalhadamente.

### 4.1 Topologia e Equipamentos Utilizados

A Figura 08, representa como foi construída a rede utilizada para realizar os testes e as análises de desempenho, que é composta de 01 *desktop* com Linux *Ubuntu*, sendo o servidor, conectado cabeado diretamente no roteador e outros 02 notebooks, um com, Windows 7 e outro com Linux *Ubuntu*, sendo os *clients*, conectados via Wi-Fi, em um roteador que aceita uma configuração de IP no formato IPv4 e IPv6. A análise será realizada utilizando primeiramente IPv4 puro, e em seguida IPv6 puro.

Essa rede, possui os clientes conectados via Wi-Fi, sendo assim, sua resposta é um pouco diferente quando comparada com uma rede cabeada. Foi decidido utilizar esse tipo de conexão, porque é o mais usado em grandes, médias ou pequenas empresas, em questão de mobilidade e praticidade, quando se utiliza um notebook, pode se deslocar livremente para qualquer ponto da empresa sem se preocupar se terá acesso ao cabeamento ou não.

Figura 08 - Topologia de rede utilizada para os testes.



Fonte: O autor.

O quadro 02, detalha os hardwares dos dispositivos utilizados na topologia apresentada:

Quadro 02 - Configurações dos Dispositivos Utilizados.

Dispositivos Utilizados	
Tipo	Descrição dos Dispositivos
Roteador	TP-Link Dir 615 (N300)
Desktop	Intel i5 4430 3.2 Ghz 8GB RAM 1TB
Notebook_01	Intel Core 2 duo 2.3 Ghz 4GB RAM 500 GB
Notebook_02	Intel i3 Dual Core 2.1 GHz 4GB RAM 500 GB

Fonte: O autor.

## 4.2 Cenários Utilizados Para as Análises

A topologia apresentada no tópico anterior, foi utilizada nos dois cenários deste trabalho. Lembrando que os cenários abaixo foram aplicados em todos os computadores que foram utilizados para o estudo.

- **Cenário 1 – Rede IPv4 Pura:** Neste cenário, todas as funções de IPv6, como DHCPv6 do roteador, responsável por disponibilizar um endereço IPv6 para as máquinas foram desabilitados, restando somente a função de IPv4, assim, tornando a rede IPv4 pura, onde foram realizadas as medições de latência, perda de pacotes e vazão.
- **Cenário 2 – Rede IPv6 Pura:** Neste cenário, todas as funções de IPv4, como DHCPv4 do roteador, responsável por disponibilizar um endereço IPv4 para as máquinas foram desabilitados, restando somente a função de IPv6, assim, tornando a rede IPv6 pura, onde foram realizadas as medições de latência, perda de pacotes e vazão.

## 5. ESTUDO DE CASO

Como o foco deste trabalho é a utilização do IPv4 e IPv6 em uma rede real, o estudo de caso foi baseado em um servidor para transferência de arquivos, pensando em um ambiente corporativo, onde pode-se ter uma ou mais pastas para compartilhamento de arquivos usados no dia-a-dia.

Para esse estudo de caso, foi utilizado a criação de um servidor Samba, em ambiente Linux *Ubuntu*, para realizar as transferências de arquivos.

O Samba é um sistema servidor para Linux (e outros sistemas baseados em Unix), ele permite o compartilhamento e gerenciamento de recursos entre os computadores. Pode ser usado como servidor de armazenamento de arquivos, servidor de impressão, entre outros. É usado para fazer a comunicação entre computadores Windows *versus* Linux.

Dentre suas funcionalidades, pode-se destacar como principais:

- Compartilhamento de arquivos, diretórios, impressoras, com máquinas que possuem Windows;
- Controle total de acessos e privilégios;
- Pode-se configurar através de um ambiente remoto.

A principal vantagem de um servidor Samba, é simular um servidor Windows, mais precisamente as distribuições do Windows Server, quando colocado na balança o custo x benefício, o servidor Samba leva a vantagem.

O SAMBA é um serviço muito útil, tendo em vista a necessidade de compartilhamento de informações e sistemas de autenticação que possam integrar diferentes tipos de tecnologias, tais como: Windows e Linux. É comum encontrar-se que utilizam computadores com sistemas operacionais de plataformas diferentes, o serviço SAMBA vem se mostrando uma eficiente ferramenta para suprir as necessidades de grande parte dos administradores de redes, que sabem da importância da integração harmônica entre plataformas distintas em uma rede. (CAMPOS, 2006)

