UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE INFORMÁTICA
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

RODOLPHO DE CASTRO ALVES
THIAGO SANTOS DE MATOS

PLANEJAMENTO DE UMA INFRAESTRUTURA DE REDE HIERÁRQUICA UTILIZANDO BOAS PRÁTICAS DE IMPLEMENTAÇÃO

TRABALHO DE CONCLUSÃO DE CURSO

CURITIBA

2016

RODOLPHO DE CASTRO ALVES
THIAGO SANTOS DE MATOS

PLANEJAMENTO DE UMA INFRAESTRUTURA DE REDE HIERÁRQUICA UTILIZANDO BOAS PRÁTICAS DE IMPLEMENTAÇÃO

Trabalho de Conclusão de Curso apresentada ao Bacharelado em Sistemas de Informação da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do grau de "Bacharel em Sistemas de Informação".

Orientador: Prof. Fabiano Scriptore de Carvalho, MSc

CURITIBA

2016

Ministério da Educação
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
Câmpus Curitiba
Diretoria de Graduação e Educação Profissional
Departamento Acadêmico de Informática
Coordenação do Curso de Bacharelado em Sistemas de Informação

TERMO DE APROVAÇÃO

“PLANEJAMENTO DE UMA INFRAESTRUTURA DE REDE HIERÁRQUICA UTILIZANDO BOAS PRÁTICAS DE IMPLEMENTAÇÃO”

por

“Rodolpho de Castro Alves e Thiago Santos de Matos”

Este Trabalho de Conclusão de Curso foi apresentado às _____ **hs** do dia **5** de **dezembro** de **2016** como requisito parcial à obtenção do grau de Bacharel em Sistemas de Informação na Universidade Tecnológica Federal do Paraná - UTFPR - Câmpus Curitiba. O(a)(s) aluno(a)(s) foi(ram) arguido(a)(s) pelos membros da Banca de Avaliação abaixo assinados. Após deliberação a Banca de Avaliação considerou o trabalho _____.

_____ **Prof. Fabiano Scriptore de Carvalho** (Presidente - UTFPR/Curitiba)	_____ **Prof. Anelise Munaretto Fonseca** (Avaliador 1 – UTFPR/Curitiba)
_____ **Prof. Luiz Augusto Pelisson** (Avaliador 2 - UTFPR/Curitiba)	_____ **Prof. Leyza Elmeri Baldo Dorini** (Professor Responsável pelo TCC – UTFPR/Curitiba)
_____ **Prof. Leonelo Dell Anhol Almeida** (Coordenador do curso de Bacharelado em Sistemas de Informação – UTFPR/Curitiba)	

“A Folha de Aprovação assinada encontra-se na Coordenação do Curso.”

AGRADECIMENTOS

Agradeço a meus pais e aos meus avós, por toda a paciência, apoio e compreensão durantes esses últimos 4 anos. Eu não teria conseguido realizar metade do que realizei se não fosse pelo apoio deles. Os últimos anos não foram fáceis, mas foram o maior aprendizado de toda a minha vida.

Dedico este trabalho à memória de meu pai Guanito Prado Alves Filho, sem o qual eu jamais teria conseguido me mudar para Curitiba e cursar o ensino superior. Foi graças aos esforços dele que pude perseguir a oportunidade e no fim conquistar a possibilidade de me mudar para outro estado e conseguir me dedicar aos estudos.

Agradeço aos meus amigos Rafael José, Israel Laurensi e Vítor Tozzi por toda a amizade, companheirismo e paciência que tivemos durante toda a graduação.

Um agradecimento ao nosso orientador, professor e amigo Fabiano Scriptore. Graças a ele que me interessei pela área de redes, em especial toda a área de segurança.

Rodolpho de Castro Alves

AGRADECIMENTOS

Agradeço minha família, por toda paciência e compreensão da dificuldade e tensão decorridos do desenvolvimento deste trabalho, o apoio destes foi fundamental para que certos problemas fossem solucionados.

Um agradecimento à minha namorada Nadinne Zem, a qual foi fundamental ao longo do processo, em momentos difíceis e complicados. O apoio e carinho que recebi dela foram muito importantes para continuar focado e determinado no processo de desenvolvimento deste trabalho.

Agradeço aos meus amigos Ricardo Bonato, Carlos Mayrhofer, Guilherme Kira, Vitor Tozzi, Rafael José e Israel Laurensi por toda amizade e companheirismo demonstrados não apenas no desenvolvimento deste trabalho de conclusão de curso, mas ao longo de toda a graduação.

Um agradecimento em especial ao professor Fabiano Scriptore que me apresentou a disciplina de redes de computadores, e foi o responsável por me mostrar a área que tenho mais interesse dentro do curso. Os ensinamentos que me foram passados foram extremamente proveitosos e valiosos.

Thiago Santos de Matos

RESUMO

Alves, Rodolpho, Matos, Thiago. PLANEJAMENTO DE UMA INFRAESTRUTURA DE REDE HIERÁRQUICA UTILIZANDO BOAS PRÁTICAS DE IMPLEMENTAÇÃO. 92 f. Trabalho de Conclusão de Curso – Bacharelado em Sistemas de Informação, Universidade Tecnológica Federal do Paraná. Curitiba, 2016.

As redes de computadores, no cenário atual, se mostram indispensáveis à empresas, universidades, ou até mesmo para uso pessoal. Entretanto, muitas redes de computadores são implementadas sem levar em consideração os aspectos de funcionalidade e segurança da rede em questão. Desta forma, o principal objetivo deste trabalho é apresentar uma maneira de desenvolver uma topologia de rede, cujas características definam um cenário mais seguro e funcional aos seus usuários. Com isso, os recursos de Etherchannel, protocolo Spanning-Tree, Port-Security e VoIP, são apresentados e utilizados para garantir tal objetivo. O trabalho leva em consideração a implementação de boas práticas em redes locais, procurando minimizar problemas de segurança e desempenho da rede. A topologia a ser apresentada neste trabalho foi planejada com base no modelo hierárquico de camadas, visando também contribuir para a funcionalidade da rede de modo geral.

Palavras-chave: Redes de Computadores, Segurança da Informação, VoIP, QoS, Topologia de Rede

ABSTRACT

Alves, Rodolpho, Matos, Thiago. PLANNING A HIERARCHICAL NETWORK ARCHITECTURE IN ACCORDANCE TO THE GOOD INDUSTRY PRACTICE. 92 f. Trabalho de Conclusão de Curso – Bacharelado em Sistemas de Informação, Universidade Tecnológica Federal do Paraná. Curitiba, 2016.

Nowadays computer networks are indispensable to enterprises, universities and even for personal use. However, many networks are poorly implemented, without taking into consideration all the possible funcionalities and the best security possible. Thus, the main goal of this thesis is to present a way to better develop a network topology, which characteristics define a safer and better network to its users. To achieve that we'll present and use tecnologies such as Etherchannel, Spanning-Tree Protocol, PortSecurity, VoIP and QoS in order to reach the goal. This thesis takes into account the good industry practices in order to minimize issues related to the network's security and performance. The resulting topology from this thesis has been planned taking into account the hierarchical network architecture, in order to allow for full network functionality.

Keywords: Computer Networks, Information Security, VoIP, QoS, Network Topology

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

No passado as empresas que utilizavam tecnologia da informação (TI) em seu negócio possuíam um compartimento físico exclusivo para computadores, um ambiente muitas vezes isolado do resto da instituição, onde seus *softwares* eram executados de maneira isolada em computadores com acesso restrito a apenas técnicos altamente capacitados para aquela tarefa, era um conceito de "Central de Computadores". Atualmente, o conceito de "Datacenter" persiste, mas não da mesma maneira que outrora, pois atualmente uma infraestrutura organizada de TI não é mais um diferencial: É uma necessidade.

Os computadores de uma empresa devem estar conectados a computadores localizados em ambientes diferentes, a informação deve estar amplamente disponível para garantir o bom funcionamento da empresa e seu negócio.

Para garantir essa comunicação, surgiram as redes locais de computadores (LANs), em que dois ou mais computadores são interligados por um meio comum de comunicação Tanenbaum (2003). Graças às redes locais tornou-se possível interligar grupos de computadores pertencentes à mesma empresa, permitindo a descentralização dos equipamentos de TI, com isto, não é preciso que todo o equipamento esteja isolado dos colaboradores da instituição em uma sala isolada.

Para assegurar o bom funcionamento das redes locais surgiram tecnologias como o Quality of Service (QoS) e artefatos como roteadores e *switches* mais avançados, que permitem melhor gerenciamento da rede. Também houve o advento da tecnologia *Voice over Internet Protocol* (VoIP) que permite voz seja transmitida pela rede local. Em conjunto com a tecnologia de QoS, que assegura a qualidade necessária, a tecnologia de VoIP torna-se uma alternativa factível à telefonia convencional, com diferencial de uma manutenção mais acessível, maior qualidade e de custos mais baixos.

Sendo assim é desejável que as empresas que se utilizam de redes locais consigam realizar seus trabalhos com garantias de que esta tecnologia suporta tais ações. Neste ponto a rede em si e os equipamentos que a compõe devem garantir a QoS, que corresponde

ao nível de desempenho entre aplicações. A estrutura da rede local também deve ser planejada e executada de maneira a assegurar a disponibilidade dos dados e atrelada a políticas de segurança da informação para que nenhum elemento na rede possa ser comprometido por um invasor ou que dados sejam interceptados e lidos por indivíduos não autorizados.

1.1 OBJETIVOS

1.1.1 OBJETIVO GERAL

Implementar uma infraestrutura hierárquica de redes locais (LAN) para o estudo de boas práticas, implementação de *Quality of Services* (QoS), segurança de dados e voz sobre IP (VoIP).

1.1.2 OBJETIVOS ESPECÍFICOS

- Fazer o mapeamento físico da topologia a ser criada;
- Fazer o projeto lógico da topologia;
- Fazer um estudo das ferramentas que serão utilizadas para a implementação da topologia que será abordada no trabalho;
- Implementar na prática o projeto físico e lógico;
- Realizar os devidos testes de disponibilidade, segurança e qualidade para gerar resultados sobre o trabalho desenvolvido;

1.2 JUSTIFICATIVA

Neste trabalho foram abordadas algumas práticas para implementação e desenvolvimento de uma rede local de modo eficiente, tendo em vista a utilização de QoS para assegurar prioridade a certos tipos de pacotes de dados, políticas de segurança da informação e e as boas práticas de infraestrutura para garantir o pleno funcionamento da rede.

Com isso o trabalho irá fornecer base e subsídios para a montagem de uma futura rede local, que poderá ser utilizada inclusive na própria Universidade Tecnológica Federal do Paraná, a fim de promover melhorias neste aspecto.

2 REFERENCIAL TEÓRICO

2.1 VISÃO GERAL DE REDES DE COMPUTADORES

2.1.1 MODELOS DE CAMADAS

Esta seção do referencial teórico visa fornecer uma visão geral sobre o assunto de redes de computadores, bem como esclarecer certos termos e nomenclaturas que serão utilizados ao longo do trabalho.

Um bom exemplo de rede de computadores, segundo Kurose e Ross (2010), é a Internet que temos a nossa disposição diariamente, que permite a troca de informações e o compartilhamento de recursos entre seus diversos usuários. Entretanto nem sempre houve esta facilidade para realização destas operações consideradas simples hoje em dia para redes de computadores. Conforme menciona Mendes (2007), existiu um período em que havia muita incompatibilidade entre produtos desenvolvidos por empresas diferentes para redes de computadores, dessa forma as empresas acabavam ficando totalmente dependentes de um único fornecedor, uma vez que seus produtos eram incompatíveis com produtos concorrentes.

Para solucionar este problema, Mendes explica que a International Organization for Standardization (ISO) definiu um padrão universal de troca de informações dentro de uma mesma rede e entre redes distintas. Este padrão é conhecido como Modelo de Referência OSI, definido em 7 camadas conforme ilustrado na figura 1

Apesar do desenvolvimento do Modelo OSI, Mendes alega que levou um tempo demasiadamente longo para sua conclusão, de forma que o Departamento de Defesa do Governo dos Estados Unidos da América (DoD – Department of Defense) acabou desenvolvendo um Modelo de Protocolo que foi concluído antes do Modelo ISO (International Organization for Standardization). Este Modelo é chamado de TCP/IP (Transmission Control Protocol), e possuía em um primeiro momento a simples ideia de manter os equipamentos conectados por um determinado tempo. Dessa forma, o Modelo de Referência

Figura 1: Modelo de Referência OSI
Fonte: Autoria Própria.

OSI acabou não se tornando um padrão, uma vez que quando foi finalizado o Modelo de Protocolo TCP/IP já era bastante utilizado, servindo de base inclusive pra internet. A figura 2 apresenta o modelo de protocolo TCP/IP.

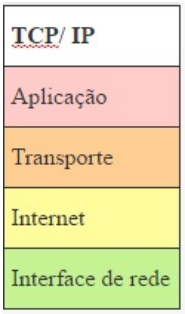

Figura 2: Modelo de Protocolo TCP/IP
Fonte: Autoria Própria.

2.1.2 COMPONENTES DE UMA REDE DE COMPUTADORES

Conforme IESDE (2010), existem alguns equipamentos que podem compor uma rede de computadores:

- **Hub**: Este equipamento é utilizado para interligar pontos de uma rede de computadores entre si. O hub funciona enviando um mesmo pacote de dados a todos os pontos que estejam associados a ele, o que é conhecido como *Broadcast*.

- **Switch**:
  - **Switch Não-Gerenciável**: De acordo com IESDE (2010), o switch é um equipamento utilizado genericamente igual ao hub, com o ideal de conectar pontos de uma rede entre si. Entretanto, a grande diferença entre os dois equipamentos é que o switch apresenta uma tabela dinâmica alocada em sua memória que permite encaminhar o pacote de dados especificamente para uma de suas portas, sem que as outras portas recebam o mesmo pacote. Além disso, este equipamento não possui o recurso de criação de VLANs, como possui o switch gerenciável.
  - **Switch Gereciável**: Este equipamento permite a criação de VLANs (Virtual Local Area Network), redes locais virtuais (KUROSE; ROSS, 2010), ou seja, as máquinas que compõem a rede local não precisam necessariamente estar no mesmo ambiente físico. Sendo assim, segundo (PILLOU, 2014), a criação das VLANs é possível uma vez que o agrupamento das máquinas é feito com base em critérios diferentes, como o protocolo utilizado, número da porta, endereço MAC, entre outros.
- **Router**: Este equipamento possui como objetivo promover a interligação de duas redes distintas entre si, conforme explicado por IESDE (2010). O uso dos roteadores se faz necessário entre redes distintas, ainda que esta comunicação pudesse ser provida apenas por switches, entretanto o gerenciamento se torna demasiadamente complexo e lento.

2.1.3 PROTOCOLOS

Os protocolos, conjunto de regras e definições de comunicação, servem para promover uma comunicação entre duas ou mais máquinas em uma rede em um determinado contexto de serviço de rede (RIOS, 2010). Os serviços de rede são suportados pelos diversos protocolos existentes, como por exemplo ao realizar um download de um arquivo qualquer da Internet é utilizado o protocolo FTP (File Transfer Protocol),ou ao ser utilizado o serviço de email o protocolo SMTP (Simple Mail Transfer Protocol) é utilizado.

Kurose e Ross (2010) afirmam que um protocolo no universo de redes de computadores pode ser comparado a um protocolo na esfera social de pessoas, e este protocolo gerencia a comunicação entre as entidades participantes do processo. Além disso, o autor ainda afirma que os protocolos são responsáveis por estabelecer uma ordem e um formato

definidos para a troca das mensagens.

A seguir mostraremos a relação das camadas do Modelo de Protocolo TCP/IP, com uma breve descrição de cada camada e seus respectivos protocolos:

1. **Camada de Aplicação**: Corresponde a sétima camada do modelo OSI, e é responsável por prover serviços para as aplicações (KUROSE; ROSS, 2010). Sendo assim, esta camada corresponde àquela mais próxima do usuário, e seus protocolos são: HTTP, FTP, SMTP, DNS, entre outros, conforme apresentado por Teleco (2013).

2. **Camada de Transporte**: Conforme descrito por Rios (2010), depois de processar a requisição da aplicação, a camada de aplicação se comunica com a camada de transporte via uma interface chamada socket. Sendo assim, a camada de transporte oferece dois protocolos principais: o TCP (Transmission Control Protocol) e o UDP (User Datagram Protocol)

   - **TCP**: Rios (2010) menciona que o TCP é um protocolo orientado a conexão, ou seja garante uma entrega confiável dos dados entre dois pontos de uma rede, além de eliminar dados duplicados. Sendo assim é considerado um protocolo seguro e confiável.
   - **UDP**: O protocolo UDP não apresenta as mesmas garantias que o TCP, ou seja, não é um protocolo orientado a conexão, logo não fornece garantia de que conseguirá entregar os dados (RIOS, 2010). O autor ainda afirma que apesar das desvantagens aparentes, o UDP é uma escolha viável para aplicações em tempo real como som, vídeo e jogos, uma vez que existem menos trocas de informações, logo acaba sendo um protocolo mais rápido.

3. **Camada de Rede**: Esta camada possui como principal protocolo o Internet Protocol (IP) (RIOS, 2010). De acordo com o autor, toda e qualquer máquina que deseje possuir acesso à Internet é necessário que a mesma possua um endereço IP associado a ela. Este protocolo é responsável por agregar ao datagrama[1] recebido o endereço IP do emissor de dados e do receptor destes dados. Rios (2010) ainda afirma que inicialmente foi desenvolvido a versão IPv4 deste protocolo, que era composto de 4 conjuntos de 8 bits cada. Entretanto com a popularização da informática e com o passar do tempo, este protocolo acabou saturando seus endereços disponíveis, tornando-os escassos. A solução apresentada foi o desenvolvimento de uma nova

[1]Unidade de transferência básica em uma rede de computadores.

versão deste protocolo que disponibilizasse um maior número de endereços para o crescente número de dispositivos no mundo. A nova versão foi chamada de IPv6, e possui 8 grupos com 4 dígitos hexadecimais em cada grupo. Dessa forma, o problema de escassez de endereços foi resolvido com base na nova versão do protocolo IP, lançada no ano de 2012.

4. **Camada de Enlace**: De acordo com Kurose e Ross (2005), o meio que promove a ligação entre nós adjacentes em uma rede de computadores é chamado de enlace. Esta camada tem por função justamente fazer a transferência de um datagrama de um nó componente da rede para outro nó adjacente sobre um determinado enlace que os interligue. O autor ainda afirma que o pacote de dados nesta camada recebe o nome de quadro e engloba o datagrama proveniente da camada de rede. Outro ponto importante que o autor ressalta é que cada enlace pode atuar com base em um protocolo de camada de enlace diferente, ou seja, certos serviços e características que são garantidos em uma determinada parte da rota do pacote de dados, podem não ser garantidos em outra parte desta rota. Segundo Kurose e Ross (2005), além do endereço IP, o endereço MAC (Media Access Control) é bastante utilizado pela camada de enlace. Isso porque o endereço IP define a rede em que o computador está situado, é um identificador para a conexão com a Internet, ao passo que o endereço MAC é atribuído pelo fabricante diretamente à placa de rede. O autor afirma que para uma máquina obtenha o endereço MAC de outra máquina na rede é necessário a utilização do protocolo ARP (Address Resolution Protocol). Neste caso uma máquina manda uma mensagem broadcast com o IP da máquina destinatária, e esta máquina responde com o seu endereço MAC. De acordo com Kurose e Ross (2005) uma das tecnologias de LAN mais utilizadas é a Ethernet, que é especificada no padrão 802.3.

