CENTRO DE ENSINO SUPERIOR DE FOZ DO IGUAÇU- CESUFOZ
CURSO SUPERIOR DE CIÊNCIA DA COMPUTAÇÃO

REESTRUTURAÇÃO DE REDE LOCAL NAS CAMADAS DE ENLACE E INTERNET, COM ÊNFASE EM DESEMPENHO E SEGURANÇA.

ALEX SANDER SABINO ROCHA
CARLOS EDUARDO KUMMER
OSCAR MEDINA GOMES DA COSTA

FOZ DO IGUAÇU
2017

ALEX SANDER SABINO ROCHA
CARLOS EDUARDO KUMMER
OSCAR MEDINA GOMES DA COSTA

REESTRUTURAÇÃO DE REDE LOCAL NAS CAMADAS DE ENLACE E INTERNET, COM ÊNFASE EM DESEMPENHO E SEGURANÇA.

Trabalho de Conclusão de Curso apresentado à disciplina de Trabalho de Curso I, do Curso Superior de Ciência da Computação do CESUFOZ – Centro de Ensino Superior de Foz do Iguaçu, como requisito parcial para obtenção do título de Bacharel.

Orientador: Prof. Wilson Varaschin

FOZ DO IGUAÇU
2017

REESTRUTURAÇÃO DE REDE NAS CAMADAS DE ENLACE E INTERNET, COM ÊNFASE EM DESEMPENHO E SEGURANÇA.

ALEX SANDER SABINO ROCHA
CARLOS EDUARDO KUMMER
OSCAR MEDINA GOMES DA COSTA

Este exemplar corresponde à redação final de conclusão de curso apresentado como requisito parcial para obtenção do grau de Bacharel em Ciência da Computação, CESUFOZ- Centro de Ensino Superior de Foz do Iguaçu, aprovada pela comissão formada pelos professores:

Prof.
Wilson Varaschin

Prof. MSc.
Jésus Henrique Segantini

Prof. MSc.
Fernando Nakayama de Queiroz

RESUMO

Este projeto consiste em projetar e executar uma reestruturação de uma rede local na empresa Friella, com ênfase nas camadas de enlace e internet. Será realizado a análise de desempenho e de segurança da informação dessa rede antes e após a reestruturação e será colocado em evidência os motivos para manter a rede sempre estruturada, segmentada e seguindo as boas práticas de segurança, melhorando o trabalho da equipe de suporte técnico no gerenciamento e monitoramento da rede e também em novos *upgrade*.

Palavras-chave: Reestruturação. Camada de enlace. Camada de internet. Segurança. Desempenho. Gerenciamento.

ABSTRACT

This project consists in make a project and execute a local network restructure in Friella's company, with emphasis in the data-link and network layers. Will be realized an analyze of performance security of this network before and after the project and will be placed in evidence the reasons to maintain a network always structured, segmented and following the good practices of security, improving the work of the technical support team in the management and monitoring of the network and also in new upgrades.

Key-words: Restructure. Data-link layer. Network layer. Security. Performance. Management.

LISTAS DE ABREVIATURAS

IP	INTERNET PROTOCOL
TCP	TRANSMISSION CONTROL PROTOCOL
VLAN	VIRTUAL LOCAL AREA NETWORK
IEEE	INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS
MAC	MEDIA ACCESS CONTROL
OUI	ORGANIZATIONALLY UNIQUE IDENTIFIER
ARPANET	ADVANCED PROJECTS RESEARCH AGENCY NETWORK
DOD	DEPARTMENT OF DEFENSE
EUA	ESTADOS UNIDOS DA AMÉRICA
ARPA	ADVANCED RESEARCH PROJECTS AGENCY
IMP	INTERFACE MESSAGE PROCESSORS
UDP	USER DATAGRAM PROTOCOL
FTP	FILE TRANSPORT PROTOCOL
DNS	DOMAIN NAME SYSTEM
VTP	VLAN TRUNKING PROTOCOL
P2P	PEER-TO-PEER
STP	SPANNING TREE PROTOCOL
DEC	DIGITAL EQUIPMENT CORPORATION
LAN	LOCAL AREA NETWORK
RSTP	RAPID SPANNING TREE PROTOCOL
WAN	WIDE AREA NETWORK
MAN	METROPOLITAN AREA NETWORK
POP	POST OFFICE PROTOCOL
DHCP	DYNAMIC HOST CONFIGURATION PROTOCOL
HTTP	HYPER TEXT TRANSFER PROTOCOL
SNMP	SIMPLE NETWORK MANAGEMENT PROTOCOL
HTTPS	HYPER TEXT TRANSFER PROTOCOL SECURE
API	APPLICATION PROGRAMMING INTERFACE
IMAP	INTERNET MESSAGE ACCESS PROTOCOL
NETACAD	CISCO NETWORKING ACADEMY
Gbps	GIGABITS POR SEGUNDO
Mbps	MEGABITS POR SEGUNDO

Kbps	KILOBITS POR SEGUNDO
AP	ACCESS POINT
CID	CONFIDENCIALIDADE, INTEGRIDADE E AUTENTICIDADE
SSH	SECURE SHELL
MPLS	MULTI-PROTOCOL LABEL SWITCHING
IGRP	INTERIOR GATEWAY PROTOCOL
RIP	ROUTING INFORMATION PROTOCOL
OSPF	OPEN SHORTEST PATH FIRST
EIGRP	ENHANCED INTERIOR GATEWAY PROTOCOL
USB	UNIVERSAL SERIAL BUS
ICMP	INTERNET CONTROL MESSAGE PROTOCOL

LISTAS DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Quando uma rede sem um projeto de estruturação é iniciada, ocorrem muitos problemas e dificuldades no decorrer da implantação, principalmente o desperdício de material, como aquisição de equipamentos sem necessidade, perda de tempo por falta de um cronograma, e tudo isso acaba gerando alguns custos extras. Outras dificuldades decorrentes do não planejamento adequado, também dificultam a manutenção da rede posteriormente e a interfere negativamente na qualidade do serviço.

Reestruturar uma rede baseando-se nas normas e melhores práticas de mercado, proporcionará benefícios no desempenho, na segurança e no gerenciamento da mesma, principalmente quando essas redes estão na fase de rápida transição para um porte maior. Este projeto abordará uma comparação entre uma rede que atualmente não está estruturada e a mesma após a aplicação de boas práticas de estruturação, visando evidenciar as diferenças de desempenho, organização e manutenção.

O local onde será implementado a reestruturação, é uma rede que teve um crescimento rápido e passou de pequeno para médio porte e ainda se encontra em expansão. Hoje trafegam pela rede, voz sobre *IP*, estações de trabalho, servidores, automação, impressoras de rede, entre outros serviços.

Para realizar a reestruturação foi considerado os diversos fluxos de dados existentes na rede, e revisaremos toda a parte física e lógica para aplicar através de boas práticas e referências técnicas e teóricas a reorganização da estrutura da rede, assim garantindo a melhoria em desempenho, segurança e gerenciamento da mesma.

1.1 OBJETIVO GERAL

Com base em estudos de autores influentes na área de redes de computadores, o objetivo é verificar através de boas práticas e recomendações bibliográficas os motivos que levam uma rede a ficar lenta e vulnerável. Posteriormente, será levantado as possibilidades que a rede nos oferece para

elaborar o plano de reestruturação. Verificado a possibilidade de reestruturação, será elaborado um projeto de reestruturação de acordo com a necessidade da empresa. Com o levantamento dos dados, será dado início a reestruturação da mesma.

1.2 OBJETIVOS ESPECÍFICOS

- Realizar pesquisa bibliográfica;
- Realizar levantamento atual do estado da rede;
- Planejar a nova estrutura da rede;
- Implementar a estruturação da rede;
- Comparar resultados obtidos.

1.3 JUSTIFICATIVA

Por falta de conhecimento sobre o assunto a administração da empresa acredita ser desnecessária uma reestruturação de rede, pois é apenas um meio de mandar informações de um lado para outro, conectar câmeras de monitoramento, entre outras coisas. Mas isso se faz necessário para que os integrantes da equipe de suporte técnico tenham maior controle do que trafega pela rede, além de ganho em desempenho e em segurança.

Geralmente a alta direção das empresas ignoram o ganho de qualidade, velocidade, segurança e demais vantagens quando se tem uma rede corretamente estruturada, que apesar de como eles pensam, os gastos que temos para implantar uma boa infraestrutura é pequeno em relação aos benefícios obtidos.

Será realizada a reestruturação da rede buscando a melhoria em termos de desempenho, segurança e gerenciamento de rede, através de configurações estudadas e planejadas adequadamente, demonstrando com isso seus respectivos benefícios.

1.4 ESTRUTURA DO TRABALHO

No capítulo 2, será abordado os conceitos sobre o modelo *TCP/IP* de modo geral e explicado detalhadamente as camadas de enlace de dados com ênfase em *VLANs*, posteriormente na camada de rede serão abordados os conceitos de roteamento.

No capítulo 3, será apresentado uma breve descrição dos equipamentos e softwares que serão utilizados para desenvolver o projeto.

No capítulo 4, será demonstrado como foi planejado o novo projeto de rede e sua aplicação.

No capítulo 5, será demonstrado os resultados obtidos e as comparações com o antigo cenário.

Por fim, no capítulo 6, será apresentado as conclusões obtidas através de análises e comparações dos resultados atingidos.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo será abordado conceitos sobre o modelo *TCP/IP* e todas as suas camadas, frisando a importância das *VLANs* em uma rede para melhor gerenciamento, monitoramento e organização, e quais as opções de agrupamento que este protocolo possui. Neste ponto, será colocado em ênfase a importância nos temas como cascateamento, empilhamento, roteamento, *loop* em redes e por último abordando à segurança da informação.

2.1 MODELO *TCP/IP*

Segundo Tanenbaum (2011), este modelo é usado como referência no mundo desde a primeira rede, a ARPANET e é usada até hoje. A ARPANET começou no final da guerra fria, quando o Departamento de Defesa (DoD) dos EUA precisava de uma rede confiável para se comunicar, tendo em conta que a rede de telefone da época era vulnerável e de pequena redundância, pois se algumas centrais fossem destruídas ficaria complicada a comunicação. Quando os EUA perdeu a corrida espacial contra a União Soviética, seu atual presidente queria descobrir o que tinha dado errado e acabou vendo que seus três exércitos estavam em disputa por orçamento, assim, limitando os três. Foi ai que criaram a ARPA.

Em 1967, Larry Roberts começou a voltar a atenção da ARPA para redes, procurou vários especialistas até que Wesley Clark teve a ideia de criar uma sub-rede comutada por pacotes, dando a cada *host* seu próprio roteador. Após apresentar a proposta, decidiu construir o que um dia ficaria conhecido como ARPANET e depois também como Internet.

