FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

CLEBER FERNANDES VALÉRIO

REDES VIRTUAIS: conceitos e aplicações

Americana, SP

2017

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Tecnologia em Segurança da Informação

CLEBER FERNANDES VALÉRIO

REDES VIRTUAIS: conceitos e aplicações

Projeto de pesquisa apresentado a disciplina de Trabalho de Graduação II do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação da/do Prof. Me. Alberto Martins Junior.

Americana, SP.

2017

CHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

V256r VALÉRIO, Cleber Fernandes

Redes virtuais: conceitos e aplicações. / Cleber Fernandes Valério. – Americana, 2017.

55f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Alberto Martins Júnior

1. Redes virtuais I. MARTINS JÚNIOR, Alberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.519

Cleber Fernandes Valério

REDES VIRTUAIS – CONCEITOS E APLICAÇÕES

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – Fatec Americana.
Área de Concentração: Segurança da Informação

Americana, 12 de dezembro de 2017

Banca Examinadora:

Alberto Martins Júnior (Presidente)
Mestre
CEETEPS/Faculdade de Tecnologia de Americana – FATEC-AM

Maria Cristina Luz Fraga Moreira Aranha
Mestre
CEETEPS/Faculdade de Tecnologia de Americana – FATEC-AM

Francisco Carlos Mancin
Mestre
CEETEPS/Faculdade de Tecnologia de Americana – FATEC-AM

AGRADECIMENTOS

Agradeço primeiramente a Deus, pois sem ele não sou nada nem ninguém.

Á minha família, pois nunca me faltou incentivo e apoio.

A minha namorada Alana pela paciência, pelos momentos de incentivo e colaboração no período da realização deste trabalho.

Ao meu orientador Prof. Me. Alberto Martins Junior, pelo seu enorme conhecimento e pelas diversas vezes que me ensinou, também por ter me creditado confiança, respeito e por ter acreditado desde o princípio na realização deste trabalho.

Agradeço também a cada professor pelo incentivo, carinho e apoio durante todo esse período que estudei nessa renomada instituição.

À todos, meu mais profundo agradecimento e respeito.

RESUMO

Esse trabalho tem a intenção de demonstrar a importância da implementação de Vlans (Virtual Lans) nas redes de dados, em que essa tecnologia contribui para a os alicerces da segurança da informação quando se trata de confidencialidade, disponibilidade e integridade da informação em uma organização. Foi desenvolvido o estudo de forma que se entenda em que nicho ou camadas dos modelos OSI (Open System Interconnection) e TCP/IP (Transmission Control Protocol – Internet Protocol) a Vlan trabalha e como ela trabalha. Para se ter parâmetros da função e utilidades das Vlans foi realizado um experimento comparativo (com VLan e sem VLan) em que é demonstrado o quanto uma rede configurada com Vlan se torna mais segura. Também será evidenciado o quanto ela colabora para reduzir o tráfego de informações irrelevantes de forma a utilizar menos infraestrutura da rede para realizar tudo o que ela já faz, utilizando menos recursos para isso.

Palavras chaves: VLan, segurança, *switch*, camada, *broadcast* e rede.

ABSTRACT

This work intends to demonstrate the importance of the implementation of “VLans” (Virtual Lans) in data networks, in wich this tecnology contributes for information security’s bases when its comes to confidentiality, availability and integrity of information at organization. A research was developed in order to understand in wich niche or layers of the OSI (Open System Interconnection) e TCP/IP (Transmission Control Protocol – Internet Protocol) the VLan works and how it works. In order to get the functions’ parameters and utilities of Vlans was conducted a comparative experimentation (with VLan and whithout VLan) in wich will be demonstrated how the network composed with VLan becomes more safety, and also be evidenced how much it colaborates to reduce the traffic of irrelevant’s informations in order to use less network’s infrastructure to perform all it is alredy done and using less resource for this.

Keywords: VLan, security, switch, layer, broadcast and network.

SUMÁRIO

LISTA DE FIGURAS

1 INTRODUÇÃO

O tema dessa monografia é *Virtual Lan* (VLan) conforme definido por Fey e Gauer (2015), focando em explicar seus conceitos de forma que fique claro como funciona a VLan e o motivo pelo qual deve-se implementar essa tecnologia na área doméstica ou corporativa, evidenciando suas vantagens relacionadas à segurança e desempenho.

Será pontuado as vantagens de usar VLans como também as desvantagens em não se usa-las e o quanto a rede fica lenta e vulnerável pela falta de sua implementação.

O trabalho será estruturado em capítulos, fazendo uma breve introdução sobre comunicação de dados e suas ramificações, em sequência será apresentado assunto do modelo de referência OSI (*Open System Interconnection*) e TCP/IP (*transmission Control Protocol*) e o IP (*Internet* Protocol), um pouco da camada de enlace que é onde a VLan trabalha, introdução em VLans, como criar e configurar VLans e por último será realizada uma pesquisa aplicada da comunicação de dados nas VLans.

A monografia será montada de forma de que ela entre no conceito de rede de maneira que se entenda em que parte da rede e de que forma serão implementadas as VLans e como elas trabalham a favor de que a rede possa trafegar dados de uma maneira mais segura, mais inteligente, mais rápida e principalmente haja menos incidência de *broadcast* o que tornaria a rede mais lenta. Segundo Filippetti (2008), "*broadcast*" é quando um frame ou quadro uma chega a uma interface do switch e o endereço do hardware de destino desse frame é desconhecido, então o *switch* propaga esse frame para todas os dispositivos conectados em cada uma de suas portas.

A implementação de Vlans também tem como objetivo facilitar administração da rede de acordo com a necessidade da empresa, separando ou segmentando a rede por equipamentos em seus devidos setores, departamentos ou projetos, seguindo sempre critérios e politicas pré-estabelecidas pelo administrador da rede. Essa segmentação lógica de rede separando-a em grupos podendo estar ou não nas mesmas redes físicas, acaba protegendo os dados por exemplo dos colaboradores

do setor de rh ou financeiro de uma determinada empresa de usuários de colaboradores de outros setores, sendo essas informações pertinentes apenas aquele setor, e também, caso algum setor esteja trafegando muita informação e estando ele na mesma VLan o tráfego fica restrito a apenas aquela VLan deixando o restante da rede com um melhor desempenho.

Lembrando que nem sempre um computador ou dispositivo que está fisicamente do lado de outro quer dizer que o mesmo esteja na mesma VLan, garantindo que cada informação que trafega na rede seja pertinente apenas ao grupo ou setor interessado e responsável pela mesma, evitando que curiosos ou invasores tenham a informação confidencial sendo acessada ou divulgada para outros setores ou empresas.

Quando a rede não é segmentada seus computadores, impressoras e diversos outros dispositivos conectados disseminam uma enorme quantidade de *broadcast* causados por falhas em cabos, problemas causados pelas placas de rede e protocolos e aplicações com erros que causam lentidão excessiva na rede em questão.

Vale lembrar que o tema escolhido tem muito a ver com segurança da informação e seu tripé (confidencialidade, a integridade e a disponibilidade) com explicações sobre como se relacionam. Conceitos sobre Segurança da Informação serão apresentados posteriormente.

A escolha do tema **justifica-se** pelo fato do assunto agregar muito na questão da segurança da informação, melhorar substancialmente a segurança da rede de dados, aumentando de forma considerável seu desempenho e também facilitando o seu gerenciamento.

A área de TI segue a tendência mundial de produzir mais com cada vez menos recursos. Esse mantra mundialmente conhecido por diversos segmentos da economia também impacta esse setor forte e promissor.

As organizações seguem o mesmo caminho, sempre com o intuito de agilizar processos, aumentar lucros, diminuir custos sem que se perca qualidade no produto final.

Sobre a segmentação de rede ela foi criada para evitar proliferação de *broadcast* que causam transtornos na rede de dados. A princípio limitava-se em colocar roteadores na rede que evitavam que esses pacotes trafegassem por suas interfaces.

Essa segmentação pode ser encontrada com a mesma qualidade e um custo inferior implementando segmentações lógicas através das Vlans que se utilizam de *switches* para realização da operação, pois bons roteadores custam caro.

A Lan Virtual é uma tecnologia de grande valia para qualquer rede de dados, tanto para implementar e gerenciar o acesso a certos pontos da rede quanto pelo fato das VLans agregarem economia e flexibilidade para rede local que cresce de forma ininterrupta. Usando os recursos de Vlans também poderão crescer de forma segura e de fácil administração.

O **problema** foi constatado durante auditoria interna que qualquer funcionário que coloque um *notebook* na rede Lan (*Local Área Network*) tem acesso a equipamentos e dados confidenciais de vários setores. Em determinados momentos do dia existem diversas ocorrências de *broadcast* impactando no trabalho de usuários que precisam de largura de banda de alto desempenho.

Existem projetos em andamento que precisam de restrição e proteção para sua rede. O problema é: como minimizar vulnerabilidade dos projetos em andamento?

A partir do problema estabelecido, algumas **hipóteses** foram levantadas, a seguir:

a) Foi detectado através de software de monitoração de rede que a mesma está com grande incidência de *broadcast* fazendo com que um enorme volume de dados irrelevantes trafegue por ela sem necessidade, deixando a rede toda lenta.
b) Grande tráfego de dados oriundos rede WIFI decorrente grande uso de chamadas de voz, acessos a sites e *downloads* diversos de celulares dos colaboradores.
c) Grande quantidade de equipamentos infectados por algum tipo de vírus que fazem trafegar na rede uma enorme quantidade de dados desnecessários.
d) Ocorrendo excesso de colisões entre pacotes na área logica *(*domínio de colisão*)* tornando a rede menos eficaz. Segundo McQuery (2002) é chamado de “domínio de colisão” quando um grupo de dispositivos interligados ao mesmo meio físico, e dois desses dispositivos

> acessarem o meio físico ao mesmo tempo, resultará na colisão dos dois sinais.

Na questão da segurança será segmentada a rede de forma a cada setor ficar recluso a ele mesmo sem que outros computadores da rede os acessem. O estudo validará a importância da implantação das Vlans nas redes corporativas agregando ganho de desempenho e segurança.

O **objetivo** geral é mostrar através do *Packet Tracer* (programa educacional da Cisco que permite simular uma rede de computadores) que a segmentação agrega valores a rede de dados no quesito segurança e desempenho e a torna mais prática e administrável.

E como **objetivos específicos**:

- Mostrar funcionamento da Ferramenta no *Packet Tracer*.
- Mostrar comandos para criação e remoção de VLans.
- Mostrar a comunicação nas VLans.
- Mostrar o ganho de desempenho nas VLans.
- Mostrar o aumento de segurança nas VLans.

Levando-se em conta os métodos científicos, no trabalho em questão será considerado todo tema investigado compreendendo-o na sua totalidade, dando uma direção ao método, obtendo a descrição compreensão completa das relações e fatores de cada caso independentemente do número de casos sendo tratados conforme descrito por Fachin (2006).

Também segundo a autora conforme entendimento, é válido investigar fatos e entendê-los pelas suas semelhanças e diferenças. Serão abordados dois fatos ou séries de tipo análogo, a fim de detectar algo comum entre ambos e ao explicar fenômenos, fatos e objetos, o **método** comparativo dá a oportunidade de analisar os dados concretos e deduzir os elementos constantes, abstratos e gerais, propiciando investigar de forma indireta.

Seguindo com a mesma autora vale ressaltar as variáveis que são aspectos ou dimensões de um fenômeno, que no decorrer da pesquisa pode exibir ou assumir valores diferentes. Segundo Fachin (2006) “variável é qualquer quantidade ou característica que pode assumir diferentes valores numéricos.”

Ainda segundo a autora, essas variáveis podem ser classificadas por:

- Gênero;
- Espécie;
- Categoria.

Dentro da Variável Categoria trabalha-se com a variável **qualitativa** que se caracteriza pelos seus atributos e se associa a aspectos descritivamente e não apenas a aspectos não mensuráveis, o conjunto de valores que divide essa variável é chamada de sistemas de valores segundo o mesmo autor, ainda de acordo com a natureza ou objeto do pesquisador ou ainda, das técnicas que serão usadas, a variável deve ser categorizada.

A metodologia utilizada foi a de pesquisa aplicada, pois houve a realização de um experimento em um ambiente controlado através de um cenário de rede na ferramenta *Packet Tracer* para exemplificar o funcionamento das Lans Virtuais e o quanto ele agrega a rede. Foi criado outro cenário de rede sem as Lans Virtuais para comparar os dois casos.

As características da pesquisa aplicada segundo Marconi e Lakatos (2011), indicam seu interesse prático e que seus resultados sejam aplicados e utilizados em cenários reais, na solução de seus problemas.

Ainda segundo os mesmos autores, havendo na pesquisa controle sobre determinados fatores e tornando-se importante nas relações causa e efeito sendo descrito o que acontecerá, tem-se descrita uma pesquisa experimental.

Ainda segundo os mesmos autores, pelo fato de ser exposta uma simples descrição de um fenômeno torna esse tipo de pesquisa descritiva.

2 CONCEITOS TEORICOS

2.1 Comunicação de dados

Segundo Fontes (2008), a informação há muito tempo é um dos bens mais importantes das organizações e sua proteção tem sido uma das maiores preocupações dos executivos e proprietários das empresas, principalmente de instituições financeiras, empresas de transportes aéreos e as organizações virtuais da *Internet*, caso ocorra um desastre ou ataque cibernético essas empresas sofreriam grandes impactos financeiros ou sua imagem prejudicada, por isso é se faz necessário a existência de um processo de segurança da informação.

A comunicação de dados junto às redes está mudando o modo de viver e a maneira de se fazer negócios. Todos precisam obter as informações cada vez mais precisas e cada vez mais rápidas para que decisões em todos os âmbitos sejam tomadas. Hoje não se imagina um cenário de um relatório que tenha que vir pelo correio sendo que o mesmo poderia ser transmitido de forma instantânea. Hoje é muito importante como essas redes se comunicam, na sua velocidade, tipo de tecnologia utilizada, e qual arquitetura atende melhor um conjunto de necessidades (FOROUZAN, 2008).

A Internet segundo Kurose e Ross (2010) é uma rede de computadores que tem a função de conectar milhares de diferentes dispositivos pelo mundo, podendo ser eles de todos os tipos, celulares, *laptops*, TVs, automóveis, sistemas elétricos de segurança dentre outros. Esses dispositivos são denominados sistemas finais que são conectados a uma rede intermitente, ainda segundo autor em um trabalho que envolva redes, nada melhor do que começar falando sobre a *Internet* que conecta esporadicamente milhares de usuários pelos seus celulares, Assistente Digital Pessoal (PDAs), dispositivos de sensores, console de jogos, computadores e outros dispositivos.

Para Kurose e Ross (2010) esses sistemas finais são conectados entre si por *links* de comunicação e comutadores de pacotes, são constituídos por diferentes tipos de meios físicos como coaxial, fios de cobre, fibras óticas e ondas de rádios. Nesses enlaces são transmitidos os dados em taxas de transmissão diferentes medidas em

bit (*Binary digit*) por segundo. Toda essa informação indo e vindo da *Internet* em todo mundo, sendo ela oriunda de um dispositivo de uma das diversas redes LANs que existem, que eram apenas sistemas ou entidades de redes separadas que coexistiam no mesmo *hardware*. Isso levou a criação da intranet que é uma rede privada que disponibiliza uma solução completa para gerenciar toda informação que as corporações necessitam e que estão funcionando a base de processos, padrões e protocolos Internet segundo Tittel e Stewart (1997).

Segundo Forouzan (2008), os avanços da tecnologia estão resultando no transporte cada vez maior de dados em cada vez menos tempo, trazendo uma evolução dos serviços com isso, como teleconferências, correios de voz identificação de chamadas dentre outros. Com todos esses avanços na comunicação de dados criou-se a expectativa de troca de dados como texto, áudio, vídeo com todo mundo, fazer *download* e *upload* de forma rápida, precisa e tudo ao mesmo tempo.

A comunicação é feita com o compartilhamento de informações, sendo ele local ou remoto. A comunicação local é feita em geral frente a frente, enquanto a remota se dá à distância. “O termo telecomunicação abrange telefonia, telegrafia e televisão e comunicação a distância (tele, em grego, quer dizer “distante”) (FOROUZAN, 2008).

2.2 Fluxo de Dados

Para Forouzan (2008) existem três formas de comunicação entre dois dispositivos:

Modo Simplex: Comunicação unidirecional, apenas um dispositivo pode transmitir de cada vez, funciona como uma via de mão única. Como exemplo o monitor que só mostra a saída das informações e o teclado que só entra com as informações e não recebe.

Modo Half-Duplex: Nesse modo de transmissão os dispositivos podem receber e transmitir os dados, porém não podem fazer isso ao mesmo tempo, enquanto um dispositivo transmite o outro apenas recebe.

Modo Full-Duplex: Assim como uma via de mão dupla, os dispositivos transmitem e recebem informações ao mesmo tempo.

Segundo o mesmo autor, a comunicação de dados é a troca de dados entre dispositivos feita por um meio de transmissão como por exemplo um cabo condutor formado por fios e para que isso ocorra eles devem fazer parte de um sistema de comunicação composto de *hardware* (equipamento físico) e *software*. Sua eficácia depende de 4 itens:

1. Entrega. Os dados devem ser encaminhados para o destino correto e apenas no dispositivo e para o usuário correto.

2. Precisão: Os dados devem ser entregues de forma precisa sem que os mesmos sejam alterados e deixados sem correção.

3. Sincronização: Os dados devem ser entregues pelo sistema no momento correto, principalmente vídeos e áudios. Essa entrega é chamada de transmissão em tempo real.

4. *Jitter*: Variação do tempo na chegada dos dados, caso os atrasos da entrega dos pacotes sejam desiguais a qualidade do vídeo será irregular.

