UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

DEPARTAMENTO ACADEMICO DE ELETRONICA

ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDE

DIOGO TOMIO YOSHIZAWA

IMPLEMENTAÇÃO DE UMA INFRAESTRUTURA DE REDES DE COMPUTADORES NA EMPRESA FEAD

TRABALHO DE CONCLUSÃO DE CURSO

CURITIBA

2017

DIOGO TOMIO YOSHIZAWA

IMPLEMENTAÇÃO DE UMA INFRAESTRUTURA DE REDES DE COMPUTADORES NA EMPRESA FEAD

Trabalho de Conclusão de Curso de Especialização, apresentado ao Curso de Especialização Semi Presencial em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Fabiano Scriptore de Carvalho

CURITIBA

2017

TERMO DE APROVAÇÃO

IMPLEMENTAÇÃO DE UMA INFRAESTRUTURA DE REDES DE COMPUTADORES NA EMPRESA FEAD

por

DIOGO TOMIO YOSHIZAWA

Esta Monografia foi apresentada em 01 de dezembro de 2017 como requisito parcial para a obtenção do título de Especialista em Gerenciamento de Servidores e Equipamentos de Rede. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Augusto Foronda
Prof. Coordenador do Curso

_____
Fabiano Scriptore de Carvalho
Prof. Orientador

_____
Kleber Kendy Horikawa Nabas
Membro da Banca

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

Dedico este trabalho à minha esposa Carla de Souza por todo o apoio e dedicação empenhado ao nosso relacionamento.

AGRADECIMENTOS

Agradeço ao meu orientador Professor Fabiano Scriptore de Carvalho por toda a ajuda, dedicação e conselhos para que este trabalho pudesse ser concluído.

RESUMO

YOSHIZAWA, Diogo Tomio. **Implementação de uma Infraestrutura de Redes de Computadores na Empresa Fead.** 2017. 32f. Trabalho de Conclusão de Curso de Especialização Semi Presencial em Configuração e Gerenciamento de Servidores e Equipamentos de Rede, Departamento Acadêmico de Informática, Universidade Tecnológica Federal do Paraná, 2017

O presente trabalho foi realizado na infraestrutura de redes de computadores da empresa Fead, objetivando a implementação de melhores práticas do mercado de forma a obter uma rede de computadores melhor gerenciável, minimizando possíveis falhas. Apresenta também um estudo prático de caso da mudança da infraestrutura de redes de computadores da empresa, demonstrando como a rede estava configurada, os problemas enfrentados e analisados. Este trabalho também procurou mostrar alguns aspectos importantes da implementação e dos resultados práticos obtidos após todas as modificações e melhorias propostas e implementadas. Pôde-se ainda analisar algumas documentações criadas para a infraestrutura de redes de computadores, assim como as novas funcionalidades de monitoramento e análise de trafego. Com a execução do trabalho, obteve-se uma melhora na rede de computadores e no seu monitoramento, assegurando melhor desempenho e segurança, com isso mitigando possíveis erros causados por uma má configuração da rede de computadores.

Palavras chave: Infraestrutura, redes, implementação.

ABSTRACT

YOSHIZAWA, Diogo Tomio. **Implementação de uma Infraestrutura de Redes de Computadores na Empresa Fead..** 2017. 31f. Trabalho de Conclusão de Curso de Especialização Semi Presencial em Configuração e Gerenciamento de Servidores e Equipamentos de Rede, Departamento Acadêmico de Informática, Universidade Tecnológica Federal do Paraná, 2017

The present work was performed in a infraestructure of computers network of company Fead, objectifying the implementation of best Market practices in order to obtain a better managed computer network, minimizing possible failures. Also presents a case study a change of infraestructure of computers network of company, demonstrating how the computer network was configured, the problems faced and analyzed. This work also tried to dhow some importants aspects of implementation and the practical results obtained after all modifictaions and improvements proposed and implemented. It was also possible analized some documentation created for the infraestructure od computers network, as well as the new features of traffic monitoring and analysis. With the executation of the work, an improvement in the computer network and in this monitoring was obtained, asuring better performance and security, with this mitigating possible errors caused by a bad configuration of the computer network.

Keywords: Infraestructure, network, implementation.

LISTA DE ILUSTRAÇÔES

LISTA DE TABELAS

LISTA DE ABREVIATURAS, SIGLAS E ACRÔNIMOS

BYOD - Bring Your Own Device

IEEE - Instituto de Engenheiros Eletricistas e Eletrônicos

IoT - Internet of Things

IP - *Internet Protocol*

IRF - *Intelligent Resilient Framework*

ISDN - *Integrated Service Digital Network*

ISO - *International Standard Organization*

ISP - *Internet Service Protocol*

LAN - *Local Area Network*

MAC - *Media Access Control*

MAN - *Metropolitan Area Network*

NTP – *Network Time Protocol*

PA - Posto de Atendimento

PAN - *Personal Area Network*

QoS - *Quality of Service*

STP - *Spanning Tree Protocol*

TI - Tecnologia da Informação

URA - Unidade de Resposta Audível

VoIP - *Voice Over Internet Protocol*

VPN - *Virtual Private Network*

WAN - *Word Area Network*

SUMÁRIO

1 INTRODUÇÃO

1.1 TEMA

A etapa de projeto de redes de computadores pode ser considerada uma das etapas mais importantes para qualquer reestruturação ou para o início de uma rede de computadores. Nesta fase é necessário conhecer todo o ambiente e ter controle sobre o que deve ser entregue a empresa.

O projeto apresentado neste trabalho visa mostrar a reestruturação de rede da sede administrativa da empresa Faculdade Educacional a Distância, neste trabalho denominado FEAD (nome fictício, visto que a empresa estudada em questão não liberou a utilização do nome), sede situada na cidade de Curitiba. A empresa conta em sua sede administrativa com aproximadamente 100 funcionários com expectativa de crescimento em mais de 20% para o próximo ano. O principal objetivo é promover a reestruturação da rede atual por meio da realização de um novo projeto de redes, que tem como principal objetivo a correção de falhas que existem atualmente, disponibilizando segurança, disponibilidade, confiabilidade, integridade e velocidade, auxiliando a área de negócios ao alcance dos resultados esperados.

Para que o projeto de redes seja feito de maneira que agregue valor a empresa, deve-se ter conhecimento sobre a forma de utilização da rede por parte dos colaboradores, os tipos de acessos e aplicativos utilizados, assim como devem ser levados em consideração vários fatores, tais como segurança, disponibilidade da rede, integridade dos dados, tipos de trafego que a rede irá suportar, aplicações e sistemas que serão acessados, quantidade de funcionários da empresa dentre outras variáveis.

Como resultado esperado deste projeto estão a padronização dos equipamentos e das configurações dos mesmos, a documentação do projeto, com todas as informações sobre os equipamentos de rede e suas interligações, um mapa de como a rede ficará após a sua implementação. Todas essas melhorias têm por finalidade deixar a rede documentada para que seja mais fácil e ágil qualquer intervenção que seja necessário efetuar no futuro.

1.2 DELIMITAÇÃO DO ESTUDO

O estudo de caso foi realizado na sede administrativa da empresa Fead no período de agosto/2017 a novembro/12017. Apesar da empresa contar com mais sedes, como uma produtora de vídeo, um pólo onde os alunos vão para a realização de provas e *workshops*, e mais uma filial, situada na cidade da Lapa/PR, o estudo focou na sede administrativa, por ser a maior sede e por ser a centralizadora de conexões com as outras filiais, sendo considerada a controladora, onde estão o maior número de colaboradores e os principais serviços.

1.3 PROBLEMA

O estudo de caso foi realizado na sede administrativa da empresa Fead no período de agosto/2017 a novembro/12017. A empresa possui atualmente aproximadamente 100 funcionários em sua sede administrativa e prevê crescimento de até 25% para os próximos 18 meses. A sede conta com os seguintes setores: administrativo (7 colaboradores), Ti Desenvolvimento (12 colaboradores), Ti Infraestrutura (7 colaboradores), Financeiro e Contábil (17 colaboradores), Desenvolvimento Humano (10 colaboradores), Recrutamento e Seleção (5 colaboradores), Comercial (5 colaboradores), Marketing (13 colaboradores), Projetos (5 colaboradores), Gestão de Rede de Negócios (5 pessoas) e Call center (15 pessoas).

Ao analisar a rede da empresa, foram encontrados alguns pontos críticos que comprometiam o bom funcionamento da rede de computadores, levando a alguns momentos de lentidão, mau funcionamento de algumas aplicações, relatos de usuários de telefonia (VoIP) que reclamavam que em alguns momentos a voz apresentava robotizada, e até mesmo queda das ligações. Dentre os problemas encontrados podemos exemplificar alguns:

- *Spanning Tree Protocol* (STP) configurado indevidamente que pode gerar *loop* ou descontinuidade da rede;

- Políticas de controle de trafego que podem estar provocando o descarte dos pacotes na rede;
- Falta de documentação atualizada que possa indicar a identificação dos equipamentos e suas conexões;
- Falta de gerência em alguns equipamentos;
- Firmwares dos switches desatualizadas;
- Falta de redundância.