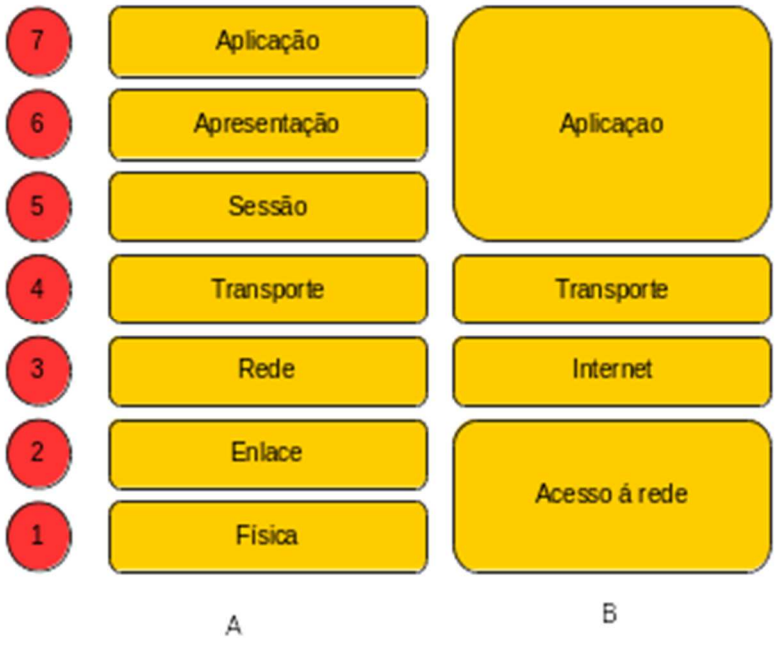
A sub-rede era formada por minicomputadores (IMPs) conectados por linhas de transmissão e para garantir sua disponibilidade seriam conectados a no mínimo mais dois IMPs, para que se algumas linhas fossem destruídas não perdessem comunicação. Cada IMP deveria ter um *host* na mesma sala, para enviar mensagens de até 8063 *bits* para seu IMP onde ele dividiria em pacotes de no máximo 1008 *bits* e encaminharia até o destino. Foi a primeira rede onde primeiro se recebia o pacote por inteiro antes de ser encaminhado. Quando

começou a ser implantado, aconteceram muitos problemas por incompatibilidade, tanto de *software* quanto de máquina, o que levou os pesquisadores a procurar novos protocolos.

Em 1974 Cerf e Kahn criaram o protocolo mais usado e conhecido do mundo, o *TCP/IP*. “[...] O *TCP/IP* foi criado especificamente para manipular a comunicação sobre inter-redes, algo que se tornou mais importante à medida que um número maior de redes era conectado à ARPANET.” (TANENBAUM, 2002).

Para ampliar a área de proliferação do protocolo, a ARPA propôs integrar ele ao UNIX de Berkeley. Com isso os pesquisadores da Berkeley criaram um *software* para a rede (soquetes) e criaram programas de gerenciamento para facilitar a interligação de redes. Como muitas universidades tinham acabado de adquirir alguns computadores, está ferramenta veio bem a calhar para conectar os computadores tanto na sua rede *LAN* quanto na ARPANET.

Figura 1 - Modelo *TCP/IP* vs OSI.



Fonte: Autores (2017).

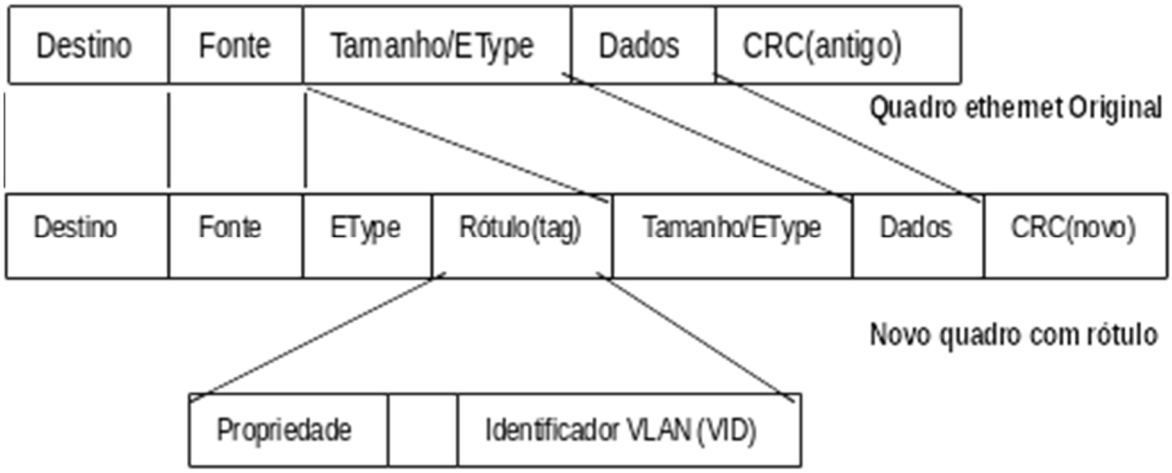
Diferente do modelo OSI, como mostra a figura A, o *TCP/IP*, na figura B, se resume a quatro camadas onde enlace e física se unificam e apresentação e sessão, no TCP ficam presentes na aplicação.

Abaixo, será justificado e referenciado cada um dos modelos de CAMADA no *TCP/IP*.

2.1.1 Camada de enlace

A parte física de acesso, como conectores, são definidos esta camada, como também o padrão de dados adotado, serialmente ou paralelamente. (FILIPPETTI, 2016).

Figura 2 - Quadro Ethernet



Fonte: CCNA(2016) – adaptado.

Segundo Filippetti (2016), em meados dos anos 70, o pesquisador Roberto Metcalfe criou o protocolo *Ethernet*. Alguns anos após cria-lo, resolveu homologar o padrão ao IEEE para sanar os problemas de venda e pesquisa, que pela falta de padrão aconteciam com frequência. Quando homologada, suas especificações foram totalmente disponibilizadas, para não ocorrer mais esses problemas.

O padrão *ethernet* concentra seu trabalho na camada de interface física, onde inicialmente ele trabalhava em até 10Mbps e cada *frame* varia de 64 até 1518

bits. Ele consiste basicamente em três elementos. O meio físico, as regras de controle de acesso e os *frames*.

A função do meio físico é definir como serão transmitidos os dados pelos cabos de rede, agrupar os dados entregues pelos protocolos de alto nível e colocar nos *frames* que serão enviados através da rede.

O endereçamento da rede é feito através do endereço *MAC*, que são representados por seis números hexadecimais. Cada hexadecimal equivale a um número de quatro *bits*. Os endereços *MAC* são padronizados da seguinte forma: os três primeiros *bytes* são o endereço OUI que indicam o fabricante da placa de rede, os três últimos são controlados pelo fabricante, e cada unidade produzida recebe um número diferente.

Quando os dados são transmitidos na rede local usamos o *frame*, pois o endereço *MAC* é o necessário para ir do equipamento de origem até o equipamento de destino. Se precisarmos mandar dados a outro local pela internet, o endereço da rede no pacote contém o destino final do *host* para o qual o pacote está sendo enviado.

Este padrão usa uma arquitetura onde cada nó recebe tudo o que é transmitido pelos outros, em redes com tráfego muito intenso seu desempenho cai, assim não alcançando seus valores nominais que estatisticamente possibilita um rendimento máximo de 37% do total. O tamanho da carga se torna mais importante quando as aplicações que usam grandes arquivos utilizam a rede, onde a taxa de utilização fica comprometida.

Como maioria das tecnologias a *ethernet* ainda está se desenvolvendo, e assim foram surgindo novas versões como 100Mbps, 1000Mpbs e até velocidades ainda mais altas. O cabeamento físico também melhorou consideravelmente, além de outros recursos também. (TANENBAUM, 2002).

De acordo com Kurose (2013), os serviços oferecidos na camada de enlace são:

Enquadramento dos dados: Neste serviço, é feito um encapsulamento do dos pacotes em quadros, onde, os dados são quebrados e inseridos em datagramas para somente assim, ser transmitido pelo enlace. A estrutura desse quadro e definido pelo protocolo deste enlace. A definição e organização de transmissão e recebimento desses datagramas está definida no cabeçalho. Acesso ao Enlace: O *MAC* (*médium access control*), denominado um protocolo de enlace,

define e organiza a estrutura de permissão e comunicação o qual um quadro é enviado pelo enlace.

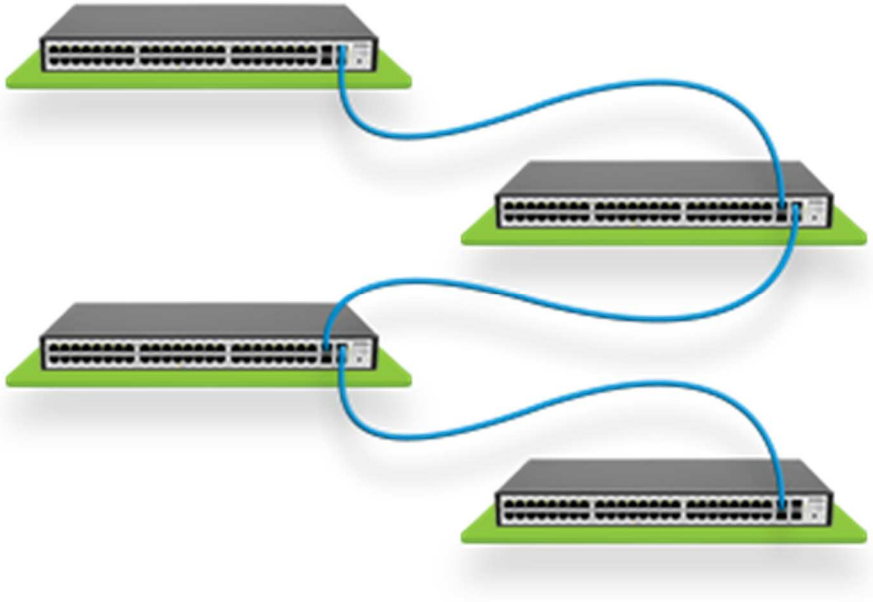
Entrega confiável: Aqui temos protocolos de enlace, que garantem a entrega dos pacotes de forma segura e completa pelo enlace, como por exemplo, o TCP. Os quadros e confiabilidade desses pacotes transmitidos estão ligado ao tempo de resposta, tamanho e *jitter*, onde *jitter* é a latência de tempo e resposta da transmissão pelo enlace.

Detecção e correção de erros: Muitos protocolos de enlace disponibilizam esse mecanismo, onde o nó transmissor, encaminha também *BITS* de detecção de erro ao destino. Assim, o nó receptor faz uma análise desse pacote e verifica sim ou não a necessidade da correção de erros deste pacotes perdidos. A correção é feita, quando o nós transmissor, é requisitado para reenviar o pacote, anteriormente inválido.

Atualmente falando, é muito presente esse cenário de detecção e correção de erro, no enlace de sinal *wireless*, onde pode acontecer ruídos ou interferências eletromagnéticas dos sinais transmitidos e recebidos.

- CASCATEAMENTO

Figura 3 - Exemplo de cascateamento.



Fonte: Televit(2015) – adaptado.

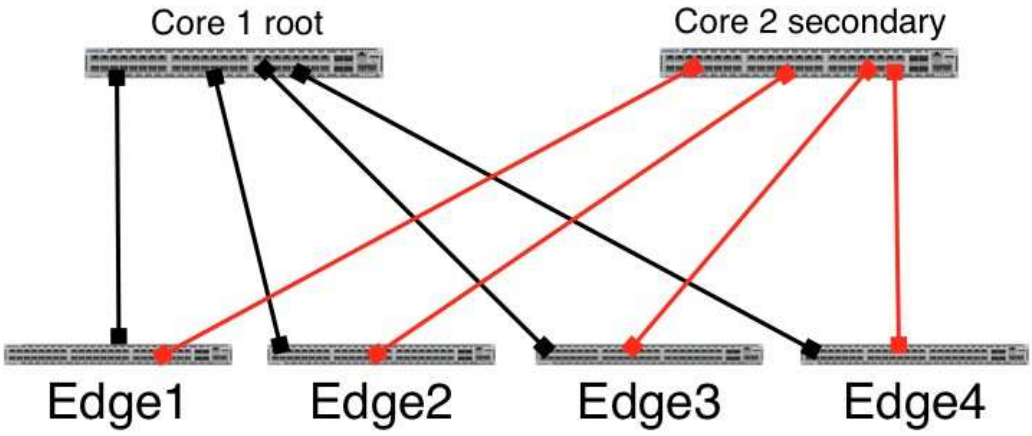
Cascateamento é um modo de interligar vários *hubs* de um modo prático e barato. A ligação deles é através de uma porta de *link* nos dois equipamentos,

sendo limitadas a velocidade de banda *Gigabit*. Além das limitações de cada fabricante, existem algumas regras para utilizar o cascateamento entre *hubs*. Uma delas é a regra 5-4-3 onde o 5 limita o número de segmentos e no máximo 100 metros cada, o quatro é o número máximo de repetidores e o três mostra que apenas 3 segmentos podem conter *host*s, mas ela só deve ser usada em *hubs Megabit*. Em redes com *switch*es *Gigabit* não é permitido cascateamento pois o *broadcast* fica incontrolável.

