UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM TECNOLOGIA
ESPECIALIZAÇÃO EM GERENCIAMENTO DE REDES E SERVIDORES

DANIEL SOUZA BERTON

MODELO DE IMPLEMENTAÇÃO DE UMA ESTRUTURA DE REDE COM FOCO EM CRESCIMENTO

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA

2017

DANIEL SOUZA BERTON

MODELO DE IMPLEMENTAÇÃO DE UMA ESTRUTURA DE REDE COM FOCO EM CRESCIMENTO

Monografia apresentada à Universidade Tecnologica Federal do Paraná para conclusão do curso de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes

Orientador: Prof. Fabiano Scriptore de Carvalho. Msc.

CURITIBA

2017

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Campus Curitiba

DIRPPG
DAELN
GESER

TERMO DE APROVAÇÃO

MODELO DE IMPLEMENTAÇÃO DE UMA ESTRUTURA DE REDE COM FOCO EM CRESCIMENTO

por

DANIEL SOUZA BERTON

Esta Monografia foi apresentada em 14 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 -

RESUMO

Berton, Daniel. **MODELO DE IMPLEMENTAÇÃO DE UMA ESTRUTURA DE REDE COM FOCO EM CRESCIMENTO**. 2017. 34f. Monografia de especialização (obtenção de título de especialista em gerenciamento de redes e servidores) – Curso de pós-graduação latu sensu, Universidade Tecnológica Federal do Paraná, Curitiba, 2017.

Quando se projeta um ambiente de rede, é muito importante conhecer e saber dimensionar o escopo de onde se deseja chegar e quais objetivos atingir. Este projeto apresenta um modelo para o desenvolvimento de um ambiente de alta disponibilidade de entrega de serviço e que esteja preparado para futuras tecnologias. Se propõe a criação de uma documentação para prever o crescimento de forma saudável e evitar o retrabalho. É demonstrado formas de configurações de equipamentos de rede para prover segurança da informação, otimização da entrega de serviços e prover uma alta disponibilidade afim de diminuir ou até anular o tempo de parada caso ocorra algum imprevisto. Esse trabalho permitiu confirmar a importância do desenho da infraestrutura antes do início de implantação do projeto, visto que a falta dela acarreta em prejuízos financeiros, perda de tempo e retrabalho para a correção de propostas que não haviam sido consideradas.

Palavras chave: Modelo de infraestrutura. MikroTik. Alta disponibilidade. Crescimento de rede.

ABSTRACT

Berton, Daniel. **MODEL OF IMPLEMENTATION OF A NETWORK STRUCTURE WITH FOCUS ON GROWTH.** 2017. 34p. Monograph (Specialization in Network and Server Management) – Federal Technology University - Paraná., Curitiba, 2017.

When designing a network environment, it is very important to know and know how to scale the scope of where you want to reach and what goals to achieve. This project presents a model for the development of an environment of high availability of service delivery and that is prepared for future technologies. It proposes to create documentation to predict growth in a healthy way and avoid rework. It is demonstrated ways of configuring network equipment to provide information security, optimize the delivery of services and provide high availability to reduce or even cancel downtime in the event of unforeseen events. This work allowed to confirm the importance of the design of the infrastructure before the start of project implementation, since the lack of it entails financial losses, loss of time and rework for the correction of proposals that had not been considered.

Keywords: Infrastructure model. MikroTik. High Availability. Network growth.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ADSL	*Asymmetric Digital Subscriber Line*
DHCP	*Dynamic Host Configuration Protocol*
DNS	Domain Name System
HTML	*HyperText Markup Language*
IDE	*Integrated Development Environment*
IP	*Internet Protocol*
IPSEC	*IP Security*
L2TP	*Layer 2 Tunnel Protocol*
LACP	*Link Aggregation Control Protocol*
MAC	*Media Access Control*
MPLS	*Multi-Protocol Label Switching*
NAT	*Network Address Translation*
PPPOE	*Point-toPoint Protocol over Ethernet*
RFC	*Request for comments*
RIP	*Routing Information Protocol*
SSH	*Secure Shell*
SSID	*Service Set Identifier*
UDP	*User Datagram Protocol*
USSEC	*United States Securities And Exchange Comission*
VLAN	*Virtual LAN*
VPN	*Virtual Private Network*
WPA2	*Wi-fi Protect Access 2* ^{0} *Version*

SUMÁRIO

1. INTRODUÇÃO

PROPOSTA

O foco desse trabalho é projetar uma rede estruturada para uma rede de restaurantes fictícia. O objetivo da empresa onde está sendo desenvolvido este trabalho de final de curso é ter ao mínimo 100 restaurantes em *Shoppings Centers* espalhados pelo Brasil, e a infraestrutura lógica deve acompanhar e prever esse crescimento exponencial. Algumas particularidades devem ser levadas em consideração devido ao foco do negócio, e que o ambiente de TI deve suprir essa necessidade da empresa:

- Pelo modelo de negócio, o restaurante será instalado em *Shopping Centers* pelo Brasil, o que dificulta a contratação de uma única empresa para fornecer serviços de Internet e telefonia para atender todas as filiais. A escolha da tecnologia de interligação com a matriz será a VPN;
- O restaurante deverá suportar tecnologias e equipamentos que ainda estão por vir, ou seja, que ainda não foi desenvolvida e instaladas. Por esse motivo os equipamentos poderão ser superdimensionados para o modelo atual (ex: switch de 48 portas para poucos pontos atuais, mas criar uma regra para desabilitar portas não usadas);
- O restaurante precisa de uma redundância no enlace de saída de para a Internet, mesmo que ela não seja vital para o negócio. Geralmente em *Shoppings* a entrega de um ponto de conexão ao enlace da Internet se dá fisicamente no mesmo local, gerando um ponto de falha não-controlávelj, então a segunda opção poderá ser um enlace com conexão à Internet por meio de rádio ou uma contingência 4G.

Esse modelo não levará em conta o aspecto financeiro, pois a partir de superdimensionar os equipamentos para prever uma futura necessidade, esses aparelhos mais robustos geralmente possuem um valor mais alto, mas que farão diferença quando houver a necessidade de utilizar todo seu potencial.

OBJETIVO PRINCIPAL

O principal objetivo desse projeto é criar um modelo de uma estrutura de rede autossuficiente para um estilo específico de negócio, levando em consideração a necessidade de crescimento da rede interna quanto de suas congruentes.

OBJETIVOS ESPECÍFICOS

- Identificar os equipamentos que serão utilizados;
- Escolher os protocolos a serem utilizados de acordo com a necessidade do negócio, levando em consideração o ambiente, a proposta, e o escopo do modelo;
- Mapear e documentar a estrutura de rede para documentação e padronização, visando o crescimento ordenado e previsto;
- Configurar os dispositivos de rede para otimizar suas características;
- Prover segurança para o ambiente para o uso não desejado e não prevista da infraestrutura;
- Construir uma rede em que ela seja autossuficiente em caso de falha de comunicação com a matriz.