5. **Camada Física**: Segundo afirma Tanenbaum (2003), o principal objetivo da camada física do modelo de referência em questão é a transferência de um fluxo bruto de bits de um ponto ao outro da rede. Ainda segundo o autor os meios físicos são agrupados em duas categorias principais: guiados (fio de cobre e fibras óticas) e não-guiados (ondas de rádio e raio laser). A categoria de não-guiados é uma modalidade voltada para certos tipos de usuários, como por exemplo locais com acidentes geográficos. Neste caso a tecnologia de transmissão sem fio se encaixa pra solucionar o problema em questão

6. **Camada Física - Guiados**:

- **Par trançado**: Este é o meio mais antigo e mais comum de transmissão de dados (TANENBAUM, 2003). Nesta categoria os fios são enrolados de forma helicoidal, deste modo o produto final apresenta menor interferência quando comparado ao mesmo produto composto por dois fios paralelos. A principal aplicação do par trançado, segundo Tanenbaum (2003) é o setor da telefonia, no qual a ligação estabelecida entre diversos telefones e a estação central da companhia telefônica é feita por meio de par trançado. Pela relação entre o custo e o desempenho do composto, o par trançado é utilizado em larga escala, e segundo o autor, a probabilidade é que esse cenário seja mantido em um futuro próximo.
- **Fibra Óptica**: Um sistema de transmissão óptico é composto de 3 principais elementos: a fonte de luz, o meio de transmissão e o detector (TANENBAUM, 2003). O autor afirma que conforme convenção adotada um pulso de luz corresponde a um bit 1, e a ausência de luz representa um bit 0. O meio de transmissão corresponde a uma fibra de vidro de baixa espessura, e o detector produz um pulso elétrico quando entra em contato com a luz proveniente da transmissão.

7. **Camada Física - Não-Guiados**: Já dentro da categoria dos não-guiados da camada física do Modelo de Protocolo TCP/IP, Tanenbaum (2003) descreve ser uma modalidade voltada para certos tipos de usuários, como por exemplo locais com acidentes geográficos ou com obstáculos que impossibilitam ou dificultam a transmissão através dos meios guiados. Neste caso a tecnologia de transmissão sem fio se encaixa para solucionar o problema em questão. Dois métodos são descritos por Tanenbaum (2003) a seguir:

   - **Transmissão de Rádio**: O autor afirma que ondas de rádio são fáceis de serem geradas e alcançarem seus alvos. Isso porque se propagam de forma omnidirecional a partir do ponto emissor do sinal, ou seja, se propagam em todas as direções. A desvantagem deste modo de transmissão, segundo afirma o autor é que apesar da facilidade de geração e propagação das ondas, em todas as frequências as ondas estão sujeitas a sofrerem interferências de fatores externos. Além disso, esta modalidade de comunicação de dados oferece uma baixa largura de banda na troca de dados entre dois pontos de uma rede segundo Tanenbaum (2003).
   - **Transmissão de Microondas**: Segundo Tanenbaum (2003) a ideia desta

modalidade de transmissão é concentrar as ondas de transmissão em uma faixa estreita, uma vez que todas possuem frequência acima de 100 MHz. Como as microondas viajam em linha reta, a ideia neste modo de transmissão é instalar torres de transmissão em linha reta e sem obstáculos entre os transmissores, de modo a propagar o sinal. Entretanto se a distância for demasiadamente grande entre estas torres, Tanenbaum (2003) afirma que é necessário o uso de repetidores para conseguir propagar o sinal com qualidade para a próxima torre. O autor ainda afirma que ao contrário das ondas de rádio, as microondas não conseguem atravessar paredes de um prédio com a mesma facilidade, o que configura uma desvantagem neste modo de transmissão.

2.1.4 REDES LOCAIS

As redes locais podem ser entendidas, segundo Tanenbaum (2003), como todas aquelas redes que são compreendidas em um prédio ou um câmpus universitário, por exemplo. Este tipo de rede permite a conexão de computadores pessoais, o que possibilita o compartilhamento de dados e informações com outros computadores pertencentes à mesma rede. Ainda de acordo com Tanenbaum (2003), as redes locais possuem algumas características que a diferenciam de outros tipos de redes, como por exemplo:

- **Tamanho da Rede**: As redes locais possuem um tamanho limitado, o que é compatível com a ideia de uma rede local corresponder ao escopo de um prédio ou campus universitário. Além disso, este tamanho reduzido de rede favorece o gerenciamento desta, uma vez que sua abrangência é menor que de outros tipos de rede.
- **Tecnologia de Transmissão**: Basicamente a tecnologia de transmissão utilizada é um cabo ao qual todas as máquinas que integram a rede de computadores se conectam.
- **Topologia**: As redes locais permitem o desenvolvimento de duas topologias:
  - **Rede de Barramento**: Neste tipo de topologia em um dado intervalo de tempo apenas uma única máquina componente da rede tem a possibilidade de se comportar como máquina-mestra, ou seja, tem a possibilidade de transmitir dados. Ou seja, quando uma máquina tem o poder de mestre, as outras máquinas não devem manifestar a capacidade de transmissão de dados. A figura 3 apresenta um exemplo de uma topologia em barramento.

– **Rede em Anel**: Neste sistema de difusão os pacotes não são trafegados na íntegra, e sim com o ideal de que cada bit é independente do restante que compõe o pacote. Um exempo de uma rede em anel pode ser observado na figura 4.

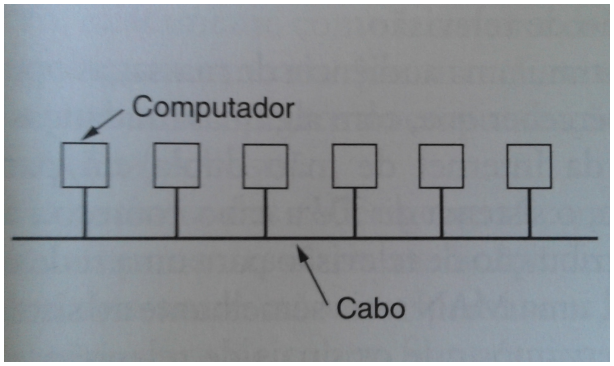

Figura 3: Exemplo de uma rede de barramento lógico.
Fonte: (TANENBAUM, 2003)

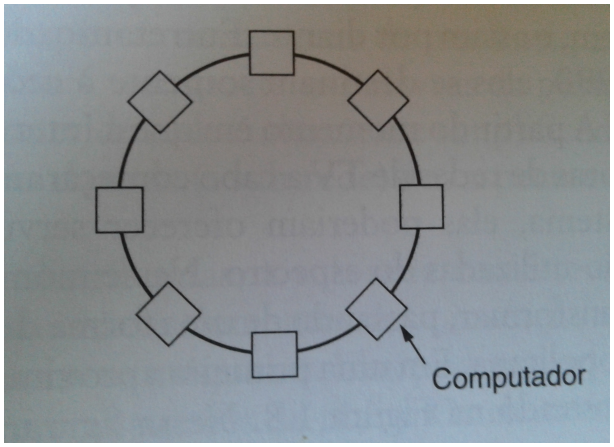

Figura 4: Exemplo de uma rede em topologia em anel.
Fonte: (TANENBAUM, 2003)

2.2 REDES HIERÁRQUICAS

Para a implementação dos requisitos propostos para a rede a ser desenvolvida neste trabalho, torna-se necessário a definição de o que é, e como funciona uma rede hierárquica.

Segundo Hucaby (2014), uma rede hierárquica é uma rede caracterizada pela redundância entre seus elos e a divisão em três camadas, tal divisão permite à rede uma

alta escalabilidade e disponibilidade, além de permitir uma ótima divisão em domínios específicos, onde podemos aplicar regras e políticas específicas de segurança.

As três camadas que compoem uma rede hierárquica são (HUCABY, 2014):

- **Camada de Acesso (Access Layer)**: Composta por switches gerenciáveis (preferencialmente) ou não-gerenciáveis, *access points* e maquinas de *end-point*(*Desktops*, *Laptops*, Telefones VoIP e Servidores de Email, Bancos de Dados, Web e FTP). É a camada mais baixa da rede, permite que os usuários se conectem à rede e utilizem os recursos nela presentes. Os equipamentos dessa camada não precisam de alto desempenho. As falhas nessa camada são toleráveis e normalmente simples de resolver.

- **Camada de Distribuição (Distribution Layer)**: Composta por switches camada 3. É a camada média da rede, permitindo a comunicação entre os diferentes nodes da camada de acesso. Nesta camada são implementadas as regras de VLAN, permitindo a segregação do tráfego conforme necessário. Os equipamentos dessa camada precisam de um nível médio de desempenho, devido à quantidade média de dados que passaram por essa camada, falhas nessa camada afetam vários nodes, sendo necessário uma correção mais ágil do que as da camada de acesso.

- **Camada de Núcleo (Core Layer)**: Composta por switches camada 3 e roteadores. É a principal camada da rede, responsável por comunicar os diferentes nodes da camada de distribuição e de realizar o enlace com a rede externa (WAN). Os equipamentos desta camada precisam ser de alto desempenho, falhas nessa camada não são toleráveis pois afetam subdomínios inteiros, as falhas nessa camada devem ser resolvidas urgentemente.

A tabela 1 apresenta as camadas hierárquicas e os dispositivos que compoem cada camada, a figura 5 apresenta um exemplo de uma rede hierárquica dividida nas três camadas propostas.

Camada Hierárquica	Dispositivos
Camada de Acesso	Desktops, Laptops, Access Points, Servidores e Switches L2
Camada de Distribuição	Switches L3 Gerenciáveis
Camada de Núcleo	Switches L3 Gerenciáveis, Roteadores

Tabela 1: Camadas Hierárquicas e dispositivos que as compoem.

Fonte: Autoria Própria.

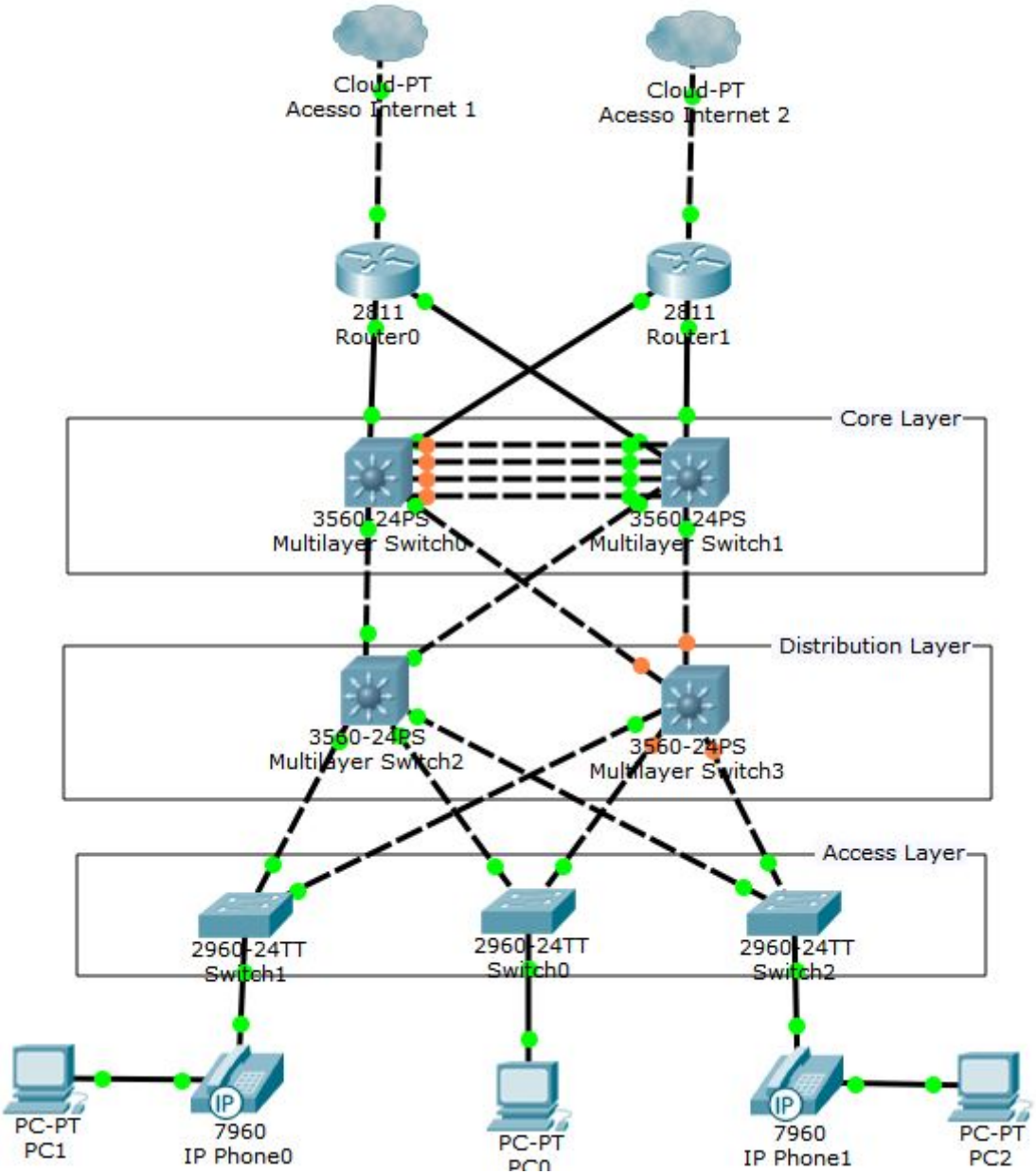

Figura 5: Uma topologia de uma rede hierárquica de três camadas.
Fonte: Autoria Própria.

Conforme pode ser observado na figura 5 uma rede hierárquica depende da boa divisão entre suas camadas e da redundância entre os pontos da rede, essa redundância entre os elos permite que caso uma falha ocorra, a rota seja alterada para o elo seguinte, assim não comprometendo o acesso aos recursos da rede.

2.3 QUALIDADE DE SERVIÇO (QOS)

O trabalho proposto até então visa o desenvolvimento de topologia de rede local baseada em boas práticas que garantam qualidade de serviço (QoS) ao que está sendo implementado. Sendo assim, QoS é a capacidade que a rede possui de garantir uma taxa mínima de transmissão de dados entre dois pontos distintos entre si (MACURA et al., 2011). Ainda segundo o autor existem certos recursos para verificação da qualidade de serviço em uma rede, como por exemplo a qualidade da imagem e do som que chegam ao local que fez as requisições.

Atualmente o tráfego de dados multimídia consome grande largura de banda, e pode ser exemplificado por meio de vídeo conferências, ensino e aprendizado a distância e transmissões em tempo real (PHONPHOEM; JANSANG, 2001). Sendo assim, este é o caso em que o atraso na entrega de pacotes de informações é de extrema importância, uma vez que se houver um atraso ou perda de pacotes no lado receptor, necessariamente haverá perdas de informações, e por consequência menor qualidade no serviço em questão. Vale lembrar ainda que não são apenas as aplicações de multimídia que consomem grande parte da largura de banda, mas os serviços regulares da Internet como email e troca de arquivos também competem pelos mesmos recursos (PHONPHOEM; JANSANG, 2001).

Sendo assim, segundo (FALSARELLA, 2009), as aplicações de dados, videoconferência e voz sobre IP (dados multimídia) possuem requisitos diferentes entre si, como ilustrado na tabela 2.

Tabela 2: Relação entre tipos de dados de aplicação, tamanho e atraso para envio

Aplicação	Tamanho	Atraso	Banda Mínima	Tempo de Envio[2]
Dados	Variável, até 1500 bytes	Variável	Variável	47ms
Videoconferência	700 bytes	30 ms	160 kbps	22 ms
VoIP	60 bytes	20 ms	24 kbps	2 ms

Fonte: (FALSARELLA, 2009)

Para suportar cada uma destas transações de maneira eficiente, o principal ideal é que as perdas de pacotes de dados seja inexistente ou a menor possível (FALSARELLA, 2009). Para isso, uma maneira de se alcançar o objetivo é com a definição de um buffer interno de alta capacidade do roteador. Entretanto esta solução para atender as demandas das transações pode acarretar uma alta variação no atraso entre os envios de pacotes (conhecida como jitter). O QoS tem a função de buscar um equilíbrio entre o que pode ser ganho para corrigir uma deficiência de uma transação e o que pode ser um prejuízo

de modo geral, trata de modo diferenciado o tráfego a fim de garantir o nível de qualidade pretendido em cada uma das transações. O autor ainda exemplifica esta situação ao mencionar que dados convencionais conseguem lidar e suportar o jitter, porém ao abordar dados de transmissão em tempo real como VoIP e vídeo, este conceito acaba sendo extremamente prejudicial ao objetivo final de transmissão de dados.

As especificações do QoS de uma determinada aplicação devem ser especificadas em cada nó ou roteador integrante de uma rede, para que haja uma noção clara do limite mínimo de informações que deveriam chegar ao nó requisitor (PHONPHOEM; JANSANG, 2001). Ainda segundo o autor, o tráfego de dados pode ser classificado em duas categorias principais baseado nos requisitos necessários do QoS:

1. **Tráfego de Tempo Real**:

   Esta categoria contempla os dados de multimídia que são dependentes de uma troca de informações sem que haja perda de dados ao longo da rede, uma vez que o ideal é que o nó requisitante receba na íntegra o que foi respondido originalmente pelo nó emissor.

2. **Tráfego de Tempo Não-Real**:

   Esta categoria por sua vez aborda dados que podem sofrer pequenas perdas ao longo do caminho pela rede, como os dados convencionais, não associados ao conceito de voz ou vídeo. Diferentemente dos dados de multimídia explicados na categoria acima, em que não podem ocorrer perdas de informações.

   Uma vez que existem diferenças entre os requisitos dos diversos pacotes de dados que são trocados pelas redes, é necessário alcançar cada requisito destes dados a fim de garantir o QoS (FALSARELLA, 2009). Segundo o autor, essa é a grande razão por se utilizar os serviços de QoS, uma vez que uma rede IP comum como a Internet não diferencia os requisitos dos diversos e distintos pacotes com que lida. Além disso, segundo Matties e Moraes (2008), outra razão para utilizar o QoS seria otimizar o uso da banda, sem que haja a necessidade de aquisição de mais recursos de banda para a rede em um curto prazo.

   Falsarella (2009) afirma que os roteadores componentes de redes IP sem os serviços de QoS operam com base no mecanismo de melhor esforço (*best effort*), no qual o roteador tenta enviar os pacotes de dados aos seus respectivos destinos com base em todos os recursos que ele possui disponíveis naquele intervalo de tempo. Entretanto

esse padrão de operação não garante que o pacote efetivamente será entregue ao seu destino, ou que será entregue integralmente.

O autor ainda afirma que os roteadores atuam nas redes sem serviços de QoS com base no mecanismo de fila conhecido como FIFO (First in, First out), no qual os pacotes serão enviados na mesma ordem em que chegaram ao roteador. Dessa forma, o serviço de melhor esforço oferecido por redes IP comuns acaba não sendo compatível com o que grande parte do volume de dados requer.

Ao ser abordado a importância do QoS e revelar a falta de garantias existentes em uma rede de IP comum, será elencado os diferentes tipos de serviços QoS existentes atualmente segundo Matties e Moraes (2008):

- **IntServ**:

  Segundo Silva (2014), este modelo é um tipo de QoS baseado em fluxo. o IntServ é um modelo que opera com base em reservas de recursos feitas nos roteadores que operam ao longo de uma certa rota a ser utilizada. Sendo assim, como o QoS foi desenvolvido para redes IP, é necessário o auxílio de um protocolo para efetuar esta reserva de recursos junto aos roteadores. O protocolo em questão é o RSVP (Protocolo de Reserva de Recurso), que auxilia o IP na criação de um fluxo, ou seja, na reserva dos recursos de largura de banda e tempo de conexão. Portanto, o protocolo RSVP garante ao usuário que exista uma conexão com uma determinada largura de banda (bits a serem transmitidos) e um tempo estabelecido.

- **DiffServ**:

  Este modelo foi desenvolvido para corrigir os problemas e erros manifestados no IntServ de acordo com Silva (2014). É um modelo no qual o tráfego é tratado por sistemas intermediários, cujas prioridades são baseadas no campo ToS. Este campo é definido como um campo de 8 bits que é responsável pela indicação do tipo de serviço ao qual o pacote faz parte. Sendo assim, é possível criar uma classificação para os pacotes, e usando esta como base, é possível proceder com certas ações específicas para cada classificação. Segundo o autor a IETF está tentando modificar este campo ToS no IPV4 para DS, assim como no IPV6, onde corresponde ao Campo de Classe.

- **Multi-Layer Protocol Label Switching (MPLS)**:

  É um protocolo que segundo Matties e Moraes (2008) engloba todas as funcionalidades mencionadas anteriormente no IntServ e DiffServ, e um pré-roteamento

é feito com base no rotulamento de pacotes.

