EDUARDO LUIZ SCHINDLER

SEGMENTAÇÃO DE REDE LOCAL USANDO O MODELO HIERÁRQUICO DE REDE

MEDIANEIRA

2016

EDUARDO LUIZ SCHINDLER

SEGMENTAÇÃO DE REDE LOCAL USANDO O MODELO HIERÁRQUICO DE REDE

Monografia apresentada a Universidade Tecnológica Federal do Paraná – Campus Medianeira, como requisito à conclusão do curso de Tecnologia em Análise e desenvolvimento de Sistemas.
Orientador: Prof. Neylor Michel, Dr.

MEDIANEIRA
2016

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

RESUMO

Este trabalho foi elaborado com o propósito de apresentar o conceito e as funcionalidades da utilização das Redes Locais Virtuais. Com a utilização de VLANs pode-se conter os broadcasts e desta forma, além de melhorar o desempenho, aumenta-se a segurança impossibilitando os acessos indevidos de outras VLANs. É apresentada uma topologia da rede com a utilização de VLANs e tecnologias complementares que, ao estarem operacionais simultaneamente agregam desempenho ao sistema.

ABSTRACT

This project intends to present the concept and functions of the usage of Virtual Local Networks. With the usage of VLANs, the broadcasts can be avoided and therefore, the network performance and safety improve, making impossible for unwanted access to happen. Also, this project presents a network topology that uses VLANs and other technologies that enhance the system performance when operated simultaneously.

1. INTRODUÇÃO

Atualmente, é possível notar uma revolução nas formas de comunicação entre pessoas. É a chamada Revolução da Informação, cuja ocorrência se deu, principalmente, em virtude do desenvolvimento dos computadores pessoais (PC - *Personal Computers*) e das redes de computadores.

"As redes de computadores são indispensáveis ao funcionamento de praticamente todas as estruturas da sociedade. No nosso dia-a-dia, é quase certa a utilização de pelo menos um serviço dependente de uma rede de comunicação" (Véstias, 2005).

Para Torres (2001), mesmo fora do ambiente da informática, todos nós temos contato com algum tipo de rede em maior ou menor grau. O autor cita como exemplo os caixas eletrônicos. O autor cita que cada terminal não passa de um computador ligado a um computador central que armazena as informações da sua conta. Quem vive em grandes centros se depara com redes de computadores em supermercados, farmácias e inúmeros outros lugares.

A introdução em larga escala das redes de computadores trouxe novos problemas sociais, éticos e políticos, porém, o papel delas é fundamental.

Forouzan e Mosharraf (2012) afirma que a maior rede de computadores do mundo, a Internet, tem mais de um bilhão de usuários.

Nesse contexto, também estão inseridas as Redes Locais (LANs - *Local Area Networks*), presentes em maior número nas organizações e universidades.

Para Jung e Pellis (2013), atualmente uma das principais metas em uma rede é que ela seja confiável, organizada e estável para todos os usuários e equipamentos que dependem de seu bom funcionamento. Porém muitas vezes nos deparamos com situações inesperadas, que acabam dificultando o controle e a segurança da rede. Sejam elas por excesso de tráfego provocando uma sobrecarga nos ativos da rede, equipamentos não autorizados ocupando recursos e em alguns casos invadindo a rede local em busca de informações sigilosas, largura de banda ocupada por tráfego desnecessário e a falta de uma estruturação hierárquica o que que pode resultar em um tempo maior para a resolução de algum problema.

No decorrer desse trabalho, serão apresentados algumas soluções para esses tipos de problemas que visam um melhor aproveitamento dos ativos de rede,

estruturando e preparando a rede local para lidar com possíveis falhas, reduzindo seu tempo de indisponibilidade ou em alguns casos inibindo a mesma de falhas e principalmente propiciando um ambiente seguro para todos os que estão conectados na mesma.

1.1. Justificativa

Quanto mais tecnologia presente nas organizações, mais é exigido dos profissionais que atuam com as mesmas, esses profissionais cuidam do bem mais precioso de qualquer organização “a informação” e esta, por sua vez é vítima de constates ataques. Para isso existem variadas formas de proteger essas informações. Entre essas formas de proteção, caso trabalharem de forma independente poderão não ter o resultado esperado mas, caso trabalharem em conjunto, uma verdadeira muralha se forma em torno dessas informações que devem protegidas com tanto afinco, podendo chegar a 100% de proteção ou muito perto disso.

A proposta dessa explanação é tratada em um nível de segurança pouco explorado por administradores de redes, ou por falta de conhecimento ou em outros casos, pelo comodismo dos modelos tracionais de proteção, comodismo esse que muitas vezes deixa de explorar recursos valiosos dos dispositivos presentes na rede e em muitos casos deixam de fazer uso de um melhor desempenho do rede apenas com a aplicação de algumas técnicas de gerenciamento e controle de fluxo.

O projeto será desenvolvido com foco em *Virtual LAN’s*, suas definições e configurações. Será focado com o modelo RM-OSI dando ênfase ao funcionamento da camada de enlace de dados e rede.

Assim, serão aperfeiçoados conhecimentos na área de Redes de Computadores e suas configurações. O fator motivador foi a observação do cenário atual das comunicações e o interesse pessoal em aprimorar conhecimentos na referida área.

