# Redes de Alto Desempenho utilizando os protocolos MPLS/VRF e BGP

**Victor Afonso Tirloni[1], Sylvio Andre Garcia Vieira[1]**

[1]Sistemas de Informação – Universidade Franciscana (UFN)
97010-491 – Santa Maria – RS – Brasil

{victortirloni, sylviovieira}@gmail.com

***Abstract.*** *Considering the large growing of information necessity for companies that operate using an connectivity services, this study consists in development of a network topology that aggregate value for reception this information to these companies, matching the use of BGP and MPLS protocols and VRF technology. To achieve this goal, we chose topology construction using the Eve-Ng network emulator, applied to the use of images from real routers, in a virtual access. Getting a high availability, secure and effective network.*

***Resumo.*** *Dado o grande crescimento da necessidade de informação para que empresas operem fazendo o uso de serviços de conectividade, este estudo consiste no desenvolvimento de uma topologia de rede que agregue valor para o recebimento desta informação às empresas, combinando o uso dos protocolos BGP e MPLS e da tecnologia VRF. Para atingir este objetivo, optou-se pela construção da topologia utilizando o emulador de redes Eve-Ng, aplicado com o uso de imagens de roteadores reais, num acesso virtual. Obtendo assim, uma rede de alta disponibilidade, segura e eficaz.*

## 1. Introdução

O ambiente de competitividade em que se encontra a economia mundial infere à certas empresas a necessidade de ter suas unidades interconectadas. A confiabilidade desta conexão é fator que pode promover crescimento empresarial ou levar a empresa ao descrédito e a uma consequente queda nas receitas. Assim, grande parte das organizações trata a informação e as comunicações como elementos cruciais para o negócio, investindo em ambientes de alta disponibilidade e alto desempenho quando se refere a serviços de conectividade [Redação Eveo 2019].

Desta forma, muitas dessas organizações, baseadas em suas necessidades, buscam empresas que prestam serviços de telecomunicações diferenciados e que agreguem valor nas suas tarefas diárias, garantindo o acesso da informação que seja necessária a qualquer momento.

Nas últimas décadas, ocorreu uma evolução constante na forma de aplicação dos protocolos de redes que promovem a estabilidade da comunicação, por meio de redundância de canais de conexão, operando em conjunto. Isto permite maior qualidade e maior tempo de disponibilidade dos serviços. Um dos protocolos de maior destaque nesta área é o BGP (*Border Gateway Protocol*), que permite implementar redundância com múltiplas operadoras.

Da mesma forma que a estabilidade de um circuito é importante, a concentração de múltiplos serviços com o propósito de abranger a maioria dos usuários e das aplicações também é fundamental. O MPLS (*Multiprotocol Label Switching*), pode ser definido como um protocolo de *backbone*[1] que foi desenvolvido para transporte de elementos multimídia como, dados, voz e vídeo, onde ele apresenta três principais benefícios: VPN[2] (*Virtual Private Networking*), Engenharia de Tráfego (TE) e QoS (*Quality of Services*), permitindo também o uso da tecnologia VRF (*Virtual Routing and Forward*) para virtualização de diferentes tabelas de roteamento. Este protocolo é utilizado pelas maiores operadoras de serviços de internet para permitir um encaminhamento eficiente de tráfego de dados.

## 1.1. Justificativa

Com base nas pesquisas realizadas, percebeu-se que a internet se tornou uma parte essencial na vida moderna, pois, a partir de meados de 2010, teve um aumento de aproximadamente 1.114% no número de usuários conectados [Genbeta 2019].

Considerando que diversas empresas dependem da informação para operar, e essa informação é obtida geralmente por serviços de conectividade, é dada uma preocupação cada vez maior dos setores de Tecnologia da Informação (TI) dessas empresas referente à perda desta informação, por isso está sendo investido cada vez mais em serviços e parcerias com ISP que agregue melhores resultados na disponibilidade dos clientes.

## 1.2. Objetivo Geral

O objetivo deste trabalho é projetar e implementar uma topologia de rede de uma operadora de telecomunicações (ISP - *Internet Service Provider*), fazendo uso dos protocolos de rede BGP e MPLS juntamente com a tecnologia VRF, obtendo assim um ambiente de alta disponibilidade, desempenho e segurança para os clientes no que se refere à serviços de conectividade.

## 1.3. Objetivos Específicos

De acordo com o objetivo geral, pode-se destacar os seguintes objetivos específicos:

- Desenvolvimento de uma topologia de rede de um ISP;
- Desenvolvimento de uma topologia de rede de duas redes de supermercados distintas, com matriz e filiais;
- Realizar a implementação virtual destas topologias por meio de um emulador de redes;
- Demonstrar o funcionamento das topologias pela visão do administrador da rede do ISP e também na visão do cliente.

## 1.4. Estrutura do trabalho

A Seção 2 apresenta o referencial teórico, onde é abordado os conceitos e as tecnologias que foram necessárias para a concepção deste projeto. Na Seção 3 são apresentadas as

---

[1] *Backbone* é a espinha dorsal de uma rede, sendo a rede principal de um provedor, onde é o responsável pelo tráfego de dados entre diferentes localidades.

[2] VPN trata-se de uma rede que permite o tráfego de dados de forma privada e segura. Em redes MPLS, uma VPN é criada na "nuvem" do provedor.

pesquisas referentes aos trabalhos correlatos a este que foram de extrema importância para o entendimento geral do projeto a ser desenvolvido. A Seção 4 aborda a metodologia de como este trabalho foi desenvolvido. Na Seção 5 apresentam-se os resultados obtidos e na Seção 6, as conclusões sobre a concepção deste trabalho.

## 2. Referencial Teórico

Nesta seção serão abordados os tópicos e os conceitos dos conteúdos que são necessários para o desenvolvimento deste projeto. Serão apresentados os conceitos sobre os protocolos BGP, MPLS e a tecnologia VRF, e também uma caracterização da tecnologia que sustenta o desempenho de aplicações críticas, o QoS (*Quality of Service*). Finalmente, será realizada uma breve descrição de alguns dos simuladores e emuladores de redes e como eles funcionam.

### 2.1. Roteadores

Um roteador é um dispositivo projetado para enviar, receber, analisar e repassar pacotes de dados entre redes distintas, utilizando diversos protocolos de roteamento. Estes pacotes são repassados aos roteadores até que cheguem ao dispositivo de destino [Reis 2017].

Existem diversos fabricantes de roteadores, porém neste trabalho destaca-se dois: Cisco e Mikrotik.

A Cisco Systems é uma das empresas de mais destaque no mundo todo por seus equipamentos de telecomunicações. Fundada em 1984, hoje a empresa conta com mais de 60 mil funcionários para contribuir no desenvolvimento da empresa. A Cisco utiliza como sistema operacional o Cisco IOS (*Internetwork Operating System* [Cisco Systems 2019].

A Mikrotik é uma empresa sediada em Letônia, fundada em 1995, também fabricante de equipamentos para rede de computadores. Seus roteadores contam com um sistema operacional baseado em Linux chamado Mikrotik RouterOS [Mikrotik 2019].

### 2.2. Protocolo BGP

O *Border Gateway Protocol* (BGP) é um protocolo de roteamento dinâmico utilizado por Sistemas Autonômos[3] (AS) e que requer um número único (ASN) para o seu funcionamento. O protocolo foi criado para troca de informações de roteamento entre operadoras de telecomunicações [Cisco 2008].

O BGP possui duas formas para divulgação de rotas (ou prefixos de rede), o iBGP (*Internal BGP*), que é utilizado para troca de rotas dentro de um mesmo AS, e o eBGP (*External BGP*), utilizado para troca de rotas entre diferentes AS [Rekhter *et al.* 2006]. Pode-se observar na Figura 1 um exemplo utilizando dois ISP com seus respectivos ASN, onde a troca de informações entre eles é feito por um eBGP, e a troca de informações internas de um ISP é realizado por um iBGP.

[3] Sistemas Autônomos são empresas que possuem sua própria rede de IP, que é propagada no mundo inteiro. Cada AS recebe um número único de sistema autônomo (ASN).

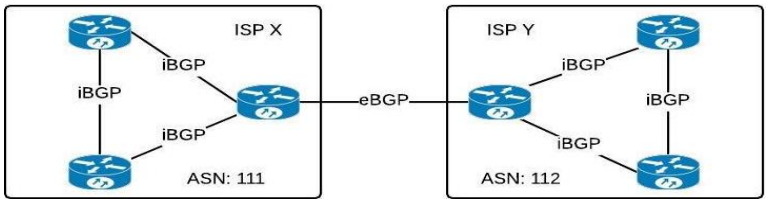


**Figura 1. Diagrama utilizando iBGP e eBGP [dos Autores].**

Quando dois roteadores trocam informações de roteamento utilizando o protocolo BGP, estes estabelecem uma relação de vizinhança, ou *peers* [Junior 2012]. Cada AS possuí o seu ASN que o identifica entre os demais.

### 2.3. Multiprotocol Label Switching

O *Multiprotocol Label Switching*, ou MPLS é uma tecnologia muito utilizada pelos ISP para fornecer serviços de conectividade, pois permite gerenciar tráfego, controlar diferentes tipos de serviços e também auxilia na redução de custos de infraestrutura, pois permite o compartilhamento de uma mesma infraestrutura entre diversos clientes [Lipp 2016].

O MPLS foi desenvolvido sob a RFC 3031, onde foi inicialmente apresentada como uma solução que permite melhorar o desempenho de redes IP no que se refere à encaminhamento de pacotes entre roteadores [Zanon 2015]. Na Figura 2, é demonstrado a topologia padrão de uma rede MPLS.