A seguir, é apresentado alguns componentes importantes para uma rede MPLS (Multi-Layer Protocol Label Switching) segundo Assis et al. (2002):

– **Label**:

Este atributo se trata de um identificador para cada um dos pacotes, corresponde a um campo componente do pacote de dados na sua íntegra. Todo pacote que entra em uma rede MPLS recebe um cabeçalho MPLS, do qual o campo Label faz parte. Este cabeçalho fica localizado entre os dados da camada 2 (camada de enlace) e os dados da camada 3 (camada de Rede). Além do campo Label, existem outros campos formadores do cabeçalho MPLS, como o EXP, que refere-se a prioridade do pacote de dados ou sua classe de serviço; o campo S que diz respeito ao enfileiramento de Labels caso o pacote em questão receba mais de uma Label; e por fim o campo TTL que possui papel semelhante ao desempenhado no datagrama da camada 3, ou seja, contar por quantos roteadores o pacote de dados passou em um máximo de 255 antes de ser descartado. Este conceito é apresentado na figura 6.

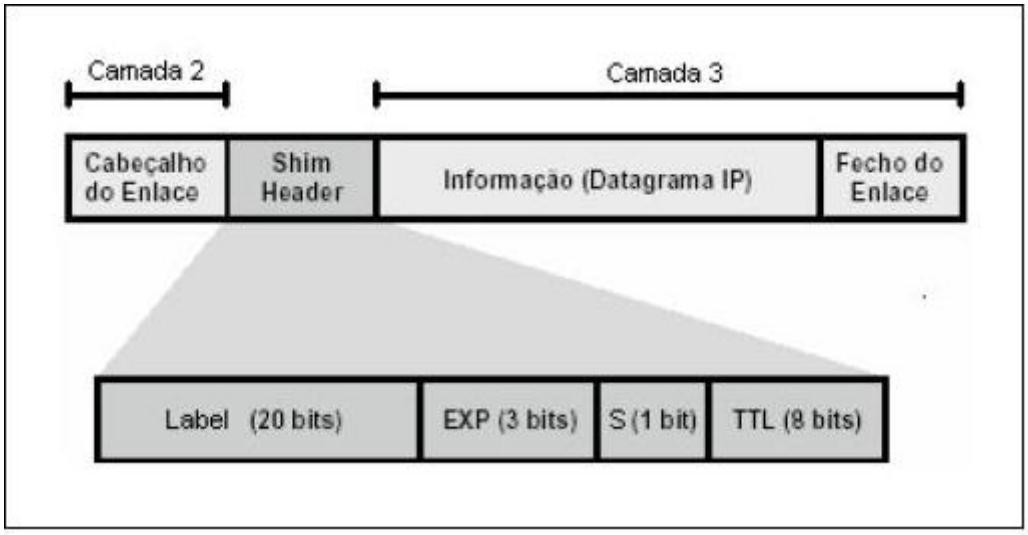

Figura 6: Cabeçalho MPLS - Shim Header
Fonte: (ASSIS et al., 2002)

– **Label Switch Path (LSP)**:

Ao entrar em uma rede MPLS o pacote de dados é adicionado a uma Classe de Equivalência, e uma rota é criada dentro desta rede para todos os integrantes desta Classe de Equivalência. Esta rota então recebe um Label próprio chamado Label Switch Path.

– **Label Distribution (LDP)**:

Este é um protocolo que permite que roteadores de comutação de rótulos descubram outros roteadores e atribuam Labels (rótulos) a estes novos roteadores recém descobertos. Este mecanismo permite a criação das Label Switch Path(LSPs).

– **Classe de Equivalência**:

Determina um caminho para um conjunto de pacotes. Todos os pacotes que compuserem uma mesma classe de equivalência necessariamente irão percorrer o mesmo caminho dentro da rede MPLS. As classes de equivalência são nomeadas com *Labels*, e cada classe de equivalência possui uma rota (LSP) associada a si. Sendo assim, existe uma ordem de ações até o ponto apresentado: primeiramente o pacote de dados recebe um Label que o identifica, em seguida este pacote é associado a uma classe de equivalência, que determina a rota que este pacote deve traçar dentro da rede MPLS, e por fim ele percorre a rota (LSP) determinada. A associação do pacote a uma classe de equivalência ocorre tão logo o pacote entre na rede MPLS, desta forma é possível atribuí-lo a um grupo que já possua uma rota na rede. O gerente de rede pode determinar alguns parâmetros que definem a classe de equivalência, como por exemplo: QoS, ID do protocolo IP, número da porta da fonte ou destino, entre outros.

– **Label Information Base (LIB)**:

Este atributo apresenta uma tabela de encaminhamento entre os Labels dos pacotes com as diversas interfaces dos roteadores. Quando uma LSP (rota) é criada, a relação do Label com a interface é armazenada no Label Information Base (LIB).

– **Label Switch Router (LSR)**:

São os roteadores que compõem a rede MPLS. Existem dois tipos de roteadores, os roteadores de borda e os que pertencem ao núcleo da rede. Os roteadores de borda são responsáveis por atribuir um Label ao pacote de dados, bem como uma classe de equivalência, além de atribuir uma LSP (rota) ao pacote em questão. Quando o roteador está localizado na saída da rede MPLS ele é responsável pela remoção do Label e deve entregar este pacote a uma outra rede que não seja MPLS. Os outros tipos de roteadores são os que integram o núcleo da rede, e possuem como funções o encaminhamento do pacote baseado no Label que apresenta. Cada vez que

um pacote alcança um roteador de núcleo ele recebe um novo Label e é encaminhado adiante na sua LSP com base neste novo Label que recebeu. Este procedimento é repetido a cada novo roteador de núcleo alcançado, até chegar em um roteador de saída.

2.3.1 QOS EM REDES LOCAIS

Já no cenário de QoS aplicado em redes locais (LANs), conforme descrito por Cisco (2010), em alguns equipamentos gerenciáveis de camada 2 é possível a implementação de Qualidade de Serviço (QoS) para priorizar determinados fluxos de informações. Assim, é possível indicar em um switch Cisco, modelo 2960, que a porta a ser utilizada para o tráfego de voz deverá apresentar uma prioridade superior a prioridade registrada pelo tráfego de dados comuns. Por padrão, as portas estão configuradas para trabalhar com o método de "melhor esforço", ou seja, as máquinas tentarão utilizar o máximo disponível de taxa de transmissão.

Ainda levando em consideração o que é descrito por Cisco (2010), em rede camada 2 estruturada, o administrador deve indicar níveis de QoS para separar determinados tráfegos. Para isso, o administrador configura manualmente cada porta do switch ou VLan por meio uma interface de linhas de comando, dessa forma atribuindo prioridades distintas sobre os pacotes de dados em tráfego para cada porta componente do switch em questão.

Figura 7: Um switch Cisco 2960, com 48 portas. Um modelo de switch gerenciável que permite a aplicação de QoS

Fonte: (CISCO, 2010)

Em relação às prioridades atribuídas as diversas portas do switch em redes locais, segundo o Cisco (2010), existe uma relação de agrupamento entre os diversos tipos de dados existentes. Cada tipo de dado ocupa uma determinada categoria dentro desse agrupamento, e com base nisso, o administrador de rede consegue indicar a qual categoria a prioridade no tráfego de dados é mais importante para sua rede. O agrupamento de

dados segue a ordem indicada na tabela 3.

Tipo de Tráfego	Nível de Prioridade	Aplicações
Network Control	6 e 7	BGP, EIGRP, OSPF
VoIP	5	Cisco IP Phones, Jabber
Multimedia	4	CCTV, SCCP, SIP
Critical Data	3	Https, Email, CRM
Bulk-Data	2	FTP, Backup, IPTV
Scavenger	1	YouTube, Jogos, P2P
Class-Default	0	Tráfego IPV6, broadcasts e tráfego sem classificação

Tabela 3: Relação entre as categorias de tráfego de dados, seus exemplos e prioridades.

Fonte: Autoria Própria

Com isso, é possível ao administrador de rede, com base no que é descrito por Cisco (2010), separar grupos de portas do switch e atribuir a este grupo uma prioridade de tráfego em relação a voIP por exemplo, enquanto outro grupo de portas do mesmo switch trata como prioridade máxima os dados de video (multimídia).

2.4 VOIP

Segundo Tanenbaum (2003), em torno do ano 2000, muitas empresas destinaram suas atenções para o tráfego de voz sobre suas redes de dados. Este fato foi decorrente, segundo o autor, da percepção de que não seria necessário praticamente nenhuma modificação na rede atual, apenas suporte a uma largura de banda ligeiramente superior. Com isso, as operadoras de redes de dados vislumbraram uma boa oportunidade de crescerem comercialmente e financeiramente.

Para que o VoIP seja um substituto eficiente para a telefonia PSTN (Public Switched Telephone Network), deve atender a certos requisitos que mantenham o novo serviço nos mesmos padrões de funcionamento que o atual serviço de telefonia PSTN. Sendo assim, o VoIP tem requisitos e características particulares para promover e definir seu funcionamento, como o fato de ser uma aplicação de tempo real, e com isso ser extremamente sensível a atrasos de pacotes. Com isso, a ideia é que, em conjunto, seja implementado um sistema que garanta QoS (Quality of Service). Dessa forma, o VoIP consegue garantir a entrega dos pacotes de voz entre dois dispositivos e a funcionalidade plena desta aplicação, apenas se os pacotes de voz tiverem prioridade sobre os pacotes de dados comuns, caracterizando o conceito de QoS para este cenário. Um dos requisitos

necessários para que o VoIP funcione de modo eficiente é o acesso a uma largura de banda suficiente. Cabe ao QoS fornecer um serviço de rede compatível com tais necessidades, e fornecer os requisitos necessários para o desenvolvimento das funcionalidades do VoIP (CISCO, 2008).

O VoIP é normalmente implementado em um cenário que se utiliza de telefones comuns, e necessita de roteadores que possuam suporte a voz, convertendo a voz analógica em pacotes IP Uma vez que os pacotes IP são gerados, eles são encaminhados pela rede de dados para seus destinos adequados. Essa é uma solução que apresenta um menor custo financeiro para as empresas, no entanto o nível de qualidade final da comunicação não é tão elevado quanto em uma solução de telefonia IP.

A telefonia IP por sua vez, é uma implementação que não necessita de um roteador com suporte a voz, uma vez que o próprio aparelho de telefone faz a conversão da voz analógica para os pacotes IP correspondentes. Nesse cenário, o custo financeiro acaba sendo mais elevado para a empresa que opta por essa solução, no entanto a qualidade final da comunicação estabelecida é superior à apresentada pela solução de VoIP.[3]

2.5 SEGURANÇA DA INFORMAÇÃO

Segundo Cisco (2016), é importante definir-se uma segurança voltada para as portas do switch antes que este seja disponibilizado em uma topologia final de rede para uso. Este procedimento gera uma camada extra de segurança no processo de comutação e funcionamento da rede de modo geral, de acordo com Balchunas (2014b).

Ainda de acordo com Cisco (2016), é possível utilizar-se do recurso de segurança de portas do switch como um mecanismo de filtragem, ou seja, endereços MAC permitidos conseguem se conectar à porta do switch e ter acesso à rede, enquanto dispositivos com endereços MAC não autorizados não conseguem este acesso à rede.

É possível realizar a configuração da segurança de portas, em relação ao aprendizado dos endereços permitidos nas portas, de algumas maneiras distintas, como por exemplo:

- **Endereços MAC seguros estáticos:** seguros estáticos: nesta modalidade de configuração da segurança de portas de um switch, o endereço MAC permitido é configurado e especificado explicitamente por meio do comando: *switchport port-security*

[3]Material consultado de Cisco (2016), disponível para acesso mediante login em: https://goo.gl/Fysq2m

mac address "mac-address". Neste cenário, o endereço configurado manualmente é salvo na tabela de endereços da porta do switch em questão, além de ser salvo nas configurações em execução do switch, em sua memória RAM.

- **Endereços MAC seguros dinâmicos:** esta configuração faz com que não haja necessidade de explicitar o endereço que é permitido, tornando o processo automatizado e dinâmico. No entanto, a lista de endereços permitidos nas portas do switch é armazenada apenas na tabela de endereços referente à cada porta do switch, sem que qualquer uma destas configurações seja vinculada nas configurações em execução da memória RAM.

- **Endereços MAC com segurança sticky:** o diferencial desta modalidade em relação à modalidade elencada anteriormente é que os endereços são aprendidos dinamicamente, salvos na tabela de endereços de cada porta do switch, e alocados na configuração em execução da memória RAM do switch em questão. Para ativar esta configuração de segurança de porta em alguma interface do switch, deve-se utilizar o seguinte comando: *switchport port-security mac-address sticky*. Segundo Cisco (2016), esta modalidade de proteção de portas do switch apresenta tantas vantagens quanto a modalidade de proteção estática. Ainda segundo Cisco (2010), a vantagem do modo de segurança sticky em relação ao modo de segurança de portas dinâmico consiste no fato de que ao utilizarmos o comando write memory ou copy running-config startup-config, o switch reiniciára ainda com as configurações de proteção de porta ativas. Em contrapartida, na modalidade de proteção de porta dinâmica, esse cenário não ocorre, uma vez que não há relação com o arquivo de configuração em execução.

Outro ponto válido de destacar, seria o cenário de uma violação de segurança de porta (CISCO, 2016). Uma situação que poderia ser verificado este cenário de violação seria no caso de uma porta de switch ter sido configurada para receber um número máximo de conexões com endereços de dispositivos. No entanto, quando um endereço que não está presente na relação de endereços permitidos, contidos na tabela de endereços da porta do switch em questão, há uma situação de violação da segurança de portas do switch. Existem 3 configurações que uma porta de switch pode contemplar em decorrência desta situação de violação (BALCHUNAS, 2014b). São elas:

- **Protect (Protegido):** Refere-se ao cenário em que uma violação ocorre em uma dada porta de switch, e esta porta comporta-se de acordo com o que define este

modo de violação. Esta modo de violação refere-se ao comportamento de não aceitar pacotes provenientes de endereços MAC que não compõem a tabela de endereços MAC da interface em questão. Estes quadros são descartados, porém nenhuma notificação ou ação mais intensa é tomada nesta modalidade de violação de segurança de porta.

- **Restrict (Restrito):** Nesta modalidade de violação da segurança de portas, quando um pacote proveniente de um endereço MAC desconhecido chega à uma porta do switch que se utilize de tal recurso de segurança, o pacote inicialmente é descartado. A diferença em relação à modalidade de segurança de porta protect evidencia-se no fato de que na modalidade de segurança restrict há o envio de uma notificação alertando sobre o processo de violação da porta.

- **Shutdown (Desligado):** Esta modalidade de violação de segurança corresponde à ação padrão (default) que vem configurada nos switches. Neste caso, quando um pacote chega à uma interface de switch, ocasionando uma situação de violação de segurança de portas, o switch entra em um estado chamado errdisable. Uma vez neste estado, a porta do switch bloqueia todo e qualquer tipo de tráfego destinado a ela, mesmo que seja proveniente de um endereço MAC presente na sua lista de endereços permitidos. Para que a porta do switch volte a encaminhar tráfego é necessário tirá-la do modo errdisable. Para proceder à recuperação utiliza-se o comando shutdown seguindo pelo comando no shutdown no modo de configuração de interface da CLI do switch.

Outro recurso importante é a definição de uma quantidade máxima de endereços MAC seguros aceitos por uma porta do switch. Por padrão, o switch vem com este número definido com o valor de 1, no entanto é possível ao administrador de rede alterar este valor conforme desejado.

É apresentado, na figura 8, o ambiente de linhas de comando do *switch* CLI (*Command Line Interface*) com os comandos apresentados e explicados nesta seção. Através desta figura pode-se visualizar que a segurança de porta foi pensada em três etapas: foi definido um número máximo de endereços MAC para a interface fastethernet 0/5; foi definido que o aprendizado referente aos endereços MAC permitidos para esta interface é sticky, ou seja, serão aprendidos dinamicamente, armazenados na tabela de endereços na interface e no arquivo de configuração em execução; além disso, o modo de violação da porta fastethernet 0/5 foi definido como shutdown, ou seja, a porta irá ser desativada

quando uma situação de violação for apresentada, não irá encaminhar tráfego proveniente de nenhum dispositivo.