Já os *switch*es podem segmentar um rede sem aumentar a latência e não limitam o uso de segmentações no geral, mas cada fabricante tem uma indicação diferente. O endereço de destino do pacote é verificado para determinar a qual segmento se destina e este é colocado somente no segmento-destino.

- EMPILHAMENTO

Figura 4 - Exemplo de empilhamento.



Fonte: Site HP(2017) - adaptado

Já no empilhamento a interligação dos *switch*es ocorre através de uma porta especifica para esse serviço, chamada *stack*. Cada fabricante tem sua interface e determina qual a velocidade da *stack* que geralmente é maior que a velocidade das outras portas. O empilhamento só pode ser feito através de equipamento da mesma marca, já que quando empilhados se tornam praticamente um equipamento só. Uma de suas vantagens é que a porta usada para empilhar os aparelhos é traseira e dedicada exclusivamente para esse fim, então assim todas as portas frontais ficam disponíveis para uso de rede.

2.1.2 Camada de internet

A camada de rede existe por conta de duas razões:

- Identificação lógica de redes e elementos a elas conectados.
- Roteamento dos pacotes de dados de um domínio lógico para outro.

O objetivo da camada de Internet e providenciar a parte de compatibilidade de protocolos definidos na camada de acesso à rede. Esse papel importante de roteamento lógico dos pacotes é feito somente pela camada de internet. A camada de internet é extremamente importante, pois ela promove através do protocolo *IP*, uma rede unificada fornecendo comunicação entre as aplicações dentro de um mesmo cenário. (FILIPPETTI, 2016).

A camada de rede se define através do protocolo *IP*. O protocolo em referência disponibiliza da interligação e comunicação entre redes com diferentes topologias. O objetivo deste protocolo é criar um modelo homogêneo entre os diferentes tipos de datagramas de aplicações permitindo assim, a comunicação entre esses processos.

O *IP* é um protocolo orientado a conexão, que garante um serviço confiável de comunicação entre os pacotes enviados e recebidos utilizando, por exemplo, controle de fluxo.

- ROTEAMENTO

De acordo com Filippetti (2016), o conceito de roteamento, se baseia a “Um conjunto de regras que definem como dados originados em uma determinada rede devem alcançar uma rede distinta”.

Logo, um roteador ou então um serviço de roteamento deve conseguir fazer o direcionamento dos pacotes, de acordo com o cabeçalho que possui informações de origem e destino e consultando a rota por onde deve transmitir. Assim, sendo uma ponte.

> O roteamento é a principal forma utilizada na Internet para a entrega de pacotes de dados entre hosts (equipamentos de rede de uma forma geral, incluindo computadores, roteadores etc.). O modelo de roteamento utilizado é o do salto-por-salto (hop-by-hop), onde cada roteador que recebe um pacote de dados abre-o, verifica o endereço de destino no cabeçalho IP, calcula o próximo salto que vai deixar o pacote um passo mais próximo de seu destino e entrega o pacote neste próximo salto. Este

> processo se repete e assim segue até a entrega do pacote ao seu destinatário. No entanto, para que este funcione, são necessários dois elementos: tabelas de roteamento e protocolos de roteamento.
> (DE MOURA, 2004)

Atualmente, a comunicação entre redes, é feita de modo *hop-by-hop*(de salto em salto), onde cada roteador recebe um pacote, abre e verifica quem é o destino, caso não seja ele, ele retransmite para a rota mais próxima, assim, até que o pacote chegue ao destino. Assim é feito o roteamento mundial. E um dos principais protocolos deste modelo é o DNS. No entanto, neste cenário, as tabelas de roteamento se tornam indispensáveis.

O roteamento interno de uma rede é possível através de protocolos internos, estes são: IGRP, RIP, OSPF e EIGRP.

2.1.3 Camada de transporte

Entre a camada de aplicação e rede, está a camada de transporte. Ela é importante e central, pois fornece serviços de comunicação para as aplicações que rodam em diferentes hospedeiros. Oferecendo assim, comunicação LÓGICA e não física entre aplicações. (KUROSE, 2013).

No modelo *TCP/IP* a camada de transporte, também chamada de *host-to-host*, permite que as entidades pares dos *hosts* de origem e de destino mantenham uma conversação. (TANENBAUM, 2002).

Nesta camada, destaca-se dois protocolos de redes, o TCP e o UDP. O TCP recebe um fluxo de dados de uma aplicação e divide em partes, ou melhor, quebra em pedaços menores e são numerados, assim transmitidos sequencialmente, esses segmentos, assim, permitindo a remontagem dos dados na camada de transporte do destino. A partir deste modelo, há uma qualidade maior e melhor da informação e da validação e garantia de entrega e recebimento dos pacotes. (FILIPPETTI, 2016).

UDP, a transmissão de pacotes é feito de forma não confiável. Diferente do TCP, não é feito a verificação de resposta e entrega do pacote, assim não tendo a total garantia e confiabilidade do mesmo. O meio de transmissão de mensagens

UDP percorre por uma porta, assim, verificado o mesmo serviço no endereço de entrega, há a conexão e compartilhamento dos dados transmitidos.

O UDP trabalha na camada e protocolo de *IP* para receber e enviar mensagem entre cliente e servidor. Um ponto interessante no UDP é que ele não consome tanta banda da rede, pois é um meio de transporte simples e eficiente. (CARMONA e HEXSEL, 2005)

2.1.4 Camada de aplicação

Também chamada de camada de acesso ou de enlace, a partir desta camada é verificado o meio físico de acesso e também os conectores. O padrão seguido define como será transmitida a informação bem como os protocolos de comunicação. Por exemplo, o mais conhecido conector é do tipo RJ-45 onde ele utiliza um tipo de barramento e meio físico de transmissão e recepção de informação, assim como o RS-232 utiliza de outro barramento e possui suas particularidades. (FILIPPETTI, 2016).

É a camada mais simples e palpável do modelo *TCP/IP*, pois está diretamente presente no nosso dia a dia, tanto a nível administrador de sistemas como um simples usuário. Nesta camada, encontramos aplicações finais, como aplicações de comunicação, de acesso. Exemplos: Skype, P2P.

As APIs, que são interfaces que vão utilizar os protocolos de comunicação para transferir e receber pacotes, como TCP e UDP.

> Temos os operadores de rede, que são os serviços por trás da aplicação para que a rede funcione, que o pacote seja transferido e recebido. Um exemplo é o DNS que faz a conversão do domínio de um site ou um local e permite a conexão diretamente para o IP real daquele destino. Assim convertendo o nome do HOST para seu real IP de rede. (TANENBAUM, 2002).
> Outro também bastante importante é o SNMP que permite monitoramento e gerenciamento de rede e DHCP, criado em 1993 que permite a configuração e disponibilidade de ENDEREÇOS automáticos de ativos em uma rede de comunicação. (FILIPPETTI, 2016).

As aplicações de usuários citadas anteriormente, que dependem das camadas anteriores para funcionar, englobam programas e aplicações ligadas e disponibilizadas ao usuário. Alguns protocolos são de extrema importância, como o HTTP que permite a comunicação a partir do *browser* de navegação do cliente.

Outro protocolo que será citado sem muitas delongas, é o FTP que permite o transporte de arquivos entre os usuários.

2.2 IEEE

Conhecido como IEEE, a *Institute of Eletrical and Eletronic Engineers* se trata de uma organização que tem por objetivo fomentar conhecimentos na área de eletrônica e computação. Fundada em 1963 nos Estados Unidos a companhia conta com uma grande equipe de colaboração para o projeto espalhada em todas as partes do mundo, inclusive no Brasil onde um dos maiores projetos e destaque, é a criação, padronização e organização de normas técnicas para o campo de atuação e padrões de dispositivos eletrônicos e computadores.

O IEEE agrega com mais de 400.000 associados e colaboradores para o projeto, entre cientistas, engenheiros, pesquisadores e outros profissionais, em cerca de 150 países.

O Instituto é o responsável por normas e regulamentação que são implementadas internacionalmente nas áreas da engenharia elétrica e informática. Por exemplo, os padrões de redes sem fio ou com fio, formatos e códigos são atribuídos pelo IEEE. Ao exercer essa função, o Instituto deixa a ISO e a ABNT menos carregada para focar nas normas de outras áreas e campos.

A IEEE foi originalmente formada pela fusão de duas outras instituições, o AIEE (*American Institute of Electrical Engineers*) e o IRE (*Institute of Radio Engineers*). Em janeiro de 1963, os dois Institutos foram formalmente fundidos, e o resultado dessa fusão, o IEEE, se expandiu por todo o mundo, desempenhando atividades de pesquisa e criação de normas nos campos das engenharias elétrica e computação.

2.3 NORMA 802.1Q

Em uma rede sem configuração nos *switches*, todos os *frames* que vão em direção a alguma máquina da rede, chegam a todas as máquinas que nele estiverem conectadas. Quando o *frame* fica trafegando pela rede a outros lugares

que não seja seu destino, causa um problema chamado tempestade de *broadcast*, que acaba acarretando problemas de lentidão para ela. Para resolver esta dificuldade foi elaborada uma normativa que regularizou uma forma de criar *LANs* virtuais, onde ela separa as redes e vai segmentando uma grande parte de domínios de *broadcast* sem precisar usar *routers*, pois os *broadcasts* criados dentro de uma *VLAN* continuarão somente nela, assim não afetando as outras *VLANs*, mesmo sendo no mesmo *switch* físico.

Segundo Carmona e Hexsel (2005), as *VLANs* são atualmente a melhor opção custo benefício para se estruturar uma rede, pois não precisaria comprar um *switch* para cada serviço, pois a função dela é criar dentro de um *switch* várias sub-redes lógicas, que são definidas pelo IEEE conforme o padrão 802.1Q, dentro de uma só rede, as unindo depois através de um roteador.

Sobre as *VLANs* é possível dizer que são suportadas por diversos tipos de *switches*, atualmente quase todos. Nelas as estações de trabalho, por exemplo, podem ser separadas em uma única *VLAN* jogando os quadros de *broadcast* somente entre a mesma *VLAN*. Os principais objetivos da *VLAN* são basicamente:

- Melhorar o desempenho geral do tráfego de rede;
- Aumentar a segurança de um determinado segmento de tráfego, separando-o do tráfego comum (utilizado por todas as estações de rede);
- Impedir as interrupções e quedas de rede causada pelo retorno de quadros inválidos, enviados pelo broadcast de rede a endereços inexistentes ou inválidos. (CARMONA e HEXSEL, 2005)

Segundo Freeman e Passmore (1996), as *VLANs* podem ser classificadas em quatro formas de agrupamento: Por portas, endereços *MAC*, camadas de rede e IP *multicast*.

2.3.1 Agrupamento por endereço físico (*MAC*)

O agrupamento por endereço físico é um estilo de configuração onde é cadastrado o endereço *MAC* do computador na *VLAN*. Suas vantagens são que mesmo ela mudando de local físico ela ainda vai pertencer a mesma *VLAN* de antes, pois o *switch* armazena seu *MAC* na memória.