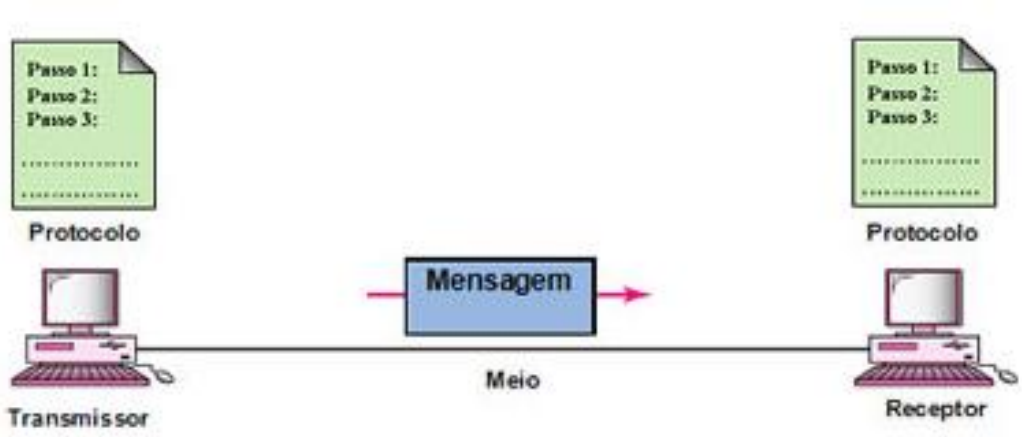
Segundo Kurose e Ross (2010) as propriedades relacionadas à segurança de redes de comunicação segura são:

- Confidencialidade: Apenas remetente e destinatário pertinentes a mensagem podem interpretar o seu conteúdo.
- Autenticação do ponto final: Tanto remetente como destinatário precisam confirmar a identidade para ocorrer a comunicação.
- Integridade da Mensagem: O conteúdo da mensagem não pode ser alterado durante a transmissão do remetente para o destinatário.
- Segurança operacional: Mecanismos operacionais devem ser implantados como *Firewalls* e sistemas de detecção de invasão para detectar atividades suspeitas.

2.3 Componentes da comunicação

Segundo Fourouzan (2008) qualquer sistema de comunicação de dados é formado por cinco componentes conforme ilustrados na Figura 1 e descritos a seguir:

Figura 1: Os 5 Componentes da comunicação.



Fonte: Brasil escola[1]

1. Mensagem. São as informações que serão transmitidas, dentre elas estão mensagens em formato de texto, áudio, vídeo, figuras, etc.

2. Emissor. É o dispositivo que envia a mensagem de dados, pode ele ser um computador, telefone, televisão, *notebook*, etc.

3. Receptor. É o dispositivo incumbido de receber a mensagem de dados, podendo ser este um computador, *notebook*, telefone etc.

4. Meio de transmissão. É o caminho físico por onde a mensagem é encaminhada do emissor parar o receptor, por exemplo: cabo coaxial, par trançado, fibra óptica e ondas de rádio.

5. Protocolo. É o conjunto de regras que controla toda essa comunicação de dados, representa um acordo ente dispositivos para que a comunicação aconteça, para que por exemplo uma pessoa que fale francês entenda uma que fale japonês.

2.4 Topologia para redes locais e metropolitanas

Para Colcher *et al*. (2005) uma *rede de comunicação* é composta por um conjunto de módulos processadores (qualquer dispositivo que se comunique pelo meio de comunicação), que tem a capacidade de compartilhar recursos e trocar informações interligados por um sistema de comunicação. Nesse arranjo topológico

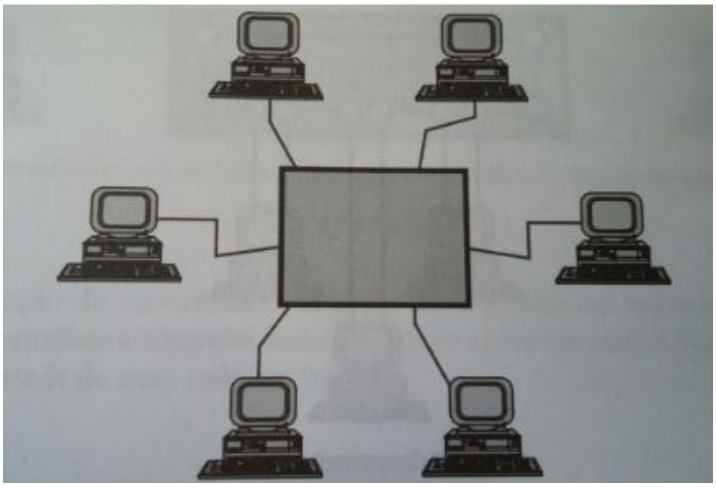
[1] Disponível em: <http://brasilescola.uol.com.br/informatica/comunicacao-dados.htm>. Acessado em: 15 set. 2017

são ligados os módulos processadores que através de conjuntos de regras (protocolos) que trafegam pelos meios de comunicação. São pontuados a seguir pelo mesmo autor as três topologias mais usadas em redes locais e metropolitanas.

- TOPOLOGIA ESTRELA

Nessa topologia cada dispositivo ou nó é interligado a um nó central (mestre) que age como centro de controle da rede por onde as mensagens devem trafegar conforme Figura 2, não havendo necessidade de roteamento pois a informação sempre passa por um nó central sendo as informações chaveadas por pacotes ou circuitos. Esse nó central estabelecerá a conexão do nó de origem da informação ao nó de destino.

Figura 2: Topologia em estrela.

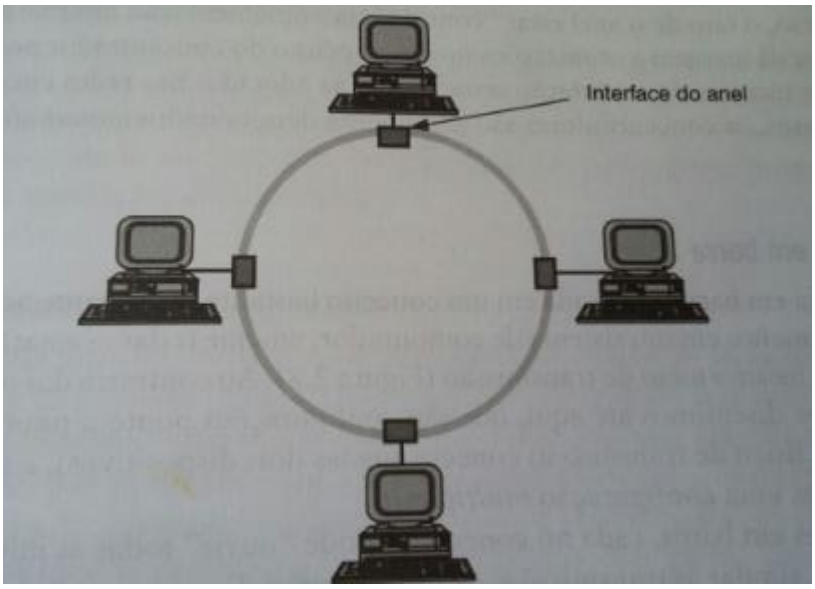


Fonte: Colcher *et al*. (2005).

- TOPOLOGIA ANEL

Para Colcher *et al*. (2005) o modelo de rede anel são definidas por estações ligadas através de um caminho fechado, esse anel não interliga os anéis diretamente porem consiste em repetidores ligados em cada estação conforme Figura 3.

Figura 3: Topologia Anel.



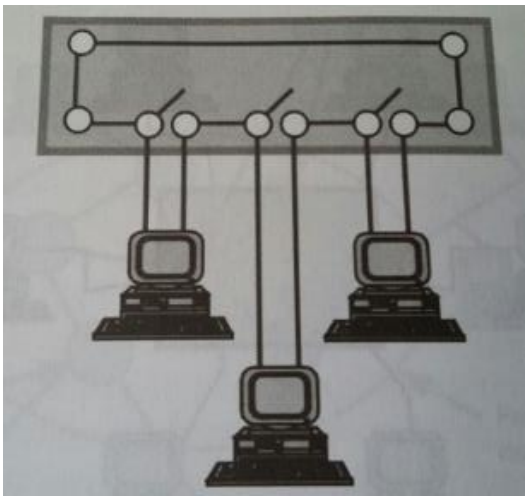
Fonte: Colcher *et al*. (2005).

Diversas melhorias nessa topologia foram sugeridas, uma delas foi a introdução de *hubs*[2] (Figura 4) de forma passiva que concentrava todo cabeamento, também tinha um mecanismo de relés que permitia o isolamento de estações em falha, e só mais tarde passaram a utilizar concentradores dos repetidores do anel (concentradores ativos). Ainda segundo mesmo autor, o uso de concentrados é vantajoso pois:

- ✓ Torna-se mais simples o isolamento de falhas pois existe um ponto de acesso central para o sinal.
- ✓ Possibilidade de adição de estações sem a parada da rede.
- ✓ Com o anel “contido” na implementação interna do concentrador abre possibilidade para otimizá-lo com técnicas de comutação idênticas as utilizadas nas redes tipo estrela. Os concentradores nesse caso são denominados *comutadores* ou *switches*.

[2] Dispositivo que interliga computadores em rede local, ele recebe dados de um computador transmite a todas as maquinas da rede e nesse momento nenhum dispositivo consegue enviar outro sinal qualquer, isso só acontece após o sinal anterior for completamente entregue. Disponível em Disponível em: < https://www.infowester.com/hubswitchrouter.php>. Acessado em: 14 nov. 2017

Figura 4: Hub/Concentrador Passivo.



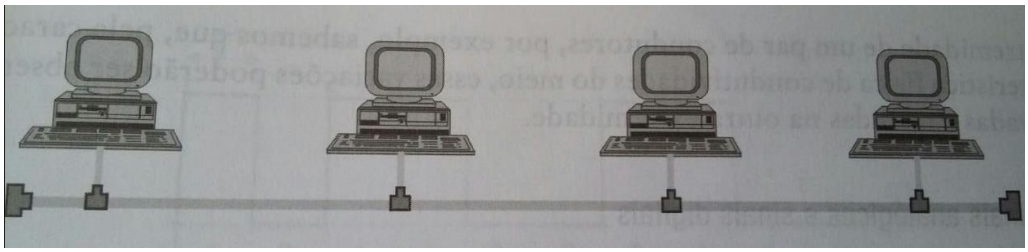
Fonte: Colcher *et al*. (2005).

- TOPOLOGIA EM BARRA

Ainda segundo mesmo autor, essa topologia assemelha-se muito ao conceito de barramento em um sistema de computador, onde todos os dispositivos trafegam informações pelo mesmo meio de transmissão (Figura 5), diferente da topologia em anel e estrela que são configurações ponto a ponto onde cada enlace físico de transmissão conecta apenas dois dispositivos, essa topologia em barra é dotada de configuração *multiponto*.

Para o mesmo autor ainda, nas redes em barra cada dispositivo conectado pode “ouvir” todas as informações que trafegam na rede.

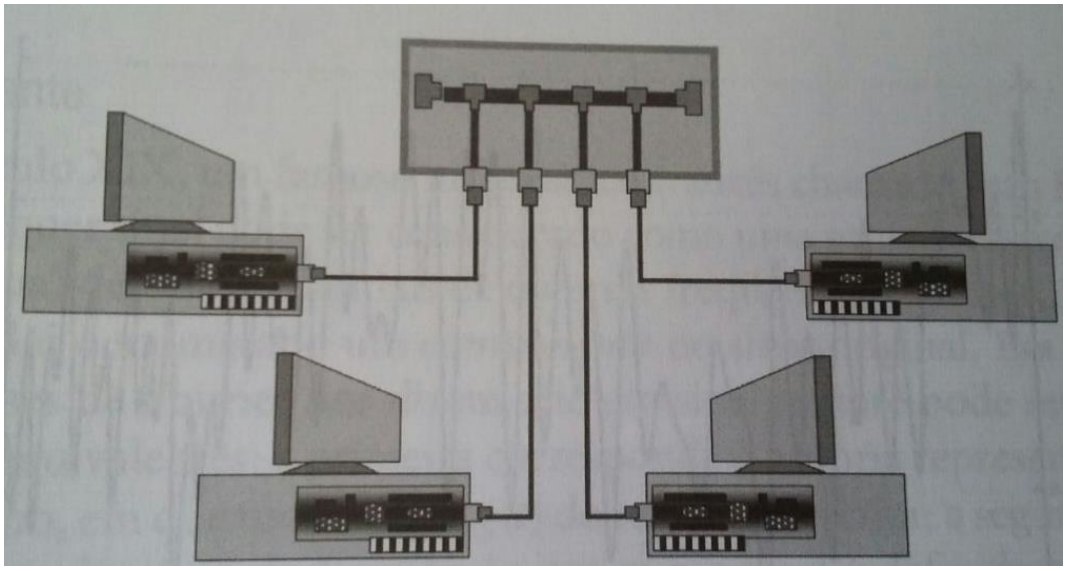
Figura 5: Topologia em barra.



Fonte: Colcher *et al*. (2005).

Ainda segundo Colcher *et al*. (2005) o uso de concentradores como *hubs* e *switches* (Figura 6) nas redes em barra trazem melhorias semelhantes as conseguidas nas redes em anel.

Figura 6: Rede em barra utilizando hub/switch.



Fonte: Colcher *et al*. (2005).

2.5 Modelos de protocolo e referência

Para Fey e Gauer (2015) quando surgiram as primeiras redes de computadores as mesmas só podiam trocar mensagens com computadores que tinham o mesmo conjunto de protocolos dos quais eram compatíveis. Quando os fabricantes de computadores eram diferentes havia problemas para interconectar esses dispositivos, para tentar corrigir isso. Criou-se então um padrão mundial para isso e nisso surgiram os modelos TPC/IP e OSI.

Para elaborar esses padrões para redes locais de computadores nasceu então o projeto IEEE 802, composto por um comitê instituído em fevereiro de 1980 pela IEEE *Computer Society* segundo Colcher *et al*. (2005). Também segundo autor o comitê 802 tem publicado um conjunto de padrões que habituam ser seguidamente revisados e republicados como padrões internacionais pela ISO.

Ainda segundo autor esse modelo de referência idealizado pela IEEE determinou uma arquitetura em que estão presentes as duas camadas inferiores do modelo OSI (física e enlace).

Segundo site da Cisco ([s.d]) para representar a operação da rede temos dois tipos básicos de modelos de rede que podem ser de protocolo ou de referência.

Conforme descrito no mesmo site o modelo de protocolo fornece um modelo de orientação muito próximo a estrutura de um conjunto de protocolos. Esse conjunto contém toda funcionalidade exigida para fazer interface da rede humana com a rede de dados, o modelo de protocolo TCP/IP é o modelo que descreve o que ocorre em cada camada dos protocolos do conjunto TCP/IP, já o modelo de referência tem como objetivo auxiliar um entendimento mais claro das funções e processos, o modelo mais usado e conhecido é o OSI que auxilia na elaboração de redes de dados e resolução de problemas.

2.6 Modelo OSI

Segundo McQuery (2002) quando se fala em modelo de referência OSI lembra-se de várias funções desempenhada por ela como por exemplo servir como diretriz para criação e implementação de padrões de rede e auxiliar na compreensão do conjunto de redes. Dentre as suas maiores vantagens estão a subdivisão da complexa operação de rede em elementos mais simples, priorizar as funções modulares nos desenvolvimentos e *design* dos engenheiros e por último definir interfaces padronizadas para os fabricantes e compatibilidades de "*plug-and-play*[3]".

Na Figura 7 do livro de McQuery (2002), são apresentadas as 7 camadas do modelo de referência OSI.

Figura 7: Modelo e referência OSI.

Fonte: McQuery (2002).

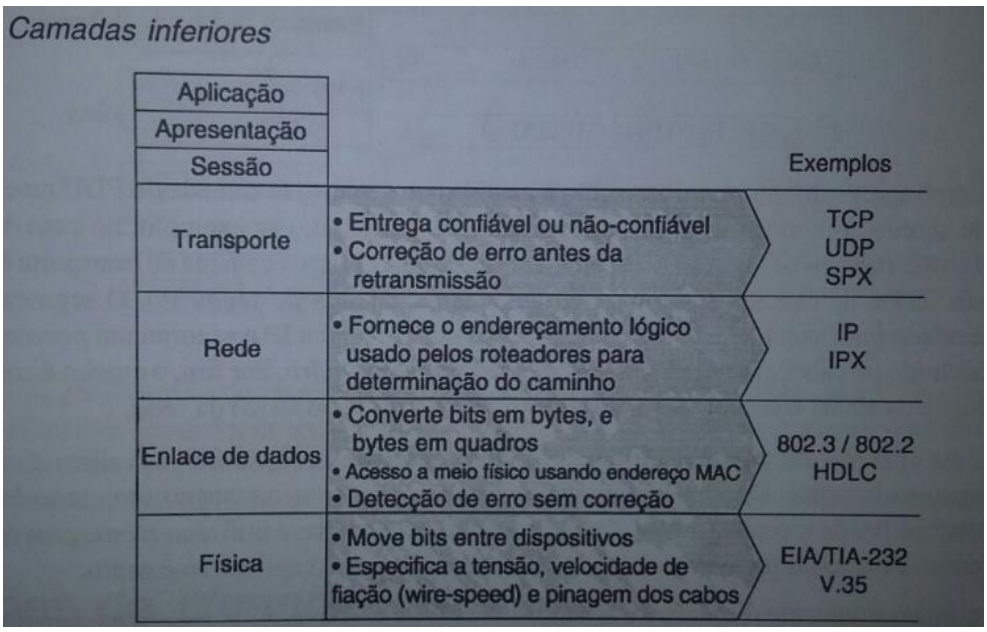
[3] Traduzindo plug-and-play tem-se "conecte e use", o objetivo principal desse padrão seria que o micro reconheça e configure qualquer periférico de forma automática. Disponível em: <https://www.portaleducacao.com.br/conteudo/artigos/administracao/sobre-o-plug-and-play/46231>. Acessado em: 21 nov. 2017.

Conforme explicado por Fey e Gauer (2015) as camadas.