JUSTIFICATIVA

A necessidade de um modelo para esse formato se dá na importância da documentação e do levantamento das necessidades, mesmo que futuras ou no momento não-previstas, mas que pode ocorrer por causa de uma nova tecnologia ou de um novo projeto da empresa. É importante ter uma estrutura bem definida, pois qualquer mudança de projeto no meio da implantação, pelo tamanho e necessidade

da empresa, acarretará na revisão minuciosa de toda a infraestrutura implantada anteriormente, a fim de corrigir ou adequar para a nova realidade, o que não ocorrerá caso fosse previsto o problema anteriormente. Dessa forma, é imprescindível que haja um consenso de onde quer chegar e quais equipamentos utilizar.

Por esse mesmo motivo, o superdimensionamento desse modelo, apesar de ser financeiramente mais caro, trará benefícios a médio e longo prazo. Desta forma evita-se uma necessidade de troca do equipamento por um modelo mais robusto e preserva-se toda uma cadeia de serviços que não terão que ser refeitos, como por exemplo a nova negociação dos novos equipamentos, a visita de técnicos para a troca do dispositivo, o tempo parado da empresa para a configuração do novo equipamento (o que pode acarretar prejuízos financeiros) e a necessidade de achar um destino para os dispositivos obsoletos.

Novas tecnologias surgem a cada momento, e com isso é necessário ter a disposição a infraestrutura de redes para comportar essas novidades. Caso haja, por exemplo, a instalação de um totem de autoatendimento no restaurante, a infraestrutura já estará pronta para receber ela, independentemente de ser uma conexão cabeada ou sem fio. Quando uma nova instalação de restaurante em um *Shopping Center* em que o provedor de Internet somente poderá fornecer uma conexão PPPoE, deverá ter um equipamento que suporte esse enlace, da mesma forma que suportaria um enlace dedicado, uma conexão ADSL ou à radio, com a mesma qualidade e transparência para o usuário final, independente se for um cliente ou funcionário do restaurante.

2. REFERENCIAL TEÓRICO

2.1 TECNOLOGIAS DE REDE

Conhecer os serviços de rede é fundamental para o alcance do objetivo do modelo. A correta parametrização dos protocolos é fundamental para o desenvolvimento do modelo, acompanhando as necessidades do negócio.

2.1.1 *Dynamic Host Configuration Protocol* (DHCP)

O DHCP, *Dynamic Host Configuration Protocol*, segundo Comer (2016), é um protocolo que distribui os endereços estipulados automaticamente para os *hosts* da rede que o solicitarem, diminuindo os esforços da configuração dos nós de rede. Esse protocolo foi criado em 1993 e sofreu uma atualização em 1997 na RFC 2131. Ele fornece ao host um endereço IP não-utilizado, uma máscara de sub-rede, um *gateway* padrão e um ou mais endereço de DNS.

Quando um dispositivo se conecta na rede, ele envia um pacote UDP em broadcast com uma requisição DHCP. Quando o servidor DHCP ouve a solicitação, ele fornece os dados para o host de acordo com suas características (qual rede está, o endereçamento da VLAN, etc). De acordo com a RFC 2131 (1997), esse processo de concessão é dividido em 4 fases: DHCPDISCOVERY, DHCPOFFER, DHCPREQUEST e DHCPACK.

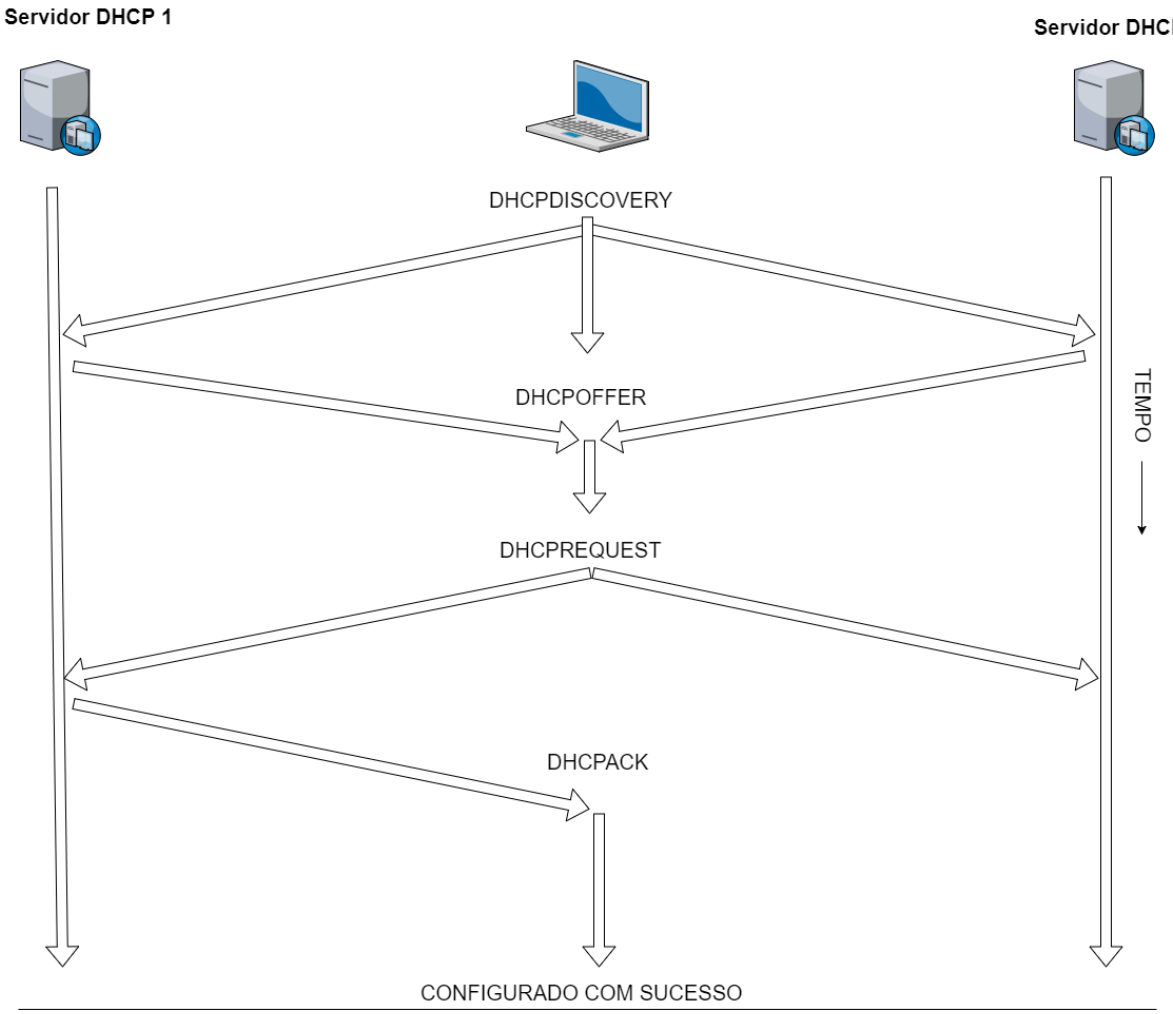

FIGURA 1: Representação do ciclo do DHCP

Fonte: Autoria própria

DHCPDISCOVERY

Segundo o RFC 2131 (1997), na fase DHCPDISCOVERY, o dispositivo cliente envia pacotes UDP em broadcast na rede para descobrir os servidores DHCP. Dessa forma ele tentará alcançar todos os IPs possíveis para que o servidor ouça sua solicitação e prosseguir para a próxima fase.