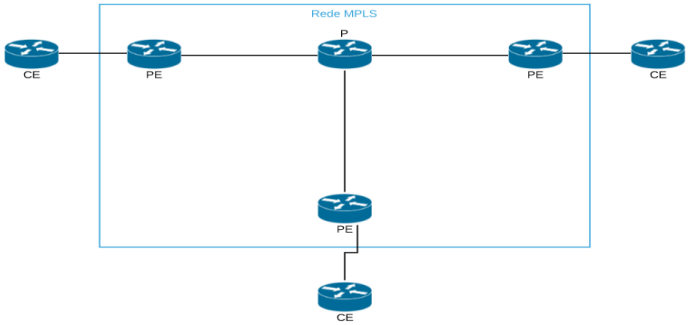


**Figura 2. Exemplo de uma arquitetura de rede MPLS [Dos Autores].**

Conforme é visto na Figura 2, uma topologia padrão MPLS contém roteadores P (*Provider*), PE (*Provider Edge*) e os roteadores dos clientes, que é designado como CE (*Customer Edge*). Cada roteador possui sua função:

- Roteador P: numa rede MPLS, o roteador P funciona como um roteador de trânsito da rede principal. Este roteador é conectado a um ou mais roteadores PE, pois uma das funções deste roteador é fornecer acessibilidade entre os dispositivos PE. As informações de clientes não são aprendidas pelo roteador P, e sim pelo PE.
- Roteador PE: o roteador PE executa as funcionalidades de roteamento de saída dos clientes. Esses dispositivos são conectados em roteadores P, e também são neles em que os clientes estão conectados, ou seja, toda a configuração de uma rede de cliente, é configurada no roteador PE [Silva 2018].

Com a rede MPLS implementada na estrutura da operadora, é possível conectar diversos clientes em um roteador PE e atribuir cada cliente em sua VRF própria, assim todos os roteadores que estão dentro da rede MPLS e que possuem a VRF configurada

vão conhecer a rede daquele cliente. O roteamento entre o PE e o CE pode ser estático ou dinâmico.

Nos roteadores de uma rede de *backbone* que possuem o protocolo MPLS configurado, as informações de roteamento são conduzidas por meio de um encaminhamento baseado em *labels*, ou etiquetas. Tais etiquetas são números inteiros utilizados no protocolo MPLS e, por meio destes, a decisão de qual interface encaminhar o datagrama é tomada [Rosen *et al.* 2001].

De acordo com Zanon (2015), com a utilização do protocolo MPLS, é criado uma rede para agilizar as transferências de informação entre matriz e filiais. Com ela, as empresas podem integrar as suas aplicações de dados, voz e vídeo operando em uma única infraestrutura, ganhando qualidade e economia na condução dos seus negócios.

## 2.4. Virtual Routing and Forwarding

*Virtual Routing and Forward*, ou simplesmente VRF, é uma técnica de virtualização de diferentes tabelas de roteamentos em um mesmo roteador. Conforme Brito (2014), a tecnologia VRF é normalmente utilizada por provedores na oferta do serviço VPN/MPLS para conectividade dos seus clientes por meio de um núcleo comum de equipamentos de grande porte, o que permite o compartilhamento da sua infraestrutura.

Com a utilização desta tecnologia, é possível criar tabelas de roteamento independentes para cada cliente, conforme pode-se observar na Figura 3, quando mesmo compartilhando da mesma infraestrutura de *backbone*, o tráfego destes clientes não será envolvido, permanecendo apenas na VRF proposta de cada um, onde também não é agregada na tabela de roteamento global dos roteadores.


**Figura 3. Exemplo de diferentes VRF num mesmo roteador [Cisco 2008].**

## 2.5. Quality of Service

*Quality of Service*, ou QoS, é a medição do desempenho geral de um serviço, levando em conta a experiência do usuário. Conforme o tráfego de clientes é compartilhado entre diferentes aplicações, como voz e vídeo por exemplo, na área de redes de computadores, esta técnica é utilizada para ordenar e priorizar estes diferentes tipos de tráfegos dentro de um *backbone*, garantindo uma melhor qualidade para os clientes no que se refere à conectividade [Lipp 2016].

## 2.6. OSPF

O *Open Shortest Path First* é um protocolo de roteamento dinâmico desenvolvido para uso interno de um AS. O protocolo é utilizado principalmente para prover redundância em redes que possuem mais de uma saída, onde têm como objetivo encontrar o melhor caminho baseado no estado destas saídas. Caso alguma saída ficar indisponível, se houver OSPF configurado no roteador, o tráfego deverá emergir à outra saída de forma instantânea [Moy 1998].

### 2.7. Simuladores de rede

Simuladores e emuladores de redes são ferramentas utilizadas para representar equipamentos reais e que permitem conceber uma topologia de rede virtual, sem que haja a necessidade de possuir os roteadores físicos. Este tipo de recurso é ideal para estudantes que desejam adquirir conhecimento e prática na área de redes, e também profissionais que já possuem um certo entendimento do assunto e desejam analisar o funcionamento de alguma configuração a ser implementada em um ambiente real, antes de colocá-la em produção [Borges Filho *et al.* 2015].

Nesta seção, será realizada uma breve análise de alguns dos principais simuladores de redes disponíveis no mercado, incluindo o emulador que será utilizado para contemplar este trabalho.

#### 2.7.1. GNS3

GNS3 é um emulador de redes *open source* que permite emular imagens[4] de diversas marcas de roteadores reais, possibilitando a manipulação destes em um ambiente virtual. O GNS3 pode ser instalado em Windows, Mac OSX ou Linux, e por ser um software de código aberto, qualquer pessoa que possui conhecimentos em programação poderá corrigir bugs e realizar customizações [GNS3 2019]. A figura que demonstra a interface gráfica deste emulador pode ser vista no Apêndice A.

#### 2.7.2. Packet Tracer Simulator Tool

O Packet Tracer é um programa de simulação de redes mais simples desenhado pela própria Cisco para aqueles que estão começando seus estudos na área de redes ou se preparando para alguma certificação da Cisco, como o CCNA, por exemplo. O Packet Tracer possui alguns roteadores com comandos mais limitados que o GNS3, pois ele não permite a emulação de um roteador real, portanto, não é possível construir uma topologia de redes complexas [Cisco Packet Tracer 2019]. A figura que demonstra a interface gráfica deste simulador pode ser vista no Apêndice A.

#### 2.7.3. Eve-Ng

O Eve-Ng será o emulador utilizado para a implantação deste projeto. É uma plataforma gratuita (também possui uma versão comercial) que foi desenvolvido por Andrea Dainese. Nele, assim como o GNS3, é possível emular imagens de roteadores reais de diferentes fornecedores, como Cisco, Juniper, Mikrotik, entre outros, permitindo a construção de ambientes mais complexos [Eve-NG 2019].

O Eve-Ng se destaca por não utilizar tanto recurso de uma máquina no momento de sua execução (se comparar com o GNS3), por possuir uma ampla lista de imagens de equipamentos que são suportados e também pela facilidade de uso do mesmo, pois o software permite a construção de laboratórios por meio de um navegador. A figura que demonstra a interface gráfica deste emulador pode ser vista no Apêndice A.

## 3. Trabalhos Relacionados

Os trabalhos apresentados tratam de um estudo realizado sobre a utilização e as funções do protocolo BGPv4 (*Border Protocol Gateway* – Versão 4), do protocolo MPLS/VRF e

[4] Imagens de equipamentos é o Sistema Operacional do equipamento, permitindo a sua configuração como se fosse no equipamento real, porém, em um ambiente virtual.

o valor que a utilização destes protocolos agrega numa topologia de rede, tanto para o ISP quanto para o seu cliente.

### 3.1. Descrição das Características e funções do protocolo BGPv4

O projeto apresentado por Junior (2012) teve como objetivo descrever as características e as funções do protocolo BGPv4, explicando os componentes necessários para o funcionamento do protocolo entre sistemas autônomos e suas etapas até o estabelecimento de uma sessão.

Para demonstração do funcionamento do protocolo, o autor implementou uma topologia de rede utilizando o *software* GNS3 para virtualização das imagens do sistema operacional utilizado em roteadores Cisco.

No trabalho, o autor concluiu sobre a importância do protocolo BGP para que a internet seja mantida em pleno funcionamento, pois hoje é o principal protocolo utilizado pelas operadoras para troca de tráfego entre elas. O projeto mostra que o protocolo não irá ser substituído tão cedo, pois o mesmo é tolerante e compatível às mudanças de tecnologias.

### 3.2. Um estudo de VPNs Layer 3 MPLS-BASED utilizando multiprotocol BGP

O trabalho elaborado por Filho e Moreira (2016) descreve os conceitos do protocolo MPLS e suas funções se aplicado em uma topologia de rede, demonstrando os seus benefícios para uma operadora de telecomunicações.

No projeto, os autores também utilizam o protocolo BGP, sugerindo que a combinação das tecnologias visa aumentar a velocidade da transmissão de pacotes em uma rede, tornando a mesma altamente escalável.

Para validação dos conceitos mostrados no trabalho, também foi utilizado o software GNS3. Foi utilizado uma imagem de um roteador que é compatível com todos os protocolos estudados no projeto.

### 3.3. Isolamento de tráfego e garantias de desempenho em redes MPLS: Um estudo teórico e prático de VRF e QOS sob o ponto de vista de um provedor de serviço

O trabalho de Lipp (2016) também aborda a utilização do protocolo MPLS, porém com ênfase na combinação deste com a tecnologia VRF. O autor também explica o funcionamento do QoS para garantia da qualidade de diferentes tipos de serviços.