Todos esses problemas encontrados poderiam prejudicar o resultado da empresa, pois se algum equipamento apresentasse problemas, não havia nenhum plano de contingência, o que poderia causar a paralisação total do acesso a rede de computadores.

1.4 JUSTIFICATIVA

Independente do grau de complexidade e do tamanho, o objetivo principal de uma rede de computadores é garantir que todos os recursos, informações e dispositivos sejam compartilhados de forma segura, com disponibilidade, integridade e confiabilidade dos dados. Para que isso ocorra são necessários estudos para o entendimento de como a rede de computadores está nos dias atuais e como é o desejado pela empresa, com todas as suas regras e particularidades, seguindo do pressuposto que toda a mudança deve ocorrer no intervalo de 3 dias corridos.

1.5 OBJETIVOS

1.5.1 Objetivo Geral

Implementar uma estrutura de redes da empresa, levando em consideração os aspectos de disponibilidade, confiabilidade, segurança e integridade das informações para uma melhor infraestrutura de redes.

1.5.2 Objetivos Específicos

- Realizar a análise da rede de computadores e documentar toda a parte física e lógica da rede de computadores;
- Planejar previamente para a mudança de sede para que o impacto na mudança seja o menor possível;
- Verificar e implementar melhorias para a nova estrutura, analisando, identificando e corrigindo possíveis falhas;
- Monitorar os enlaces e ativos de rede de forma gráfica e em tempo real.

1.6 PROCEDIMENTOS METODOLÓGICOS

Este trabalho foi desenvolvido por meio de algumas etapas que incluíram o levantamento e coleta das informações dentro da empresa, no estudo com os funcionários da empresa e nas melhores práticas de mercado para aplicar as transformações.

A análise e conclusão do estudo se dará baseado nos métodos e conceitos apresentados no referencial teórico, nas melhores práticas do mercado e em pesquisas na literatura atual.

1.7 ESTRUTURA DO TRABALHO

Este trabalho está organizado em quatro capítulos. No primeiro capítulo são abordados o tema, justificativa, objetivos e métodos da pesquisa, sendo discutido o motivo do estudo. No segundo foi descrito a fundamentação teórica, onde são abordados temas relevantes para o trabalho como arquitetura de redes, equipamentos de rede, roteamento, ISO, VLANs, QoS entre outros e a análise da rede da empresa anteriores alterações propostas neste trabalho. No capítulo seguinte são abordados o desenvolvimento do trabalho, e as novas ferramentas de análise e de monitoramento da infraestrutura de redes da empresa, com a apresentação e a análise dos

resultados. Para finalizar, no quarto capítulo são apresentadas as considerações finais referentes a esse trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 REDES DE COMPUTADORES

Este item irá apresentar uma visão geral sobre a estrutura de redes de Computadores. A infraestrutura de redes de computadores sempre foram e ainda é a base para que toda a Tecnologia da Informação de uma empresa tenha um desempenho adequado. Uma definição de redes de computadores pode ser apresentada como dois ou mais computadores interligados, trocando informações e compartilhando recursos físicos e lógicos entre si. Segundo Miranda (2008), rede de computadores é um conjunto de computadores interligados entre si de maneira a possibilitar a comunicação de dados local ou remoto, incluindo todos os equipamentos eletrônicos necessários a interconexão. Esses dispositivos são chamados de nós, estação de trabalho ou também de dispositivos de rede. Bastariam apenas dois comutadores ou nós para formarmos uma rede. O número máximo não é predeterminado, porque teoricamente todos os computadores do mundo poderiam ser interligados. Para isso chamamos de Internet.

Ainda segundo Miranda, o principal objetivo das redes de computadores é tornar disponível aos usuários os programas dados e outros recursos, proporcionando maior confiabilidade e disponibilidade dos recursos. Podemos citar como exemplo de uma rede de computadores a Internet, uma rede doméstica ou a Intranet de uma empresa.

2.2 TIPOS DE REDES DE COMPUTADORES

As Redes de computadores podem ser classificadas seguindo diversos critérios, entre eles Dimensão da Rede (redes Pessoais, redes locais, redes metropolitanas), Topologia (estrela, anel, *bus*). A seguir será analisada as redes conforme a sua dimensão. Pode-se classificá-las em quatro classes de rede.

2.2.1 PAN - Personal Area Network

O conceito de PAN (*Personal Area Network*) ou Rede de Área Pessoal, são redes de curta distância, constituída de uma rede de computadores com nós muito próximos uns dos outros. Um exemplo de uma PAN são dois *notebooks* dentro de um ambiente compartilhando a mesma impressora, utilizando o frequências de rádio ou raios infravermelhos para efetuar a troca de informações entre eles.

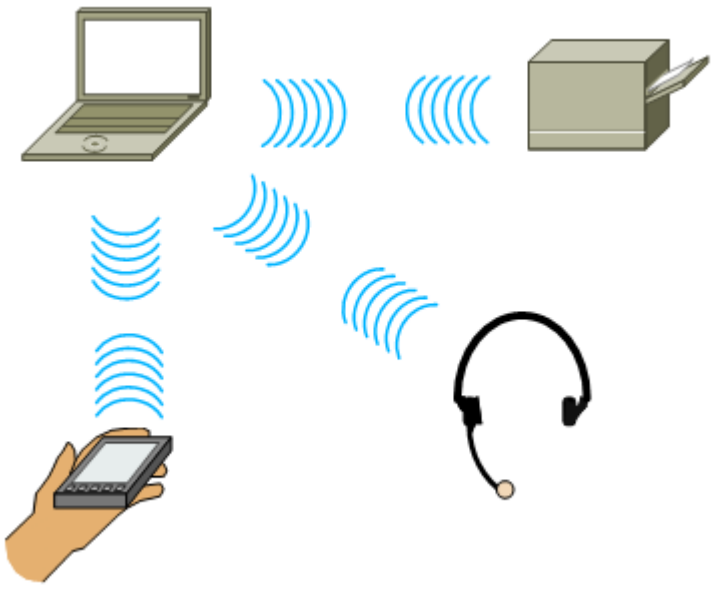

Figura 1: PAN – Personal Area Network
Fonte: LAWRENCE

2.2.2 LAN - Local Area Network

O conceito de LAN (*Local Area Network*) ou Rede Local de Computadores, geralmente é composta por vários computadores conectados entre si, por meio de dispositivos como placas de redes, *switches*, entre outros, possibilitando o compartilhamento de recursos e a troca de informações. A limitação geográfica de uma LAN faz com que elas sejam utilizadas em escritórios, empresas, escolas, entre outros locais.

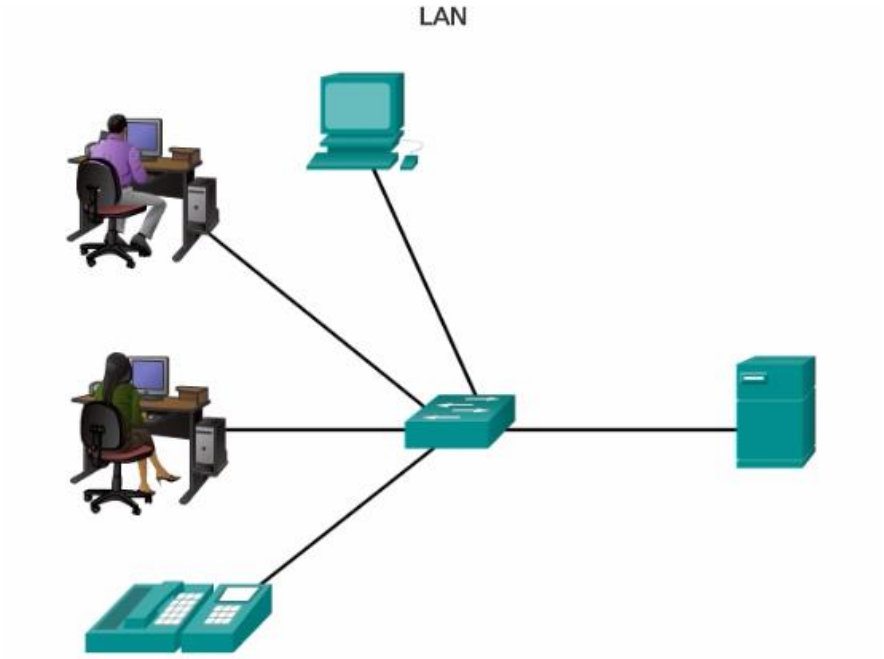

Figura 2: LAN – *Local Area Network*
FONTE*: *Cisco Networking Academy

2.2.3 MAN - Metropolitan Area Network

O conceito de MAN (*Metropolitan Area Network*) ou Rede de Área Metropolitana, é a rede de computadores que corresponde um espaço de grande dimensão como uma cidade, uma região ou um campus. Normalmente uma MAN conecta várias LANs. As redes ISP (*Internet Service Protocol*) ou provedor de serviço de internet, ou seja, um provedor que fornece acesso à internet é um exemplo de uma MAN.