DHCPOFFER

Quando um servidor DHCP recebe o pacote do cliente, esse servidor reserva um IP disponível. Ele prepara um pacote com as informações necessárias, como IP, máscara de sub-rede, o tempo de permanência de uso do IP, entre outros. Com o pacote pronto, ele oferece a informação ao cliente (RFC 2131, 1997).

DHCPREQUEST

De acordo com o RFC 2131 (1997), quando o cliente recebe o pacote da fase DHCPOFFER, ele responde novamente em *broadcast* solicitando o IP que lhe foi oferecido. Esse pacote é disparado em *broadcast* pois pode haver mais de um servidor DHCP na rede, e o dispositivo precisa avisar a todos que ele está solicitando o IP de um servidor específico. Quando outros servidores escutarem essa mensagem, eles retiram a oferta de IP disponibilizada pelo DHCPOFFER. É nessa fase também em que o cliente tenta renovar o IP caso acabe o tempo de concessão cedido.

DHCPACK

Essa é a fase final, em que o servidor DHCP reconhece o provimento do IP e dá-se como concluído a solicitação DHCP (RFC 2131, 1997).

Segundo o RFC 2131 (1997), algumas características do DHCP são importantes e fundamentais para o seu pleno funcionamento e que são necessárias a correta configuração para o objetivo do modelo.

- Escopo (ou *pool* de DHCP): São os IPs dentro de uma máscara que serão disponibilizados pelo servidor DHCP para oferecer aos dispositivos que solicitarem uma conexão;
- Concessão (ou *lease*): É o tempo cronológico em que o cliente terá permissão para usar o IP. Depois de esgotado o tempo, caso o cliente precisar novamente do IP, ele poderá solicitar novamente ao servidor

DHCP, caso contrário o IP é devolvido novamente para o escopo de DHCP para preencher novamente as fileiras para novos clientes que o solicitarem;

- Reserva de IP: Um IP pode ser reservado para um dado endereço MAC de um cliente. Dessa forma, toda vez que esse mesmo equipamento se conectar na rede onde a reserva for configurada, ele sempre irá pegar o mesmo IP reservado, e esse IP será exclusivo para esse *host*, não sendo disponibilizado para mais nenhum cliente. Essa configuração é apropriada para o caso de ser necessário o IP de um dispositivo precisar ser padronizado, mas esse equipamento não é possível ter o IP fixado.

2.1.2 *Virtual Private Network* (VPN)

VPN, *Virtual Private Network*, é uma rede que tem por objetivo interligar duas ou mais redes de forma segura e privada, ou ainda, gerenciar redes corporativas através de uma rede pública (TANENBAUM, 2006). Para garantir esse objetivo, algumas características precisam ser atingidas:

- Confidencialidade dos dados: proteger os dados para não ser descriptografada por uma fonte não autorizada;
- Integridade dos dados: Garantir que a integridade dos dados está correta, ou seja, não foi violada ou modificada no transito entre as pontas;
- Autenticação da mensagem: Garantir que o pacote foi enviado por uma fonte legitima e para uma fonte legítima.

A VPN recebe o nome virtual pois ela cria um túnel lógico em uma rede desprotegida, como a Internet, e dentro desse túnel é trafegado os dados protegidos. Essa forma de conexão é vantajosa pois para ela ocorrer basta ter acesso à Internet nas pontas necessárias, sem necessidade de um cabeamento especial ou serviços adicionais contratados com empresas de conectividades, e dessa forma, outra vantagem é o baixo custo.

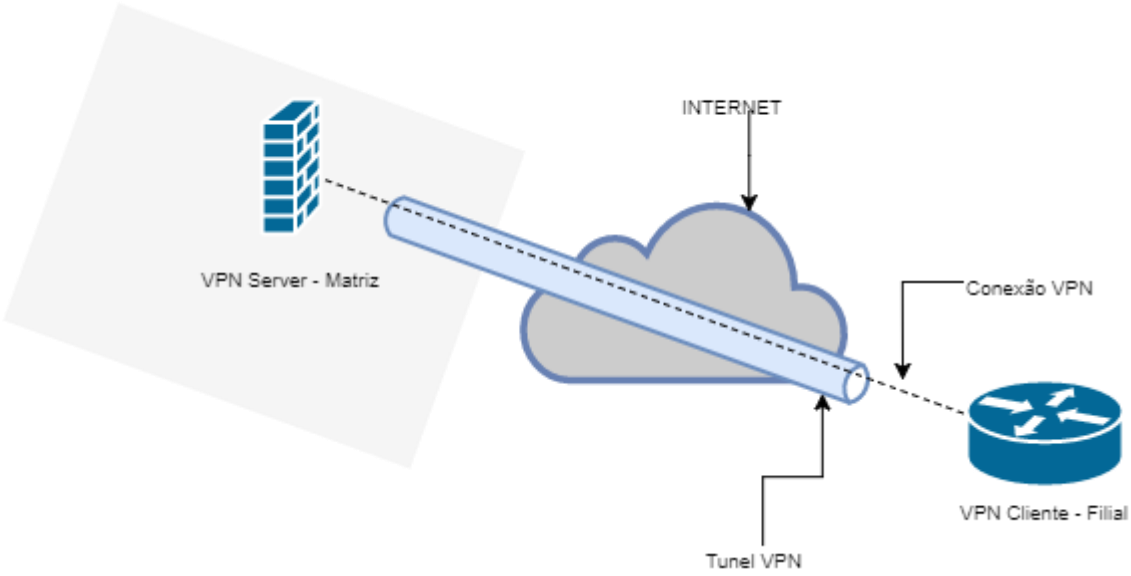

FIGURA 2: Conexão entre matriz e filial através de um túnel VPN

Fonte: Autoria própria

Os protocolos de conexão VPN que serão utilizados serão o L2TP/IPSEC, um conjunto de protocolos para a otimização da segurança. O protocolo L2TP, *Layer 2 Tunneling Protocol*, é um protocolo da Camada 2, e também é o padrão utilizado na indústria. Como esse protocolo é carente de segurança, ele é comumente usado em conjunto com o IPSEC (*IP Security*). O IPSEC garante a troca de chaves de forma criptografada, garantindo a autenticidade, integridade e confidencialidade (KUROSE, 2010).