Levando em conta a facilidade de uso, da mesma forma que nos outros projetos estudados, neste o autor também utilizou o simulador GNS3 para demonstrar a sua topologia de rede, emulando imagens de roteadores Cisco.

Por fim, o autor comprovou que com a utilização de VRF, clientes que compartilham de uma mesma estrutura de *backbone* de uma operadora, podem ter o seu tráfego totalmente reservado e seguro, pois cada tabela VRF dentro de um roteador é totalmente isolada da tabela de roteamento principal e também de outras VRF existentes, demonstrando que a tecnologia MPLS é eficaz para um provedor de serviços.

### 3.4. Conclusão sobre os trabalhos relacionados

Os trabalhos selecionados ilustram diversos temas correlatos para o desenvolvimento deste projeto, destacando que a utilização de diferentes tipos de tecnologias dentro de uma rede pode agregar valor ao negócio.

O trabalho de Junior (2012) relaciona-se com este projeto devido à necessidade da implantação do protocolo BGP para concluí-lo com sucesso, pois é uma das principais tecnologias para troca de tráfego entre operadoras e também troca de tráfego interno de uma operadora juntamente com o protocolo MPLS.

Filho e Moreira (2016) desenvolveram uma topologia de rede aplicando VPN sob o protocolo MPLS, em que o autor demonstra com experimentos práticos os conceitos necessários para tal aplicação.

Para Lipp (2016), a segmentação de diferentes tabelas de roteamento com o uso das VRF é uma ótima prática para as operadoras, pois pôde comprovar que clientes que utilizam do mesmo *backbone*, não terão acesso ao tráfego de outros clientes da mesma operadora.

Todos os trabalhos foram importantes para o desenvolvimento deste projeto que, destaca-se entre os outros por propor o uso destas tecnologias entre duas fabricantes de equipamentos conhecidas, e também agregando a integração de redes de *backbone* com redes de dois clientes com diversas unidades que são geograficamente distintas. O projeto também demonstrará a facilidade que o protocolo MPLS propõe para a troca de informações entre clientes que fazem parte desta rede.

## 4. Metodologia

Para obter um melhor resultado final na organização deste trabalho e um melhor entendimento do funcionamento da metodologia, esta foi dividida em duas fases de construção da topologia de rede, iniciando com a rede de *backbone*, onde é descrito todo o funcionamento da rede principal da operadora. Em seguida, foi abordada a rede de cliente, onde é representado o funcionamento desta topologia e as configurações que foram implementadas para satisfazer as necessidades dos clientes. Essas topologias foram construídas no simulador de redes Eve-Ng, utilizando uma máquina com 16 Gb de memória RAM, com processador AMD Ryzen 5 1500X e HD SSD de 240Gb.

### 4.1. Rede de Backbone

Nesta fase, foi construída uma topologia de rede MPLS, utilizando em conjunto com os protocolos BGP e OSPF. Na rede de *backbone*, foram implementados dez roteadores para contribuir na rede MPLS da operadora. Entre os roteadores que são diretamente conectados, foi configurado o protocolo OSPF por questão de contingência de rotas, onde foi desenhada uma topologia em malha, portanto, caso algum lado da malha fique sem comunicação, o tráfego será automaticamente redirecionado para o outro lado.

Foi realizada a configuração de uma rede do tipo *full-mesh*, ou seja, todos os roteadores que estão dentro da rede MPLS terão comunicação entre si. Para facilitar esse tipo de configuração, um dos roteadores da rede MPLS é o *Route-Reflector*, ou simplesmente RR. Caso não houvesse o RR na topologia de rede, cada roteador de *backbone* teria que estabelecer uma sessão BGP entre si, por exemplo, se a estrutura tivesse ao total 5 roteadores, seria necessário estabelecer um total de 4 sessões BGP em cada roteador. Com o RR, todos os roteadores da estrutura de *backbone* estabeleceram apenas uma sessão BGP com o RR, onde ele é o responsável por informar as rotas dos roteadores entre todos os equipamentos que fazem parte da rede MPLS. Em uma topologia de rede pode-se ter diversos roteadores RR, onde caso um desses roteadores

falhem, outro roteador RR fica de responsável por propagar as rotas. Neste trabalho, foi utilizado apenas um roteador RR. A Figura 4 demonstra o resultado da rede de *backbone*.

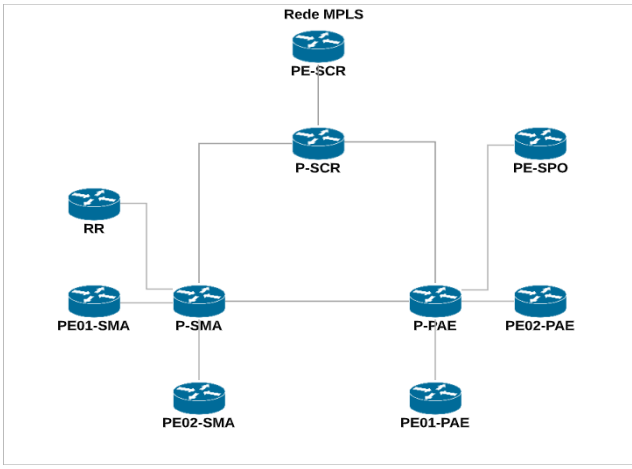


**Figura 4. Topologia da rede de *Backbone*.**

Conforme observa-se na Figura 4, a rede dispõe de três roteadores P, seis roteadores PE e um roteador RR, onde cada roteador cumpre a sua função pré-estabelecida. Foram utilizadas imagens de roteadores Cisco nos equipamentos de *backbone*.

## 4.2. Rede de Clientes

Para demonstração das redes dos clientes, foram definidos dois clientes fictícios de duas redes de supermercados distintas: o supermercado Venâncio e o supermercado Borges. Os dois clientes solicitaram serviço de conectividade entre as filiais e a matriz, sendo que na matriz fica localizado os seus servidores principais, portanto, todas as filiais precisam ter acesso a ela.

Também foi solicitado que a Matriz fosse duplamente abordada, para caso venha a perder a comunicação principal, a comunicação do cliente opere pela segunda abordagem. Uma indisponibilidade total na matriz causa inoperância dos serviços nas filiais, pois as unidades perderão acesso aos servidores principais que ficam na matriz, consequentemente o acesso à internet das unidades também será interrompido, pois este depende da comunicação com a matriz.

Para garantir esta estabilidade de serviços foi utilizado o protocolo BGP entre os roteadores das unidades dos supermercados e da operadora. O tipo de tráfego que é transportado entre matriz e filiais é do tipo dados principalmente, onde para um melhor desempenho no acesso aos servidores, foi realizada a configuração de QoS para garantir a qualidade da comunicação com a matriz mesmo se o tráfego de dados encontrar-se ao limite total da banda contratada nas unidades, que neste caso, é de 1Mb. A configuração foi realizada para garantir pelo menos 40% do tráfego total da unidade para acesso aos servidores.

Para cada rede de supermercados foi designada uma VRF própria, desta forma seu tráfego é totalmente isolado de outros clientes que compartilham da mesma infraestrutura de *backbone*, e mesmo que possuam endereçamentos de IP semelhantes, não causará nenhum problema de conflitos de IP. Os nomes das VRF dos supermercados são exatamente os próprios nomes dos supermercados: "Venâncio" e "Borges".

A matriz do supermercado Venâncio fica localizada na cidade de Santa Maria - RS, e do supermercado Borges na cidade de Porto Alegre – RS, onde, em cada uma dessas cidades, conforme visto na Figura 4, dispõe de dois roteadores PE, e em cada um deles estará conectado uma das abordagens da matriz.

Para as filiais, diferente da matriz, foi solicitado apenas uma abordagem, e também foi utilizado o protocolo BGP entre o roteador da filial e o equipamento da operadora para propagação das rotas. A distribuição das unidades juntamente com as interconexões da rede de *backbone* do ISP é apresentada na Figura 5.

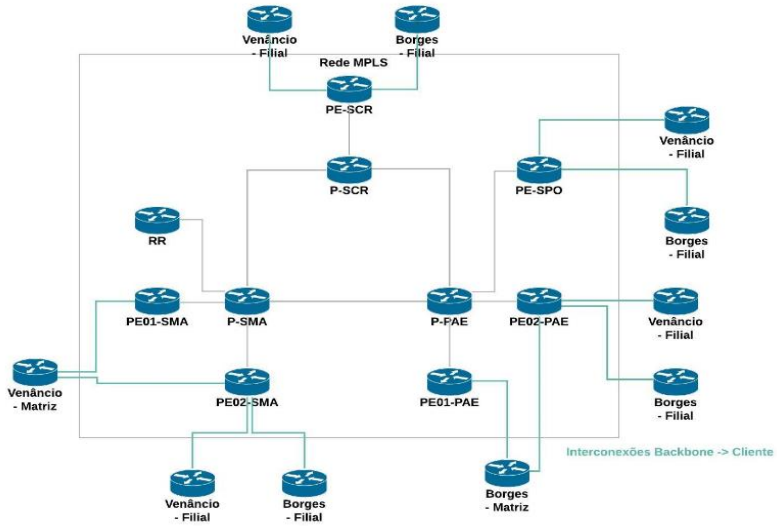


**Figura 5. Topologia da rede de Cliente.**

Conforme pode ser observado na Figura 5, cada rede de supermercado tem no total cinco unidades, contanto com a matriz e as filiais. As unidades dos supermercados estão em locais geograficamente diferentes, e foram espalhadas entre os PE da rede da operadora de cada local. A sigla dos PE possui as seguintes definições, conforme o código nacional de localidade (CNL) [Anatel 2005]:

- SMA – Santa Maria;
- PAE – Porto Alegre;
- SCR – Santa Cruz do Sul;
- SPO – São Paulo.

