UNIVERSIDADE FEDERAL DO PARÁ

FACULDADE DE COMPUTAÇÃO

CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

DAVID RAFAEL AIRES DE AZEVEDO

ANÁLISE E DESEMPENHO DE REDES METROPOLITANAS: UTILIZANDO O SIMULADOR CISCO PACKET TRACER 5

CASTANHAL - PARÁ

2022

DAVID RAFAEL AIRES DE AZEVEDO

ANÁLISE E DESEMPENHO DE REDES METROPOLITANAS: UTILIZANDO O SIMULADOR CISCO PACKET TRACER 5

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Sistemas de Informação da Universidade Federal do Pará, como requisito para obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Prof. Dr. José Jailton Henrique Ferreira Júnior.

CASTANHAL - PARÁ

2022

DAVID RAFAEL AIRES DE AZEVEDO

ANÁLISE E DESEMPENHO DE REDES METROPOLITANAS: UTILIZANDO O SIMULADOR CISCO PACKET TRACER 5

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Sistemas de Informação da Universidade Federal do Pará, como requisito para obtenção do grau de Bacharel em Sistemas de Informação.

APROVADA EM: 09 / 05 / 2022

BANCA EXAMINADORA:

_____

Prof. Dr. José Jailton Henrique Ferreira Júnior

(Orientador – FACOMP/UFPA)

_____

Prof. Dr. Tássio Costa de Carvalho

(Avaliador Interno – FACOMP/UFPA)

_____

Prof. Dr. Igor Ruiz Gomes

(Avaliador Interno – FACOMP/UFPA)

AGRADECIMENTOS

Em primeiro lugar, gostaria de agradecer a Deus que até aqui me sustentou com saúde e esteve sempre me provendo sabedoria e oportunidades de crescimento, amparando me nos momentos difíceis e nunca me abandonando.

Em segundo lugar, à minha família, em especial a minha mãe: Eliane Ayres, meu pai David Azevedo e Meu Irmão Kaio Azevedo que estão a todo momento dando-me forças e se colocando como meus principais incentivadores.

Em seguida, gostaria de agradecer ao meu orientador Professor Doutor José Jailton Junior por todo conhecimento compartilhado comigo, além da enorme paciência e da atenção dada a mim não só na realização deste trabalho, mas também durante minha vida acadêmica, levo este grande mestre como um amigo para minha vida.

À minha amiga mestranda Adrianne Veras de Almeida que me deu um suporte imenso e contribuiu muito com sua experiência em pesquisas acadêmicas, auxiliando-me e clareando-me a mente em muitos pontos.

Aos meus amigos e colegas de curso com quem compartilhei experiências, conhecimento nessa fase da minha vida que foi incrível.

À todos os professores e colaboradores da Universidade federal do Pará/ campus castanhal onde pude vivenciar momentos marcantes e de muito aprendizado, agradeço pela paciência, pelos ensinamentos e exemplos passados a mim.

Às pessoas que me deram oportunidades e instituições por onde pude está exercendo os meus conhecimentos e também aprendendo ainda mais, a toda equipe do Colégio Conexão, Mercúrio Alimentos, Ave Center, Câmara Municipal de Santa Izabel do Pará, Instituto Vitória Régia e ao Grupo Mateus.

À minha amiga Licenciada em Pedagogia Geiziane Lima que sempre me manteve informado e atualizado sobre os informes da Faculdade e ajudou muito, facilitando o entendimento de alguns procedimentos e me dando bons conselhos e opiniões.

Ao meu amigo Professor de Língua Portuguesa Robert Freitas que estendeu a mim um pouco da sua experiência e conhecimento.

RESUMO

Com o auxílio da ferramenta de simulação de redes Cisco Packet Tracer 5, irá se reproduzir, neste trabalho, um modelo de rede metropolitana que interligue a matriz e três filiais de uma suposta empresa e que estas também estejam interligadas, cada uma com sua rede local com características e configurações próprias. Usando também a aplicação de simulação para realizar testes como ping e traceroute e assim coletar dados do projeto para serem analisados e servirem de base para decisões de melhor configuração ou ajuste na execução do propósito.

Através da simulação, pretende-se reduzir erros, custos e o tempo de aplicação de um projeto real, além de se otimizar o projeto antes mesmo dele ser executado. Pois, na simulação já será identificada quaisquer dificuldades e atrasos e nela já se pode aplicar mudanças que resultem em melhorias nos resultados finais. Dessa forma, a intenção deste trabalho é mostrar que através das simulações de um projeto de rede, antes da sua própria execução, ganha-se tempo e recursos.

Palavras-chave: Redes, Simulação, Cisco Packet Tracer 5, Ping, Traceroute.

ABSTRACT

With the help of the Cisco Packet Tracer 5 network simulation tool, this work will reproduce a metropolitan network model that interconnects the headquarters and three branches of a supposed company and that these are also interconnected, each with its local network with its own features and settings. Also using the simulation application to perform tests such as ping and traceroute and thus collect project data to be analyzed and serve as a basis for decisions for better configuration or adjustment in the execution of the purpose.

Through the simulation, it is intended to reduce errors, costs and the application time of a real project, in addition to optimizing the project even before it is executed. Because, in the simulation, any difficulties and delays will be identified and changes can already be applied that result in improvements in the final results. Thus, the intention of this work is to show that through the simulations of a network project, before its own execution, time and resources are saved.

Keywords: Networks, Simulation, Cisco Packet Tracer 5, Ping, Traceroute.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AS	Autonomous Systems - Sistemas Autônomos
BGP	Border Gateway Protocol - Protocolo de Gateway de Borda
BSD	Berkeley Software Distribution - Distribuição de software de Berkeley
DHCP	Dynamic Host Configuration Protocol - Protocolo de configuração dinâmica de host
DNS	Domain Name System - Sistema de Nome de Domínio
EGP	Exterior Gateway Protocol - Protocolo de Gateway Exterior
FTP	File Transfer Protocol - Protocolo de Transferência de Arquivo
ICMP	Internet Control Message Protocol - Protocolo de Mensagens de Controle de Internet
IGP	Interior Gateway Protocol - Protocolo de Gateway Interior
IP	Internet Protocol - Protocolo de Internet
IPV4	Protocol version 4 - Versão do protocolo 4
IPV6	Protocol version 6 - Versão do protocolo 6
IS-IS	Intermediate System to Intermediate System
LAN	Local Area Networks - Redes Locais
MAC	Media Access Control - Controle de acesso de mídia
MAN	Metropolitan Area Network - Rede de Área Metropolitana
OSC'S	Civil Society Organizations - Organizações da Sociedade Civil
OSI	Open System Interconnection - Interconexão de sistemas abertos
OSPF	Open Shortest Path First - abrir o caminho mais curto primeiro
PING	Packet Internet Network Groper - Agrupador de pacotes da internet
QOS	Quality of Service - Qualidade de Serviço
RIP	Routing Information Protocol - Protocolo de Informações de Roteamento
RTT	Round Trip Time -Tempo de ida e volta
TCP	Transmission Control Protocol - Protocolo de Controle de Transmissão
TOS	Type of Service - Tipo de Serviço
TTL	Time-to-live - Tempo de Vida
UDP	User Datagram Protocol - Protocolo de datagrama do usuário
VLAN	Virtual Local Area Network - rede local virtual
XNS	Xerox Network System - Sistema de Rede Xerox

SUMÁRIO

1. INTRODUÇÃO

Com a constante evolução das tecnologias e a crescente geração de informação, é cada vez maior a busca por ferramentas que aperfeiçoem a comunicação, o armazenamento de dados e que facilitem a rotina das pessoas e das sociedades modernas. As redes de computadores, hoje em dia, são sem dúvida grandes ferramentas atuais que contribuem nesta busca.

Concernente a isso, as redes MAN's (Redes Metropolitanas) são ferramentas que dão suporte para que empresas, repartições públicas, OSC's e outras instituições possam se comunicar entre vários prédios, fábricas, campus e etc. basicamente, as redes MAN's interligam várias Redes Lan's (Redes de Área Local), sendo o canal de comunicação de Matrizes com filiais, núcleos e extensões de uma instituição só.

Contudo, por conta da maneira como é formada uma rede Man, pode-se ter diversos problemas, falhas de comunicação, perda de dados, insegurança, indisponibilidade e outros. Com isso, surge a necessidade de criar modelos de teste simulados e aplicar métricas para sanar ou até reduzir os possíveis problemas de uma nova rede MAN e também sugerir adoção de medidas que possam melhorar a utilização desse tipo de rede.

1.1 Objetivo Geral

Demonstrar como a aplicação da ferramenta de simulação de redes de computadores Cisco Packet Trace vai encontrar as possíveis dificuldades na implantação, gerência e escalabilidade de uma rede metropolitana de computadores (MAN).

1.2 Objetivos específicos

- ✓ Descrever os principais protocolos que irão ser usados na construção da simulação;
- ✓ Analisar resultados de testes de conexão e roteamento;
- ✓ Evidenciar as principais vantagens de se utilizar uma ferramenta de simulação;
- ✓ Recomendar melhores opções de configuração, organização, estrutura e reduzindo também os erros na aplicação do projeto.

1.3 Estrutura

O trabalho está organizado na seguinte estrutura: o segundo capítulo fez-se tecido a partir dos pressupostos teóricos que embasaram esta produção, apresentando conceitos referentes ao estudo de rede de computadores. O Terceiro capítulo volta-se para a apresentação da metodologia aplicada para a coleta de dados e obtenção dos resultados, este também apresenta o simulador Cisco Packet Tracer e as configurações aplicadas no projeto. No quarto capítulo serão expostas as telas com as simulações e teste feito nas mesmas e as tabelas de roteamento dos principais roteadores que estão presentes nas análises. Por fim, no quinto capítulo há a disposição das considerações finais desta pesquisa, seguida da visão geral do projeto, dos resultados obtidos, das dificuldades encontradas para realização do trabalho e as recomendações para trabalhos futuros.

2. FUNDAMENTAÇÃO TEÓRICA

Neste capítulo serão abordados os elementos introdutórios relacionados ao estudo de redes de computadores de interesse para este trabalho, no qual pode-se encontrar os seguintes tópicos: Protocolo da Internet (IP), Rede de Área Local Virtual (VLAN), Protocolo de Roteamento, *Routing Information Protocol* (RIP), *Open Shortest Pathe First* (OSPF), ICMP (*Internet Control Message Protocol)* e *Traceroute*.

2.1 Protocolo da Internet (IP)

“Um protocolo que define o formato e a ordem das mensagens trocadas entre duas ou mais entidades comunicantes, bem como as ações realizadas na transmissão e/ou no recebimento de uma mensagem ou outro evento” (KUROSE & ROSS, 2003). Em outras palavras, protocolo é um conjunto de regras que determinam como será feita a comunicação entre os hosts em uma rede.

O papel essencial desse protocolo é receber os dados enviados pela camada de transporte e enviá-los para a camada de enlace. “No módulo IP, os dados são empacotados em datagramas, que ao chegarem na camada de enlace serão empacotados em quadros.” (TORRES, 2001).

O protocolo IP é não orientado à conexão, isto é, não verifica se o datagrama chegou ou não ao destino. Isso é feito pelo protocolo TCP, discutido a seguir.

Ainda de acordo com o Torres (2001), “a principal função do IP é o roteamento, ou seja, adicionar mecanismos para que o datagrama chegue mais rapidamente possível ao seu destino”. Isso é feito com o auxílio dos roteadores da rede, que escolhem os caminhos mais rápidos entre a origem e o destino.

A camada rede é implementada pelo protocolo IP, o qual oferece um serviço de datagramas, onde cada datagrama é tratado como uma unidade independente e não recebe nenhum tratamento de erros ou reconhecimento fim a fim.

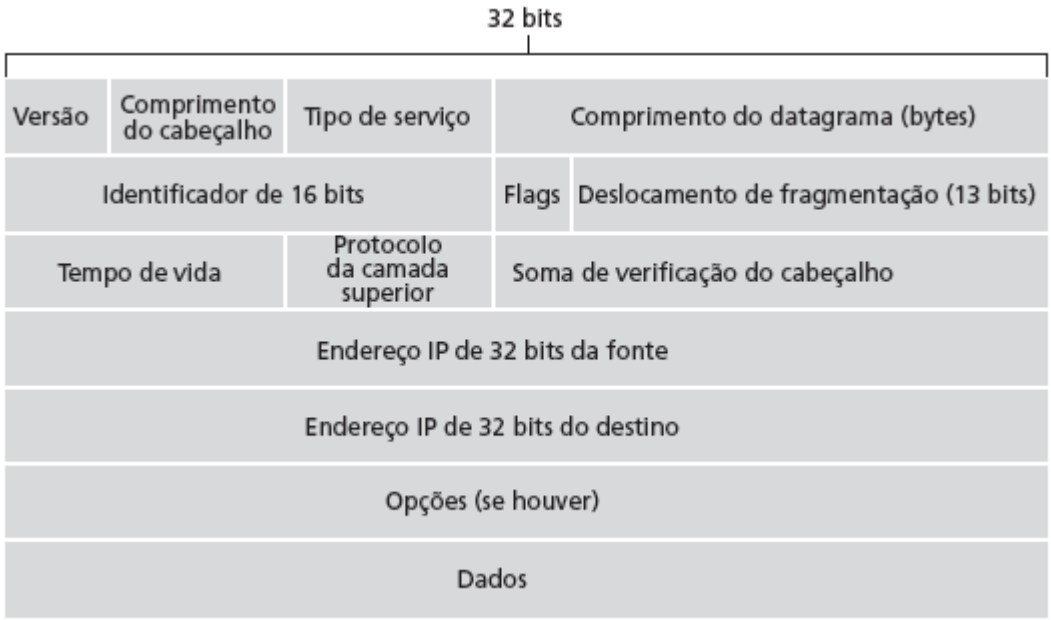
Diógenes (2002) explica a comunicação na camada de rede da seguinte forma:

1- O protocolo IP recebe os segmentos vindos da camada de transporte e fragmenta-os em datagramas.

2- O protocolo IP do host de destino reagrupa estes datagramas de volta em segmentos e passa para a camada de transporte.

Um datagrama IP é a unidade básica de transferência na Internet. O formato do datagrama apresenta um cabeçalho, que contém os endereços IP da fonte e do destino, além de outros campos e uma área de dados. De acordo com o Kurose & James (2009) o formato do datagrama IPv4 é mostrado na Figura 1.

Figura 1 Formato do datagrama IPv4



Fonte: Kurose, 2009, p.248.

Número da versão. Esses quatro bits especificam a versão do protocolo IP do datagrama. Examinando o número da versão, o roteador pode determinar como interpretar o restante do datagrama IP. Logo, diferentes versões de IP usam diferentes formatos de datagramas.

Desse modo, o Comprimento do cabeçalho. Como um datagrama IPv4 pode conter um número variável de opções (incluídas no cabeçalho do datagrama IPv4), esses quatro bits são necessários para determinar onde, no datagrama IP, os dados realmente começam.

Acerca do Tipo de serviço. Os bits de tipo de serviço (*type of service* — TOS) foram incluídos no cabeçalho do IPv4 para poder diferenciar os diferentes tipos de datagramas IP (por exemplo, datagramas que requerem, particularmente, baixo atraso, alta vazão ou confiabilidade) que devem ser distinguidos uns dos outros. Por

exemplo, poderia ser útil distinguir datagramas de tempo real (como os usados por uma aplicação de telefonia IP) de tráfego que não é de tempo real (por exemplo, FTP).

Sobre o ‘Comprimento do datagrama’. É o comprimento total do datagrama IP (cabeçalho mais dados) medido em bytes.

Pelo conceito de ‘Identificador, flags, deslocamento de fragmentação’ ver-se que esses três campos têm a ver com a fragmentação do IP, um tópico que em breve vamos considerar detalhadamente. O interessante é que a nova versão do IP, o IPv6, não permite fragmentação em roteadores.

A notar acerca do ‘Tempo de vida’. O campo de tempo de vida (*time-to-live* — TTL) é incluído para garantir que datagramas não fiquem circulando para sempre na rede (devido a, por exemplo, um laço de roteamento de longa duração). Esse campo é decrementado de uma unidade cada vez que o datagrama é processado por um roteador. Se o campo TTL chegar a 0, o datagrama deve ser descartado.

Ao se postular sobre a questão do ‘Protocolo’ observa-se que esse campo é usado somente quando um datagrama IP chega a seu destino final. O valor desse campo indica o protocolo de camada de transporte específico ao qual a porção de dados desse datagrama IP deverá ser passada.

A ‘Soma de verificação do cabeçalho’ Surge para auxiliar um roteador na detecção de erros de bits em um datagrama IP recebido

Sobre ‘Endereços IP de fonte e de destino’. Se dá quando uma fonte cria um datagrama, insere seu endereço IP no campo de endereço de fonte IP e insere o endereço do destino final no campo de endereço de destinatário IP.

Opções. É o campo de opções permite que um cabeçalho IP seja ampliado. A intenção é que as opções de cabeçalho sejam usadas raramente — por isso a decisão de poupar sobrecarga não incluindo a informação em campos de opções em todos os cabeçalhos de datagrama.

Em suma, Dados (carga útil). Finalmente, chegamos ao último e mais importante campo — a razão de ser do datagrama! Em muitas circunstâncias, o campo de dados do datagrama IP contém o segmento da camada de transporte (TCP ou UDP) a ser entregue ao destino. Contudo, o campo de dados pode carregar outros tipos de dados.

2.2 Endereçamento IP

O protocolo IP é o responsável por estabelecer a rota pela qual seguirá cada pacote na malha de roteadores da Internet. Esta rota é construída tendo como base o endereço de destino de cada pacote, conhecido como endereço IP.

Além de um endereço IP, um nome também pode ser associado a um sistema terminal a fim de facilitar sua identificação por nós humanos. Por exemplo: 200.135.233.1 é o endereço IP e www.ufpa.edu.br é o nome do servidor da UFPA em Castanhal. A aplicação *Domain Same System* (DNS) associa dinamicamente nomes a endereços IP.