2.1.3 *Virtual LANs* (VLAN)

VLANs (*Virtual LANs*) são redes que são isoladas logicamente através de software, mas que podem coexistir fisicamente em um mesmo equipamento (KUROSE, 2010). Esse conceito é fundamental para fazer a separação de redes para utilização para fins diferentes, como por exemplo, uma rede destinada para o acesso de clientes a Internet e uma outra rede corporativa para o ambiente de trabalho e produção. As vantagens da utilização de VLANs (FILIPPETTI, 2008) em um ambiente são várias, entre elas:

- Segurança: As VLANs podem ser tratadas de forma isolada, podendo ser bloqueado o roteamento e o acesso entre elas;
- Redução de custo: Como elas podem utilizar o mesmo equipamento e até o mesmo cabo, economizasse na quantidade necessária. Também o uso eficiente da largura de banda;
- Melhor desempenho: Dividir a rede em VLANs diminui o *broadcast* na rede, isolando os problemas que podem ocorrer por uma tempestade de *broadcast*. Essa divisão também reduz o tráfego desnecessário na rede;
- Facilidade de gerenciamento: Como são redes virtuais, o gerenciamento dela se dá por *software*, sem a necessidade expressa de um técnico alterar fisicamente em caso de manutenção ou alteração.

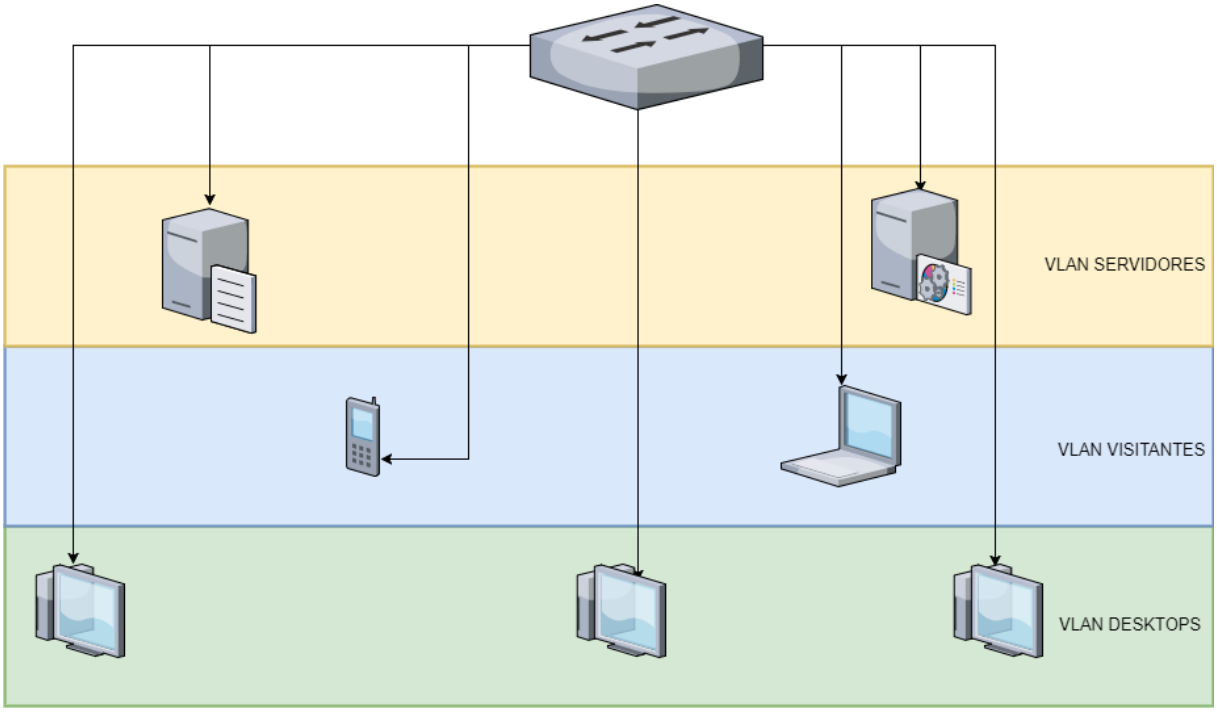

FIGURA 3: Dispositivos isolados logicamente por meio de VLANs em um mesmo switch.

Fonte: Autoria própria

Em um roteador, é possível ter até 4096 VLANs cadastradas. Cada VLAN recebe um código, indo de 1 até 4096, sendo a VLAN 1 a VLAN padrão de equipamentos com configurações padrões de fábrica. Essas VLANs são

configuradas na porta de um switch gerenciável compatível com a tecnologia, onde pode ser programado para ser o “modo *access*” ou “modo *trunk*”. A porta do switch em modo *access* recebe somente uma VLAN, sendo usada para dispositivos finais. Já as portas em modo *trunk* receberá vários IDs de VLAN, usualmente utilizado entre roteadores, switches ou access-point.

Existe também o conceito de VLAN *Black Hole*. Essa VLAN, que por padrão recebe um ID 999, é uma VLAN não roteável e sem *gateway* padrão, utilizada em portas do switch que não serão utilizadas. Essa medida é uma camada a mais de segurança para evitar a invasão física na rede.

2.2 EQUIPAMENTOS

2.2.1 Roteador – MikroTik

MikroTik é uma empresa fundada em 1996 na Letônia, país central Europeu. Essa empresa desenvolveu em 1997 um sistema operacional próprio para roteadores chamado RouterOS, com foco em estabilidade, controle e flexibilidade das interfaces de dados e roteamento. Em 2002 começaram a fabricar os próprios *hardwares* já com esse sistema operacional embarcados. Esses *hardwares* foram chamados de RouterBOARD. Hoje em dia esses equipamentos são muitos utilizados provedores de acesso a Internet, por seu preço e sua confiabilidade e grande poder de customização. Hoje o RouterOS suporta várias funções, como ser um *firewall*, VPN, RIP, MPLS, PPPoE, servidor DHCP, roteamento de VLAN, LACP, entre outras características. Por esses motivos, o *hardware* foi eleito para ser o roteador padrão das filiais, pois como ele abrange muitas tecnologias à nível de *software*, ele pode se tornar um equipamento coringa para futuras tecnologias que possam vir a existir.

Figura 4: RouterBOARD 1100AHx4, modelo utilizado nesse trabalho.

Fonte: Mikrotik.com (2017)

Existem várias formas de acessar a console de configuração do RouterBOARD, entre eles acesso via SSH, Telnet, via navegador por HTML ou o acesso via um IDE desenvolvido pela MikroTik chamado WinBox. Esse *software* é muito útil para a programação do equipamento, pois por meio dele é possível enviar configurações

visualmente, através de cliques, ao invés da necessidade de digitar linhas de comando para fazer alterações.

O *hardware* escolhido para a configuração desse projeto foi o modelo RouterBOARD 1100AHx4. A escolha foi devida a algumas características desse equipamento que vão de encontro com a necessidade da empresa, como alta escalabilidade, alto processamento, suporte a tecnologias eleitas e o seu custo em comparação a outros *hardwares* semelhantes que oferecem a mesma proposta. Esse modelo possui memória interna dedicada de 1 GB, processador de 1,4 GHZ, fonte redundante para a alimentação de energia, 13 portas *Gigabit ethernet*, sendo um equipamento para ser fixado em *rack*, de tamanho de 1U, o que ajuda na manutenção e prevenção de acidentes, por ser um equipamento muito importante para a filial. Ele será configurado como o roteador principal da filial, tendo os serviços de *firewall*, servidor DHCP e VPN *Client*, conectando no VPN *Server* que ficará na matriz. Duas portas *Ethernet* serão dedicadas a fazer a agregação de enlace com o switch, dessa forma aumentando a disponibilidade e gerando redundância de dados. Duas ou mais portas serão dedicadas para receber os enlaces de Internet, sendo eles os disponíveis no local, mas todos sendo entregues via cabo ethernet em uma dada porta. Esses enlaces serão adicionados como uma interface e será criado um roteamento de redundância entre eles, onde caso o enlace principal caia, os enlaces backups assumam o fornecimento de Internet. Será por meio desses enlaces de Internet em que haverá a criação do túnel L2TP entre o servidor e cliente VPN, para o tráfego seguro de dados prioritários e que é necessário sigilo e integridade dos dados.