Uma das desvantagens é que nenhuma máquina pode ficar sem uma *VLAN* configurada, mas dependendo da marca do *switch*, ele vem com um programa pra detectar todos os *MACs* que não estão atribuídos a nenhuma *VLAN* e avisa sobre o ocorrido. Outro problema que mostra as limitações deste agrupamento é que quando um usuário com um *notebook*, por exemplo, usa a rede através de cabo e através de *Wi-Fi* ao mesmo tempo, o computador pode acabar se perdendo, devido a máquina estar com dois *MACs* diferentes acessando a rede ao mesmo tempo sendo um da *Wi-Fi* e outro da placa de rede via cabo.

2.3.2 Agrupamento por IP multicast

Segundo Freeman e Passmore (1996), este agrupamento funciona através de um *proxy*. Cada grupo de *VLAN* possui um *IP* especifico que funciona como um *proxy*, onde todos os pacotes chegam até ele. Cada estação de trabalho recebe a oportunidade para responder afirmativamente a uma notificação de pacotes, que sinaliza a existência desse grupo. Todas as estações que entram naquele grupo podem ver os membros da mesma *LAN*. Entretanto, eles são membros desse grupo somente por um determinado tempo. Assim sendo, a natureza dinâmica das *VLANs* definidas por *IP multicast* permite um grau muito elevado de flexibilidade e sensibilidade da aplicação. Além de tudo, as *VLANs* definidas por grupos de *multicast IP* seriam capazes de abranger roteadores e, portanto, conexões *WAN*.

2.3.3 Agrupamento por camada de rede

As *VLANs* baseadas nas informações da camada 3 levam em consideração o tipo de protocolo ou o endereço da camada de rede (sub-redes) para determinar a *VLAN*. Apesar de ser baseada na camada 3, essa *VLAN* não tem uma função de encaminhamento e não deve ser confundida com roteamento da camada de internet.

Mesmo que um *switch* inspecione de qual IP vem o pacote para determinar sua *VLAN*, não é calculada nenhuma rota. Às vezes, o *switch* que tem essas *VLANs*

baseados nas informações e roteamento da camada 3, a conectividade dentro de uma *VLAN* ainda é vista como uma topologia plana.

Há algumas vantagens nesta *VLANs*. Ela permite a partição por tipo de protocolo. Esta pode ser uma boa opção para redes dedicadas a serviços ou aplicativos. Ela também permite que os usuários pudessem mover-se fisicamente suas estações de trabalho sem ter que reconfigurar o endereço de rede. Mas tem desvantagens também, como o *desempenho*. Inspecionar os pacotes é mais demorado do que olhar para endereços *MAC*. Por esse motivo, os *switches* que usam essas informações para definição de *VLAN* são geralmente mais lentas do que aquelas que usam informações da camada 2.

2.3.4 Agrupamento por portas

É o modo mais comum e simples de se configurar uma *VLAN*, como o próprio nome diz é uma *VLAN* que separa as *LANs* por portas no *switch*.

Será utilizado o agrupamento por porta, pois segundo Held (2003), o ganho de desempenho é muito maior comparado aos outros agrupamentos. As vantagens incluem a habilidade de se usar as capacidade de comutação do equipamento de interconexão e a habilidade de suportar cascateamento.

Freeman e Passmore (1996) cita alguns pontos negativos nesse agrupamento, sendo um desses pontos; como cada cabo de rede poderá estar conectado somente a uma porta no *switch*.

2.3.5 VLAN Trunking Protocol

Como em redes de grande porte era praticamente inviável configurar *VLANs* em todos os *switch*es, a Cisco criou o VTP, o qual seria um gerenciador de *VLAN*. Para ser possível trabalhar com este tipo de serviço é necessário ter um domínio de VTP onde todos os *switch*es desejáveis estarão conectados e dentro deste domínio haverá um servidor de VTP que gerenciará todas as ações nas *VLANs* dos mesmos, aplicando em todos os eles, toda e qualquer alteração que for feita no servidor. Outra possibilidade para aumentar a segurança deste protocolo é

que pode ser implementada uma senha para este domínio de VTP onde só tem acesso as informações do servidor os clientes onde a senha estiver correta, diminuindo a probabilidade de algum *switch* que não necessite configuração ingressar no VTP. Caso a rede necessite de uma redundância para o *switch* servidor, é só configurar outro *switch* como servidor e deixa-lo rodando normalmente, pois o único ativo da rede será o mais antigo. Como este protocolo foi criado pela Cisco, uma empresa privada, ele foi patenteado e para usar do mesmo terá que ter toda sua rede que pretende configurar neste protocolo os equipamentos da Cisco.

Algumas das vantagens que vemos sobre o VTP são: Ele permite que se adicione, exclua ou altere as *VLANs* de forma centralizada. Outra vantagem é que o controle que se tem das *VLANs* é muito maior, do que em uma rede sem VTP.

Não só de vantagens é feito esse protocolo, também temos algumas desvantagens como: Toda vez que for instalado um novo equipamento no domínio VTP você corre o risco de ter que refazer uma revisão de configuração e também é bom evitar uma *VLAN* que meça toda a rede.

Modos de Operação VTP: Existem quatro estados em que os *switch*es podem ser configurados neste ambiente. Segue uma explanação entre eles.

Server Mode: É o modo servidor, quem em uma rede desde ambiente tem que existir pelo menos um e não tem uma limitação de quantidade, mas somente um será o primário e todos os outros serão denominados secundários e toda a configuração que o primário fizer eles aceitarão essa atualização. Ele tem a permissão para criar, modificar e excluir *VLANs* dentro do domínio VTP.

Client Mode: É um modo onde a *switch* recebe informação e repassa, a única diferença do modo servidor é que ele não tem o poder de gerenciar as *VLANs*.

Transparent Mode: Neste modo, o *switch* recebe as informações do servidor VTP e transmite para os *switch*es vizinhos dele, mas não pega a configuração recebida, pois tem sua própria configuração. Mesmo tendo sua própria configuração ele não a propaga para lugar algum.

Mode Off: Basicamente a mesma coisa que um *switch* em modo transparente, a única diferença é que ele não propaga a configuração recebida do servidor VTP.

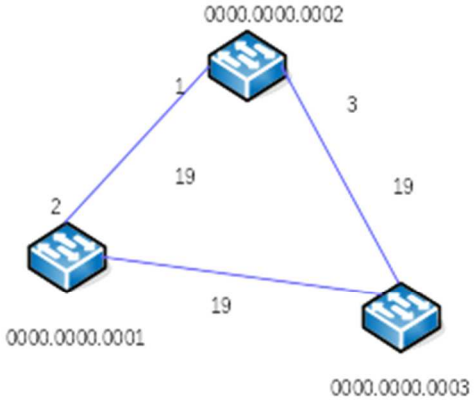
2.4 NORMA 802.1D

Uma rede ótima não se priva a somente qualidade na transmissão de *frames*, mas também a estar sempre disponível, se recuperando de pequenas falhas. Criada pela DEC foi homologada posteriormente pela IEEE como norma 802.1d. Este protocolo consiste principalmente em monitorar a rede para que não tenha nenhuma conexão redundante, evitando *loops*. Ele monitora toda a rede e quando encontra algum ponto redundante usa alguns critérios para definir uma porta primária e desativa a outra. Caso a porta primária falhe, ele reativa a porta secundária que estava desativada, não deixando a rede parar.

O STP funciona da seguinte forma: O protocolo determina através do *MAC* um *switch* para ser o *switch* raiz, escolhendo o que tem o menor *MAC*, onde os outros *switches* da rede são denominados *switches* de menor custo. Em uma rede pode existir apenas um *switch* raiz. Para determinar qual será a porta que ficará em *stand-by* utiliza-se uma tabela de custo, onde o custo de cada caminho é calculado e após calcular, uma ou mais portas de algum *switch* é desativada.

"[...] O custo é inversamente proporcional à largura da banda do caminho. Isso significa que, quanto menor o custo, maior a largura da banda do caminho. [...]" (FILIPPETTI, 2016).

Figura 5 - Exemplo de STP.



Switch	Porta	Custo
2	1	19
2	3	19+19
3	1	19
3	2	19+19

Fonte: Filippetti(2016) – adaptado.

No exemplo acima, como dois caminhos tem o mesmo valor para ser desativado, ainda levamos em conta o *MAC* do *switch* para determinar qual porta será bloqueada. Neste caso foi desativada a porta 2 do *switch* 3.

Um dos problemas aparentes deste protocolo é a demora para ativar um *link* secundário quando o primário falha, pois até passar pelas verificações do protocolo demora em torno 30 segundos ou mais para ativar novamente a rede.

2.4.1 Norma 802.1W

O protocolo 802.1w é uma versão melhorada do protocolo 802.1d. Quando a Cisco aplicou algumas melhorias em alguns pontos do protocolo 802.1d, o IEEE regulamentou ela com outra norma para essa nova versão, criando o protocolo RSTP ou 802.1w. A Cisco desenvolveu três novas funcionalidade que foram implementadas no 802.1w nos aparelhos da própria marca. O *PortFast*, o *UplinkFast* e o *BackboneFast*. Como as tecnologias que eles aplicaram sobre esse protocolo eram deles, eles tinham os direitos autorais legais para usa-las. Para sanar este problema, o IEEE regulamentou essas melhorias criando este novo protocolo.

A tecnologia do *PortFast* refere-se aos equipamentos da sua rede onde é certo que não ocasionará um *loop*, como um computador ou uma impressora de rede que tem só uma porta *ethernet*, sendo assim você pode informar ao *switch* que a porta onde esse equipamento está pode ficar fora da verificação do protocolo 802.1w. Para evitar verificações desnecessárias e ocupar processamento sem necessidade foi criado esta tecnologia.

O *UplinkFast*, é a tecnologia que identifica o erro no *link* primário e ativa o *link* secundário. O grande problema do protocolo 802.1d é que demorava cerca de 30 segundos para identificar o erro e ativar o *link* de *backup*, e com essa nova tecnologia o tempo passou para menos de 2 segundos.

A última melhoria do protocolo 802.1d foi o *BackboneFast*. Quando ele se encontra ativado, faz uma varredura na rede em todos os *switches* que estão no mesmo seguimento, em cascateamento, analisa e identifica se tem algum problema no *link* e se tem alguma solução possível onde ele mesmo possa corrigir. Seu

monitoramento de rede pode diminuir em até 20 segundos o tempo de convergência de uma rede STP.

2.5 SEGURANÇA

De acordo com Stallings (2014) segurança de rede possui métricas para contornar, precaver, detectar e reparar violações de segurança que possua tráfego de informações. Essa definição apresenta os três pilares da segurança da informação: confidencialidade, integridade e disponibilidade, conhecidos normalmente como tríade CID.

Confidencialidade: Ela é a responsável por garantir a autorização e restringir o acesso as informações confidenciais, garantindo que somente pessoas autorizadas tenha acesso a tais informações. Uma quebra na confidencialidade seria a perca dessas informações possibilitando o público não autorizado ter acesso ao mesmos.

Integridade: Responsável por garantir a não alteração ou a destruição da informação. Uma perda de integridade seria a modificação ou exclusão não autorizada das informações.

Disponibilidade: Garante que o sistema esteja sempre disponível juntamente com seus serviços para que quando os usuários permitidos necessitarem acessar o mesmo tenham sucesso. Uma indisponibilidade seria a a perda do acesso no sistema. Embora o emprego da tríade CID esteja bem estabelecido, algumas pessoas influentes na área de segurança da informação percebem que alguns conceitos adicionais são necessários para se apresentar um quadro completo como, autenticidade e responsabilização.