2. OBJETIVOS

Neste item, serão explanados os objetivos deste trabalho.

2.1. Geral

Ampliar conhecimentos em Virtual LANs apresentando algumas soluções que visam um melhor aproveitamento dos ativos de rede, estruturando e preparando a rede local para lidar com possíveis falhas, reduzindo seu tempo de indisponibilidade e, em alguns casos inibindo a mesma de falhas, principalmente propiciando um ambiente seguro para todos os que estão conectados na mesma.

2.2. Específicos

Serão listados os objetivos específicos do projeto:

- Compreender o funcionamento e atuação de um modelo de rede em camadas;
- Assimilar as grandes vantagens na implementação de uma VLAN;
- Elaborar uma proposta de melhoria na estrutura da rede;
- Realizar um método de averiguar o desempenho da rede;

3. REVISÃO BIBLIOGRÁFICA

Para o desenvolvimento deste trabalho, foram utilizadas várias tecnologias. Este item fará uma breve introdução sobre cada uma destas tecnologias.

3.1. O Modelo RM-OSI

Cada um dos três séculos passados foi dominado por uma única tecnologia. O século XVIII foi a era dos grandes sistemas mecânicos acompanhando a Revolução Industrial. No século XIX foi marcado pelas máquinas a vapor. Durante o século XX, a tecnologia chave foi a coleta, processamento e distribuição da informação. Entre outros desenvolvimentos, presenciou-se a instalação de uma linha mundial de telefones, a invenção do rádio e televisão, o nascimento e o crescimento sem precedentes da indústria de computadores, o lançamento de satélites de comunicação e é claro, a Internet (TANENBAUM; WETHERALL, 2011). Isso resultou um dos maiores avanços na área de tecnologia. Atualmente, é indispensável que uma organização tenha meios de comunicação tanto internos quanto externos.

Soares, Souza e Colcher (1995) explicam que quando as redes de computadores surgiram, as soluções eram na maioria das vezes proprietárias, isto é, uma determinada tecnologia era suportada somente pelo próprio fabricante. Não existia a possibilidade de mesclar soluções entre fabricantes diferentes. Assim, um mesmo fabricante acabava sendo responsável pela construção da maior parte da rede. Consequentemente, foram criados padrões buscando solucionar problemas de incompatibilidades entre os dispositivos. Especificado no próprio site da *International Organization For Standardization* (2016), a ISO (*International Standards Organization*) é uma organização internacional fundada em 1946 que tem por objetivo a elaboração de padrões internacionais a fim de facilitar a coordenação e unificar os padrões industriais. Os membros da ISO são órgãos de padronização internacional. Por exemplo, o representante do Brasil é a ABNT (Associação Brasileira de Normas Técnicas) e o representante dos Estados Unidos é a ANSI (*American National Standards Institute* - Instituto Nacional Americano de Padronização).

Segundo Soares, Souza e Colcher (1995), a ISO é organizada em Comitês Técnicos (*Technical Committees* – TC's) que tratam de assuntos específicos. O TC97 trata da padronização de sistemas de processamento de informações.

Rosario (2009) cita que, em 1997, a ISO desenvolveu um modelo de referência para interconexão aberta em um sentido mais universal intitulado *Open Systems Interconnection* (OSI), para que os fabricantes pudessem criar protocolos a partir desse modelo.

Tanenbaum e Wetherall (2011) definem que este modelo é chamado assim porque trata-se de conectar sistemas abertos, ou seja, sistemas que são abertos para comunicação com outros sistemas.

De acordo com o documento da ISO (ISO 84, ISO 92), o objetivo do padrão internacional 7498 (OSI) é fornecer uma base comum que permita o desenvolvimento coordenado de padrões para interconexão de sistemas. Seguindo essa padronização, quebraram-se as barreiras envolvidas no processo de comunicação. Desta forma, foi possível a interoperabilidade entre os dispositivos de rede de fabricantes diferentes.

Para Torres (2007), o modelo OSI é extremamente didático, pois através dele a possibilidade de entender como deveria ser um protocolo ideal, além de facilitar a comparação do funcionamento de protocolos criados por diferentes fabricantes.

Torres (2007) ainda explica que a ideia básica do modelo é que cada camada do modelo de referência, é responsável por algum tipo de processamento e cada uma dessas camadas apenas se comunica com a camada imediatamente inferior ou superior. Por exemplo, não é possível comunicação entre a camada de enlace e a camada de transporte.

A **Erro! Fonte de referência não encontrada.** mostra as 7 camadas do modelo RM-OSI. É interessante notar que a ordem numérica das camadas é decrescente, ou seja, o processo começa na camada física, onde os sinais elétricos são convertidos em zeros e uns e termina na camada de aplicação, onde atuam protocolos como o FTP (*File Transfer Protocol*), que consiste no protocolo para troca de arquivos.