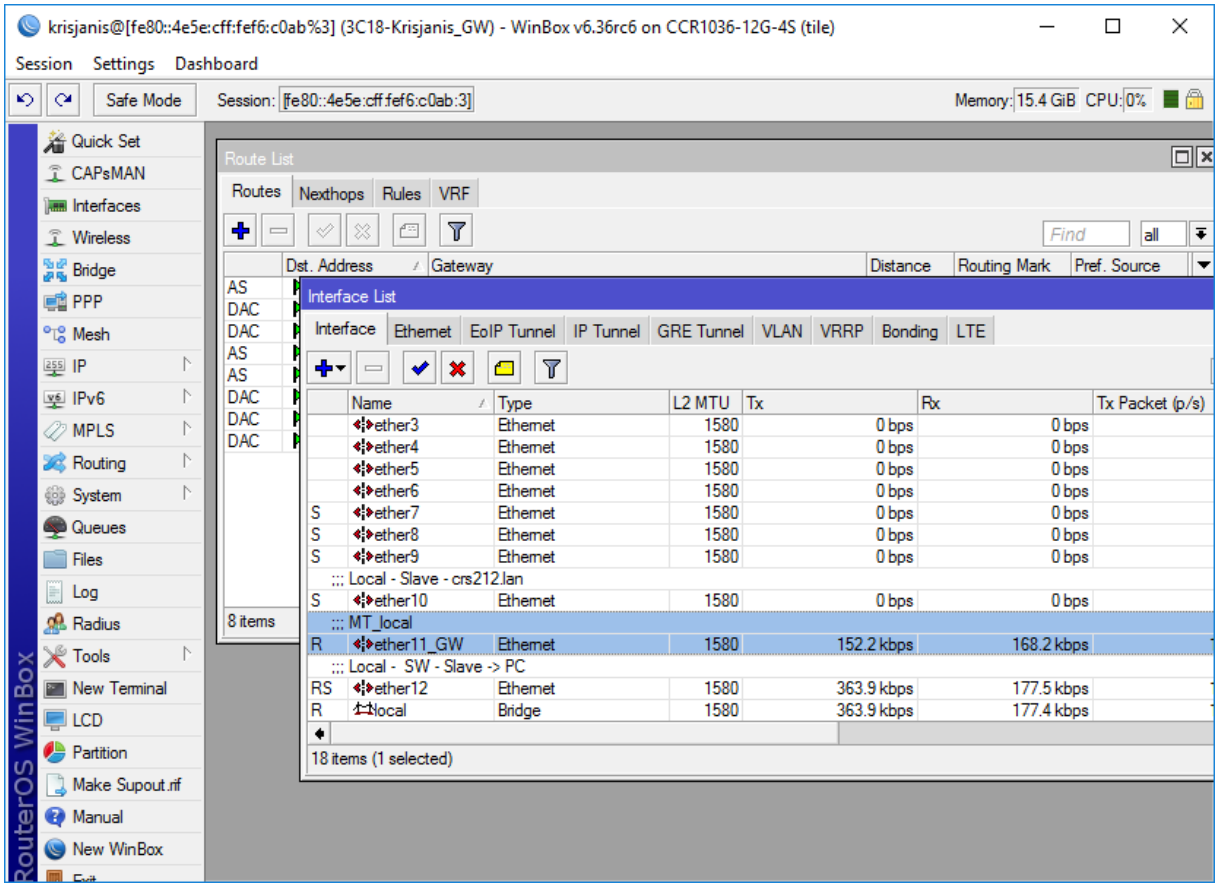

Figura 5: Tela do IDE Winbox para acesso ao MikroTik

Fonte: mikrotik.com (2017)

O RouterBOARD também funcionará como um *firewall*, onde é possível a criação de regras de tráfego e o bloqueio da comunicação entre a VLAN corporativa e a VLAN de clientes, que também será roteada pelo equipamento. Como as redes estão configuradas dentro do mesmo *hardware*, é necessário o bloqueio do roteamento dessas redes.

2.2.2 Switch

A nomenclatura Switch é dado ao equipamento que tem o trabalho de filtrar, encaminhar e preencher quadros, levando em consideração o endereço de destino dos quadros que recebe. Dessa forma, podemos dizer que esse dispositivo é um comutador de pacotes da camada de enlace (KUROSE, 2010).

Em uma rede corporativa, é fundamental a utilização de um switch, pois ele oferece um controle de distribuição de dados, já que os quadros não são transmitidos durante um mesmo seguimento, evitando assim colisões de pacote. Em um switch, o pacote é enviado devidamente para a porta em que o dado foi solicitado, evitando assim um *broadcast* na rede, garantindo a integridade dos dados e uma melhor performance.

No projeto será utilizado um switch gerenciável, ou seja, um switch em que pode-se fazer configurações específicas em cada porta ethernet. Ele tem 48 portas *gigabit*, para prever o aumento da quantidade de equipamentos em um projeto interno futuro. Como o switch será gerenciável, as portas não utilizadas deverão ser desabilitadas.

2.2.3 Enlaces de Internet

Os enlaces são os meios em que a filial se conectará com a Internet, por intermédio de contratação do serviço com uma operadora. A conexão com a Internet é necessária para a conexão da filial com a matriz, para poder enviar e receber dados por meio da VPN. Esses enlaces devem ser redundantes, com dois ou mais enlaces de Internet, idealmente de mídia e fornecedores diferentes. Como a empresa terá o foco de atividade basicamente em *Shoppings Center*, a contratação fica restrita com uma operadora que já atende o local ou que possui um contrato de exclusividade com a gestora do condomínio comercial. Por essa forma é difícil a contratação de alguma tecnologia de interconexão de empresas, como MPLS, por esse motivo foi escolhida a tecnologia VPN, pois para sua conexão basta apenas uma conexão simples de Internet.

Existem vários tipos de mídia de distribuição de Internet, as mais utilizadas e de fácil contratação são:

- ADSL: a Internet ADSL é entregue na empresa por meio de uma linha de telefone, sendo essa linha ligada em um modem. É o modelo de negócio mais comum e mais simples de utilização, sendo o modelo que é o mais encontrado em *Shoppings Center*, visto que também é vendido em conjunto com uma linha

telefônica para a comunicação da empresa contratante. Geralmente é a que fornece melhores velocidades de conexão, sendo assim eleita para ser o enlace principal

- Rádio: esse tipo de tecnologia depende de uma antena que captará os sinais da operadora, o que redirecionará o sinal através de um cabo até um equipamento próprio, o que fornecerá Internet para o roteador. Essa tecnologia é dependente de condições climáticas favoráveis e também da “visada”, ou seja, a antena da filial ser apontada para a antena da operadora sem obstruções, como prédios ou árvores.