Autenticidade: Garante que a transmissão da mensagem na origem e no destino sejam legitimas ou seja garante que o usuário que está realizado essa transmissão seja autentico e cada acesso no sistema seja verdadeiro.

Responsabilização: Neste ponto, o objetivo da segurança é quem cria o requisito para que execução de um indivíduo sejam concedido exclusivamente a ela. Isso fornece irretratabilidade, dissuasão, isolamento de falhas, detecção e precaução contra invasão, além da restauração pós-ação e ações jurídicas. Os sistemas não são totalmente seguros, é necessário que seja capaz de associar a

quebra de segurança a um responsável. Os sistemas devem armazenar os registros das ações para que possa ser realizada análise forense caso necessário, assim podendo encontrar as quebras de segurança ou ajudar em concorrência de transação.

3 AMBIENTE EXPERIMENTAL

Neste capítulo será explicado as ferramentas técnicas e físicas as quais fornecerão fundamento para o desenvolvimento deste trabalho, como por exemplo modo de aplicação, *softwares*, *hardwares* e os métodos a serem utilizados. A partir destas ferramentas, será elaborado uma métrica qual servirá de base para análise e comparativo entre resultados.

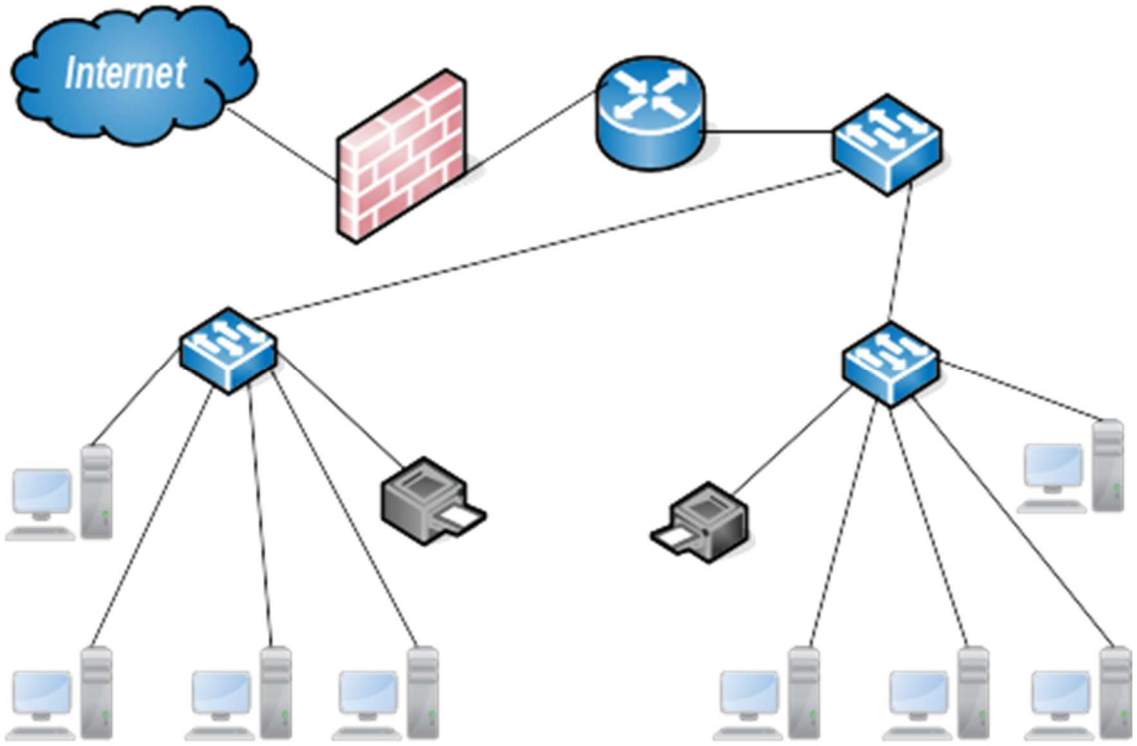
Protocolos de redes, juntamente com os itens abaixo relacionados, formam um conjunto ferramental de grande importância para o desenvolvimento do trabalho.

- Roteador;
- *Switch*es;
- Servidores;
- Computadores;
- *Packet Tracer;*
- *Wireshark;*

3.1 REDE LOCAL ATUAL

A rede onde será realizada a reestruturação, teve um crescimento muito rápido no começo, e ainda se encontra em expansão. Hoje trafegam pela mesma vários equipamentos variados como: estações de trabalho, servidores, equipamentos de automação, impressoras de rede, telefones *VoIP*, entre outros. A reserva administrativa dos mesmos é um segmento único onde todos os dispositivos trabalham na mesma rede, sendo assim muitos dos problemas encontrados acontecem por conta ou decorrente desse mal planejamento de implementação, pois baseando-se nas boas práticas do mercado e em estudos de grandes autores da área, existindo somente um domínio de *broadcast* na rede a perda de desempenho e de segurança é enorme pois todos os serviços se compartilham da mesma segmentação, sendo assim de qualquer lugar da empresa alguém pode acessar um servidor, por exemplo, e derrubar a rede com ataques. Pode-se observar um exemplo da rede atual abaixo na Figura 4.

Figura 6 - Configuração atual de rede.



Fonte: Autores (2017)

Atualmente nosso endereçamento de rede, se resume as seguinte faixas de IP:

Tabela 1 – Sub-Redes do endereçamento atual.

ENDEREÇO DE IP	SERVIÇO
10.101.0.0/16	Voz
10.201.0.0/16	Dados

Fonte: Autores (2017)

Como pode-se observar na tabela 1, o primeiro item de Sub-Redes possui duas faixas de IPs, um sendo para trafego de voz e o outro para trafego de dados.

Tabela 2 – Faixa de endereçamento de IP atual.

ENDEREÇO DE IP	SERVIÇO
10.101.10.0/16	VoIP
10.201.13.0/16	Estações de Trabalho
10.201.25.0/16	Impressoras de Rede
10.201.30.0/16	Relógio Ponto
10.201.40.0/16	*Switches* e Roteadores

Fonte: Autores (2017)

No item faixas de endereços de IP na tabela 2 pode-se observar a classificação dos serviços por faixa de IPs, mas tudo dentro da mesma rede.

3.2 PROPOSTA DE REDE

Conforme dito acima, na rede atual os serviços são separados por faixas de IP e a proposta é realizar as configurações necessárias para que cada serviço possua sua própria *VLAN*, assim trazendo ganho na organização e, desempenho da rede, na segurança das informações que trafegam pela mesma. As *VLANs* serão separadas pelo tipo de seu serviço, e nomeadas para uma melhor identificação, como pode ser visto na tabela 3.

Tabela 3 - - Faixa de endereçamento de IP proposto.

ENDEREÇO DE IP	*VLAN ID*	SERVIÇO
10.80.0.0/23	10	*VoIP*
10.80.2.0/23	20	*Wi-Fi*
10.80.4.0/23	40	Estações de Trabalho
10.80.6.0/24	60	Servidores
10.80.7.0/24	70	Gerencia
10.80.8.0/24	80	Impressoras de rede
10.80.9.0/24	90	Câmeras de Monitoramento
10.80.10.0/24	100	*Storage*
10.80.11.0/26	110	Rede da TI
10.80.11.128/27	111	Relógio Ponto
10.80.11.192/27	112	Automação Industrial

Fonte: Alex Sander S Rocha, Carlos E. Kummer e Oscar Medina Gomes (2017)

3.2.1 Equipamentos de rede

Os equipamentos como impressoras de rede, estações de trabalho e telefonia não mudarão em relação aos que já existiam e também não irão interferir no projeto, portanto será dado sequência com os mesmos nessa reestruturação.

Nesta nova rede existem algumas opções de *switches* e roteadores a serem usados e será demostrado algumas opções e será explicado o motivo da escolha dos *hardwares*.

Na empresa possui alguns modelos de *switches* assim possibilitando várias opções de escolha entre o equipamento a ser usado. Em um primeiro momento, hoje existe um *switch* da TP-Link, modelo SG-2424 onde tem algumas opções de configuração de protocolos, como IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3x, IEEE 802.1d, IEEE 802.1s, IEEE 802.1w e IEEE 802.1q. Também tem outras características, como segurança onde tem suporte ao *SSH* v2, SSL v3, TLS v1. Atualmente, ele está sendo usado somente como *hub*, não tendo nenhuma configuração ativa dentro dele. Além de tudo que foi citado acima, ele também se destaca por ter um *BackPlane* de 48Gbps, pode ter *VLAN* de voz, suporta até 512 *VLANs* simultaneamente e interface de gerenciamento *WEB*.

O *switch* HP v1910 será utilizado para este projeto, pois o mesmo possui as configurações que atendem as necessidades para realização do projeto, além dele ser mais acessível pois já contamos com o equipamento na empresa. O equipamento conta com diversos padrões suportados como: IEEE 802.1Q, IEEE 802.1w, IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3af, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z e ISO 8802-3, e também algumas certificações de segurança, de emissões e de imunidade.

3.2.2 Softwares

- Roteamento;

De acordo com pesquisas realizadas, verificou-se que será necessário a utilização de um serviço de roteamento estruturado, seguro e confiável. Desta maneira será utilizado o sistema operacional Linux com a distribuição CentOS 7, na qual será criada as *VLANs* e as rotas de toda a rede, criando as permissões de comunicação entre elas através de regras no *iptables,* assim obtendo um maior controle sobre a rede.

Foi optado por essa distribuição devido a equipe de suporte técnico ter um conhecimento maior sobre a mesma, mas pode-se realizar o roteamento e a criação de *VLANs* em uma outra distribuição Linux, desde que tenha-se conhecimento para

realizar a mesma. Também foi realizado testes com o *routerOS* da Mikrotik e o mesmo atendeu perfeitamente as configurações necessárias, porém não foi utilizado devido o sistema operacional da mesma necessitar de licença para ativação, sendo assim foi optado por utilizar o sistema operacional Linux.

- *Packet Tracer;*

Desenvolvido pela Cisco, o *packet tracer* é um programa influente e voltado para nível educacional que tem como função simular uma rede *LAN, MAN* e *WAN* de computadores com alguns equipamentos como *Hub*, *switch*, Roteadores, Pontes e Roteadores AP. A partir destas redes é possível visualizar, capturar e até mesmo avaliar o desempenho de uma rede.

Packet Tracer permite a criação de uma rede com um número limitado de dispositivos na versão estudantil, incentivando a prática, descoberta e solução de problemas. O ambiente de aprendizagem baseado em simulação ajuda os alunos a desenvolver habilidades do século XXI, como tomada de decisão, resolução de problemas e pensamento criativo e crítico.

Para adquirir o *Packet tracer* você deve ser aluno matriculado em cursos oficiais da Cisco *Networking Academy* (NetAcad) pois o mesmo necessita de *login* para obter todos os recursos oferecido pelo mesmo, e para que não for aluno da NetAcad existe a opção *guest login* em que cada acesso ao programa deve-se esperar 15 segundos, com a opção visitante o programa possui limitações de recursos.

- *Wireshark;*

Atraente pelo fato de ser uma ferramenta *open source*, ela permite a captura de pacotes e análise de tráfego de rede de computadores mesmo em tempo de execução, disponível para os sistemas operacionais Windows, Linux e MacOS, a ferramenta é altamente recomendada para administradores de redes e sistemas.

A partir de uma estação conectada à rede, o *Wireshark* realiza a captura de pacotes na mesma e organiza a visualização por protocolo, permitindo posteriormente filtragem por IP, protocolos entre outras expressões de filtragem e dependendo da plataforma ou do dispositivo que realizará a captura, a ferramenta oferece suporte a leitura dos dados por Ethernet, IEEE 802.11,PPP, ATM, USB, BLUETOOTH, etc.