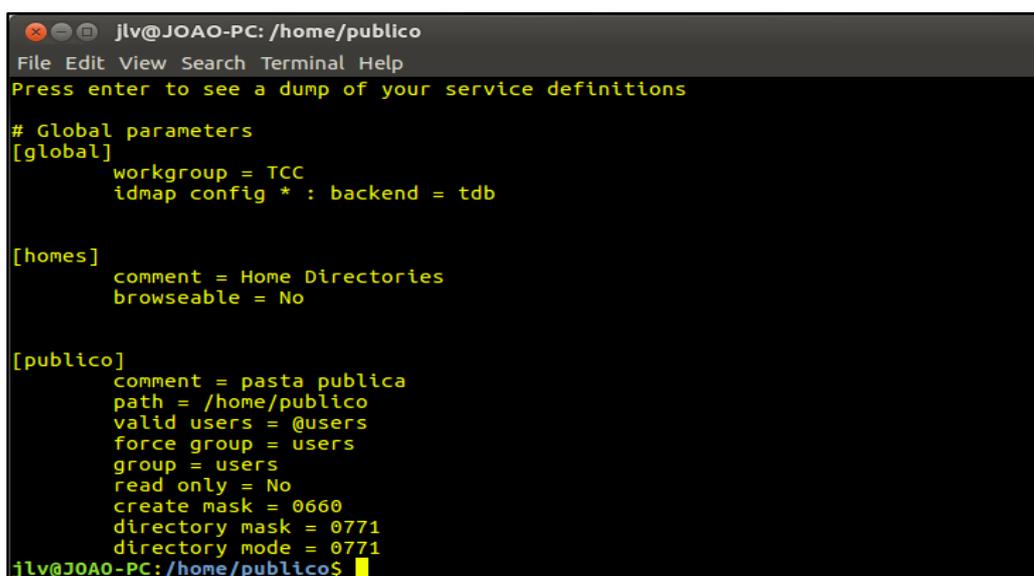
De acordo como Campos (2006) descreve, o SAMBA é um pacote de software que foi desenvolvido a partir da necessidade de interação entre as

diferentes plataformas de sistemas operacionais, visando desta forma facilitar a vida dos administradores de rede, que nem sempre administram redes com tecnologias totalmente homogêneas. É um exemplo de software servidor livre que vem conquistando o mercado em larga escala, pela sua eficiência e por tudo que oferece desde o seu desenvolvimento, em 1992.

Após a instalação do servidor, deve-se fazer ou alterar a configuração através do arquivo “*SMB.CONF*”, localizado em */etc/samba/smb.conf*, utilizando o editor de arquivos que a pessoa preferir, *nano*, *vi*, etc.

Neste estudo, foi realizada uma configuração simples, somente pensando no servidor de transferência de arquivos, não foi configurado um servidor de impressora. A configuração ficou da seguinte maneira, como mostra a figura 09 a seguir.

Figura 09 - Configuração do servidor Samba.



```
jlv@JOAO-PC: /home/publico
File Edit View Search Terminal Help
Press enter to see a dump of your service definitions

# Global parameters
[global]
    workgroup = TCC
    idmap config * : backend = tdb

[homes]
    comment = Home Directories
    browseable = No

[publico]
    comment = pasta publica
    path = /home/publico
    valid users = @users
    force group = users
    group = users
    read only = No
    create mask = 0660
    directory mask = 0771
    directory mode = 0771
jlv@JOAO-PC: /home/publico$
```

Fonte: O autor.

Explicando rapidamente as configurações, a seção [global] indica alguns parâmetros que afetam todo o servidor, por exemplo, o nome do servidor.

Seção [homes] contém as configurações do diretório home, para cada usuário.

Seção [público] contém a configuração para a pasta que será

compartilhada, seu caminho, grupo de usuários aptos a acessar esse conteúdo, nesse caso serão todos do grupo @users, e as permissões que eles possuírem.

Para este estudo de caso, utilizamos como servidor, uma máquina Linux Ubuntu e como clientes, as máquinas contendo Windows 7 e 8. Lembrando que o propósito de um servidor Samba para o compartilhamento de arquivos, é fazer essa comunicação entre Windows e Linux.

O servidor foi configurado como mostrado na figura anterior e nele contém alguns arquivos, como imagens, vídeos, músicas, etc, que geralmente são os tipos de arquivos mais compartilhados em uma rede. A figura 10 exibe os arquivos contidos nesse servidor e o tamanho total da pasta no momento do teste.