- **Camada de transporte:** Responsável pelo controle de troca de dados entre dispositivos fim a fim, sendo essa troca orientada a conexão ou não.
- **Camada de rede:** Responsável pelo encaminhamento dos pacotes entre os dispositivos de rede ou intermediários, e pelo gerenciamento dos endereços dos dispositivos na rede.
- **Camada de enlace**: Responsável pela comunicação entre dispositivos vizinhos, separados apenas pelo meio físico.
- **Camada física**: Responsável pelo gerenciamento da comunicação dos bits (transmitidos e recebidos) e sua devia aderência ao meio físico.

Segundo McQuery (2002), as quatro camadas inferiores (Figura 8) correspondem as vias nas quais as estações finais estabelecem as conexões e trocam informações.

Figura 8: Camadas inferiores do modelo de referência OSI.

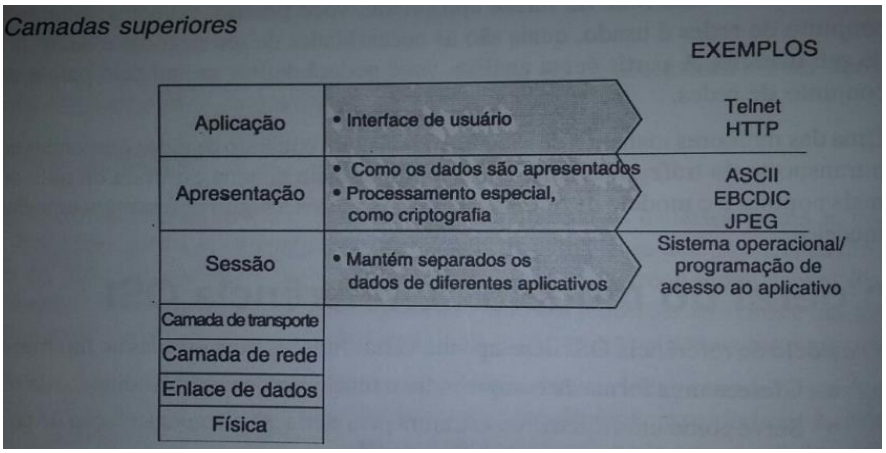


Fonte: McQuery (2002).

Conforme escrito por McQuery (2002), no caso das camadas superiores (Figura 9) elas definem como as aplicações interagem entre elas e os usuários, abaixo detalhes sobre elas:

- **Camada de aplicação:** A camada que conecta as interfaces do usuário ou aplicativo com os protocolos que acessam a rede.
- **Camada de apresentação:** Essa camada oferece diversas funções que convertem e codificam as informações afim de que elas sejam lidas pela aplicação em outro sistema.
- **Camada de sessão:** Gerencia, estabelece e termina as sessões da camada de apresentação. São solicitações e respostas de serviços entre aplicativos comunicando em diversos dispositivos.

Figura 9: Camadas superiores do modelo OSI.



Fonte: McQuery (2002).

Segundo Fey e Gauer (2015) em cada camada do modelo de referência OSI existe uma unidade básica de dados conhecida como PDU (*Protocol data unit*) conforme Figura 10, A PDU seria a matéria-prima básica para um serviço.

Figura 10:PDUs das Camadas modelo de referência OSI.

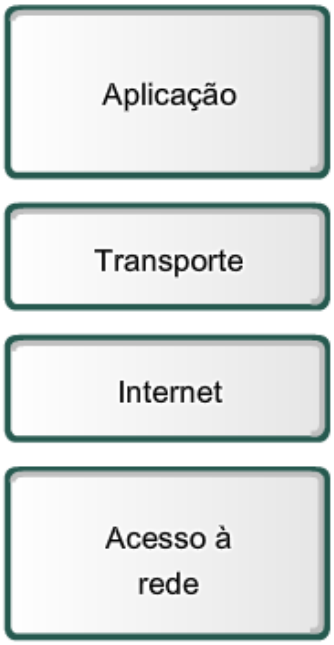
Número da camada	Nome da Camada	PDU da Camada
7	Aplicação	Dados ou Mensagem
6	Apresentação	Dados ou Mensagem
5	Sessão	Dados ou Mensagem
4	Transporte	Segmento
3	Rede	Pacote
2	Enlace	Frame
1	Física	Bit

Fonte: Fey e Gauer (2015).

2.7 Modelo TCP/IP

Segundo site da Cisco ([s.d]) esse modelo de protocolo de camadas para comunicação de rede define quatro categorias de funções que devem acontecer para que a comunicação aconteça (Figura 11). Os modelos de protocolos listam uma grande quantidade de protocolos especificas de um fornecedor, porem pelo fato do TCP/IP ser um padrão aberto, nas definições de padrões e dos protocolos TCP/IP são alinhadas em fórum público e também é fruto disso é disponibilizado um conjunto de documentos que são chamados *Requests for Comments* (RFCs), esses documentos contemplam as especificações formais de protocolos de comunicações, os recursos que descrevem seu uso, documentos técnicos sobre a internet e documentos de política criados pela Internet *Engineering Task Force* (IETF).

Figura 11: Modelo de Protocolo TCP/IP.



Fonte: (Cisco[s.d]).[4]

Fey e Gauer (2015) no modelo de protocolo TCP/IP, a camada de aplicação faz a função das camadas de sessão, apresentação e aplicação do modelo de

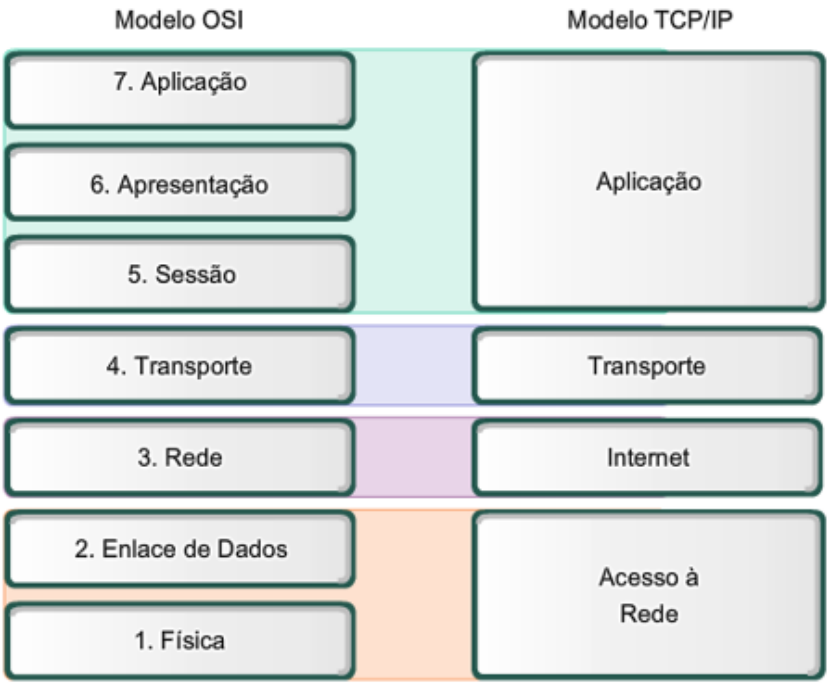
[4] Disponível em: <https://static-course- assets.s3.amazonaws.com/Exploration/E140PT/theme/cheetah.html ?cid=0600000000&l1=tl&l2=en&chapter=2 (2.4.3.1)> Acessado em: 12 set. 2017

referência OSI oferecendo condições para a transmissão de dados entre as diversas aplicações em questão conforme Figura 12.

A camada de transporte tem a mesma função da camada idêntica no modelo de referência OSI ela também é responsável pelo controle de troca de dados entre dispositivos fim a fim, sendo essa troca orientada a conexão ou não segundo o mesmo autor.

Segundo site da Cisco ([s.d]) camada de Internet define o melhor caminho para a informação trafegar pela rede. E para o mesmo autor a camada de acesso a rede tem a função de controlar o meio físico e todo *hardware* que fazem parte da rede de dados.

Figura 12: Comparando Modelo OSI com Modelo TCP/IP.



Fonte: (Cisco[s.d]).[5]

Para Fey e Gauer (2015) é válido ressaltar que não existe unanimidade no que se refere a quantidade de camadas no modelo TCP/IP, existes autores que defendem o modelo com três e quatro camadas, porém na atualidade existem o modelo de cinco

[5] Disponível em: <https://static-course- assets.s3.amazonaws.com/Exploration/E140PT/theme/cheetah.html ?cid=0600000000&l1=tl&l2=en&chapter=2 (2.4.8.1)> Acessado em: 12 set. 2017

camadas (Figura 13) que padronizam a camada de enlace e física idêntica ao modelo OSI.

Figura 13: Modelo TCP/IP versão moderna com cinco camadas.

Camada	Nome	Protocolos da Camada
5	Camada de Aplicação	DNS, FTP, SMTP, POP, HTTP, etc...
4	Camada de Transporte	UDP, TCP
3	Camada de Rede	IP
2	Camada de Enlace	PPP, Ethernet, Frame Relay, HDLC
1	Camada Física	V35, V36, G703, V24

Fonte: Fey e Gauer (2015)

Segundo site da Cisco ([s.d]) a forma que cada pedaço de dado se transforma em cada uma de suas camadas é chamada de PDU e nesse encapsulamento cada PDU tem um nome diferente para definir sua aparência, e eles são chamados conforme os protocolos do conjunto de TCP/IP.

- Dados – PDU criada na camada de Aplicação
- Segmento – PDU oriunda da camada de transponde
- Pacote – PDU correspondente a camada de rede
- Quadro – PDU referente a camada de acesso a rede
- Bits – Uma PDU usada para trafegar os dados através do meio físico.

A Cisco alega que o TCP/IP implementa protocolos no *host* (hospedeiro) de origem/destino que fazem parte do conjunto de protocolos TPC/IP a fim de fornecer, entregar aplicações fim-a-fim pela rede de dados. A Cisco listou um processo de comunicação completo:

1. Criação dos dados no dispositivo de origem na camada de aplicação.
2. Segmentação e encapsulamento desses dados passando pela pilha de protocolo no dispositivo de origem.
3. Construção desses dados no meio físico na sua camada de acesso a rede de origem.
4. Transporte desses dados pelo meio físico.
5. Recepção dos dados camada de acesso do dispositivo de destino.

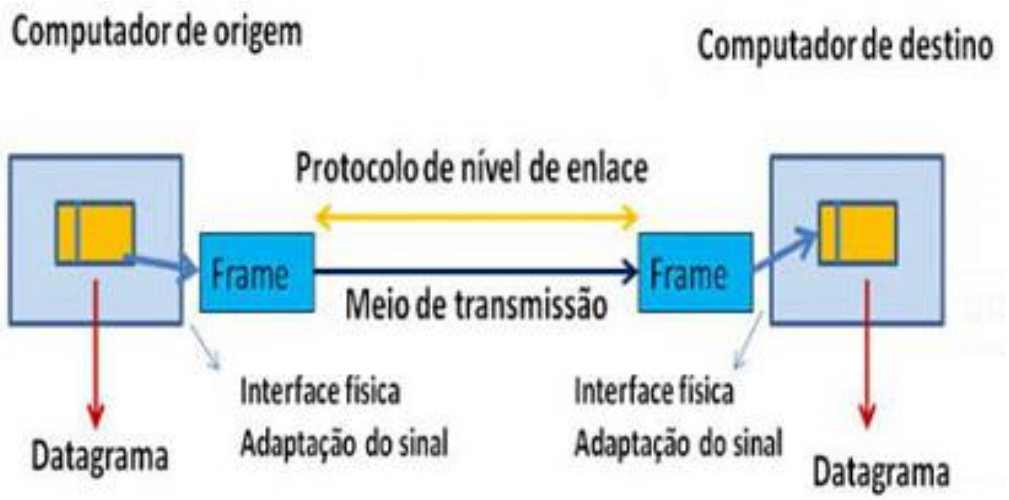
6. Desencapsulamento e reorganização dos dados conforme esses passam pela pilha do dispositivo de destino.
7. Transferência desses dados para aplicação e sua camada do dispositivo de destino.

Ainda segundo o mesmo site, conforme dados gerados da aplicação, atravessam a pilha de protocolo em seu trajeto para o meio físico da rede vai-se adicionando protocolos de informações em cada um de seus níveis, esse processo é chamado de encapsulamento.

2.8 Camada de enlace

Segundo Fey e Gauer (2015) a camada de enlace que corresponde a camada 2 do modelo OSI tem como principal função fornecer condições e estrutura ao Pacote recebido na camada 3 através de um circuito de comunicação de dados, a fim de garantir um ambiente organizado, controlado e livre de erros conforme evidenciado na figura 14.

Figura 14: Função da camada de enlace.



Fonte: Fey e Gauer (2015)

Ainda segundo o autor a informação que trafega no meio de transmissão é *bit* a *bit* até ser repassado a Camada de enlace que segue seus protocolos estabelecendo suas regras para poder interpretar as informações associada aos *bits* para que haja entendimento entre os dispositivos de comunicação.

Para o autor a função da Camada 2 seria prestar serviço para a camada 3 montando uma estrutura baseada nas regras do protocolo especifico da camada de enlace denominada “quadro” ou “*frame*” e a encapsula o pacote para que o mesmo trafegue na Camada Física. Ainda para o autor, diferentes protocolos desta camada possuem diferentes regras mesmo que todos formem um Quadro ou *Frame* onde temos o cabeçalho inserido em frente do pacote da camada 3 e o controle de erros inserido no final da mesma camada conforme descrito na Figura 15.

Figura 15: Estrutura da camada de enlace.

Fonte: Fey e Gauer (2015)

Para Fey e Gauer (2015) independente em qual modelo de protocolos for dado, camada de enlace (OSI) ou camada de acesso à rede (TCP/IP), sua função será sempre montar o *frame* ou quadro e transmiti-lo pelo meio físico para o equipamento vizinho. Ainda segundo autor, os protocolos de Camada 2 trabalham entre a camada 3 e camada 1, e de certa forma dificulta definir onde começa e onde termina a responsabilidade da camada física e de enlace, por isso que no modelo de protocolo TCP/IP de 4 camadas a camada 1 e 2 são unificadas e denominada camada de Acesso à Rede, (não confundi-la com a camada 3 desse mesmo Modelo TCP/IP chamado Internet/Rede/Inter-rede).

Segundo Fey e Gauer (2015) é importante recordar as funções da camada de enlace do modelo OSI, ou camada 2, pois a VLan é baseada no trabalho do Switch de nível 2.

2.9 Protocolos da camada de enlace

Segundo Fey e Gauer (2015) existem dois grupos de protocolos de camada 2.

1. Protocolos que operam em redes locais (LAN).

- *Ethernet*.[6]
- 802.11 Wi-Fi
- IEEE 802.1q
- 802.11g
- *Token Ring*
- FDDI

2. Protocolos de rede de Longa Distância (WAN).

- PPP
- HDLC e
- *Frame Relay*

[6] Padrão de transmissão de dados para rede local, tendo como principio que todos os equipamentos da rede estão conectadas na mesma linha de comunicação.

3 VLAN

3.1 Conceito LANS VIRTUAIS

Segundo Filippetti (2008) as redes comutadas são planas, isso significa que todos os pacotes de *broadcast* transmitidos e chegam a todos os dispositivos conectados na rede, mesmo que o dispositivo não seja o destinatário dos pacotes, sendo assim quanto maior a quantidade de dispositivos e usuários maior o volume desses *broadcasts*.

Para o mesmo autor os roteadores mantêm os *broadcasts* na mesma rede que as originou, já os *switches* os propagam para toda rede, por isso chamados a rede comutada de "*plana*", por se tratar de um grande domínio de *broadcast*.

Para controlar a propagação de *broadcast* em redes *bridge*[7] ou comutadas é importante segmentá-la em diversos domínios de colisão. Os roteadores trabalham na camada 3 do modelo OSI e contêm segmentação de domínio de *broadcast* e por isso não os propagam. A forma com que os *switches* apresentam um método de segmentação de domínio de *broadcast se* denomina LANs virtuais (VLans), a VLan pode ser considerada um domínio de *broadcast*, algumas vantagens em usar VLan de acordo com McQuery (2002):

- Segurança;
- Segmentação;
- Flexibilidade.

Segundo o mesmo autor competem às VLans agrupar usuários em um mesmo domínio de *broadcast* independentemente da sua posição no aglomerado da rede. A existência de VLans melhora o desempenho e aumenta a segurança da rede controlando a propagação de *broadcast*. Em um ambiente de *Broadcast,* os pacotes são enviados por um host em um único segmento e propagado para todos da rede saturando a largura da banda da rede toda, antes da existência dos *Switches*[8] e VLans

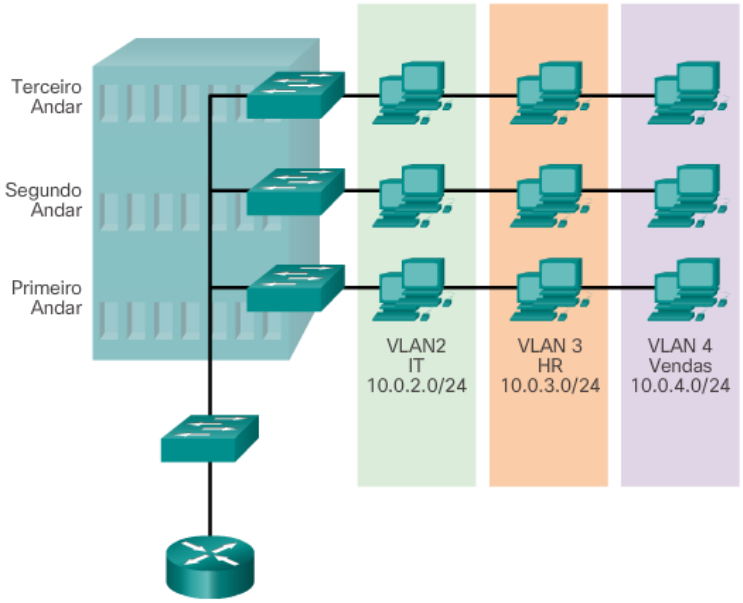
[7] Traduzindo Bridge significa Ponte, tem a função de conectar duas redes distintas para que se comuniquem.
[8] Switch (ou comutador) é um equipamento ativo que funciona normalmente na camada 2 do modelo OSI (Data Link) e tem como principal funcionalidade a interligação de equipamentos (estações de trabalho, servidores, etc) de uma rede uma vez que possui várias portas RJ45 (ou ISO 8877) fêmea. Disponível em: <https://pplware.sapo.pt/microsoft/windows/redes-como-funciona-um-switch/ > Acessado em: 15 ago. 2017

as redes eram divididas em diversos domínios de *Broadcast* de acordo com a conectividade dos roteadores.