3.3 DESENVOLVIMENTO

Neste capítulo será demostrado como será realizado a preparação do ambiente e dos equipamentos no local de aplicação do projeto. Também será abordado como será realizado a implantação a reestruturação de rede, as dificuldades que foram encontradas e as soluções para as mesmas e quais os melhores métodos encontrados para implementação do projeto.

3.4 PREPARAÇÃO DO AMBIENTE E EQUIPAMENTOS

A preparação do ambiente deve ser realizada com muita atenção, pois instalar um rede do início é menos trabalhoso do que reestruturar uma rede que já está pronta. Um problema existente no local da reestruturação é o cascateamento de *switches* e *hubs*, além disso eles ainda estão todos conectados sem nem uma restrição física ou lógica.

Para ajustar esse problema será realizado a troca de um *switch* comum não gerenciável por um *switch* gerenciável a qual permite vários recursos de configurações permitindo um melhor controle.

Foi optado pela switch da marca HP, modelo v1910 como explicado anteriormente, pois a switch atual não atende as necessidades para realização do projeto, devido sua limitação de configuração.

Após deixar pronta a estrutura física da rede para receber a implantação, o próximo passo é realizar as configurações dos equipamentos a serem utilizados neste projeto.

3.5 CONFIGURAÇÕES

Os equipamentos que serão configurados para este projeto, é um *switch* e um roteador. O *switch* é um HP modelo v1910-16ports conforme descrito anteriormente.

Com a segmentação dessa rede e a criação de mais de uma V*LAN*, se faz necessário a existência de um roteador para coordenar o compartilhamento de informações entre essas redes.

Portanto, para roteamento foi utilizado o sistema operacional CentOS 7, na qual foi realizado as configurações de redes e criado as regras no *iptables*.

3.5.1 Configurando e aplicando regras no *switch*

Com o *switch* fixado no rack da sala de T.I e preparado para receber as configurações, foi realizado o primeiro acesso no mesmo iniciando as configurações e no menu de administração de *VLAN* foram criadas todas as *VLAN* cada uma com seu serviço.

Após este, foi configurado cada porta de rede do *switch* para trabalhar em sua devida rede *VLAN*, também foi definido a porta de administração geral do *switch* e a porta que fara a comunicação com o roteador, a porta *trunk*.

Como pode-se observar no apêndice B, possui uma demonstração de como foi realizado a configuração do switch via linha de comando.

Uma das dificuldades encontradas nesse ponto foi que a parte de configuração via console do *switch* é toda em inglês, sendo assim quem não tem um conhecimento pelo menos básico na língua, terá um pouco de dificuldade se for configurar por linha de comando.

Por fim, após esses procedimentos conclui-se a configuração do switch e foi passado para próximo passo à organização do rack juntamente do switch e marcação dos pontos de rede através de uma máquina etiquetadora.

3.5.2 Configurando o roteador

O roteamento consiste em definir e regulamentar o encaminhamento de pacotes entre as *VLAN*, mostrando para a rede qual *VLAN* irá se comunicar com qual de acordo com o que nós definimos conforme apêndice A. Dessa maneira facilita para a rede ter um nível maior de segurança e de certa forma, com performance melhor em alguns momento, pois todo o trafego estará disponível

semente dentro de cada *VLAN*, tento um *gateway* para cada uma, deixando assim de estar dentro de uma única rede como era anteriormente nesta rede.

A listagem completa da configuração e definição da regra de negócio e política de acesso de todas as redes *VLAN* criadas no *switch,* conforme podemos ver no apêndice C. Essas regras foram definidas por nós, baseando-se pela estrutura da empresa em questão e nível de acesso dos usuários. Então, a partir do apêndice A, foi obtido o padrão para poder configurar o roteamento.

3.6 APLICAÇÃO

Durante uma semana foi realizado o pré-teste para implantação, realizados entre o dia 02 e 06 de outubro. No dia 07 de outubro, entre as 09 e 19 horas iniciou-se a implantação e realização final de testes em uma das unidades da empresa, em Medianeira/PR.

Após identificar todos os cabos e equipamentos, substituição do antigo para o novo *switch*, configuração do novo *switch* e também instalação e configuração do roteador de acordo com os capítulos anteriores, foi verificado e feito a validação do funcionamento da restruturação na rede.

Os testes de validação foram feitos através de testes de conectividades, demonstrado no capítulo a seguir.

4 RESULTADOS E DISCUSSÕES

Neste capítulo serão abordados os testes que foram realizados durante a aplicação e será discutido sobre os resultados, comparando os resultados obtidos com os que eram esperados. Também será analisado se as opiniões dos autores que foi levado em conta, se elas são ou não de acordo com nossos resultados.

4.1 TESTES

Antes de se iniciar a discussão dos resultados dos testes feitos, será esclarecido que na antiga configuração de rede, se fosse conectado uma máquina a partir de qualquer ponto de rede dentro da empresa, você teria acesso a todos os outros serviços que se encontravam disponíveis na rede, sendo assim não existia nenhuma segurança em relação a isso.

A partir da reestruturação feita, iniciou-se o teste de conectividade e comunicação entre as redes *VLAN*, que basicamente, consiste em testar via protocolo *ICMP* a comunicação entre dois ou mais hosts locais.

Para este efeito, foi elaborado os seguintes testes de conectividade que se encontram abaixo, todos baseados na regra de negócio apontada no apêndice A. Para comprovar o funcionamento do isolamento de trafego, foram feitos alguns testes de modo em que o acesso é permissivo e também foi exposto alguns testes de negação entre as redes.

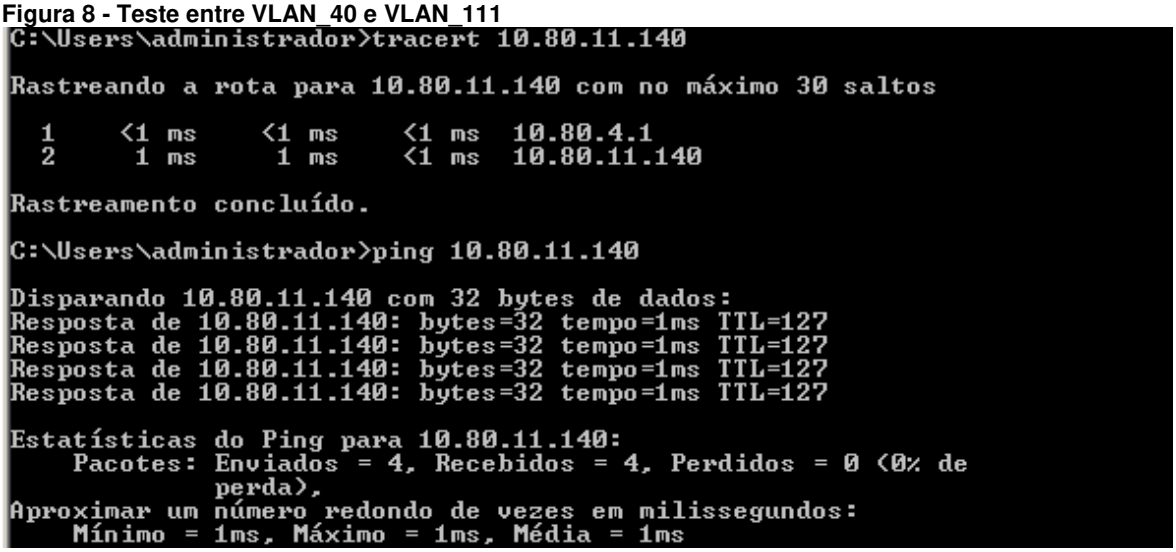
Conforme figura 7, foi realizado o teste de uma estação de usuário localizada na *VLAN* de estações de ID 40 para impressora localizada na *VLAN* de *ID* 80, neste cenário, permissiva entre elas. Neste teste em particular, também pode-se ressaltar que como o único interesse de envio de dados vem da estação, pode-se impedir o envio de pacotes desta *VLAN* de impressoras de rede para a estação, deixando assim um caminho só de envio de pacotes.

Figura 7 - Teste entre VLAN_40 e VLAN_80.

Fonte: Autores (2017)

Neste ponto, na figura 8 foi verificado uma estação local localizada na *VLAN* de estações ID 40 para a *VLAN* de relógio ponto na ID 111. Essas comunicações também são permissivas. Neste caso, terá que deixar habilitado a comunicação de pacotes de ambos os lados, pois a estação envia uma requisição de informações para o relógio ponte, onde ele irá retorna-las para a mesma.

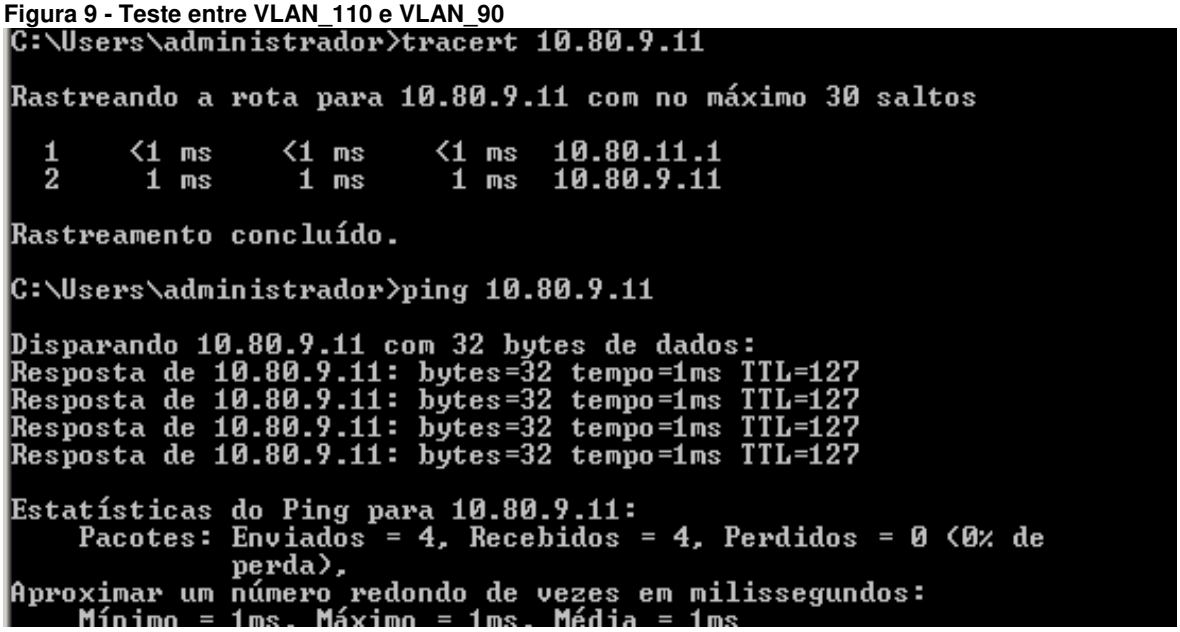
Figura 8 - Teste entre VLAN_40 e VLAN_111



Fonte: Autores (2017)

Na figura 9, foi realizado o teste de uma estação localizada na rede de T.I da V*LAN* 110 para rede de câmeras na *VLAN* de ID 90. Outra comunicação permissiva.