Figura 10 - Arquivos contidos no servidor Samba.

```
jlv@JOAO-PC:/home/publico$ ls -l
total 26380144
-rw-rw-r-- 1 jlv jlv 1716429981 Ago 26 16:34 Game.of.Thrones.S07E01.1080p.WEBRip.H264-TBS.DUAL-RK.tar.gz
-rw-rw-r-- 1 jlv jlv 4638591650 Ago 26 16:38 Game.of.Thrones.S07E03.1080p.WEB-DL.DD+S.1.H.264-GoT.DUAL-BARRY.tar.gz
-rw-rw-r-- 1 jlv jlv 3343267886 Ago 26 16:42 Game.of.Thrones.S07E04.1080p.WEB-DL.DD+S.1.H.264-GoT.DUAL-BARRY.tar.gz
-rw-rw-r-- 1 jlv jlv 3442416714 Ago 26 16:45 Game.of.Thrones.S07E05.1080p.WEBRip.DDP5.1.x264-GoT.DUAL-RK.tar.gz
-rw-rw-r-- 1 jlv jlv 2353732661 Ago 26 16:47 Game.of.Thrones.S07E06.1080p.HDRip.x264.AC3-Manning.tar.gz
-rw-rw-r-- 1 jlv jlv 4985178153 Ago 26 16:46 OnePiece.tar.gz
-rw-r--r-- 1 root root 816286722 Jun 27 23:06 Pictures.tar.gz
-rw-rw-r-- 1 jlv jlv 518173418 Ago 26 16:31 Prison.Break.S05E05.1080p.WEB-DL.x265.HEVC.6CH-MRN.tar.gz
-rw-rw-r-- 1 jlv jlv 520015036 Ago 26 16:32 Prison.Break.S05E06.1080p.WEB-DL.x265.HEVC.6CH-MRN.tar.gz
-rw-rw-r-- 1 jlv jlv 523876884 Ago 26 16:32 Prison.Break.S05E07.1080p.WEB-DL.x265.HEVC.6CH-MRN.tar.gz
-rw-rw-r-- 1 jlv jlv 516399926 Ago 26 16:32 Prison.Break.S05E08.1080p.WEB-DL.x265.HEVC.6CH-MRN.tar.gz
-rw-rw-r-- 1 jlv jlv 525665440 Ago 26 16:28 Prison.Break.S05E09.1080p.WEB-DL.x265.HEVC.6CH-MRN.tar.gz
-rw-rw-r-- 1 jlv jlv 311028 Jun 27 22:34 Screenshot from 2017-06-27 22-33-31.png
-rw-rw-r-- 1 jlv jlv 1227424 Jul 1 17:50 Screenshot from 2017-07-01 17-50-06.png
-rw-rw-r-- 1 jlv jlv 948901 Jul 1 17:51 Screenshot from 2017-07-01 17-50-53.png
-rw-rw-r-- 1 jlv jlv 179269 Jul 1 17:54 Screenshot from 2017-07-01 17-53-59.png
-rw-rw-r-- 1 jlv jlv 1512387 Jul 1 18:03 Screenshot from 2017-07-01 18-03-24.png
-rwxrwxr-x 1 jlv jlv 2226846870 Jul 1 17:44 Supernatural2.tar.gz
-rwxrwxr-x 1 jlv jlv 877610460 Jul 1 17:45 Supernatural.tar.gz
-rw-rw-r-- 1 jlv jlv 339970 Jul 1 17:45 wallpaper-102115.jpg
-rw-rw-r-- 1 jlv jlv 213035 Jul 1 17:45 wallpaper-1572411.jpg
-rw-rw-r-- 1 jlv jlv 63840 Jul 1 17:45 wallpaper-1663364.jpg
-rw-rw-r-- 1 jlv jlv 262353 Jul 1 17:45 wallpaper-2430918.jpg
-rw-rw-r-- 1 jlv jlv 323362 Jul 1 17:45 wallpaper-2533254.jpg
-rw-rw-r-- 1 jlv jlv 638392 Jul 1 17:45 wallpaper-2982878.jpg
-rw-rw-r-- 1 jlv jlv 606973 Jul 1 17:45 wallpaper-301287.jpg
-rw-rw-r-- 1 jlv jlv 333702 Jul 1 17:45 wallpaper-401841.jpg
-rw-rw-r-- 1 jlv jlv 398703 Jul 1 17:45 wallpaper-486016.jpg
-rw-rw-r-- 1 jlv jlv 172354 Jul 1 17:45 wallpaper-536158.jpg
-rw-rw-r-- 1 jlv jlv 259122 Jul 1 17:45 wallpaper-701873.jpg
-rw-rw-r-- 1 jlv jlv 474950 Jul 1 17:45 wallpaper-71890.jpg
-rw-rw-r-- 1 jlv jlv 389968 Jul 1 17:45 wallpaper-753386.jpg
```

Fonte: O autor.

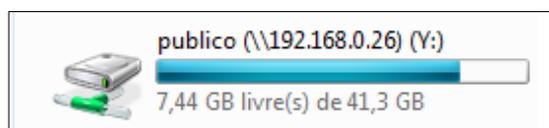
Após a criação do servidor Samba, os clientes podem se conectar no servidor Samba, pelo cmd do Windows ou pela barra de navegação dentro dos diretórios.

Para se conectar através da barra de navegação é usado somente “\ip\_do\_servidor” e apertar a tecla enter. Ao tentar conectar, será pedido o login para entrar no servidor, após confirmação do usuário, as pastas compartilhadas serão exibidas.

Para se conectar através do *cmd*, que foi o caso utilizado neste trabalho, é utilizado o comando “*net \* user ip\_do\_servidor A-Z*” (É escolhida uma letra que será utilizada como nome da nova partição de compartilhamento, neste trabalho foi utilizada a letra Y para mapear as unidades). Primeiramente foi mapeada uma unidade IPv4 e realizados os testes, em seguida, essa unidade IPv4 foi desconectada. Na sequência foi mapeada uma unidade IPv6 e os mesmos testes foram realizados.

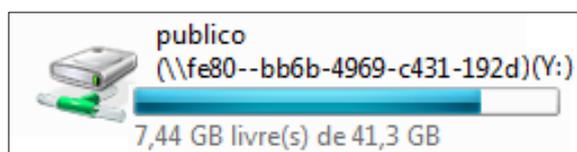
As Figuras 11 e 12 exibem os servidores IPv4 e IPv6 mapeados no sistema.

Figura 11 - Servidor Samba IPv4 mapeado no sistema.



Fonte: O autor.

Figura 12 - Servidor Samba IPv6 mapeado no sistema.



Fonte: O autor.