Uma VLan é um domínio de *broadcast* lógico que pode abranger vários segmentos físicos da rede *LAN* e ela pode ser projetada com a ideia de disponibilizar domínios de *broadcast* independentes de acordo com as necessidades da empresa ou projeto sem levar em consideração a localização física dos usuários e poderá ser atribuída cada porta de um switch a apenas a uma VLan (MCQUERY, 2002).

Segundo site da Cisco ([s.d]) as VLans apresentam uma forma de agrupar dispositivos dentro de uma Lan fazendo com que esse grupo de dispositivos se comunique como se estivessem conectados no mesmo fio. Ainda segundo a Cisco os dispositivos da Vlan trabalham de forma independente mesmo compartilhando da mesma infraestrutura da rede conforme figura 16.

Figura 16: VLans diferentes usando a mesma infraestrutura.



Fonte: (Cisco[s.d])[9]

Para McQuery (2002) as VLans permitem que os *switches* criem vários domínios de *broadcast* em uma mesma rede e também oferecem recursos de segmentação e flexibilidade organizacional podendo agrupar portas de *switches*, e os usuários a ela conectados em comunidades de interesses comuns, definidas de

[9] Disponível em: <https://static-course-assets.s3.amazonaws.com/RSE503/pt/index.html#3.1.1.1>. Acessado em 17/11.

maneira lógica como departamentos, ou grupos de usuários distintos que utilizam os mesmos aplicativos de rede, pode haver uma VLan em um ou vários *switches*, elas podem estar em um prédio ou sua infraestrutura estar em vários prédios distantes, podendo conectar-se por meio de redes remotas.

As características da configuração típica de VLan são segundo McQuery, (2002).:

- VLan lógica é como se fosse uma *bridge* física separada;
- As VLans podem estender-se por vários *switches*;
- São transmitidos pelos troncos o trafego de diversas VLans.

Ainda segundo McQuery, (2002), as VLans são uma incorporação de Camada 2 na estrutura da rede, sendo assim estão atuantes da camada de enlace de dados e não dependem de protocolo. Para conectar uma porta a uma VLan deve-se fazer esse procedimento no switch e após definir isso a comunicação *broadcast* e unicast só serão encaminhados pelos switches para as portas da mesma VLan. E para que haja necessidade de comunicação entre VLans será necessário adicionar um roteador para atuar na camada três da rede. Ainda segundo mesmo autor tendo como parâmetro o switch da Cisco Catalyst 1900, segundo o mesmo autor os modos de associação de VLans são:

Estático – Atribuição da VLan é realizada na porta sendo configurada de forma estática por um administrador da rede segundo McQuery, (2002).

Fazendo um adendo segundo Fey e Gauer (2015):

- VLan estática
    - Forma mais usual de criar VLan
    - O administrador designa as portas a serem configuradas
    - São VLans configuradas porta a porta, designando cada porta a uma determinada VLan.
    - Na VLan estática é configurado manualmente o mapeamento de cada porta e VLan pelo administrador.

Dinâmico – O switch da Cisco modelo catalyst 1900 utiliza-se de um servidor VMPS (VLan Membership Policy Server). O VMPS pode ser um servidor externo ou um o switch do Cisco modelo catalyst 5000 que contém um banco de dados que mapeia o endereço MAC para atribuição de VLan, quando um quadro chega na porta

dinâmica do switch do Cisco catalyst 1900 o mesmo verifica sua atribuição da VLan na VMPS baseando-se no endereço de origem do quadro segundo McQuery, (2002).

Para Fey e Gauer (2015):

- VLan dinâmica
    - As portas são designadas automaticamente sendo necessário a criação manual de uma tabela de consulta MAC.
    - Usa-se aplicação de Gerenciamento Inteligente (VMPS da Cisco por exemplo).
    - Portas de uma VLan ajustam-se a suas configurações de VLan.
    - Nem sempre é fato que as VLans dinâmicas são mais fáceis de configurar.
    - Usa-se um banco de dados de endereços MAC para realizar o mapeamento de VLan no qual é criado manualmente.

Segundo McQuery (2002) uma porta dinâmica pode pertencer a apenas uma VLan por vez. E para que na mesma porta haja vários hosts ativos os mesmos devem pertencer a mesma VLan.

3.2 Tipos de lans virtuais

Segundo site da Cisco ([s.d]) os vários tipos de VLans são usados nas redes atuais, outras são definidos por classes de tráfego e outros tipos de VLans são definidos pela função no qual atendem.

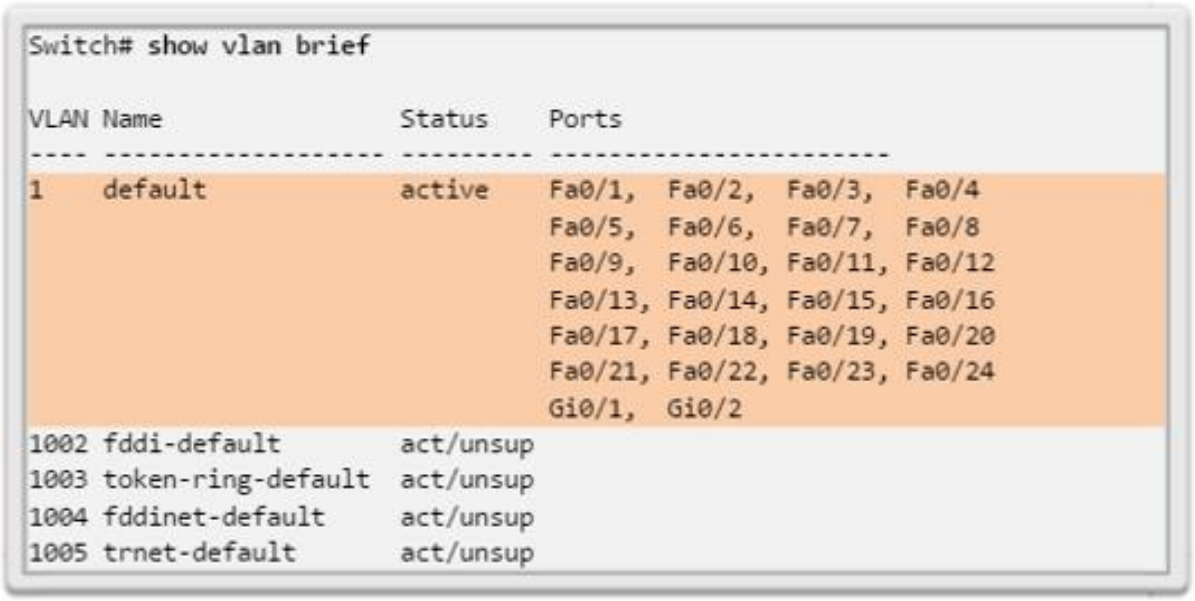
Data VLan

Para o mesmo autor uma VLan de dados é geralmente uma VLan definida para transportar dados oriundos do usuário. Se faz necessário separar esses diferentes tipos de VLans. Às vezes, uma VLan de dados é definida como uma VLan de usuário. As VLans de dados são configuradas para dividir a rede em grupos de usuários ou dispositivos conectados.

VLan padrão

Por padrão todas as portas de switch são adicionadas a VLan padrão após a primeira inicialização de um switch com sua configuração padrão. Sendo assim todas as portas de switch que são adicionadas a VLan padrão pertencem ao mesmo domínio de *broadcast* fazendo com que qualquer dispositivo conectado nessa mesma VLan se comunique com outros dispositivos em outras portas de switch. A VLan padrão para os switches Cisco também por padrão é VLan 1. Na figura 17, o comando show vlan brief foi executado em um switch com uma configuração padrão. Neste exemplo todas as portas são atribuídas à VLan 1 por padrão. Um detalhe importante da VLan padrão é que ela não pode ser renomeada ou deletada, todo trafego de controle de camada dois é associada a ela e a mesma tem todos os recursos de qualquer VLan segundo site da Cisco ([s.d]).

Figura 17: Resultado do comando show vlan brief.



Fonte: (Cisco[s.d])[10]

VLan nativa

Segundo site da Cisco ([s.d]) a VLan nativa está associada a porta de tronco 802.1Q que são links entre *switches* que suportam trafego de mais de uma VLan. Uma porta desse tipo de tronco suporta “trafego marcado” que se referem a uma marca

[10] https://static-course-assets.s3.amazonaws.com/RSE503/pt/index.html#3.1.1.3

"*tag*" de 4 *bytes*(oito bits) inserida no cabeçalho do quadro ou *frame* e que especifica qual VLan o quadro pertence. A porta tronco 802.1Q direciona o trafego não marcado pra VLan nativa que por padrão seria a VLan um que serviria como identificador comum entre as extremidades de um link de tronco.

Ainda segundo mesmo autor é de boa pratica e altamente recomendável configurar a VLan nativa como não utilizada deixando-a dedicada a atender a função de VLan nativa para todas as portas de tronco trabalhando no domínio comutado.

VLan de Gerência.

Para o site da Cisco ([s.d]) como próprio nome da VLan de gerência diz, essa VLan é qualquer VLan configurada para acessar os recursos de gerenciamento de um *switch*. Por padrão a VLan de gerência é a VLan 1, vinda de fábrica o que seria incorreto deixa-la assim e para criar essa VLan de gerencia sua interface virtual do *switch* (SVI) recebe um endereço IP[11] e uma máscara de sub-rede[12] para que ele seja gerenciado via HTTP, Telnet, SSH ou SNMP.

Ainda segundo mesmo autor, é possível haver nas redes mais de uma VLan de gerenciamento porém isso seria considerado um risco desnecessário a segurança da rede.

VLan de voz

Ainda segundo site da Cisco ([s.d]) uma VLan a parte se faz necessária para comportar a Voz sobre IP (*VoIP*) nessa VLan tem os seguintes itens de requisitos:

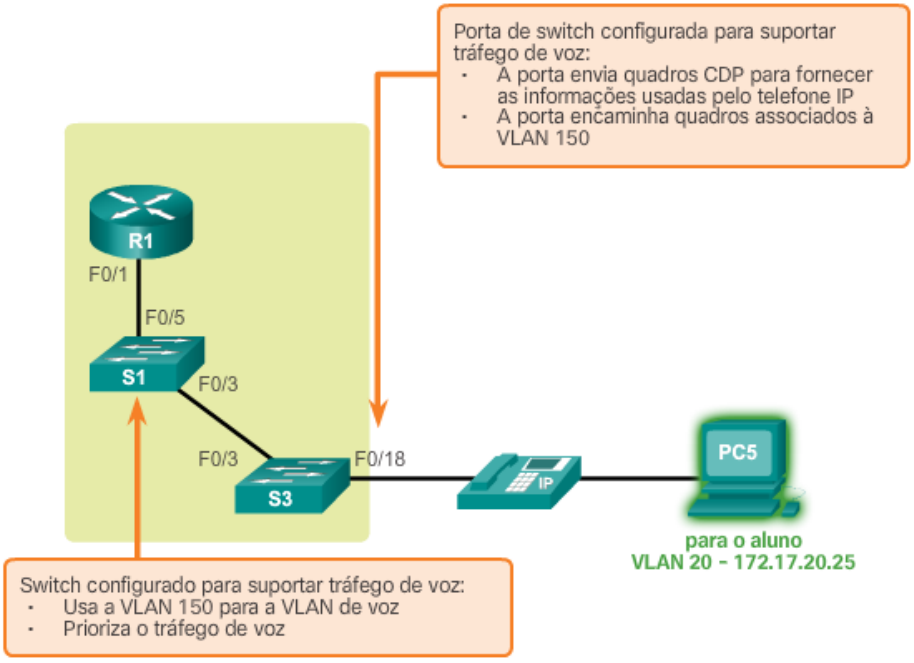
- Altar largura de banda para garantir a qualidade de voz.
- Prioridade no trafego sobre os outros tipos de VLans.
- Capacidade de roteamento nas áreas mais congestionadas da rede.
- Atraso menor que 150ms (milissegundos) na rede em que opera.

[11] O ip (*Internet* Protocol) é o endereço logico que todo equipamento (notebook, computador, etc) tem na rede e na rede local. Ele é como se fosse um endereço de uma residência que a identifica onde a encomenda será entregue. Disponível em < https://www.portaleducacao.com.br/conteudo/artigos/direito/afinal-o-que-e-ip-mascara-gateway-e-dns/49129>. Acessado em: 20 nov. 2017.

[12] É um número de 32 bits usada para separar em um ip a parte que ela corresponde a rede pública. Disponível em: < https://imasters.com.br/artigo/12876/redes-e-servidores/dicas-sobre-mascaras-de-rede?trace=1519021197&source=single>. Acessado em: 21 nov. 2017.

Para o mesmo autor a rede toda tem que ser desenhada para suportar *VOIP*, pois em muitas vezes teremos um computador que trafega dados em diferentes VLans ligados via cabo de rede a um telefone *VOIP* da Cisco que está trafegando voz em uma VLan diferente conforme Figura 18.

Figura 18: VLan de voz.



Fonte: (Cisco[s.d])[13]

3.3 Identificação DE VLans

Segundo Filippetti (2008) as VLans podem estar espalhadas por um grande "emaranhado" de *switches* que são capazes de identificar os frames ou quadros e a VLans na qual pertencem graças a um recurso chamado *Frame tagging* (etiquetamento de frames ou identificação de *frames*) que fazem com que os switches direcionem os frames para as portas pertinentes.

[13] https://static-course-assets.s3.amazonaws.com/RSE503/pt/index.html#3.1.1.4

Para Fey e Gauer (2015) existem dois tipos de links por onde trafegam os frames:

- *Links* de acesso (*access links*): Links que ligam a porta do *switch* com o elemento conectado à porta dele de forma direta e fazem parte de uma única VLan.
- Link de transporte (*trunk link*): *Links* que trafegam os *frames* ou quadros entre as VLans, esses links fazem parte de todas as VLans de um *switch*.

Segundo Filippetti (2008) o conceito de “entroncamento” de links permite que você torne uma porta ou interface de switch ou servidor membro de múltiplas VLans ao mesmo tempo e concomitante fazendo com que um servidor seja acessado por usuário de várias VLans sem que para isso tenham de atravessar algum roteador. Ainda segundo autor esse processo de “entroncamento” é muito usual na conexão entre *switches* (*uplinks*), já que os links de transportes tem a capacidade de transmitir informações sobre todas as VLans existentes através de apenas um link físico, se por acaso esse link não for entroncado serão transmitidos apenas informações da VLan um (VLan *default*) e ao criar a VLan de transporte (*trunk port*) as informações de todas as VLans poderão trafegar na rede por default, outro detalhe importante é que VLans indesejadas deverão ser excluídas manualmente para que suas informações não sejam propagadas através dela.

Segundo Fey e Gauer (2015) para se criar VLan é necessário ter o conhecimento das técnicas independente de qual fabricante de switch seja ou modelo, também é variável a quantidade de VLans permitidas em cada modelo de cada fabricante.

3.4 Frame TAGGING

Para o mesmo autor a tecnologia *frame tagging* foi desenvolvida para acompanhar o *frame* que atravessa o *link* de transporte (*trunked link*), onde sua identificação de VLan é removida antes que ele deixe o *link* de transporte o que torna o processo transparente, fazendo também que em cada *switch* atravessado pelo *frame* ou quadro deve ser identificado o (tag) da VLan que ele pertence utilizando a tabela de filtragem (*filter table*) para decidir o que será feito com o *frame*, ele será

encaminhado através dos switches através dos links de transporte até chegar ao switch de destino no link de acesso e assim remover a identificação de VLan, fazendo com que o dispositivo receba o *frame* sem tomar conhecimento de qual VLan o *frame* pertenceu.

3.5 Métodos de identificação de vlans

Ainda segundo mesmo autor existem dois métodos de identificação de VLans e cada método é um tipo de encapsulamento diferente:

- ISL (*Inter-Switch Link*): Exclusividade dos *switches* Cisco, esse tipo de encapsulamento pode é utilizado somente em links *Fast* e *Gigabit* Ethernet sendo aplicado as interfaces de switches, roteadores de servidores para seu entroncamento que se torna mais útil em VLans funcionais e valendo-se da regra de 80/20 (80% do trafego mantido localmente) mantendo o servidor truncado e membro de todas as VLans simultaneamente evitando assim que os usuários necessitem atravessar um dispositivo de camada 3 para acessar tal servidor, aumentando assim o desempenho da rede e reduzindo a complexidade da operação.

Para Filippetti (2008) esse método encapsula *frames* com informações sobre VLans de forma externa ao mesmo sem que o original seja alterado, dentre suas vantagens estão a baixa latência a velocidade limitada ao meio físico, o método ISL permite a multiplexação de VLans (transmissão de múltiplas VLans) por meio de apenas um *link* de transporte, trabalhando também com a interconexão de múltiplos *switches* mantendo a segregação de cada VLan enquanto os dados trafegam nos *links* de transporte pela malha de *switches*.

Ainda segundo autor no ISL o *frame* é encapsulado por um cabeçalho de 26 bytes fazendo com que apenas dispositivos compatíveis com ISL possam decodifica-lo, outro detalhe importante seria que esse *frame* ISL pode chegar a um comprimento de até 1522 bytes fazendo com que dispositivos incompatíveis com essa tecnologia entenda o *frame* como anormal uma vez que os padrões *Ethernet* normais seriam de 1518 bytes.