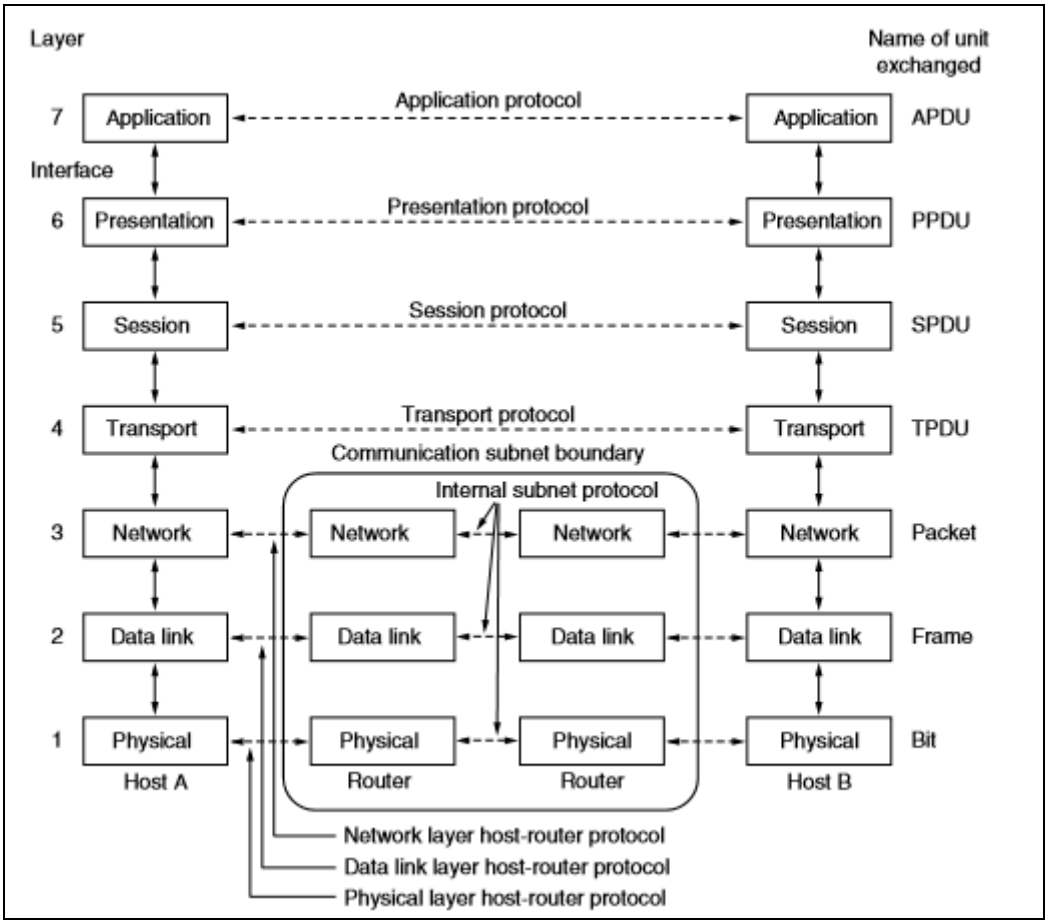

Figura 1 - Camadas do modelo RM-OSI

Tanenbaum e Wetherall (2011) afirmam que os princípios aplicados para chegar às sete camadas podem ser brevemente resumidos em:

1. Uma camada deve ser criada onde é necessário uma diferente abstração.
2. Cada camada deve realizar uma função bem definida.
3. A função de cada camada deve ser escolhida considerando a definição de protocolos internacionalmente padronizados.
4. As bordas da camada devem ser escolhidas visando minimizar o fluxo de informações através das interfaces.
5. A quantidade de camadas deve ser grande o suficiente para distinguir funções que não tem necessidade de funcionar na mesma camada e pequena o suficiente para que a arquitetura não se torne desajustada.

Tanenbaum e Wetherall (2011) explicam que a camada de nível físico consiste em transmitir dados brutos por um canal de comunicação. Os mesmos dados brutos podem ser transmitidos em fios através de variações de alguma propriedade física tais como tensão ou corrente. Ele afirma que o *design* foi projetado para garantir que quando um dispositivo envia 1 *bit* e isso é recebido por outro dispositivo como 1 *bit* e não como 0.

Strata (2016) define que o processo de transmissão de dados através das camadas é chamado de encapsulamento ou empacotamento. O empacotamento é o processo de criação de pacotes IP. O processo de criação desses pacotes inicia na camada de aplicação do modelo OSI e continua através da camada física. Por exemplo, quando você transfere um arquivo de um computador para outro, este arquivo sofre uma transformação de um arquivo completo para vários pequenos pedaços de informação (pacotes).

Durante a transmissão de um dado, cada uma das camadas recupera as informações passadas pela camada superior, acrescenta informações pelas quais ela seja responsável e então, passa os dados para a camada imediatamente inferior. Essa transmissão é iniciada na camada 1 (física), onde o sinal vindo da rede elétrica é convertido em *bits* (0 e 1). A camada física identifica como 0, o sinal elétrico com -5 *volts* e como 1 o sinal elétrico com +5 *volts*.

Soares (1995) define que o nível físico fornece as características mecânicas, elétricas, funcionais e de procedimento, que têm o objetivo de ativar, manter e desativar conexões físicas para a transmissão de bits entre as entidades do nível de enlace. Simplificando, a camada física trata de aspectos como: comprimento máximo dos cabos, conectores físicos, pulsos elétricos, entre outros. Alguns dos dispositivos que atuam na camada física são os hubs, cabos e conectores.