A distribuição das unidades com a rede de *backbone* da operadora é a seguinte: em São Paulo, cada cliente possui uma unidade. Em Porto Alegre, o supermercado Borges possui duas unidades, e o Venâncio tem uma unidade. Em Santa Cruz do Sul cada cliente tem uma unidade e em Santa Maria, o supermercado Venâncio possui duas unidades e o Borges uma unidade. Foram utilizadas imagens de roteadores Mikrotik nos equipamentos de cliente.

### 4.3. Implementação da Rede

Todos os comandos dos protocolos e funcionalidades que foram implementados tanto na rede de *backbone* quanto na rede de cliente são apresentados nos Apêndices de acordo com as indicações abaixo. Conforme foram utilizados equipamentos de duas empresas distintas na implementação desta rede, serão explanados os códigos do equipamento

Cisco primeiramente, onde será utilizado apenas um equipamento da rede de *backbone* como modelo (será utilizado o "PE01-SMA"), que possui todos os comandos que foram citados nesta metodologia. Posteriormente, serão abordados também os códigos do equipamento da rede de cliente, que foi utilizado dispositivos do fabricante Mikrotik (será utilizado como exemplo o equipamento da matriz do supermercado Borges).

- OSPF (Apêndice B);
- BGP (Apêndice C);
- VRF (Apêndice D);
- MPLS (Apêndice E);
- QoS (Apêndice F);
- Rede Cliente (Apêndice G).

## 5. Resultados

A construção desta topologia resultou numa rede de *backbone* de alto desempenho e uma rede de cliente de alta disponibilidade, que, no caso da unidade matriz dos clientes, uma rede tolerante a falhas, baseada nas abordagens duplicadas.

Na Figura 6, apresenta-se a topologia de rede completa, onde foram acrescentados os ativos (computadores, servidores, switches) para torná-la completa e para apresentar os resultados obtidos de uma maneira efetiva.

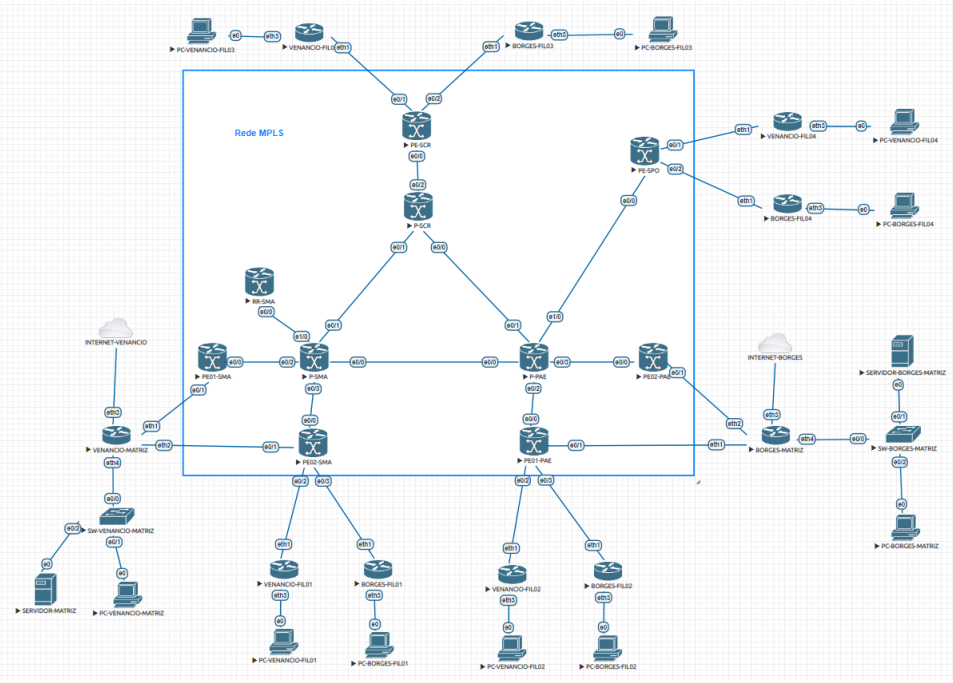


**Figura 6. Resultado final da topologia de rede.**

Na Figura 7, demonstra-se a semelhança da tabela de roteamento da VRF borges e da VRF venancio que, pelo fato de estarem atreladas à uma VRF, não ocorre conflitos de endereçamentos IP e rotas.

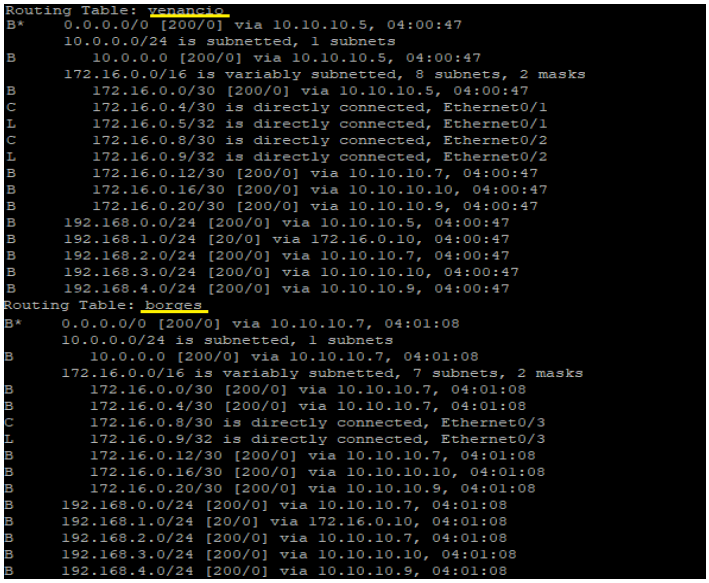


**Figura 7. Tabela de roteamento das VRF.**

Na Figura 8 é demonstrado o acesso pela Filial 01 do supermercado Venâncio no servidor da matriz. Observa-se que a conectividade entre o servidor da matriz e a Filial 01 do supermercado Venâncio ocorreu com sucesso, onde foi feito um teste de *ping* para o IP do servidor (a tabela completa dos endereçamentos IP que foram utilizados tanto na rede de *backbone* quanto na rede de cliente pode ser verificada no Apêndice H), e em seguida, foi realizado o acesso no servidor digitando o IP do mesmo no navegador.

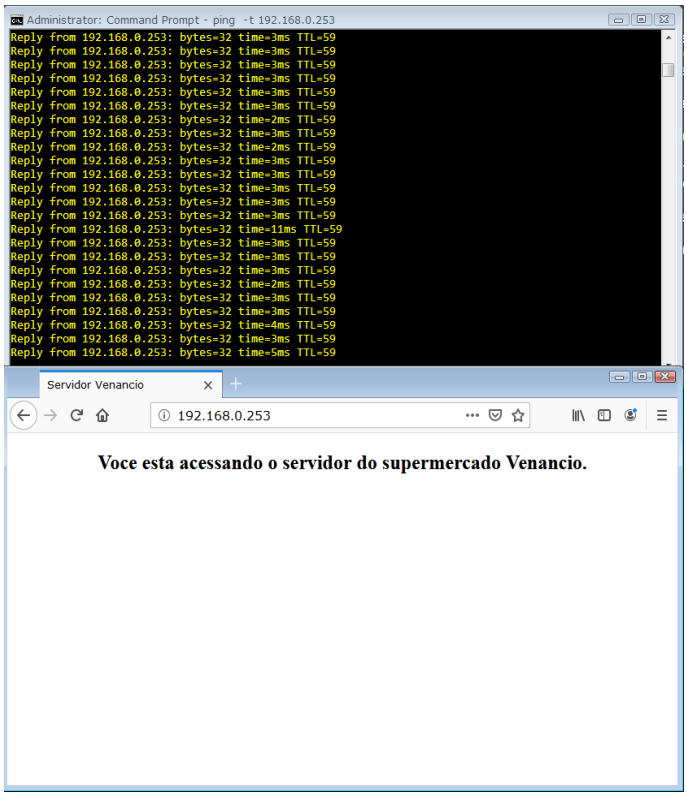


**Figura 8. Acesso ao servidor da Matriz do supermercado Venâncio via Filial 01.**

Para demonstração do teste de contingência, foi realizado o comando "*tracert*" a partir da Filial 01 do supermercado Borges para o IP do servidor da matriz, onde é observado na Figura 9 dois caminhos distintos após a comunicação principal da matriz ser interrompida.

```
C:\Users\Administrator>tracert 192.168.0.153        Linha Verde - Figura 10

Tracing route to intranet.borges.local [192.168.0.153]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2     3 ms     3 ms     1 ms  172.16.0.9
  3    60 ms     3 ms     3 ms  172.16.0.21
  4     3 ms     4 ms     4 ms  172.16.0.2
  5     4 ms     4 ms     3 ms  172.16.0.1
  6     3 ms     3 ms     3 ms  172.16.0.2
  7     7 ms     5 ms     6 ms  intranet.borges.local [192.168.0.153]

Trace complete.
C:\Users\Administrator>tracert 192.168.0.153        Linha Azul - Figura 10

Tracing route to intranet.borges.local [192.168.0.153]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2     2 ms     1 ms     2 ms  172.16.0.9
  3     5 ms     4 ms     4 ms  172.16.0.21
  4     5 ms     4 ms     4 ms  172.16.0.2
  5     3 ms     3 ms     4 ms  172.16.0.5
  6     4 ms     3 ms     5 ms  172.16.0.6
  7     3 ms     3 ms     3 ms  intranet.borges.local [192.168.0.153]

Trace complete.
```

**Figura 9. Tracert para visualização do caminho entre as unidades.**

Na Figura 10, é demonstrado o caminho real da comunicação entre a Filial 01 e a matriz do supermercado Borges após a abordagem principal da matriz (linha verde) ser interrompida. A linha azul demonstra o trajeto secundário desta comunicação.