Após a unidade ser mapeada, o usuário tem acesso ao sistema de arquivos compartilhados. Neste estudo, todos os comandos foram utilizados pelo *cmd*, mas para isso foi criado um arquivo “.bat”, onde contém os comandos utilizados para realizar a transferência dos arquivos entre servidor Samba e servidor Windows.

A seguir, a figura 13 exhibe o conteúdo do arquivo “.bat”, utilizado para fazer as transferências dos arquivos.

Figura 13 - Conteúdo do arquivo .bat

```

1 @echo off
2 echo Inicio da Tranferencia: %time%
3 cd y:
4
5 copy y:One* C:\Users\User\Desktop\Copysamba
6 copy y:Game* C:\Users\User\Desktop\Copysamba
7 copy y:Pris* C:\Users\User\Desktop\Copysamba
8 copy y:Screenshot* C:\Users\User\Desktop\Copysamba
9 copy y:wallpaper* C:\Users\User\Desktop\Copysamba
10 copy y:Pictur* C:\Users\User\Desktop\Copysamba
11 copy y:Supernatu* C:\Users\User\Desktop\Copysamba
12
13
14 echo Final de transferencia: %time%
15 echo Obrigado!
16 pause

```

Fonte: O autor.

Após executar esse arquivo, a transferência será iniciada. A figura 14 exibe como fica o console do Windows ao término da execução do *script*.

Figura 14 - Exemplo de saída após transferências de arquivos (IPv4).

```

C:\WINDOWS\system32\cmd.exe
z:Prison.Break.S05E05.1080p.WEB-DL.x265.HEVC.6CH-MRN.tar.gz
  5 arquivo(s) copiado(s).
z:Screenshot from 2017-07-01 17-50-06.png
z:Screenshot from 2017-07-01 17-50-53.png
z:Screenshot from 2017-06-27 22-33-31.png
z:Screenshot from 2017-07-01 18-03-24.png
z:Screenshot from 2017-07-01 17-53-59.png
  5 arquivo(s) copiado(s).
z:wallpaper-486016.jpg
z:wallpaper-71890.jpg
z:wallpaper-753386.jpg
z:wallpaper-2430918.jpg
z:wallpaper-536158.jpg
z:wallpaper-1572411.jpg
z:wallpaper-1663364.jpg
z:wallpaper-301287.jpg
z:wallpaper-701873.jpg
z:wallpaper-2982878.jpg
z:wallpaper-102115.jpg
z:wallpaper-401841.jpg
z:wallpaper-2533254.jpg
  13 arquivo(s) copiado(s).
z:Pictures.tar.gz
  1 arquivo(s) copiado(s).
z:Supernatural2.tar.gz
z:Supernatural.tar.gz
  2 arquivo(s) copiado(s).
Final de transferencia: 23:45:07,61
Obrigado!
Pressione qualquer tecla para continuar. . .

```

Fonte: O autor.

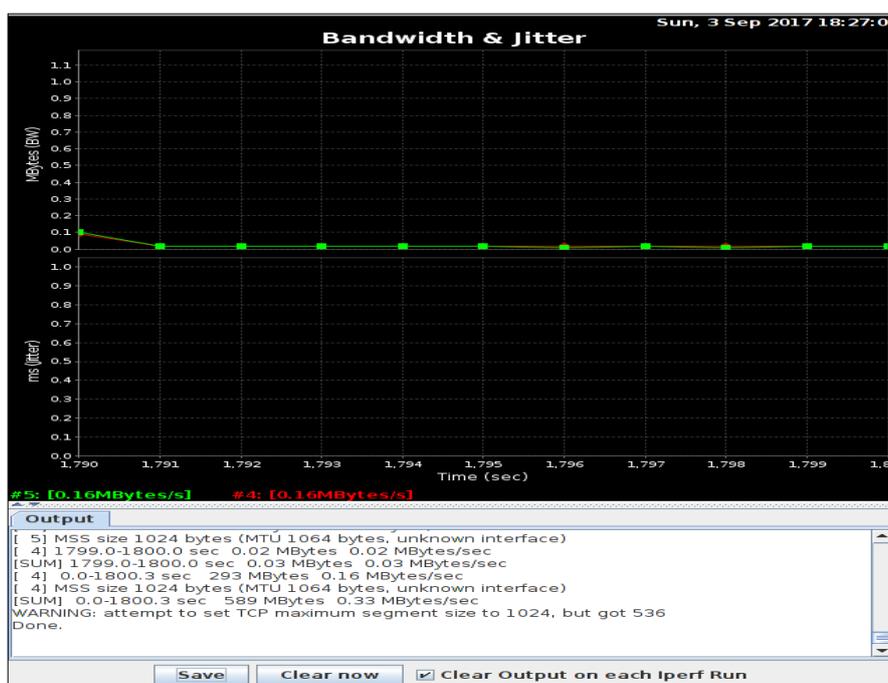
## 5.1 Teste de Desempenho e Métricas

Para realizar os testes deste estudo, foi utilizado o comando *ping*, através do terminal de comando do *Ubuntu* para medir perda de pacotes e latência. Também foi usado o *software* *Iperf*, para medir a vazão. O *software* *Iperf* é uma ferramenta de desempenho de rede versátil que pode ser usada nos ambientes *Linux* e/ou *Windows*. Sua especialidade é determinar os melhores tamanhos de janela TCP para conexões TCP, permitindo que o administrador do sistema configure hosts de rede para um ótimo desempenho. (BLUM, 2003, p. 115)

Para que as medições com o programa sejam realizadas, um dos computadores deverá estar programado no modo “*Server*”, nos demais computadores o *Iperf* deve ser executado no modo “*Client*”. Ao término dos testes, um arquivo “.*txt*” é gerado com os resultados experimentais. Para todos os dados deste estudo, deve-se consultar o DVD em anexo.