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation shutdown
```

Figura 8: Relação dos comandos de configuração da segurança de porta.
Fonte: Autoria Própria.

2.6 SPANNING TREE PROTOCOL

Segundo Diógenes (2004), o protocolo Spanning-Tree encarrega-se de remover os loops lógicos na rede, porém mantém a redundância física da rede, ou seja, é interessante a rede possuir enlaces redundantes para garantir a confiabilidade da rede, porém o STP atua removendo essas redundâncias lógicas. O autor ainda afirma que o protocolo Spanning-Tree possui duas grandes funcionalidades:

- Detectar e eliminar loops lógicos presentes na rede em questão;
- Detectar quando um enlace utilizado sofre algum dano ou é desativado, e utilizar-se de outros caminhos para alcançar o destino. Ou seja, quando há um loop físico, um dos caminhos que leva ao destino é desativado pelo protocolo Spanning-Tree. Quando o link utilizado sofre uma desativação, o outro link que estava desativado antes é ativado para manter a rede funcional.

De acordo com Balchunas (2014a), uma rede sem a configuração do protocolo Spanning-Tree apresentaria um problema conhecido como tempestade de broadcast (Broadcast Storm). A seguir é apresentada a figura 9 ilustrando uma topologia com redundância de enlaces e sem o uso do protocolo STP em questão:

Na figura 9, conforme afirma Balchunas (2014a), há uma redundância de enlaces físicos na topologia. Isso faz com que em um cenário em que o HostA emita uma mensagem de broadcast, esta mensagem será encaminhada para o switchD, e o switchD por sua vez encaminhará esta mensagem por todas as suas portas, ou seja, para o switchE e switchB. O switchB encaminhará a mensagem de broadcast para o switchA, e assim por diante, de forma que esse ciclo só será encerrado se os switches forem desligados manualmente, ou se algum enlace físico for desativado. Com isso, o autor afirma que o protocolo Spanning-Tree foi desenvolvido justamente com o objetivo de resolver este tipo de situação descrita por meio da figura anterior.

Balchunas (2014a) afirma que para que o protocolo STP esteja plenamente estabelecido e funcional na rede, algumas etapas devem ser cumpridas:

1. Um switch raiz deve ser definido;
2. As portas raízes devem ser identificadas;
3. As portas designadas devem ser identificadas;

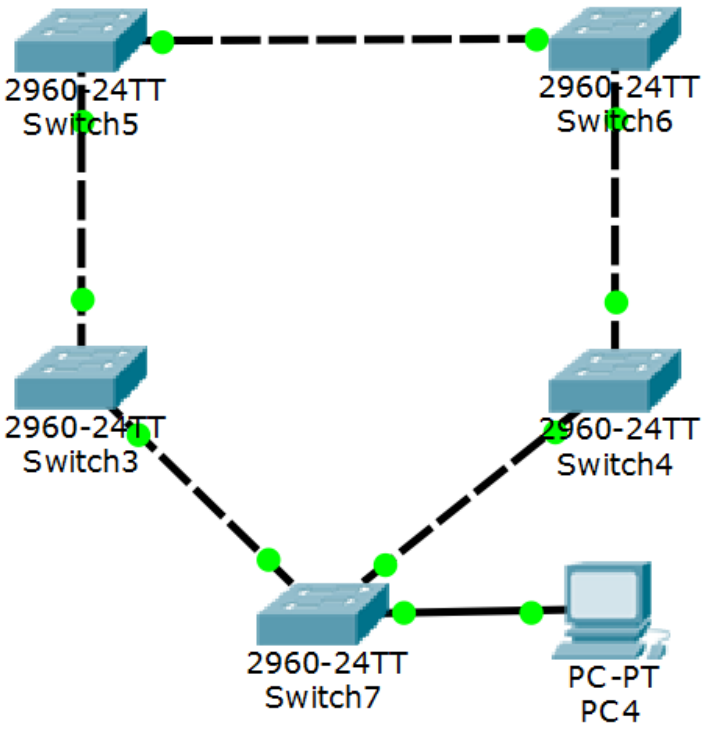

Figura 9: Representação da topologia sem uso do protocolo Spanning-Tree.
Fonte: Autoria Própria.

4. Algumas portas são colocadas em estado bloqueado para eliminar loops na rede.

Diógenes (2004) afirma que o processo de eleição do switch raiz é relativamente simples, cada switch possui um ID próprio, o switch com menor ID é eleito o switch raiz. Quando há um empate entre os IDs dos switches, o switch raiz é determinado com base no menor endereço MAC destes switches componentes da topologia. Segundo Balchunas (2014a), o ID do switch (conhecido também como Bridge ID) possui um tamanho de 64 bits, sendo 16 bits referentes à prioridade do switch, e 48 bits referentes ao endereço MAC deste switch. O autor afirma que a prioridade padrão é referente ao valor de 32.768. Será eleito o switch raiz o switch cujo valor de prioridade for menor. Em caso de empate nesse valor, será levado em conta o menor endereço MAC como critério de desempate no processo de eleição do switch raiz.

Segundo afirma Diógenes (2004), o processo de eleição do switch raiz é feito com base na troca de pacotes de dados chamados Bridge Protocol Data Unit (BPDU). A ideia desta troca de pacotes é fornecer informação do Bridge ID de cada switch aos seus vizinhos. Isso porque inicialmente, cada switch tenta se tornar o switch raiz da topologia. O switch aceita que outro switch é o raiz quando recebe um pacote BPDU deste switch vizinho contendo o Bridge ID deste, e verificando que este Bridge ID é menor que o seu próprio Bridge ID, condição necessária para eleger o switch raiz.

2.7 ETHERCHANNEL

Em uma rede comum, usuários se conectam a switches que então propagam as requisições do usuário até o ponto em que o roteamento ocorre. Neste mesmo cenário, é comum que as conexões entre os próprios switches se dêem por meio de um único enlace. Um problema comum que ocorre neste cenário é o gargalo (*Bottleneck*) de rede, onde o tráfego proveniente dos usuários é demasiadamente intenso para a largura de banda disponibilizada pelos links de conexão com os outros switches. Uma representação visual de um gargalo é apresentado na figura 10.

Uma boa analogia, conforme descrita por Deguchi e Santos (2012) é imaginar uma rodovia com 5 pistas subitamente sendo convertida em uma rodovia de apenas 2 pistas, onde o tráfego terá então de gastar mais tempo "parado"no gargalo para então prosseguir para a rodovia de menor capacidade e continuar sua jornada. Um exemplo de gargalo em uma topologia de rede é apresentado na figura 11.

A tecnologia etherchannel surgiu para resolver o problema descrito previamente

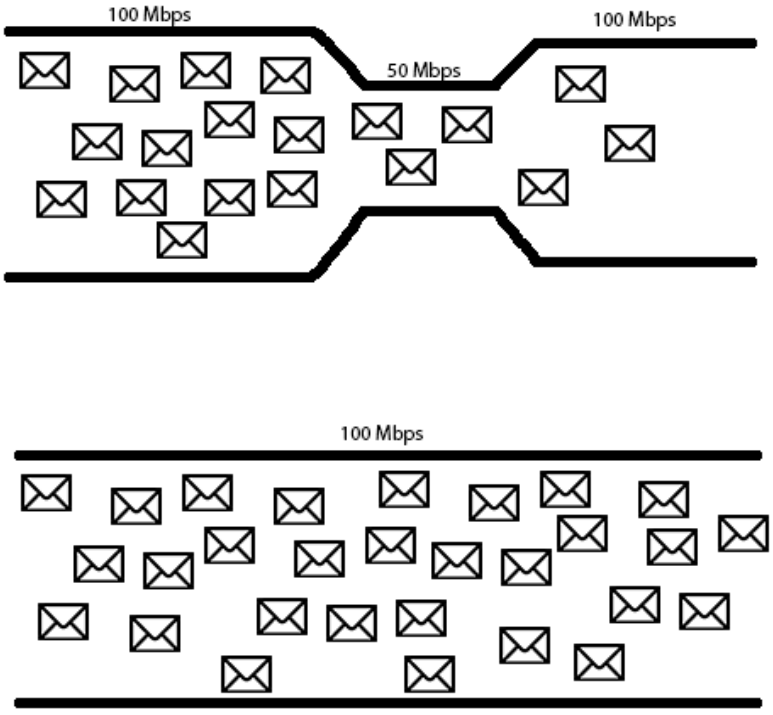

Figura 10: Representação visual de um gargalo em uma rede.
Fonte: Autoria Própria.

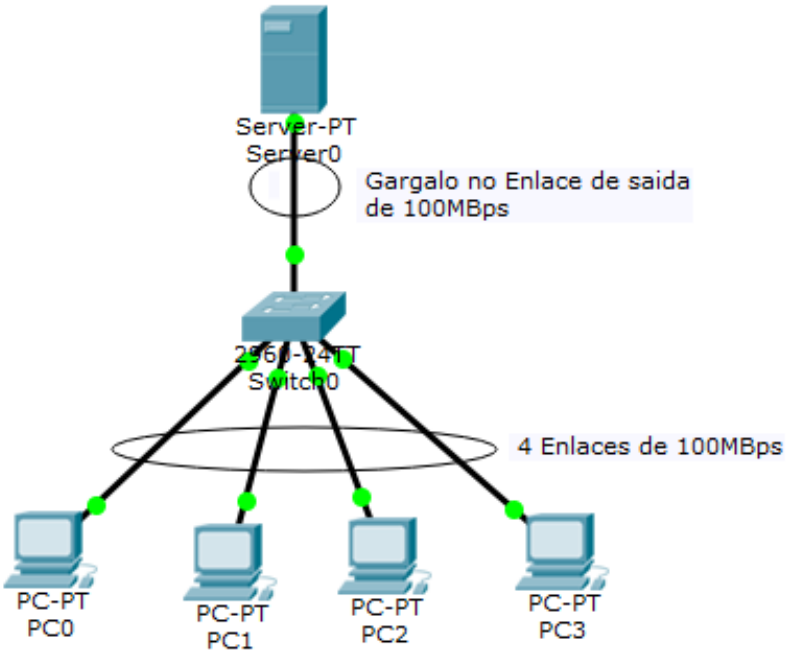

Figura 11: Representação de topologia com um possível gargalo.
Fonte: Autoria Própria.

sem a necessidade da troca de equipamentos, devido ao alto custo e trabalho envolvido em substituir todos os equipamentos de rede. A solução consiste em agregar duas ou mais portas de um switch de maneira que um novo link lógico seja criado, conforme representado na figura 12. O link lógico criado permite que o tráfego seja paralelizado nas portas presentes no agrupamento, permitindo assim que o link opere com o somatório da velocidade de seus agregados (CISCO, 2014).

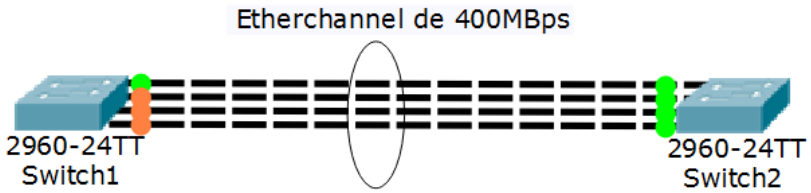

Figura 12: Criação de um Etherchannel entre dois switches.
Fonte: Autoria Própria.

Conforme descrito por Cisco (2014) existem dois protocolos para a negociação e um protocolo para configuração manual:

- **Port Aggregation Protocol (PAgP)**: Proprietário da Cisco;

- **Link Aggregation Control Protocol (LACP)**: Padrão aberto definido pelo IEEE 802.3;
- **Persistência Estática ("On mode")**: Nenhum protocolo de negociação será utilizado, toda a configuração será manual.

A principal diferença entre os modos de negociação, salvo o fator do LACP ser um padrão aberto, é a quantidade máxima de portas que podem ser agrupadas em um único etherchannel: O limite do PAgP é de 8 portas enquanto que o limite do LACP é de 16 portas, onde 8 são portas ativas e 8 são portas em estado de espera (DEGUCHI; SANTOS, 2012).

Outra vantagem da utilização de etherchannel é a redundância presente em caso de falha de uma ou mais portas do agrupamento e o balanceamento automático do tráfego entre as portas presentes no agrupamento. A tecnologia consegue, em questão de milisegundos, automaticamente redirecionar todo o tráfego da porta que caiu para as outras portas do enlaces, apresentando o mínimo impacto para a experiência de uso do usuário (FARRINGTON, 2014).

Contudo, conforme apresentado por Farrington (2014) a tecnologia Etherchannel apresenta alguns defeitos, entre eles:

- Requer configuração via *software*;
- Uma má configuração pode levar a loops e a tempestades de broadcast;
- Existência de overhead devido ao balanceamento de carga automático.

Um ponto levantado por Farrington (2014) e notável é que a tecnologia Etherchannel tenta resolver um problema de hardware através de uma solução de *software*, o que, segundo Farrington (2014), não é uma boa prática.

3 METODOLOGIA

Nesta seção será exposta a metodologia adotada para a execução deste trabalho, serão apresentadas as diferentes fases do projeto e as abordagens a serem realizadas para coletar os dados necessários para a análise.

O ambiente de desenvolvimento do projeto foi o Laboratório de Redes de Computadores (LabRedes) do Departamento Acadêmico de Informática (DAINF) da Universidade Tecnológica Federal do Paraná (UTFPR) – Curitiba, os equipamentos e materiais necessários serão detalhados na seção "Recursos de Hardware e Software".

A primeira fase do projeto envolve o planejamento da infraestrutura da rede, a divisão dos endereços IPV4, planejamento das VLANs, das regras de QoS e das políticas de segurança necessárias para o pleno funcionamento.

A segunda fase do projeto consiste na implementação da primeira fase, além de testes de segurança e de desempenho da rede.

3.1 PLANEJAMENTO

Para o planejamento dos endereços de IP a serem distribuídos será levado em conta a possibilidade de escalabilidade da rede, seguindo as boas práticas e métodos propostos por Cisco (2010).

As VLans (Redes locais virtualizadas) foram planejadas de acordo com a necessidade de cada sub rede e a necessidade de acesso aos recursos necessários para a execução de suas tarefas, cada VLans também terá sua própria regra de QoS e políticas de seguranças próprias.

Políticas de segurança foram definidas também para o acesso e manutenção dos equipamentos de infraestrutura da rede (*Switches* e Roteadores) e para os pontos de acesso (Desktops, Notebooks, Telefones VoIP).

O planejamento também contemplou a implementação da política "*Bring Your Own Device*"(BYOD), uma tendência crescente nas empresas.

3.2 IMPLEMENTAÇÃO

Durante a fase de implementação as políticas e planejamentos efetuados foram efetivados nos equipamentos presentes no laboratório. Devido à limitação de espaço físico e material a implementação e os testes foram realizados em um ambiente com abrangência reduzida.

Após a implementação, foram realizados testes para avaliar a qualidade das políticas e regras implementadas. Os testes serão detalhados nas seções subsequentes.

3.2.1 TESTES DE DISPONIBILIDADE

Os testes de disponibilidade possuem como finalidade avaliar se a divisão em camadas hierárquicas foi efetiva para garantir a disponibilidade de rede. Podem ser comparados a situações reais e cotidianas, como uma falha de hardware ou uma falha humana acarretando em indisponibilidade de uma seção da rede.

Para a realização desses testes, foram desligados seletivamente alguns elementos da rede, observando via um computador se o acesso a outros recursos da rede, internos ou externos, foi comprometido ou não.

3.2.2 TESTES DE SEGURANÇA

Os testes de segurança ou pentest (do inglês, penetration test) possuem como finalidade detectar possíveis brechas de segurança presentes na rede ou em pontos de acesso da rede. Os testes de segurança podem replicar uma situação real de invasão ou apenas buscar pelas brechas com a ciência dos usuários e administradores do sistema.

Para a realização dos testes foram utilizados *softwares* e *scripts* disponíveis na distribuição Kali do Sistema Operacional Linux, os *softwares* e *scripts* a serem utilizados estão listados na seção "Requisitos de Software", o tipo de teste a ser realizado será do tipo *White Box*, uma vez que não temos usuários para simular o uso comum e, por sermos os administradores da rede implementada, teremos conhecimento dos testes.

3.2.3 AVALIAÇÃO DA DESEMPENHO DA REDE

Por fim, após a obtenção dos resultados dos testes realizados, foi realizada uma avaliação total da rede, vendo se a rede implementada obteve o desempenho esperado frente aos esforços e possíveis custos para a realização de uma rede desse tipo em uma escala real.

4 IMPLEMENTAÇÃO

Nesta seção, são apresentados diversos cenários da área de redes de computadores, com o objetivo de apresentar individualmente algum recurso que será utilizado na topologia final deste trabalho. Também são elencados os requisitos de hardware e software utilizados para a implementação destes cenários.

Ao todo, foram desenvolvidos: 1 cenário base, que conterá uma topologia de rede simples, sem nenhuma implementação visando possíveis benefícios de performance; 4 cenários em que cada cenário apresentará uma determinada característica abordada no trabalho e contemplada na topologia final, são estas: Etherchannel, VoIP (QoS), Protocolo Spanning - Tree, e Segurança em redes de computadores. A ideia é que cada cenário apresente apenas uma dessas características, de forma a tornar mais prático e direto o entendimento do que tal recurso agrega para a rede de computadores, além da sua importância e funções de modo geral. Por fim, é apresentado o cenário final deste trabalho, o qual contém uma topologia em estado da arte, contendo todos os cenários até então apresentado e todas as características de melhoria de implementação e desempenho de redes de computadores apresentadas até aqui.

O trabalho foi distribuído desta forma em função de haver uma clara evolução nas configurações eleitas ao longo dos cenários. Com isso, foi apresentada desde a topologia mais simples no cenário base, até a topologia mais complexa no cenário final, passando por cada um dos cenários e suas devidas características implementadas, mostrando individualmente a importância de cada um. Ao final, a ideia é que todos os recursos utilizados na configuração e implementação da rede no cenário final não sejam tão complexos, e sim devidamente conhecidos por meio dos cenários anteriores.

4.1 RECURSOS DE SOFTWARE E HARDWARE

Nessa seção serão abordados os recursos necessários para a realização deste projeto. Na seção 4.1.1 serão descritos os recursos de *hardware* necessários e na seção 4.1.2

serão descritos os recursos de *softwares* necessários. A seção 4.1.3 apresenta a viabilidade de realização do projeto.

4.1.1 RECURSOS DE HARDWARE

Para a implementação da hierarquia proposta foram necessários switches gerenciáveis, roteadores e telefones VoIP. Para a realização dos testes foram necessárias máquinas nas seguintes configurações: Processadores 32 bits @ 2.0 GHz, 2 GB ou mais de *RAM* com sistemas Linux, preferencialmente a distribuição Kali Linux.

As versões dos switches a serem utilizados são:

- Cisco Catalyst 2960;
- Cisco 2948 L3;

A versão do roteador utilizada será:

- Cisco 1841 Integrated Services Router

Para a implementação do cenário *VoIP* apresentado na seção 4.4 foram utilizados dois telefones *VoIP* da marca Cisco.

4.1.2 RECURSOS DE SOFTWARE

Para a implementação do servidor VoIP foi necessário acesso ao sistema operacional dos equipamentos da Cisco descritos na seção 4.1, para a realização dos testes serão utilizadas as ferramentas open-source disponíveis na distribuição "Kali Linux".

As ferramentas disponíveis na distribuição que foram utilizadas são:

- **Macof**: *Script* utilizado para alterar o *Mac Address* de uma máquina de maneira rápida e aleatória.

4.1.3 VIABILIDADE

Os recursos de *software* que não são open-source estão disponíveis nos próprios hardwares da Cisco. Os recursos de hardware utilizados serão do laboratório de redes, não sendo necessária a aquisição de novas máquinas. Portanto o projeto é economicamente viável.

4.2 CENÁRIO BASE

4.2.1 DESCRIÇÃO DO CENÁRIO

A seguir será ilustrada uma topologia que servirá de base para os cenários que serão apresentados em sequência. Partindo de uma topologia simples, sem nenhuma implementação visando ganho em segurança e/ou performance desta rede em questão. Ao passarmos pelos cenários seguintes, buscamos manter a mesma rede de modo geral, apenas incorporando as novas implementações contemplando o tópico abordado em cada cenário.

Cada cenário contemplará uma situação, um problema e uma solução específicos, referenciando algum tópico previamente abordado no referencial teórico deste trabalho. O cenário base contempla a estrutura mais simples de uma rede, uma topologia genérica com base nos padrões definidos pela maioria dos equipamentos de rede e sem ênfase em propor a melhor solução ou a máxima eficiência e efetividade em se tratando de redes locais.

É importante salientar que todos os cenários foram devidamente planejados e implementados de forma prática. Isso é, não foram desenvolvidos utilizando-se de qualquer *software* ou simulador de redes. Os cenários foram implementados no laboratório de redes da Universidade Tecnológica Federal do Paraná de Curitiba, campus Sede, sob a supervisão e orientação do Professor Fabiano Scriptore de Carvalho. Com isso, fica evidente o contato direto com os equipamentos e configurações relativos ao desenvolvimento deste trabalho, sem que qualquer contato ou configuração remota tenha sido utilizada ou pretendida.

4.2.2 ENDEREÇAMENTO E DISPOSITIVOS PRESENTES NA TOPOLOGIA:

Rede utilizada: 192.168.0.0

Máscara de Sub-rede: 255.255.255.0 ou /24

A relação de equipamentos utilizados na implementação deste cenário pode ser encontrada na tabela 4.

Quantidade	Dispositivo	Endereços IP
1	Roteador	192.168.0.1
3	Switch Gerenciável	Não aplicável
3	Computador	192.168.0.2 192.168.0.3 192.168.0.4

Tabela 4: Equipamentos utilizados no cenário base.
Fonte: Autoria própria

4.2.3 REPRESENTAÇÃO DA TOPOLOGIA CORRESPONDENTE AO CENÁRIO:

A representação da topologia correspondente ao cenário base pode ser observada na figura 13.

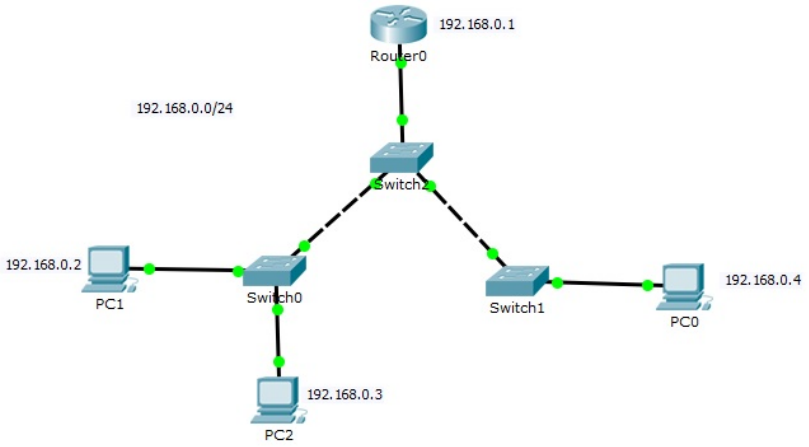

Figura 13: Representação da topologia do cenário base.
Fonte: Autoria própria

4.2.4 IMPLEMENTAÇÃO

Nas figuras 14, 15 e 16 pode-se verificar a etapa de atribuição de endereços IP aos dispositivos finais da rede correspondente ao cenário base. Com base na topologia correspondente ao cenário base apresentada anteriormente na figura A, os dispositivos finais PC0, PC1 e PC2 são apresentados de modo prático por meio das imagens 14, 15 e 16, onde os devidos endereços IP são atribuídos. Neste caso o PC1 recebe o endereço 192.168.0.2, como indica a figura 14; o PC2 recebe o endereço 192.168.0.3, como indica a figura 15, e o PC0 recebe o endereço 192.168.0.4, como indica a figura 16.

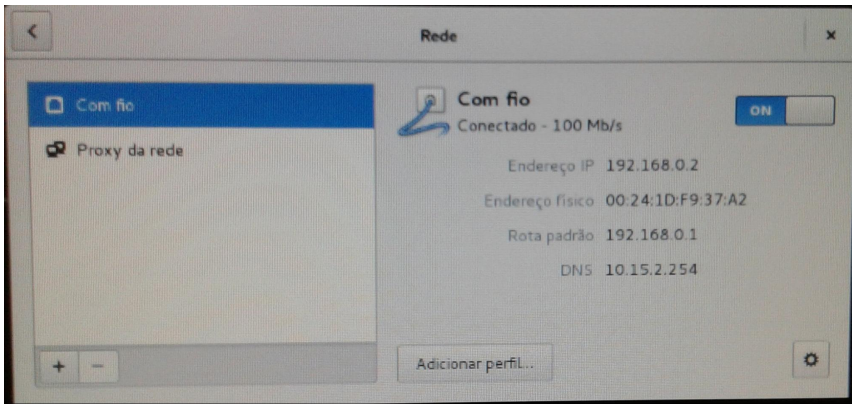

Figura 14: Configuração de endereço IP no Pc 1.

Fonte: Autoria própria

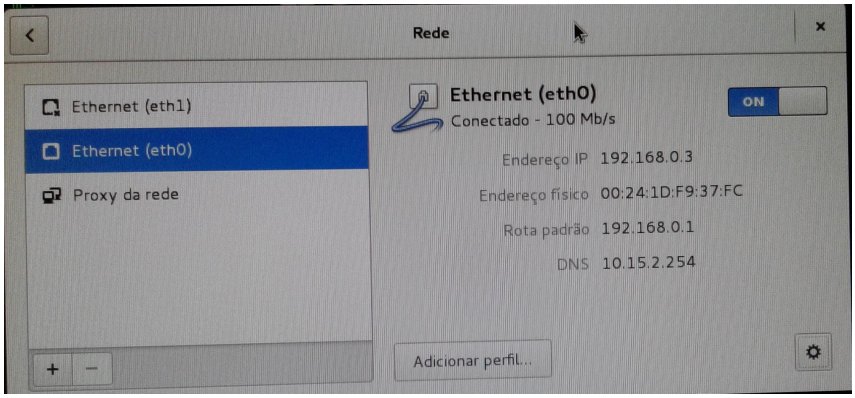

Figura 15: Configuração de endereço IP no Pc 2.

Fonte: Autoria própria

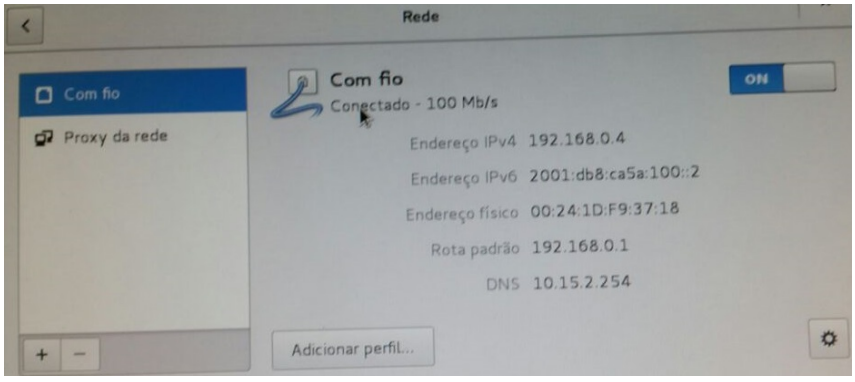

Figura 16: Configuração de endereço IP no Pc 3.

Fonte: Autoria própria

Uma vez que os devidos endereços são atribuídos aos dispositivos finais, e o endereço da porta do roteador que corresponde ao gateway padrão da rede é devidamente configurado, a rede encontra-se pronta para a realização de testes. No caso da rede em questão, o gateway padrão encontra-se na porta fastEthernet 0/0, e possui o seguinte endereço IP: 192.168.0.1.

Neste teste, como trata-se de uma rede local, o gateway padrão não é utilizado, uma vez que não esta se comunicando com uma rede externa. No entanto, o teste realizado é justamente acerca da comunicação entre os dispositivos finais e seu gateway padrão, no caso, o endereço 192.168.0.1, configurado na interface fastEthernet 0/0 do roteador em questão. Para a realização do teste, utilizamos o comando PING para verificar se há uma comunicação entre o dispositivo final e seu gateway padrão.

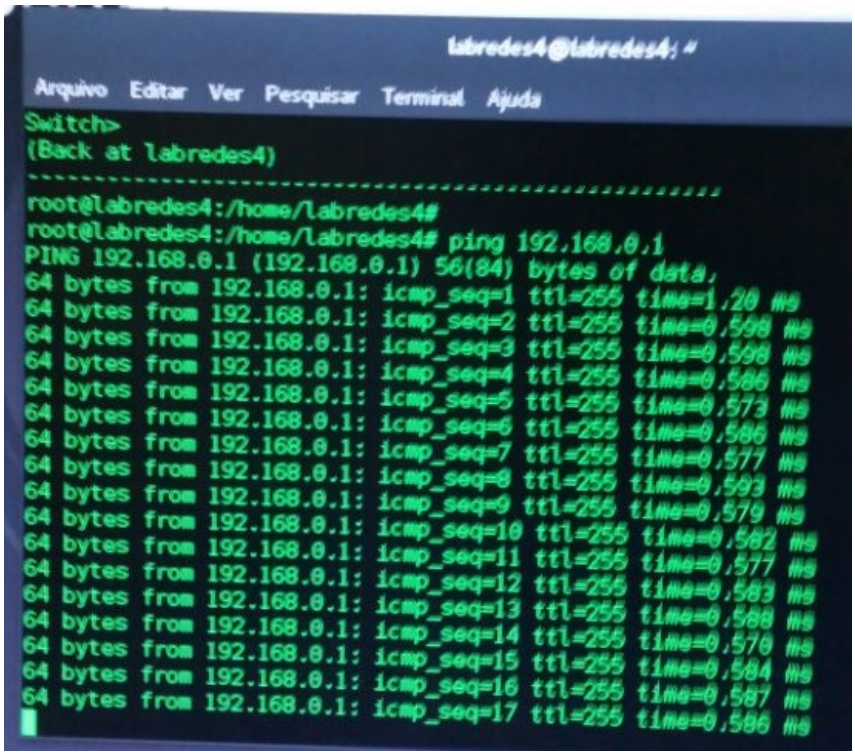

Figura 17: Resultado do comando PING para o seu gateway padrão.
Fonte: Autoria própria

Neste caso, a figura 17 revela que o comando PING foi bem sucedido, uma vez que mostra o tempo de resposta que o echo reply emitido pelo roteador em seu gateway padrão levou para alcançar o dispositivo final emissor do echo request. Caso não houvesse comunicação entre ambos, o problema seria revelado no comando PING, ou por meio do comando TRACEROUTE.

Os comandos utilizados para a implementação desta topologia podem ser encontrados no apêndice A.

4.3 CENÁRIO ETHERCHANNEL

4.3.1 DESCRIÇÃO DO CENÁRIO

Um dos problemas comumente encontrados em redes é a sobrecarga de enlaces, onde o fluxo de dados permitido pelo enlace é menor do que o necessário para a carga da rede. Por exemplo: em uma rede interna FastEthernet (100mbps) pode-se encontrar gargalos em que um enlace necessita de mais potencial de fluxo do que o ofertado pela tecnologia presente em seus conectores ou, até mesmo, cabos.