- Modem 4G: essa tecnologia fornece Internet mediante uma conexão através da Internet 4G, com sinal de celular. Essa tecnologia não é necessária negociação com o shopping, pois o sinal 4G funciona na maioria dos ambientes. Independente disso, a grande desvantagem dela é que essa Internet é baseada em consumo de franquia de dados, sendo assim, essa conexão deve ser usada como último recurso, em casos emergenciais.

2.2.4 Ponto de acesso sem fio

O acesso a rede por meio sem fio se dará por antenas de pontos de acesso sem fio. Esse equipamento tem a função de entregar tanto a cliente quanto para agentes corporativos o acesso a rede com mobilidade, de forma confiável e segura. Esse *hardware* será ligado ao switch em uma porta pré-configurada em modo tronco, para o fornecimento tanto da VLAN de clientes quanto da VLAN corporativa, aproveitando assim, o mesmo equipamento. O equipamento deverá fornecer as frequências 2,4 GHZ e 5,0 GHZ, para cobrir todos os possíveis dispositivos que poderão ser conectados na rede.

Figura 6: Ponto de acesso, modelo Ubiquiti Unifi

Fonte: ubnt.com (2017)

A quantidade de antenas de pontos de acesso instaladas deverá ser de acordo com o tamanho físico da filial, ou da quantidade de pontos cegos que podem ocorrer no local. Dessa forma, o ideal é que cada antena suporte no máximo 30 conexões, para que a entrega de pacotes não sofra perda de qualidade.

2.2.5 Cabeamento CAT6a

O método de transmissão que é mais utilizado em redes locais é o cabeamento de par trançado. Esse tipo de cabeamento consiste em 4 pares de fios de cobre encapados e enrolados em forma de trança. Quando esses pares são trançados, as ondas eletromagnéticas geradas por eles são canceladas (TANEMBAUM, 2003).

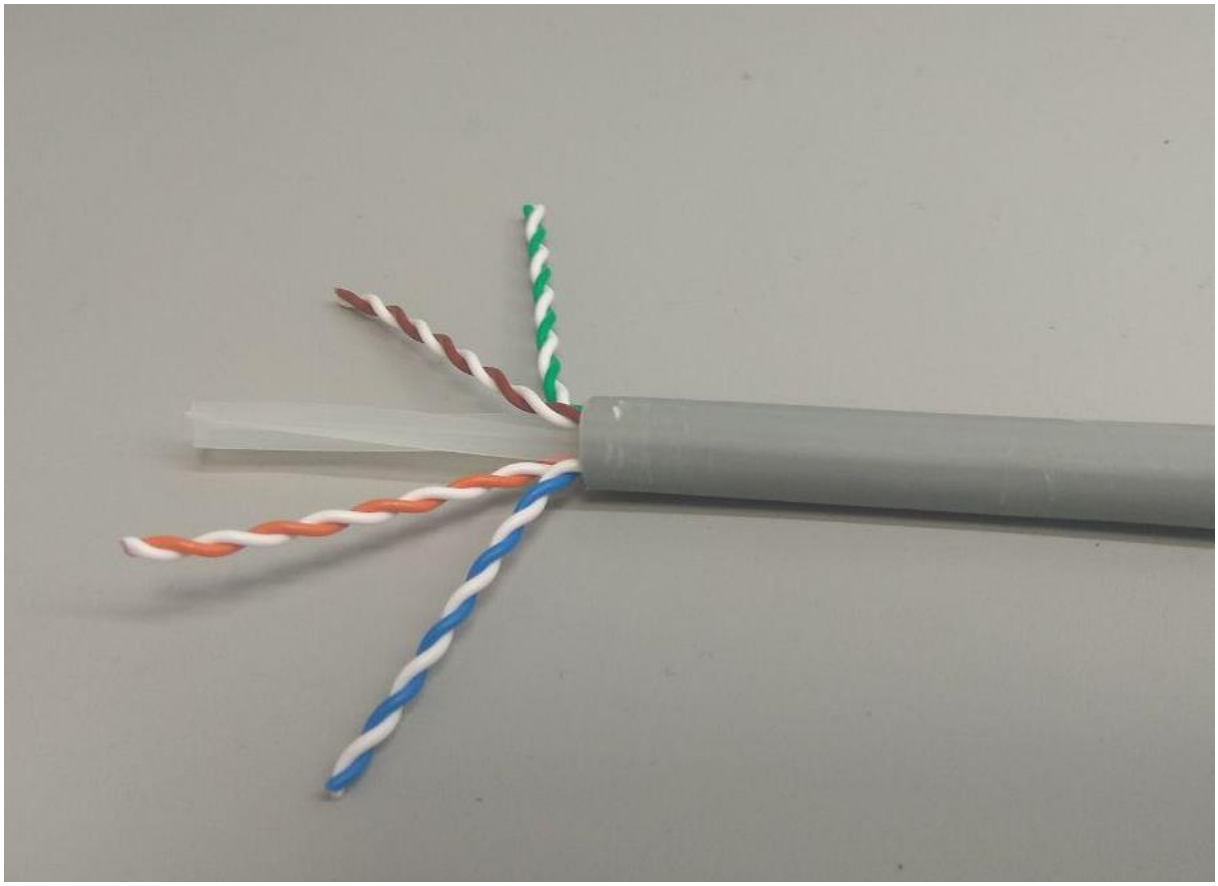

Figura 7: Cabo Cat6A com os pares trançados e proteção interna com divisória
Fonte: Autoria própria

O tipo de cabo utilizado será o modelo CAT6a, cuja vantagem é que ele trabalha com taxa de velocidade de 10 gigabits, sendo possível o comprimento do cabo até 100 metros, e uma redução significativa no recebimento de interferência externa, como ondas eletromagnéticas de cabos de energia, entre outros.

3 DESENVOLVIMENTO

3.1. ESCOPO

Como as filiais precisam ser independentes da matriz mesmo após a queda da Internet que eventualmente poderá ocorrer, os serviços de rede precisam ser entregues na rede local, como por exemplo DHCP, roteamento, aplicação e banco de dados.

De acordo com as normas da RFC1918, será usado o um range de IP Classe A, o 10.0.0.0/8. Essa faixa vai da rede 10.0.0.1 até 10.255.255.255, o que representa 65.536 sub-redes com 254 *hosts* cada. Quando levado em consideração o número de 5561 municípios no Brasil (IBGE, 2000), com essa quantidade de sub-redes é possível instalar uma média de 11 restaurantes por município no Brasil inteiro. Para fins de comparação, o restaurante *Mac Donalds* possui mais de 36,900 filiais espalhada ao redor do planeta (USSEC, 2016). Com essa ideia, o crescimento da rede é sustentado de maneira estruturada e conhecida. Sabendo a quantidade de redes, o desenho irá ultrapassar com folga qualquer taxa de crescimento no número de filiais.