Na Internet, cada host e cada roteador tem um endereço IP que codifica seu número de rede e seu número de host. A combinação é exclusiva: em princípio, duas maquinas na Internet nunca têm o mesmo endereço IP. “Todos os endereços IP têm 32 bits e são usados nos campos *Source address* e *Destination address* dos pacotes IP”. (TANENBAUM, 2003)

Kurose (2009) complementa a citação acima afirmando que “O endereço lP é um endereço lógico de 32 bits, escrito em quatro octetos representados em decimal, cada um variando de O a 255. Os números são separados por pontos”. Por exemplo, 193.32.216.9 seria um endereço válido, e sua notação em binário seria:

11000001 00100000 11011000 00001001

Cada computador que esteja rodando o TCP/IP exige um endereço IP exclusivo. Logo, a exclusividade de endereço deve ser sempre mantida, mesmo ao se conectar à Internet.

Sendo assim, cada endereço IP engloba duas partes: o identificador da rede - identifica a rede onde se encontram todos os computadores da mesma rede local. O identificador do host - identifica um dispositivo em uma rede local, como um computador ou roteador.

2.3 Rede de Área Local Virtual (VLAN)

Para Dantas (2005), “VLAN é uma facilidade de operação em uma rede comutada. Esta facilidade permite que o administrador configure a mesma como sendo uma única entidade interligada, enquanto são assegurados aos usuários a conectividade e a privacidade como se estivessem em múltiplas redes separadas.”

As VLANs são baseadas em equipamentos de redes chamados *Switches*. “Na configuração da rede com VLANs, o administrador da rede decide quantas delas haverá, quais dispositivos estarão em cada VLAN e qual será o nome de cada uma.” (TANENBAUM & WETHERALL, 2011).

São redes locais logicamente conectadas, podendo ser criadas em um único *switch* ou entre vários *switches*. “Elas têm o objetivo de resolver um problema que acontece normalmente em grandes redes, conhecida como tempestades de *broadcast*, que é uma replicação de quadros broadcast para todas as portas dos *switches*, ocasionando assim congestionando da rede.“ (MORAES, 2010).

Dessa maneira, é provável formar redes totalmente separadas para os alunos e professores dentro do mesmo ambiente físico, aplicando políticas de segurança diferentes para os grupos, utilizando o conceito de VLAN’s.

2.3.1 As características VLAN’s

De acordo com Forouzan (2006), “a principal característica atribuída ao uso de VLAN’s é a possibilidade de agrupar estações pertencentes a uma ou mais LAN’s físicas, de forma a criar um único domínio de broadcast, garantindo a comunicação entre estas LAN’s, mesmo que façam parte de segmentos físicos diferentes.”

Nos parágrafos seguintes será mostrada uma breve explicação das características das VLANs.

> Em uma rede não segmentada, computadores, impressoras e outros dispositivos conectados disseminam uma grande quantidade de pacotes de broadcasts por diversos motivos, seja por falhas na conexão dos cabos, mau funcionamento de interfaces de rede ou até mesmo por protocolos e aplicações que geram este tipo de tráfego, podendo assim causar atraso no tempo de resposta e lentidão na rede local (FILHO & PEDRO, 2013).

“No modelo de VLANs, existe um domínio lógico de difusão por onde os pacotes de broadcast ou multicast são contidos e não se propagam a outras redes virtuais.” (FRINHAN, 2005). Assim sendo, “os pacotes de difusão ficam contidos apenas em sua rede local, reduzindo drasticamente o volume de tráfego na rede.” (FILHO & PEDRO, 2013).

> A implementação de VLANs, para segmentar uma rede, melhora a performance. Como visto anteriormente, os pacotes de broadcast e multicast ficam presos somente na VLAN onde trafegam, evitando congestionamentos. Outra característica é o fato de diminuir o número de estações que compartilham o mesmo canal lógico, reduzindo com isso, o tempo de acesso.
>
> De modo concernente ao exposto, observa-se que segurança é uma das características mais importantes quando se decide segmentar a rede em VLANs, já que ela permite que dispositivos localizados em diferentes segmentos físicos, mas em uma mesma VLAN, comuniquem-se sem que dispositivos fisicamente próximos tenham acesso (FRINHAN, 2005).

VLAN Trunking é um padrão definido pelo IEEE 802.1ad e tem como característica a transmissão de pacotes para diferentes VLANs em um mesmo link. Barros (2009) define “VLAN Trunking como um link ponto a ponto em uma rede comutada que suporta várias VLANs.”

2.3.2 Tipos de VLANs

Segundo Filippetti (2014), “as VLANs são divididas em dois tipos: As estáticas onde os dispositivos finais são configurados manualmente pelo administrador e as dinâmicas onde são atribuído-os automaticamente.”

2.3.2.1 VLAN dinâmica

> As VLAN’s dinâmicas determinam a atribuição de uma VLAN para um dispositivo automaticamente. Através da utilização de softwares específicos de gerenciamento, é possível o mapeamento de endereços de hardware MAC (Media Access Control), protocolos e até mesmo aplicações ou logins de usuários para VLAN’s específicas (FILIPPETTI, 2014).

> De acordo com Haffermann (2009), com as VLAN’s dinâmicas os dispositivos são conectados e/ou desconectados da rede automaticamente por meio de políticas configuradas pelo administrador da rede. Essa

> configuração é suportada em qualquer tamanho de rede e é a mais recomendada para redes de grande porte, facilitando o controle e a administração.

No entanto, o modo dinâmico é aprendido pelo dispositivo de rede e não permiti quer sejam criadas ou atualizadas novas políticas por gerenciamento. “Esse dispositivo observa a porta de onde o quadro partiu, após captura o endereço fonte e o identificador VLAN e os cadastram no servidor.” (VARARADAJAN, 2012).

2.3.2.2 VLAN estática

O tipo mais comum, fácil de implementar e monitorar é a VLAN no modo estático. “Neste caso, a associação de portas no Switch é criada manualmente pelo administrador de rede, que designa uma ou mais portas do Switch por VLAN.” (FILIPPETTI, 2014).

Como afirma Filippetti (2014), “o modo estático é indicado para redes em que não existem muitas mudanças de dispositivos. Como por exemplo, um escritório onde cada usuário possui um computador desktop.”

Segundo Santos (2010), “as VLANs estáticas se formam quando os terminais que pertencem a uma determinada VLAN possuem posição fixa na rede. Isto gera facilidade de administração da rede e elevação do nível de segurança”.

“Nas VLANs estáticas, as configurações iniciais e todas as alterações posteriores são responsabilidade do administrador da rede, proporcionando um alto grau de controle para a administração. Mas esse tipo de implementação pode se tornar impraticável por depender da interferência de um operador.” (HAFFERMANN, 2009).

2.4 Protocolo de Roteamento

Os protocolos de roteamento operam na camada 3 do modelo OSI, ou seja, na camada de Rede, onde encontramos o IP, o protocolo IP é o protocolo que será roteado, ou seja, é nesta camada que o roteador trabalha, ele lê, escreve e soluciona tudo o que é referente a endereços IP’s que corresponde a identidade de cada dispositivo em uma rede (CARRARO, 2014).

> Os Protocolos de roteamento têm a tarefa de determinar o conteúdo das tabelas de roteamento, ou seja, são eles que ditam a forma como a tabela é montada e de quais informações ela é composta. Nesse caso, existem dois tipos de algoritmos em uso por estes protocolos: um algoritmo baseado em Vetor de Distância e o outro baseado no estado de Enlace. (FILIPPETTI, 2008).

Segundo os autores Neves & Torres (2017), “acerca dos protocolos de roteamento usados na Internet, podemos distinguir claramente dois tipos: os protocolos de roteamento interno e os protocolos de roteamento externo.”

Os protocolos de roteamento externo são utilizados entre sistemas autônomos da Internet para que se possa permitir a interconexão entre estas redes. Alguns protocolos de roteamento externo utilizam o algoritmo de vetor de distância, como o BGP, ou um protocolo mais simples como o EGP (usado para anunciar os endereços IP das redes internas para um roteador externo).

Ainda segundo os autores Neves & Torres (2017), “sobre os protocolos de roteamento interno, temos o RIP (Routing Information Protocol) que utiliza o algoritmo vetor de distância. Este algoritmo é responsável pela construção de uma tabela que informa as rotas possíveis dentro de um AS.”

O OSPF (Open Short Path First) é um outro protocolo de roteamento utilizado no interior de sistemas autônomos (Interior Gateway Protocol – IGP) para troca de informações de rotas dos pacotes IP. Ele surgiu em substituição ao protocolo RIP – Routing Information Protocol, mas diferente deste, o OSPF pode obedecer a uma hierarquia. O OSPF é um protocolo link-state, isto é, os roteadores que rodam este protocolo trocam, entre si, informações sobre os estados dos enlaces de comunicação ligados às suas portas.

2.4.1 Routing Information Protocol (RIP)

> O RIP (Routing Information Protocol) foi um dos primeiros protocolos de roteamento intra-AS da Internet, e seu uso é ainda amplamente disseminado. Sua origem e seu nome podem ser traçados até a arquitetura XNS (Xerox Network Systems). A ampla disponibilização do RIP se deve, em grande parte, à sua inclusão, em 1982, na versão do UNIX do Berkeley Software Distribution (BSD), que suportava TCP/IP. A versão 1 do RIP está

> definida no [RFC 1058] e a versão 2, compatível com a versão 1, no [RFC 2453] (KUROSE & ROSS, 2010).

Assim, a principal diferença entre o RIP versão 1 e versão 2 é que o primeiro usa o modelo classfull e o outro, classless. Portanto, RIPv1 não pode ser usado em sub-redes, pois sem as máscaras, os roteadores vão classificar os endereços como classes de redes A, B e C. (JAIRO, 2018).

> Segundo Torres (2001), no que concerne ao protocolo RIP, os roteadores enviam suas tabelas de outros roteadores que eles consigam acessar diretamente de 30 em 30 segundos. Essa tabela de roteamento inclui, além de redes conhecidas, a distância até elas. Na qual é medida pelo número de roteadores que o datagrama necessita passar até chegar ao destino (essa distância é chamada hop – pulo).

Ainda segundo Torres (2001) assim, “o roteador atualiza sua tabela de roteamento baseado nas tabelas de roteamentos dos demais roteadores que ele consegue acessar diretamente, aprendendo não só novas rotas, mas também redefinindo rotas baseada em menor distância para atingir uma determinada rede.”

2.4.1.1 Funcionamento do RIP

De acordo com Cunha (2018), em rotas muito grandes, é possível implementar métodos para preservar essa característica, conforme descrito a seguir:

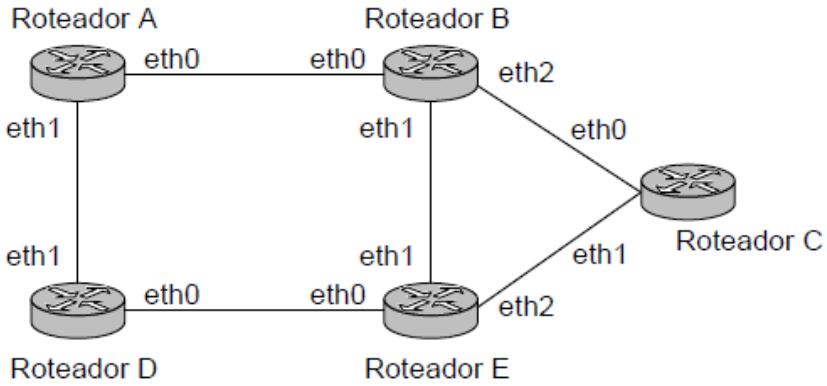
• Split Horizon With Poisonous Reverse: esse método indica quando um pacote não deve ser enviado por um determinado caminho pela possibilidade dele se chocar com outros, entrar em loop e não chegar ao destino desejado.[11]

• Split Horizon, método que indica quando o roteador não pode enviar atualizações pela mesma interface usada para recebê-las.

• Triggered Update, método que não espera o tempo de envio estipulado para atualizar a tabela de roteamento, o que reduz os erros e a ocorrência de loops, porém, sobrecarrega a rede.

[11] Um Sistema Autônomo (AS) é um grupo de redes IP que é gerenciado por um ou mais operadores de rede que possuem uma clara e única política de roteamento.

Figura 2: Funcionamento do RIP



Fonte: Bezerra e Neto, 2002, p.7.

Para um melhor controle desse processo, os autores Bezerra e Neto (2002) simularam o RIP usando o exemplo acima com cinco roteadores interconectados por seis links. Ao iniciar o sistema a tabela de cada roteador só contém a sua própria rota.

Ex.:

De A para Enlace Métrica	De A para Enlace Métrica	De A para Enlace Métrica
A Local 0	A Local 0	A Local 0

Estipulando-se a métrica 1 para todos os nós, isto é, admite-se a distância de cada roteador para seus respectivos vizinhos como 1. E ainda supondo que A envie primeiro sua tabela de atualização, B e D atualizarão as suas tabelas conforme são mostradas abaixo:

De B para Enlace Métrica	De B para Enlace Métrica	De B para Enlace Métrica
B Local 0	B Local 0	B Local 0
A A para B 1	A A para B 1	A A para B 1

De D para Enlace Métrica	De D para Enlace Métrica	De D para Enlace Métrica
D Local 0	D Local 0	D Local 0
A A para D 1	A A para D 1	A A para D 1

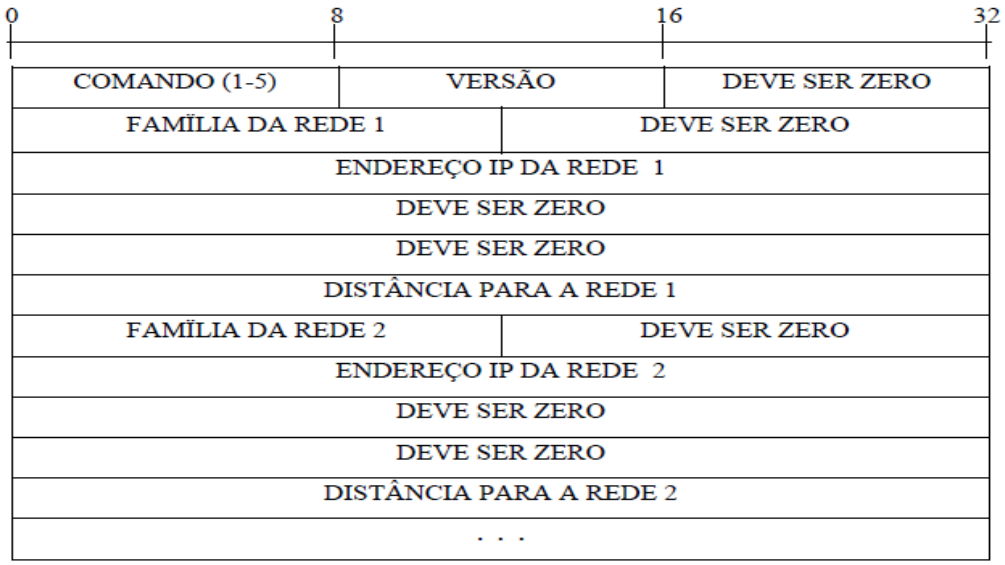
Agora que B e D atualizaram suas tabelas, B transmite sua tabela para seus vizinhos A, C e E. D que faz o mesmo para A e E. A, ao receber a mensagem de B e D, atualiza sua tabela.

Quando um nó recebe uma tabela de atualização de outro nó, ele verifica cada rota de modo a privilegiar as rotas de menor métrica com mesmo destino. Desta forma, as mensagens vão se atualizando até as tabelas convergirem.

2.4.1.2 Especificação do RIP

Bezerra & Neto (2002) expõem que o RIP utiliza o protocolo UDP (User Datagram Protocol) na porta 520 no processo de transmissão e recepção de suas mensagens, o formato da mensagem também é idêntico e pode ser visto a seguir:

Figura 3: A estrutura do Protocolo RIP



Fonte: Bezerra e Neto, 2002, p.11.

Nos campos onde aparece “DEVE SER ZERO”, são campos não utilizados na primeira versão do RIP. Estes campos são utilizados nas versões RIPv2 e RIPng (para redes com IPv6). (BEZERRA & NETO 2002).

O campo comando é usado para especificar o propósito do datagrama de acordo com a tabela a seguir:

Figura 4: Tabela de comandos

Comando	Descrição
1	Solicitação de informações de roteamento parcial ou complexo
2	Resposta contendo pares de distância de rede a partir da tabela de roteamento
3	Ativar o modo de rastreio (hoje obsoleto)
4	Desativar o modo de rastreio (hoje obsoleto)
5	Reservado para uso interno

Fonte: Bezerra e Neto, 2002, p.11.

O formato do pacote permite ao RIP carregar informações de roteamento de vários protocolos diferentes. “Portanto, cada rota da tabela contém um identificador de endereço da família para indicar que tipo de endereço está especificado. Na prática, o RIP não tem sido usado para suportar senão o próprio IP.” (BEZERRA & NETO 2002).

> Diante de uma resposta, o roteador verifica se a rota pertence ao endereço de classe válida (A, B ou C), se o endereço de rede não é 127 (loop-back) ou 0 (endereço broadcast) e, por último, se a métrica não é maior que infinito. Logo após, é feita a análise da tabela com a mensagem recebida para verificar a necessidade de atualização. (CUNHA, 2018).

“O RIP consegue tracejar até 25 rotas por mensagem, sendo que o tamanho máximo de cada uma é de 512 bytes. Se houver necessidade de reportar mais de 25 rotas, será enviado um outro pacote.” (ASSIS; ALVES JÚNIOR, 2001).

2.4.2 Interior Gateway Routing Protocol (OSPF)

> Em 1988, a Internet Engineering Task Force começou a trabalhar em um sucessor, chamado de OSPF (Open Shortest Path First), que se tornou padrão em 1990. Muitos fornecedores de roteadores passaram a aceitá-lo, e ele se tornou o principal protocolo de gateway interior (TANENBAUM, 2003).

“Baseado no protocolo de roteamento IS-IS (Intermediate System toIntermediate System), o OSPF é otimizado para redes IP em particular.” (BEZERRA & NETO 2002).