Uma das possíveis soluções para o problema de gargalos em redes internas, além de distribuição de carga, é a tecnologia de Etherchannel. Essa tecnologia permite que dois enlaces físicos sejam unidos em um grupo de enlaces, de maneira que esse grupo de enlaces opera com a capacidade somada dos enlaces físicos presentes no grupo atribuído ao Etherchannel.

Neste cenário foi realizada a implementação de um Etherchannel utilizando dois enlaces FastEthernet, totalizando um enlaces de 200 mbps. Para a realização do teste, foi utilizado um computador conectado a um *switch*, e que não possui conexão direta com o roteador, e um simples envio de pacotes, para testar se o etherchannel está funcionando como desejado e permitindo a passagem do tráfego. Foi escolhida uma opção mais simples de teste devido a limitações de hardware presentes no nosso laboratório: Nosso link externo está limitado a 100mbps e nossos equipamentos internos possuem apenas interfaces FastEthernet, tornando impossível realizar um teste de velocidade com valor superior a 100mbps.

4.3.2 ENDEREÇAMENTO E DISPOSITIVOS PRESENTES NA TOPOLOGIA:

Rede utilizada: 192.168.0.0 (Vlan 5) e 192.168.1.0 (Vlan 4)

Máscara de sub-rede: 255.255.255.0 ou /24

A relação de equipamentos utilizados na implementação deste cenário pode ser encontrada na tabela 5.

Quantidade	Dispositivo	Endereços IP
1	Roteador	F0/1.4: 192.168.1.1 F0/1.5: 192.168.0.1
3	Switch Gerenciável	Não aplicável
3	Computador	192.168.0.11 (Vlan 5) 192.168.1.51 (Vlan 4)

Tabela 5: Equipamentos utilizados no cenário Etherchannel.
Fonte: Autoria própria.

4.3.3 REPRESENTAÇÃO DA TOPOLOGIA CORRESPONDENTE AO CENÁRIO:

A representação da topologia correspondente a este cenário pode ser observada na figura 18.

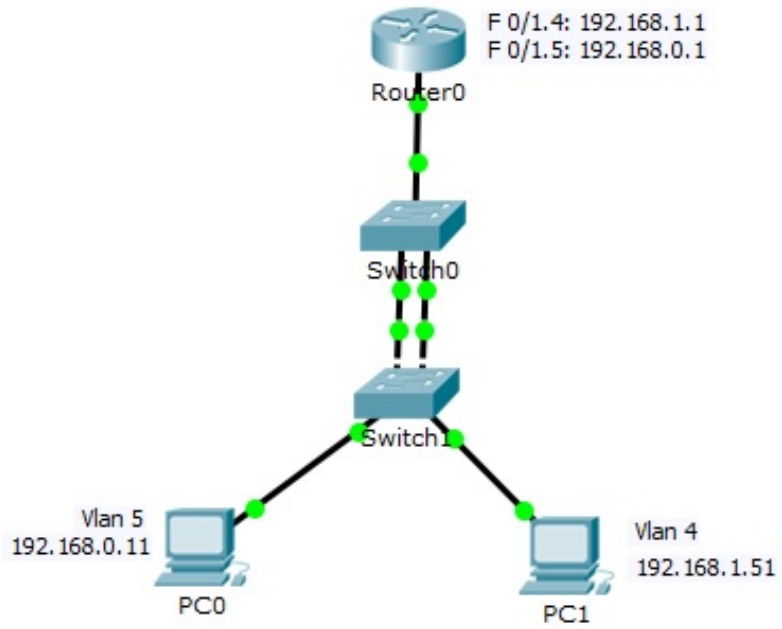

Figura 18: Representação da topologia do cenário etherchannel.
Fonte: Autoria própria

4.3.4 IMPLEMENTAÇÃO

A topologia apresentada na 18 corresponde a uma representação fiel da topologia que foi implementada no ambiente de laboratório de redes de modo prático para registro neste trabalho.

Sendo assim, para facilitar a visualização e não poluir a disposição dos dados nesta seção, foram disponibilizados os comandos utilizados para promover a configuração correta da topologia em questão no Apêndice B deste trabalho.

O Apêndice B deste trabalho é composto por 3 seções: a seção B.1, que apresenta os comandos utilizados para a configuração de um switch em laboratório que corresponde ao Switch0 da topologia apresentada na figura 18; a seção B.2, que apresenta os comandos utilizados para configurar adequadamente um switch que corresponde ao Switch1 na topologia apresentada na figura 18; e a seção B.3, que corresponde aos comandos utilizados para configurar o roteador da topologia.

Com isso, a ideia é que se possa fornecer uma visão mais técnica e mais apurada sobre quais comandos foram configurados ao longo do processo de desenvolvimento da topologia. No fim de cada seção, executamos um comando show running-config para exibir tudo que foi configurado nos dispositivos e de que modo cada um destes está operando no momento. Vale ressaltar que outro objetivo em disponibilizar os comandos utilizados ao longo do processo de desenvolvimento consiste em fornecer o máximo de informações, possibilitando um maior entendimento acerca do que cada cenário se propõe a fazer em relação à topologia em si, benefícios, problemas, soluções, entre outros.

4.4 CENÁRIO VOIP E QOS

4.4.1 DESCRIÇÃO DO CENÁRIO

O principal objetivo deste cenário é promover uma apresentação de uma implementação correta com suporte para VoIP. Este cenário visa promover uma apresentação de tal recurso, bem como seus possíveis benefícios para os usuários. Alguns destes benefícios podem ser listados como:

- Redução de custos para o usuário de tal tecnologia;
- Uma rede configurada para o tráfego de voz pode ser utilizada para o tráfego de dados também, sem que haja necessidade de qualquer aquisição ou custo extra;
- Uma vez configurada a rede com suporte a VoIP, as ligações executadas por meio do VoIP podem ser executadas sem custo, o que representa uma economia ao usuário deste recurso;

Sendo assim, o cenário voltado para a configuração de VoIP, tem ainda como objetivo, apresentar os comandos utilizados para promover o funcionamento adequado da topologia pretendida, bem como apresentar novidades em relação aos cenários passados no desenvolvimento e aprimoramento da topologia.

Para o desenvolvimento deste cenário, foi necessário o uso de um roteador modelo 2811 da Cisco, por apresentar suporte a tecnologia de Voz sobre IP (VoIP). Além disso, no processo de configuração do roteador, como mostrado no Apêndice C, foi utilizado o recurso de DHCP tanto para os telefones IP, como para os computadores pertencentes a topologia em questão. Com isso, a ideia é que cada tipo de dispositivo (telefones IP e computadores), pertencem a uma Vlan diferente (telefones IP pertencem à Vlan 2, e computadores pertencem a Vlan 3). Dessa forma, cada tipo de dispositivo apresenta seu próprio pool DHCP de endereços configurados no roteador desta rede.

4.4.2 ENDEREÇAMENTO E DISPOSITIVOS PRESENTES NA TOPOLOGIA:

Rede utilizada: 192.168.0.192 (Vlan 2) 192.168.0.32 (Vlan 3)

Máscara de Sub-rede: 255.255.255.224 ou /27

A relação de equipamentos utilizados na implementação deste cenário pode ser encontrada na tabela 6.

Quantidade	Dispositivo	Endereços IP
1	Roteador	F0/0.2: 192.168.0.193 F0/0.3: 192.168.0.33
1	Switch Gerenciável	Não aplicável
2	Computador	DHCP (Pool DHCP-Dados)
2	Telefone IP	DHCP (Pool DHCP-VoIP)

Tabela 6: Equipamentos utilizados no cenário VoIP.

Fonte: Autoria Própria.

4.4.3 REPRESENTAÇÃO DA TOPOLOGIA CORRESPONDENTE AO CENÁRIO:

A representação da topologia correspondente a este cenário pode ser observada na figura 19.

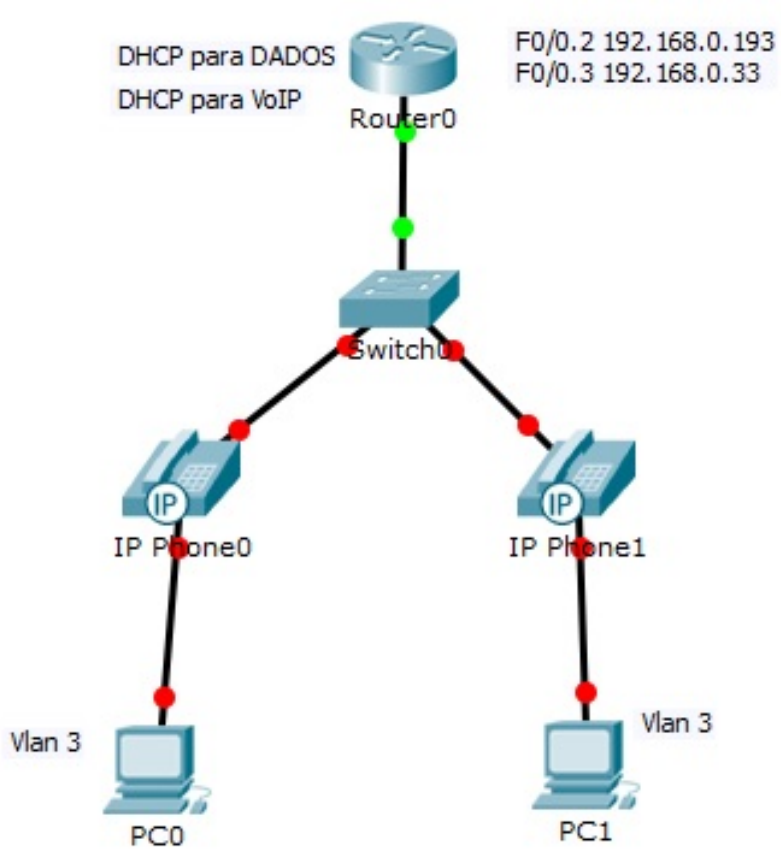

Figura 19: Representação da topologia do cenário VoIP.

Fonte: Autoria própria

4.4.4 IMPLEMENTAÇÃO

A topologia apresentada na figura 19 corresponde a uma representação fiel da topologia que foi implementada no ambiente de laboratório de redes de modo prático para registro neste trabalho.

Sendo assim, de modo semelhante ao que foi feito para o cenário 1 - Etherchannel (Seção 4.3), visando facilitar a visualização e não poluir a disposição dos dados nesta seção, disponibilizamos os comandos utilizados para promover a configuração correta da topologia em questão no Apêndice C deste trabalho.

O Apêndice C deste trabalho é composto por 2 seções: a seção C.2, que apresenta os comandos utilizados para a configuração de um switch em laboratório que corresponde ao switch da topologia apresentada na figura 19; e a seção C.1, que corresponde aos comandos utilizados para configuração de um roteador, que no caso equivale ao roteador da topologia apresentada na figura 19.

A ideia desta seção de Implementação é similar a seção de Implementação do cenário 1 - Etherchannel. O principal objetivo é fornecer uma abordagem mais técnica, evidenciando todos os comandos utilizados e configurações feitas para alcançarmos uma topologia adequada e funcional.

A topologia desenvolvida em ambiente de laboratório corresponde na íntegra à topologia apresentada na figura 19. Com isso, foi disponibilizada a figura 19 apenas como uma forma de facilitar o entendimento do leitor acerca de qual topologia foi desenvolvida em ambiente de laboratório para este trabalho.

Ao final da implementação deste cenário foi efetuada uma ligação entre os dois telefones IP configurados na rede em questão para verificarmos a funcionalidade das configurações aplicadas. A ligação apresentou-se clara e sem ruídos, dessa forma as configurações da topologia funcionaram, e a rede convergida em questão conseguiu trabalhar com os diferentes tipos de dados com que lida, sem que houvesse grandes perdas de dados de voz.

4.5 CENÁRIO STP E LOAD-BALANCING

4.5.1 DESCRIÇÃO DO CENÁRIO

O objetivo desse cenário é apresentar uma topologia com uma solução não-padrão de STP, implementando o balanceamento de carga para cada Vlan de maneira que o próprio sistema presente nos equipamentos será capaz de realizar o balanceamento de carga para cada Vlan, definindo switches raízes primárias e secundárias e permitindo que todos os enlaces sejam utilizados conforme a necessidade e sem que ocorram tempestades de broadcast.

Para o desenvolvimento desse cenário foram utilizados três switches e um roteador. O protocolo utilizado para a implementação do spanning-tree e do load-balancing foi o PVST. Devido aos requerimentos do PVST também foram criadas duas sub-redes e Vlans.

O funcionamento foi testado através de um teste de ping a partir de uma máquina para os gateways de cada rede. Durante os testes retiramos os cabos de alguns enlaces para simular a perda de conexão e atestar que mesmo após a queda de um enlace o protocolo automaticamente daria prioridade para a rota disponível em sua raiz secundária.

4.5.2 ENDEREÇAMENTO E DISPOSITIVOS PRESENTES NA TOPOLOGIA:

Rede utilizada: 192.168.0.0 (Vlan 4) e 192.168.1.0 (Vlan 5)

Máscara de sub-rede: 255.255.255.0 ou /24

A relação de equipamentos utilizados na implementação deste cenário pode ser encontrada na tabela 7.

Quantidade	Dispositivo	Endereços IP
1	Roteador	F0/0.4: 192.168.0.1 F0/0.5: 192.168.1.1
3	Switch Gerenciável	Não aplicável
2	Computador	192.168.0.3 192.168.1.3

Tabela 7: Equipamentos utilizados no cenário STP e Load-Balancing.

Fonte: Autoria Própria.

4.5.3 REPRESENTAÇÃO DA TOPOLOGIA CORRESPONDENTE AO CENÁRIO:

A representação da topologia correspondente a este cenário pode ser observada na figura 20.

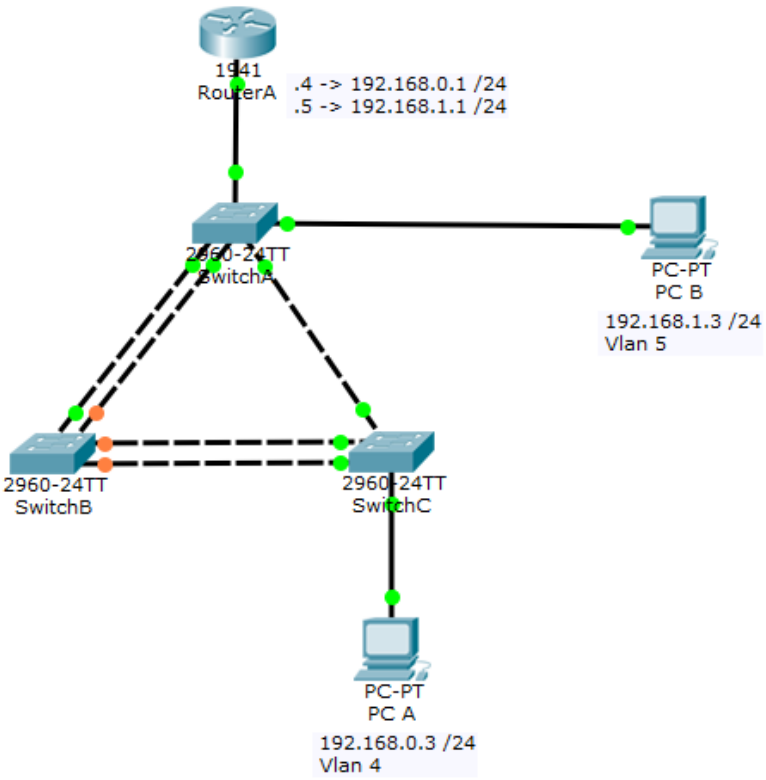

Figura 20: Representação da topologia do cenário STP e Load-Balancing.
Fonte: Autoria própria

4.5.4 IMPLEMENTAÇÃO

A topologia apresentada na figura 20 corresponde à real implementação realizada no ambiente de laboratório de redes.

De modo similar aos cenários anteriores, os comandos não estão apresentados na figura de modo a preservar uma visualização clara da topologia. Os comandos utilizados para configurar os equipamentos da topologia estão disponíveis no Apêndice D deste trabalho.

O Apêndice D é composto por 4 seções, apresentando em cada seção os comandos utilizados para configurar individualmente cada equipamento da topologia apresentada na figura.

É notável que neste cenário não foi configurado um etherchannel para realizar um agrupamento dos links entre os switches. Houve a opção pela não configuração do etherchannel nessa implementação para demonstrar que os enlaces conseguiriam operar separadamente, devido às prioridades de raiz conforme a VLAN, fazendo com que todas as interfaces ficassem em estado "UP" devido à implementação do PVST em contraste ao clássico STP.

A divisão de carga nesta topologia foi configurada para que cada switch fosse a raíz da VLAN que mais tivesse end-points conectados, dessa maneira o switch A tornou-se raíz primária da vlan 5, o switch C tornou-se raiz primária da vlan 4 e o switch B tornou-se raíz secundária de todas as vlans.

4.6 CENÁRIO PORTSECURITY

4.6.1 DESCRIÇÃO DO CENÁRIO

O objetivo deste cenário é apresentar uma topologia com uma implementação de portsecurity e divisão em Vlans, de maneira a separar o fluxo e permitir diferentes níveis de acesso para diferentes setores.

Durante a implementação foram explicitados os comandos específicos para a criação de Vlans, troncos e a aplicação de portsecurity.

Para o desenvolvimento desse cenário foram necessários apenas os switches gerenciáveis L2. O roteador apenas foi utilizado para permitir a transmissão de pacotes entre as Vlans presentes na topologia (o que se fez necessário devido aos nossos testes de conectividade utilizando ping e tracert).

4.6.2 ENDEREÇAMENTO E DISPOSITIVOS PRESENTES NA TOPOLOGIA:

Rede utilizada: 192.168.0.0 (Vlan 4), 192.168.1.0 (Vlan 5) e 192.168.3.0 (Vlan 6)

Máscara de sub-rede: 255.255.255.0 ou /24

A relação de equipamentos utilizados na implementação deste cenário pode ser encontrada na tabela 8.

Quantidade	Dispositivo	Endereços IP
1	Roteador	F0/0.4: 192.168.0.1 F0/0.5: 192.168.1.1 F0/0.6: 192.168.3.1
3	Switch Gerenciável	Não aplicável
4	Computador	192.168.0.2 192.168.0.3 192.168.1.2 192.168.3.2

Tabela 8: Equipamentos utilizados no cenário PortSecurity.
Fonte: Autoria Própria.

4.6.3 REPRESENTAÇÃO DA TOPOLOGIA CORRESPONDENTE AO CENÁRIO:

A representação da topologia correspondente a este cenário pode ser observada na figura 21.

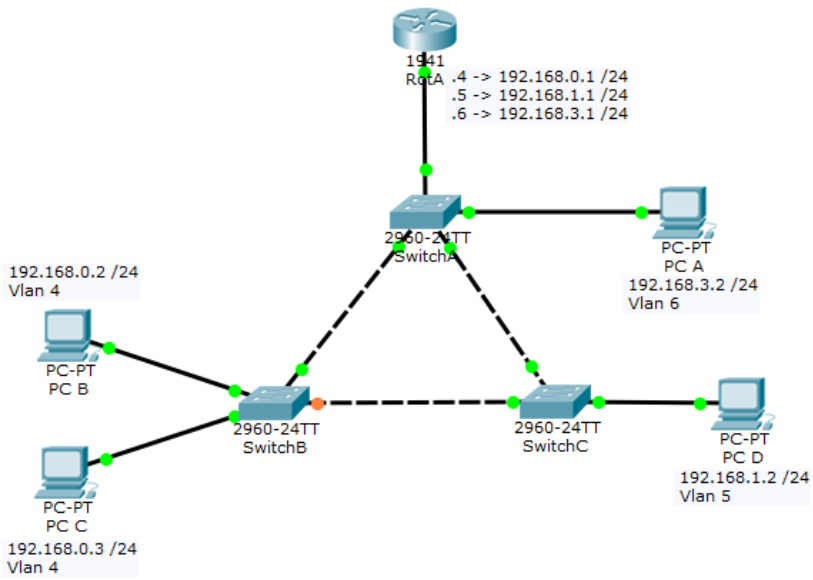

Figura 21: Representação da topologia do cenário portsecurity.
Fonte: Autoria própria

4.6.4 IMPLEMENTAÇÃO

De modo similar aos cenários anteriores, os comandos não estão apresentados na figura de modo a preservar uma visualização clara da topologia. Os comandos utilizados para configurar os equipamentos da topologia estão disponíveis no Apêndice D deste

trabalho.

O Apêndice E é composto por 4 seções, apresentando em cada seção os comandos utilizados para configurar individualmente cada equipamento da topologia apresentada na figura 21.

As configurações de PortSecurity foram aplicadas apenas às interfaces com as quais o usuário final teria fácil acesso. As interfaces reservadas para a comunicação entre os switches e o roteadores, por serem de difícil acesso físico em um cenário real, não receberam nenhuma configuração de segurança.

4.7 CENÁRIO FINAL

4.7.1 DESCRIÇÃO DO CENÁRIO

Após a análise e implementação de todos os cenários elencados até este ponto do trabalho, foi realizado o desenvolvimento do cenário final, objetivo principal deste trabalho. A ideia deste cenário é promover a implementação de uma topologia em estado da arte, sendo composta por cada cenário anteriormente descrito neste capítulo. Sendo assim, este cenário final a ser apresentado contempla as configurações e conceitos do Etherchannel, VoIP, Spanning-Tree Protocol e conceitos de Segurança, apresentados no cenário de Portsecuritiy. Com isso, o ideal ao longo deste capítulo foi fornecer um contato inicial com cada recurso que utilizaremos nesta implementação final, de forma que facilite o entendimento não apenas teórico destes, como práticos também.

Vale ressaltar também, que a topologia final foi desenvolvida levando-se em conta o modelo hierárquico de camadas de redes de computadores. Isso porque, segundo Cisco (2016), este modelo proporciona uma maior facilidade no sentido de entendimento acerca da função de cada dispositivo em sua respectiva camada, além de simplificar a implementação e o gerenciamento desta rede em questão

Devido a limitações relacionadas ao tempo e aos equipamentos que nos foram disponibilizados optamos por uma implementação com abrangência reduzida e com testes limitados.

No quesito Etherchannel, conforme descrito na seção 2.7, houve a opção por realizar uma implementação sem utilizar os protocolos de negociação automática de Etherchannel.

Sendo assim, ao final do processo de desenvolvimento desta topologia, o objetivo

é que se trate de uma rede totalmente convergida, que consiga lidar e manejar os diversos tipos de dados existentes (voz, dados comuns, imagens,...) e consiga desempenhar essa funcionalidade de forma satisfatória, ou seja, atribuindo prioridades diferentes aos diversos tipos de dados existentes e componentes da rede em questão como um todo.

4.7.2 ENDEREÇAMENTO E DISPOSITIVOS PRESENTES NA TOPOLOGIA:

Rede utilizada: 192.168.0.192 (Vlan 2), 192.168.0.32 (Vlan 3) e 192.168.0.64 (Vlan 4)

Máscara de Sub-rede: 255.255.255.224 ou /27

A relação de equipamentos utilizados na implementação deste cenário pode ser encontrada na tabela 9.

Quantidade	Dispositivo	Endereços IP
1	Roteador	Rot1: 192.168.100.1
1	Roteador 2811 (Suporte ao VOIP)	192.168.0.193
3	Switch Gerenciável (L2)	Não aplicável
1	Switch Gerenciável (L3)	Fa21.3: 192.168.0.33 Fa21.4: 192.168.0.65
3	Computador	192.168.0.66 (Vlan 4) 192.168.0.67 (Vlan 4) 192.168.0.35 (Vlan 3)
2	Telefone IP	DHCP (pool DHCP-VoIP)

Tabela 9: Equipamentos utilizados no cenário Final.
Fonte: Autoria Própria.

4.7.3 REPRESENTAÇÃO DA TOPOLOGIA CORRESPONDENTE AO CENÁRIO:

A representação da topologia correspondente a este cenário pode ser observada na figura 22.

4.7.4 IMPLEMENTAÇÃO

Assim como nos cenários anteriores, não foram dispostas as configurações realizadas nos dispositivos para compor a topologia deste cenário nesta seção de Implementação diretamente. Os comandos utilizados e configurados para desenvolver a topologia final

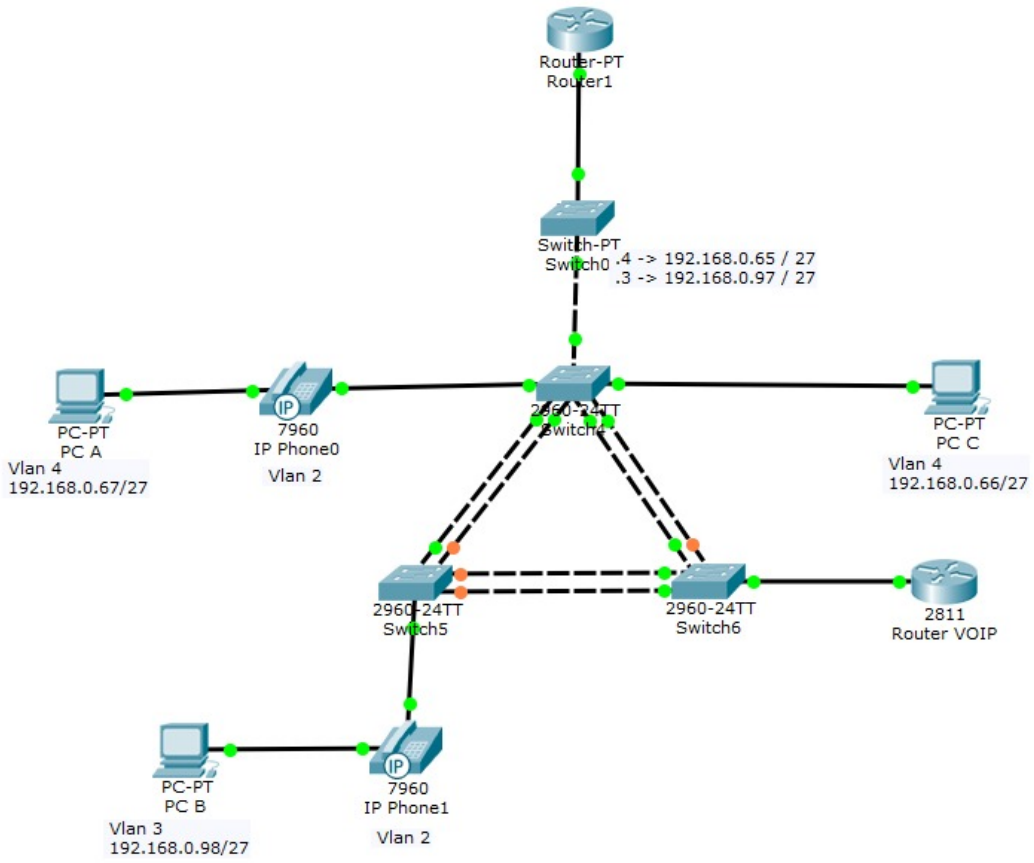

Figura 22: Representação da topologia do cenário Final.

Fonte: Autoria própria

deste trabalho estão alocados no Apêndice F, de forma que não haja uma sobrecarga da seção de Implementação do cenário final.

Inicialmente, foram configurados os endereços IP, máscaras de sub-rede e gateways padrão nos dispositivos finais que correspondem aos computadores desta topologia. Para o desenvolvimento da topologia em questão, foi adotada essa estratégia antes de configurar qualquer comando em outros dispositivos de rede. Acreditamos que a configuração inicial e básica dos computadores seria um ponto inicial bem determinado e impediria possíveis problemas futuros.

Em um segundo momento, foram criadas as Vlans da topologia(Vlan 2, Vlan 3 e Vlan 4), foram definidas as portas do switch que seriam configuradas como modo de acesso, e a porta tronco, que corresponde à porta do switch 4 da topologia da figura A, apresentada anteriormente, que se relaciona com o switch L3. Neste ponto da implementação, foram desenvolvidos mecanismos de segurança apenas nas portas de acesso direto aos computadores, uma vez que estas seriam as portas vulneráveis à interação com possíveis usuários mal-intencionados.

Foi necessário o uso de um switch L3, que atua na camada de rede, com portas roteadas, uma vez que o embasamento desta topologia é feito pelo modelo hierárquico de camadas. Sendo assim, estão presentes duas camadas hierárquicas na topologia apresentada neste trabalho: camada de acesso e camada principal recolhida. A nomenclatura destas camadas é diferente do modelo hierárquico de três camadas, que é composto pelas camadas de acesso, distribuição e núcleo, conforme mencionado por Cisco (2016).

Uma vez que o planejamento da topologia foi desenvolvido visando o modelo hierárquico mencionado, seria necessário a integração de um switch L3 na topologia em questão. Dessa forma, para este cenário final, o switch L3 foi configurado de modo a conter as subinterfaces de cada Vlan criada nesta implementação. No entanto, vale ressaltar, que a Vlan 2, referente ao VoIP, não possui uma subinterface neste equipamento. Isso porque, como este tráfego de dados não sairia da rede local foi adicionado um roteador 2811 nesta rede local, com o intuito de atender especificamente à esta Vlan.

Neste ponto da implementação, já possuímos os computadores configurados com endereços IP, máscaras de sub-rede e gateways padrão adequados; Vlans devidamente criadas contendo as portas de acesso e tronco configuradas e os comandos de segurança instalados nas portas de acesso dos switches componentes deste cenário final. Em seguida, procedemos com a configuração do Etherchannel nesta topologia de rede, visando aumentar a largura de banda, fazendo com que dois enlaces físicos se comportem como

um único enlace de forma lógica com uma maior largura de banda. Esta configuração de Etherchannel é feita para a ligação dos três switches de camada de enlace da rede do cenário final.

As configurações de segurança buscaram proteger certos aspectos das portas dos switches utilizados nesta topologia. Basicamente foram utilizados quatro principais comandos para garantirmos um nível satisfatório de segurança nos switches:

```
switchport port-security
switchport port-security maximum "number"
switchport port-security ip address sticky
switchport port-security violation shutdown
```

As configurações de segurança apresentadas anteriormente foram utilizadas com o objetivo de restringir acessos indevidos às portas do switch, além de tentar garantir acesso aos dispositivos que de fato estejam autorizados a estabelecer conexões com este switch. Sendo assim, o comando switchport port-security maximum "number" visa estabelecer um número limite de dispositivos distintos (baseia-se em endereços MAC diferentes) que estão autorizados a conectar-se com o switch em questão. O comando switchport port-security ip address sticky tem como objetivo fazer com que a interface do switch que é configurada desta forma aprenda de forma dinâmica os endereços MAC que podem conectar-se, sem que seja necessário especificar tais endereços MAC de forma manual. Por fim, o comando switchport port-security violation shutdown garante que se houver alguma violação no cenário de segurança configurado, a interface será desativada e não encaminhará dados até ser reativada novamente. O comando switchport port-security, emitido antes dos comandos explicados anteriormente, garante que a porta do switch estará apta a receber as configurações de segurança seguintes.

Em cima desta situação, é configurado o Spanning-Tree Protocol, permitindo que não só a topologia fique protegida de tempestades de broadcast mas que, em conjunto com a configuração do etherchannel, permita a redundância entre os diferentes equipamentos. Para a distribuição de carga inerente ao PVST optamos por transformar os switches A e B em raízes primárias das vlans 4 e 3, respectivamente, pois estes possuíam o maior número de usuários presentes nestas vlans.

Por fim, foram realizadas as configurações necessárias para que a topologia deste cenário final possa suportar o tráfego de voz sobre ip, ou VoIP, como é mais conhecido. Para que o tráfego de voz possa ser devidamente deslocado pela rede, é necessário que

este tráfego seja encaminhado por um roteador que possua suporte a este recurso, como é o caso do modelo 2811 da Cisco. Sendo assim, um exemplar deste modelo foi devidamente anexado ao que corresponde à topologia do cenário final deste trabalho. Além disso, foram utilizados dois telefones IP da Cisco nesta topologia, da forma semelhante ao cenário 2 - VoIP e QoS. O roteador foi configurado como um servidor DHCP para estes telefones, de modo que os telefones recebem um endereço IP dinâmico via servidor DHCP configurado no roteador 2811. A implementação das configurações de VoIP e QoS utilizadas no trabalho contemplam os seguintes comandos:

```
SwiA(config)#interface fastEthernet 0/6
SwiA(config-if)#switchport mode access
SwiA(config-if)#switchport access vlan 4
SwiA(config-if)#switchport voice vlan 2
SwiA(config-if)#exit
```

O comando switchport voice vlan 2 refere-se à atribuição de uma prioridade superior aos dados de voz na Vlan 2 (Vlan VoIP) de forma automática, sem que seja necessário a configuração de modo manual. Este comando promove uma configuração em que a prioridade dos dados referentes a voz é elevada para o valor 5 em uma escala de prioridades dos diversos tipos de dados.

No entanto, esta configuração para garantir o QoS na rede em questão poderia ter sido implementada de modo diferente, por meio dos seguintes comandos:

```
SwiA#conf t
SwiA(config)#mls qos
SwiA(config)#interface range fa 0/1-5
SwiA(config-if-range)#mls qos
SwiA(config-if-range)#mls qos cos 5
SwiA(config-if-range)#mls qos trust cos
SwiA(config-if-range)#exit
```

No exemplo apresentado acima as portas de aplicação do QoS são distintas do trecho de configuração anterior, porém o objetivo de garantir a maior prioridade aos dados de voz (prioridade 5) é o mesmo. A diferença apresentada entre os dois métodos é que no primeiro, e selecionado para a configuração deste trabalho, a atribuição de prioridade é feita de forma automática para a Vlan em questão, ou seja, a Vlan 2 neste caso passa

a lida com os dados de voz em prioridade 5. Por outro lado, na segunda configuração apresentada, a atribuição da prioridade é feita de forma manual, para um grupo específico de portas do switch em questão.

Devido a limitações de tempo e dificuldades técnicas não foi possível realizar uma implementação com mais de um roteador de saída. Idealmente a topologia apresentada deveria ter mais de um roteador de saída para que não houvesse um ponto de falha única.

Dessa forma, todos os cenários foram devidamente contemplados na implementação do cenário final deste trabalho. Cada cenário, de modo individual e geral, contribui para formar uma topologia final mais robusta, confiável e mais facilmente gerenciável.

São apresentados, na figura 23, os equipamentos utilizados para a implementação do cenário final.

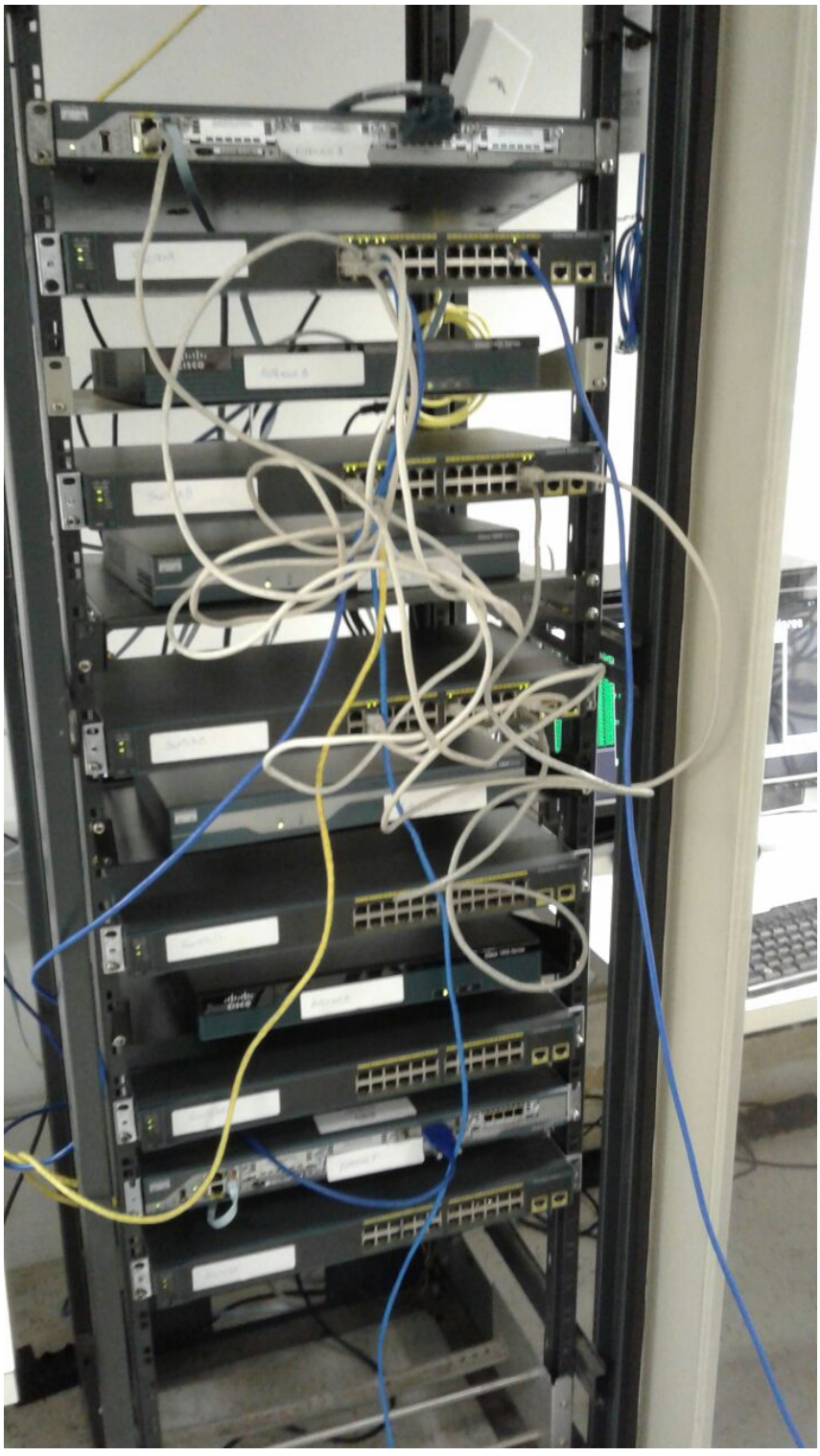

Figura 23: Equipamentos utilizados na implementação do cenário Final.

Fonte: Autoria própria

5 CONSIDERAÇÕES FINAIS

5.1 CONCLUSÃO

Com o desenvolvimento do presente trabalho, busca-se a análise de uma infraestrutura implementada de forma hierárquica e estruturada, estudando a melhor forma de configurar os equipamentos de redes que integram esta infraestrutura.

Uma parte das implementações de redes locais (LANs) atuais são feitas de forma não planejada, o que acarreta problemas como tempestades de broadcast, falhas de segurança e uma utilização ineficiente dos recursos de rede. Quando se tem uma implementação de voz sobre IP (VoIP) em uma LAN não estruturada, o serviço pode ficar degradado e a sua utilização pode ser comprometida. A implementação de uma infraestrutura de redes locais (LAN) de forma hierárquica e estruturada evita os problemas comuns, e fornece escalabilidade, disponibilidade, e um melhor desempenho dos serviços implementados dentro da rede em questão.

Inicialmente, foi pensada em uma topologia de rede que levasse em consideração o modelo hierárquico de camadas, visando sanar certos problemas que as redes que não se utilizam deste modelo apresentam. Uma topologia de rede que não implemente o modelo hierárquico de camadas apresenta certos problemas, como por exemplo:

- Muitos saltos a serem percorridos na topologia, conforme o número de switches interligados cresce. Tal prática predispõe a rede a problemas como tempestades de broadcast (broadcast storm), entre outros;
- Maior quantidade de cabos a serem utilizados para interligar todos os switches que adentram na rede;
- Menor grau de escalabilidade da rede, uma vez que é mais complicado acrescentar um novo switch na rede em questão;
- Além de tudo mencionado anteriormente, uma rede que não se utilize do modelo

hierárquico de camadas apresenta dificuldade para a solução de problemas de modo geral. Isso porque não apresenta o conceito de modularização dos dispositivos, ou divisão em camadas. Tal disposição dos dispositivos aumenta o grau de complexidade dos problemas na rede e dificulta a solução e isolamento deste por parte do administrador de redes.

Desta forma, uma vez que todos estes problemas são elencados, visamos o desenvolvimento de uma topologia de rede que conseguisse solucionar cada um destes problemas. Sendo assim, optamos pelo desenvolvimento de uma topologia de rede baseada no modelo hierárquico de camadas, o que não apenas serviria para solucionar tais problemas, como trazer benefícios para a rede em questão, como por exemplo:

- **Maior escalabilidade**: Com o uso do modelo hierárquico de camadas é maior a facilidade de adição de novos switches na topologia de rede;
- **Disponibilidade**: Com a expansão da topologia de rede em questão, é importante que a rede contemple enlaces redundantes entre as camadas do modelo hierárquico, de forma que a rede se torna disponível sempre que for requisitada.
- **Gerenciabilidade**: Como a rede é disposta em camadas, há a modularização de funcionalidade de cada camada. As camadas são compostas por switches adequados e voltados para atender a funcionalidade específica da camada em questão. Dessa forma, quando surge um problema em uma determinada camada, é mais fácil e acessível para o administrador de rede localizar e isolar o problema para proceder com a solução.

Em um segundo momento foi definido que a topologia da rede a ser implementada neste trabalho deveria abordar práticas que visassem a melhoria da rede como um todo, contemplando conceitos como: segurança, suporte à voz, maior largura de banda, entre outros.

Dentre estes conceitos elencados anteriormente, o primeiro a ser implementado, uma vez que o planejamento e desenho da topologia de rede haviam sido feitos, foi o etherchannel, que visa promover uma agregação de enlaces físicos da topologia de rede, formando um enlace lógico detentor de uma maior largura de banda. Como a topologia final utiliza-se de recursos de voz sobre IP (VoIP), houve uma preocupação em fornecer uma largura de banda adequada para que todos os dispositivos componentes desta rede pudessem ter acesso de forma plena e satisfatória. Desta forma, foram verificadas as

configurações dos diversos dispositivos desta implementação de rede de computadores, a fim de identificar e sanar qualquer configuração equivocada que pudesse interferir e gerar uma largura de banda inferior.

Em seguida, visamos promover uma proteção aos switches no sentido de garantir a segurança de porta destes dispositivos. Foi utilizada uma abordagem buscando garantir a segurança de porta dos switches em diferentes aspectos, como por exemplo:

- Estabelecer um número máximo de diferentes usuários (endereços MAC distintos) que podem se conectar a uma determinada porta de switch configurada com a segurança de porta.
- Determinar o modo como a porta do switch em questão aprenderá os endereços MAC permitidos. Neste caso, foi selecionado o modo de aprendizado dinâmico, ou seja, sem que haja a necessidade de um administrador de rede informar manualmente os endereços que podem estabelecer conexão com as portas de switch configuradas desta maneira.
- Estipular um modo de violação de segurança para a porta de switch em questão. Uma vez que um cenário de segurança é violado, a porta do switch possui mecanismos de configuração que apontam respostas distintas. Por exemplo, uma vez que uma porta é configurada como receptora de uma máximo de três endereços MAC distintos, quando um quarto endereço MAC de usuário tenta uma conexão, configura-se um cenário de violação de segurança. Na tipologia de rede deste trabalho, a segurança de porta escolhida promove um desligamento da porta de switch que sofre com essa violação de segurança. Esta situação impede que a porta encaminhe qualquer dado até ser reativada, garantindo um nível maior de segurança aos usuários autorizados da rede em questão.

Uma vez que houvessem configurações que garantissem uma maior largura de banda e a segurança estivesse sido estabelecida, foi procedido com o desenvolvimento da implementação do protocolo Spanning-Tree. A principal ideia ao configurar o protocolo STP nesta topologia é a eliminação de problemas como a tempestade de broadcast (broadcast storm). Isso porque, o protocolo STP atua eliminando loops lógicos, mas os enlaces físicos que apresentam redundância são mantidos. A redundância em enlaces físicos é algo benéfico para a rede, uma vez que atua assegurando questões como confiabilidade e disponibilidade da rede. Porém, quando há um loop lógico, o cenário se torna adverso, uma vez que não há uma segurança ou controle sobre os rumos do encaminhamento de uma

mensagem. Uma mensagem enviada em broadcast pode ser propagada indefinidamente quando não há a configuração do protocolo STP, comprometendo a comunicação da rede analisada.

Por fim, foi configurado um cenário que permitisse uso e suporte à tecnologia VoIP, ou seja, que permitisse com que os usuários utilizassem telefones IP de modo pleno, ou seja, com uma rede configurada adequadamente para dar base à tal recurso. O principal objetivo da agregação desta funcionalidade à topologia final, era desenvolver uma topologia de rede convergida que oferecesse base para uso pleno da telefonia IP. Muitas redes de computadores atualmente utilizam-se dos serviços e benefícios fornecidos pela telefonia IP, no entanto, não apresentam configurações adequadas para fornecer suporte para tal. Neste trabalho, fornecemos uma configuração que garante prioridade mais elevada aos dados de voz que trafegam na Vlan reservada para VoIP. Dessa forma, minimizamos as chances de perdas ou atrasos de pacotes de dados referentes a este tipo de dados.

Com isso, percebemos a importância destes cenários e suas respectivas configurações para uma rede de computadores. Em muitos casos, os usuários de uma rede local têm pressa para que ela esteja funcional, porém, não levam em conta aspectos de segurança e melhoria de desempenho como os que foram elencados ao longo deste trabalho. Uma topologia de rede que não contemple os aspectos de desempenho e segurança mencionados será concluída e disponibilizada para uso de seus usuários em um intervalo de tempo inferior em relação ao tempo destinado para configurar a topologia de rede mencionada neste trabalho. Porém, as chances desta rede mais simples apresentar problemas de diversas naturezas, sem contar possíveis ataques de invasores, são muito mais reais e elevadas do que a rede apresentada neste trabalho.

Ao projetar e desenvolver uma rede de computadores para os estabelecimentos, estes cenários deveriam ser priorizados. Uma rede projetada sem levar em consideração tais cenários, acaba sobrecarregando seu administrador de rede com retrabalhos e soluções que eventualmente não aconteceriam em uma rede robusta, configurada de modo a priorizar o desempenho e a segurança de seus usuários.

A seguir descrevemos os trabalhos futuros que podem ser desenvolvidos de modo a complementar e aperfeiçoar o que foi apresentado neste trabalho.

5.2 TRABALHOS FUTUROS

Esta seção é destinada à apresentação de trabalhos futuros que podem ser realizados tendo como base o que foi apresentado até então neste trabalho:

- Futuramente, uma forma de complementar a topologia desenvolvida e apresentada neste trabalho, seria uma maneira de configurar o gateway de último recurso da rede em questão. A rede apresentada neste trabalho é subdividida em Vlans, e possui subinterfaces para cada Vlan definidas em uma interface de um switch L3. Este switch L3 conecta-se a um roteador, cuja função é servir como gateway de último recurso para a rede abordada neste trabalho. Ou seja, todos os pacotes que chegam ao switch L3, caso não possuam o endereço destino como componente da tabela de roteamento deste switch L3, serão devidamente encaminhados ao roteador encarregado de fornecer o gateway de último recurso. No entanto, pensando em tornar esta topologia em uma implementação ainda mais segura e robusta, poderia ser implementado o protocolo HSRP, visando promover uma maior confiabilidade para a rede. O objetivo do protocolo HSRP, no contexto da topologia final apresentada neste trabalho, seria permitir a configuração de dois roteadores como gateway de último recurso, com apenas um deles em funcionamento. Dessa forma, o roteador adicional seria uma medida de segurança caso o outro roteador sofresse algum problema e tivesse seu funcionamento interrompido. Com isso, o funcionamento da rede não depende de um único link. Caso ocorram problemas, existem mecanismos neste cenário que possibilitam com que o problema seja contornado sem que a rede sofra com grandes prejuízos aos seus usuários.

- Este trabalho não contemplou redes compostas por equipamentos de diferentes marcas e por modelos mais simples de equipamentos de rede (por exemplo, *switches* não-gerenciáveis), contemplando apenas os equipamentos (*switches*, roteadores e telefones IP) da marca Cisco. Uma expansão para os temas abordados neste trabalho seria a implementação das boas práticas em uma rede com equipamentos de diferentes marcas e capacidades, prezando pela implementação de todas as tecnologias apresentadas e pelas boas práticas de redes de computadores.

- Outra possível expansão seria a realização de testes mais precisos e abrangentes sobre a topologia apresentada e desenvolvida ao decorrer deste trabalho. Ataques de segurança como Man-in-the-Middle (MITM), MAC e DHCP Spoofing, entre outros, não puderam ser realizados devido a limitantes de tempo e equipamentos.

REFERÊNCIAS

ASSIS, A. U. de et al. Protocolo mpls. **CBPF-NT-007**, v. 7, n. 2, 2002.

BALCHUNAS, A. **Spanning-Tree Protocol**. [S.l.: s.n.], 2014.

BALCHUNAS, A. **Switch and Vlan Security**. [S.l.: s.n.], 2014.

CISCO. **Qualidade de serviço de voz sobre IP**. Cisco Systems Inc., set 2008. Disponível em: <http://www.cisco.com/cisco/web/support/BR/10/107/107770_tech_tk652_tk698_technologies_whit

CISCO. **Catalyst 2960 and 2960-S Switch Software Configuration Guide**. [S.l.]: Cisco IOS Release 12.2(53)SE1, 2010.

CISCO. **Catalyst 3750-X and 3560-X Switch Software Configuration Guide, Release 12.2(55)SE**. Cisco Systems Inc., nov 2014. Disponível em: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swethchl.html>.

CISCO. **Cisco Net Academy**. Cisco Systems Inc., 2016. Disponível em: <http://static-course-assets.s3.amazonaws.com/ITN50PT/module11/index.html>.

DEGUCHI, P. H. M.; SANTOS, F. B. dos. **REESTRUTURAÇÃO DAS CAMADAS 2 E 3 (ENLACE E REDE) DA UTFPR CÂMPUS CURITIBA** — Universidade Tecnológica Federal do Paraná, 2012. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/676/1/CT_COTSI_2012_1_05.pdf>.

DIóGENES, Y. **Certificação Cisco, CCNA 4.0 Guia de Certificação para o Exame 640-801**. [S.l.: s.n.], 2004.

FALSARELLA, D. **Conceitos Básicos de QoS**. jun 2009. Disponível em: <http://imasters.com.br/artigo/13011/redes-e-servidores/conceitos-basicos-de-qos/>.

FARRINGTON, N. **The Dawn of Channelized Ethernet**. SemanticsScholar, ago 2014. Disponível em: <https://pdfs.semanticscholar.org/2fa2/0fcedee589b0071c0875cb4c8f9146e38eba.pdf>.

HUCABY, D. **CCNP Routing and Switching SWITCH 300-115 Official Cert Guide**. first. [S.l.]: Cisco Press, 2014.

IESDE. **Redes de Computadores - Topologia e Hardware**. 2010. Disponível em: <http://uol.iesde.com.br/aprovaconcursos/demo_aprova_concursos/informatica_07>.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet - Uma abordagem top-down**. fourth. [S.l.]: Pearson, 2005.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet - Uma abordagem top-down**. fifth. [S.l.]: Pearson, 2010.

MACURA, A.; MISSONI, E.; MAKOVIC, B. Quality of service in multimedia computer networks. **Annals of DAAAM & Proceedings**, v. 22, n. 1, 2011.

MATTIES, A. S.; MORAES, A. **QoS em roteadores Cisco**. 2008.

MENDES, D. R. **Redes de Computadores - Teoria e Prática**. [S.l.]: Novatec, 2007.

PHONPHOEM, A.; JANSANG, A. A simple network management architecture for supporting network administrator and qos requirements. **ICCC 2002**, v. 15, 2001.

PILLOU, J.-F. **VLAN - Redes Virtuais**. jul 2014. Disponível em: <http://br.ccm.net/contents/289-vlan-redes-virtuais>.

RIOS, R. O. **Protocolos e Serviços de Rede**. [S.l.]: Ministério da Educação, 2010.

SILVA, K. R. **Seminário 1: QoS**. 2014. Http://wiki.sj.ifsc.edu.br/wiki/index.php/RED29004-2014-1-Seminario1-QoS.

TANENBAUM, A. S. **Redes de Computadores**. fourth. [S.l.]: Pearson, 2003.

TELECO. **Redes IP: Fundamentos Redes**. mar 2013.

APÊNDICE A – COMANDOS - CENÁRIO BASE

A.1 COMANDOS - ROUTER A

Esta seção corresponde aos comandos emitidos no roteador da topologia apresentadas na seção 4.2.

```
Router>ena
Router#conf t
Router(config)#interface fa 0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#end
```

APÊNDICE B – COMANDOS - CENÁRIO ETHERCHANNEL

B.1 COMANDOS - SWITCH 0

Esta seção corresponde aos comandos emitidos no switch 0 da topologia apresentada na seção 4.3.