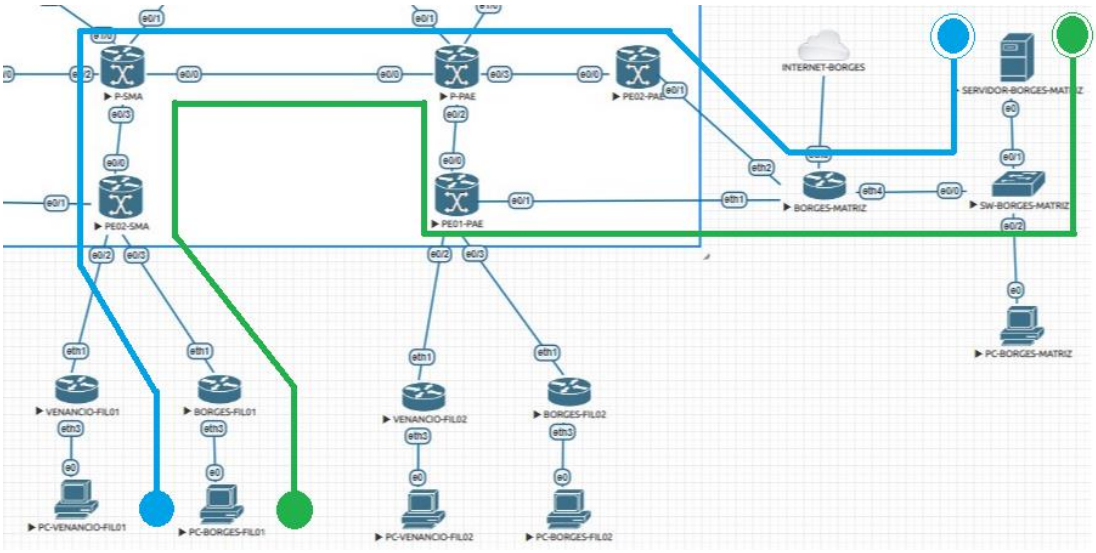


**Figura 10. Caminho físico da comunicação entre os ativos das unidades pelas duas abordagens da matriz.**

Para análise da segurança das redes dos clientes, demonstra-se na Figura 11 a tentativa de acesso no servidor do cliente Venâncio a partir da Filial 04 do cliente Borges, que fica localizado em São Paulo. O teste é realizado primeiramente com comando *ping* para o IP do servidor (conforme Tabela 4 do Apêndice H, o IP do servidor do cliente Venâncio é 192.168.0.253), que não obteve resposta. Em seguida foi realizado um *tracert*

para analisar por quais ativos ocorre esta tentativa de comunicação, e pôde ser constatado que o destino final é o roteador da matriz do supermercado Borges, no entanto, como o IP 192.168.0.253 não existe na rede interna da matriz, esse destino não é alcançado, comprovando assim que não existe comunicação entre os dois clientes.

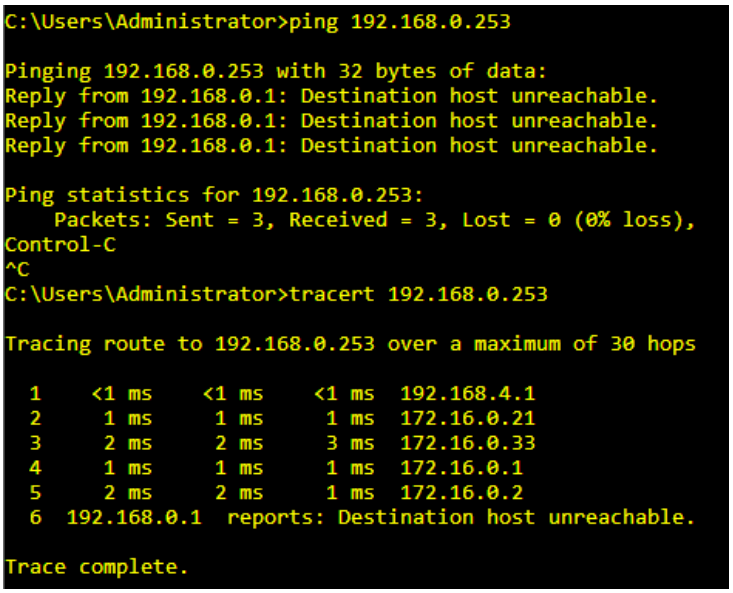


**Figura 11. Tentativa de acesso no servidor do cliente Venâncio a partir da Filial do cliente Borges.**

Para demonstração do funcionamento do QoS, foi realizado um *ping* para o IP do servidor da matriz do supermercado Venâncio com origem do computador da Filial 03 do mesmo cliente, que, conforme demonstra a Figura 12, no total de 20 pacotes que obtiveram resposta do *ping*, todos eles foram agrupados na classe configurada do QoS para garantia da qualidade desta comunicação.

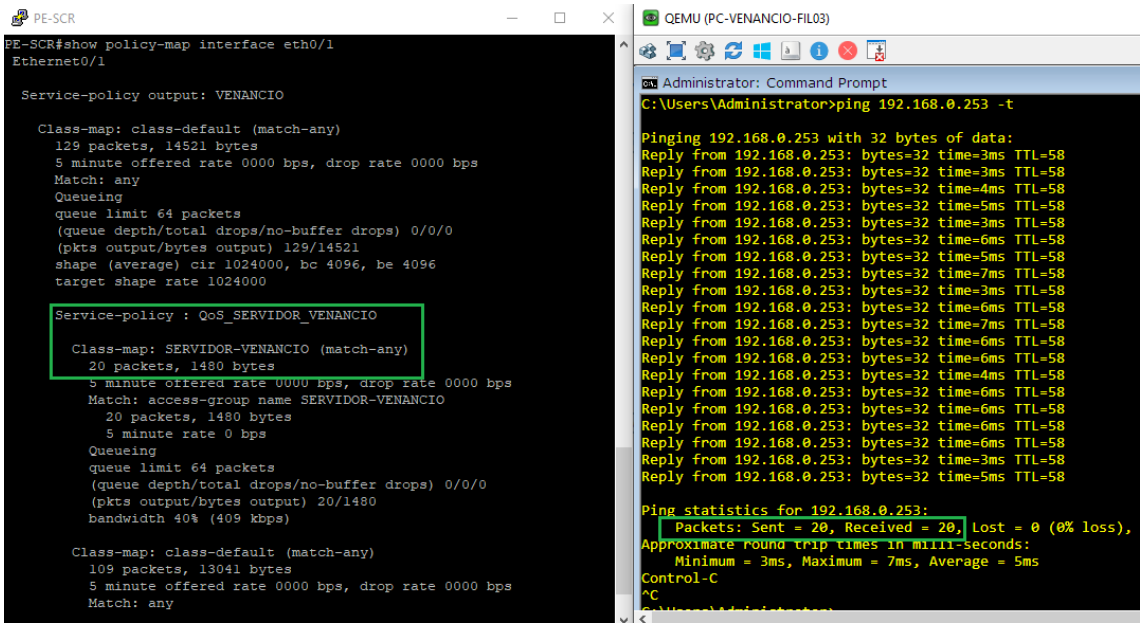


**Figura 12. Demonstração do funcionamento do QoS.**

## 6. Conclusão

Este trabalho proporcionou o desenvolvimento de uma topologia de rede de uma operadora de telecomunicações que combina os protocolos BGP e MPLS, fazendo o uso da tecnologia VRF para segmentar a rede dos clientes.

Este trabalho destaca-se das demais pesquisas na área, pois há poucas pesquisas acadêmicas neste segmento. Não sendo, inclusive, encontrado nenhum trabalho que propõe circuitos de alta disponibilidade, utilizando a combinação dos protocolos MPLS, BGP e a tecnologia VRF com a utilização do emulador Eve-Ng para a implementação. Abordando ainda a utilização de QoS para garantia de desempenho.

Os trabalhos relacionados foram de extrema importância para a concepção desta pesquisa, pois serviram como base para um estudo mais detalhado dos protocolos que foram utilizados.

Na visão do cliente, uma topologia de rede que utiliza o protocolo MPLS é altamente eficaz, segura e de menor custo, pois interliga as suas unidades diante de uma rede privada e utiliza de uma mesma infraestrutura de *backbone*. Também permite a criação de QoS diante de diferentes tipos de serviços, como dados, voz, vídeo, entre outros para classificação e priorização de tráfego, obtendo um desempenho ainda mais satisfatório. Com o uso do protocolo BGP foi possível obter uma melhor disponibilidade do circuito, pois como se trata de um protocolo de roteamento dinâmico, permite distribuir informações de rotas mais rapidamente que em uma configuração de roteamento estática.

Diante disso, observaram-se trabalhos futuros que poderão ser desenvolvidos utilizando os conceitos de uma tecnologia chamada *Software-Defined Networking in a Wide Area Network,* ou SD-WAN, que é uma tecnologia de gerenciamento de redes WAN definidas por *software,* que, assim como o protocolo MPLS, é uma tecnologia que fornece conectividade entre filiais e matriz, podendo ser realizado comparações entre estas tecnologias e, por fim, demonstrar o funcionamento desta nova solução no que diz respeito a interligação entre empresas.