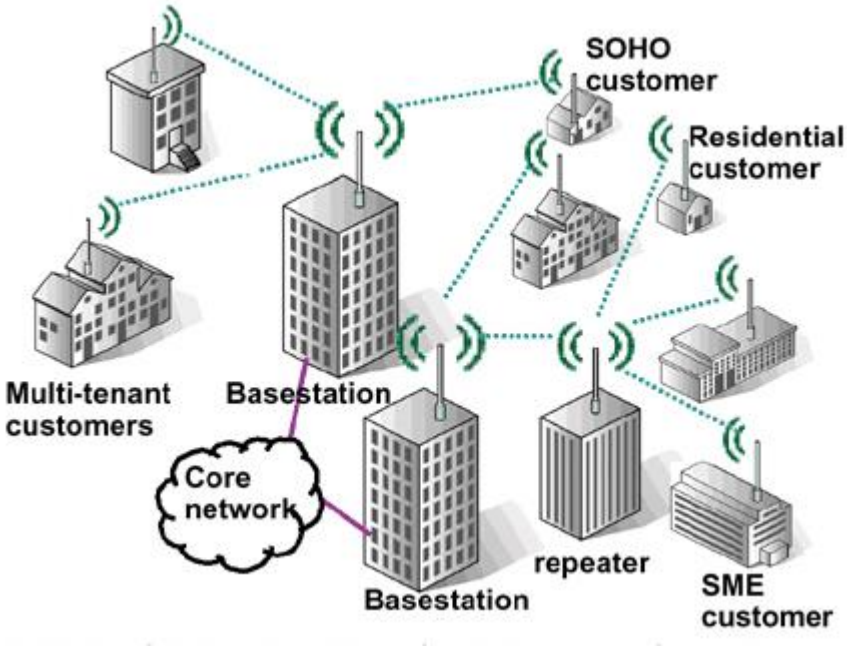

Figura 3: MAN – *Metropolitan Area Network*
Fonte: Imagem da internet [1]

2.2.4 WAN - Wide Area Network

O conceito de WAN (*Wide Area Network*), ou rede de longa distância, são as redes de computadores que abrange uma grande área geográfica, como um pais, um continente.

Figura 4: WAN - *Word Area Networkig*
Fonte: Cisco Networking Academy

2.3 ARQUITETURA DE REDES

No início da popularização das redes de computadores, cada fabricante entregava o seu componente e o protocolo de comunicação não seguiam nenhum padrão pré-estabelecido. O conceito de WAN (*Wide Area Network*), ou rede de longa distância, são as redes de computadores que abrange uma grande área geográfica, como um pais, um continente.

2.4 ROTEAMENTO

Segundo OLIVEIRA (2012), Roteamento é o nome dado ao processo de escolha do caminho a ser seguido pelos dados a serem transmitidos uma rede espalhada geograficamente. Ainda segundo OLIVEIRA (2012), nas redes de datagrama, incluindo as redes IP, o roteamento é tratado pacote a pacote. O protocolo IP, com sua simplicidade e flexibilidade possui grande sucesso na função do roteamento, sendo este protocolo responsável pela entrega das informações geradas pelas aplicações aos seus destinos de forma correta e eficiente.

2.5 VOIP (*VOICE OVER INTERNET PROTOCOL*)

VoIP (*Voice over Internet Protocol* ou Voz Sobre Protocolo de Internet) é uma tecnologia que permite que chamadas telefônicas sejam feitas por meio de uma rede comutada por pacotes, no lugar dos serviços de telefonia convencionais. Para KELLER (2010), a utilização maciça da Internet instigou o surgimento de várias tecnologias, muitas vezes substituindo algumas já existentes, como no caso do VoIP. O VoiP é um protocolo de rede, isto é, trata-se de normas e regras implementadas para que a voz saia de uma origem, seja dividida em pacotes, trafegue por rede de dados através do TCP/IP, chegue ao destino e os pacotes sejam reorganizados, reconstruindo a voz para que esta seja reproduzida no destino. Com a ampliação das velocidades de acesso à Internet, o VoIP passou a fazer parte do dia a dia das grandes empresas, com o principal objetivo de reduzir os custos com a telefonia.

Dentre os benefícios da utilização de VoIP, pode-se citar:

- Redução de Custo;
- Mobilidade;
- Infraestrutura única;
- Controle do sistema de telefonia;
- Novas funcionalidades.

2.6 QOS (*QUALITY OF SERVICE*)

QoS (*Quality of Service*) é uma técnica diretamente relacionada ao trafego de dados. É o responsável por controlar o trafego de uma rede de computadores, definindo limites e prioridades com o intuito de melhorar o uso dos serviços, assim como utilizá-lo de forma mais eficiente possível. Ele também permite a garantia de largura de banda e prioridade.

Os diferentes fluxos de dados, provenientes de diversos pontos da rede, compartilham entre si a mesma banda de dados disponível. Caso ocorra algum congestionamento, os pacotes de dados serão descartados sem nenhum filtro.

Segundo GIMENES (2003), as redes IPs sempre utilizaram um serviço de menor esforço (*best effort)*. Para este tipo de serviço, não existe nenhum tipo de reserva ou garantia para qualquer tipo de trafego de rede.

O principal objetivo da aplicação de Qualidade de Serviço (QoS) é minimizar os efeitos dos congestionamentos de enlaces para otimizar as aplicações trafegadas pela rede de computadores.

Para PINHEIRO (2004), QoS de uma rede é garantida pelos equipamentos utilizados na rede de computadores, que deve atuar na comunicação dos equipamentos envolvidos. Ainda segundo Pinheiro, QoS é um aspecto de implantação e operação importante para as redes de computadores, tornando um aspecto operacional importante para o desempenho fim-a-fim.

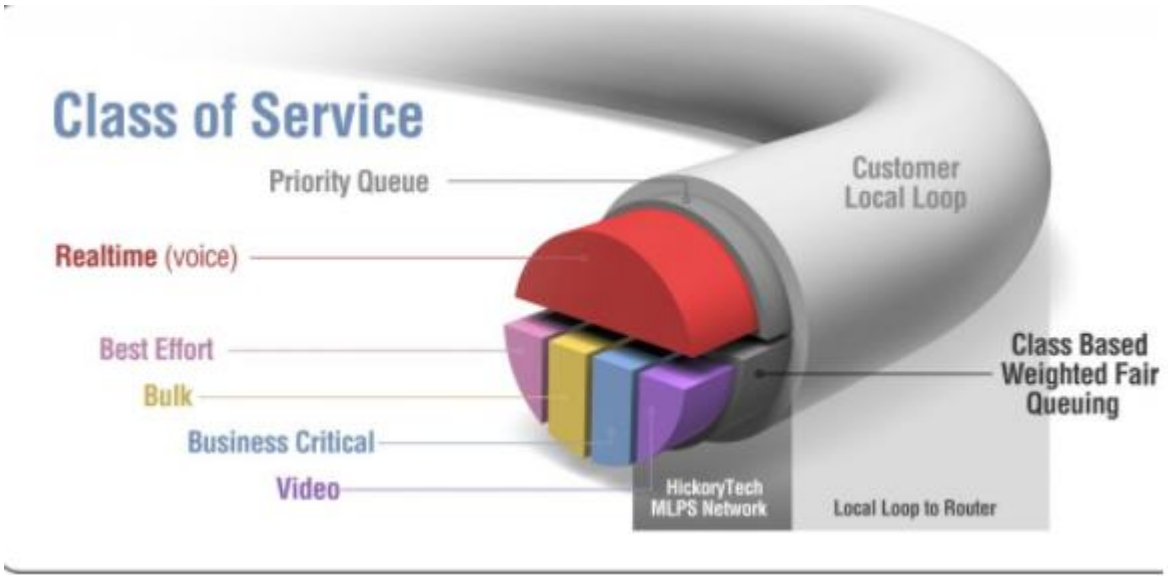

Figura 5: Ilustrando QoS na rede
FONTE: Imagem da Internet [2]

2.7 FIREWALL

Firewall é um sistema do qual trafega o trafego entre duas redes de computadores distintas, permitindo a aplicação de regras de segurança que defina o que pode ou não ser acessado ou o que pode ou não passar de uma rede a outra. Um *firewall* pode ser um *hardware*, um *software* ou ambos. Segundo a CISCO (2017), um *firewall* é um dispositivo de segurança da rede que monitora o trafego de entrada e saída da rede e permite ou bloqueia tráfegos específicos de acordo com um conjunto definido de regras de segurança.

Segundo CHESWICK, STEVEBELLOVIN (2011), *Firewall* é um ponto entre duas ou mais redes no qual circula todo o trafego. A partir desse trafego, é possível controlar e autenticar o trafego, além de registrar por meio de *logs* todo o tráfego da rede, auxiliando a sua auditoria. É um dos maiores desafios para *hackers*, pois se o mesmo conseguir acessá-lo, pode alterar suas permissões e alcançar o bem mais valioso das empresas – a informação.

Para TANEMBAUM (2003), fazendo uma analogia, da mesma forma que os medievais construíam muros e fossos profundos em torno dos seus castelos, forçando quem quisesse entrar ser revistado, ao passar por uma ponte levadiça, o *firewall*

analisa os pacotes que entram e saem, para que sejam descartados os pacotes que possam fazer algum tipo de ameaça a segurança da rede.