Dessa forma podemos mapear:

Filial 1	10.0.1.0/24
Filial 2	10.0.2.0/24
Filial 3	10.0.3.0/24
(...)	
Filial 254	10.0.254.0/24
Filial 255	10.1.0.0/24
Filial 256	10.1.1.0/24
Filial 257	10.1.2.0/24
Filial 258	10.1.3.0/24

Tabela 1 – Exemplos de faixas de IPs para filiais

Fonte: Autoria própria

Sendo assim, podemos perceber que o primeiro octeto da rede será mantido fixo, e o segundo e terceiro octeto terá crescimento incremental de acordo com o número de filiais, sendo exclusivo para cada localização. A combinação desses dois octetos serão os identificadores da filial perante a matriz. O último octeto é reservado para os IPs internos da rede, sendo variáveis para cada tipo de equipamento. Para seguir uma padronização e facilitar o suporte técnico e o conhecimento da rede, os IPs serão separados por tipo de equipamentos, para também evitar conflitos de rede:

Equipamento	Faixa de IP	Total de IPs
DHCP	1 ao 50	50
Servidores	51 ao 55	5
Switchs	56 ao 60	5
DVR	61 ao 65	5
Impressoras de produção	66 ao 90	25
Access Point Wifi	91 ao 110	20
Terminais de venda	111 ao 130	20
Reservado	131 ao 253	123
Roteador	254	1
	Total:	**254**

Tabela 2 – Distribuição de hosts de acordo com os equipamentos

Fonte: Autoria própria

A faixa de IPs reservados será considerada para futuros projetos, para equipamentos que serem adicionados no escopo no futuro, já está garantido o seu encaixe na rede.

Com essa ideia, é possível segmentar a rede de uma maneira contínua e sem conflitos de comunicação com a matriz, podendo receber e enviar dados sem problemas de roteamento e sem preocupação com uma futura necessidade de alteração de padronização devido ao esgotamento de classes de IP.

3.2. CONFIGURAÇÃO DAS VLANS

Será separado as VLANs dentro do restaurante, uma para a rede empresarial e outra VLAN para a disponibilização de acesso à Internet para os clientes. Essas VLAN terão seus tráfegos bloqueados entre elas através de configuração de firewall do Mikrotik, para haver uma maior segurança e a inibição de tentativas de invasão na rede principal, tanto da filial quanto da matriz.

As VLANs utilizadas serão:

ID da VLAN	**Utilização**
1	Padrão
100	Rede empresarial
42	Rede para clientes
999	*Black hole*

Tabela 3 – Orientação de uso das VLANs

Fonte: Autoria própria

No switch, será inserido como VLAN 100 modo *access* todas as portas em que equipamentos de rede empresarial irão se conectar diretamente. Nos pontos de acesso sem-fio iremos colocar como modo *TRUNK* e as VLANS 100 e 42, pois o único método de entrega de Internet para os clientes será por meio de conexão sem fio. Todas as outras portas que não forem utilizadas deverão entrar no modo shutdown e apontadas para a VLAN de *black hole*, que será a 999. Essa VLAN não possuirá *gateway* e não será roteável, para aumentar a segurança e não ser mais conectados nenhum equipamento adicional sem o conhecimento da equipe técnica de TI. Por questões de boas práticas na TI e também por questão de segurança para diminuir os pontos comuns da infraestrutura, a VLAN nativa não será usada como VLAN *black hole*. Sendo assim, a VLAN 1 não será utilizada nas portas do switch e também não será roteável, mas poderá ficar na configuração do switch para evitar possíveis problemas de configurações futuras.

3.3. CONFIGURAÇÃO DO DHCP

A utilização do DHCP irá diferir entre as redes corporativa e a de clientes. Na rede corporativa, os equipamentos deverão ter os seus IP's fixados para prever um possível problema no roteador ou conflito de entrega de IP's. Se por algum motivo o roteador parar o seu funcionamento, a rede corporativa, através do switch e dos IP's fixos corretamente e na mesma subrede, poderão continuar comunicando-se entre si, já que os equipamentos locais estarão na mesma rede e não será necessário o roteamento dos pacotes. Pensando dessa forma, o *pool* de DHCP não precisará ser grande, pois ele não poderá contemplar o range dos IP's dos equipamentos fixados. Outra configuração também que deve ser vista é o *lease* do DHCP, que no caso da rede corporativa poderá ser alto, sendo aproximadamente de 3 dias, pois os mesmos equipamentos serão sempre utilizados no mesmo local físico.

Mesmo assim, a rede corporativa, cujo VLAN será 100, deverá possuir um pool de DHCP. Esse pool será definido com 50 IP's válidos, para o uso de equipamentos corporativos de visitantes, como por exemplo um notebook de um supervisor. O pool definido será o começo da rede, para ser mais fácil de identificação, de acordo com a tabela X. Todos os outros IP's restantes deverão estar reservados para equipamentos internos com IP's fixados.

Na rede de clientes, como é previsto uma rotatividade alta de clientes, subsequentemente de equipamentos para se conectar a rede como, como smartphones, tablets, notebooks, o pool de DHCP deverá ser o maior possível e o lease um valor baixo, para poder devolver rapidamente um IP de volta para o pool quando algum cliente termine a refeição e vá embora. Como a rede de clientes não terá conexão com a matriz da empresa, ela será padronizada para todas as filiais. Como definido, ela será a rede 192.168.42.0/24, na VLAN 42. Os IP's fornecidos serão do 192.168.42.1 até 192.168.42.253, sendo o IP 192.168.42.254 reservado para ser o gateway, isolando logicamente a rede de clientes da rede corporativa. Será definido também o *lease* de DHCP para ser de 60 minutos. Com essas características a rede irá suportar até 253 dispositivos conectados simultaneamente, com uma devolução rápida de IP, gerando rotatividade das conexões.

3.4. CONFIGURAÇÃO DO ROTEADOR

Dentro da infraestrutura, o roteador Mikrotik servirá como gateway da rede e o responsável com a conexão via VPN com a matriz. A rede da filial será apenas roteável com a matriz, não sendo configurada nem permitida o roteamento entre as filiais. Por padrão e regulação, o gateway terá o IP final de 254. Esse mesmo roteador também servirá de firewall e também como servidor DHCP da rede. O modelo de Mikrotik utilizado será o RB1100ahx2, que possui alto poder de processamento e 10+3 portas ethernet gigabits customizáveis de acordo com a necessidade, sendo as 10 portas iniciais divididas em 2 blocos de 5 portas, e um último bloco de 3 portas próprias para bypass. O primeiro grupo de portas será dedicada à conexão ao switch, com dois cabos para o switch fazendo um *link aggregation* para aumentar a capacidade de tráfego de dados dentro da rede. O segundo bloco será dedicado para o recebimento da Internet da filial, através dos modems das operadoras. O restaurante deverá possuir no mínimo 2 acessos à Internet, uma principal e outra de redundância de outra operadora, se possível de outra tecnologia de conexão da principal, como por exemplo, Internet à radio. Idealmente poderá haver uma terceira Internet utilizando um modem 4G, para casos emergenciais de necessidade de conexão. A última porta do Mikrotik será dedicada a conexão manual e presencial ao console de configuração do roteador. Essa porta deve ser isolada e nenhum cabo conectado, sendo utilizada somente caso em que se perca o acesso através do IP de gateway do equipamento.