O *software* possui também um modo gráfico (*Jperf*), que permite uma melhor visualização enquanto os testes são realizados.

Figura 15 - Exemplo de Saída em modo Gráfico (*Jperf*).



Fonte: O autor.

## 5.2 Perda de Pacotes

Trata-se do número de pacotes enviados por um emissor, mas não recebidos pelo receptor, sendo, geralmente, obtido como um percentual de perda de pacotes na rede. Esse percentual é calculado com base no número total de pacotes perdidos dividido pelo total de pacotes enviados. (JUNIOR e SILVA, 2014)

A causa mais comum para este problema é o congestionamento da rede: ao trafegar do transmissor ao receptor, o pacote passa por *buffers* nos roteadores, sendo possível que estes estejam lotados e o roteador faça o descarte destes pacotes. (KUROSE e ROSS, 2010)

Para a medição de perda de pacotes, é utilizado o comando ping, que é utilizando também, para medir a latência. Neste estudo, foram lançados 21000 pacotes na rede, com tamanho de 750 bytes cada, durante aproximadamente 6 horas para cada ambiente.

No Cenário I – Rede IPv4 Pura, foram utilizados os seguintes comandos:

- **Cliente Ubuntu:** ping 192.168.0.26 -l 21000 -n 750 > PingIPv4.txt

No Cenário II – Rede IPv6 Pura, foram utilizados os seguintes comandos:

- **Cliente Ubuntu:** ping6 fe80::bb6b:4969:c431:192d -l 21000 -n 750 > PingIPv6.txt

Foi analisada a Perda de pacotes durante a transferência de arquivos em uma rede IPv4 e IPv6. A rede com o menor percentual de pacotes perdidos, é a mais eficiente nesse quesito.

## 5.3 Latência

O conceito de latência é o atraso de tempo entre o momento que um evento iniciou e o momento que os efeitos iniciam, ou seja, a latência de uma rede é medida como o atraso de ida e volta de um pacote. (CHESHIRE, 2006).

Segundo Filippetti (2008), pode-se expressar latência em rede de computadores como:

Latência: *tempo de transmissão + tempo de propagação.*

Dessa forma,

- Tempo de transmissão: *dimensão de pacotes (bits) / Velocidade de transmissão (bps)*
- Tempo de propagação: *Dimensão do Canal (Km) / Velocidade de propagação (km/s).*

Existem outros dois tipos de atraso que podem provocar a latência: o tempo de processamento e o tempo de enfileiramento. Porém, esses dois tempos só podem ser medidos em uma rede com utilização de tráfego significativamente elevado. (KUROSE, 2006)

Para isso, foi utilizado o comando *ping*, o mesmo utilizado para medição de perda de pacotes.

No Cenário I – Rede IPv4 Pura, foram utilizados os seguintes comandos:

- **Cliente Ubuntu:** `ping 192.168.0.26 -l 21000 -n 750 > PingIPv4.txt`

No Cenário II – Rede IPv6 Pura, foram utilizados os seguintes comandos:

- **Cliente Ubuntu:** `ping6 fe80::bb6b:4969:c431:192d -l 21000 -n 750 > PingIPv6.txt`

#### 5.4 Vazão (*Throughput*)

Throughput ou vazão trata-se da quantidade de dados transferidos de um ponto a outro da rede em um determinado período de tempo. (JUNIOR e SILVA, 2014).

De acordo com Leal (2010), a vazão de um sistema geralmente aumenta à medida que a carga do sistema aumenta. Assim que o valor da carga alcança determinado valor, ela pode parar de aumentar, onde na maioria dos casos pode até diminuir.

Os fatores que interferem no *throughput* são (FOROUZAN, 2006):

- Topologia de rede;

- Número de usuários;
- Sistema operacional;
- Taxa das interfaces de rede.

Resumidamente a vazão, pode ser descrita como a velocidade em que os dados trafegam pela rede. Essa taxa de transferência pode ser menor do que a largura de banda, devido às perdas e atrasos. (NUNES, 2013)

Para os testes desse experimento, foi utilizado uma configuração padrão do Iperf, mas deixando configurado 2 conexões simultâneas e 21000 pacotes sendo lançados na rede.

No Cenário I – Rede IPv4 Pura, foram utilizados os seguintes comandos:

- Servidor IPv4: `-s -P 2 -i 1 -m -p 5001 -w 56K -M 1.0K -l 2.0M -f M`
- Cliente IPv4: `-c 192.168.0.26 -P 2 -i 1 -m -p 5001 -f M -t 21000`

No Cenário II – Rede IPv6 Pura, foram utilizados os seguintes comandos:

- Servidor IPv6: `-s -P 2 -i 1 -m -p 5001 -V -w 56K -M 1.0K -l 2.0M -f M`
- Cliente IPv6: `-c fe80::bb6b:4969:c431:192d -P 2 -i 1 -m -p 5001 -V -f M -t 21000`

## 6.RESULTADOS EXPERIMENTAIS

Neste tópico, será apresentado os resultados obtidos durante a fase de transferência dos arquivos, enquanto as medições de latência, perda de pacotes e vazão foram executadas com as configurações descritas no capítulo 5.