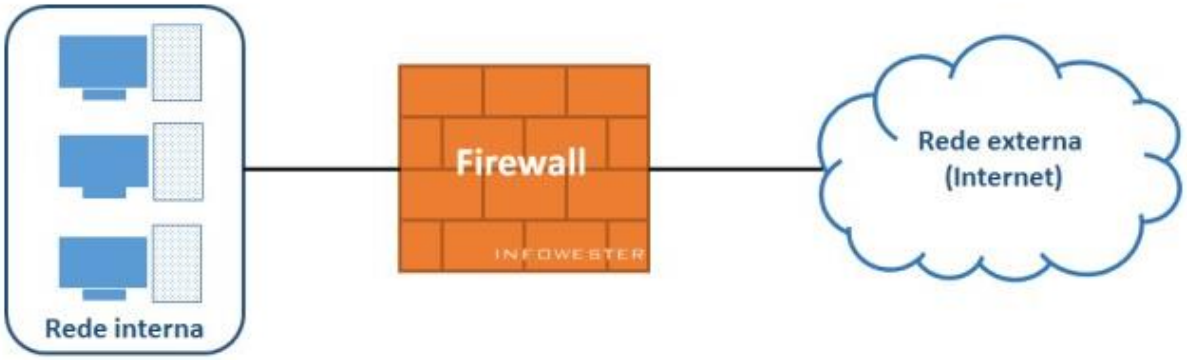

Figura 6: Imagem básica de um *Firewall*
Fonte: ALECRIM

2.8 WIRELESS

Atualmente, a rede sem fio (*Wireless*) está bastante disseminada, chegando em muitos casos a ultrapassar a rede cabeada na quantidade de dispositivos conectados, e o número de dispositivos que se conectam à rede sem fio só tende a aumentar. IoT (*Internet of Things*) e BYOD (*Bring Your Own Device*) são duas tendências que comprovam que as redes sem fio irão superar em número de dispositivos conectados as redes cabeadas.

Segundo ENGST e FLEISHMAN (2005), A primeira rede sem fio foi desenvolvida no Havaí para a conexão entre quatro ilhas sem a utilização de cabos. Na década de 1980 iniciou a ideia de compartilhamento de dados pela rede sem a utilização de cabos. As primeiras redes sem fio utilizavam o infravermelho como como forma de conexão entre os dispositivos. A partir da década de 90, as redes sem fio começaram a utilizar as ondas de rádio, porém com vários problemas referentes a custos e compatibilidade. No fim da mesma década, foi criado pelo IEEE o novo padrão de rede sem fio, chamado de IEEE 802.11 e ficou evidente que a tecnologia poderia ser muito explorada.

De acordo com TORRES (2009), existem várias tecnologias para montar uma rede sem fio, e o padrão 802.11 é o mais popular, também conhecido como Wi-fi, porém 802.11 e Wi-fi não são a mesma coisa. Wi-fi é uma marca registrada da Aliança Wi-fi, um grupo formado por vários fabricantes. Para que um equipamento seja chamado de wi-fi, ele obrigatoriamente tem que passar pelo crivo desse grupo para poder utilizar o nome. Todo equipamento wi-fi é 802.11, porém nem todo equipamento 802.11 é wi-fi. Na Apple por exemplo, 802.11 é chamado de AirPort. Na prática, porém todos utilizam o termo Wi-fi, IEEE 802.11, *Wireless* e Sem Fio como sinônimo.

2.9 VLAN

VLAN (*Virtual Local Area Network*) é uma rede local virtual, uma rede lógica onde é possível agrupar várias máquinas de acordo com vários critérios. Elas permitem a segmentação da rede física, e a comunicação entre equipamentos de rede em diferentes VLANs deverá passar obrigatoriamente por um roteador ou outro equipamento capaz de realizar o encaminhamento de pacotes entre VLANs.

Segundo a CISCO (2017), As VLANs são baseadas em conexões lógicas e não fiscais e fornecem segmentação e flexibilidade, oferecendo uma maneira de agrupar dispositivos dentro de uma LAN. Elas permitem segmentar as redes baseadas em fatores como a função, a equipe ou o projeto, independentemente da localização física do usuário ou dispositivo. Cada VLAN é considerada uma rede lógica separada e os pacotes destinados as estações que não pertencem a VLAN devem ser enviados através de um dispositivo que suporte para esse roteamento. Uma VLAN cria um domínio lógico de broadcast que pode abranger vários segmentos de LAN. As VLANS melhoram o desempenho da rede separando grandes domínios de broadcast em menores. Permitem também a implantação de políticas de acesso e segurança de acordo com grupos específicos de usuários.

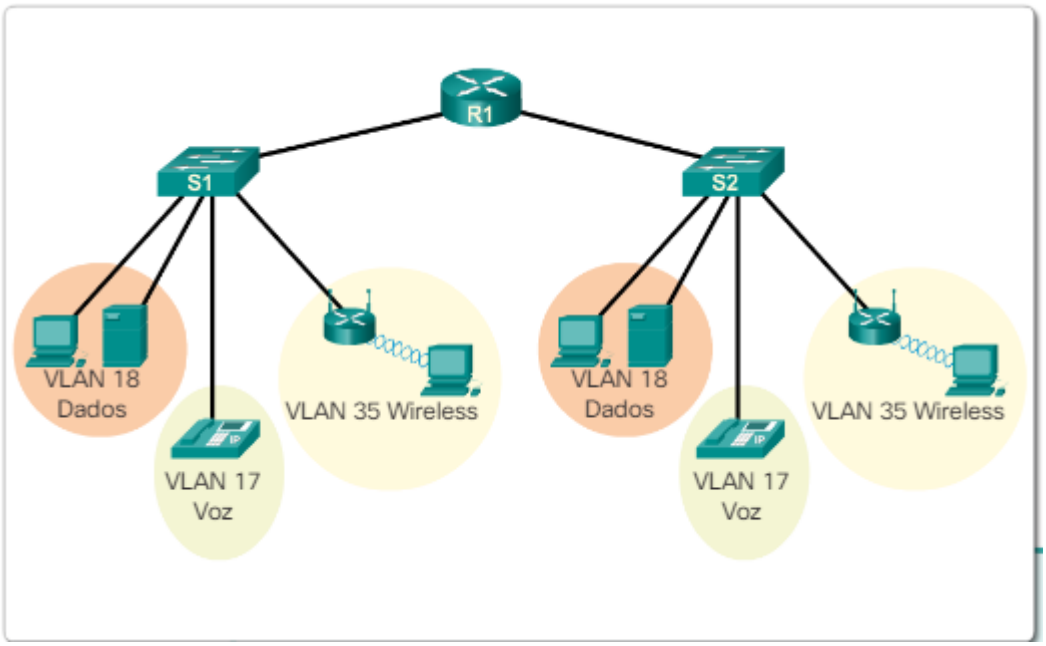

Figura 7. Exemplo de VLANs.
Fonte: CISCO

2.10 VPN

Muitas empresas dispõem de escritórios e filiais espalhadas pela cidade ou muitas vezes pelo país ou pelo mundo. Antigamente era comum as empresas arrendarem as linhas dedicadas das empresas de telefonia para criar uma rede privada. Essas redes funcionam muito bem e são muito seguras, porém tem um custo elevado para o aluguel. Com a popularização da Internet muitas empresas mudaram para enviar o tráfego de dados para a rede pública (Internet) mas sem descuidar da segurança dos dados. Essa demanda levou a criação das VPN (*Virtual Private Networks*), que são redes sobrepostas as redes públicas. São criados tuneis virtuais pela internet, fornecendo integridade e segurança para os dados trafegados.

2.11 MONITORAMENTO

Segundo Filho, A dependência das redes e da infraestrutura de tecnologia da informação aumentam a medida que as aplicações e os serviços evoluem e se tornam mais complexos mais largura de banda é necessário para manter o bom desempenho desses serviços. Identificar o perfil de trafego, a tendência e o comportamento destes ambientes são vitais para garantir do desempenho. Deixar de monitorar os seus principais parâmetros de desempenho, pode significar muitas perdas e prejuízos. Por esse motivo. Gerenciar e monitorar essas redes tornaram-se imprescindíveis, pois mais importante que saber quais os problemas que estão relacionados a rede, é conhecer o impacto deles nos lucros das empresas.

As cinco áreas da gerencia de redes conhecidas como FCAPS são:

- Gerência de falhas: realiza a detecção, isolamento, notificação e correção em softwares e hardwares encontrados na rede;
- Gerência de configuração: responsável pelo registro e manutenção dos parâmetros de configuração dos serviços de rede;
- Gerência de contabilidade: responsável pelo registro do uso da rede de computadores pelos usuários;
- Gerência de desempenho: responsável pela medição e disponibilização das informações de desempenho;
- Gerência de segurança: responsável pela proteção do acesso a rede evitando que usuário utilizem a rede de maneira prejudicial, intencional ou não;

2.12 SEGURANÇA

Não se pode falar em projeto de redes de computadores sem tocar no assunto segurança. Segundo TANEMBAUM (2003), no início da história das redes de computadores, a sua utilização foi principalmente utilizada por pesquisadores universitários, com o propósito de enviar mensagens e para empresas para o compartilhamento de impressoras. Sob essa ótica, segurança nunca foi um problema.

Ainda segundo TANEMBAUM (2003), a maioria dos problemas de segurança são causados intencionalmente por pessoas maliciosas que tentam obter algum tipo de benefício ou prejudicar alguém.