- IEEE 802.1q: É o método padrão da identificação de *frames*, nesse método é inserido um campo especifico dentro do *frame* sendo responsável pela identificação da VLan do *frame*. Esse método foi criado pelo IEEE (Instituto de Engenheiros Elétricos e Eletrônicos) e funciona tanto em switches Cisco como de outros fabricantes. Os switches novos da Cisco suportam apenas o método IEEE 802.1q mostrando uma forte tendência de a Cisco abandonar o ISL em um futuro bem próximo.

3.6 Roteamento entre vlans

Para Filippetti (2008) todos os dispositivos dentro da mesma VLan estão dentro de um mesmo domínio de *broadcast* e se comunicam normalmente. Como já dito anteriormente a função das VLans é segmentar a rede criando vários domínios de *broadcast* e para que diferentes dispositivos de diferentes VLans se comuniquem se faz necessário a presença de um dispositivo de camada três como um roteador ou um switch L3 que suporte os ISL ou IEEE 802.1q com uma interface para cada VLan. Para o uso de duas ou três interfaces *Ethernet* já atenderiam as necessidades.

Ainda segundo autor no caso de mais VLans do que interfaces disponíveis, pode-se adotar um roteamento ISL ou IEEE 802.1q em uma única interface *FastEthernet* que habilitado para tal encapsulamento é conhecido como *router-on-a-stick*. Outra forma de implementar tal roteamento entre VLans seria com o uso de switches L3 que implementam a pilha de protocolos TCP/IP e não se restringe apena a camada 2 do modelo de referência OSI tornando-se capaz de rotear pacotes IP.

PROTOCOLO VTP

Para Fey e Gauer (2015) o protocolo VTP (*VLan Trunking Protocol*) é proprietário Cisco que tem a função de criar, excluir e renomear VLans, sendo ele muito útil nas grandes estruturas de rede onde os administradores precisam gerenciar as VLans pois as configurações aplicadas e inseridas no banco de dados de VLans é replicado automaticamente para os demais *switches* da rede.

Protocolo existente nas versões um, dois e três e baseado em sistema cliente/servidor o VTP é instala em um servidor e os clientes enviam dados para ele

em uma determinada faixa de tempo, seu uso previne erros de inconsistência de configuração de VLans e facilita a administração das VLans segundo afirmação do mesmo autor.

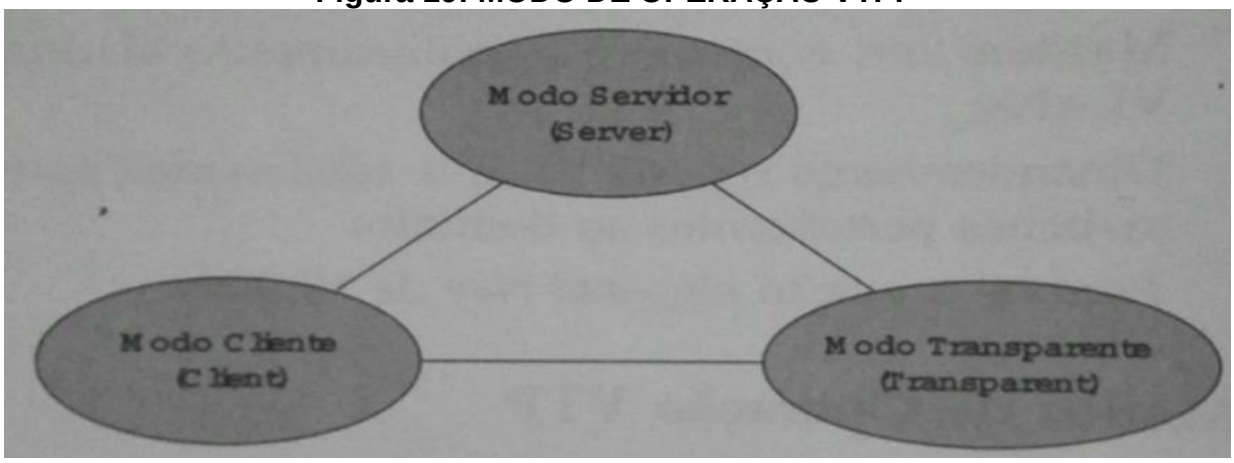
VTP *SERVER*

Segundo Fey e Gauer (2015) nesse modo VTP *server* o *switch* anuncia o domínio VTP, a configuração de VLan e o número de revisão para os vários *switches* pertencentes ao domínio VTP, lembrando também que o *switch* em modo VTP *server* cria, deleta e renomeia as VLans, provendo sincronismo da base de dados das VLans no domínio VTP. Qualquer alteração realizada no switch modo VTP *server* (adicionar, remover ou renomear VLan) é replicado através do domínio VTP, sincronizando as configurações de VLan.

VTP *CLIENT*

Segundo mesmo autor, no modo VTP *Client* o switch repassa para seus vizinhos sua configuração de VLans, o switch nesse modo não cria, deleta ou renomeia VLans deixando essas demandas para o switch VTP modo server realizar, conforme Figura 19.

Figura 19: MODO DE OPERAÇÃO VTP.



Fonte:Filippetti (2008).

VTP *TRANSPARENT*

Ainda segundo as publicações do mesmo autor o switch em modo VTP transparente não participa do domínio VTP nem repassa suas configurações de

LANs para os switches vizinhos, ele necessita que suas configurações sejam feitas manualmente, e essas configurações estarão operantes localmente nele.

VTP *PRUNING*

Para Filippetti (2008) o processo VTP *pruning* (“poda”) ajuda a conservar a largura de banda e reduz o volume de *broadcasts*, ele propaga as atualizações apenas para os *link*s de transporte que necessitem da informação, daremos como exemplo um *switch* que não tem nenhuma porta associada a VLan 12 e essa mensagem de *broadcast* for oriunda dessa mesma VLan essa mensagem não atravessara o link de transporte até esse *switch*, importante lembrar que o VTP *pruning* encontra-se desabilitado em todos os switches Cisco, também vale ressaltar que o *Pruning* não pode ser habilitado na VLan um por ser a VLan administrativa sendo ele hábil para implementação da VLan 2 a 1005, e uma vez que habilitado o VTP *pruning* no VTP server ele estará habilitada para toda rede.

3.7 Vantagens se usar VLan

Segundo site da Cisco ([s.d]) com o uso de VLans tem-se o aumento da produtividade do usuário e uma rede melhor adaptada e que suporte os objetivos da organização, fora isso os principais objetivos do uso das VLans são:

- Segurança – Podemos separar grupos confidenciais do resto da rede mitigando as chances de informações sigilosas sejam violadas.
- Redução de custos – Uso mais eficiente e enxuto da rede, economizando na banda e nos *uplinks* existentes. E menor necessidade de atualização de redes caras.
- Melhor desempenho – Dividindo a rede de camada 2 em vários domínios de *broadcast* aumenta o desempenho da rede.
- Diminuir domínios de *broadcast* - Segmentar rede em VLans reduz o número de domínios de *broadcast*.
- Maior eficiência da equipe de TI – Facilita o gerenciamento da rede atribuindo nomes as VLans, os usuários do mesmo projeto compartilham dos mesmos

recursos residem na mesma VLan, políticas e procedimentos são aplicados em todas as portas da mesma VLan.

- Gerenciamento mais simples de projetos e aplicativos - As VLans assimilam usuários e seus dispositivos de rede para suportar a empresa ou os requisitos geográficos.

3.8 Processo de Simulação

O experimento tem a finalidade de reproduzir 2 cenários simulados diferentes (1 cenário com VLan, 1 cenário sem VLan) com o intuito de entender o comportamento das VLans e a falta delas.

3.9 Ferramenta de Simulação

Para manipulação dos cenários das VLans em ambiente simulado será utilizada a ferramenta educacional de simulação de configuração de rede da Cisco o Packet Tracer 7.1. Será usado equipamentos configurados e periféricos idênticos aos existentes em situações real.

3.10 Definição das métricas

As métricas definidas serão a realização da tentativa de acesso por parte de um desktop de uma VLan para outro desktop em outra VLan, também será feito esse procedimento em cenário sem VLan, ambos testes serão realizados na Ferramenta Educacional Packet Tracer 7.1, também será disparado broadcast nos cenários com e sem VLan para realizar a comparação conforme metodologia comparativa, descrita e utilizando de variáveis qualitativas.

3.11 Criação do Ambiente

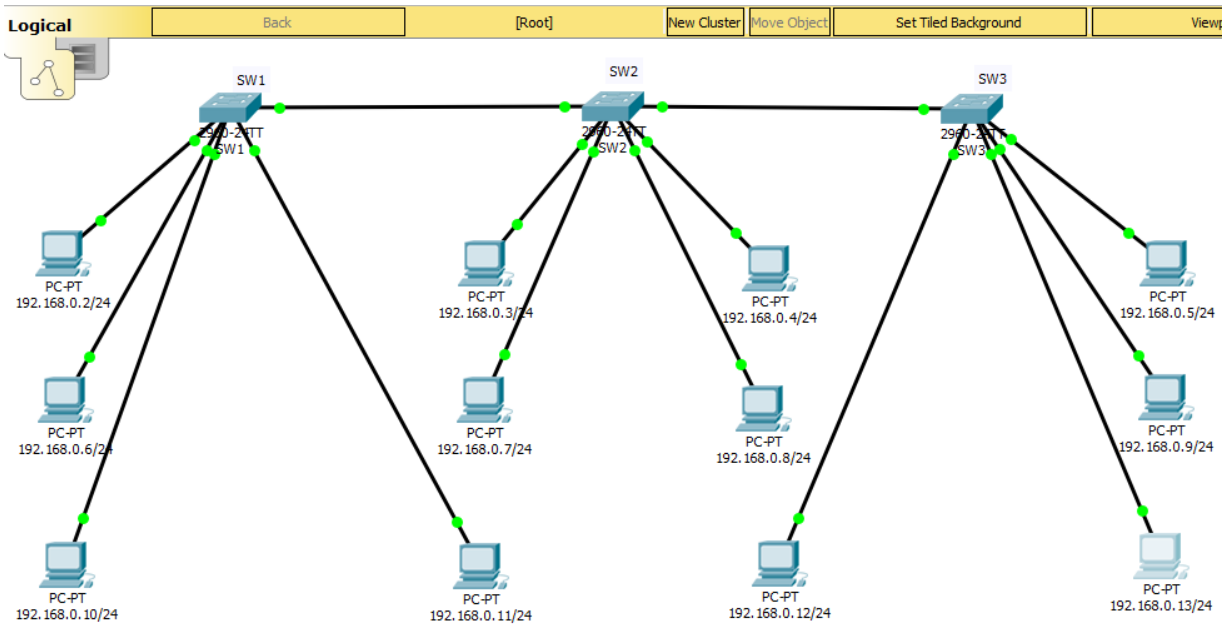
Conforme evidenciado na Figura 20, foram conectados na rede 12 computadores completos em três switches idênticos, cada um com um ip diferente, com as mesmas mascaras de sub-rede e no mesmo gateway[14].

No *switch* 2 será configurado o VTP *server* que tem o banco de dados das Vlans, já no *switch* 1 e o *switch* 3 serão configurados VTP client que recebem as informações de Vlans do *switch* configurado como VTP *server*.

A seguir um tem-se um levantamento detalhado do *hardware* usado e da quantidade de cabos necessários:

- três *Switches* CISCO Catalyst 2960 24 portas ethernet 10/100 e 2 portas *uplink* 10/100/1000
- 200 metros Cabo par trançado CAT5.
- 28 unidades de RJs 45 para crimpar[15] os cabos.
- 12 desktops completos com placa ethernet 10/100.

Figura 20: Cenário com 12 computadores.



Fonte: Próprio autor.

[14] Computador ou roteador que fica localizado entre 2 redes, traduzindo perfeitamente do inglês para o português tem-se a palavra "portal" que é exatamente como ele se comporta na rede. Disponível em: < https://www.palpitedigital.com/o-que-e-gateway/>. Acessado em: 16 nov. 2017

[15] Ato de esmagar o os contatos do conector rj45 para que eles entrem em contato com os fios do cabo de rede usando um alicate de crimpagem que é próprio para isso. Disponível em < http://www.hardware.com.br/tutoriais/cabeamento-rede/pagina2.html>. Acessado em: 20 nov. 2017

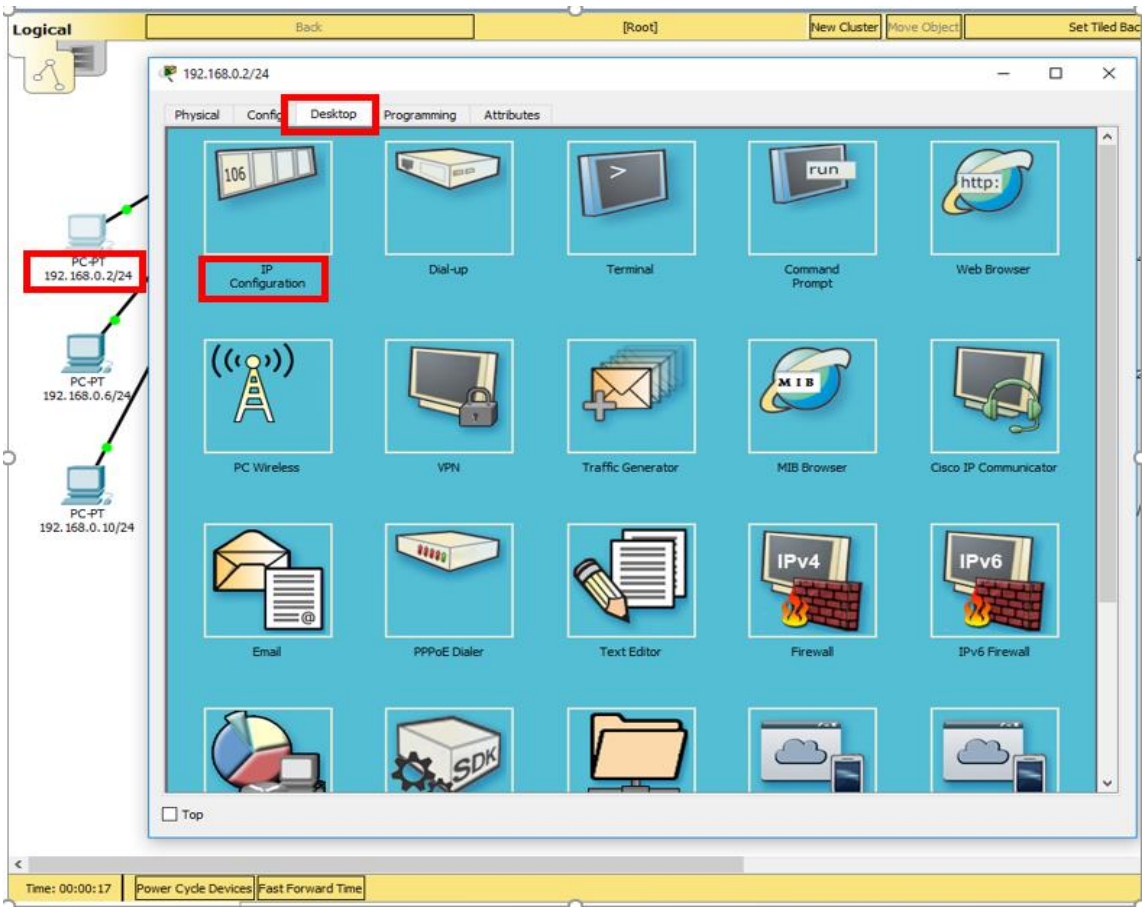
Os testes bem-sucedidos foram realizados com os switches CISCO Catalyst 2960 na ferramenta de simulação Packet Tracer, não impedindo que qualquer interessado no tema experimente realizar os mesmos testes com outros modelos de switches, deixando claro que não haverá garantia de que funcione. Também é valido deixar informado que a tecnologia VLan não é exclusividade da Cisco e que a mesma é configurável em outros tipos de fabricantes e modelos de switches.

3.12 Configurações dos ips nos computadores

Na figura 21 temos o passo a passo para configuração manual dos ips, máscara de sub-rede e gateway, chegamos na configuração seguindo a seguinte sequência:

1 Clique no computador a ser configurado com o botão esquerdo do mouse
2 Clique em Desktop
3 Clique em IP Configuration.

Figura 21: Inserir IP em computador no Packet Tracer.

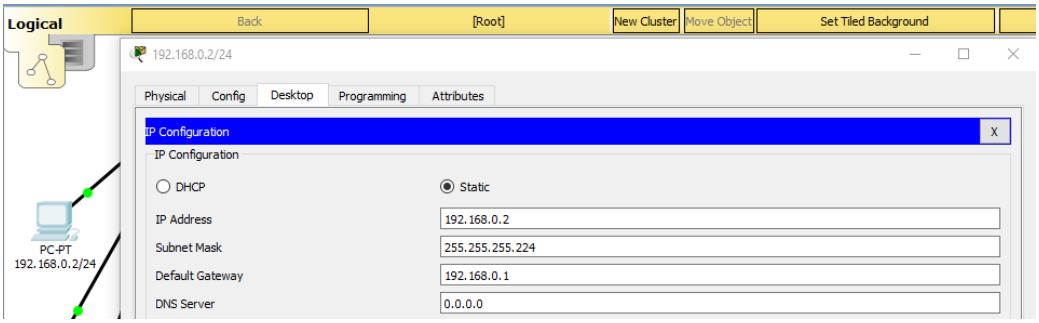


Fonte: Próprio autor.

4 Preencha os dados das colunas IP Adreess, Subnet Mask (máscara de sub-rede) e Default Gateway conforme Figura 22 e feche a janela.

5 Faça o procedimento anterior (4) em todos os equipamentos da rede colocando os endereços pertinentes em cada computador conforme Tabela 1.

Figura 22: Configuração do primeiro computador da rede.



Fonte: Próprio autor.