Os resultados obtidos serão apresentados nos cenários I e II:

### **Cenário I - Rede IPv4 Pura:**

- Perda de pacote: Foram enviados 21000 pacotes, 20236 recebidos com sucesso e 764 perdidos, uma taxa de 3.63% de perda;
- Latência: A latência média para o envio destes mesmos 21000 pacotes foi de 152.112ms, com um máximo de 8667.788ms;
- Vazão: Foram feitas 21000 repetições, atingindo uma média de 0.50 MBytes/sec e transferência máxima de 0.99 Mbytes/sec.

### **Cenário II - Rede IPv6 Pura:**

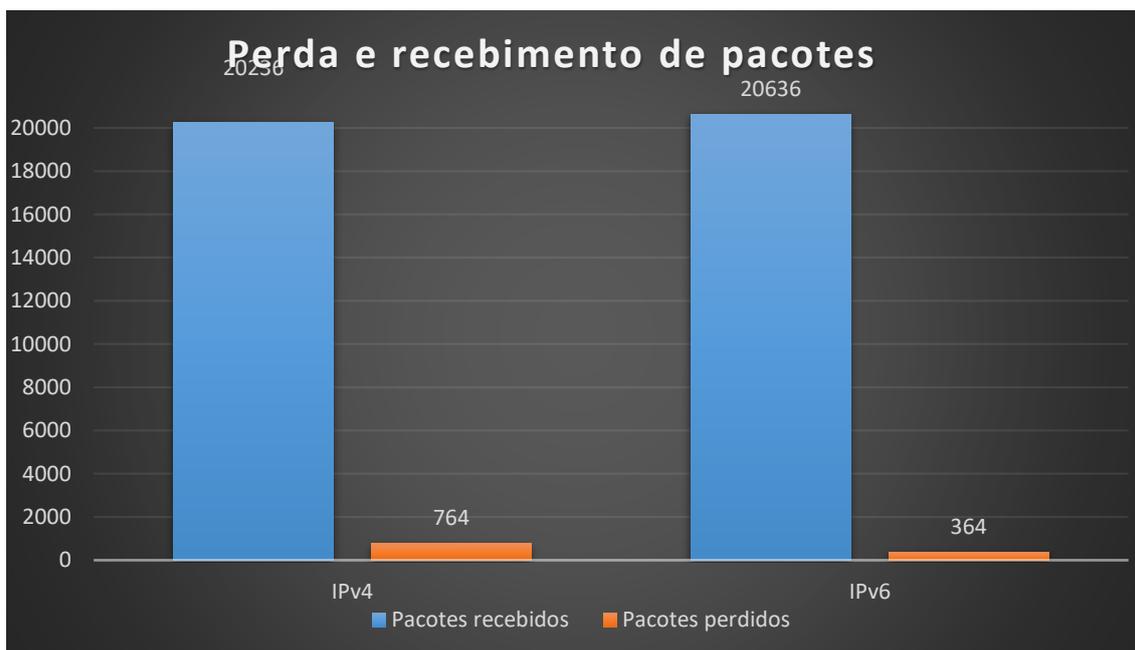
- Perda de pacote: Foram enviados 21000 pacotes, 20636 recebidos com sucesso e 364 perdidos, uma taxa de 1.73% de perda;
- Latência: A latência média para o envio destes mesmos 750 pacotes foi de 149.942ms, com um máximo de 8574.090ms;
- Vazão: Foram feitas 21000 repetições, atingindo uma média de 0.64 MBytes/sec e transferência máxima de 1.36 Mbytes.

### **6.1 Análise dos Resultados**

Neste tópico, serão apresentados de uma maneira gráfica, os resultados obtidos durante o estudo, a comparação entre os dois protocolos após os testes realizados, e qual foi melhor ou pior em cada tipo de teste e ambiente utilizado.

A análise de perda de pacotes será apresentada no gráfico 01 a seguir:

Gráfico 01 - Representação da perda de pacotes.



Fonte: O autor.

No gráfico acima, podemos ver a representação no quesito de perda de pacotes em cada um dos protocolos utilizados. O protocolo IPv6 foi um pouco melhor nesse teste, mais precisamente, o IPv6 se mostrou 1.9% melhor que o IPv4 nesse teste, em relação a perda total de pacotes. Lembrando que no teste foram enviados 21000 pacotes, com 750 bytes de dados cada um, quanto maior a rede e o número de requisições, maior será essa diferença.

A seguir, no gráfico 02 será apresentado os resultados do teste de latência:

Gráfico 02 - Representação da latência.