De acordo com SILVA (2003), os pontos principais para a implementação da segurança da informação em redes de computadores devem seguir os cinco princípios básicos:

- Relação custo X benefício, garantir os investimentos necessários para a implementação e manutenção de segurança da informação, e o retorno que proporciona a prevenção e a proteção das informações;
- Princípio da concentração, possibilidade de administrar as medidas necessárias de segurança da informação para atender medidas necessárias de segurança da informação;
- Princípio da proteção em profundidade, proteção de segurança física e lógica como câmeras de segurança, biometria, fechaduras, salas hermeticamente fechadas;
- Princípio da consistência, as medidas de proteção das informações possuam um nível para que reduzam as falhas dos programas de segurança de informação e o princípio da redundância, que prega a medida de se adotar mais de uma forma de proteção da informação.

A ISO 27002 (2006) indica que a informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Definir, alcançar, manter e melhorar a segurança da informação devem ser atividades essenciais para assegurar a competitividade e a imagem da organização. Ainda de acordo com a ISO, a segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e procedimentos apropriados.

2.13 SWITCH

Switches são equipamentos de rede utilizados para a interconexão e informações entre duas ou mais estações de trabalho de uma estrutura de redes de computadores. Pode ocupar a função central de uma rede, realizando a

conexão entre várias maquinas numa LAN. *Switches* normalmente possuem um recurso chamado VLANs, que basicamente faz a separação da das portas físicas conectadas ao mesmo *switch* formando domínios de broadcast diferentes, o que reduz problemas na rede.

Para FOROUZA (2006), os *switches*, também chamados de comutadores, podem ser divididos em dois grupos: os *switches* de camada 2, que operam na camada física e enlace e os *switches* de camada 3, utilizados na camada de rede, realizando o roteamento de pacotes.

A principal função de um switch é conectar diferentes segmentos de rede. O *switch* aprende quais estações estão conectadas em cada porta, examina o trafego de entrada, traduz os endereços MAC de todas as estações conectadas em suas portas e utiliza essas informações para construir sua tabela de roteamento local. Desta forma, quando recebe um pacote, ele determina qual o destino e qual a origem, encaminhando o pacote para a porta correta.

Os métodos de comutação dos *switches* são:

- *store and forward*: Este método recebe e analisa todo o pacote antes de encaminhá-lo para a porta de saída, guardando todo quadro em um *buffer.* Este método permite a detecção de erro, evitando sua propagação pela rede;
- *cut through:* Esse método apenas examina o endereço de destino e encaminha o pacote, reduzindo dessa forma a latência, e diminuindo o atraso na entrega dos pacotes. Este método não detecta erros.
- *fragment free*: Mesma funcionalidade do *cut through* porém examina os primeiros 64 bytes de cada pacote, assegurando que o quadro tenha pelo menos o tamanho mínimo, evitando o encaminhamento de pacotes corrompidos.

2.14 STP (*SPANNING TREE PROTOCOL*)

O STP é um protocolo implementado na camada 2 do modelo OSI e seu objetivo é analisar a topologia de rede, descobrir possíveis *loopings* e por meio de eleições interromper esse *loopings* evitando problemas de rede.

O protocolo *Spanning Tree* desobriga o administrador da rede de qualquer configuração manual durante a operação da rede. Novos equipamentos podem ser inseridos, mesmo com a rede em funcionamento, que o protocolo irá reconfigurar a rede de modo a garantir a unicidade de caminhos entre a origem e o destino (TANEMBAUM, 2006).

O protocolo STP deve estar habilitado em todos os *switches* que compõe a rede para que o problema não ocorra, somente dessa forma é possível garantir que não ocorra loopings na rede. Caso o STP descubra que existam caminhos redundantes dentro da rede, ele executará um processo de eleição onde irá eleger um dos switches como primário e após essa etapa irá bloquear os demais, desabilitando as portas associadas ao caminho que foi bloqueado.

3 PROJETO DE RESTRUTURAÇÃO DA REDE DE COMPUTADORES

O projeto desenvolvido tem a finalidade de demonstrar e auxiliar na configuração, reparos e ampliações da estrutura da rede de dados da empresa citada. Como todo projeto, esse também tem uma duração determinada, não é repetitivo, sendo único e visa a atender objetivos pré-estabelecidos que foram discutidos com gerentes de áreas, diretores e usuários finais.

A empresa, antes da restruturação situava-se em um prédio antigo, onde melhorias na parte estrutural era muito difícil, tanto por motivos estruturais quanto por encontrar na diretoria grande voz contrária a qualquer tipo de investimento na área. Outra situação que verificamos foi o rápido crescimento da empresa, sem que fosse dada todas as condições para que a equipe responsável atualizasse a rede de computadores de forma organizada, o que gerou um quadro que acontece em muitas empresas.

Rápido crescimento, falta de controle na rede e no final vários problemas que poderíamos verificar na rede. Dentre eles podemos citar: falta de segurança, tanto física (acesso a sala de *datacenter* e outros equipamentos sem a segurança adequada) quanto lógica (várias VLANs criadas, a maioria sem documentação, vários equipamentos sem senha de acesso ou senhas muito fracas, total descontrole sobre a interligação dos equipamentos, falta de documentação

adequada informando sobre os dispositivos de rede, suas ligações e configurações).

Por todos esses motivos, no momento que a empresa decidiu realizar a mudança da sua sede, foi discutido e levantado a necessidade de um projeto e implementação do projeto de redes para que todos os requisitos de melhor prática do mercado fossem seguidos.

3.1 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Neste capitulo a proposta é analisar e apresentar uma visão geral da infraestrutura da rede de computadores da empresa após a mudança da sua sede administrativa. Serão apresentados alguns dos principais equipamentos que fazem parte da rede de computadores, assim como os principais documentos gerados após a implementação.

Por padrão, todos os *switches* que fazem parte da rede de computadores são da marca HP, sendo 2 HPE 5130 24G, que são os *switches core* da rede, 3 *Switches* HPE 5130 48G, que são switches de acesso para as áreas mais sensíveis as oscilações da rede, como o *call center* e o financeiro, 3 HPE 24G 1920, que são switches de acesso e dois *switches* HPE 1950 24G, que são utilizados uma para a telefonia e outro para serviços.

Como *Firewall* foi implementada a solução Cisco Meraki MX 100 com alta disponibilidade e redundância. A configuração e monitoramento do *Firewall* é realizado pela *cloud*, o que facilita em muitos casos. Na imagem a seguir é possível verificar que a rede em questão é referente ao FW-ESTAÇÃO, o gráfico com o monitoramento de uso da rede das últimas 24 horas, assim como os clientes que mais utilizaram a rede.

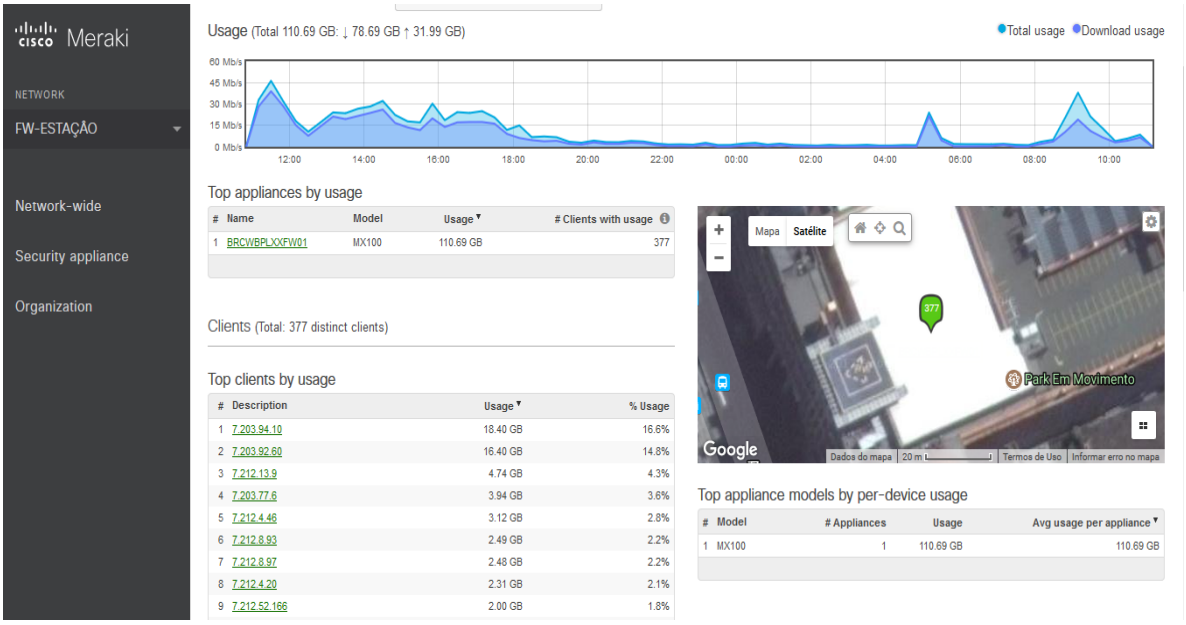

Figura 8: Cisco Meraki
Fonte: Autoria Própria

Nas filiais Castro Alves e Lapa também foram implementados a solução Cisco Meraki MX 84. Como pode ser visualizado na figura a seguir, o gerenciamento ocorre no mesmo painel, sendo necessário apenas selecionar a rede que deverá ser gerenciada.