Na Tabela 1 um estão listados os endereços ips dos computadores, máscara de sub-rede e gateway dos periféricos, suas VLans, em qual switches e em que portas estão conectadas também está registrado em qual departamento cada computador está.

Tabela 1: Periféricos e configurações

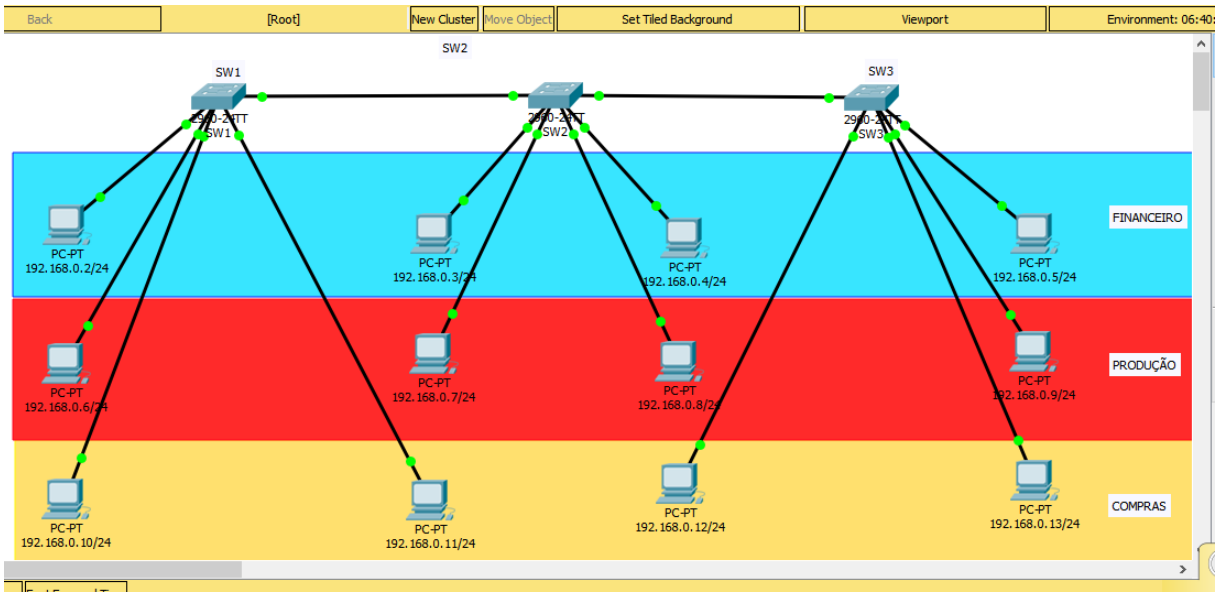
DEPARTAMENTO	VLan	Porta/Switch	IP	Subnet Mask	GATEWAY
FINANCEIRO	10	0/1 SW1	192.168.0.2	255.255.255.224	192.168.0.1
FINANCEIRO	10	0/1 SW2	192.168.0.3	255.255.255.224	192.168.0.1
FINANCEIRO	10	0/3 SW2	192.168.0.4	255.255.255.224	192.168.0.1
FINANCEIRO	10	0/2 SW3	192.168.0.5	255.255.255.224	192.168.0.1
PRODUÇÃO	20	0/2 SW1	192.168.0.6	255.255.255.224	192.168.0.1
PRODUÇÃO	20	0/2 SW2	192.168.0.7	255.255.255.224	192.168.0.1
PRODUÇÃO	20	0/4 SW2	192.168.0.8	255.255.255.224	192.168.0.1
PRODUÇÃO	20	0/3 SW3	192.168.0.9	255.255.255.224	192.168.0.1
COMPRAS	30	0/3 SW1	192.168.0.10	255.255.255.224	192.168.0.1
COMPRAS	30	0/4 SW1	192.168.0.11	255.255.255.224	192.168.0.1
COMPRAS	30	0/1 SW3	192.168.0.12	255.255.255.224	192.168.0.1
COMPRAS	30	0/4 SW3	192.168.0.13	255.255.255.224	192.168.0.1

Fonte: Próprio autor.

3.13 Configuração das Vlans nos switches

Para ilustrar as Faixas das VLans que serão configuradas foram desenhadas três faixas de cores diferentes no cenário, onde na Faixa azul está a VLan 10 (FINANCEIRO), na Faixa vermelha está a VLan 20 (PRODUCAO) e por último na VLan 30 está em amarelo (COMPRAS).

Figura 23: Faixas de cores para ilustrar a Vlans.



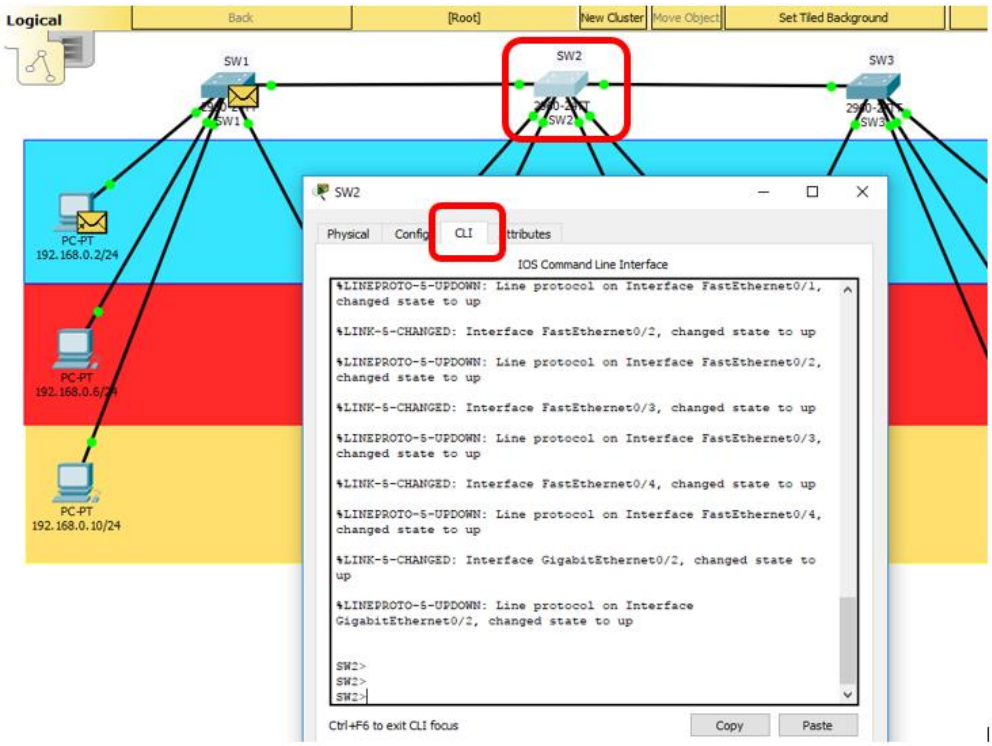
Fonte: Próprio autor.

3.14 Configuração do VTP server

Como foi definido que o Switch 2 será o VTP server então ele será configurado primeiro.

Sendo assim clique com o botão esquerdo do mouse no Switch 2, selecionado na figura 24 e logo após clique em CLI (*Comand Line Interface*).

Figura 24: Entrando na interface CLI do Switch 2.



Fonte: Próprio autor.

Logo após realizar a sequência anterior, digite os comandos conforme figura 25:

Figura 25: Configurar no switch 2 trunk entre switches e VTP server.

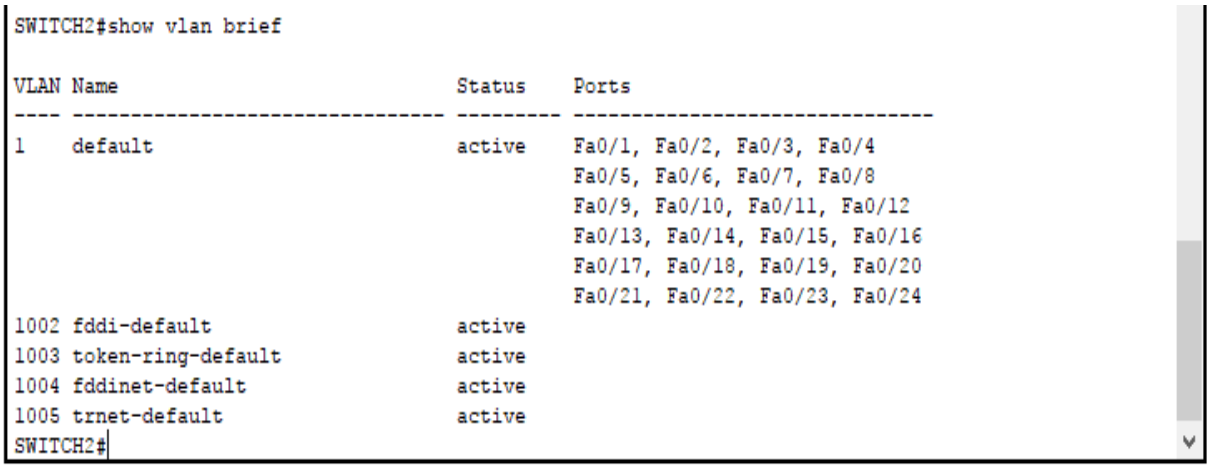
```
SWITCH2#enable
SWITCH2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH2(config)#interface gigabitEthernet 0/1
SWITCH2(config-if)#switchport mode trunk

SWITCH2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

SWITCH2(config-if)#switchport trunk allowed vlan all
SWITCH2(config-if)#interface gigabitEthernet 0/2
SWITCH2(config-if)#switchport mode trunk

SWITCH2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up

SWITCH2(config-if)#switchport trunk allowed vlan all
SWITCH2(config-if)#vtp mode server
Device mode already VTP SERVER.
SWITCH2(config)#vtp domain MONOGRAFIA
Changing VTP domain name from NULL to MONOGRAFIA
SWITCH2(config)#
```

Fonte: Próprio autor.

3.15 Criando as VLans no Switch 2

Para verificar as Vlans configuradas no *Switch* 2, digite o comando conforme figura 26, na figura só existe a VLan default.

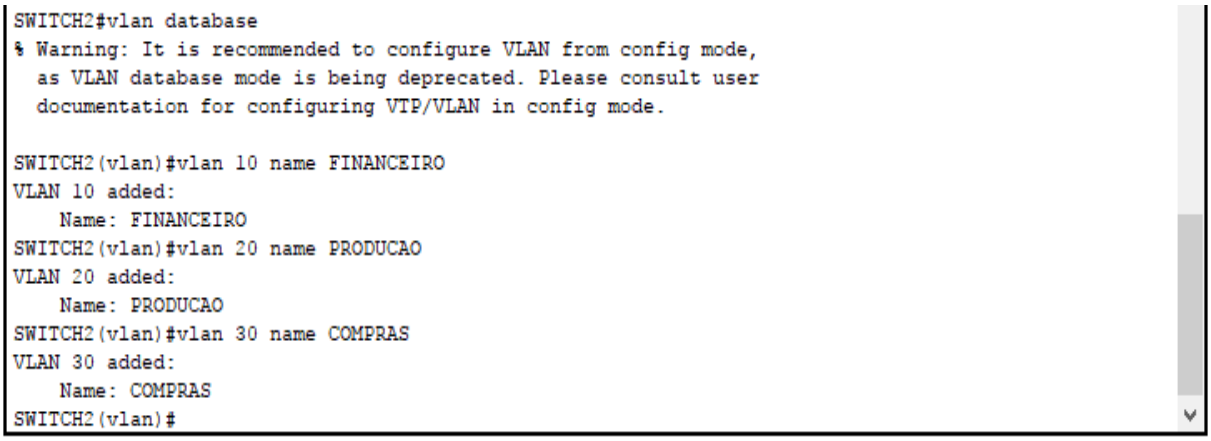
Figura 26: Show vlan brief switch 2.



Fonte: Próprio autor.

Agora criar-se as VLans no *switch* vtp *server* digitando os comandos conforme Figura 27:

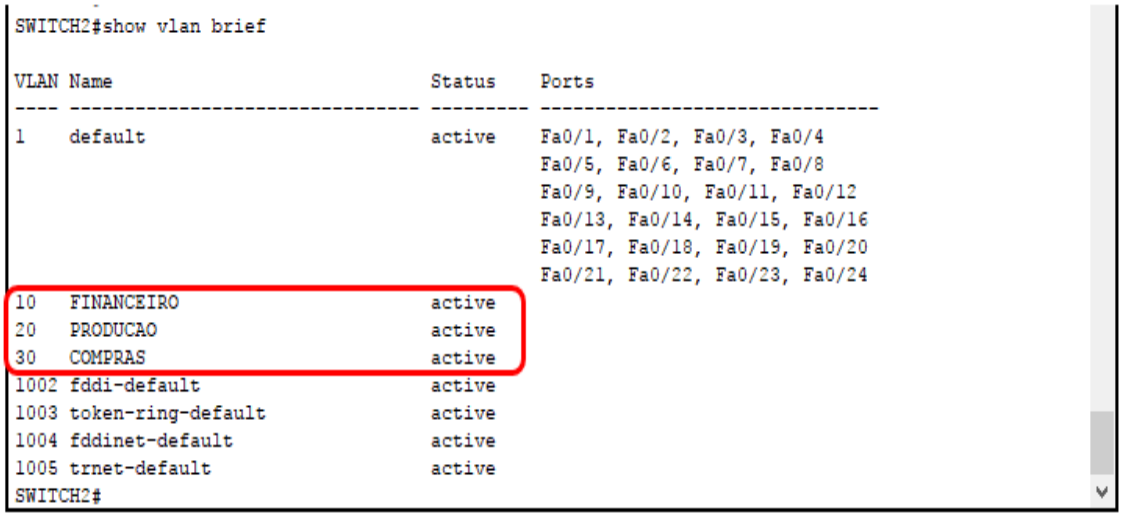
Figura 27: Criando VLans no Switch mode VTP server.



Fonte: Próprio autor.

Logo após criar as VLans, consulte-as conforme Figura 28:

Figura 28: Switch2 com as Vlans criadas.

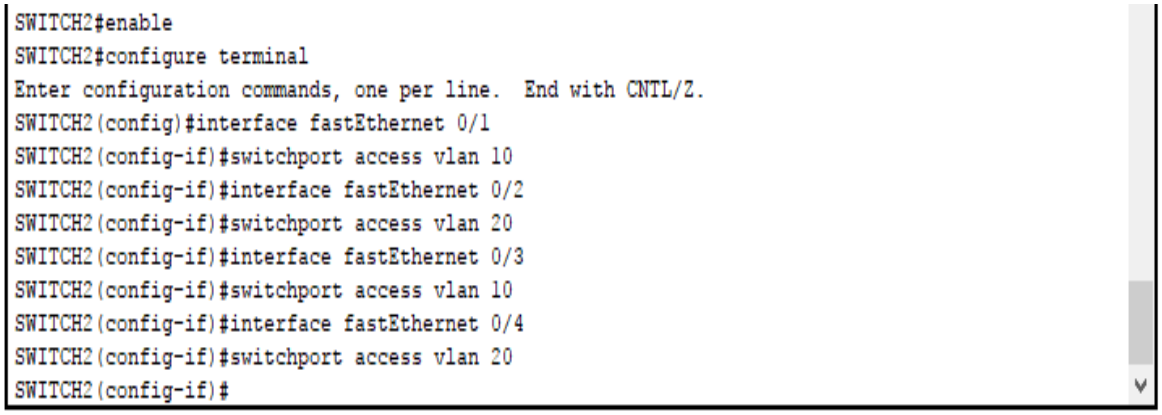


Fonte: Próprio autor.

3.16 Configurando os Portas do Switch nas Vlans do Switch 2

Digitar no switch 2 os comandos da Figura 29 para associar as portas do switch as devidas VLans conforme Tabela 1.

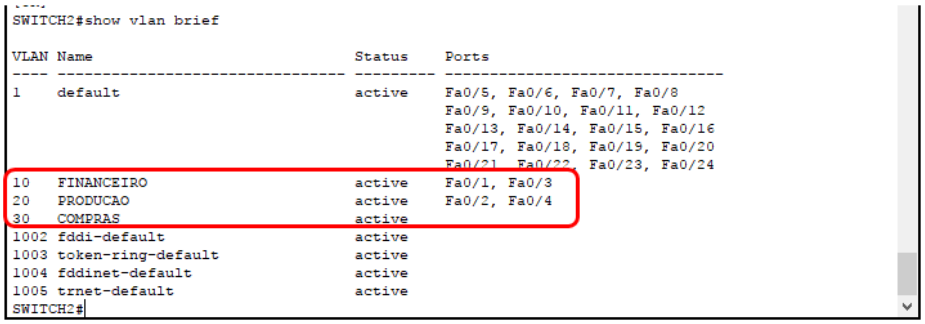
Figura 29: Associando as portas do switch 2 as devidas VLans.



Fonte: Próprio autor.

Após comandos inseridos na interface CLI do *switch* 2 e associadas as portas as devidas VLans elas ficarão descritas de acordo com a figura 30.

Figura 30: Switch 2 com as portas configuradas nas devidas VLans.