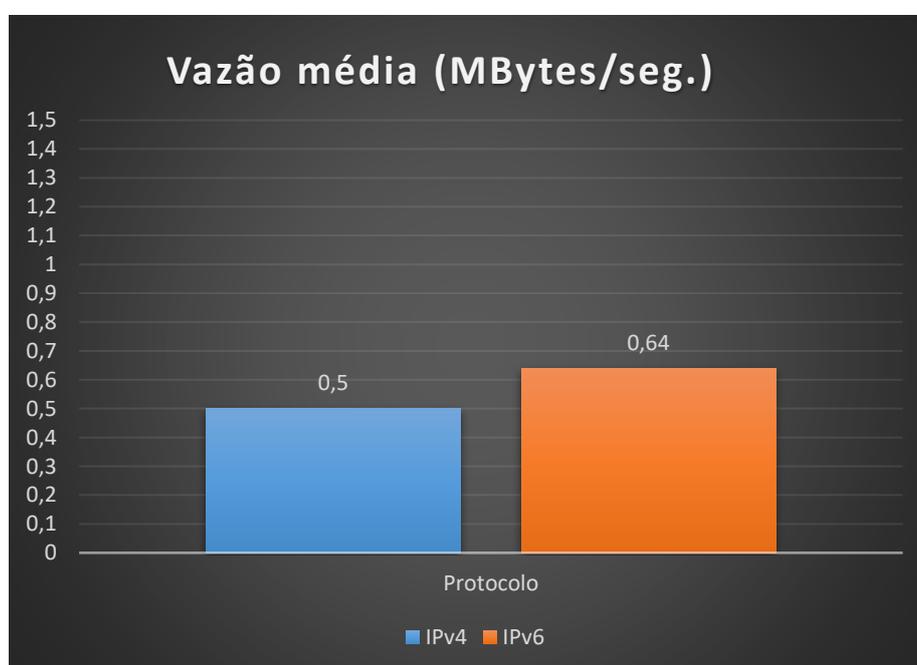


Fonte: O autor.

No gráfico anterior, podemos comparar a média de latência entre os protocolos IPv4 e IPv6 durante a transferência dos arquivos. O IPv6, se mostrou melhor também nesse quesito. Enquanto o IPv4 obteve uma média de 152.112ms, o IPv6 obteve 149.942ms, tendo menos *delay* durante a entrega destes pacotes. Se analisarmos, é uma diferença pequena, mas se colocada em uma rede de grande porte, com mais usuários, essa diferença irá aumentar.

A seguir, no gráfico 03, será apresentado o resultado obtido no teste de vazão:

Gráfico 03 - Representação da vazão média.



Fonte: O autor.

De acordo com o gráfico acima, o IPv6 obteve um desempenho de 0.14 Mbytes/segundo superior a rede IPv4, com 0.50 Mbytes/seg.

Comparando com a latência, a vazão teve uma diferença um pouco mais significativa.

## 6.2 Discussões dos Experimentos

Com o IPv4 chegando praticamente ao seu fim, o IPv6 se mostra capaz de suprir todas as necessidades, de acordo com o experimento realizado, no

questo perda de pacotes, não foi notada grande diferença entre os dois protocolos, porém, quando comparado a latência e a vazão, foi obtido um valor mais significativo, o que pode ser um diferencial na escolha do cenário que será utilizado por um administrador de rede.

Em todos os testes realizados neste trabalho, o IPv6 se mostrou superior, para o serviço de transferência de arquivos, no qual é o foco desse trabalho.

Além dos testes e das métricas obtidas, este trabalho também contribui para com que o administrador de rede entenda melhor sobre as topologias de rede e seu uso, sugestão de mudança entre os protocolos IPv4 e IPv6, além do uso da ferramenta *Jperf*, para análise da rede.

Hoje em dia temos equipamentos e ferramentas que disponibiliza a comunicação entre ambos os protocolos.

## 7. CONCLUSÃO E TRABALHOS FUTUROS

Depois dos experimentos realizados ao longo deste trabalho, os dois protocolos se mostraram parecidos apenas no quesito de latência, nos outros testes, o IPv6 se mostrou significativamente superior.

Lembrando que esse experimento foi realizado em uma rede Wi-Fi, porque é o modelo que mais usamos hoje em dia nas empresas, o computador desktop está ficando cada dia mais escasso no ambiente de trabalho de empresas de médio e grande porte, devido a mobilidade que o notebook possui.

Nesse teste, também deve ser levado em consideração que esse experimento foi realizado em uma rede de pequeno porte, quanto maior a estrutura, maiores serão as perdas ou ganhos obtidos.

Então, para o serviço de transferência de arquivos em um servidor Samba, o IPv6 se mostrou significativamente superior e deve ser levado em consideração quando o assunto for esse tipo de serviço. Dependendo da quantidade e tamanho dos dados do cliente, a agilidade obtida com esse protocolo pode ser muito grande.

Esse estudo teve o intuito de obter métricas para uma análise de desempenho e um estudo de caso em um ambiente que é bastante utilizado, ainda mais nos dias de hoje, onde a quantidade de dados trafegando pelas redes é quase incalculável.

Com esses dados em mãos, um administrador de rede pode saber a arquitetura que mais parecer eficiente para o determinado trabalho ou tarefa, sempre pensando na satisfação do cliente.