Para Tanenbaum e Wetherall (2011), a camada de enlace de dados utiliza os serviços da camada física para enviar e receber bits pelos canais de comunicação. Além disso, o autor inclui:

- Oferecer uma interface de serviço bem definida para a camada de redes.
- Tratar possíveis erros de transmissão.

- Regulação do fluxo de dados, de modo que os receptores mais lentos não tenham problema com os remetentes mais rápidos.

Tiwari (2013) diz que esta camada define as formas de acesso ao ambiente de transmissão de dados através de mais equipamentos e estabelece o modo de transferência de dados entre as camadas superiores e o modelo físico.

Após a camada física ter formatado os dados, a camada de enlace de dados atua, recebendo os *bits* provindos da camada física, e transformando em unidade de dado, subtraindo o endereço físico e em seguida encaminhando-o para a camada de rede. Ou seja, a função da camada de enlace de dados é oferecer serviços para a camada de rede. O principal serviço é transferir dados da camada de rede na máquina que gerou os dados para a camada de rede na máquina que será o destino desses dados (TANENBAUM; WETHERALL, 2011).

Para Pinheiro (2008), a camada de rede é responsável pelo gerenciamento do transporte das informações entre uma rede composta de múltiplos segmentos. A camada proporciona o encaminhamento e o endereçamento da informação, tanto na origem quanto no destinatário da transmissão. Para ele, esta camada tem como função favorecer uma trajetória de conexão de rede entre um par de entidades da camada de transportes, inclusive passando por nós intermediários.

A camada de rede não garante que um pacote chegue a seu destino, pacotes podem ser perdidos ou mesmo chegar fora da seqüência original de transmissão. Para fornecer uma comunicação verdadeiramente confiável, é necessário outro nível de protocolo, denominado transporte.

Torres (2007) afirma que a camada de transporte faz um controle do fluxo de dados (coloca os pacotes recebidos em ordem, caso não estejam), faz a correção de erros e envia um dado com a informação que o pacote foi recebido.

Tanenbaum e Wetherall (2011) diz que o objetivo final da camada de transporte é proporcionar um eficiente, confiável e ter um bom custo-benefício do serviço de transmissão de dados para seus usuários.

Segundo Torres (2007), define a responsabilidade da camada de transporte com um exemplo. “Nas redes de computadores, os dados são divididos em vários pacotes. Quando você está transferindo um arquivo grande, este arquivo é dividido em vários pequenos pacotes. No computador receptor, esses pacotes são organizados para formar o arquivo originalmente transmitido. A camada de

transporte é responsável por pegar os dados enviados pela camada de sessão e dividi-los em pacotes que serão transmitidos pela rede. No computador receptor, a camada de transporte é responsável por pegar os pacotes recebidos da camada de rede e remontar o dado original para envia-lo a camada de sessão."

Pinheiro (2008) diz que a camada de sessão fornece uma estrutura de controle para a comunicação entre aplicações. Ele também cita que esta camada executa os serviços de administração da sessão e diálogo de sessão, controlando a troca de dados, delimitando e sincronizando operações entre duas entidades.

Segundo Silva (1993), esta camada trata da coordenação e sincronização do diálogo entre entidades comunicantes. Controla o sentido permitido de comunicação, permite a definição de pontos de sincronização no diálogo (para restabelecimento da comunicação em caso de falhas) e também, a divisão da transmissão em partes logicamente distintas.

Depois de transmitidos, os dados precisam ser legíveis para o receptor. Tanenbaum e Wetherall (2011) dizem que diferente das outras camadas que eram em maioria preocupadas com a movimentação de *bits*, a camada de apresentação se preocupa com a sintaxe e semântica da informação transmitida.

Para Pinheiro (2008), a camada de apresentação realiza a conversão do formato de dados de forma que eles sejam compreendidos por todos os sistemas que estejam envolvidos na comunicação. O autor ainda cita que esta camada tem a função de fazer a compressão/descompressão, criptografia/descriptografia, resolve problemas de diferença de sintaxe entre sistemas abertos.

Torres (2007) explica que a camada de aplicação faz a interface entre o programa que está enviando ou recebendo dados e a pilha de protocolos. Ele exemplifica que quando um usuário está fazendo o download dos seus emails, o software utilizado pelo usuário entra em contato com esta camada.

Para Tanenbaum e Wetherall (2011), essa camada contém uma variedade de protocolos geralmente requeridos pelos usuários. Um dos protocolos em questão é o HTTP (*HyperText Transfer Protocol),* qual é a base para a Internet.

Zimmermann (1980) define que esta é a camada mais elevada nesta arquitetura de modelo. Protocolos dessa camada devem servir diretamente o usuário final, fornecendo o serviço de informação apropriado a uma aplicação, a sua gestão e a gestão do sistema.

As camadas da extremidade do modelo (física e aplicação) podem tanto iniciar quanto finalizar um processo de comunicação.

A Tabela 1 abaixo demonstra um resumo das funções de cada uma das camadas do modelo OSI.