> Nessa conjuntura, de acordo com Kurose & Ross (2010) assim como o RIP, o roteamento OSPF é usado amplamente para roteamento intra-AS na Internet. O OSPF e seu primo, IS-IS, muito parecido com ele, são comumente disponibilizados em ISPs de níveis mais altos, ao passo que o RIP é disponibilizado em ISPs de níveis mais baixos e redes corporativas. O ‘open’ do OSPF significa que as especificações do protocolo de roteamento estão disponíveis ao público (ao contrário do protocolo EIGRP da Cisco, por exemplo). A versão mais recente do OSPF, versão 2, está definida no RFC 2178 — um documento público.).

Ao contrário de RIP e BGP, OSPF não usa um protocolo de transporte, mas encapsula os dados diretamente em pacotes IP com protocolo número 892. “Devido a isso, OSPF implementa as suas próprias funções de detecção e correção de erros de camada de transporte.” (JAIRO, 2018).

Segundo o Tanenbaum (2003). “Devido à grande experiencia com outros protocolos de roteamento, o grupo que projetou o novo protocolo tinha uma longa lista de requisitos que deveriam ser atendidos.” Primeiro, o algoritmo teria que ser amplamente divulgado na literatura especializada, daí o "O" (de Open, ou aberto) da sigla OSPF. Uma solução patenteada de uma única empresa não funcionaria nesse caso.

Em segundo lugar, o novo protocolo teria de admitir uma variedade de unidades de medida de distância, inclusive a distância física, o retardo etc. Em terceiro lugar, ele teria de ser um algoritmo dinâmico, que se adaptasse de forma rápida e automática a alterações na topologia (TANENBAUM, 2003).

Em quarto lugar, uma novidade no caso do OSPF: ele tinha de admitir o roteamento baseado no tipo de serviço. O novo protocolo deveria ser capaz de rotear tráfego de tempo real de uma determinada maneira e outro tipo de tráfego de maneira diferente. O protocolo IP tem um campo Type of service, mas nenhum protocolo de roteamento existente o utilizava. Esse campo foi incluído no OSPF, mas ninguém o utilizava ainda e, mais tarde, ele foi removido (TANENBAUM, 2003).

Como um quinto requisito, relacionado aos anteriores, o novo protocolo tinha de balancear a carga, dividindo-a por várias linhas. A maioria dos protocolos anteriores enviava todos os pacotes pela melhor rota. Diante disso, segunda melhor

rota não era usada. Em muitos casos, a divisão da carga por várias linhas proporciona melhor desempenho (TANENBAUM, 2003).

Em sexto lugar, era necessário o suporte para sistemas hierárquicos. Em 1988, a Internet tinha crescido tanto que nenhum roteador era capaz de conhecer a topologia inteira. O novo protocolo de roteamento teve que ser projetado de forma que nenhum roteador fosse obrigado a conhecer a topologia (TANENBAUM, 2003).

Em sétimo lugar, era necessário um certo nível de segurança para evitar que estudantes em busca de diversão tentassem enganar os roteadores, enviando-lhes falsas informações de roteamento. Por fim, era necessário tomar alguma providência para lidar com os roteadores conectados à Internet por meio de um túnel — assunto que os protocolos anteriores não dominavam muito bem (TANENBAUM, 2003).

Assim, o OSPF é compatível com três tipos de conexões e redes: Ponto a ponto (por exemplo, SONET) e redes de broadcast (por exemplo, a maioria das LANS). Na realidade, ele é capaz de dar suporte a redes com vários roteadores, cada um deles podendo se comunicar diretamente com outros (chamadas redes de acesso múltiplo), mesmo que eles não tenham capacidade de broadcast. (TANENBAUM & WETHERALL, 2011).

As principais melhorias do OSPF em relação ao RIP se dão pelo fato dele:

Analisar mais métricas além do salto (hop);

Ser dinâmico ao ponto de convergir rapidamente;

Ter a capacidade de rotear baseado no Tipo do Serviço (Type of Service - ToS). Isso possibilita rotear o tráfego de tempo real (ex: stream áudio) com QoS e os outros tráfegos de maneira distinta. ToS está definido num campo do cabeçalho IP;

Possuir balanceamento de carga, que consiste em dividir o tráfego por várias linhas (enlaces);

Atender a redes muito grandes, onde nenhum roteador é capaz de conhecer a topologia inteira. Neste caso, o Sistema Autônomo (AS) pode ser dividido em grupos contíguos de redes chamadas Áreas OSPF.

Existem cinco tipos de pacotes OSPF, que são: Hello, Database Description, Link State Request, Link State Update e Link State Acknowledgement.

> Assim, o próprio protocolo OSPF tem de implementar funcionalidades como transferência confiável de mensagem e transmissão broadcast de estado de enlace. O protocolo OSPF também verifica se os enlaces estão operacionais (via uma mensagem HELLO enviada a um vizinho ligado ao enlace) e permite que um roteador OSPF obtenha o banco de dados de um roteador vizinho referente ao estado do enlace no âmbito da rede (KUROSE & ROSS, 2010).

De acordo com o Jairo (2018), num Sistema Autônomo com protocolo OSPF, os roteadores podem ser classificados nas seguintes categorias abaixo:

• Roteadores internos (internal routers): são roteadores que fazem somente roteamento interno no Sistema Autônomo, e não estão no backbone. Estes roteadores têm todas as redes diretamente conectadas e pertencem à mesma área.

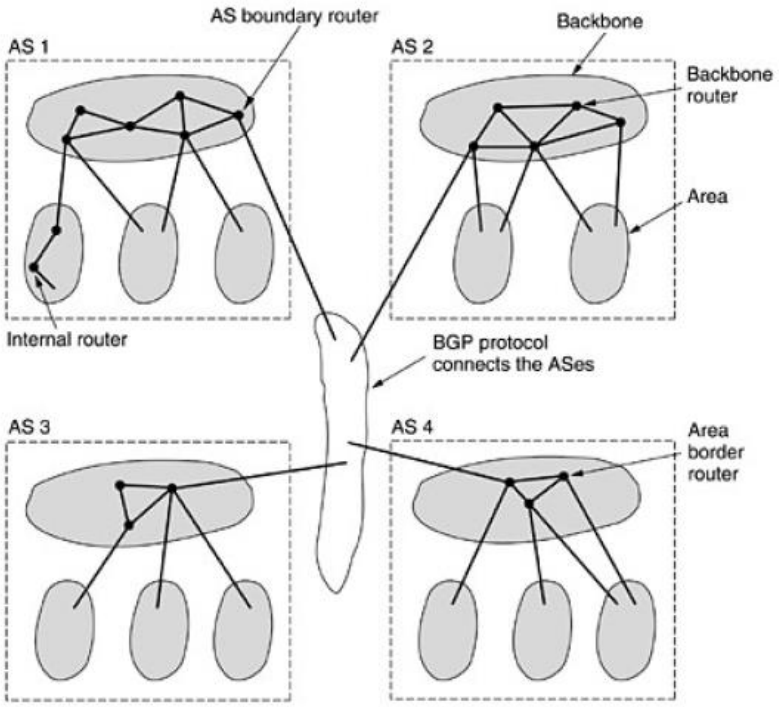
• Roteadores de borda de área (area border routers): são roteadores que pertencem tanto a uma área quanto ao backbone. Estes roteadores rodam múltiplas cópias do algoritmo básico de roteamento, uma cópia para cada área ligada a ele e uma cópia adicional para o backbone. Cada roteador de borda de área condensa a informação topológica das áreas ligadas a ele, para distribuição para o backbone.

• Roteadores de backbone (mas não de borda) são roteadores que fazem roteamento dentro do backbone, mas não no roteador de borda (boundary routers). Eles têm uma interface de rede no backbone e podem atender a uma ou mais áreas.

• Roteadores de borda (boundary routers): o roteador de borda troca informações de rotas com roteadores pertencentes a outros Sistemas Autônomos. Este roteador tem rotas para AS externos, que são anunciadas através do Sistema Autônomo. O caminho para cada roteador de borda é conhecido por todos os roteadores no interior do Sistema Autônomo. O roteador de borda usa, por exemplo, protocolo BGP para fazer roteamento entre Sistemas Autônomos.

> Essas classes podem se sobrepor. Por exemplo, todos os roteadores de borda fazem parte do backbone automaticamente. Além disso, um roteador que esteja no backbone, mas que não faça parte de nenhuma outra área, também é um roteador interno. Exemplos de todas as quatro classes de roteadores são ilustrados na figura a seguir. (TANENBAUM, 2003).

Figura 5: A relação entre SA's, backbones e áreas no OSPF



Fonte: Tanenbaum, 2003, p.352.

Ainda de acordo com os atores KUROSE e ROSS (2010) “um sistema autônomo OSPF pode ser configurado hierarquicamente em áreas. Cada área roda seu próprio algoritmo de roteamento de estado de enlace OSPF, sendo que cada roteador em uma área transmite seu estado de enlace a todos os outros roteadores daquela área.”

2.5 Internet Control Message Protocol (ICMP)

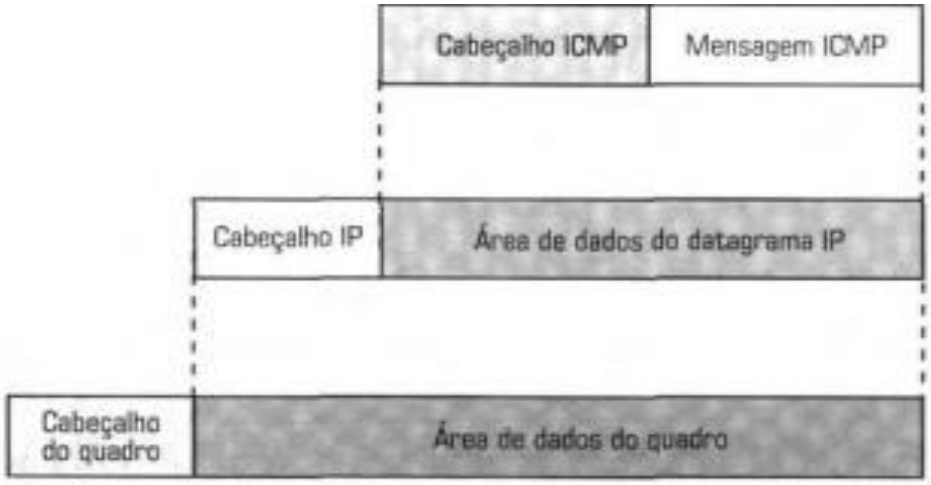
ICMP, referenciado pelo RFC 792 de setembro de 1981, é a sigla *de Internet Control Message Protocol*, ou, em português, Protocolo de Mensagens de Controle do IP. Esse é um dos mais importantes protocolos IP, pois emite avisos, em forma de mensagens, sobre a situação da rede. Com exceção do TCP (Protocolo de Controle de Transmissão), que tem seus próprios métodos de controle, quase todos os outros protocolos IP, se não todos, dependem do ICMP. (MOTA, 2013)

> ICMP é frequentemente considerado como parte do IP, em termos de arquitetura, está logo acima do IP, pois as mensagens são carregadas dentro do Datagrama do IP. Isto é, as mensagens são carregadas como carga útil

> IP. De maneira semelhantes, quando hospedeiro recebe um datagrama IP como ICMP especificado o protocolo de cada camada superior, ele de multiplexa o conteúdo do datagrama para ICMP, exatamente como de multiplexaria o conteúdo do datagrama para TCP ou UDP (User Datagram Protocol). (KUROSE & ROSS, 2010).

A operação da Internet é monitorada rigorosamente pelos roteadores. Quando ocorre algo inesperado, o evento é reportado pelo ICMP, que também é usado para testar a Internet (TANENBAUM, 2003). “O ICMP utiliza o IP para o transporte de mensagem, não oferecendo, portanto, garantia de entrega. A figura a seguir apresenta como uma mensagem ICMP é encapsulada em um datagrama IP.” (FERRAZ et at., 2002).

Figura 6: Encapsulamento de uma mensagem ICMP



Fonte: Torres, 2001, p.91.

“Existe aproximadamente uma dezena de tipos de mensagens ICMP definidas. Os mais importantes estão listados na tabela 1. Cada tipo de mensagem ICMP é encapsulado em um pacote IP.” (TANENBAUM, 2003).

Tabela 01: tipos de mensagens ICMP

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

Fonte: Tanenbaum, 2003, p.291.

A mensagem *DESTINATION UNREACHABLE* é usada quando a sub-rede ou um roteador não consegue localizar o destino, ou quando um pacote com o bit DF não pode ser entregue, porque há uma rede de "pacotes pequenos" no caminho.

A mensagem *TIME EXCEEDED* é enviada quando um pacote é descartado porque seu contador chegou a zero. Esse evento é um sintoma de que os pacotes estão entrando em loop, de que há um enorme congestionamento ou de que estão sendo definidos valores muito baixos para o timer.

A mensagem *PARAMETER PROBLEM* indica que um valor inválido foi detectado em um campo de cabeçalho. Esse problema indica a existência de um bug no software IP do host transmissor ou, possivelmente, no software de um roteador pelo qual o pacote transitou.

Antes, a mensagem *SOURCE QUENCH* era usada para ajustar os hosts que estivessem enviando pacotes demais. Quando recebia essa mensagem, um host devia desacelerar sua operação.

A mensagem *REDIRECT* e usada quando um roteador percebe que o pacote pode ter sido roteado incorretamente. Ela é usada pelo roteador para informar ao host transmissor o provável erro.

As mensagens *ECHO* e *ECHO REPLY* são usadas para verificar se um determinado destino está ativo e acessível. Ao receber a mensagem *ECHO*, o destino deve enviar de volta uma mensagem *ECHO REPLY*. As mensagens *TIMESTAMP REQUEST* e *TIMESTAMP REPLY* são semelhantes, exceto pelo fato de o tempo de

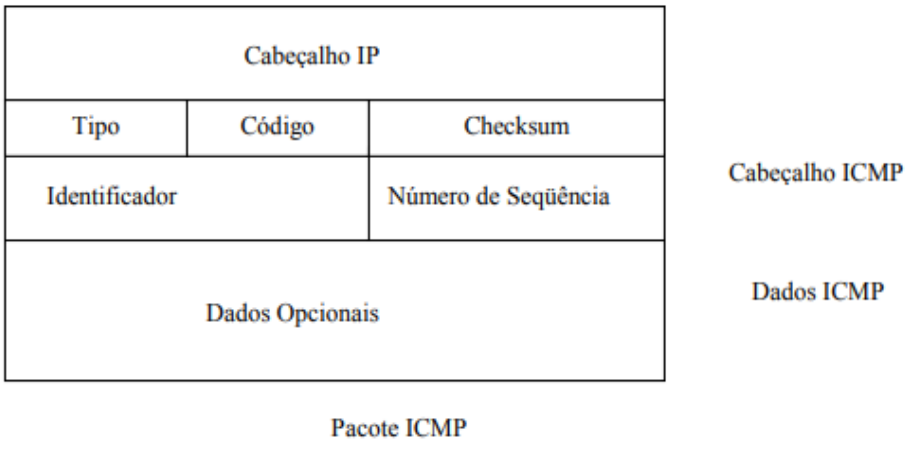
chegada da mensagem e o tempo de saída da resposta serem registrados na mensagem de resposta. Esse recurso e usado para medir o desempenho da rede.

“O ICMP, como foi dito, possui diversos tipos e códigos de mensagens. Todos estão listados no site da IANA, em www.iana.org/assignements/icmp-parameters. –“ (MOTA, 2013)

> Quando ocorre algum problema previsto pelo ICMP, uma mensagem ICMP descrevendo a situação é preparada e entregue à camada IP, que adiciona está ao seu cabeçalho e envia ao emissor do datagrama com o qual ocorreu o problema. É importante saber que o ICMP é um mecanismo de aviso de erros e não especifica a ação para correção do erro. (FERRAZ et al., 2002).

O computador de origem é quem deve relatar o erro a um programa de aplicação para correção deste problema. O formato geral de uma mensagem ICMP é apresentado na figura abaixo. O campo TIPO identifica a mensagem ICMP particular, o campo CÓDIGO é usado na especificação dos parâmetros da mensagem e o campo *CHECKSUM* corresponde ao código verificador de erro, calculado a partir da mensagem ICMP completa.

Figura 7: Cabeçalho das mensagens ICMP



Fonte: Ferraz, 2002, p.8.

2.6 Traceroute

> O Traceroute é um comando utilizado para descobrir toda a rota entre dois pontos numa rede. Em outras palavras, ele mostra os roteadores presentes em um caminho. Exemplo do comando: Instale com # apt-get install traceroute. O traceroute no GNU/Linux utiliza como protocolo-padrão o UDP com a porta 53 como padrão. (MOTA, 2013).

Para Ferraz et at., (2002) com o traceroute, o usuário pode descobrir o caminho percorrido pelo pacote até seu destino. No qual envia 3 pacotes UDP com a porta de destino não usada por nenhum aplicativo, inicialmente com TTL igual a um (1). Quando passar pelo primeiro roteador, tornar-se-á zero e uma mensagem 'ICMP tempo excedido' retornará. Com isso teremos informações sobre o primeiro roteador no meio do caminho e o RTT da fonte até este roteador. Em seguida, o TTL é aumentado para dois (2) e novamente são enviados 3 pacotes UDP, porém a mensagem ICMP ocorrerá somente no segundo roteador.

A seguir será apresentado um exemplo da execução do aplicativo traceroute, realizado numa máquina, onde o sistema operacional é:

- **WINDOWS**

C:\WINDOWS>tracert 200.20.94.50

Tracing route to guanabara.rederio.br [200.20.94.50]

over a maximum of 30 hops:

1 2 ms 1 ms 2 ms cisco7513-CBPF.cat.cbpf.br [152.84.253.1]

2 3 ms 2 ms 3 ms rederio-atm-cbpf.rederio.br [200.20.94.41]

3 3 ms 2 ms 3 ms ançaara.rederio.br [200.20.94.50]

Trace complete.