```
SW0>ena
SW0#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW0(config)#interface range fastEthernet 0/23-24
SW0(config-if-range)#channel-group 1 mode on
Creating a port-channel interface Port-channel 1
SW0(config-if-range)#
SW0(config-if-range)#no shutdown
SW0(config-if-range)#exit
SW0(config)#interface port-channel 1
SW0(config-if)#switchport mode trunk
SW0(config-if)#switchport trunk allowed vlan all
SW0(config-if)#
SW0(config-if)#switchport trunk
SW0(config-if)#exit
SW0(config)# vlan 4
SW0(config)# vlan 5
SW0(config)# interface fa 0/13
SW0(config-if)# switchport mode trunk
SW0(config-if)# switchport allowed vlan all
```

B.2 COMANDOS - SWITCH 1

Esta seção corresponde aos comandos emitidos no switch 1 da topologia apresentada na seção 4.3.

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Switch1
Switch1(config)#vlan 4
Switch1(config-vlan)#name depto2
Switch1(config-vlan)#exit
Switch1(config)#vlan 5
Switch1(config-vlan)#name depto3
Switch1(config-vlan)#exit
Switch1(config)#interface fastEthernet 0/1
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 5
Switch1(config-if)#exit
Switch1(config)#interface fastEthernet 0/3
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 4
Switch1(config-if)#exit
Switch1(config)#interface range fa 0/23-24
Switch1(config-if-range)#channel-group 1 mode on
Creating a port-channel interface Port-channel 1
Switch1(config-if-range)#channel-group 1 mode on
Switch1(config-if-range)#no shut
Switch1(config-if-range)#exit
Switch1(config)#interface port-channel 1
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#switchport trunk allowed vlan all
Switch1(config-if)#exit
```

B.3 COMANDOS - ROTEADOR

Esta seção corresponde aos comandos emitidos no roteador da topologia apresentada na seção 4.3.

```
Router>ena
Router#conf t
Router(config)#interface fa 0/0
Router(config-if)#no shut
Router(config-if)#no ip address
Router(config-if)#interface fa 0/0.4
Router(config-subif)#encapsulation dot1Q 4
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#no shut
Router(config-if)#interface fa 0/0.5
Router(config-subif)#encapsulation dot1Q 5
Router(config-subif)#ip address 192.168.0.1 255.255.255.0
Router(config-subif)#no shut
```

APÊNDICE C – COMANDOS - CENÁRIO BASE

C.1 COMANDOS - ROUTER A

Esta seção corresponde aos comandos emitidos no roteador da topologia apresentadas na seção 4.4.

```
Router>ena
Router#conf t
Router(config)#interface fastEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#
Router(config)#interface fastEthernet 0/0.3
Router(config-subif)#encapsulation dot1q 3
Router(config-subif)#ip address 192.168.0.33 255.255.255.224
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0.2
Router(config-subif)#encapsulation dot1q 2
Router(config-subif)#ip address 192.168.0.193 255.255.255.224
Router(config-subif)#end
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp excluded-address 192.168.0.33
Router(config)#ip dhcp pool DHCP-DADOS
Router(dhcp-config)#network 192.168.0.0 255.255.255.224
Router(dhcp-config)#default-router 192.168.0.33
Router(dhcp-config)#end
Router#
Router#conf t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp excluded-address 192.168.0.193
Router(config)#ip dhcp pool DHCP-VOIP
Router(dhcp-config)#network 192.168.0.192 255.255.255.224
Router(dhcp-config)#default-router 192.168.0.193
Router(dhcp-config)#option 150 ip 192.168.0.193
Router(dhcp-config)#exit
Router(config)#telephony-service
Router(config-telephony)#max-dn 10
Router(config-telephony)#max-ephones 10
Router(config-telephony)#ip source-address 192.168.0.193 port 2000
Router(config-telephony)#end
Router#
Router#conf t
Router(config)#ephone-dn 1
Router(config-ephone-dn)#
Router(config-ephone-dn)#ephone-dn 2
Router(config-ephone-dn)#
Router(config-ephone-dn)#
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#tele
Router(config)#telephony-service
Router(config-telephony)#auto a
Router(config-telephony)#auto assign 1 to 5
```

C.2 COMANDOS - SWITCH

Esta seção corresponde aos comandos emitidos no roteador da topologia apresentadas na seção 4.4.

```
Switch>ena
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Switch(config)#vlan 3
Switch(config-vlan)#name DADOS
Switch(config-vlan)#vlan 2
Switch(config-vlan)#name VOIP
Switch(config-vlan)#exit
Switch(config)#interface fastEthernet 0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#interface range fastEthernet 0/1-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 3
Switch(config-if-range)#switchport voice vlan 2
Switch(config-if-range)#end
```

APÊNDICE D – COMANDOS - CENÁRIO STP E LOAD-BALANCING

D.1 COMANDOS - SWITCH A

Esta seção corresponde aos comandos emitidos no switch A da topologia apresentada na seção 4.5.

```
SwitchA(config)#vlan 4
SwitchA(config-vlan)#vlan 5
SwitchA(config-vlan)#exit
SwitchA(config)#interface fastEthernet 0/24
SwitchA(config-if)#switchport mode trunk
SwitchA(config-if)#switchport trunk allowed vlan
SwitchA(config-if)#no shut
SwitchA(config-if)#exit
SwitchA(config)#interface fastEthernet 0/13
SwitchA(config-if)#switchport mode access
SwitchA(config-if)#switchport access vlan 5
SwitchA(config-if)#no shut
SwitchA(config-if)#exit
SwitchA(config)#interface range fastEthernet 0/1-3
SwitchA(config-if-range)#switchport mode trunk
SwitchA(config-if-range)#switchport trunk native vlan 99
SwitchA(config-if-range)#switchport trunk allowed vlan 4,5
SwitchA(config-if-range)#no shut
SwitchA(config-if-range)#exit
SwitchA(config)#
SwitchA(config)#spanning-tree mode pvst
SwitchA(config)#spanning-tree vlan 5 root primary
SwitchA(config)#
```

D.2 COMANDOS - SWITCH B

Esta seção corresponde aos comandos emitidos no switch B da topologia apresentada na seção 4.5.

```
SwitchB(config)#vlan 4
SwitchB(config-vlan)#vlan 5
SwitchB(config-vlan)#exit
SwitchB(config)#interface range fastEthernet 0/1-2
SwitchB(config-if-range)#switchport mode trunk
SwitchB(config-if-range)#switchport trunk native vlan 99
SwitchB(config-if-range)#switchport trunk allowed vlan 4,5
SwitchB(config-if-range)#no shut
SwitchB(config-if-range)#exit
SwitchB(config)#interface range fastEthernet 0/19-20
SwitchB(config-if-range)#switchport mode trunk
SwitchB(config-if-range)#switchport trunk native vlan 99
SwitchB(config-if-range)#switchport trunk allowed vlan 4,5
SwitchB(config-if-range)#no shut
SwitchB(config-if-range)#
SwitchB(config)#spanning-tree mode pvst
SwitchB(config)#spanning-tree vlan 4 root secondary
SwitchB(config)#spanning-tree vlan 5 root secondary
```

D.3 COMANDOS - SWITCH C

Esta seção corresponde aos comandos emitidos no switch C da topologia apresentada na seção 4.5.

```
SwitchC(config)#vlan 4
SwitchC(config-vlan)#vlan 5
SwitchC(config-vlan)#exit
SwitchC(config)#interface fast
SwitchC(config)#interface fastEthernet 0/13
SwitchC(config-if)#switchport mode access
```

```
SwitchC(config-if)#switchport access vlan 4
SwitchC(config-if)#no shut
SwitchC(config-if)#exit
SwitchC(config)#interface range fastEthernet 0/19-20
SwitchC(config-if-range)#switchport mode trunk
SwitchC(config-if-range)#switchport trunk native vlan 99
SwitchC(config-if-range)#switchport trunk allowed vlan 4,5
SwitchC(config-if-range)#no shut
SwitchC(config-if-range)#exit
SwitchC(config)#interface fastEthernet 0/3
SwitchC(config-if)#switchport mode trunk
SwitchC(config-if)#switchport trunk native vlan 99
SwitchC(config-if)#switchport trunk allowed vlan 4,5
SwitchC(config-if)#exit
SwitchC(config)#spanning-tree mode pvst
SwitchC(config)#spanning-tree vlan 4 root primary
```

D.4 COMANDOS - ROTEADOR

Esta seção corresponde aos comandos emitidos no roteador da topologia apresentada na seção 4.5.

```
Router(config)#interface fa 0/0
Router(config-if)#no shut
Router(config-if)#no ip address
Router(config-if)#interface fa 0/0.4
Router(config-subif)#encapsulation dot1Q 4
Router(config-subif)#ip address 192.168.0.1 255.255.255.0
Router(config-subif)#no shut
Router(config-if)#interface fa 0/0.5
Router(config-subif)#encapsulation dot1Q 5
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#no shut
```

APÊNDICE E – COMANDOS - CENÁRIO PORTSECURITY

E.1 COMANDOS - SWITCH A

Esta seção corresponde aos comandos emitidos no switch A da topologia apresentada na seção 4.6.

```
SwitchA(config)#vlan 4
SwitchA(config-vlan)#vlan 5
SwitchA(config-vlan)#vlan 6
SwitchA(config-vlan)#
SwitchA(config)#interface fastEthernet 0/11
SwitchA(config-if)#switchport mode access
SwitchA(config-if)#switchport access vlan 6
SwitchA(config-if)#switchport port-security maximum 5
SwitchA(config-if)#switchport port-security mac-address sticky
SwitchA(config-if)#switchport port-security violation shutdown
SwitchA(config-if)#no shut
SwitchA(config-if)#exit
SwitchA(config)#interface range fastEthernet 0/21-23
SwitchA(config-if-range)#switchport mode trunk
SwitchA(config-if-range)#switchport trunk allowed vlan 4,5,6
SwitchA(config-if-range)#no shut
SwitchA(config-if-range)#exit
SwitchA(config)#interface fastEthernet 0/1
SwitchA(config-if)#switchport mode trunk
SwitchA(config-if)#switchport trunk allowed vlan 4,5,6
SwitchA(config-if)#no shut
SwitchA(config-if)#exit
```

E.2 COMANDOS - SWITCH B

Esta seção corresponde aos comandos emitidos no switch B da topologia apresentada na seção 4.6.

```
SwitchB(config)#vlan 4
SwitchB(config-vlan)#vlan 5
SwitchB(config-vlan)#vlan 6
SwitchB(config-vlan)#exit
SwitchB(config)#interface range fastEthernet 0/1-3
SwitchB(config-if-range)#switchport mode access
SwitchB(config-if-range)#switchport access vlan 4
SwitchB(config-if-range)#switchport port-security maximum 5
SwitchB(config-if-range)#switchport port-security mac-address sticky
SwitchB(config-if-range)#switchport port-security violation shutdown
SwitchB(config-if-range)#no shut
SwitchB(config-if-range)#exit
SwitchB(config)#
SwitchB(config)#interface range fastEthernet 0/19-23
SwitchB(config-if-range)#switchport mode trunk
SwitchB(config-if-range)#switchport trunk allowed vlan 4,5,6
SwitchB(config-if-range)#no shut
SwitchB(config-if-range)#exit
SwitchB(config)#
SwitchB(config)#exit
```

E.3 COMANDOS - SWITCH C

Esta seção corresponde aos comandos emitidos no switch C da topologia apresentada na seção 4.6.

```
Switch(config)#hostname SwitchC
SwitchC(config)#vlan 4
SwitchC(config-vlan)#vlan 5
SwitchC(config-vlan)#vlan 6
```

```
SwitchC(config-vlan)#exit
SwitchC(config)#interface fastEthernet 0/1
SwitchC(config-if)#switchport mode access
SwitchC(config-if)#switchport access vlan 5
SwitchC(config-if)#no shut
SwitchC(config-if)#exit
SwitchC(config)#interface fastEthernet 0/1
SwitchC(config-if)#switchport port-security maximum 5
SwitchC(config-if)#switchport port-security mac-address sticky
SwitchC(config-if)#switchport port-security violation shutdown
SwitchC(config-if)#exit
SwitchC(config)#
```

E.4 COMANDOS - ROTEADOR

Esta seção corresponde aos comandos emitidos no roteador da topologia apresentada na seção 4.6.

```
RotA(config)#interface fastEthernet 0/1
RotA(config-if)#no ip address
RotA(config-if)#no shut
RotA(config-if)#exit
RotA(config)#interface fastEthernet 0/1.4
RotA(config-subif)#encapsulation dot1Q 4
RotA(config-subif)#ip address 192.168.0.1 255.255.255.0
RotA(config-subif)#exit
RotA(config)#interface fastEthernet 0/1.5
RotA(config-subif)#encapsulation dot1Q 5
RotA(config-subif)#ip address 192.168.1.1 255.255.255.0
RotA(config-subif)#exit
RotA(config)#interface fastEthernet 0/1.6
RotA(config-subif)#encapsulation dot1Q 6
RotA(config-subif)#ip address 192.168.3.1 255.255.255.0
RotA(config-subif)#exit
```

APÊNDICE F – COMANDOS - CENÁRIO FINAL

F.1 COMANDOS - BÁSICOS

Esta seção corresponde aos comandos de configurações básicas aplicados em todos os equipamentos da rede. apresentada na seção 4.7.

```
Switch>ena
Switch#conf t
SwiA(config)#vlan 2
SwiA(config-vlan)#name VOIP
SwiA(config-vlan)#vlan 3
SwiA(config-vlan)#vlan 4
SwiA(config-vlan)#exit
```

```
SwiB>ena
SwiB#conf t
SwiB(config)#vlan 2
SwiB(config-vlan)#name VOIP
SwiB(config-vlan)#vlan 3
SwiB(config-vlan)#vlan 4
SwiB(config-vlan)#exit
```

```
SwiC>ena
SwiC#conf t
SwiC(config)#vlan 2
SwiC(config-vlan)#name VOIP
SwiC(config-vlan)#vlan 3
```

```
SwiC(config-vlan)#vlan 4
SwiC(config-vlan)#exit
```

F.2 COMANDOS - PORTSECURITY

Esta seção corresponde aos comandos de configuração do PortSecurity, aplicado aos equipamentos da rede apresentada na seção 4.7.

```
SwiA(config)#vlan 3
SwiA(config-vlan)#exit
SwiA(config)#interface fastEthernet 0/5
SwiA(config-if)#switchport mode access
SwiA(config-if)#switchport access vlan 4
SwiA(config-if)#switchport port-security maximum 5
SwiA(config-if)#switchport port-security mac-address sticky
SwiA(config-if)#switchport port-security violation shutdown
SwiA(config-if)#exit
SwiA(config)#interface fastEthernet 0/6
SwiA(config-if)#switchport access vlan 4
SwiA(config-if)#switchport port-security maximum 5
SwiA(config-if)#switchport port-security mac-address sticky
SwiA(config-if)#switchport port-security violation shutdown
```

F.3 COMANDOS - ETHERCHANNEL

Esta seção corresponde aos comandos de configuração do Etherchannel, aplicado aos equipamentos da rede apresentada na seção 4.7.

```
SwiA(config)#interface range fastEthernet 0/1-2
SwiA(config-if-range)#channel-group 1 mode on
SwiA(config-if-range)#switchport trunk allowed vlan all
SwiA(config-if-range)#interface range fastEthernet 0/3-4
SwiA(config-if-range)#channel-group 2 mode on
SwiA(config-if-range)#switchport trunk allowed vlan all
SwiA(config-if-range)#switchport trunk native vlan 99
```

```
SwiA(config-if-range)#exit
SwiA(config)#interface port-channel 1
SwiA(config-if)#switchport mode trunk
SwiA(config-if)#switchport trunk native vlan 99
SwiA(config-if)#switchport trunk allowed vlan all
SwiA(config-if)#exit
SwiA(config)#exit
SwiA(config)#interface port-channel 2
SwiA(config-if)#switchport mode trunk
SwiA(config-if)#switchport trunk native vlan 99
SwiA(config-if)#switchport trunk allowed vlan all
SwiA(config-if)#exit
SwiA(config)#exit


SwiB(config)#interface range fastEthernet 0/1-2
SwiB(config-if-range)#channel-group 1 mode on
SwiB(config-if-range)#switchport mode trunk
SwiB(config-if-range)#switchport trunk allowed vlan all
SwiB(config-if-range)#switchport trunk native vlan 99
SwiB(config-if-range)#no shutdown
SwiB(config-if-range)#exit
SwiB(config)#interface port-channel 1
SwiB(config-if)#switchport mode trunk
SwiB(config-if)#switchport trunk native vlan 99
SwiB(config-if)#switchport trunk allowed vlan all
SwiB(config-if)#exit
SwiB(config)#interface range fastEthernet 0/23-24
SwiB(config-if-range)#switchport mode trunk
SwiB(config-if-range)#switchport trunk allowed vlan all
SwiB(config-if-range)#switchport trunk native vlan 99
SwiB(config-if-range)#channel-group 3 mode on
SwiB(config-if-range)#no shutdown
SwiB(config-if-range)#exit
SwiB(config)#interface port-channel 3
```

```
SwiB(config-if)#switchport mode trunk
SwiB(config-if)#switchport trunk allowed vlan all
SwiB(config-if)#switchport trunk native vlan 99
SwiB(config-if)#exit


SwiC(config)#interface range fastEthernet 0/23-24
SwiC(config-if-range)#switchport mode trunk
SwiC(config-if-range)#switchport trunk native vlan 99
SwiC(config-if-range)#switchport trunk allowed vlan all
SwiC(config-if-range)#channel-group 3 mode on
SwiC(config-if-range)#exit
SwiC(config)#interface port-channel 3
SwiC(config-if)#switchport mode trunk
SwiC(config-if)#switchport trunk native vlan 99
SwiC(config-if)#switchport trunk allowed vlan all
SwiC(config-if)#no shut
SwiC(config-if)#exit
SwiC(config)#interface range fastEthernet 0/3-4
SwiC(config-if-range)#switchport mode trunk
SwiC(config-if-range)#switchport trunk allowed vlan all
SwiC(config-if-range)#switchport trunk native vlan 99
SwiC(config-if-range)#no channel-group 3 mode on
SwiC(config-if-range)#channel-group 2 mode on
SwiC(config-if-range)#no shut
SwiC(config)#interface port-channel 2
SwiC(config-if)#switchport mode trunk
SwiC(config-if)#switchport trunk allowed vlan all
SwiC(config-if)#switchport trunk native vlan 99
SwiC(config-if)#no shut
SwiC(config-if)#exit
```

F.4 COMANDOS - STP E LOAD-BALANCING

Esta seção corresponde aos comandos utilizados para a configuração do PVST (STP com Load Balancing) em todos os equipamentos da rede apresentada na seção 4.7.

```
SwiA(config)#spanning-tree mode pvst
SwiA(config)#spanning-tree vlan 4 root primary
SwiA(config)#spanning-tree vlan 3 root secondary


SwiB(config)#spanning-tree mode pvst
SwiB(config)#spanning-tree vlan 3 root primary


SwiC(config)#end
SwiC(config)#spanning-tree mode pvst
SwiC(config)#spanning-tree vlan 4 root secondary
SwiC(config)#exit
```

F.5 COMANDOS - VOIP E QOS

Esta seção corresponde aos comandos utilizados para a configuração de VoIP (Vlan e QoS) em todos os equipamentos da rede. apresentada na seção 4.7.

```
SwiA(config)#interface fastEthernet 0/6
SwiA(config-if)#switchport mode access
SwiA(config-if)#switchport access vlan 4
SwiA(config-if)#switchport voice vlan 2
SwiA(config-if)#exit


SwiB(config)#interface fastEthernet 0/5
SwiB(config-if)#switchport mode access
SwiB(config-if)#switchport access vlan 3
```

```
SwiB(config-if)#switchport voice vlan 2


SwiC(config)#interface fastEthernet 0/13
SwiC(config-if)#no switchport access vlan 2
SwiC(config-if)#switchport mode access
SwiC(config-if)#switchport voice vlan 2
SwiC(config-if)#exit


R1(config)#interface fa 0/0
R1(config-if)#ip address 192.168.0.193
R1(config-if)#no shut
R1(config-if)#end
R1(config)#ip dhcp excluded-address 192.168.0.193
R1(config)#ip dhcp pool DHCP-VoIP
R1(dhcp-config)#network 192.168.0.192 255.255.255.224
R1(dhcp-config)#default-router 192.168.0.193
R1(dhcp-config)#option 150 ip 192.168.0.193
R1(dhcp-config)#end
R1(config)#telephony-service
R1(config-telephony)#max-dn 10
R1(config-telephony)#max-ephones 10
R1(config-telephony)#ip source-address 192.168.0.193 port 2000
R1(config-telephony)#end
R1(config)#ephone-dn 1
R1(config-ephone-dn)#number 54001
R1(config-ephone-dn)#ephone-dn 2
R1(config-ephone-dn)#number 54002
R1(config-ephone-dn)#end
```

F.6 COMANDOS - SWITCH L3

Esta seção corresponde aos comandos utilizados no Switch camada 3, responsável por fazer o roteamento entre as vlans presentes na topologia apresentada na seção 4.7.

```
SwiL3(config)#interface fastEthernet 21
SwiL3(config-if)#no shut
SwiL3(config-if)#no ip address
SwiL3(config-subif)#interface fastEthernet 21.3
SwiL3(config-subif)#encapsulation dot1Q 3
SwiL3(config-subif)#ip address 192.168.0.97 255.255.255.224
SwiL3(config-subif)#exit
SwiL3(config)#interface fastEthernet 21.4
SwiL3(config-subif)#encapsulation dot1Q 4
SwiL3(config-subif)#ip address 192.168.0.65 255.255.255.224
SwiL3(config-subif)#exit
```