Tabela 1 - Camadas do modelo OSI

Camada	Funções
Aplicação	• **Disponibiliza serviços de rede para processos aplicativos.**
Apresentação	• **"Tradução" dos dados.**
Sessão	• **Iniciar, gerenciar e terminar a conexão.**
Transporte	• **Garantir o envio e recebimento dos dados.**
Rede	• **Roteamento (traçar a melhor rota);** • **Multiplexação da conexão de rede;** • **Endereçamento e tráfego dos pacotes.**
Enlace	• **Montagem e delimitação dos quadros;** • **Controle de fluxo, acesso, erro e seqüência;** • **Gerenciamento da qualidade do serviço.**
Física	• **Estabelecimento e encerramento de conexões;** • **Transferência de dados;** • **Gerenciamento das conexões.**

Deve ser ressaltado que o RM-OSI, por si só, não define a arquitetura de uma rede, pois ele não especifica com exatidão os serviços e protocolos de cada camada.

3.2. Camada De Enlace De Dados

Tanenbaum e Wetherall (2011) afirmam que o principal objetivo da camada de enlace de dados é transformar a habilidade de transmissão bruta em uma linha que aparece livre de erros de transmissão indetectáveis.

De acordo com Soares (1995), o objetivo da camada de enlace é detectar e opcionalmente corrigir os erros que por ventura ocorram na camada física. O nível

de enlace vai converter um canal de transmissão não confiável em um canal confiável para uso da camada de rede. A técnica utilizada é a partição da cadeia de bits enviados pelo nível físico em quadros, cada um contendo alguma forma de redundância para detecção de erros.

Carthern et al. (2015) diz que esta camada deve garantir que as mensagens serão transmitidas para os dispositivos em uma LAN usando endereços físicos de hardware e, também deve converter pacotes enviados a partir da camada de rede e então, transformá-los em quadros (*frames)* para serem enviados para a camada física para transmissão. O autor cita que depois de converter os pacotes em quadros, a camada adiciona um cabeçalho que contém um dispositivo de hardware físico da fonte e do endereço de destino, controle do fluxo e um *footer* com os dados do CRC (*Cyclic Redundancy Check* – verificação de redundância cíclica).

Quando o receptor recebe um quadro, a sua camada de enlace confere se o dado chegou íntegro, refazendo o CRC. Se os dados estiverem completos, ele envia uma confirmação de recebimento (chamada *acknowledge* ou simplesmente ack). Caso essa confirmação não seja recebida, a camada do transmissor reenvia o quadro, já que ele não chegou até o receptor ou então chegou com os dados corrompidos (Torres, 2007). Para Carmona e Hexsel (2005), esse é um dos serviços mais importantes da camada de enlace, pois propicia às camadas superiores o transporte confiável dos dados entre as duas portas do enlace.

Em resumo, Tanenbaum (2003) afirma que a camada de enlace tem o objetivo de prover uma conexão confiável sobre um meio físico. As suas principais funções são:

- Estabelecimento e liberação da conexão de enlace sobre conexões físicas ativas;
- Montagem e delimitação de quadros;
- Controle da taxa de transmissão dos quadros, evitando que o sistema transmissor envie dados a uma taxa maior do que o receptor consegue processar;
- Controle de acesso: gerência do acesso ao meio de transmissão;
- Controle de erro: a camada de enlace deve detectar erros de transmissão, de formato e de operação devidos a problemas de conexão física ou mau funcionamento da própria camada. Os erros

mais comumente detectados são erros devido a perdas, duplicação, não-ordenação e danificação de quadros.

- Controle de sequência: as unidades de dados de serviço de enlace devem ser entregues à entidade de rede de destino na mesma ordem em que são recebidas da entidade de rede de origem;
- Gerenciamento: a camada de enlace deve exercer algumas funções de gerenciamento relacionadas à qualidade de serviço prestado;

Carthern et al. (2015) cita que essa camada tem a função de garantir o controle do fluxo de dados entre transmissor e receptor. Ele afirma que o controle de fluxo é necessário pois o transmissor e o receptor podem ter diferentes capacidades de velocidade.

Carmona e Hexsel (2005) descrevem a camada de enlace de dados dividida em dois subníveis:

- ***Logical Link Control*** **(LLC)** ou subnível superior;
- ***Media Access Control*** **(MAC)** ou subnível inferior;

Essa divisão permite o uso de diferentes métodos de controle de acesso ao meio, cada qual adequado às características particulares do meio físico.

3.2.1. Controle Lógico Do Enlace (LLC)

Segundo Carmona e Hexsel (2005), este subnível permite a diferenciação entre as mensagens de controle e as mensagens que transportam dados, garantindo que uma única cópia correta de cada quadro seja enviada ao nível de rede.

Esta subcamada (IEEE 802.2) também estabelece e mantém a comunicação com outros dispositivos e fornece conectividade com servidores quando os dados são transferidos. O LLC gerencia o controle do link e define os *service access points* (SAPs).

Tanenbaum e Wetherall (2011) comentam que o LLC tem como objetivo esconder as diferenças entre os diferentes variantes IEEE 802 e torná-los mais indistinguíveis tanto quanto a camada tem por objetivo. Eles também citam que isso pode ter sido uma responsabilidade significativa, porém atualmente o LLC é somente uma camada de “cola”, qual identifica o protocolo (por exemplo, IP) que é realizada dentro de um quadro 802.11.