Descrição:

30 hops: Máximo TTL

1: indica o número de quantos roteadores o pacote já passou

2ms 1ms 2ms: RTT de cada pacote enviado

cisco7513-cbpf.cat.cbpf.br: Nome do roteador

152.84.253.1: Endereço IP

- **LINUX**

[root@sodium root]# traceroute 200.20.94.50

traceroute 200.20.94.50, 30hops max, 38 bytes packets

1 cisco7513-bpf (152.84.253.1) 9.232ms 2.891ms 8.132ms

2 rederio-atm-cbpf.rederio.br(200.20.94.41) 9.321ms 3.679ms 1.677ms

3 guanabara.rederio.br (200.20.94.50) 2.421ms * 1.622ms

Descrição:

30 hops: Máximo TTL

38 bytes packets: Tamanho do pacote

1: indica o número de quantos roteadores o pacote já passou

cisco7513-cbpf.cat.cbpf.br: Nome do roteador

152.84.253.1: Endereço IP

9.232ms 2.891ms 8.132ms: RTT de cada pacote enviado

*: Indica que o tempo de “timeout” expirou antes que a mensagem ICMP fosse recebida pelo datagrama.

Algumas chaves interessantes do comando Traceroute:

Tabela 02: Chaves interessantes do Comando Traceroute

Chave	Função
- n	Com a chave -n, como a maioria dos comandos de rede, não resolve nome. Isto acelera bastante a resposta do comando.
-4	Força a utilização de IPV4.
-6	Força a utilização de IPV6. É equivalente ao comando traceroute6.
-I	Trabalha com ICMP em vez de UDP.
-T	Utiliza TCP com flag SYN em de UDP. A porta default é 80. É equivalente ao comando tcptraceroute.
-p	Determine a porta a ser utilizada pelos protocolos TCP e UDP em vez do padrão.

Fonte: Ferraz, 2002, p.10.

3. METODOLOGIA

Neste trabalho, estará sendo utilizada como base simulação através do software Cisco Packet Tracer na versão 5.3, estaremos simulando o funcionamento uma rede metropolitana que vai fazer a comunicação de quatro redes locais, representando uma empresa com sua sede e três filiais interligadas, e devidamente configuradas com suas particularidades, estrutura de cabeamento, endereçamento, configuração de roteamento e configuração de host's.

Através desta simulação será feita a coletar dados, a análise e serão propostas melhorias no projeto de redes a fim de extrair o máximo desempenho, usabilidade e recursos da rede. Estes dados serão mostrados com a ajuda de teste na rede simulada, sendo estes, teste de ping e traceroute.

3.1 Simuladores de Redes de Computadores

Sabe-se que a tecnologia se faz necessária, atualmente, em diversas as áreas. E mais do que isso, no ramo da computação é indispensável trabalharmos com ferramentas tecnológicas que nos proporcionam simular trabalhos já realizados ou em construção. Quando se trata de elaboração de projeto a simulação se torna algo crucial na análise e implementação de sistemas de rede de computadores, levando em conta todos os desafios de ter um laboratório real. Assim, a realização de algumas tarefas nos simuladores de redes pode colocar os alunos o mais próximo possível de suas experiências profissionais posteriormente.

Diante disso, o uso desses simuladores de redes vem crescendo nas universidades de forma positiva e significativa já que nem todos podem disponibilizam recursos tão altos para a criação de um ambiente real com tantas variedades de ferramentas. Segundo Silva et at. (2019) outro ponto que vale ressaltar sobre os simuladores é que, permitem testar o desempenho de protocolos em várias redes e ambientes, onde em um laboratório real ou uma empresa, talvez fosse impossível uma preparação como ocorre nos simuladores por questão de tempo. Assim, facilitam a execução dos protocolos em vários cenários.

De acordo com Neto (2018) existem diversos modelos que têm como objetivo avaliar e medir o desempenho de uma rede simulada, sendo que os mesmos servem para garantir a qualidade e coerência dos cenários em estudo, garantindo a qualidade

do processo de simulação. Dentre os principais modelos contidos nos simuladores, destacam-se:

1. O modelo com cenários reais: esse modelo faz uso de uma infraestrutura real para simular os diversos cenários desejados. Logo, possui um grande custo, demanda muito tempo para instalar e adaptar os equipamentos a cada cenário desejado e necessita de técnicas para coletar e analisar os dados obtidos por meio da simulação; por outro lado, oferece uma visão ampla e realística do que se deseja.

2. Modelos analíticos: faz uso de modelos estatísticos e matemáticos para analisar os cenários simulados das diversas formas possíveis, garantindo um alto grau de confiança nos dados obtidos. Eles têm como desvantagem a necessidade de pessoal específico para adaptar as diversas variáveis e analisar os dados obtidos.

3. Modelos computacionais: Os modelos computacionais funcionam por meio de softwares específicos que simulam os diversos cenários possíveis, garantindo uma previsão do funcionamento daquilo que se deseja simular. Sua principal vantagem é seu baixo custo de implementação, que dispensa a necessidade de grandes gastos com infraestrutura. Por outro lado, é necessário que exista um treinamento por parte do usuário para que se use os recursos de forma correta, sem que sejam gerados dados inconsistentes.

E as algumas das principais ferramentas de simulações de redes são: OMNeT ++, NETPLANNER, Network Simulator – NS3, GNS3, Packet Tracer (Cisco), VIRL (Cisco) e EVE-NG. Alguns desses são usados para auxiliar pesquisas e outros para testes, buscando aperfeiçoar equipamentos ou programas antes de lançá-los no ambiente real. Para o trabalho em questão, será usado a simulação com base no modelo computacional – Cisco Packet Tracer. É necessário contar com a importância das práticas e uso de todas ferramentas vistas na teoria, pois foi o simulador usado nas aulas práticas, após cursar disciplinas voltada ao tema, já despertando um interesse nesse ambiente virtual.

3.2 Simulador Cisco Packet Tracer

Na atualidade, o uso de simuladores em disciplina de rede de computadores é fundamental para o desenvolvimento do aluno, visto que algumas das universidades e instituições de ensino não dispõem de laboratórios de informáticas, bem estruturados, que possam ser propícios para uma aula prática da disciplina, com isso, faz-se necessário a utilização de simuladores, uma vez que representam um papel essencial na tarefa de desenvolver, analisar e aperfeiçoar atividades, com caráter temático no conteúdo específico da disciplina.

De acordo com o Cisco, “O Packet Tracer ajuda os alunos a criarem seus próprios “mundos de rede” virtuais para exploração, experimentação e explicação de conceitos e tecnologias de rede” (CISCO NETWORKING ACADEMY, 2010).

O Packet Tracer, além de ser um software de simulação de redes de fácil instalação e sem custo algum para download e ser bastante didático, é uma ferramenta que simula múltiplos dispositivos e protocolos (routers, switches, wireless, RADIUS, SNMP) que atualmente vêm sendo utilizados também para fins acadêmicos.

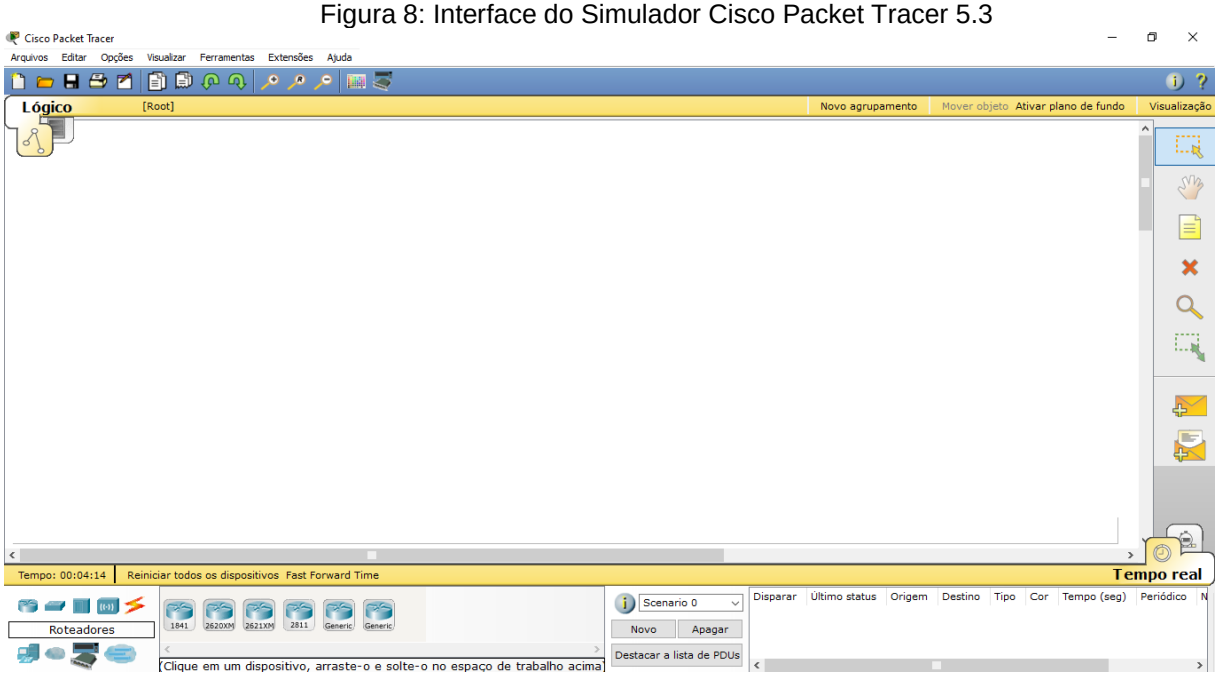
O uso do simulador permite expor o aluno a situações que seriam custosas na vida real e com as quais ele não lidaria em um treinamento convencional. Apostando nisso, segundo Silva et at. (2019) a utilização deste software possibilita gerar tráfego na rede criada, acompanhar visualmente os pacotes e frames e simular aplicações específicas, sendo um simulador bastante interativo com o usuário, em que o mesmo oferece alguns outros recursos, como autoria, avaliação e colaboração, facilitando o ensino e aprendizagem de conceitos tecnológicos para o aluno.

3.3 Interface e os Recursos do Simulador

O simulador Cisco Packet Trace 5.3 oferece vários recursos em sua interface; usando a sua área de trabalho (imagem abaixo) podemos inserir e operar diversos dispositivos, cabos e complementos que podem ser encontrados na parte inferior da tela da ferramenta, na barra lateral do lado direito há alguns recursos de ajuste da organização dos itens que estão sendo usados no projeto.

Ainda é possível fazer configurações na parte física e lógica dos projetos podendo assim prever diversas situações que podem ser otimizadas em simulação, aplicando testes e administrando resultados em tempo real.

Figura 8: Interface do Simulador Cisco Packet Tracer 5.3



Fonte: Capturada pelo Autor, 2022.

3.4 Configuração

Nesta subseção serão apresentadas as configurações internas (LAN'S) das redes e os macros que interligam os roteadores (MAN). A princípio, para o endereçamento da rede da Matriz, utilizou-se duas redes para que não haja acesso entre elas, se não pelo roteador de borda e tendo assim uma maior segurança dentro da rede. Na primeira rede (192.168.0.x) destinado para os servidores (DHCP, DNS, HTTPS, FTP e EMAIL) e PC, e na segunda rede (192.168.1.x) utilizou Access Point destinados para os funcionários, essa alternativa foi criada para limitar o acesso dos mesmos de tentar se conectarem à rede em que estão os servidores. Diante disso, evitando assim que eles tenham acesso ao servidor e consequentemente aos arquivos da rede. Tais informações serão demonstradas na tabela 03.

Tabela 03. Configuração das redes LAN's da Matriz

	ITEM	NOME DO HOST	IP	PORTA DO HOST	SWITCH0
LAN 192.168.0.0 DA MATRIZ	1	MATRIZ	192.168.0.1	FA 0/0	FA 0/24
	2	PC0	192.168.0.2	FastEthernet	FA 0/1
	3	PC1	192.168.0.3	FastEthernet	FA 0/2
	4	DHCP	192.168.0.4	FastEthernet	FA 0/3
	5	DNS	192.168.0.5	FastEthernet	FA 0/4
	6	HTTP/HTTPS	192.168.0.6	FastEthernet	FA 0/5
	7	FTP	192.168.0.7	FastEthernet	FA 0/6
	8	EMAIL	192.168.0.8	FastEthernet	FA 0/7
	9	PC11	192.168.0.10	FastEthernet	FA 0/8
	10	SWITCH0	-	-	-
LAN 192.168.1.0 DA MATRIZ	1	MATRIZ	192.168.1.1	FA 1/0	FA 0/24
	2	PC2	192.168.1.2	FastEthernet	FA 0/2
	3	PC3	192.168.1.3	FastEthernet	FA 0/3
	4	Pda0	192.168.1.4	WIFI	-
	5	Laptop0	192.168.1.5	WIFI	-
	6	SWITCH2	-	-	-
	7	Wifi_Matriz	-	FastEthernet	FA 0/1

Fonte: Elaborado pelo autor, 2022.

Nesse sentido, obtém-se três filiais e cada uma ter a sua própria rede LAN por questão, também, de segurança. Como mencionado anteriormente, na segunda rede da matriz, que é destinada para os funcionários, às redes das filiais funcionarão da mesma forma. A rede (192.168.7.x) da Filial 01, (192.168.70.x) da Filial 02 e (192.168.100.x) da Filial 03. Serão apresentadas nas tabelas 04, 05 e 06.

Tabela 04. Configuração da LAN da Filial 01

LAN 192.168.7.0 DA FILIAL 01				
ITEM	NOME DO HOST	IP	PORTA DO HOST	SWITCH2
1	Filial01	192.168.7.1	FA 0/0	FA 0/1
2	PC4	192.168.7.2	FastEthernet	FA 0/2
3	Impressora0	192.168.7.3	FastEthernet	FA 0/3
4	Laptop1	192.168.7.4	FastEthernet	FA 0/4
5	Pda2	192.168.7.5	WIFI	-
6	SWITCH1	-	-	-
7	Wifi_Filial01	-	FastEthernet	FA 0/5

Fonte: Elaborado pelo autor, 2022.

Tabela 05. Configuração da LAN da Filial 02

LAN 192.168.70.0 DA FILIAL 02					
ITEM	NOME DO HOST	IP	PORTA DO HOST	SWITCH3	SWITCH4
1	Filial02	192.70.0.1	FA 0/0	FA 0/1	-
2	PC5	192.70.0.2	FastEthernet	FA 0/3	-
3	PC6	192.70.0.3	FastEthernet	FA 0/4	-
4	PC7	192.70.0.4	FastEthernet	FA 0/5	-
5	PC8	192.70.0.5	FastEthernet	FA 0/6	-
6	PC9	192.70.0.6	FastEthernet	FA 0/7	-
7	Impressora2	192.70.0.7	FastEthernet	FA 0/8	-
8	Laptop2	192.70.0.8	FastEthernet	-	FA 0/2
9	Laptop3	192.70.0.9	FastEthernet	-	FA 0/3
10	Laptop4	192.70.0.10	FastEthernet	-	FA 0/4
11	Laptop5	192.70.0.11	FastEthernet	-	FA 0/5
12	Laptop6	192.70.0.12	FastEthernet	-	FA 0/6
13	Impressora1	192.70.0.13	FastEthernet	-	FA 0/7
14	SWITCH3	-	-	-	FA 0/1
15	SWITCH4	-	-	FA 0/2	-

Fonte: Elaborado pelo autor, 2022.

Tabela 06. Configuração da LAN da Filial 03

LAN 192.168.100.0 DA FILIAL 03					
ITEM	NOME DO HOST	IP	PORTA DO HOST	SWITCH5	Vlan
1	Filial03	192.168.100.1	FA 0/0	FA 0/1	-
2	Fl03PC01	192.168.100.2	FastEthernet	FA 0/2	Vlan1
3	Fl03PC02	192.168.100.3	FastEthernet	FA 0/3	Vlan1
4	Fl03PC03	192.168.100.4	FastEthernet	FA 0/4	Vlan1
5	Fl03PC04	192.168.100.5	FastEthernet	FA 0/5	Vlan1
6	Fl03PC05	192.168.100.6	FastEthernet	FA 0/6	Vlan1
7	Fl03PC06	192.168.100.7	FastEthernet	FA 0/7	Vlan1
8	Fl03PC07	192.168.100.8	FastEthernet	FA 0/8	Vlan1
9	Fl03PC08	192.168.100.9	FastEthernet	FA 0/9	Vlan1
10	Fl03PC09	192.168.100.10	FastEthernet	FA 0/10	Vlan1
11	Fl03PC10	192.168.100.11	FastEthernet	FA 0/11	Vlan1
12	Fl03PC11	192.168.100.12	FastEthernet	FA 0/12	Vlan1
13	Fl03PC12	192.168.100.13	FastEthernet	FA 0/13	Vlan1
14	Fl03PC13	192.168.100.14	FastEthernet	FA 0/14	Vlan2
15	Laptop7	192.168.100.15	FastEthernet	FA 0/15	Vlan2
16	Impressora3	192.168.100.16	FastEthernet	FA 0/16	Vlan2
17	Servidor0	192.168.100.17	FastEthernet	FA 0/17	Vlan2
18	SWITCH5	-	-	-	-

Fonte: Elaborado pelo autor, 2022.

Abaixo segue as tabelas de configurações de rede das redes que interligam as filias e a matriz (MAN).

Tabela 07. Configuração da MAN da Matriz para Filial 01

MAN 10.0.0.0				
	Origem	Destino	Rede	Largura de Banda
	Matriz	Filial01	10.0.0.0	1Mb
IP	10.0.0.1	10.0.0.2		
Porta	Serial 2/0	Serial 2/0		

Fonte: Elaborado pelo autor, 2022.

Tabela 08. Configuração da MAN da Filial 01 para Filial 03

MAN 11.0.0.0				
	Origem	Destino	Rede	Largura de Banda
	Filial01	Filial03	11.0.0.0	2Mb
IP	10.0.0.2	10.0.0.1		
Porta	Serial 3/0	Serial 2/0		

Fonte: Elaborado pelo autor, 2022.

Tabela 09. Configuração da MAN da Matriz para Filial 02

MAN 12.0.0.0				
	Origem	Destino	Rede	Largura de Banda
	Matriz	Filial02	12.0.0.0	1Mb
IP	12.0.0.1	12.0.0.2		
Porta	Serial 3/0	Serial 2/0		

Fonte: Elaborado pelo autor, 2022.

Tabela 10. Configuração da MAN da Filial 03 para Filial 02

MAN 7.0.0.0				
	Origem	Destino	Rede	Largura de Banda
	Filial03	Filial02	7.0.0.0	2Mb
IP	7.0.0.1	7.0.0.2		
Porta	Serial 3/0	Serial 3/0		

Fonte: Elaborado pelo autor, 2022.