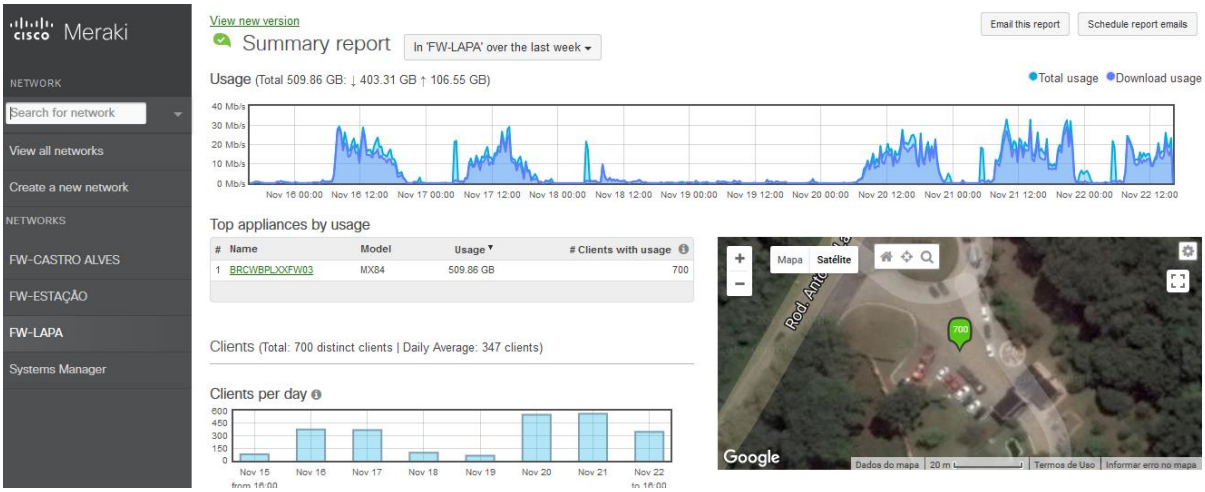

Figura 9. Cisco Meraki
Fonte: Autoria Própria

Os enlaces de dados contratados para essa nova sede são dois IPS dedicados, o principal da Algar Telecom de 60 Mbps e o secundário da Copel de 15 Mbps. Não é utilizado o balanceamento dos enlaces, sendo o secundário utilizado apenas em caso de falha do enlace principal. O *Firewall* está configurado para que caso o enlace principal esteja indisponível, o enlace secundário assumirá a função sem nenhuma intervenção e transparente para o usuário.

Conforme podemos verificar na imagem a seguir, os equipamentos *core* da rede de computadores estão em redundância para garantir alta disponibilidade todo o tempo.

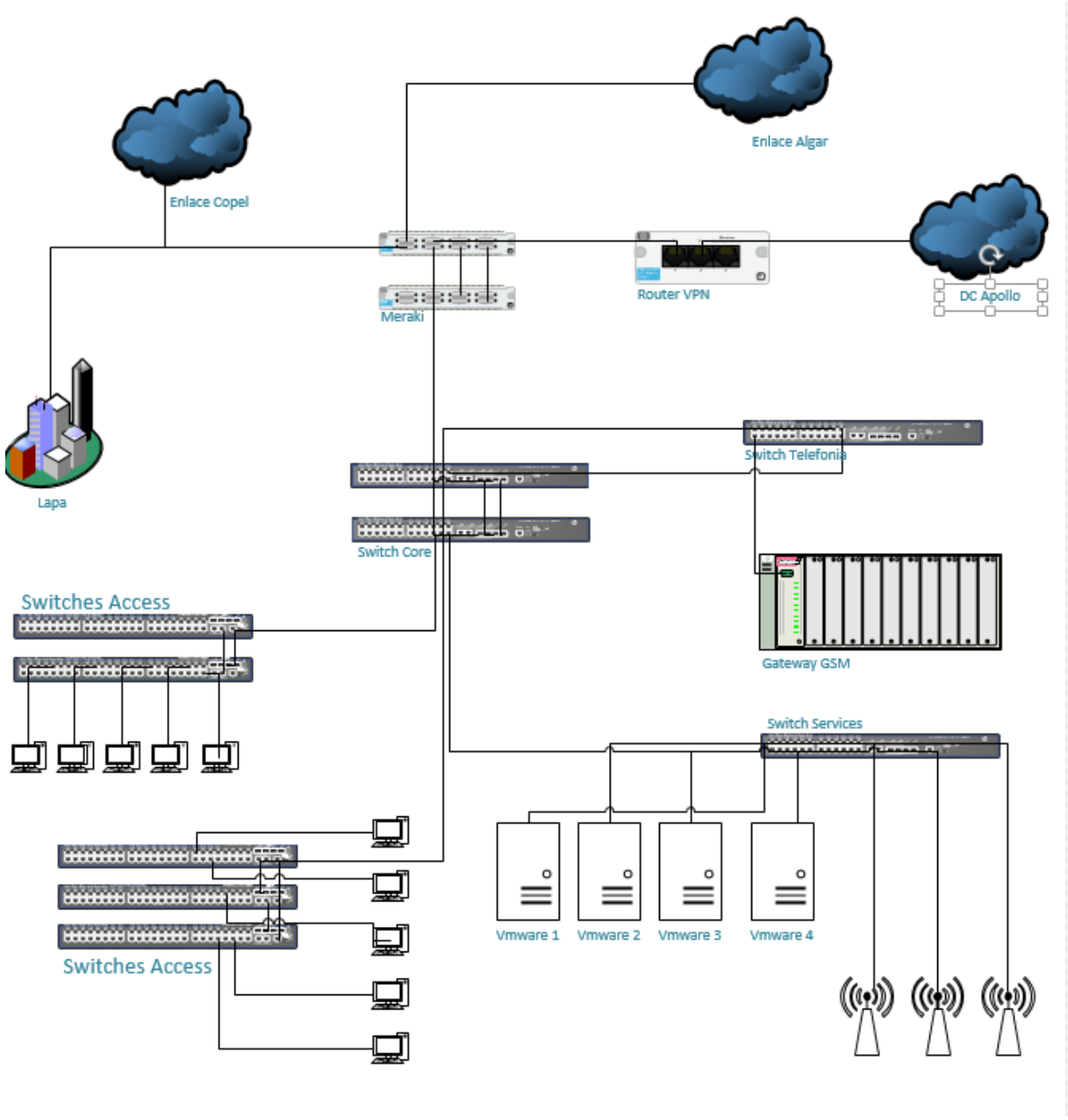

Figura 10: Mapa de rede
Fonte: Autoria Própria

A alta disponibilidade também está sendo implementado nas centrais telefônicas. Ao todo a empresa mantém 3 centrais telefônicas, situadas na cidade de Uberlândia (*host* alugado pela operadora Algar), na cidade da Lapa onde encontra-se um *call center* com 50 PAs e um na cidade de Curitiba, onde encontra-se a sede administrativa e um *call center* com 10 PAs. A empresa possui dois 0800, um para atendimento a alunos e assistentes acadêmicos e outro para o comercial. Todas as ligações para o 0800 da empresa chegam em Uberlândia,

passa pela URA e é encaminhado para a sua fila (Curitiba ou Lapa). Será implementado um data center na cidade de Campinas (SP). Com os dois data centers em cidades diferentes, cada cidade receberá a ligação de 0800 e encaminhará para a fila selecionada. Os dois data centers serão redundantes, ou seja, caso o 0800 que esteja na cidade de Uberlândia (MG) apresente alguma falha, automaticamente as ligações serão encaminhadas para Campinas (SP), assim como caso ocorra o problema no outro data center.

.