Pinheiro (2008) afirma que o LLC é utilizado quando é necessário controle de fluxo ou comunicação confiável.

3.2.2. Controle De Acesso Ao Meio (MAC)

Carmona e Hexsel (2005) mostram que esse subnível decide o momento em que cada estação tem direito a transmitir seus quadros. Essa decisão é baseada no princípio de equidade no acesso ao meio físico, procurando garantir que todas as estações apareçam na transmissão e impedindo que uma delas monopolize a utilização do meio físico em detrimento das demais.

A subcamada MAC mantém uma tabela dos endereços físicos dos dispositivos. Cada dispositivo será atribuído e deverá ter um endereço MAC exclusivo se o dispositivo for participar na rede.

Essa subcamada possui alguns protocolos importantes, como o IEEE 802.3 (*Ethernet*), IEEE 802.4 (*Token Bus*) e IEEE 802.5 (*Token Ring*). O protocolo de nível superior pode usar ou não o subnível LLC, dependendo da confiabilidade esperada para esse nível.

Os protocolos usados nessa camada incluem o *High Level Data Link Control* (HDLC) para conexões da WAN, incluindo transmissões síncronas e assíncronas. O protocolo LLC (IEEE 802.2) oferece um controle de fluxo nessa camada.

As tecnologias que operam nessa camada incluem mais de 18 variedades de Ethernet (especificadas no IEEE 802.3 e em outros padrões), Token Ring (IEEE 802.5) e outras tecnologias LAN que dependem dos quadros. As comunicações com a placa de rede também são fornecidas.

Os dispositivos que funcionam nessa camada incluem placas de rede, bridges e switches. Embora os roteadores estejam classificados como dispositivos da camada 3, a fim de executar suas funções, eles devem operar também nas camadas 1 e 2.

Torres (2001) cita uma importante função “O controle de acesso ao meio (MAC) define, entre outras coisas, o uso de um endereço MAC em cada placa de rede”.

3.3. Domínios De Colisão

Segundo Peicevic (2016), o domínio de colisão é, assim como o nome implica, a parte da rede onde a colisão de pacotes ocorre. A colisão acontece quando dois dispositivos enviam um pacote ao mesmo tempo no segmento de rede compartilhada. Os pacotes colidem e ambos os dispositivos devem enviar os pacotes novamente, o que reduz a eficiência da rede.

Bonaventure (2011) cita que transmissões simultâneas são chamadas de colisões. Ele também explica que uma colisão pode envolver quadros transmitidos por dois ou mais dispositivos conectados à rede local. As colisões são a principal causa de erros em redes locais com fio (quais pode-se citar, redes com hubs).

O uso de hubs em uma rede Ethernet pode definir um domínio de colisão, já que as máquinas “competem” entre si para o envio de seus pacotes e o hub não tem meios de filtragem ou controle do tráfego. Portanto, não importa se uma rede tem um ou dez hubs, ela será um único domínio de colisão.

Os problemas inerentes às colisões aumentam exponencialmente à medida que a rede cresce e com isso seu desempenho é seriamente afetado. Logo, eliminar a ocorrência de colisões ou reduzir o tamanho dos domínios de colisão seria muito benéfico para uma rede.

A **Erro! Fonte de referência não encontrada.** a seguir demonstra uma rede simples, com 4 *hosts* e um *hub* para interligá-los.

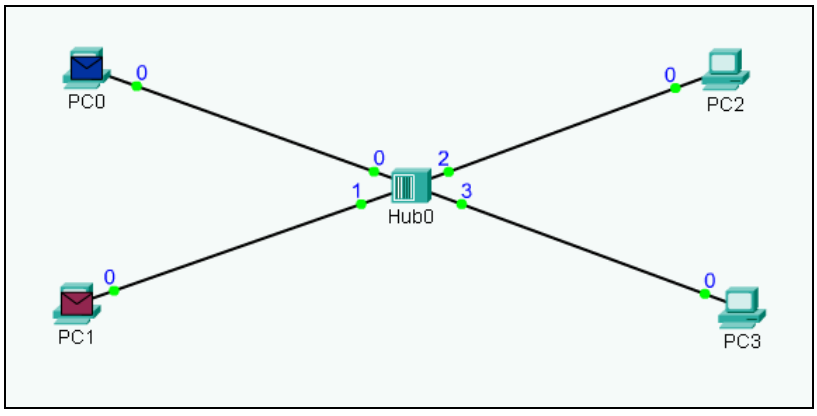

Figura 2 - Rede simples, utilizando hub para conexão

Ao tentar transmitir um pacote do *host* 0 para o *host* 3 e outro pacote do *host* 1 para o *host* 4 ocorre uma colisão entre os pacotes, fazendo com que nenhum

dos *hosts* receba o pacote corretamente, como mostram as **Erro! Fonte de referência não encontrada.** e **Erro! Fonte de referência não encontrada.** a seguir.