Tabela 11. Configuração da MAN da Filial 01 para Filial 02

MAN 5.0.0.0				
	Origem	Destino	Rede	Largura de Banda
	Filial01	Filial02	5.0.0.0	500Kbs
IP	5.0.0.1	5.0.0.2		
Porta	Serial 6/0	Serial 6/0		

Fonte: Elaborado pelo autor, 2022.

Tabela 12. Configuração da MAN da Matriz para Filial 03

MAN 6.0.0.0				
	Origem	Destino	Rede	Largura de Banda
	Matriz	Filial03	6.0.0.0	500Kbs
IP	6.0.0.1	6.0.0.2		
Porta	Serial 7/0	Serial 6/0		

Fonte: Elaborado pelo autor, 2022.

3.5 Cenário do Projeto no Packet Tracer

Para montar o diagrama da rede, foi usado o software do Cisco Packet Tracer 5.3, no qual foi elaborado toda a configuração da rede. Como a MAN, LAN, IP e entre outros. Na Figura X representa todo o mapa da rede para reproduzir um modelo de rede MAN que interliga a Matriz (na área amarela) e as três filiais sendo que de cada Filial tem sua própria rede (filial 1 na área azul, 2 na área vermelha e 3 na verde).

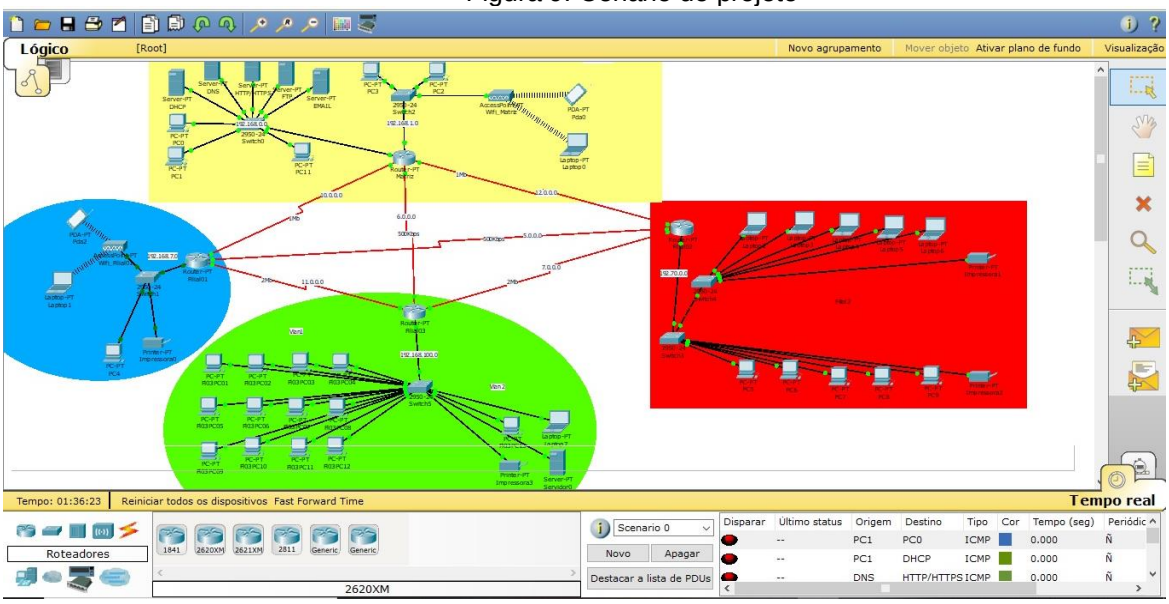
Na área amarela que abrange a matriz, estão duas redes locais e um roteador (Matriz) que faz a comunicação com as filiais 1, 2 e 3. Na primeira LAN (192.168.0.0), estão os servidores DHCP, DNS, HTTP/HTTPS, FTP, EMAIL e outros três hosts (PC0, PC1 e PC11) ligados a um switch (Switch0) de 24 Portas, já na segunda LAN (192.168.1.0) estão três Hosts (PC2, PC3 e AcessPoint Wifi_Matriz) ligados a um switch (Switch2) sendo um destes um AcessPoint que está dando conexão de rede via wireless para mais dois hosts (Pda0 e Laptop0).

Na área azul que abrange a primeira filial temos um roteador (Filial01) que faz a comunicação com a Matriz, filial 2, filial 3 e uma rede local com um Switch (Switch1) onde estão ligados: um computador (PC4), uma impressora (Impressora0) e um AcessPoint (Wifi_filial01) que está dando conexão de rede via wireless para mais dois hosts (Pda2 e Laptop1).

Na área vermelha que abrange a segunda filial, temos um roteador (Filial02) que faz a comunicação com a Matriz, filial 1 e 3 e uma rede local com dois Switches (Switch3 e Switch4) onde estão ligados cinco computadores e uma impressora no primeiro Switch (PC5, PC6, PC7, PC8, PC9 e Impressora2) e cinco Laptops e uma impressora no segundo Switch (Laptop2, Laptop3, Laptop4, Laptop5, Laptop6 e Impressora1) e este também está ligado ao primeiro.

Na área verde que abrange a terceira filial, temos um roteador (Filial03) que faz a comunicação com a Matriz, filial 1, filial 2 e uma rede local com um Switch (Switch5) onde estão ligados doze computadores (FL03PC01, FL03PC02, FL03PC03, FL03PC04, FL03PC05, FL03PC06, FL03PC07, FL03PC08, FL03PC09, FL03PC10, FL03PC11 e FL03PC12) divididos por uma rede local virtual (Vlan1), e em uma outra rede local virtual estão ligados um computador (FL03PC13), um laptop (Laptop7), um servidor (Servidor0) e uma impressora (Impressora3).

Figura 9: Cenário do projeto



Fonte: Capturada pelo Autor, 2022.

4. RESULTADOS

Com o projeto já todo montado e configurado, aplicou-se várias sequências de testes e foram coletados diversos resultados do estado de conexão da rede e do funcionamento e desempenho da mesma, assim podendo se analisar, com mais detalhes, cada característica medida e o estado em que ela foi coletada.

Com os resultados já prontos, nos subtópicos seguintes estarão sendo comentados e mais detalhados os principais resultados coletados, começando pelas tabelas de roteamento que irão mostrar informações sobre as conexões de cada roteador, vindo em seguida os testes de ping que irão visualizar dados sobre a conectividade e por último os testes de traceroute que irão transparecer as rotas percorridas pelos pacotes.

4.1 Tabela de Roteamento

A tabela de roteamento possui registro dos destinos para o encaminhamento dos pacotes. As rotas podem ser estudadas manualmente por rotas estáticas ou redes diretamente conectadas e também podem ser aprendidas, dinamicamente, via protocolo de roteamento dinâmico como OSPF, BGP e outros, cada roteador possui sua própria tabela que é a base para toda funcionalidade do mesmo.

Neste trabalho, veremos as rotas estáticas sendo demonstradas pelo protocolo RIP que é representado pela letra “R” no terminal de comando dos roteadores do simulador Packet Tracer 5.3 e também pelas redes diretamente conectadas que se são representadas pela letra “C”; já as rotas dinâmicas serão demonstradas pelo protocolo OSPF que é representado pela letra “O”, a seguir estão expostas a tabelas de roteamento dos principais roteadores que estão presentes na simulação.

A seguir estarão sendo apresentadas as tabelas de roteamento da matriz e das filiais da empresa simulada, exibindo como estas estão configuradas e qual protocolo está fazendo o roteamento.

4.1.1 Matriz

Figura 10: Tabela de roteamento da matriz

```
Matriz(config)#do show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O    5.0.0.0/8 [110/300] via 12.0.0.2, 01:24:08, Serial3/0
               [110/300] via 10.0.0.2, 01:24:08, Serial2/0
C    6.0.0.0/8 is directly connected, Serial7/0
O    7.0.0.0/8 [110/150] via 12.0.0.2, 01:24:08, Serial3/0
C    10.0.0.0/8 is directly connected, Serial2/0
O    11.0.0.0/8 [110/150] via 10.0.0.2, 01:24:08, Serial2/0
C    12.0.0.0/8 is directly connected, Serial3/0
O    192.70.0.0/24 [110/101] via 12.0.0.2, 01:24:08, Serial3/0
C    192.168.0.0/24 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet1/0
O    192.168.7.0/24 [110/101] via 10.0.0.2, 01:24:08, Serial2/0
O    192.168.100.0/24 [110/151] via 12.0.0.2, 01:24:08, Serial3/0

Matriz(config)#
```

Fonte: Capturada pelo Autor, 2022.

Na imagem acima está exposta a tabela de roteamento do roteador alocado na matriz empresa, nele estão ligadas diretamente às redes 6.0.0.0, 10.0.0.0,12.0.0.0, 192.168.0.0 e 192.168.1.0 e através dos protocolos RIP e OSPF são configuradas e identificadas as outras redes indiretamente ligadas à rede da matriz. O roteador identifica as rotas e aplica o protocolo com melhor desempenho, por meio disso, podemos observar a predominância na escolha do Protocolo OSPF, apesar de todas as rotas terem se construídas pelo protocolo RIP.

Indiretamente, foram encontradas pelo Protocolo OSPF as Redes 5.0.0.0, 7.0.0.0, 11.0.0.0, 192.70.0.0, 192.168.7.0 e 192.168.100.0.

4.1.2 Filial 01

Figura 11: Tabela de roteamento da filial 01

```
Filial01>enable
Filial01#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Filial01(config)#do show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    5.0.0.0/8 is directly connected, Serial6/0
O    6.0.0.0/8 [110/250] via 11.0.0.1, 01:32:18, Serial3/0
O    7.0.0.0/8 [110/100] via 11.0.0.1, 01:32:18, Serial3/0
C    10.0.0.0/8 is directly connected, Serial2/0
C    11.0.0.0/8 is directly connected, Serial3/0
O    12.0.0.0/8 [110/200] via 10.0.0.1, 01:32:18, Serial2/0
                [110/200] via 11.0.0.1, 01:32:18, Serial3/0
O    192.70.0.0/24 [110/101] via 11.0.0.1, 01:32:18, Serial3/0
O    192.168.0.0/24 [110/101] via 10.0.0.1, 01:32:18, Serial2/0
O    192.168.1.0/24 [110/101] via 10.0.0.1, 01:32:18, Serial2/0
C    192.168.7.0/24 is directly connected, FastEthernet0/0
O    192.168.100.0/24 [110/51] via 11.0.0.1, 01:32:18, Serial3/0
Filial01(config)#
```

Fonte: Capturada pelo Autor, 2022.

Na figura 11 está sendo demonstrada a tabela de roteamento do roteador alocado na filial 01 da empresa, nele estão ligadas diretamente às redes 5.0.0.0, 10.0.0.0, 11.0.0.0 e 192.168.7.0 que também e através dos protocolos RIP e OSPF são configuradas e identificadas as outras redes indiretamente ligadas à rede da Filial 01. Aqui, também, o roteador identifica as rotas e aplica o protocolo com melhor desempenho, podemos observar a predominância na escolha do Protocolo OSPF apesar de todas rotas também estarem feitas pelo protocolo RIP.

Indiretamente, foram encontradas pelo Protocolo OSPF as Redes 6.0.0.0, 7.0.0.0, 12.0.0.0, 192.70.0.0, 192.168.0.0, 192.168.1.0 e 192.168.100.0.

4.1.3 Filial 02

Figura 12: Tabela de roteamento da filial 02

```
Filial02>enable
Filial02#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Filial02(config)#do show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    5.0.0.0/8 is directly connected, Serial6/0
O    6.0.0.0/8 [110/250] via 7.0.0.1, 00:09:06, Serial3/0
C    7.0.0.0/8 is directly connected, Serial3/0
O    10.0.0.0/8 [110/200] via 12.0.0.1, 00:09:06, Serial2/0
                [110/200] via 7.0.0.1, 00:09:06, Serial3/0
O    11.0.0.0/8 [110/100] via 7.0.0.1, 00:09:06, Serial3/0
C    12.0.0.0/8 is directly connected, Serial2/0
C    192.70.0.0/24 is directly connected, FastEthernet0/0
O    192.168.0.0/24 [110/101] via 12.0.0.1, 00:09:16, Serial2/0
O    192.168.1.0/24 [110/101] via 12.0.0.1, 00:09:16, Serial2/0
O    192.168.7.0/24 [110/101] via 7.0.0.1, 00:09:06, Serial3/0
O    192.168.100.0/24 [110/51] via 7.0.0.1, 00:09:06, Serial3/0
Filial02(config)#
```

Fonte: Capturada pelo Autor, 2022.

A tabela de roteamento do roteador alocado na filial 02 da empresa que está sendo mostrada na figura 12, onde estão ligadas diretamente às redes 5.0.0.0, 7.0.0.0, 12.0.0.0 e 192.70.0.0 que também e através dos protocolos RIP e OSPF são configuradas e identificadas as outras redes indiretamente ligadas à rede da Filial 02. Bem como também ocorre o mesmo processo no roteador que identifica as rotas e aplica o protocolo com melhor desempenho.

Indiretamente foram encontradas pelo Protocolo OSPF as Redes 6.0.0.0, 10.0.0.0, 11.0.0.0, 192.168.0.0, 192.168.1.0, 192.168.7.0 e 192.168.100.0.

4.1.4 Filial 03

Figura 13: Tabela de roteamento da filial 03

```
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#do show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O    5.0.0.0/8 [110/250] via 7.0.0.2, 01:00:44, Serial3/0
               [110/250] via 11.0.0.2, 01:00:44, Serial2/0
C    6.0.0.0/8 is directly connected, Serial6/0
C    7.0.0.0/8 is directly connected, Serial3/0
O    10.0.0.0/8 [110/150] via 11.0.0.2, 01:00:44, Serial2/0
C    11.0.0.0/8 is directly connected, Serial2/0
O    12.0.0.0/8 [110/150] via 7.0.0.2, 01:00:44, Serial3/0
O    192.70.0.0/24 [110/51] via 7.0.0.2, 01:00:44, Serial3/0
O    192.168.0.0/24 [110/151] via 7.0.0.2, 01:00:44, Serial3/0
                    [110/151] via 11.0.0.2, 01:00:44, Serial2/0
O    192.168.1.0/24 [110/151] via 7.0.0.2, 01:00:44, Serial3/0
                    [110/151] via 11.0.0.2, 01:00:44, Serial2/0
O    192.168.7.0/24 [110/51] via 11.0.0.2, 01:00:44, Serial2/0
C    192.168.100.0/24 is directly connected, FastEthernet1/0
Router(config)#
```

Fonte: Capturada pelo Autor, 2022.

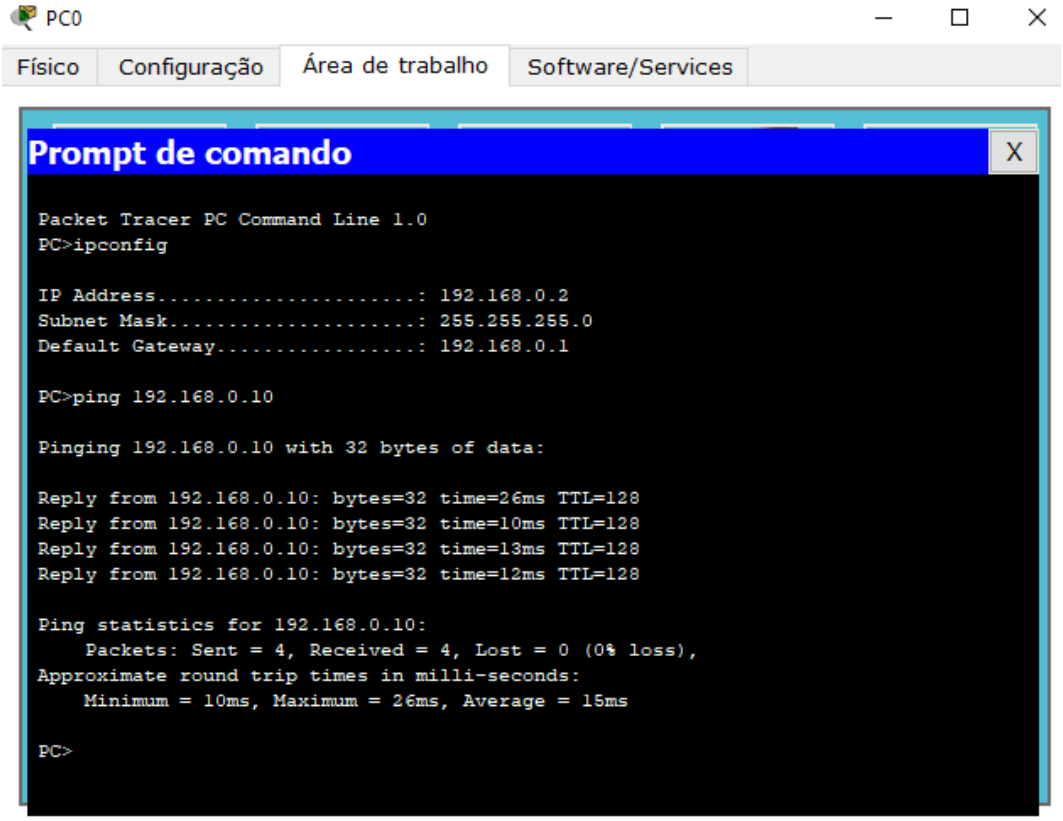
Conforme se pode observar na imagem acima onde está sendo exposta a tabela de roteamento do roteador alocado na filial 03 da empresa, nele estão ligadas diretamente às redes 6.0.0.0, 7.0.0.0, 11.0.0.0 e 192.168.100.0 que também e através dos protocolos RIP e OSPF são configuradas e identificadas as outras redes indiretamente ligadas à rede da Filial 03. Também ocorre o mesmo processo no roteador que identifica as rotas e aplica o protocolo com melhor desempenho.

Indiretamente foram encontradas pelo Protocolo OSPF as Redes 5.0.0.0, 10.0.0.0, 12.0.0.0, 192.70.0.0, 192.168.0.0, 192.168.1.0 e 192.168.7.0.

4.2 PING

Teste que tem como finalidade verificar o estado da conexão entre dois host's distintos e retorna se há perdas, tempo de resposta e quanto de perda está tendo.