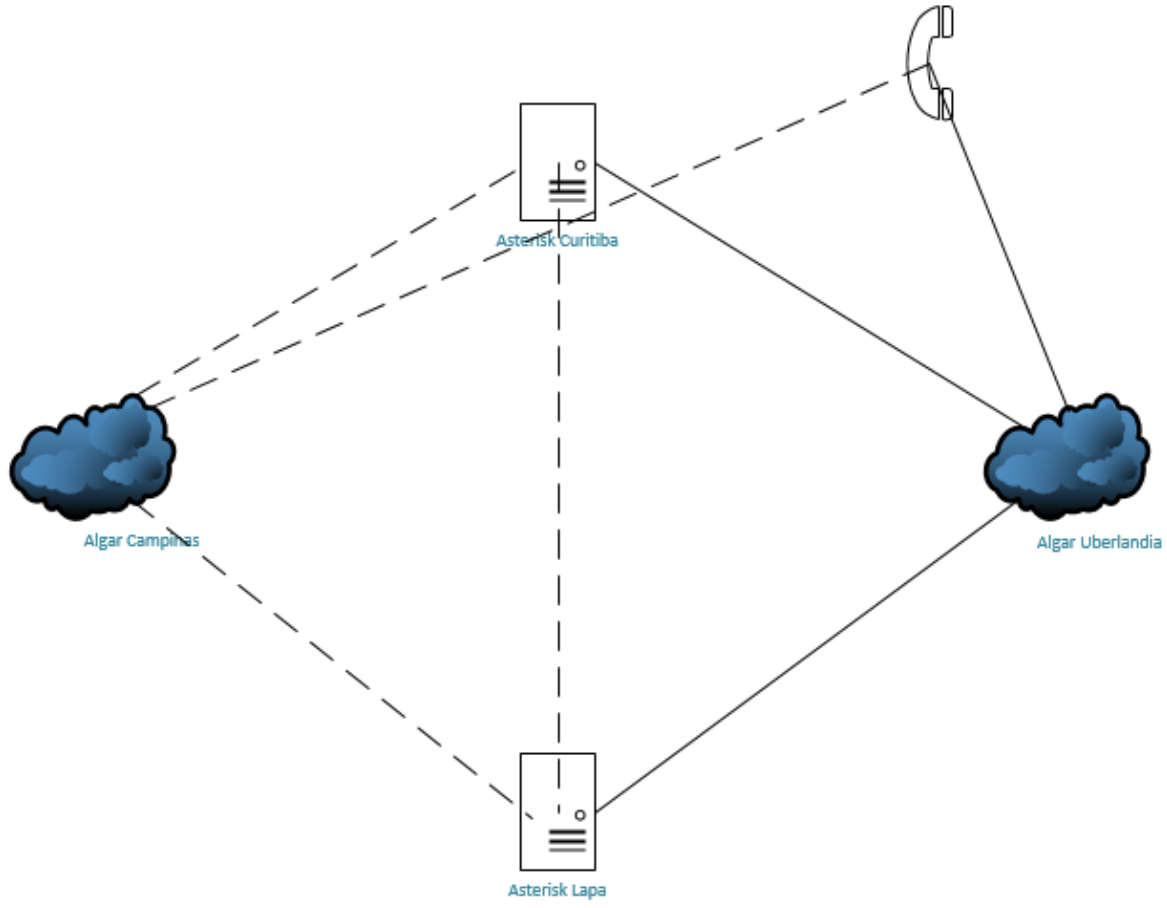

Figura 11. Demonstra de forma simples a redundância dos enlaces para recebimento de chamada do 0800
Fonte: Autoria Própria.

Foram alteradas também o escopo das *VLANs*, de forma a garantir mais segurança e priorizar alguns serviços como a telefonia IP. A seguir podemos verificar a lista de *VLANs* e suas descrições.

Tabela1. Lista das Vlans criadas.

VLAN	Nome	Range
100	Voice LAN	7.212.0.0-7.212.1.255
200	Staff LAN	7.212.4.0-7.212.4.255
300	Staff Wireless	7.212.8.0-7.212.9.255
350	Guest Wireless	7.220.8.0-7.220.13.255
50	Voice Services	7.212.12.0-7.212.12.127
901	Wireless Services	7.212.12.128-7.212.12.255
500	Staff Services	7.212.13.0-7.212.13.255
900	Management	7.212.14.0-7.212.14.255

Fonte: Autoria Própria

Como as redes *wireless* se transformaram em uma necessidade dos dias de hoje, a solução *wireless* implementada na empresa são duas controladores Cisco 2504 e 18 *Access Points*. Na sede administrativa foram designados 4 A*ccess Points*, que irá suprir todas as necessidades da empresa. Nesta nova adequação todos os computadores pessoais ficarão em rede cabeada, deixando o *wireless* para os dispositivos móveis e para casos de salas de reunião ou para colaboradores que estiverem em trânsito.

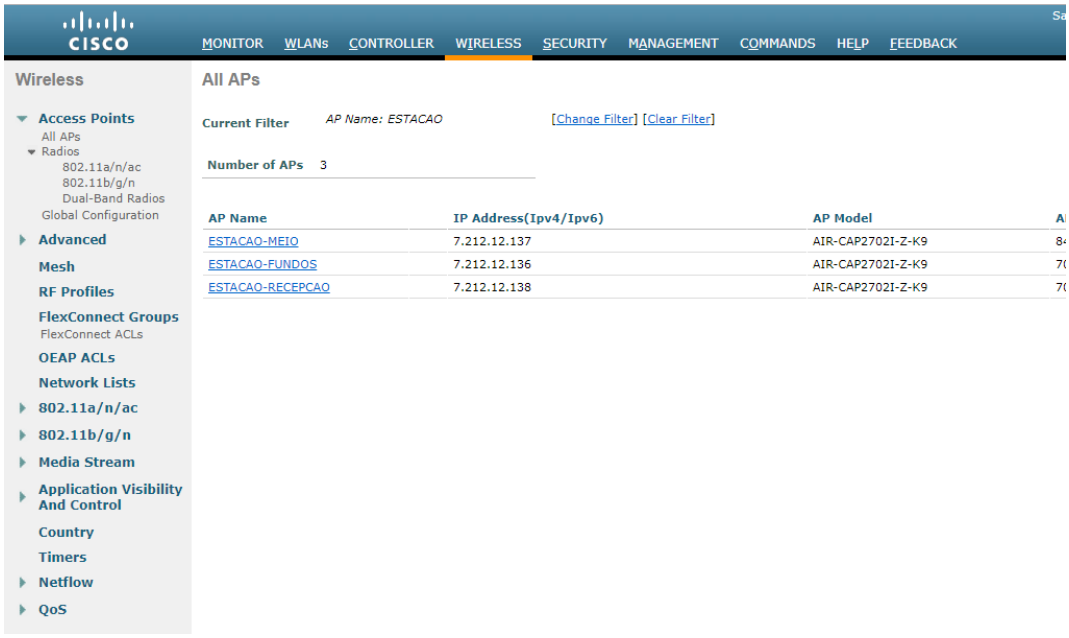

Figura 12. Tela da controladora mostrando os Access Points da empresa
Fonte: Autoria Própria

Nos *switches core* da rede foram implementados a tecnologia IRF (*Intelligent Resilient Framework*), que permite transformar diversos *switches* físicos em um único *switch* lógico, com os equipamentos sendo visualizados como um único *switch*, que oferece benefícios como resiliência, redundância, agregação de enlaces e facilidade no gerenciamento. Abaixo a configuração do *switch* com a informação do irf ativo.

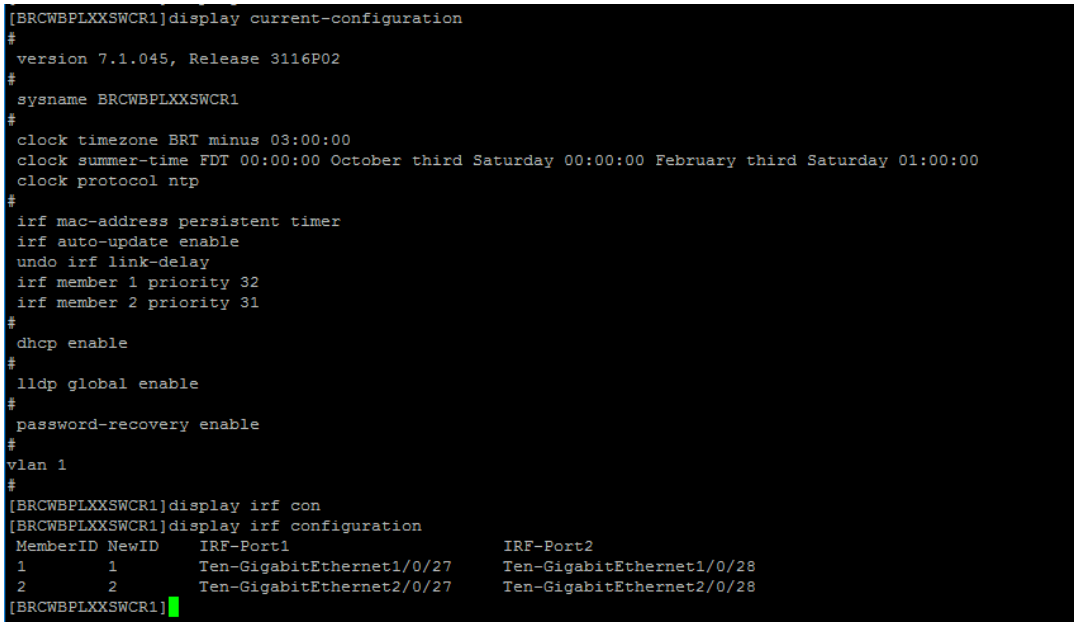

Figura 13. Mostra o irf configurado nos switches
Fonte: Autoria Própria

O Data Center principal da empresa encontra-se nos Estados Unidos, na sede da controladora do grupo, com todo o gerenciamento das máquinas sendo compartilhado entre o grupo norte americano e a equipe de infraestrutura da empresa. Para acessar os serviços, foi adquirido um roteador cisco 4130, que é utilizado somente para fechar a VPN com o outro lado, garantindo assim disponibilidade, velocidade e segurança das informações trafegadas.

```
interface Tunnel301
 description /* GBL POD VPN */
 bandwidth 100000
 ip address 7.252.247.8 255.255.255.128
 no ip redirects
 ip mtu 1400
 ip nhrp authentication poddmvpn
 ip nhrp map multicast 204.17.18.29
 ip nhrp map 7.252.247.1 204.17.18.29
 ip nhrp network-id 3
 ip nhrp holdtime 300
 ip nhrp nhs 7.252.247.1
 ip tcp adjust-mss 1330
 qos pre-classify
 keepalive 5 3
 tunnel source GigabitEthernet0/0/1
 tunnel mode gre multipoint
 tunnel key 301
 tunnel vrf DMVPN
 tunnel protection ipsec profile DMVPN-PROFILE shared
!
interface GigabitEthernet0/0/0
 ip address 7.203.94.6 255.255.255.248
 negotiation auto
 service-policy input 25Mbps
 service-policy output 25Mbps
!
```

Figura14. Configuração da VPN com o Data Center
Fonte: Autoria Própria

Após a mudança, todos os switches foram denominados, seguindo um padrão interno, onde é facilmente visualizado em qual localidade o equipamento está localizado, assim como a identificação de quais serviços eles servem. Eventos como falhas, alarmes ou notificações são registrados e armazenados pelos equipamentos de rede. Essas informações precisam estar com as datas atualizadas, para que os logs reflitam o momento exato da ocorrência do erro. Todos os equipamentos foram sincronizados utilizando o NTP Server para manter os equipamentos de rede atualizados com a data e hora corretas.