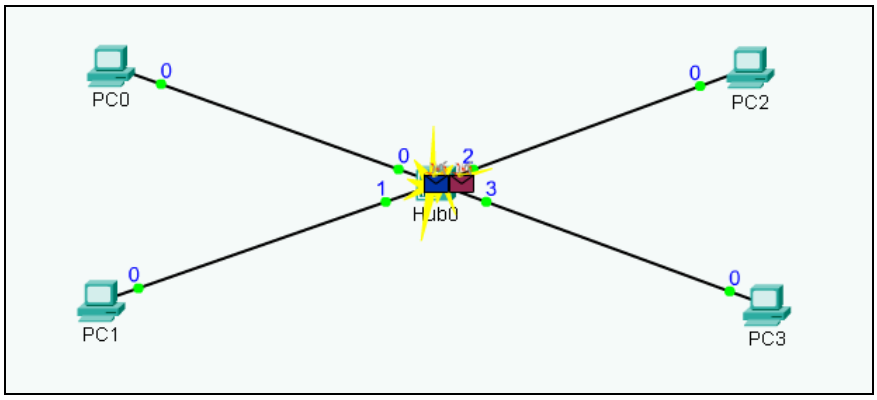

Figura 3 - Colisão de pacotes

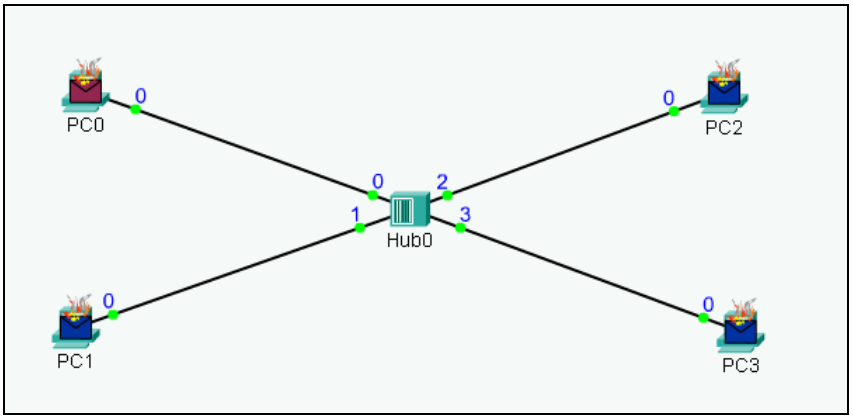

Figura 4 - Hosts recebendo o pacote com problemas

O problema dessa rede poderia ser resolvido com a utilização de um *switch*, que, assim como o *hub*, também atua na camada de enlace do modelo OSI. Isso se deve ao fato do *switch* possuir um maior número de portas e lógica mais otimizada no que diz respeito à filtragem e comutação dos quadros.

Tanenbaum e Wetherall (2011) explicam que o trabalho do *switch* é retransmitir pacotes entre computadores que estão ligados a ele usando o endereço de cada pacote para determinar qual computador se comunicará com qual.

Pode-se concluir que a vantagem do *switch* é que ele faz uma comutação virtual entre as máquinas de origem e destino, isolando as demais portas deste processo. Além de eliminar a colisão entre suas portas, o switch aumenta o número

de domínios de colisão, tornando a rede mais rápida em relação a uma rede que utiliza hubs, como visto no exemplo anterior.

As **Erro! Fonte de referência não encontrada.** e **Erro! Fonte de referência não encontrada.** abaixo apresentam a mesma rede anterior, porém com um switch no lugar do hub.

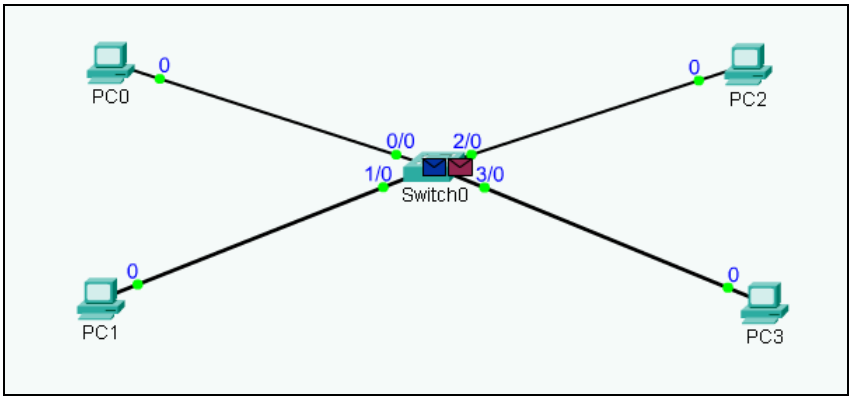

Figura 5 - Rede utilizando switch

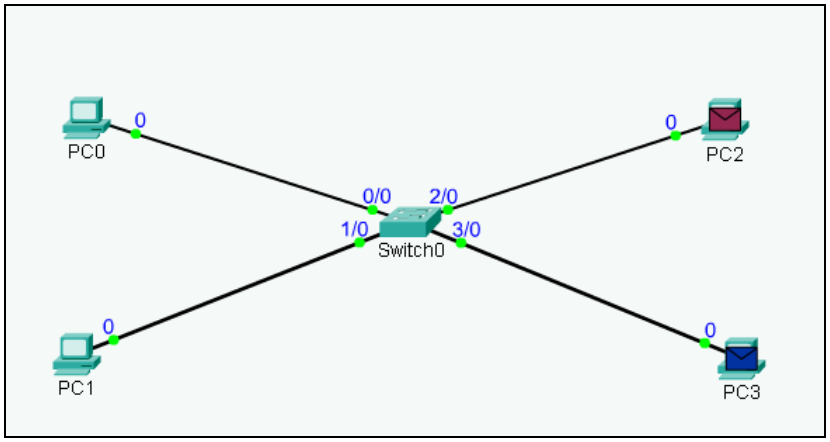

Figura 6 - Pacotes entregues ao destinatário correto

Como se pode observar, os pacotes foram gerenciados pelo switch e entregues apenas ao seu destinatário correto, ao contrário do hub, que, além de não ter evitado a colisão entre os pacotes, os enviou a todos os hosts da rede.