Figura 14: Teste de Ping do host PC0 para o host PC11 dentro da Rede 192.168.0.0



Fonte: Capturada pelo Autor, 2022.

Na figura 14 está sendo realizado um teste de conectividade utilizando ping para verificar o estado da conexão entre um host de endereço ip 192.168.0.2 dentro da rede 192.168.0.0 para um outro de endereço ip 192.168.0.10 dentro da mesma rede, foi verificado que há comunicação, pois 100% dos pacotes enviados no teste foram recebidos com média de 15ms de velocidade de resposta.

Na tabela 13 logo abaixo, estão sendo demonstrados todos os resultados de teste de ping realizados em todas redes locais da simulação, nos mesmos é possível verificar que conectividade para todas lan's é de 100% de conectividade, o que afirma que não está havendo problemas de conexão dentro das redes internas, se houvesse

sinais de perdas de pacotes a porcentagem se diminuiria e deveríamos então começar a tratar os possíveis motivos de perda de conexão.

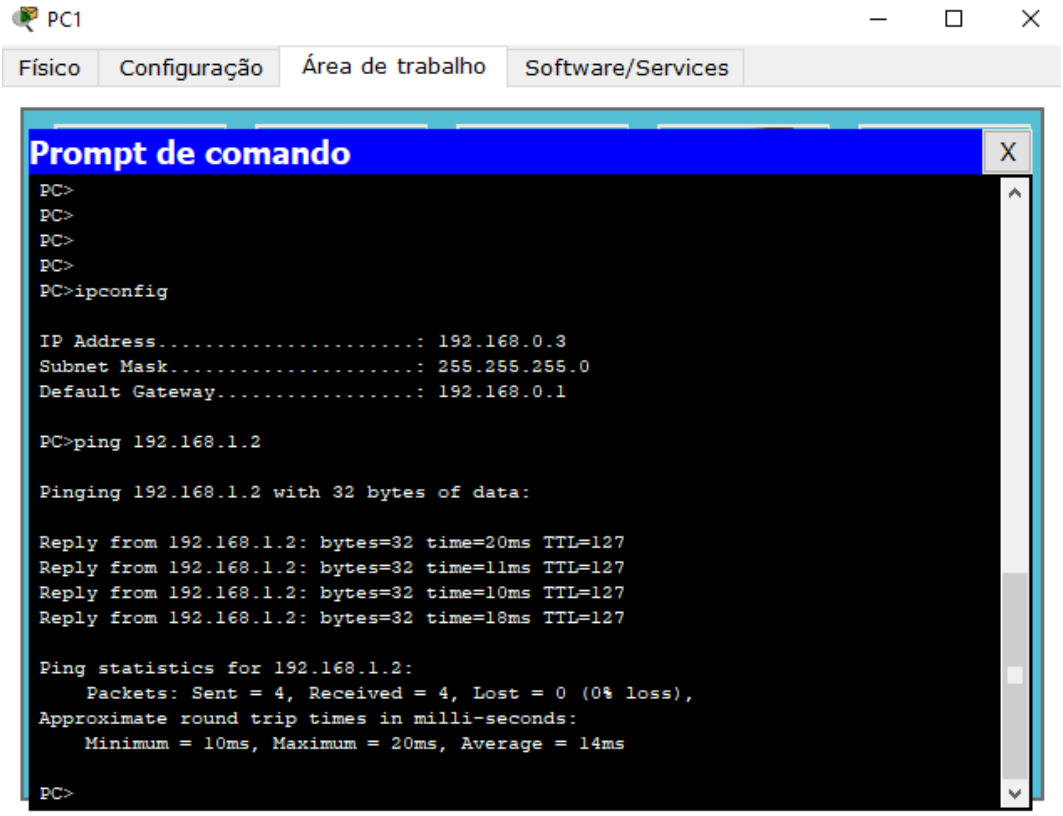
Tabela 13. Teste de ping nas redes locais

	IP's		Tempo de resposta			
Ord.	Origem	Destino	Mínimo	Média	Máximo	Conectividade
1º	192.168.0.2	192.168.0.10	10ms	15ms	26ms	100%
2º	192.168.1.4	192.168.1.5	20ms	28ms	46ms	100%
3º	192.168.7.5	192.168.7.4	22ms	28ms	42ms	100%
4º	192.168.100.14	192.168.100.15	9ms	12ms	21ms	100%
5º	192.70.0.6	192.70.0.12	10ms	14ms	17ms	100%

Fonte: Elaborado pelo autor, 2022.

Outra característica que também pode se notar ainda na tabela acima é o tempo de resposta de cada teste, que é variável em cada lan por conta de fatores como distância entre os host's, atenuação e interferência sofrida pela conexão. O que quando gerar ruídos que possam influenciar no desempenho da rede e nas atividades dos usuários deve ser tratado com a mudança de rotas, aplicação de meios mais estáveis, como exemplo mudar conexões wireless para conexões cabeadas e assim por diante. Diante disso é por essa razão que nos testes de ping realizados nas redes locais de endereços 192.168.1.0 e 192.168.7.0 se obtém médias de respostas maiores visto que essas redes são híbridas, ou seja, tem em sua composição parte cabeada e parte rede sem fio. Nota se ainda que a menor média é do teste realizado na rede 192.168.100.0 e essa é completamente cabeada e tem maior proximidade dos host's.

Figura 15: Teste de Ping do host PC1 para o host PC2 entre as redes 192.168.0.0 e a 192.168.1.0



Fonte: Capturada pelo Autor, 2022.

Constata-se na figura 15 que um teste de conectividade está sendo realizado utilizando ping para verificar o estado da conexão entre um host de endereço ip 192.168.0.3 dentro da rede local (192.168.0.0) para um outro de endereço ip 192.168.1.2 dentro de uma outra rede local (192.168.1.0), foi verificado que há comunicação pois 100% dos pacotes enviados no teste foram recebidos com média de 14ms de velocidade de resposta.

Na tabela 14 que está abaixo deste parágrafo, estão sendo expostos os resultados dos testes de ping realizados entre as redes locais, utilizando assim a estrutura de rede metropolitana, nestes testes encontramos também para todos os resultados com nenhuma perda de pacotes, deixando em evidência que há conexão entre todas as filiais. Caso houvesse algum teste dessa fase com perda, seria necessário verificamos as configurações e a infraestrutura de rede man para resolver o problema e chegar ao cenário ideal de conexão em 100% para todas as rotas.

Tabela 14. Teste de ping entre as redes locais (Man)

	IP’s		Tempo de resposta			
Ord.	Origem	Destino	Mínimo	Média	Máximo	Conectividade
1º	192.168.0.3	192.168.1.2	10ms	14ms	20ms	100%
2º	192.168.0.3	192.168.7.2	20ms	25ms	28ms	100%
3º	192.168.0.3	192.168.100.5	12ms	21ms	31ms	100%
4º	192.168.0.3	192.70.0.2	15ms	21ms	28ms	100%
5º	192.168.1.2	192.168.7.4	37ms	39ms	43ms	100%
6º	192.168.1.2	192.168.100.4	29ms	32ms	34ms	100%
7º	192.168.1.2	192.70.0.3	15ms	23ms	29ms	100%
8º	192.168.7.5	192.168.100.17	40ms	41ms	43ms	100%
9º	192.168.7.5	192.70.0.8	20ms	37ms	45ms	100%
10º	192.168.100.13	192.70.0.9	26ms	28ms	30ms	100%

Fonte: Elaborado pelo autor, 2022.

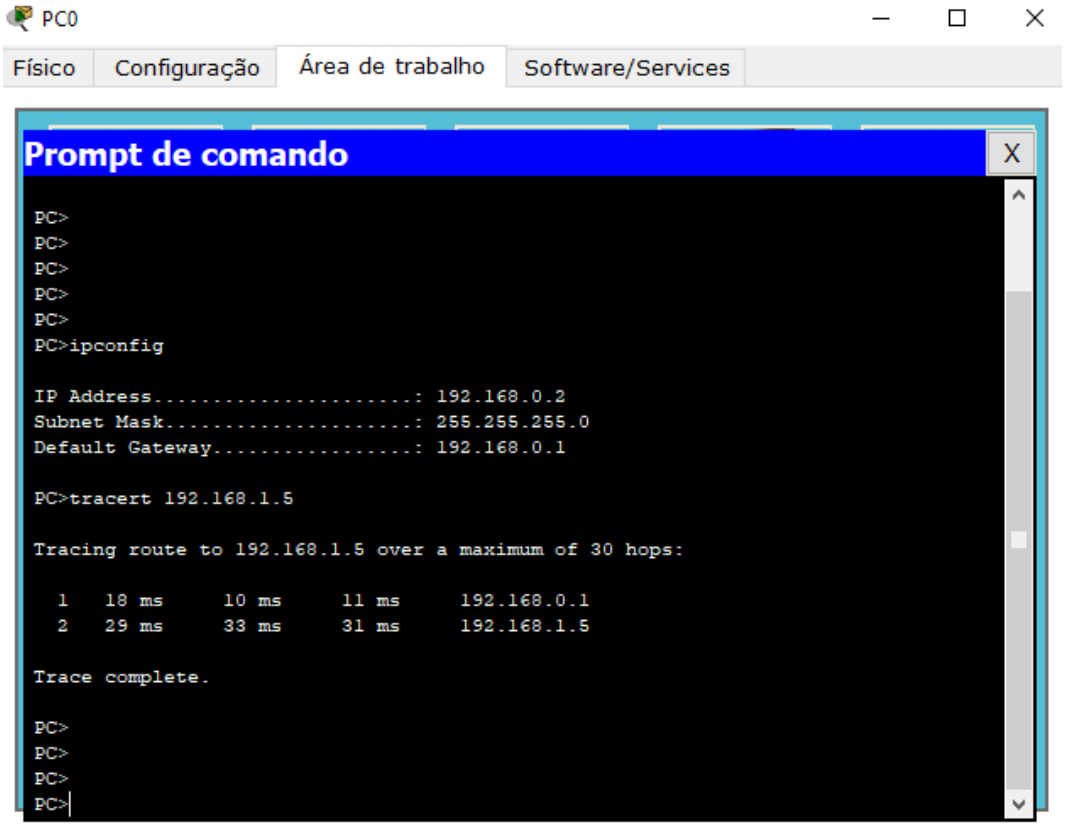
Outras informações importantes que os teste de ping na rede man descritos na tabela trazem é que as médias de tempo de resposta são maiores naqueles que são feitos onde se envolvem redes hibridas e também entre redes que tem uma distância mais acentuada, tendo como base essa informação também entendemos então o motivo do teste realizado entre as rede 192.168.0.0 e a rede 192.168.1.0 ter sido o de média mais baixa, visto que essas lan’s estão ligadas ao mesmo roteador de borda e não utilizando um backbone de ligação entre elas como as outras redes, sendo assim o roteador de borda que liga elas são utiliza portas diferentes para fazer a conexão das mesmas.

4.3 Traceroute

Ferramenta que traça rotas entre dois host's , apresentado o caminho percorrido pelos pacotes, se estes se perdem e o tempo que levam percorrendo cada parte do caminho. Foram realizados vários testes utilizando a ferramenta traceroute dentro das redes locais, estes retornaram resultados semelhantes de um salto apenas e respostas aceitáveis.

Nas figuras a seguir foram realizados teste utilizando a mesma ferramentas só que dessa vez entre as redes locais, utilizando a infraestrutura da rede man, verificando assim todo percurso que os pacotes fazem de uma filial a outra.

Figura 16: Teste de traceroute entre o host PC0 da rede 192.168.0.0 para e o host Laptop0 da rede 192.168.1.0

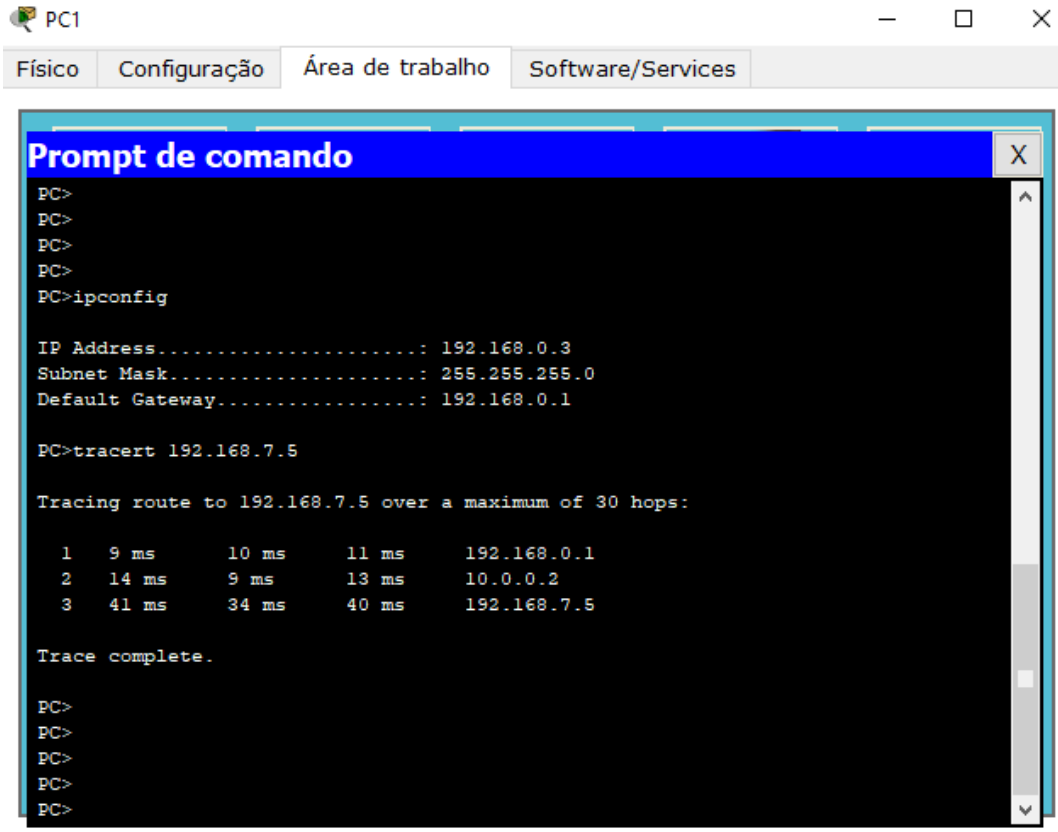


Fonte: Capturada pelo Autor, 2022.

Na figura 16 está sendo realizado um teste de traceroute que vai identificar os saltos e a rota de um host de endereço ip 192.168.0.2 dentro da rede local 192.168.0.0 para um host de endereço ip 192.168.1.5 dentro de uma outra rede local (192.168.1.0), verificando-se que, em 2 saltos, o pacote chega ao destino, este passa pelo gateway (192.168.0.1) da rede do host de origem e é encaminhado para o host de destino que é localizado em uma rede local próxima (192.168.1.0).

Teste de traceroute entre o host PC1 da rede 192.168.0.0 para e o host Pda2 da rede 192.168.7.0

Figura 17: Teste de traceroute entre o host PC1 da rede 192.168.0.0 para e o host Pda2 da rede 192.168.7.0

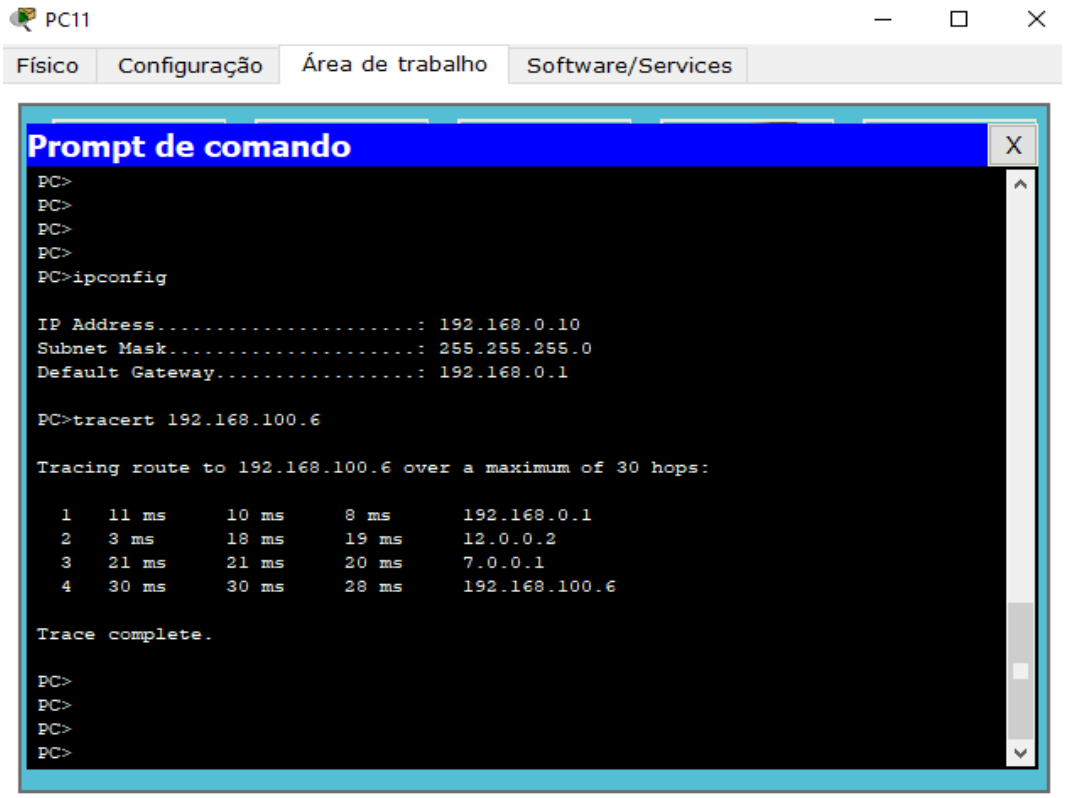


Fonte: Capturada pelo Autor, 2022.

A figura 17 mostra um teste de traceroute que vai identificar os saltos e a rota de um host de endereço ip 192.168.0.3 dentro da rede local 192.168.0.0 para um host de endereço ip 192.168.7.5 dentro de uma outra rede local (192.168.7.0), verificou-se que, em 3 saltos, o pacote chega ao destino, ele passa pelo gateway (192.168.0.1) da rede do host de origem e é encaminhado para um roteador (10.0.0.2) que sinaliza o host de destino que é localizado em uma rede local próxima (192.168.7.0).