## Referências


ANATEL. (2005) “CNL – Código Nacional de Localidade”, http://twixar.me/8tdT, Novembro.

Borges Filho, Valdinei et al. (2017) “Software Simuladores de Rede: Análise Comparativa para apresentação de funcionalidades e benefícios”, http://simtec.fatectq.edu.br/index.php/simtec/article/download/242/185, Abril.

Cisco. (2008) “Estudo de caso de BGP”, http://twixar.me/stdT, Novembro.

Cisco. (2008) “NAC Layer 3 Out of Band Design Guide That Uses VRF-Lite for Traffic Isolation”, http://twixar.me/7tdT, Abril.

Cisco Packet Tracer. (2019) “Cisco Packet Tracer”, https://www.netacad.com/courses/packet-tracer, Abril.

Cisco Systems (2019) “Cisco Systems”, https://www.cisco.com, Novembro.

EVEO. (2019) “Alta disponibilidade: como montar uma infraestrutura com o máximo de uptime”, https://www.eveo.com.br/blog/alta-disponibilidade, Maio.

Eve-Ng. (2019) “The Emulated Virtual Environment for Network, Security and DevOps professionals”, https://www.eve-ng.net, Abril.

GENBETA. (2019) “Esto es Internet en 2019: 4.000 millones de usuarios, y páginas cuatro veces más pesadas que hace 10 años”, http://twixar.me/MtdT, Maio.

GNS3. (2019) “Graphical Network Simulator-3”, https://www.gns3.com, Abril.

Junior, Mauro Bordinhão. (2012) “Descrição das Características e funções do protocolo BGPv4”, http://twixar.me/QtdT, Abril.

Lipp, Daniel. (2016) “Isolamento de tráfego e garantias de desempenho em redes MPLS: Um estudo teórico e prático de VRF e QOS sob o ponto de vista de um provedor de serviço”, https://tconline.feevale.br/NOVO/tc/files/0001_4125.pdf, Abril.

Melo Velez Filho, C. e Sardinha Moreira, T. (2016) “Um estudo de VPNs Layer 3 MPLS-BASED utilizando multiprotocol BGP”, http://bsi.uniriotec.br/tcc/textos/201612CarlosVelezThiagoSardinha.pdf, Abril.

Mikrotik (2019) “Mikrotik Routers and Wireless”, https://mikrotik.com, Novembro.

Moy, John. (1998) “OSPF Version 2”, https://tools.ietf.org/html/rfc2328, Maio.

Reis, Fabio (2017) “Curso de Redes – O que é um roteador (básico)”, http://www.bosontreinamentos.com.br/redes-computadores/curso-de-redes-o-que-e-um-roteador-basico, Novembro.

Rekhter, Y et al. (2006) “A Border Gateway Protocol 4 (BGP-4)”, https://tools.ietf.org/html/rfc4271, Abril.

Rosen, E et al. (2001) “MPLS Label Stack Encoding”, https://tools.ietf.org/html/rfc3032, Abril.

Samuel, Brito. (2014) “Fundamentos de VRF na Virtualização de Roteadores”, http://labcisco.blogspot.com/2014/05/fundamentos-de-vrf-na-virtualizacao-de.html, Abril.

Silva, Renato Antonio (2018) “MPLS Core — Principais Conceitos em Service Provider”, https://medium.com/techrebels/https-medium-com-ra-silva-mpls-core-principais-conceitos-em-service-provider-6a6b5300add0, Abril.

Zanon, André. (2015) “COMPARATIVO ENTRE AS TÉCNOLOGIAS FRAME RELAY E MPLS VPN EM CAMADA 3”, http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/6124/1/PB_ESPRC_II_2015_11.pdf, Abril.

## Apêndice A. Interfaces dos Simuladores de Redes

Na Figura 13 observa-se a interface gráfica do simulador GNS3.

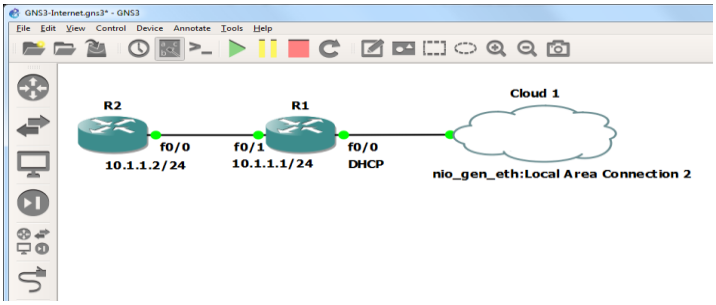


**Figura 13. Interface do Software GNS3 [GNS3 2019].**

Na Figura 14 observa-se a interface gráfica do software Cisco Packet Tracer.

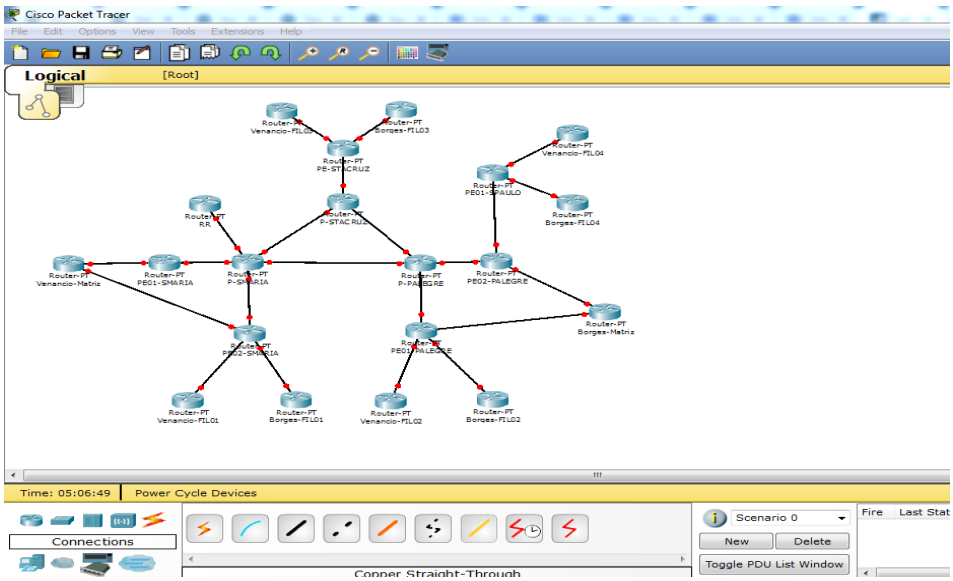


**Figura 14. Software Packet Tracer [Cisco Packet Tracer 2019]**

É demonstrado na Figura 15 um exemplo de uma topologia de rede construída utilizando o Eve-Ng, com alguns modelos de equipamentos diferentes interligados entre si.

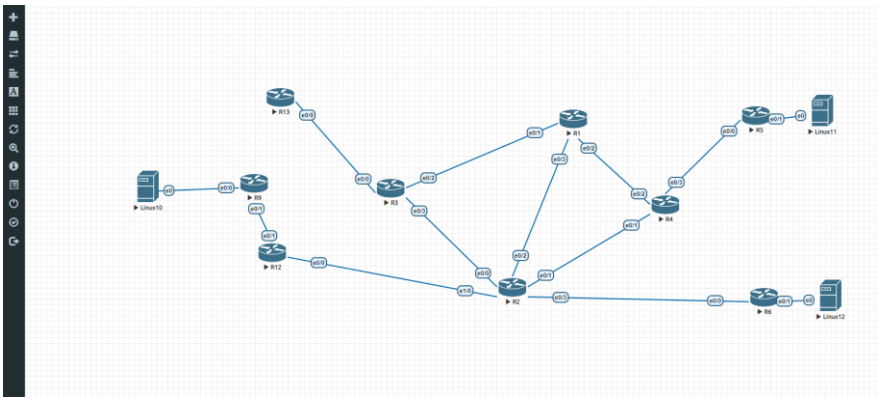

**Figura 15. Demonstração da interface do Eve-Ng [Eve-Ng 2019].**

## Apêndice B. Configuração do protocolo OSPF

Todos os equipamentos de backbone que possuem uma conexão direta entre si possuem o protocolo OSPF configurado entre eles para troca de informações (rotas), como pode ser observado na Figura 16.

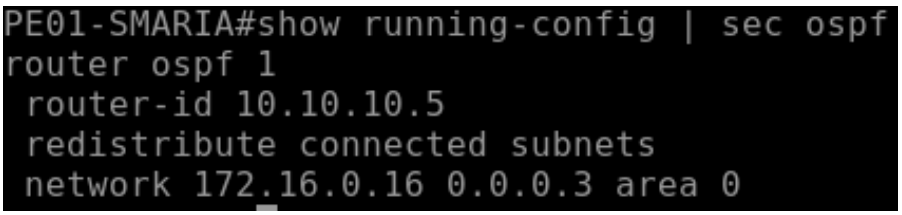


**Figura 16. Configuração do protocolo OSPF em equipamento de *backbone*.**

Em todos os equipamentos de *backbone*, foi configurado o OSPF com instância 1 ("router ospf 1" - Figura 16). O *router-id* é um IP identificador para o processo OSPF, que neste projeto os dispositivos possuem como *router-id* o endereçamento IP da interface Loopback[5](a tabela com os endereçamentos de Loopback pode ser observada no Apêndice A). Também está sendo informado no processo OSPF a redistribuição apenas das sub redes que são diretamente conectadas no roteador, e também a rede que está participando do processo OSPF na área de *backbone*, que é a área 0.