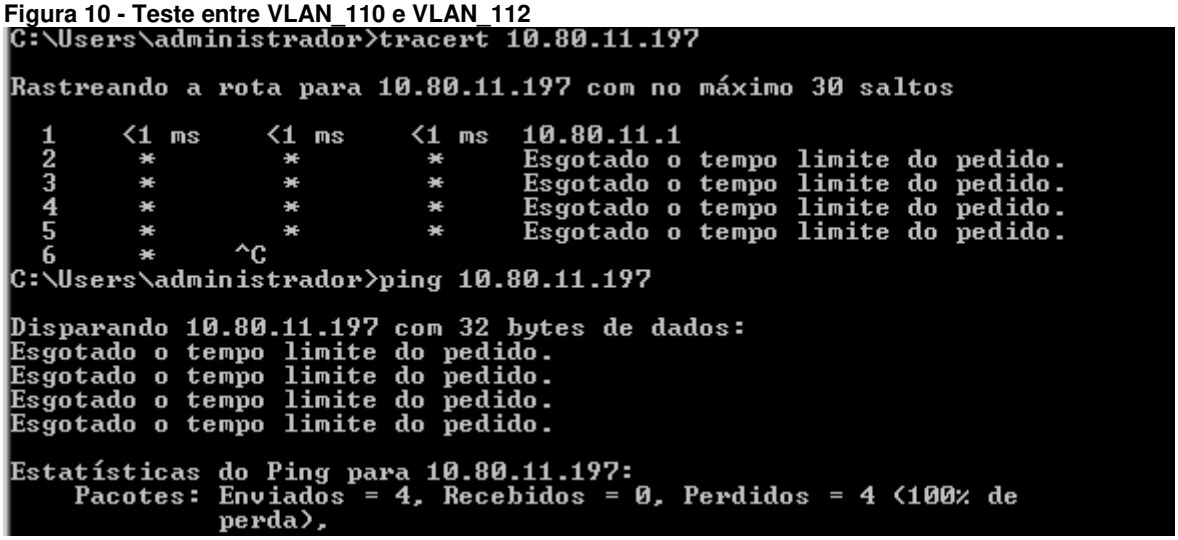
Figura 9 - Teste entre VLAN_110 e VLAN_90



Fonte: Autores (2017)

Na figura 10, realizado teste da estação de T.I na *VLAN* de ID 110 para um equipamento da rede de automação na *VLAN* de *id* 112. Este teste será um exemplo de comunicação negada.

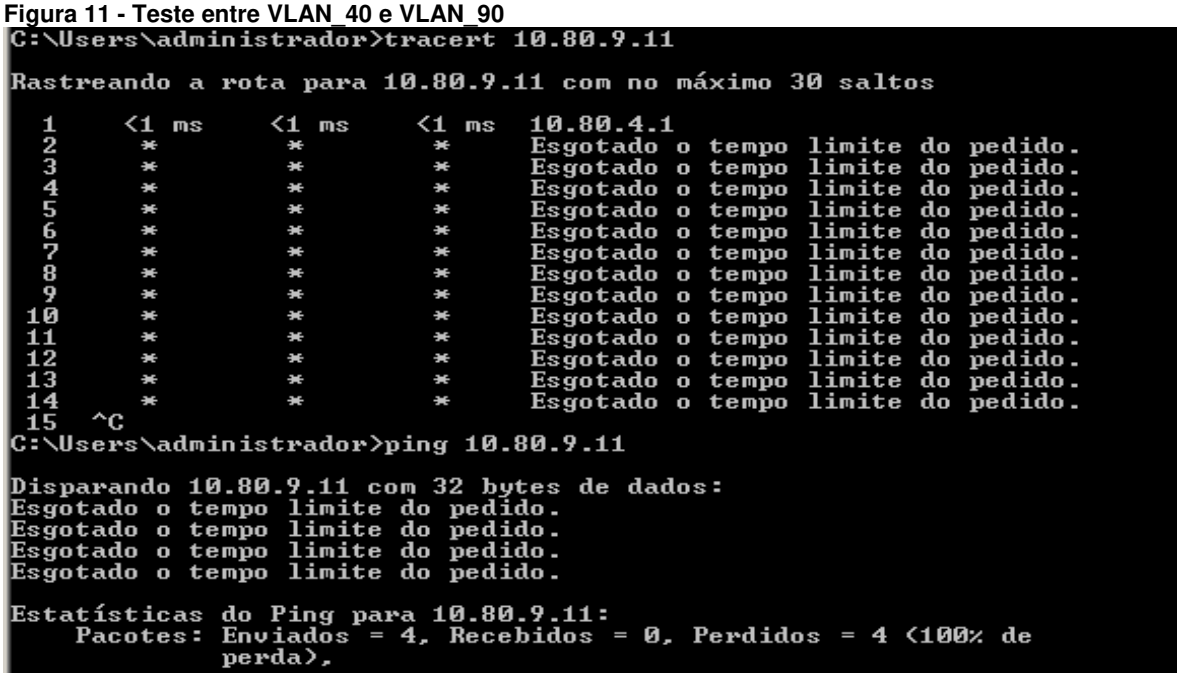
Figura 10 - Teste entre VLAN_110 e VLAN_112



Fonte: Autores (2017)

Abaixo, na figura 11 foi realizado o teste na estação de usuário na *VLAN* de *ID* 40 para *VLAN ID* 90 de câmeras. Esse exemplo também será de negação.

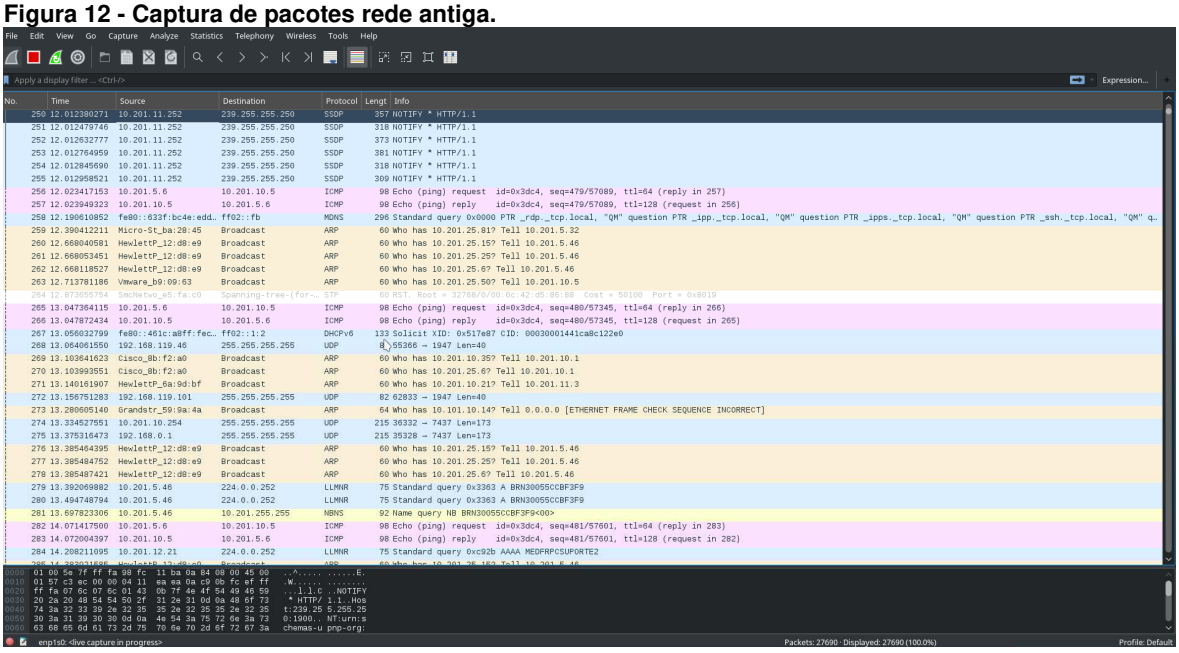
Figura 11 - Teste entre VLAN_40 e VLAN_90



Fonte: Autores (2017)

Além dos testes de conectividade já feitos, para comprovar nossa tese de que o isolamento de trafego será nítido, também será mostrado como os pacotes de rede comportaram-se depois da reestruturação em relação a como eram antes de se aplicar o projeto, com o programa *Wireshark*, como demonstrado na figura 12.

Figura 12 - Captura de pacotes rede antiga.



Fonte: Autores (2017)

Sobre os testes realizados a partir da conectividade, pode-se ver que os serviços ficaram separados, cada um na sua rede, respeitando as regras que fixamos no roteador.

5 CONSIDERAÇÕES FINAIS

5.1 CONCLUSÃO

O objetivo deste projeto foi elaborar e aplicar um projeto de reestruturação de rede na empresa Friella, levando em conta a estrutura já presente e os recursos disponíveis, como *hardware*, mão de obra e disposição de tempo da equipe de suporte.

Pode-se concluir que, de acordo com a análise dos resultados do projeto adquire-se ganhos na segurança, desempenho e gerenciamento de rede, onde a equipe de suporte pôde notar ter um melhor controle e monitoramento sobre a rede, visto que nos testes realizados ficou claro que as redes ficaram isoladas conforme sua necessidade. Além disso também traz benefícios na questão de desempenho, onde agora temos mais de um domínio de *broadcast*, evitando maiores congestionamentos de tráfego e também na parte de segurança, onde segmentamos as redes através das regras de negócio estabelecidas, o acesso é permitido ou não, levando em conta a criticidade de segurança dos aparelhos. Nos servidores, *storages* e equipamentos de gerência, podemos oferecer um nível maior de proteção a eles através do projeto.

Agora com a rede estruturada podemos realizar de maneira planejada expansões na rede conforme a necessidade de forma organizada.

O desenvolvimento do trabalho nos promoveu adquirir muito conhecimento na área, podendo assimilar e desenvolver na prática o que foi aprendido na teoria. Podemos afirmar que obtivemos muita aprendizagem e experiência ao elaborar o projeto e concilia-lo com os estudos das demais matérias vigentes na graduação, com cada integrante colaborando com êxito para o projeto visando um objetivo comum do grupo, obtermos com sucesso a reestruturação.

5.2 TRABALHOS FUTUROS

Com base no estudo realizado, algumas alterações ainda podem ser feitas. No firewall do roteador pode-se realizar algum ajuste fino na tabela do *iptables*, melhorando a política de acesso aos serviços.

Como obtivemos um resultado bem sucedido na estruturação dessa rede, podemos reproduzir o projeto nas demais unidades da empresa.

REFERÊNCIAS BIBLIOGRÁFICAS

FELIPPETTI, Marcos Aurélio, CCNA 5.0 Guia Completo de Estudo. 5 ed. Florianópolis: Visual Books Editora Ltda, 2014.

FELIPPETTI, Marcos Aurélio, CCNA 6.0 Guia Completo de Estudo. 6 ed. Florianópolis: Visual Books Editora Ltda, 2017.

TANENBAUM, Andrew S. Rdes de computadores. 5 ed. São Paulo: Pearson Education do Brasil, 2011.

CARMONA, Tadeu e HEXSEL, Roberto, Universidade de Redes: Torne-e um especialista em redes de computadores. São Paulo: Digerati Books, 2005.

PASSMORE, David e FREEMAN, John. The Virtual LAN Technology Report. U.S.A: Decisys, 1996

HELD, Gilbert, Ethernet Networks: Design, Implementation, Operation, Management. 4 ed. John Wiley & Sons LTDA, 2003.

Normas Técnicas, O que é IEEE? Disponivel em: <http://www.normastecnicas.com/ieee/o-que-e-ieee/ > Acessado em 28 de junho de 2017.

IEEE, O que é o IEEE? IEEE The Institute of Electrical and Electronics Engineers, Inc. - Latin America - Brazil Council, Disponivel em : <http://www.ieee.org.br/organizacao/> Acessado em 28 de junho de 2017.

IEEE, History of IEEE, Institute of Electrical and Electronics Engineers, Inc. Disponivel em : <https://www.ieee.org/about/ieee_history.html> Acessado em 28 de junho de 2017.