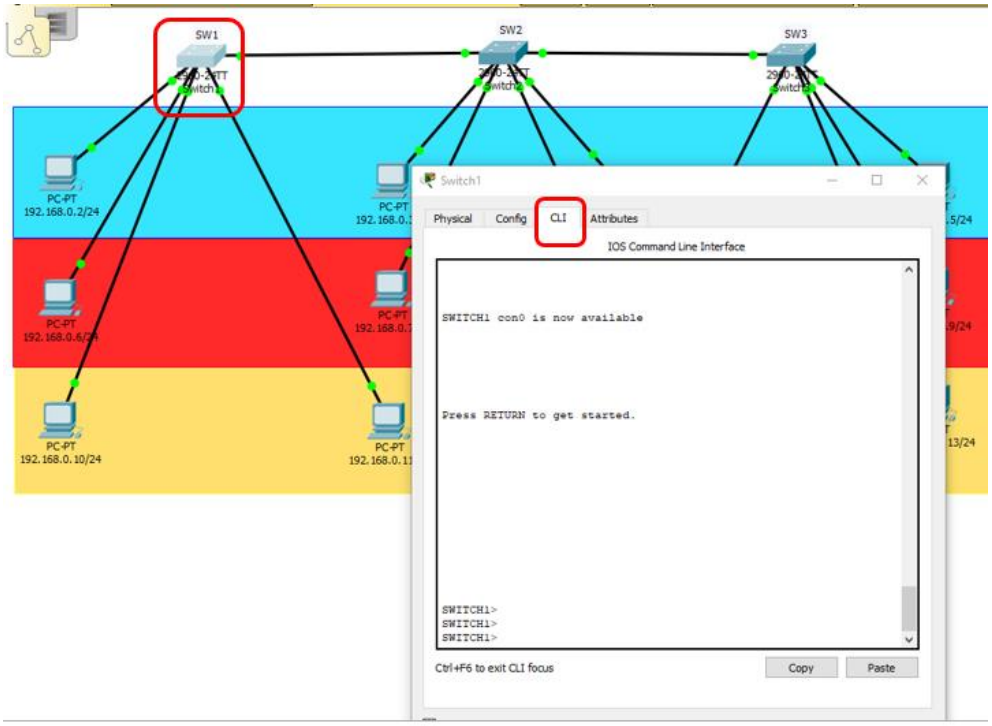


Fonte: Próprio autor.

3.17 Configurando Vtp modo *client* no Switch 1

Para configurar o switch 1 como VTP modo client clicaremos no item selecionado na figura 31, em seguida clicaremos em CLI:

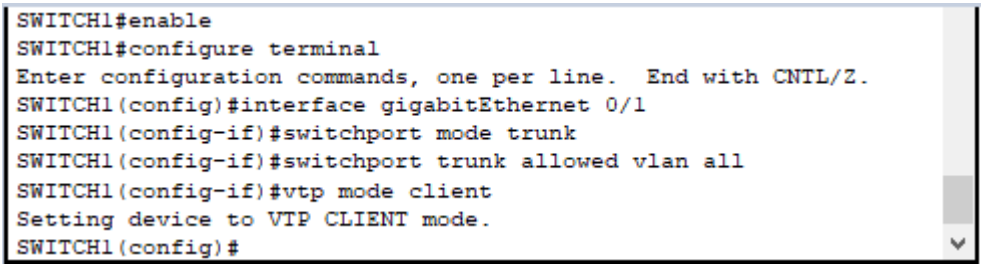
Figura 31: Entrando na interface CLI do Switch 1.



Fonte: Próprio autor.

Digitar os comandos da Figura 32 em sequência no Switch 1 para configurar o VTP client.

Figura 32: Configurar no switch 1 trunk entre switches e VTP client.

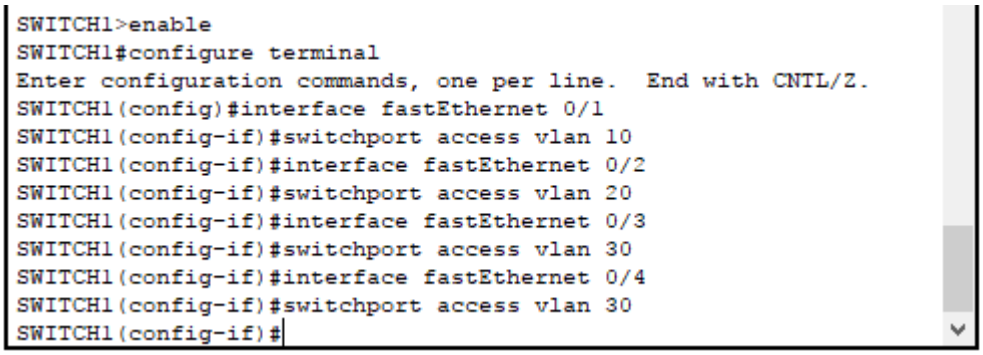


Fonte: Próprio autor.

3.18 Configurando os Portas do Switch nas Vlans do Switch 1

Digitar no switch 1 os comandos da Figura 33 para associar as portas do switch as devidas VLans conforme Tabela 1.

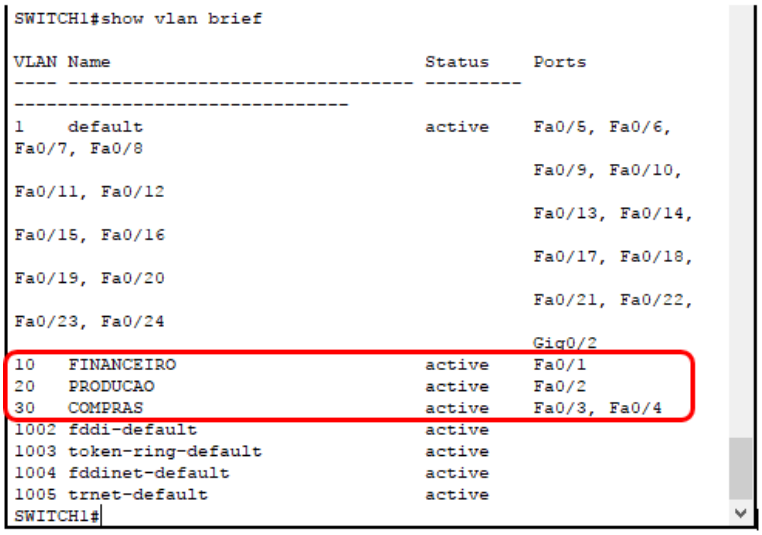
Figura 33: Associando as portas do switch 1 as devidas VLans.



Fonte: Próprio autor.

Após comandos inseridos na interface CLI do *switch* 1 e associadas as portas as devidas VLans elas ficarão descritas de acordo com a figura 34.

Figura 34: Switch 1 com as portas configuradas nas devidas VLans.



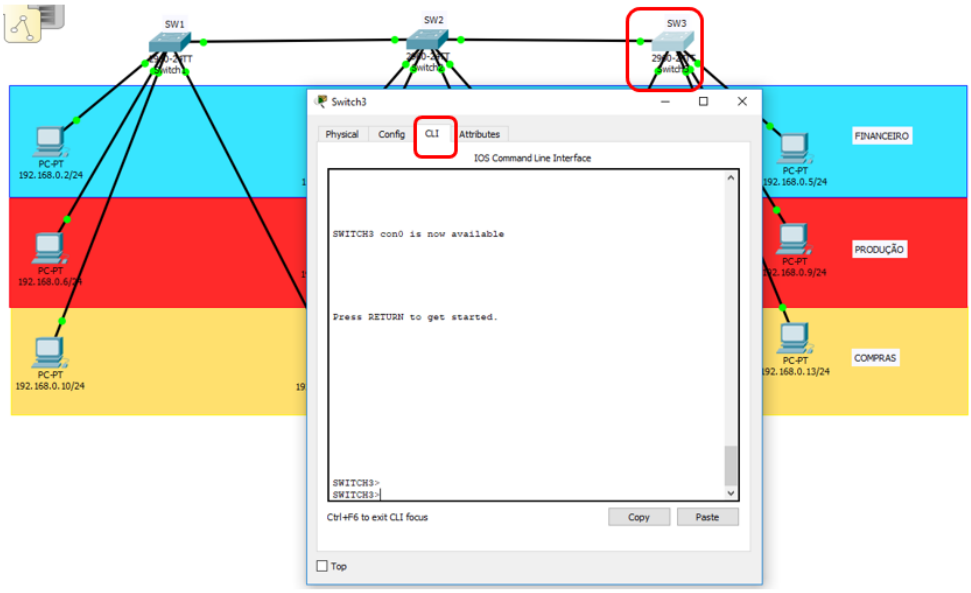
```
SWITCH1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6,
Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10,
Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14,
Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18,
Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22,
Fa0/23, Fa0/24
                                                 Gig0/2
10   FINANCEIRO                        active    Fa0/1
20   PRODUCAO                          active    Fa0/2
30   COMPRAS                           active    Fa0/3, Fa0/4
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
SWITCH1#
```

Fonte: Próprio autor.

3.19 Configurando Vlan modo client no Switch 3

Para configurar o switch 3 como VTP modo cliente clicaremos no item selecionado na figura 35, em seguida clicaremos em CLI:

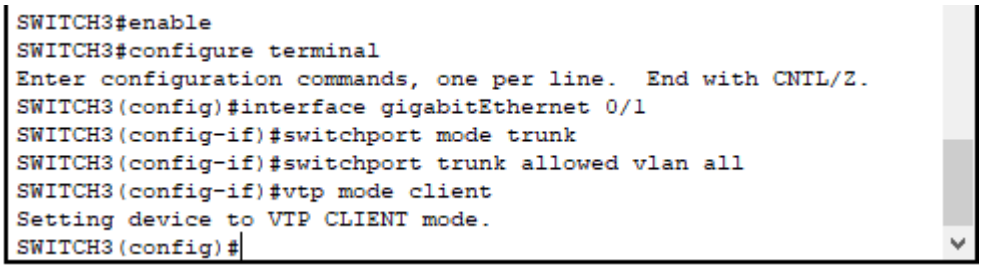
Figura 35: Entrando na interface CLI do Switch 3.



Fonte: Próprio autor.

Digitar os comandos da Figura 36 em sequência no *Switch* 3 para configurar o VTP client.

Figura 36: Configurar no switch 3 trunk entre switches e VTP client.

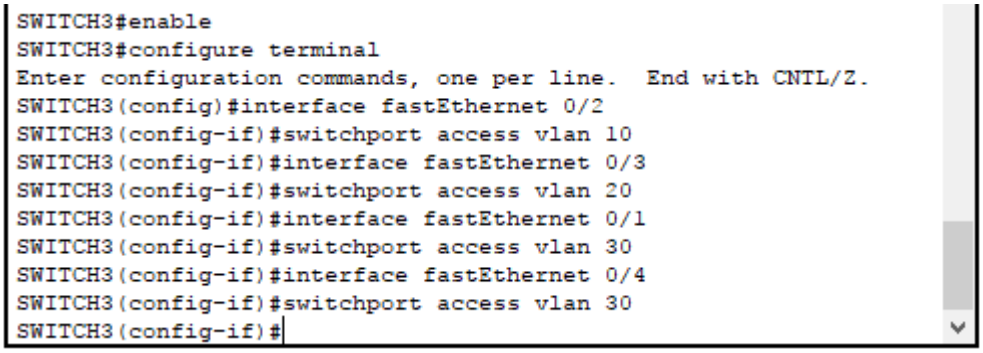


Fonte: Próprio autor.

3.20 Configurando os Portas do Switch nas Vlans do Switch 3

Digitar no switch 3 os comandos da Figura 37 para associar as portas do switch as devidas VLans conforme Tabela 1.

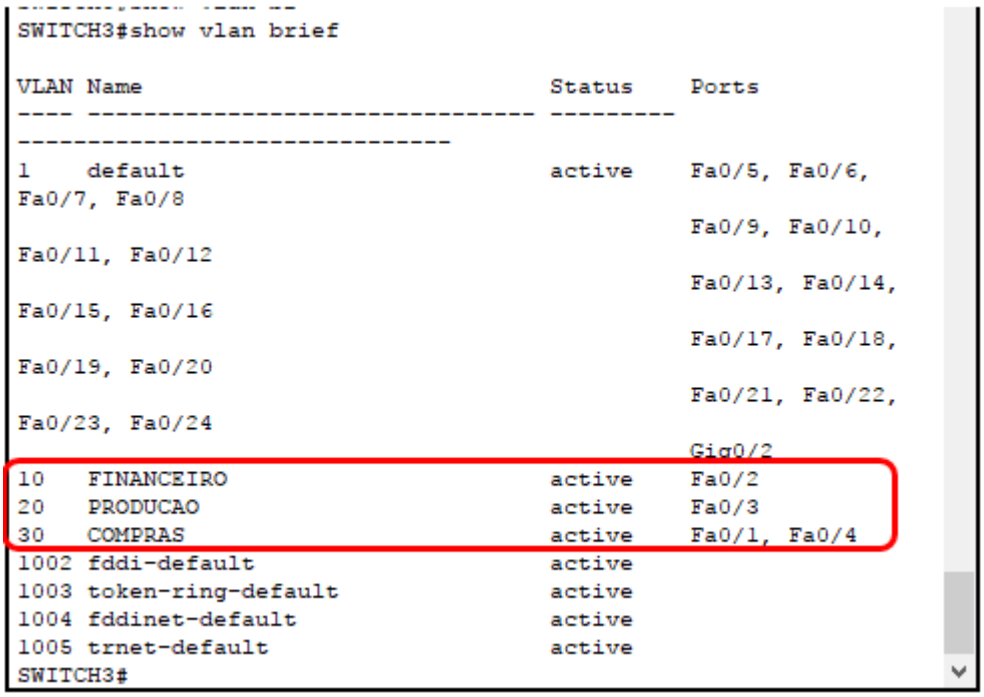
Figura 37: Associando as portas do switch 3 as devidas VLans.



Fonte: Próprio autor.

Após comandos inseridos na interface CLI do *switch* 3 e associadas as portas as devidas VLans elas ficarão descritas de acordo com a figura 38.

Figura 38: Switch 3 com as portas configuradas nas devidas VLans.



Fonte: Próprio autor

3.21 Tentativa de acesso.

Será realizado um teste de ping[16] para validar suas conectividades, e quais equipamentos estão disponíveis para quais equipamentos da rede usando os dois cenários criados para exemplificar o uso ou não de VLans.

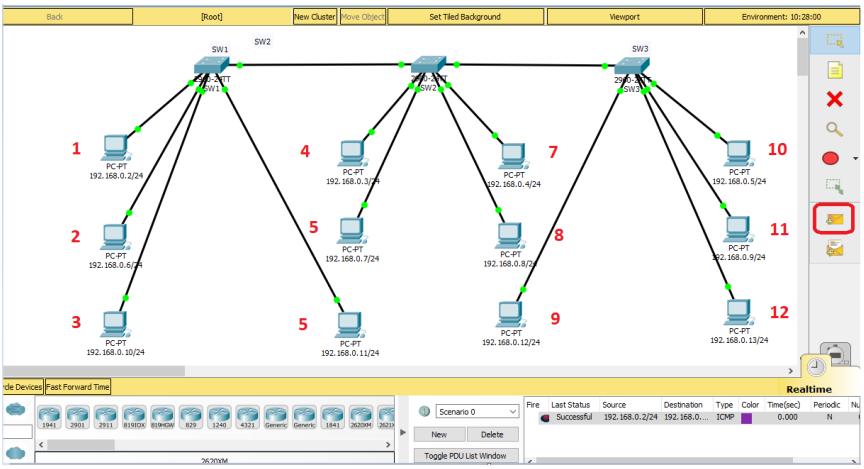
No cenário sem VLan figura 39 e cenário com VLan serão realizados os seguintes passos nos computadores conforme numeração:

1. Clique no item com a seleção retangular a direita.
2. Clique no computador 1 e depois no computador 2.
3. Clique no computador 1 e depois no computador 3.
4. Clique no computador 1 e depois no computador 4.
5. Clique no computador 1 e depois no computador 5.
6. Clique no computador 1 e depois no computador 6.
7. Clique no computador 1 e depois no computador 7.

[16] Abreviação do termo em inglês “Packet Internet Network Grouper” que traduzido temos a expressão “Agrupador de Pacotes de Internet” O comando Ping tem a função de testar a conectividade dos equipamentos de uma rede qualquer fazendo uso do protocolo ICMP, o comando ping envia dados para esses periféricos e “fiscaliza” suas respostas nos seus devidos tempos. Disponível em: < https://canaltech.com.br/internet/o-que-e-ping/>. Acessado em: 20 nov. 2017

8. Clique no computador 1 e depois no computador 8.
9. Clique no computador 1 e depois no computador 9.
10. Clique no computador 1 e depois no computador 10.
11. Clique no computador 1 e depois no computador 11.
12. Clique no computador 1 e depois no computador 12.

Figura 39: Cenário sem VLan.



Fonte: Próprio autor.

3.22 Resultado tentativa de Acesso

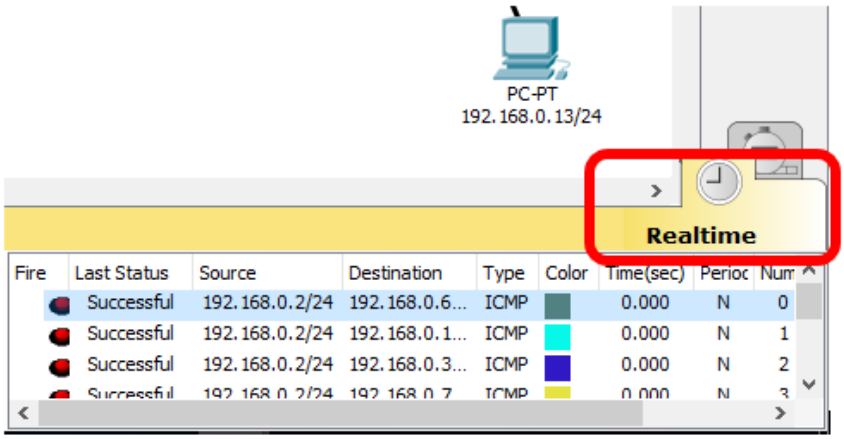
Na aba Realtime do Packet Tracer (Figura 40) é disponibilizado o resultado onde tem-se como item mais importante o sucesso ou falha da tentativa de conexão, o destino (IP) do teste e o tipo do teste. Com essas informações tem-se os resultados: No cenário sem VLan:

1. Computador 1 pingando o computador 2: Successful (Sucesso).
2. Computador 1 pingando o computador 3: Successful.
3. Computador 1 pingando o computador 4: Successful.
4. Computador 1 pingando o computador 5: Successful.
5. Computador 1 pingando o computador 6: Successful.
6. Computador 1 pingando o computador 7: Successful.
7. Computador 1 pingando o computador 8: Successful.
8. Computador 1 pingando o computador 9: Successful.
9. Computador 1 pingando o computador 10: Successful.
10. Computador 1 pingando o computador 11: Successful.
11. Computador 1 pingando o computador 12: Successful.