Teste de traceroute entre o host PC11 da rede 192.168.0.0 para e o host Fl03PC05 da rede 192.168.100.0

Figura 18: Teste de traceroute entre o host PC11 da rede 192.168.0.0 para e o host Fl03PC05 da rede 192.168.100.0

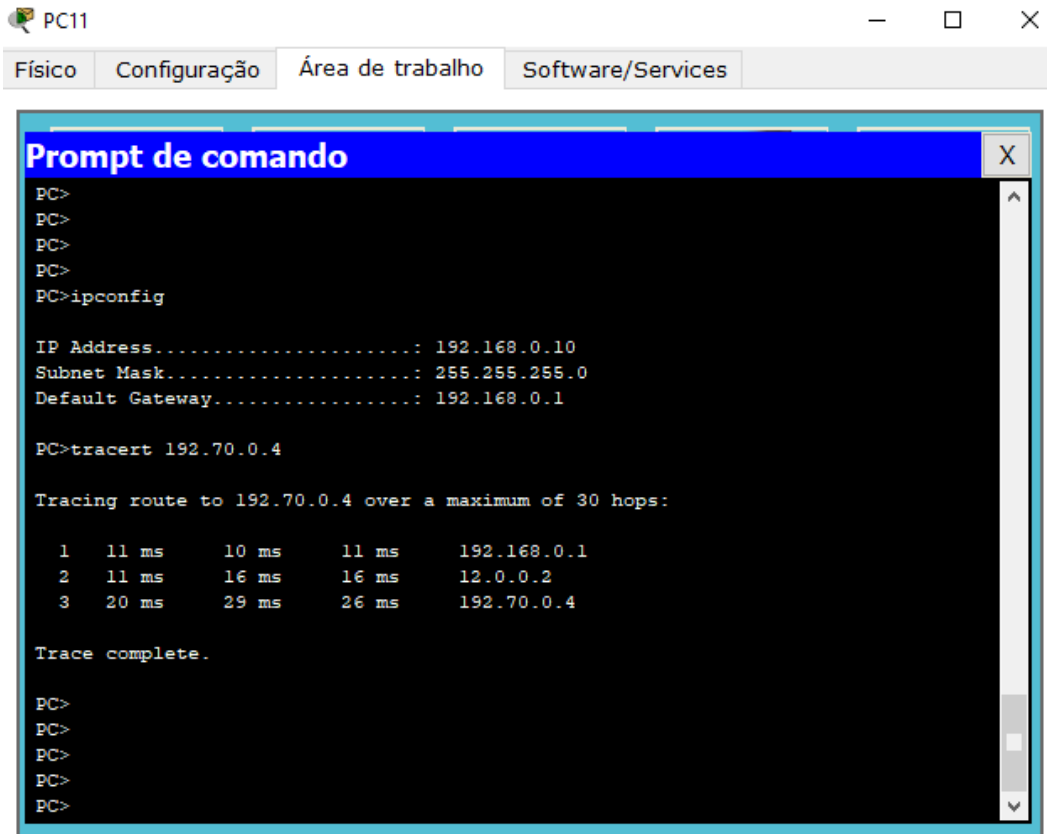


Fonte: Capturada pelo Autor, 2022.

Nota-se um teste de traceroute na figura 18, este que vai identificar os saltos e a rota de um host de endereço ip 192.168.0.10 dentro da rede local 192.168.0.0 para um host de endereço ip 192.168.100.6 dentro de uma outra rede local (192.168.100.0), verificando-se que, em 4 saltos, o pacote chega ao destino, tal pacote passa pelo gateway (192.168.0.1) da rede do host de origem e é encaminhado para um roteador (12.0.0.2) que se comunica com outro roteador (7.0.0.1) que tem na sua tabela de roteamento o endereço da rede (192.168.100.0) que o host de destino pertence e é localizado.

Teste de traceroute entre o host PC11 da rede 192.168.0.0 para e o host PC7 da rede 192.70.0.0

Figura 19: Teste de traceroute entre o host PC11 da rede 192.168.0.0 para e o host PC7 da rede 192.70.0.0

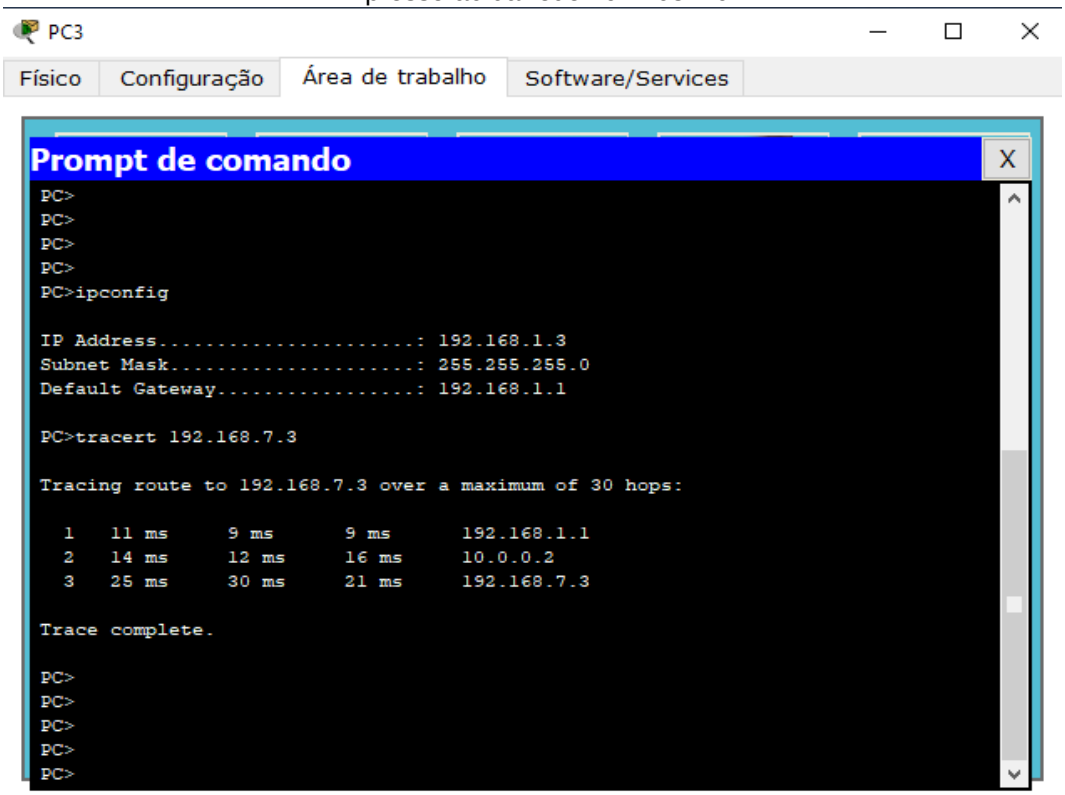


Fonte: Capturada pelo Autor, 2022.

A partir da imagem acima, é possível notar que está sendo realizado um teste de traceroute que vai identificar os saltos e a rota de um host de endereço ip 192.168.0.10, dentro da rede local 192.168.0.0, para um host de endereço ip 192.70.0.4, dentro de uma outra rede local (192.168.7.0), verificando-se assim que, em 3 saltos, o pacote chega ao destino; o pacote passa pelo gateway (192.168.0.1) da rede do host de origem e é encaminhado para um roteador (10.0.0.2) que sinaliza o host de destino que é localizado em uma rede local próxima (192.168.7.0).

Teste de traceroute entre o host PC3 da rede 192.168.1.0 para e o host Impressora0 da rede 192.168.7.0

Figura 20: Teste de traceroute entre o host PC3 da rede 192.168.1.0 para e o host Impressora0 da rede 192.168.7.0

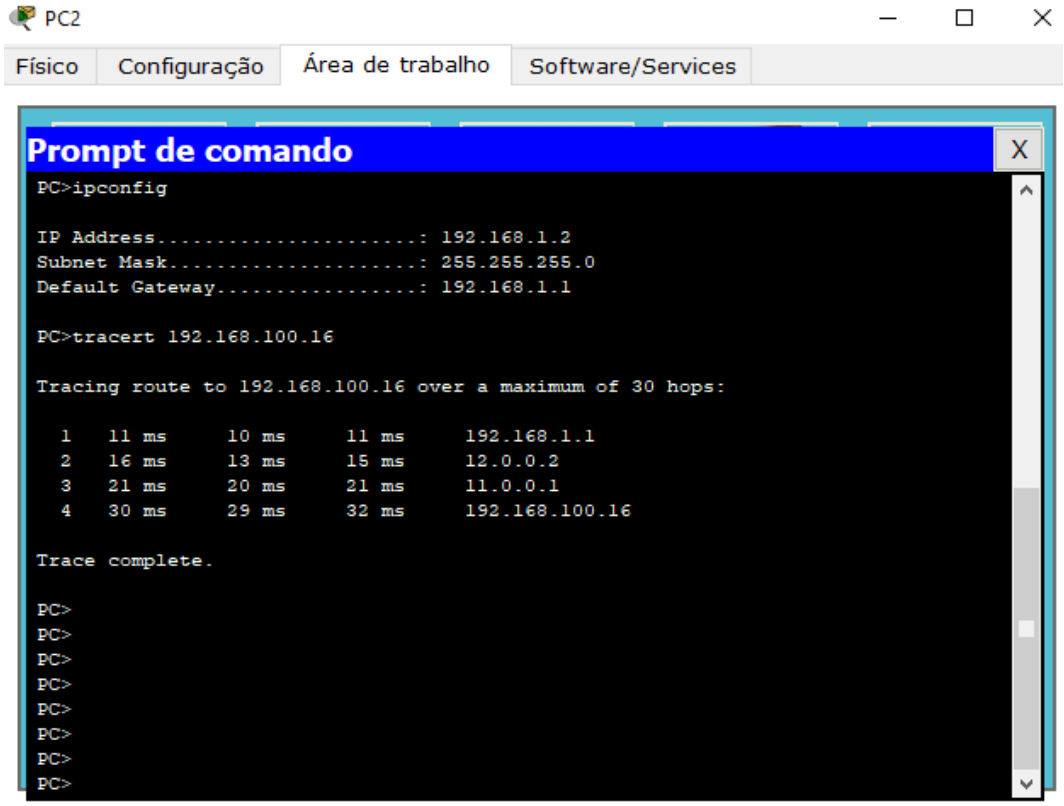


Fonte: Capturada pelo Autor, 2022.

Conforme a figura 20, onde está sendo realizado um teste de traceroute que vai identificar os saltos e a rota de um host de endereço ip 192.168.1.3, dentro da rede local 192.168.1.0, para um host de endereço ip 192.168.7.3, dentro de uma outra rede local (192.168.7.0); verificou-se se que, em 3 saltos, o pacote chega ao destino, o pacote passa pelo gateway (192.168.1.1) da rede do host de origem e é encaminhado para um roteador (10.0.0.2) que sinaliza o host de destino, localizado em uma rede local próxima (192.168.7.0).

Teste de traceroute entre o host PC2 da rede 192.168.1.0 para e o host Impressora3 da rede 192.168.100.0

Figura 21: Teste de traceroute entre o host PC2 da rede 192.168.1.0 para e o host Impressora3 da rede 192.168.100.0

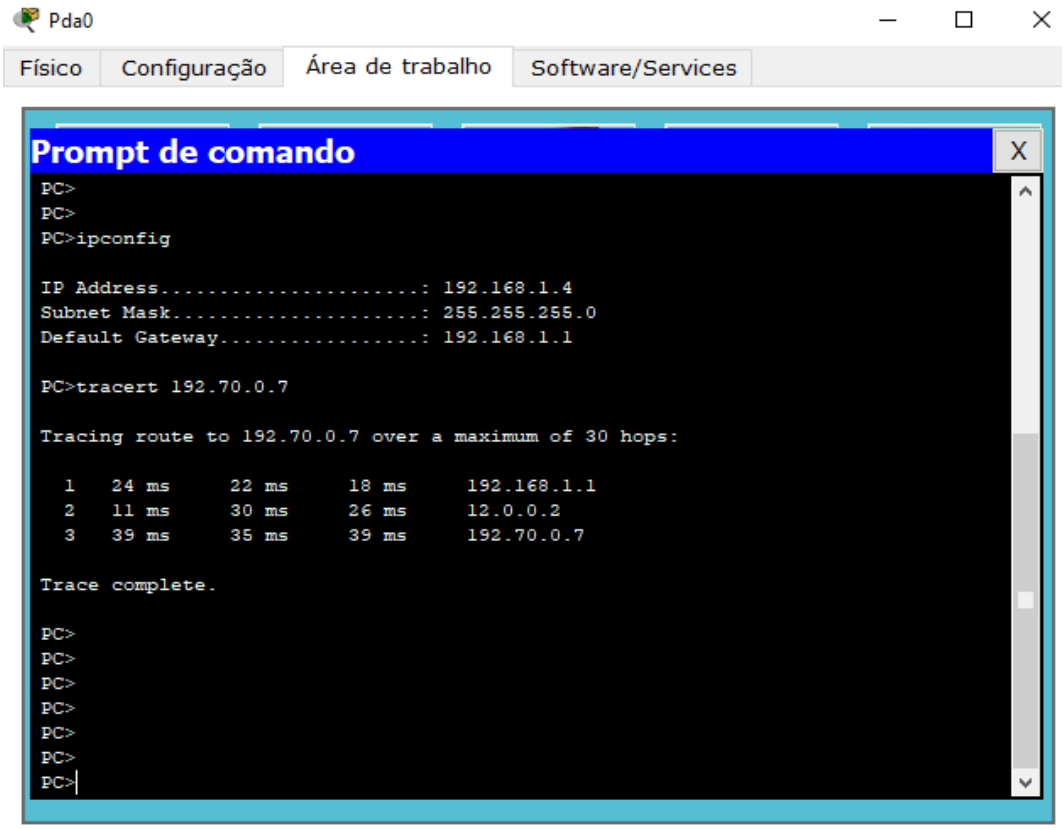


Fonte: Capturada pelo Autor, 2022.

Como mostrado na figura 21, está sendo realizado um teste de traceroute que vai identificar os saltos e a rota de um host de endereço ip 192.168.1.2, dentro da rede local 192.168.1.0, para um host de endereço ip 192.168.100.16, dentro de uma outra rede local (192.168.100.0), verificando-se que, em 4 saltos, o pacote chega ao destino, o pacote passa pelo gateway (192.168.1.1) da rede do host de origem e é encaminhado para um roteador (12.0.0.2) que se comunica com outro roteador (11.0.0.1) que tem, na sua tabela de roteamento, o endereço da rede (192.168.100.0) que o host de destino pertence e é localizado.

Teste de traceroute entre o host Pda0 da rede 192.168.1.0 para e o host Impressora2 da rede 192.70.0.0

Figura 22: Teste de traceroute entre o host Pda0 da rede 192.168.1.0 para e o host Impressora2 da rede 192.70.0.0

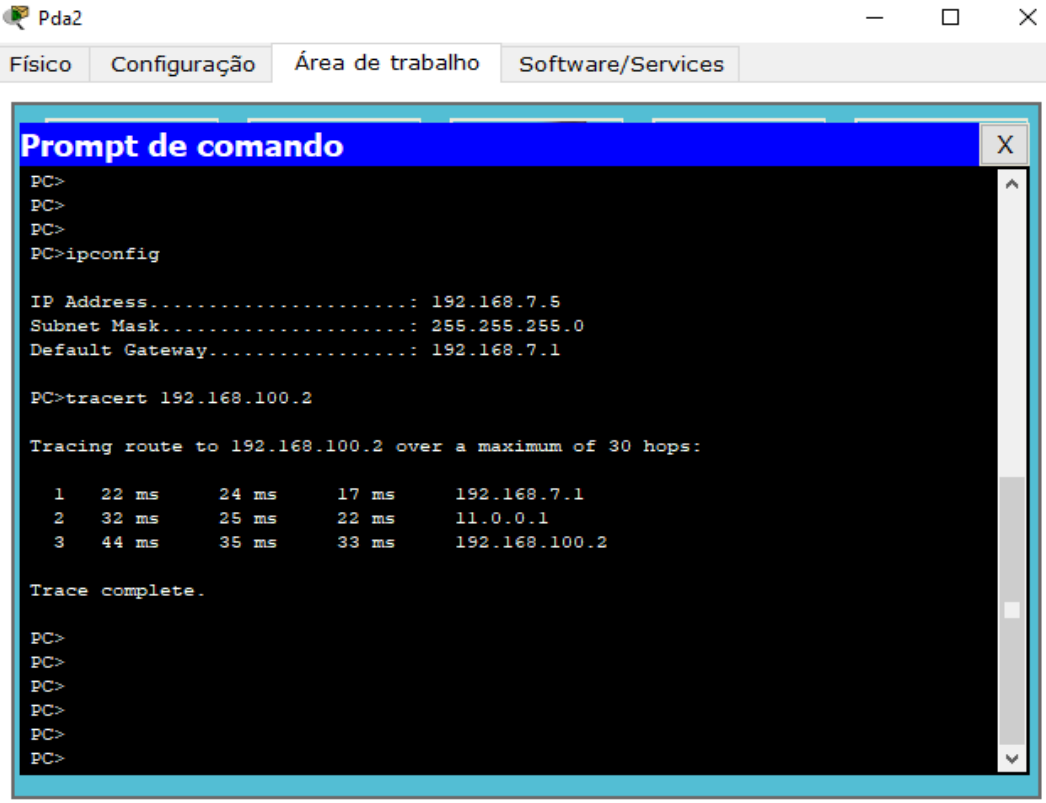


Fonte: Capturada pelo Autor, 2022.

Na figura 22 está sendo realizado um teste de traceroute que vai identificar os saltos e a rota de um host de endereço ip 192.168.1.4, dentro da rede local 192.168.1.0, para um host de endereço ip 192.70.0.7, dentro de uma outra rede local (192.70.0.0), verificando-se que, em 3 saltos, o pacote chega ao destino, o pacote passa pelo gateway (192.168.1.1) da rede do host de origem e é encaminhado para um roteador (12.0.0.2) que sinaliza o host de destino localizado em uma rede local próxima (192.70.0.0).