As regras de firewall e bloqueio de conexão entre as VLANs se fazem necessárias por questão de segurança da informação e bloqueio de ações de mal-intencionados. O acesso ao Mikrotik será protegido com senha e permitido apenas através da porta console, porta de gerenciamento configurada e através da rede corporativa. As regras de firewall deverão bloquear a comunicação da rede de clientes com a rede corporativa, e também para segurança dos clientes, a comunicação entre os equipamentos da rede de clientes, apenas conexão com o gateway, que será o próprio Mikrotik. Também por segurança, o acesso direto ao gateway também será bloqueado na rede de clientes, sendo apenas permitida o tráfego de pacotes necessários para os dispositivos que o tiverem solicitados.

A conexão através de VPN com a filial se dará através de um túnel L2TP/IPsec com a matriz, para que haja troca de informações de maneira segura e criptografada.

Como existe a troca de chave, esse protocolo garante a confidencialidade dos dados trafegados por dentro da Internet, garantindo que ele chegue ao seu real destino, sem que os dados sejam percebidos por um intermediário malicioso. Com um túnel criado entre o Mikrotik da matriz e o Mikrotik da filial, os dados de conexão entre as pontas trafegarão exclusivamente por dentro dele. Em casos extremos e de impedimento da atuação do negócio da empresa por queda do túnel, poderá ser criado uma NAT com permissão exclusiva entre os dois pontos para o reestabelecimento de tal serviço, até o problema da queda do túnel ser solucionado, dessa forma o NAT será novamente bloqueado.

3.5. CONEXÃO VIA PONTOS DE ACESSO SEM FIO

As conexões via *wi-fi* na rede da filial se dará de duas maneiras diferentes, uma forma para a conexão na rede corporativa e outra para a rede de clientes. A conexão com a rede de clientes se dará por método simples, utilizando uma SSID padrão para todas as filiais, pois todas as filais terão a mesma rede. Com isso, caso o cliente quando sair de uma filial e for visitar uma outra, não será necessária uma nova tentativa de conexão, já que o dispositivo, se assim programado, poderá se conectar automaticamente na wifi. Será utilizado para essa conexão o padrão WPA2 *Personal*, com uma senha pré-definida e padrão, que poderá ser fornecida para o cliente se assim for necessário.

Já a rede corporativa utilizará o padrão WPA2 – *Enterprise*, com autenticação em um *Active Directory*. Dessa forma é possível mapear as permissões de acesso individualmente, prevenir o vazamento de senhas, já que é possível saber qual é a conta no caso de um acesso não permitido ou improvável. Com a autenticação dessa forma é criado uma cada de segurança a mais, já que será necessário usuário e senha, sendo os dois exclusivos de uso pessoal e intransferível. No caso da necessidade de conexão de dispositivos de uso não-exclusivo, como coletores ou *tablets* de atendimento, poderá ser criado uma conta de autenticação para cada um desses dispositivos, mas essas contas com limitações de permissões, como por exemplo sem permissão para acesso à Internet e tráfego exclusivo com o serviço que

é necessário para sua operação. Essa autenticação se dará em um serviço localizado na matriz, para que funcionários que tem a necessidade de visitar as filiais possam utilizar o mesmo usuário e senha para todos os locais, inclusive na própria matriz.

4. CONCLUSÕES

Este trabalho procurou demonstrar os fatores do ambiente de rede que são importantes de serem ajustados e configurados para se atingir o objetivo do negócio proposto. Embora alguns apontamentos sejam praticamente impossíveis de serem alcançados, como o tamanho da classe de IP, esse trabalho norteará propostas semelhantes, onde é possível fazer ajustes para realidades e propostas diferentes.

Hoje em dia as empresas dão mais importância para o crescimento em infraestrutura, onde antigamente eram vistos como despesas, hoje são vistos como investimentos. Novas tecnologias são criadas ou aprimoradas com o passar do tempo, e esse modelo está pronto para o recebimento desses novos dispositivos ou serviços.

A escolha dos equipamentos adequados com o objetivo são importantes fatores do sucesso do modelo, pois como a localização física das filiais irão ter diferentes realidades, esses equipamentos deverão estar prontos e ser maleáveis a ponto de se encaixar em qualquer ambiente, não perdendo a proposta de padronização de todas as filiais. A padronização também é a palavra-chave desse modelo, pois com ele é possível conhecer e prever a estrutura em qualquer atual ou futura filial.

Procurou-se também se empenhar na segurança da rede, pois como uma parte dela será de uso público, é possível que haja tentativas de invasão a dados não autorizados. A preocupação com a segurança é constante, e foi tomado medidas para proteção da rede, como regras de *firewall* e separação por VLANs. A disponibilidade e continuidade do serviço também é importante, pois qualquer parada da infraestrutura poderá causar prejuízos financeiros e perda de credibilidade com funcionários e principalmente com os clientes.

É obvio que a tecnologia avança a passos largos, e que depois de algum tempo, os equipamentos ou até os serviços podem se tornar obsoletos, com o surgimento de processos mais eficazes ou dispositivos mais robustos. Esse modelo leva em consideração a realidade de hoje, com as tecnologias mais presentes, mas nada impede a continuidade de trabalhos futuros seguindo o objetivo geral desse modelo.

5. REFERENCIAS

COMER, Douglas E. **Interligação de redes com TCP/IP**. Vol. 1 princípios, protocolo e arquitetura. 5ª. ed. Rio de Janeiro: Campus, 2006.

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

IBGE, Instituto Brasileiro de Geografia e Estatística: **Indicadores Sociais Municipais**, 2000. Disponível em <https://ww2.ibge.gov.br/home/estatistica/populacao/indicadores_sociais_municipais/tabela1a.shtm> Acessado em Outubro de 2017.

KUROSE, James F. **Redes de computadores e a Internet**. 5ª. ed. São Paulo: Pearson, 2010.

RFC 1918, **Address Allocation for Private Internets**. Disponível em <https://tools.ietf.org/html/rfc1918>. Acessado em Outubro de 2017.

RFC 2131, **Dynamic Host Configuration**. Disponível em <https://www.ietf.org/rfc/rfc2131.txt>. Acessado em Outubro de 2017.

TANENBAUM, A. S. **Redes de Computadores**. 4 ed. Rio de Janeiro: Eselvier, 2003

USSEC - United States Securities And Exchange Comission - **ANNUAL REPORT McDonald`s Corporation**, 2016. Disponível em <http://d18rn0p25nwr6d.cloudfront.net/CIK-0000063908/62200c2b-da82-4364-be92-79ed454e3b88.pdf>. Acessado em Outubro de 2017.