[5] Uma interface Loopback é uma interface de rede virtual em um roteador que está sempre ativa, independente das interfaces físicas.

## Apêndice C. Configuração do protocolo BGP

Todos os equipamentos de backbone estabelecem uma sessão BGP com o roteador *Route-Reflector*, que possui como endereço IP de Loopack 10.10.10.4. A configuração da sessão BGP pode ser observada na Figura 17.

```
PE01-SMARIA#sh run | sec bgp
router bgp 10
 bgp log-neighbor-changes
 neighbor 10.10.10.4 remote-as 10
 neighbor 10.10.10.4 update-source Loopback0
 !
 address-family ipv4
  redistribute connected
  neighbor 10.10.10.4 activate
 exit-address-family
 !
 address-family vpnv4
  neighbor 10.10.10.4 activate
  neighbor 10.10.10.4 send-community both
 exit-address-family
```

**Figura 17. Configuração do protocolo BGP em equipamento de *backbone*.**

A operadora fictícia possui o 10 como número do Sistema Autônomo (ASN), onde na Figura 17 observamos que foi configurado uma sessão iBGP com o *Route-Reflector*, e, em uma única sessão, o BGP está transportando informações com o seu vizinho sobre dois diferentes protocolos, o IPv4 (para troca de endereços IPv4) e o VPNv4 (para troca de endereços que estão nas tabelas de rotas virtuais – VRF).

## Apêndice D. Configuração da VRF

Todos os equipamentos que são PE da rede de *backbone* possuem VRF para cada cliente configurado, pois são nestes equipamentos em que os clientes têm uma conexão física. Conforme a Figura 18 abaixo, o "PE01-SMA" possuí a VRF borges e a VRF venancio configurada, pois ambos os clientes possuem uma conexão física com este equipamento.

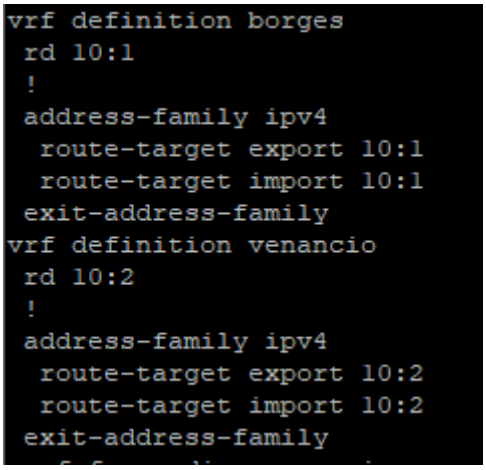


**Figura 18. Configuração das VRF no PE da rede de backbone.**

Nesta configuração, temos de atribuir um valor que distingue as rotas para cada VRF (rd – *Route-Distinguer*), onde é um número exclusivo anexado a cada rota dentro de uma VRF, e é composto por dois campos (rd 10:1 – Figura 18).

Logo após, temos de definir quais prefixos são importados e exportados na tabela de roteamento virtual. Neste caso, estamos importando e exportando todos os prefixos que contém como *Route-Distinguer* o valor atribuído nas VRF.

## Apêndice E. Configuração do protocolo MPLS

Todos os equipamentos do *backbone* possuem configurado o protocolo MPLS, que é mostrado na Figura 19 os comandos para habilitar este protocolo nos dispositivos.

```
mpls label range 500 599
mpls label protocol ldp

mpls ldp router-id Loopback0
```

**Figura 19. Configuração do protocolo MPLS no PE da rede de backbone.**

Para configuração do protocolo MPLS, temos de habilitar o protocolo de distribuição de etiquetas (*mpls label protocol ldp*) para permitir que o roteador troque informações de roteamento baseado em etiquetas com outros dispositivos que estão participando da rede MPLS.

Para cada roteador da rede de backbone é definido uma *range* de etiquetas para ser adicionado às rotas, pois assim a visualização da origem da tabela de roteamento em outro roteador é melhor definida.

No protocolo MPLS, também é definido o endereço IP de Loopback como o endereço identificador do processo MPLS. Por fim, é necessário habilitar o protocolo MPLS na interface física que vai fazer parte deste processo, conforme é mostrado na Figura 20, utilizando o comando "*mpls ip*".

```
interface Ethernet0/0
 description P-SMARIA
 ip address 172.16.0.18 255.255.255.252
 mpls ip
```

**Figura 20. Configuração do protocolo MPLS em interface física.**

Neste caso, está sendo habilitado o protocolo MPLS na interface física que interliga o PE01-SMA e o P-SMA.

## Apêndice F. Configuração do QoS

Para garantir a qualidade de comunicação entre as filiais e os servidores da matriz, foi configurado QoS nos equipamentos PE do *backbone*. Na Figura 21, observa-se a configuração de uma lista que é direcionada ao IP do servidor da matriz do supermercado Venâncio, seja qual for o tráfego de origem ou de destino para o servidor.

```
ip access-list extended SERVIDOR-VENANCIO
 permit ip any host 192.168.0.253
 permit ip host 192.168.0.253 any
```

**Figura 21. Configuração do QoS com base no endereço de IP de origem e destino.**

Também é necessário criar uma classe de mapa para classificar o tráfego que passa por uma *access-list* (ACL), conforme é observado na Figura 22.

```
class-map match-any SERVIDOR-VENANCIO
 match access-group name SERVIDOR-VENANCIO
```

**Figura 22. Configuração da *class-map* associada a ACL.**

Para concluir a configuração do QoS, é necessário classificar o tráfego de rede com base em critérios que sejam do interesse. No caso deste projeto, reserva-se 40% da banda total de 1Mb para acesso ao servidor, ou seja, têm-se garantido 400Kb na comunicação entre filial e o servidor da matriz, e 60% do tráfego restante será classificada pela classe default. Esta configuração é observada na Figura 23.

```
policy-map QoS_SERVIDOR_VENANCIO
 class SERVIDOR-VENANCIO
  bandwidth percent 40
 class class-default
  bandwidth percent 60
policy-map VENANCIO
 class class-default
  shape average 1024000
   service-policy QoS_SERVIDOR_VENANCIO
```

**Figura 23. Configuração da *policy-map* associando à *class-map* configurada.**

## Apêndice G. Configuração do cliente

Para demonstração da configuração da rede do cliente, será utilizado o roteador do supermercado Borges, onde será explanado os códigos das funcionalidades que foram configuradas para obter o desempenho desejado conforme metodologia.

Na Figura 24, demonstra-se a configuração dos endereçamentos IP nas interfaces físicas do roteador.

```
/ip address
add address=172.16.0.2/30 interface=ether1-wan-01 network=172.16.0.0
add address=192.168.0.1/24 interface=ether4-lan network=192.168.0.0
add address=172.16.0.6/30 interface=ether2-wan-02 network=172.16.0.4
```

**Figura 24. Configuração dos endereçamentos nas interfaces físicas do roteador.**

Pode ser observado na Figura 24 a configuração dos IP nas interfaces físicas que interligam com os equipamentos de *backbone* da operadora, na "ether1-wan-01" e "ether2-wan-02". Na interface designada "ether4-lan" possuí a configuração da rede interna, com o IP 192.168.0.1/24.

Conforme todas as filiais devem obter a navegação pela internet a partir da matriz, é necessário no roteador da matriz configurar um NAT [6] para todas as redes internas que possuirão navegação para a internet. A Figura 25 demonstra esta configuração.

```
/ip firewall nat
add action=masquerade chain=srcnat src-address=192.168.0.0/24
add action=masquerade chain=srcnat src-address=192.168.1.0/24
add action=masquerade chain=srcnat src-address=192.168.2.0/24
add action=masquerade chain=srcnat src-address=192.168.3.0/24
add action=masquerade chain=srcnat src-address=192.168.4.0/24
```

**Figura 25. Configuração NAT no roteador da matriz para navegação das unidades.**

Para o roteamento entre o dispositivo da matriz e o dispositivo da operadora, deve ser configurado o protocolo BGP. Na Figura 26, demonstra-se a configuração do protocolo BGP no equipamento da operadora.

[6] NAT é uma tecnologia que permite que máquinas que não possuam endereços válidos na internet, possam se conectar, utilizando um mascaramento de IP.

```
router bgp 10
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 10.10.10.4 remote-as 10
 neighbor 10.10.10.4 update-source Loopback0
 !
 address-family ipv4
  redistribute connected
  neighbor 10.10.10.4 activate
 exit-address-family
 !
 address-family vpnv4
  neighbor 10.10.10.4 activate
  neighbor 10.10.10.4 send-community both
 exit-address-family
 !
 address-family ipv4 vrf borges
  redistribute connected
  neighbor 172.16.0.2 remote-as 65000
  neighbor 172.16.0.2 description BORGES-MATRIZ-01
  neighbor 172.16.0.2 activate
  neighbor 172.16.0.14 remote-as 65002
  neighbor 172.16.0.14 description BORGES-FIL02
  neighbor 172.16.0.14 activate
 exit-address-family
```

**Figura 26. Configuração do BGP no equipamento da operadora no que se refere a rede de cliente.**

Conforme informações da Figura 26, a configuração do protocolo BGP da rede de cliente no equipamento da operadora deve estar dentro da seção “router bgp 10”, onde configura-se na “address-family ipv4 vrf borges” e é incluído as informações do *neighbor* (vizinho), que neste caso é o equipamento do cliente.