Hoje em dia existe o suporte total para o IPv6, porém pelo gasto que se tem mudando toda uma arquitetura de rede e com treinamento de profissionais para que aprendam trabalhar com esse protocolo, ou até contratar profissionais que já saibam trabalhar com esse protocolo de rede, às vezes as empresas preferem continuar com o IPv4, que apesar de, estar chegando ao seu fim, ainda é mais confortável para os donos dessas empresas.

De qualquer forma, como foi dito no capítulo 3.4.1 deste trabalho, o NAT ainda mantém o IPv4 vivo, permitindo que, com um único endereço IP ou um número pequeno deles, vários hosts possam trafegar na internet, assim, prolongando a vida útil do IPv4, que apesar de estar em escassez, ainda será utilizado por um bom tempo.

Para trabalhos futuros podem haver diversos testes entre esses dois protocolos, em diversos ambientes, como jogos online, etc, porém é necessário um estudo mais específico, tais como as ferramentas necessárias para dar continuidade a essas análises.

## 8. REFERÊNCIAS

AMARAL, Allan F. F., **Rede de Computadores**: Colatina/ES: Instituto Federal do Espírito Santo, 2012.

BARCELL, M. F., **Protocolo TCP/IP**: transparência de classe. Facultad de Ciencias Sociales y de la Comunicación. Universidad de Cádiz, 2014.

BRAGA, F. G. **A continuidade da Internet passa pelo IPv6**. Faculdade de Tecnologia do Estado de São Paulo. São Paulo/SP, 2011.

BRITO, Samuel H. B., **IPv6 - O Novo Protocolo da Internet**. São Paulo/SP. Editora: Novatec, p. 157, 2013.

BURGESS, Mark. **Princípios de Administração de Redes e Sistemas**. São Paulo/SP. 2ª ed.: LTC, 2006.

BRAGA, L. A.G. M., **Estudo de Convergência de Redes**. São Carlos/SP: Escola de Engenharia de São Carlos, 2011.

COMER, Douglas E. **Interligação de redes com TCP/IP**. Rio de Janeiro/RJ, Vol. 1, 5ª Ed., 2006.

Comer, Douglas E. **Redes de Computadores e Internet**. Tradução: Marinho Barcellos. Porto Alegre/RS, 2001.

DANTAS, Mario. **Tecnologia de Redes de Comunicação e Computadores**. Rio de Janeiro/RJ. Ed. Axcel Books do Brasil Ltda, 2002.

FILIPPETTI, Marco A. **CCNA 4.1 - Guia Completo de Estudo**. Florianópolis/SC, Editora Visual Books, 2008.

FOROUZAN, Behrouz A., **Protocolo TCP/IP**. São Paulo/SP. 3ª Edição, 2012.

FREITAS, R. N.; TERENCE, A. C.; **Estudo sobre a viabilidade de uso de NAT em IPv6**. FATEC – Faculdade Tecnológica. Americana/SP, 2016.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a Internet: uma abordagem to-down**. São Paulo/SP, 2011.

MAZZOLA, Vitório B., **Arquitetura de Rede De Computadores**. Florianópolis/SC. Universidade Federal de Santa Catarina, 2000.

MIOTELLI, A.; CASAGRANDE, R. A. **Estudo da Transição entre Protocolos de Comunicação IPv4 e IPv6**. Criciúma/SC. Universidade do Extremo Sul Catarinense, 2013.

NASCIMENTO, Edmar José do. **Introdução a rede de computadores**. Petrolina/PE. Universidade Federal do Vale do São Francisco, 2011.

NASSIF, A. T., SOARES, A. J. M., **Convergência das redes de comunicação: aspectos técnicos e econômicos**. Universidade de Tarapacá. Chile. Volume 13. 2005.

NUNES, Sérgio E. **Análise de Impacto na Transição entre os Protocolos de Comunicação IPv4 e IPv6**. Campinas/SP, Universidade Estadual de Campinas, 2013.

PERLIN, Tiago; CRISTO, Fernando de; FRANCISCATTO, Roberto. **Rede de Computadores**. Rede e-Tec Brasil. Frederico Westphalen/RS, 2014

PINHEIRO, José Maurício. **Guia Completo de cabeamento de redes**. Ed. Elsevier Ltda. Rio de Janeiro/RJ, 2003.

PAMPLONA, E. G., TOKUNAGA, R. K. **Transição IPv4/IPv6: Técnica de tunelamento**. Universidade Tecnológica e Federal do Paraná. Curitiba/PR. 2014.

SANTOS, R. R. **Curso de IPv6 básico**. 1ª ed. São Paulo/SP, 2009.

SOUSA, Lindeberg B., **Rede de computadores: dados, voz e imagem**. 8 Ed. São Paulo/SP. Editora Érica Ltda. 2005.

SCRIMGER, R. et. al. **TCP/IP: A Bíblia**. Rio de Janeiro/RJ. Ed. Elsevier, 2002.

RIOS, Renan Osorio. **Protocolos e Serviços de Rede: curso técnico em informática**. Colatina/ES, 2012.

REISSWITZ, Flávia. **Tecnologia Web e Redes**. Análise de Sistemas Volume 2. Ed. Clube de autores. Rio de Janeiro/RJ, 2012.

GUERBER, Carlos. **Rede de Computadores**: topologia de rede. Universidade do Contestado. Rio Negrinho/SC, 2009.