Além disso, são monitorados e foram criados dois documentos que demonstram quais dispositivos e serviços cada porta do switch está atrelado, facilitando muito na manutenção e em caso de atualização ou expansão da rede de computadores. Abaixo a imagem de uma tabela criada para localização e acesso aos switches da rede.

Nome	IP	Modelo	Localização
BRCWBPLXXSWCOR001	7.212.14.1	HPE 5130 24 G JG...	Estação
BRCWBPLXXSWACC001	7.212.14.10	HPE 5130 48 G JG...	Estação
BRCWBPLXXSWACC002	7.212.14.20	HPE 5130 48 G JG...	Estação
BRCWBPLXXSWSER001	7.212.14.26	HPE 1950 24 G JG...	Estação
BRCWBPLXXSWTEL001	7.212.14.15	HPE 1950 24 G JG...	Estação
BRLAPPLXXSWCOR001	7.212.30.1	HPE 5130 24 G JG...	Lapa

Tabela2. Tabela com o nome, ip, nome e localização dos switches
Fonte: Autoria Própria

Abaixo podemos verificar outra imagem do documento criado mostrando todas as interligações de cada switch presente na rede de computadores.

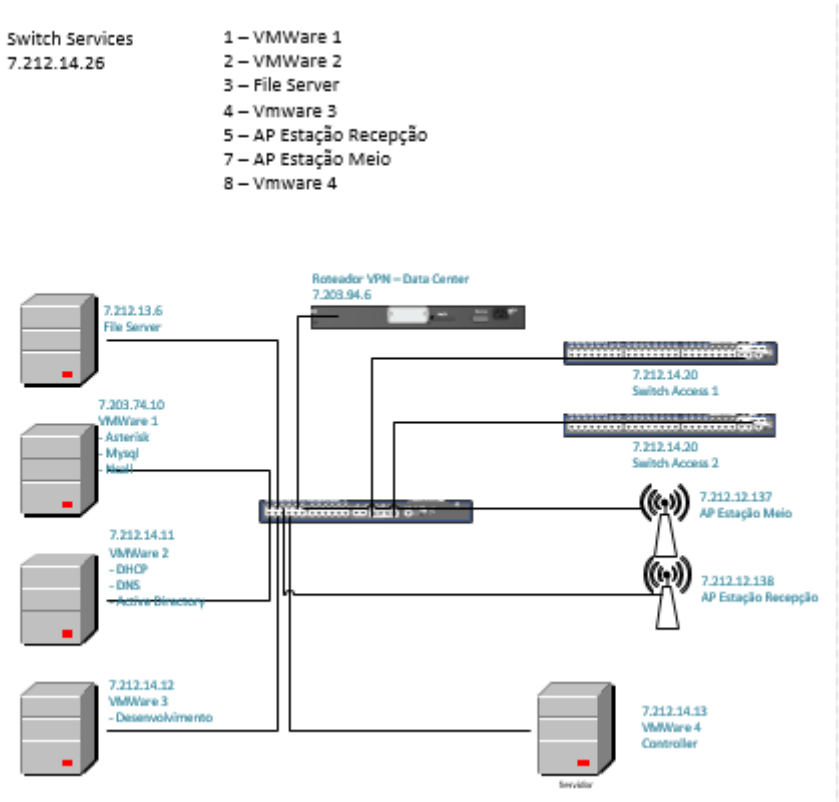

Figura 15. Imagem do documento com todas as ligações dos switches
Fonte: Autoria Própria

4 CONSIDERAÇÔES FINAIS

Buscou-se neste trabalho mostrar como a documentação e um projeto de redes de computadores se faz necessário em qualquer empresa para que possa mitigar problemas e solucionar possíveis falhas de forma mais rápida e eficiente. Mostrou que o investimento em padronização dos equipamentos e uma documentação sempre atualizada pode facilitar o trabalho de correção de diversos problemas que possam ser encontrados.

Foi analisado o estado da rede de computadores antes da mudança, apresentando seus problemas e falhas. Em seguida foram apresentados a mudança e toda a documentação gerada após toda a mudança para que problemas possam ser mitigados e problemas que possam ocorrer sejam mais facilmente descobertas e ações possam ser tomadas de forma mais ágil e assertiva.

Este projeto auxiliou o conhecimento em infraestrutura de redes, pois foi possível participar de forma ativa nas mais diversas soluções e desafios enfrentados em qualquer projeto de redes a ser implementado ou em uma readequação de qualquer ambiente de redes de forma ativa. No desenvolvimento da mudança foi possível colocar em prática muitos conhecimentos somente vistos de forma teórica e colocar em prática nos equipamentos de forma real e verificar o seu funcionamento.

REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. NBRE ISO 27002 – Tecnologia da Informação – Técnicas de Segurança – Código de pratica para a gestão da segurança da informação. 1º Ed. Rio de Janeiro, 2005.

MIRANDA, Anibal D.A. **Introdução a Rede de Computadores**. 1º ed. Vila Velha, ES: ESAB – Escola Superior Aberta do Brasil, 2008.

ALECRIM, Emerson. **O que é um Firewall? Conceitos, tipos e arquitetura.** Disponível em <https://www.infoester.com.firewall.php>, Acessado em 20/09/2017.

CHESWICK, William R.; BELLOVIN, Steven M.; RUBIN, Aviel D**. Firewalls e Segurança na Internet**. 1º Ed. Bookman Companhia, 2005.

CISCO NETWORKING ACADEMY, **CCNA2: Routing & Switching**, disponível em < https://www.netacad.com/pt/group/landing/v2/learn/ >. Acessado em 2017.

ENGST, Adam; FLEISHMAN, Glenn**. Kit do Iniciante em Redes Sem Fio: O guia prático sobre redes Wi-Fi para Windows e Macintosh.** 2ª ed.: São Paulo. Ed.: Pearson Makron Books. 2005.

FILHO, Olavo Poleto. **Gerenciamento e Monitoramento de Redes I: Análise de Desempenho.** Disponível em < http://www.teleco.com.br/pdfs/tutorialgmredes1.pdf>. Acessado em 10/09/2017.

GIMENES, E. **Voz sobre IP e qualidade de serviço em redes multisserviços**. 2003.121 f. Tese (Mestrado em Redes de Computadores) – Instituto de Psicologia, Universidade de Salvador. Bahia, 2003.

KELLER, Alexandre. **Asterisk na Prática, 1º ed**. São Paulo, SP: Novatec Editora, 2009.

LAWRENCE, Kelson. **Back to the Basics: Network and Topologies,** Disponível em **<**http://blog.boson.com/bid/87993/Back-to-the-Basics-Networks-and-Topologies>. Acessado em 18/09/2017

OLIVEIRA, José Mario; Lins, Rafael Dueire; Mendonça, Roberto. **Redes MPLS: Fundamentos e Aplicações.** 1ºed. Rio de Janeiro, RJ: Brasport, 2012.

PINHEIRO, José Mauricio santos. **Afinal, o Que é Qualidade de Serviço?,** Disponivel em **<** http://www.projetoderedes.com.br/artigos/artigo_qualidade_servico.php>. Acessado em 18/09/2017

SILVA, Pedro Tavares et all. **Segurança em sistemas de informação: gestão estratégica da segurança da empresa real.** Portugal: Centro Atlântico, 2003.

TANEMBAUM, Andrew S. **Redes de Computadores.** 4º ed. Rio de Janeiro, RJ: Ed. Campus, 2003.

TANEMBAUM, Andrew. **Organização Estruturada de Computadores**, 3º ed. São Paulo, Pearson, 2006

TORRES, Gabriel. **Redes de Computadores Versão Revisada e Atualizada.** Engenho Novo: Editora Novaterra, 2009.

[1]http://www.certiology.com/computing/computer-networking/types-of-networks.html, Acessado em 18/09/2017.

[2]<http://blogs.salleurl.edu/raising-a-data-center/the-importance-of-the-qos/>. Acessado em 20/09/2017