Por fim, a Figura 27 demonstra a configuração do protocolo BGP no equipamento do cliente.

```
/routing bgp peer
add default-originate=if-installed in-filter=BGP-IN-01 instance=MPLS name=\
    BGP-BORGES-01 out-filter=BGP-OUT-01 remote-address=172.16.0.1 remote-as=\
    10 ttl=default update-source=ether1-wan-01
add default-originate=if-installed in-filter=BGP-IN-02 instance=MPLS name=\
    BGP-BORGES-02 out-filter=BGP-OUT-02 remote-address=172.16.0.5 remote-as=\
    10 ttl=default update-source=ether2-wan-02
/routing filter
add action=accept chain=BGP-OUT-01
add action=accept chain=BGP-IN-01 set-bgp-local-pref=500
add action=accept chain=BGP-OUT-02 set-bgp-prepend=2
add action=accept chain=BGP-IN-02 set-bgp-local-pref=400
```

**Figura 27. Configuração do BGP no equipamento do cliente.**

Na Figura 27 apresenta-se a configuração de duas instâncias BGP, pelo fato da matriz ser duplamente abordada. A manipulação das rotas de entrada e saída é realizada pelos filtros configurados em “*routing filter*”, onde para uma maior preferência das rotas de entrada, é utilizado o “set-bgp-local-pref” com um valor maior (neste exemplo, foi utilizado o valor de 500), e para as rotas de saída, a que possuí valor no “set-bgp-prepend” é a menos prioritária.

## Apêndice H. Tabelas com as informações de endereçamentos IP da topologia

Na Tabela 1, apresenta-se a lista completa dos endereçamentos IP que foram utilizados nas interconexões entre equipamentos da rede de *backbone*.

**Tabela 1. Interconexões entre equipamentos de Backbone com seus respectivos endereçamento IP**

| Interconexão | Rede | Equipamento | IP |
|---|---|---|---|
| P-SMA x P-PAE | 172.16.0.0/30 | P-SMA | 172.16.0.1 |
| | | P-PAE | 172.16.0.2 |
| P-PAE x P-SCR | 172.16.0.4/30 | P-PAE | 172.16.0.5 |
| | | P-SCR | 172.16.0.6 |
| P-SMA x P-SCR | 172.16.0.8/30 | P-SMA | 172.16.0.9 |
| | | P-SCR | 172.16.0.10 |
| P-SMA x ROUTE-REFLECTOR | 172.16.0.12/30 | P-SMA | 172.16.0.13 |
| | | ROUTE-REFLECTOR | 172.16.0.14 |
| P-SMA x PE01-SMA | 172.16.0.16/30 | P-SMA | 172.16.0.17 |
| | | PE01-SMA | 172.16.0.18 |
| P-SMA x PE02-SMA | 172.16.0.20/30 | P-SMA | 172.16.0.21 |
| | | PE02-SMA | 172.16.0.22 |
| P-PAE x PE01-PAE | 172.16.0.24/30 | P-SMA | 172.16.0.25 |
| | | PE01-PAE | 172.16.0.26 |
| P-PAE x PE02-PAE | 172.16.0.28/30 | P-PAE | 172.16.0.29 |
| | | PE02-PAE | 172.16.0.30 |
| P-PAE x PE-SPO | 172.16.0.32/30 | P-PAE | 172.16.0.33 |
| | | PE-SPO | 172.16.0.34 |
| P-SCR x PE-SCR | 172.16.0.36/30 | P-SCR | 172.16.0.37 |
| | | PE-SCR | 172.16.0.38 |
| P-SMA x P-PAE | 172.16.0.0/30 | P-SMA | 172.16.0.1 |
| | | P-PAE | 172.16.0.2 |

Na Tabela 2, apresenta-se a lista completa dos endereços de Loopback que foram utilizados nos equipamentos de *backbone*.

**Tabela 2. IP Loopback dos equipamentos de *Backbone***

| Equipamento | IP Loopback |
|---|---|
| P-SMA | 10.10.10.1 |
| P-PAE | 10.10.10.2 |
| P-SCR | 10.10.10.3 |
| ROUTE-REFLECTOR | 10.10.10.4 |

| | |
|---|---|
| PE01-SMA | 10.10.10.5 |
| PE02-SMA | 10.10.10.6 |
| PE01-PAE | 10.10.10.7 |
| PE02-PAE | 10.10.10.8 |
| PE-SP | 10.10.10.9 |
| PE-SCR | 10.10.10.10 |

Na Tabela 3, apresenta-se a lista completa dos endereços que foram utilizados nas interconexões entre os equipamentos de *backbone* e os equipamentos dos clientes. Também é especificado o nome da VRF de cada unidade.

**Tabela 3. Interconexões entre equipamentos de Backbone e Cliente, com seus respectivos IP e nome da VRF que está atribuída**

| Interconexão | Rede | VRF | Equipamento | IP |
|---|---|---|---|---|
| PE01-SMA x VENANCIO-MATRIZ | 172.16.0.0/30 | venancio | PE01-SMA | 172.16.0.1 |
| | | | VENANCIO-MATRIZ | 172.16.0.2 |
| PE02-SMA x VENANCIO-MATRIZ | 172.16.0.4/30 | venancio | PE02-SMA | 172.16.0.5 |
| | | | VENANCIO-MATRIZ | 172.16.0.6 |
| PE02-SMA x VENANCIO-FIL01 | 172.16.0.8/30 | venancio | PE02-SMA | 172.16.0.9 |
| | | | VENANCIO-FIL01 | 172.16.0.10 |
| PE01-PAE x VENANCIO-FIL02 | 172.16.0.12/30 | venancio | PE01-PAE | 172.16.0.13 |
| | | | VENANCIO-FIL02 | 172.16.0.14 |
| PE01-SCR x VENANCIO-FIL03 | 172.16.0.16/30 | venancio | PE01-SCR | 172.16.0.17 |
| | | | VENANCIO-FIL03 | 172.16.0.18 |
| PE01-SPO x VENANCIO-FIL04 | 172.16.0.20/30 | venancio | PE01-SPO | 172.16.0.21 |
| | | | VENANCIO-FIL04 | 172.16.0.22 |
| | | | | |
| PE01-PAE x BORGES-MATRIZ | 172.16.0.0/30 | borges | PE01-PAE | 172.16.0.1 |
| | | | BORGES-MATRIZ | 172.16.0.2 |
| PE02-PAE x BORGES-MATRIZ | 172.16.0.4/30 | borges | PE02-PAE | 172.16.0.5 |
| | | | BORGES-MATRIZ | 172.16.0.6 |
| | 172.16.0.8/30 | borges | PE02-SMA | 172.16.0.9 |

| | | | | |
|---|---|---|---|---|
| PE02-SMA x BORGES-FIL01 | | | BORGES-FIL01 | 172.16.0.10 |
| PE01-PAE x BORGES-FIL02 | 172.16.0.12/30 | borges | PE01-PAE | 172.16.0.13 |
| | | | BORGES-FIL02 | 172.16.0.14 |
| PE01-SCR x BORGES-FIL03 | 172.16.0.16/30 | borges | PE01-SCR | 172.16.0.17 |
| | | | BORGES-FIL03 | 172.16.0.18 |
| PE01-SPO x BORGES-FIL04 | 172.16.0.20/30 | borges | PE01-SPO | 172.16.0.21 |
| | | | BORGES-FIL04 | 172.16.0.22 |

Na Tabela 4, apresenta-se a lista completa dos endereços que foram utilizados na rede interna do cliente (LAN), juntamente com o ASN do protocolo BGP que foi disposto em cada local.

**Tabela 4. Informações de endereçamento da rede LAN dos clientes e do número do AS que foi configurado em cada local**

| Cliente | Unidade | Rede LAN | ASN BGP |
|---|---|---|---|
| Venâncio | Matriz | 192.168.0.0/24 | 65000 |
| Venâncio | FIL01 | 192.168.1.0/24 | 65001 |
| Venâncio | FIL02 | 192.168.2.0/24 | 65002 |
| Venâncio | FIL03 | 192.168.3.0/24 | 65003 |
| Venâncio | FIL04 | 192.168.4.0/24 | 65004 |
| Borges | Matriz | 192.168.0.0/24 | 65000 |
| Borges | FIL01 | 192.168.1.0/24 | 65001 |
| Borges | FIL02 | 192.168.2.0/24 | 65002 |
| Borges | FIL03 | 192.168.3.0/24 | 65003 |
| Borges | FIL04 | 192.168.4.0/24 | 65004 |

Na Tabela 5, apresenta-se a lista completa dos endereços que foram utilizados nos ativos da rede interna do cliente (computadores e servidores).

**Tabela 5. Informações de endereçamento IP dos equipamentos interno de cada cliente, com seu respectivo local**

| Cliente | Unidade | Equipamento | IP |
|---|---|---|---|
| Venâncio | Matriz | SERVIDOR | 192.168.0.253 |
| | | PC | 192.168.0.254 |
| Venâncio | FIL01 | PC | 192.168.1.254 |
| Venâncio | FIL02 | PC | 192.168.2.254 |

| | | | |
|---|---|---|---|
| Venâncio | FIL03 | PC | 192.168.3.254 |
| Venâncio | FIL04 | PC | 192.168.4.254 |
| Borges | Matriz | SERVIDOR | 192.168.0.153 |
| | | PC | 192.168.0.154 |
| Borges | FIL01 | PC | 192.168.1.154 |
| Borges | FIL02 | PC | 192.168.2.154 |
| Borges | FIL03 | PC | 192.168.3.154 |
| Borges | FIL04 | PC | 192.168.4.154 |