No cenário com VLan.

1. Computador 1 pingando o computador 2: Failed (Falha).
2. Computador 1 pingando o computador 3: Failed.
3. Computador 1 pingando o computador 4: Successful.
4. Computador 1 pingando o computador 5: Failed.
5. Computador 1 pingando o computador 6: Failed.
6. Computador 1 pingando o computador 7: Successful.
7. Computador 1 pingando o computador 8: Failed.
8. Computador 1 pingando o computador 9: Failed.
9. Computador 1 pingando o computador 10: Successful.
10. Computador 1 pingando o computador 11: Failed.
11. Computador 1 pingando o computador 12: Failed.

Figura 40: Realtime do Packet Tracer.



Fonte: Próprio autor.

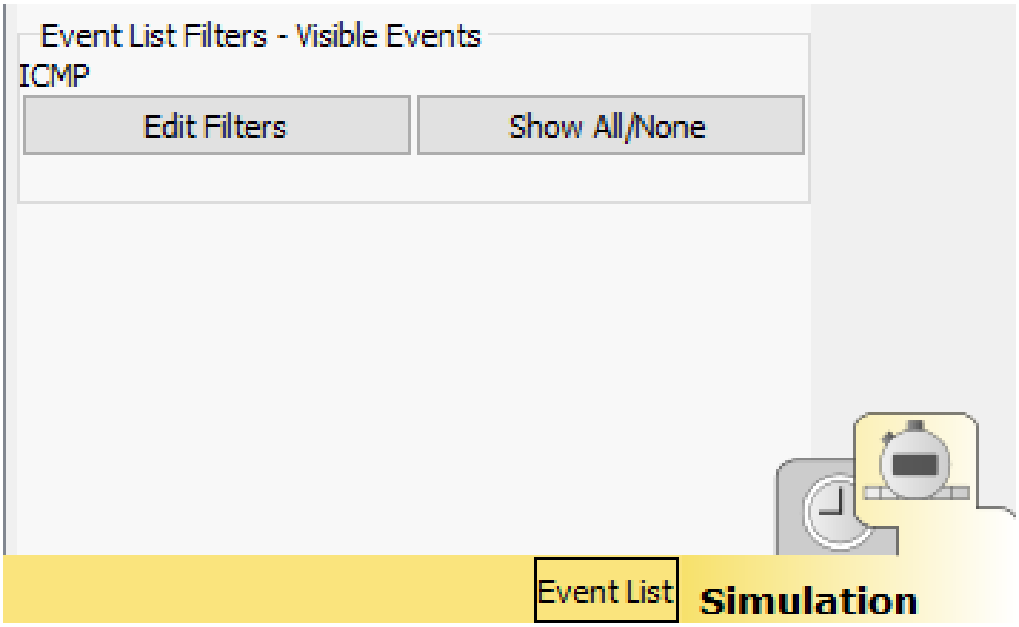
3.23 Simulação Broadcast

Será criado uma simulação de broadcast nos 2 cenários estudados, pois o procedimento de testes será o mesmo para as 2 situações. Siga os passos a seguir conforme Figura 42:

1. No cenário escolhido clique em Add complex PDU.
2. Clique no Primeiro Computador do Cenário identificado na figura 42 com o número um do lado.

3. Complete o valor de Destination IP Address com o valor 255.255.255.255[17] para que o PDU procure todos os IPs da rede.
4. No item Sequence Number coloque 1.
5. Em Simulação Settings no item One Shot coloque o valor 0 na coluna Time/Seconds.
6. Clique Creat PDU.
7. Conforme Figura 41 na aba Event List filters foi adicionado ao filtro o protocolo ICMP[18] que determina que será o tipo de PDU que trafegará pela rede em busca do IP descrito.

Figura 41: Edit Filters com os PDU ICMP que trafega pela rede.



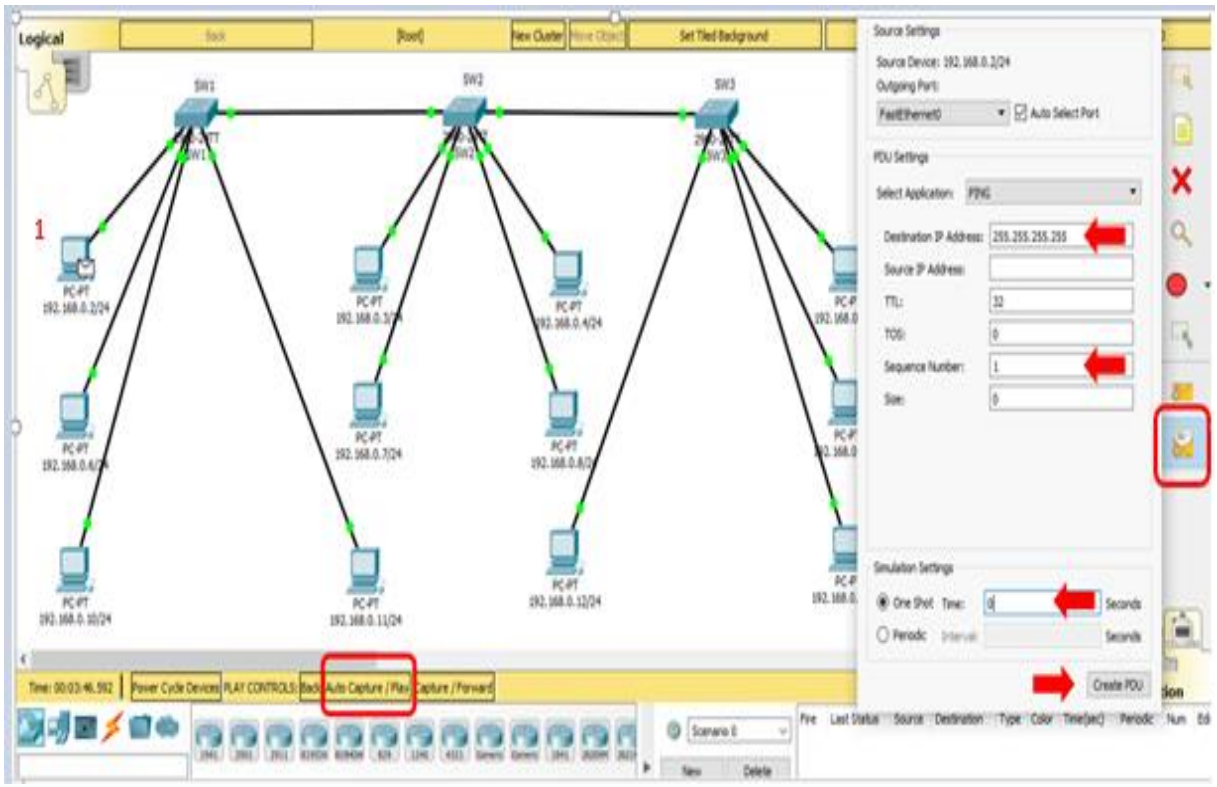
Fonte: Próprio autor.

8. Por último na figura 42 clique Auto Capture / Play para visualizar a entrega e retorno dos PDUs.

[17] Endereço comum para transmitir uma mensagem para todos os sistemas da rede. Disponível em < https://www.symantec.com/pt/br/security_response/glossary/define.jsp?letter=b&word=broadcast-address> . Acessado em: 20 nov. 2017

[18] (internet Control Message Protocol – Protocolo de Mensagens de Controle de Internet) esse protocolo gerencia informações pertinentes a erros nas maquinas da rede. Disponível em: <(internet Control Message Protocol – Protocolo de Mensagens de Controle de Internet)>. Acessado em: 20 nov. 2017

Figura 42: Add Complex PDU.



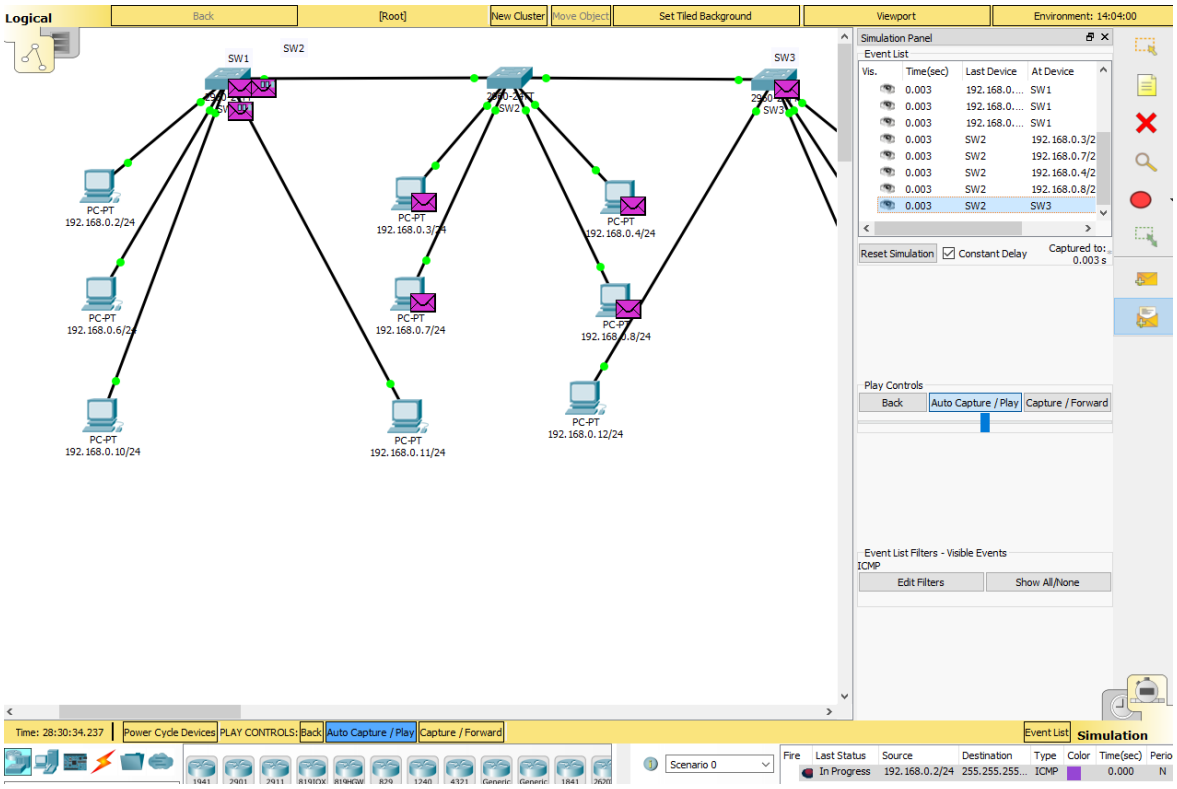
Fonte: Próprio autor.

3.24 Resultado de testes *Broadcast*

A Figura 43 mostra todo o trafego de PDUs que ocorre após o clique na ferramenta *Auto Capture / Play* no cenário criado sem VLan, assim que o PDU do tipo ICMP (conforme editados na lista de filtro) gerado pelo computador 1 é disparado, ele trafega por toda rede utilizando todo o *hardware*, fazendo que todos os computadores da rede recebam o pacote com sucesso.

Já esse mesmo teste realizado no cenário com VLan, o PDU gerado no computador 1 só é propagado pela faixa de VLan em que o computador de origem do *frame* se encontra, evitando que os PDUs cheguem a todos computadores da rede.

Figura 43: Trafego PDUs no cenário sem VLan configurada.



Fonte: Próprio autor.

3.25 Análise de resultados

Os resultados alcançados e estudados do item tentativa de acesso mostram que no cenário sem VLans o computador um tem acesso a todos os computadores da rede independente do setor que trabalha, qualquer que seja o equipamento da rede tem acesso a todos outros computadores e, o que comprometeria a confidencialidade das informações pois nenhum acesso a informação deve ser concedido a usuários e sistemas não autorizados, o que não ocorre no cenário com VLans pois conforme evidenciado no teste o computador um tem acesso apenas a computadores da mesma VLan que ele e todas tentativas de acesso do computador um para computadores de outras VLans falharam.

Ainda analisando o item tentativa de acesso, no cenário sem VLan o fato de haver essa alta disponibilidade desnecessária poderia gerar interceptação dos *frames* em algum ponto da rede o que causaria falta de integridade das informações onde

elas poderiam ser interceptadas e alteradas, já no cenário com VLans não existe toda essa disponibilidade o que tornaria essa interceptação algo mais difícil de acontecer.

Na simulação de *broadcast* do cenário sem VLans os PDUs foram disparados do computador um para todos os computadores da rede, utilizando todo *hardware* e toda infraestrutura, numa situação de tempestade de broadcast gerado por vírus ou por qualquer outro motivo poderia causar a indisponibilidade na rede, esse cenário de indisponibilidade não ocorreria no cenário com VLan pois conforme ocorreu no experimento os PDUs disparados pelo computador um só trafegaram por dentro da mesma VLan, pois os broadcasts não atravessam VLans permitindo que o problema fique contido.

Conclusões Finais

Baseado nos resultados dos testes simulados realizados no *packet tracer* com infraestrutura composta por três *switches* para suportar apenas 12 computadores, as diferenças de desempenho e segurança foram notadas de forma a não se deixar dúvidas a favor de utilizar as VLans, se pensarmos em uma infraestrutura de rede maior, com mais *switches*, computadores, adicionarmos impressoras de rede, *notebooks, tablets*, tecnologia Wifi e etc, fica difícil mensurar administrá-la sem a implementação de VLans.

Garantir que a privacidade dos dados seja mantida é permitir que somente os receptores autorizados tenham acesso as informações e deve-se sempre procurar diversas formas para proteger a rede de dados para assegurar a confidencialidade das informações, as VLans de certa forma ajudam demais nisso pois a forma com que divide a rede evita que pessoas voluntariamente ou por acidente acessem conteúdos que não são pertinentes a ele.

A atuação da VLan evitando acessos indevidos de outros setores da rede ajuda mitigar a possibilidade de interceptação e alteração das informações durante a transmissão, ajudando assim a manter a integridade da informação.

Por último e não menos importante temos de assegurar a disponibilidade da informação, de nada adianta a informação ser integra, confiável se os recursos da rede forem sobrecarregados e ficarem indisponíveis. A VLan ajuda muito nisso também, assegurando o acesso pontual e confiável a serviços e dados a apenas aos usuários ou setor pertinente a essas informações, evitando assim que uma sobrecarga de trafego de informação que deveria ser apenas local derrube a rede e a deixe indisponível.

Entre as hipóteses levantadas a partir do problema estabelecido, a hipótese atendida foi da letra A que alegava que a rede de dados estava com grande incidência de *broadcast* fazendo com que um enorme volume de dados irrelevantes trafegue por ela sem necessidade, deixando a rede toda lenta. Fica evidenciado que a solução dessa hipótese foi satisfeita nos testes realizados no ambiente controlado criado no cenário com VLan, quando o broadcast criado e disparado de um desktop ficou contido na mesma VLan no qual foi originado não sendo propagado para o restante da rede.

Os altos preços dos roteadores que não propagam *broadcast* tornam a criação das VLans em *switches* uma ótima alternativa para a melhora no desempenho e segurança da rede de dados.

Vale ressaltar que grande parte do tráfego das redes de computadores, são dados desnecessários causados por erros em cabos, placas de rede com problemas, protocolos ou aplicações com problema, a VLan ajuda a mitigar isso devido ao fato da informação incorreta e os broadcasts ficarem contidas dentro da mesma VLan.

REFERÊNCIAS BIBLIOGRÁFICAS

CISCO. **Modelos de protocolo e de referência**. 2017. Disponível em: <https://static-course-assets.s3.amazonaws.com/Exploration/E140PT/theme/cheetah.html?cid=0600000000&l1=tl&l2=en&chapter=2>. Acessado em: 19 set. 2017.

_____. **Vantagens das VLans.** <https://static-course-assets.s3.amazonaws.com/RSE503/pt/index.html#3.1.1.2>. Acessado em: 19 set. 2017

_____. **Modelo TCP/IP**. Disponível em: <https://static-course-assets.s3.amazonaws.com/Exploration/E140PT/theme/cheetah.html?cid=0600000000&l1=tl&l2=en&chapter=2>. Acessado em: 19 set. 2017

_____. **Tipos de Vlans.** <https://static-course-assets.s3.amazonaws.com/RSE503/pt/index.html#3.1.1.3>. Acessado em: 19 set. 2017

COLCHER *et al*., Sergio. **Voip:** voz sobre IP. Rio de Janeiro: Elsevier, 2005.

FACHIN, Odilia. **Fundamentos de Metodologia.** 5ª. ed. São Paulo: Saraiva, 2006.

FEY, Ademar Felipe; GAUER, Raul Ricardo. **Desvendando Vlans**. 2. ed. Caxias do Sul: Itit 2015.

FILIPPETTI, Marco Aurélio. **CCNA 4.1:** guia completo de estudo. 1. ed. Florianópolis: Visual Books, 2008.

FONTES, Edison Luiz Gonçalves. **Praticando a segurança da informação.** Fontes. 1ed. Rio de Janeiro: Brasport, 2008.

FOROUZAN, Behrouz A. **Comunicação de dados e rede de computadores**. 4. ed. São Paulo: McGraw – Hill, 2008.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a Internet:** uma abordagem top-down**.** 5. ed. São Paulo: Addison Wesley, 2010.

LAKATOS, Eva Maria, MARCONI, Marina de Andrade. **Técnicas de pesquisa**: 7. ed. São Paulo: Atlas, 2011.

MCQUERRY, STEVE. **Interconectando Cisco Network Devices**: 1. ed. Rio de Janeiro, Alta Books, 2002.

TITTEL, Ed.; STEWART, J. M. **Intranet a bíblia.** 1. ed. São Paulo: Berkeley Brasil, 1997.