STALLINGS, William. Criptografia e segurança de redes: princípios e praticas / William Stallings; tradução Daniel Vieira; revisão técnica Paulo Sérgio Licciardi Messeder Barreto, Rafael Misoczki. 6 ed. São Paulo: Pearson Education do Brasil, 2015.

APÊNDICE A – COMUNICAÇÃO ENTRE *VLANS*

SERVIÇO	*VLAN_ID*	COMUNICA COM
VoIP	10	*VLAN*_1, *VLAN*_110.
Wi-Fi	20	*VLAN*_1, *VLAN*_110.
Estações	40	*VLAN*_1, *VLAN*_60, *VLAN*_80, *VLAN*_ 110, *VLAN*_111.
Servidores	60	*VLAN*_1, *VLAN*_40, *VLAN*_80, *VLAN*_100, *VLAN*_110, *VLAN*_111.
Gerencia	70	*VLAN*_1, *VLAN*_110.
Impressoras	80	*VLAN*_1, *VLAN*_40, *VLAN*_60, *VLAN*_110.
Câmeras	90	*VLAN*_1, *VLAN*_110.
Storage	100	*VLAN*_1, *VLAN*_60, *VLAN*_110.
TI	110	*VLAN*_1, *VLAN*_10, *VLAN*_20, *VLAN*_40, *VLAN*_60, *VLAN*_70, *VLAN*_80, *VLAN*_90, *VLAN*_100, *VLAN*_110, *VLAN*_111.
Relógio	111	*VLAN*_1, *VLAN*_40, *VLAN*_60, *VLAN*_110.
Automação	112	*VLAN*_1.

APÊNDICE B – ARQUIVO DE CONFIGURAÇÃO DO *SWITCH*

```
#
 version 5.20, Release 1513P99
#
 sysname HP
#
 domain default enable system
#
 ip ttl-expires enable
#
 password-recovery enable
#
vlan 1
 description TRUNK
#
vlan 10
 description VOIP
#
vlan 20
 description WIFI
#
vlan 40
 description ESTACAO
#
vlan 60
 description SERVIDOR
#
vlan 70
 description GERENCIA
#
vlan 80
 description IMPRESSORA
#
vlan 90
 description CAMERA
#
vlan 100
 description STORAGE
#
vlan 110
 description TI
#
vlan 111
 description RELOGIO
#
vlan 112
 description AUTOMACAO
#
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
user-group system
#
local-user admin
 authorization-attribute level 3
```

```
 service-type ssh telnet terminal
 service-type web
#
 stp mode rstp
 stp enable
#
interface NULL0
#
interface Vlan-interface70
 ip address 10.80.7.6 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 70
 stp edged-port enable
#
interface GigabitEthernet1/0/2
 port access vlan 70
 stp edged-port enable
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 10 20 40 60 70 80 90 100 110 to 112
 stp edged-port enable
#
interface GigabitEthernet1/0/4
 port access vlan 110
 stp edged-port enable
#
interface GigabitEthernet1/0/5
 port access vlan 111
 stp edged-port enable
#
interface GigabitEthernet1/0/6
 port access vlan 112
 stp edged-port enable
#
interface GigabitEthernet1/0/7
 port access vlan 80
 stp edged-port enable
#
interface GigabitEthernet1/0/8
 port access vlan 80
 stp edged-port enable
#
interface GigabitEthernet1/0/9
 port access vlan 60
 stp edged-port enable
#
interface GigabitEthernet1/0/10
 port access vlan 60
 stp edged-port enable
#
interface GigabitEthernet1/0/11
 port access vlan 40
 stp edged-port enable
#
interface GigabitEthernet1/0/12
 port access vlan 40
 stp edged-port enable
#
interface GigabitEthernet1/0/13
```

```
 port access vlan 40
 stp edged-port enable
#
interface GigabitEthernet1/0/14
 port access vlan 40
 stp edged-port enable
#
interface GigabitEthernet1/0/15
 port access vlan 20
 stp edged-port enable
#
interface GigabitEthernet1/0/16
 port access vlan 10
 stp edged-port enable
#
interface GigabitEthernet1/0/17
 port access vlan 70
 stp edged-port enable
#
interface GigabitEthernet1/0/18
 port access vlan 100
 stp edged-port enable
#
interface GigabitEthernet1/0/19
 port access vlan 90
 stp edged-port enable
#
interface GigabitEthernet1/0/20
 port access vlan 90
 stp edged-port enable
#
user-interface aux 0
 authentication-mode scheme
user-interface vty 0 15
 authentication-mode scheme
#
Return
```

APÊNDICE C – SCRIPT DE CONFIGURAÇÃO DO ROTEADOR

```
#!/bin/bash
echo "Criando vlans Rede ABJ..."

ip link add link enp0s3 name enp0s3.20 type vlan id 20
ip link set dev enp0s3.20 up
echo "Vlan ID: 20 criada com sucesso!!!"

ip link add link enp0s3 name enp0s3.40 type vlan id 40
ip link set dev enp0s3.40 up
echo "Vlan ID: 40 criada com sucesso!!!"

ip link add link enp0s3 name enp0s3.70 type vlan id 70
ip link set dev enp0s3.70 up
echo "Vlan ID: 70 criada com sucesso!!!"

ip link add link enp0s3 name enp0s3.80 type vlan id 80
ip link set dev enp0s3.80 up
echo "Vlan ID: 80 criada com sucesso!!!"

ip link add link enp0s3 name enp0s3.90 type vlan id 90
ip link set dev enp0s3.90 up
echo "Vlan ID: 90 criada com sucesso!!!"

ip link add link enp0s3 name enp0s3.110 type vlan id 110
ip link set dev enp0s3.110 up
echo "Vlan ID: 110 criada com sucesso!!!"

ip link add link enp0s3 name enp0s3.111 type vlan id 111
ip link set dev enp0s3.111 up
echo "Vlan ID: 111 criada com sucesso!!!"

ip link add link enp0s3 name enp0s3.112 type vlan id 112
ip link set dev enp0s3.112 up
echo "Vlan ID: 112 criada com sucesso!!!"

echo "==================================>"
echo "--> Vlans criadas com sucesso!!!"
echo 1 > /proc/sys/net/ipv4/ip_forward

DEVICE=enp0s3.20
BOOTPROTO=none
ONBOOT=yes
IPADDR=10.80.2.1
PREFIX=23
NETWORK=10.80.2.0
VLAN=yes

DEVICE=enp0s3.20
BOOTPROTO=none
ONBOOT=yes
IPADDR=10.80.2.1
PREFIX=23
NETWORK=10.80.2.0
VLAN=yes

DEVICE=enp0s3.70
BOOTPROTO=none
```

```
ONBOOT=yes
IPADDR=10.80.7.1
PREFIX=24
NETWORK=10.80.7.0
VLAN=yes

DEVICE=enp0s3.80
BOOTPROTO=none
ONBOOT=yes
IPADDR=10.80.8.1
PREFIX=24
NETWORK=10.80.8.0
VLAN=yes

DEVICE=enp0s3.90
BOOTPROTO=none
ONBOOT=yes
IPADDR=10.80.9.1
PREFIX=24
NETWORK=10.80.9.0
VLAN=yes

DEVICE=enp0s3.110
BOOTPROTO=none
ONBOOT=yes
IPADDR=10.80.11.1
PREFIX=26
NETWORK=10.80.11.0
VLAN=yes

DEVICE=enp0s3.111
BOOTPROTO=none
ONBOOT=yes
IPADDR=10.80.11.129
PREFIX=27
NETWORK=10.80.11.128
VLAN=yes

DEVICE=enp0s3.112
BOOTPROTO=none
ONBOOT=yes
IPADDR=10.80.11.193
PREFIX=27
NETWORK=10.80.11.192
VLAN=yes


echo "Liberação de comunicação da Vlan 20"
iptables -A FORWARD -i enp0s3.20 -o enp0s3.40 -j DROP
iptables -A FORWARD -i enp0s3.20 -o enp0s3.70 -j DROP
iptables -A FORWARD -i enp0s3.20 -o enp0s3.80 -j DROP
iptables -A FORWARD -i enp0s3.20 -o enp0s3.90 -j DROP
iptables -A FORWARD -i enp0s3.20 -o enp0s3.111 -j DROP
iptables -A FORWARD -i enp0s3.20 -o enp0s3.112 -j DROP

echo "Liberação de comunicação da Vlan 40"
iptables -A FORWARD -i enp0s3.40 -o enp0s3.20 -j DROP
iptables -A FORWARD -i enp0s3.40 -o enp0s3.70 -j DROP
iptables -A FORWARD -i enp0s3.40 -o enp0s3.90 -j DROP
iptables -A FORWARD -i enp0s3.40 -o enp0s3.112 -j DROP
```

```
echo "Liberação de comunicação da Vlan 70"
iptables -A FORWARD -i enp0s3.70 -o enp0s3.20 -j DROP
iptables -A FORWARD -i enp0s3.70 -o enp0s3.40 -j DROP
iptables -A FORWARD -i enp0s3.70 -o enp0s3.80 -j DROP
iptables -A FORWARD -i enp0s3.70 -o enp0s3.90 -j DROP
iptables -A FORWARD -i enp0s3.70 -o enp0s3.111 -j DROP
iptables -A FORWARD -i enp0s3.70 -o enp0s3.112 -j DROP

echo "Liberação de comunicação da Vlan 80"
iptables -A FORWARD -i enp0s3.80 -o enp0s3.20 -j DROP
iptables -A FORWARD -i enp0s3.80 -o enp0s3.70 -j DROP
iptables -A FORWARD -i enp0s3.80 -o enp0s3.90 -j DROP
iptables -A FORWARD -i enp0s3.80 -o enp0s3.111 -j DROP
iptables -A FORWARD -i enp0s3.80 -o enp0s3.112 -j DROP

echo "Liberação de comunicação da Vlan 90"
iptables -A FORWARD -i enp0s3.90 -o enp0s3.20 -j DROP
iptables -A FORWARD -i enp0s3.90 -o enp0s3.40 -j DROP
iptables -A FORWARD -i enp0s3.90 -o enp0s3.70 -j DROP
iptables -A FORWARD -i enp0s3.90 -o enp0s3.80 -j DROP
iptables -A FORWARD -i enp0s3.90 -o enp0s3.111 -j DROP
iptables -A FORWARD -i enp0s3.90 -o enp0s3.112 -j DROP

echo "Liberação de comunicação da Vlan 110"
iptables -A FORWARD -i enp0s3.110 -o enp0s3.112 -j DROP

echo "Liberação de comunicação da Vlan 111"
iptables -A FORWARD -i enp0s3.70 -o enp0s3.20 -j DROP
iptables -A FORWARD -i enp0s3.70 -o enp0s3.70 -j DROP
iptables -A FORWARD -i enp0s3.70 -o enp0s3.80 -j DROP
iptables -A FORWARD -i enp0s3.70 -o enp0s3.90 -j DROP
iptables -A FORWARD -i enp0s3.70 -o enp0s3.112 -j DROP

echo "Liberação de comunicação da Vlan 112"
iptables -A FORWARD -i enp0s3.112 -o enp0s3.20 -j DROP
iptables -A FORWARD -i enp0s3.112 -o enp0s3.40 -j DROP
iptables -A FORWARD -i enp0s3.112 -o enp0s3.70 -j DROP
iptables -A FORWARD -i enp0s3.112 -o enp0s3.80 -j DROP
iptables -A FORWARD -i enp0s3.112 -o enp0s3.90 -j DROP
iptables -A FORWARD -i enp0s3.112 -o enp0s3.110 -j DROP
iptables -A FORWARD -i enp0s3.112 -o enp0s3.111 -j DROP
```