Teste de traceroute entre o host Pda2 da rede 192.168.7.0 para e o host Fl03PC01 da rede 192.168.100.0

Figura 23: Teste de traceroute entre o host Pda2 da rede 192.168.7.0 para e o host Fl03PC01 da rede 192.168.100.0

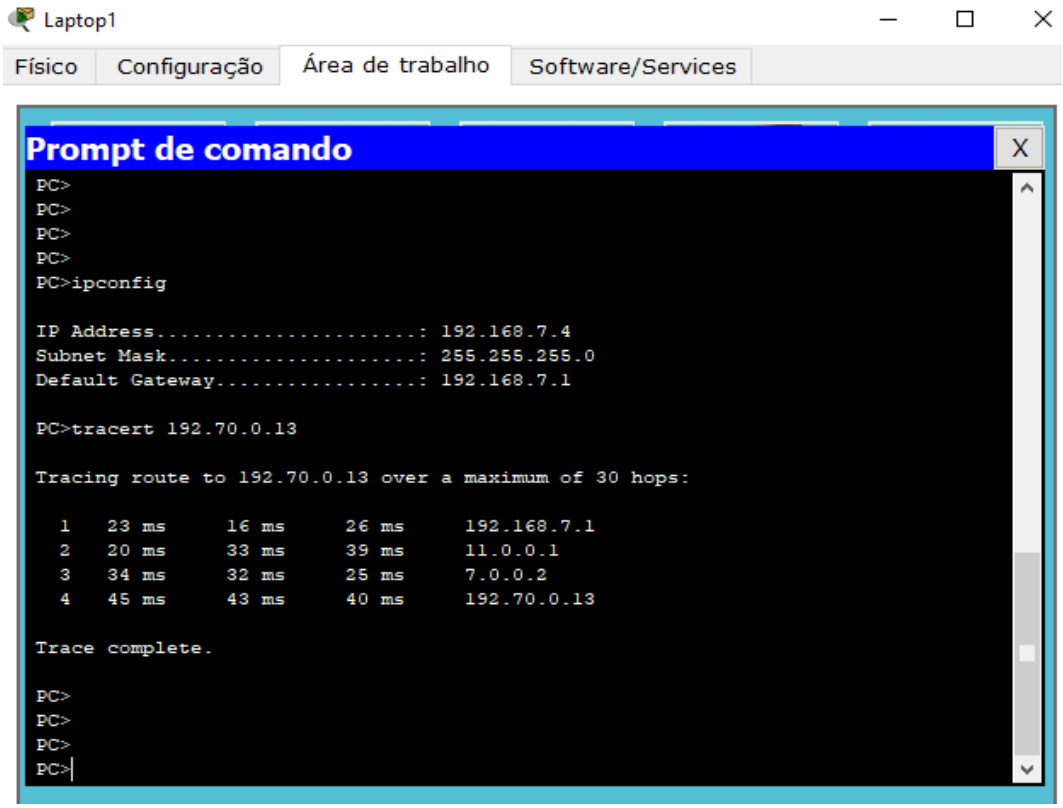


Fonte: Capturada pelo Autor, 2022.

Na imagem acima está sendo realizado um teste de traceroute que vai identificar os saltos e a rota de um host de endereço ip 192.168.7.5, dentro da rede local 192.168.7.0, para um host de endereço ip 192.168.100.2, dentro de uma outra rede local (192.168.100.0), verificando-se que, em 3 saltos, o pacote chega ao destino, o pacote passa pelo gateway (192.168.7.1) da rede do host de origem e é encaminhado para um roteador (11.0.0.2) que sinaliza o host de destino que é localizado em uma rede local próxima (192.168.100.0).

Teste de traceroute entre o host Laptop1 da rede 192.168.7.0 para e o host Impressora1 da rede 192.70.0.0

Figura 24: Teste de Teste de traceroute entre o host Laptop1 da rede 192.168.7.0 para e o host Impressora1 da rede 192.70.0.0

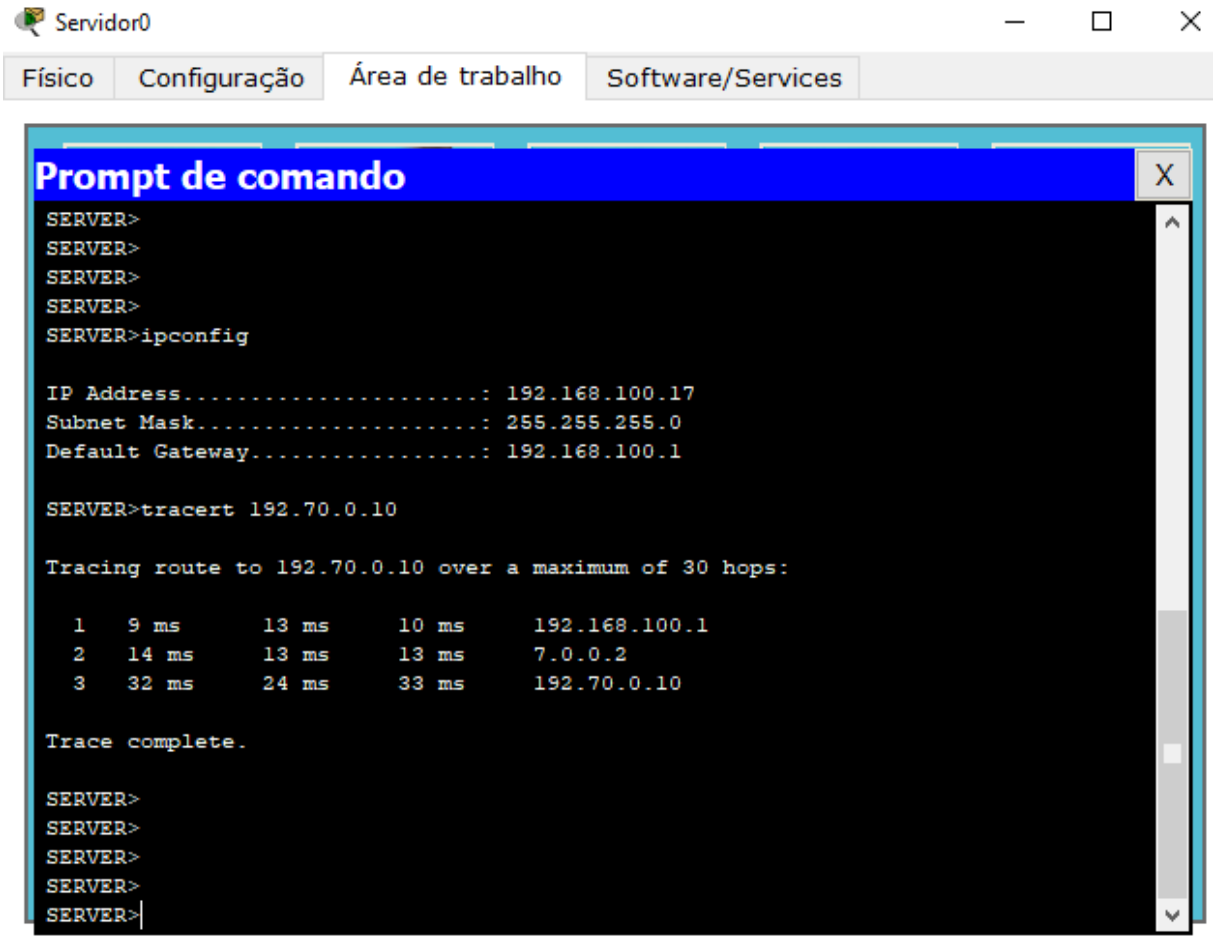


Fonte: Capturada pelo Autor, 2022.

Na figura 24 está sendo realizado um teste de traceroute que vai identificar os saltos e a rota de um host de endereço ip 192.168.7.4 dentro da rede local 192.168.7.0 para um host de endereço ip 192.70.0.13 dentro de uma outra rede local (192.70.0.0), verificando-se que, em 4 saltos, o pacote chega ao destino; o pacote passa pelo gateway (192.168.7.1) da rede do host de origem e é encaminhado para um roteador (11.0.0.1) que se comunica com outro roteador (7.0.0.2) que tem, na sua tabela de roteamento, o endereço da rede (192.70.0.0) que o host de destino pertence e é localizado.

Teste de traceroute entre o host Servidor0 da rede 192.168.100.0 para o host Laptop4 da rede 192.70.0.0

Figura 25: Teste de traceroute entre o host Servidor0 da rede 192.168.100.0 para o host Laptop4 da rede 192.70.0.0



Fonte: Capturada pelo Autor, 2022.

Conforme se pode observar na figura 25, está sendo realizado um teste de traceroute que vai identificar os saltos e a rota de um host de endereço ip 192.168.100.17, dentro da rede local 192.168.100.0, para um host de endereço ip 192.70.0.10, dentro de uma outra rede local (192.70.0.0), verificando-se que, em 3 saltos, o pacote chega ao destino; este passa pelo gateway (192.168.100.1) da rede do host de origem e é encaminhado para um roteador (7.0.0.2) que sinaliza o host de destino que é localizado em uma rede local próxima (192.70.0.0).

5. CONCLUSÃO

Tendo em vista os aspectos observados na simulação, constatou-se que esta apresenta comunicação entre as várias filiais da empresa e a sua sede, além de, entre os departamentos e hosts, conseguimos verificar o principal fundamento do uso da simulação neste projeto, que é evitar falhas, erros, bem como reduzir custos e o tempo de execução de um projeto de rede MAN.

Em suma, ainda pode se alterar alguns parâmetros e configurações na simulação, observando como ela se comporta e ainda como modifica a estrutura, adicionando outras rotas, outros host's ou até reduzindo os mesmos dentro do cenário, tudo isso para verificar falhas, escalabilidade, latência e a usabilidade da rede com as modificações realizadas.

5.1 Visão geral

Desse modo, neste cenário é possível notar, em tempo real, problemas que se apresentam ainda na simulação, já os corrigir e otimizar o projeto, verificando também como se comportariam após as modificações. Logo, é necessário usar a simulação para medir a capacidade máxima de utilização das redes, verificando os limites de banda, vazão, prevendo assim gargalhos e atrasos nos envios dos pacotes.

Observando, também, as escolhas das rotas, saltos e entendendo acerca da tomada de decisão por essas rotas, visando sempre otimizar e estabilizar as melhores rotas e diminuir o tempo de resposta.

5.2 Resultados obtidos

Os resultados coletados mostraram que após as configurações e a realização dos testes de ping, há 100% de conexão em toda rede, garantindo assim o sucesso do projeto quando reproduzido no meio físico, se usado os parâmetros aqui aplicados na simulação.

Em contrapartida, os testes de traceroute mostraram que com os protocolos RIP e OSPF configurados, todas as rotas estão funcionando e dando tempo de resposta dentro do tolerável, o protocolo OSPF se sobressai, pois busca usar sempre o caminho mais curto, é mais rápido e leve.

5.3 Principais dificuldades

Como principais dificuldades desse projeto estão as configurações das VLAN's e a falta de alguns recursos que facilitariam a coleta e a análise de dados. A escassez de matérias guias para a aplicação das configurações de VLAN's é tida como a maior dentre as mais distintas dificuldades.

O ajuste das configurações e os testes para que se chegasse a um resultado de 100% de conectividade também pode ser citado como uma dificuldade pois se fez necessário várias baterias de modificações, de erros e acertos para se encontrar os parâmetros ideais.

Outras dificuldades encontradas foram a construção da rede de maneira que essa previsse a escalabilidade para crescimento de pontos de rede, número de host's e usuários. E também a elaboração de rotas que ficassem como redundância para os canais de comunicação entre as filiais.

5.4 Trabalhos futuros

Para trabalhos futuros tem se a intenção de desenvolver simulações maiores e mais seguras, com mais divisões por VLAN's, fluxo de dados entre filiais e matriz por VPN (*Virtual Private Network*), aplicação de configurações de Proxy, portas, melhor administração de rede e exposição de resultados através de uma variedade maior de teste e configurações.

Aumentar os cenários, buscando ainda em consonância diminuir os ruídos causados por interferências e alternações.

6. REFERÊNCIAS

ASSIS, U. de, ALVES JUNIOR, N. **Protocolos de Roteamento RIP e OSPF**. Rede Rio de Computadores, FAPERJ, 2001. Disponível em: http://www.rederio.br/downloads/pdf/nt01100.pdf. Acesso em: 19 de fevereiro de 2020.

BARROS, Odair Soares. **Segurança de redes locais com a implementação de VLANs – O caso da Universidade Jean Piaget de Cabo Verde**. Universidade Jean Piaget de Cabo Verde, 2009.

BEHROUZ, A. FOROUZAN. **Comunicação de dados e Redes de computadores**. Bookman, 2006.

Bezerra, Romildo Martins da Silva e Neto, Manoel Marques. 2002. **Protocolos de Roteamento**. Salvador. Monografia da disciplina Laboratório de Redes II do CALDAS FILHO, Francisco Lopes; FERREIRA, Pedro Ernesto de Brito**. Projeto e implantação de uma nova topologia de rede de computadores para o Laboratório de Informática LINF/CIC/UnB**. 2013.

CARRARO, Kleverton S. Protocolos de Roteamento Benefícios e Características Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

CISCO NETWORKING ACADEMY (Estados Unidos). Cisco Packet Tracer. 2010. Disponível em: http://www.cisco.com/c/dam/en_us/training-events/netacad/course_catalog/docs/Cis o_PacketTracer_AAG.pdf. Acesso em: 14 de janeiro de 2019.
CUNHA, Jaqueline de Souza. **Protocolos de roteamento dinâmico RIP e OSPF** / Jaqueline de Souza Cunha. Fundação Educacional do Município de Assis – FEMA – Assis, 2018. 60p. Curso de Mestrado de Redes. UNIFACS.

DANTAS, Mario, A. R. **Computação distribuída de alto desempenho**. Axcel Books, 2005.

FERRAZ, Tatiana Lopes; ALBUQUERQUE, Marcelo Portes; ALBUQUERQUE, Márcio Portes **2002. Introdução ao ping e traceroute.** Disponível em: http://www.rederio.br/downloads/pdf/nt01002.pdf. Acesso em: 19 de fevereiro de 2020.

FILIPPETI, Marco A. **CCNA 5.0: guia completo de estudo**. Florianópolis: Visual Books, 2014.

FILIPPETTI, Marco Aurélio. **CCNA 4.1 – Guia Completo de Estudos.** Florianópolis: Editora Visual Books, 2008.

FRINHANI, Rafael de Magalhães Dias. **Projeto de Reestruturação do Gerenciamento e Otimização da Rede Computacional da Universidade Federal de Lavras**. **Universidade Federal de Lavras**, v. 4, n. 9, 2005.

HAFFERMANN, Leonardo. **Segmentação de Redes com VLAN**. 2009. 23 f. Monografia (Especialização) - Curso de Redes e Segurança de Sistemas, Pontifícia Universidade Católica do Paraná, Curitiba, 2009. Disponível em: http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Leonardo Haffermann - Artigo.pdf. Acesso em: 21 de janeiro de 2020.

JAIRO. **Roteamento: Roteamento estático, roteamento dinâmico e métricas, protocolos de roteamento (Vetor de Distância, Estado de Enlace), protocolos RIP e OSPF.** 2018. Disponível em: http://www.jairo.pro.br/arq_tcp_ip_e_redes_de_comput/roteamento.pdf. Acesso em: 12 de fevereiro de 2020.

KUROSE, JAMES F. **Redes de computadores e a Internet: uma abordagem top-down** / James F. Kurose e Keith W. Ross; tradução Opportunity translations; revisão técnica Wagner Zucchi. -- 5. ed. -- São Paulo: Addison Wesley, 2009.

MEDEIROS, Ronaldo Maia et al. **Uma Análise de Desempenho da Rede Metropolitana de Telemedicina dos Hospitais Universitários da Cidade de Natal-RN/Brasil**. **HOLOS**, v. 4, p. 153-174, 2014.

MOTA FILHO, Joao Eriberto. **Análise de tráfego em Redes TCP/IP**. **São Paulo: Novatec Editora**, 2013.

NETO, Expedito Dantas Barbosa et al. **Estudo de Redes Privadas Virtuais simuladas no software CISCO Packet Tracer**. 2018.

NEVES, Jailton Santos; TORRES, Waldeck Ribeiro. **O Protocolo OSPF**. 2017.

PRETE, Ligia Rodrigues. **Análise e desempenho de redes de acesso sem fio.** 2011. Dissertação (mestrado) – Universidade Estadual Paulista. Faculdade de Engenharia de Ilha Solteira. Área de conhecimento: Automação.

SANTOS, Ricardo Eleutério dos. **VLAN: Estudo, Teste e Analise desta Tecnologia**. 2010. 77 f. Monografia (Especialização) - Curso de Tecnologia em Sistemas de Telecomunicações, Instituto Federal de Santa Catarina, São José, 2010. Disponível em: http://wiki.sj.ifsc.edu.br/wiki/images/3/37/ProjetoFinal_RicardoEleuterio.pdf. Acesso em: 21 de janeiro de 2020.

SILVA, Rodrigo Romper Tertulino et al. **Uso do Cisco Packet Tracer como ferramenta no ensino-aprendizagem de Redes de Computadores** no IFRN– Campus Mossoró.

TANENBAUM, Andrew S. **Redes de Computadores**, 4ª edição. **Editora Campus**, 2003.

TANENBAUM, Andrew S.; WETHERALL, David. **Redes de Computadores**, 5ª edição, Ed. 2011.

TORRES, Gabriel. **Redes de computadores: curso completo**. Axcel Books, 2001.

VARADARAJAN, Suba. **Virtual Local Area Networks***.* Disponível em: http://www.cse.wustl.edu/~jain/cis788-97/ftp/virtual_lans/index.html. Acesso em: 21 de janeiro de 2020.

LOVATTO, Maico. **Gerenciamento e Segmentação de Redes: Estudo de caso em empresa do setor alimentício.** 2015. 40f. Monografia (Especialização Semipresencial em Redes de Computadores) – Universidade Tecnológica Federal do Paraná. Pato Branco, 2015.