Tanenbaum e Wetherall (2011) explicam que a colisão de pacotes não ocorre neste dispositivo, pois diferentemente de um *hub*, o *switch* tem cada uma das portas isoladas para serem seus próprios domínios de colisão. O autor ainda afirma que quando um *switch* recebe um quadro, é realizada uma extração do endereço de destino do cabeçalho desse quadro e visualiza através de uma tabela, onde este frame deve ser enviado.

3.4. Broadcast E Seus Limites

Tanenbaum e Wetherall (2011) citam que em algumas aplicações, *hosts* necessitam enviar dados para alguns ou todos os outros *hosts*. Por exemplo, um serviço distribuindo informações sobre o tempo ou um programa de rádio ao vivo podem trabalhar melhor enviando para todas as máquinas e deixando aqueles que estão interessados, lerem os dados. Os autores definem como *broadcasting* o envio de pacotes para todos os destinos simultaneamente.

Quanto maior o tamanho da rede segmentada apenas por *switches*, maior será o tráfego de *broadcasts* (normalmente utilizados em informações de controle de servidores ou de estações que “se anunciam”). Eventualmente, esse tráfego de *broadcasts* poderá ser tão intenso, que eles poderão estar competindo com pacotes de dados pela banda passante, afetando a performance da rede. Além disso, por questões de segurança, poderá ser desejável que se contenha a expansão de quadros *broadcast* pelo ambiente da rede.

CiscoPress (2016) cita que VLANs permitem que os administradores de rede segmentem logicamente uma LAN em diferentes domínios de *broadcast*. Por se tratar de uma segmentação lógica e não física, diferentemente dos roteadores que fazem uma segmentação física, as estações não precisam estar fisicamente no mesmo local e nem mesmo conectadas ao mesmo switch. Usuários de diferentes andares de um prédio, ou mesmo de diferentes prédios, podem pertencer a uma mesma LAN.

Segundo a Cisco (2016), sempre que os *hosts* de uma VLAN precisam se comunicar com *hosts* de outra VLAN, será necessário rotear o tráfego entre eles.

Com a utilização de VLANs, é possível agrupar portas de tal maneira que um *broadcast* vindo de uma porta na VLAN1 só circule nas outras portas da mesma VLAN e não em portas pertencentes a outras VLANs.

A **Erro! Fonte de referência não encontrada.** demonstra uma pequena rede com dois domínios de *broadcast* separados por um roteador. Cada domínio do *broadcast* pode ser chamado também de VLAN.

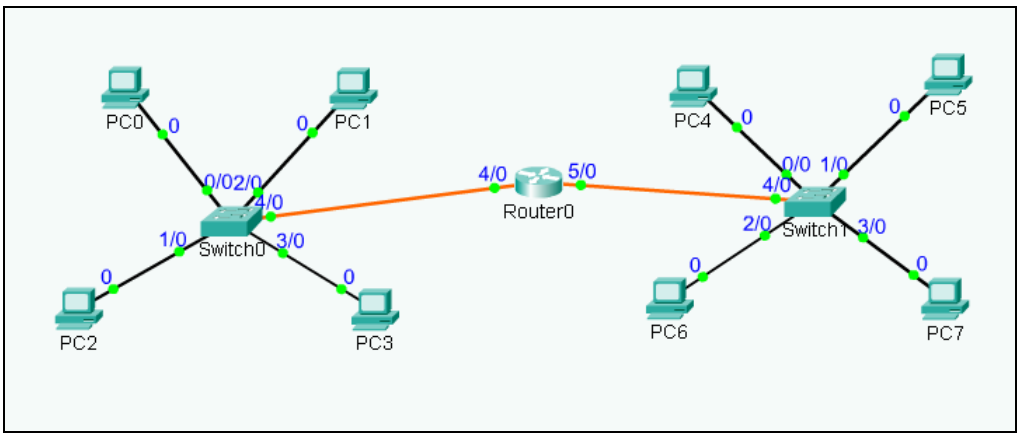

Figura 7 - Domínios de broadcast

3.5. Operação Dos Switches

Um *switch* é um dos dispositivos que possibilita a conexão de vários computadores em rede. Atua na camada de enlace do modelo OSI, logicamente semelhante a uma *bridge*.

Segundo a Cisco Press (2014), *switches* são usados para conectar múltiplos dispositivos na mesma rede. Em uma rede corretamente projetada, eles são responsáveis por direcionar e controlar o fluxo de dados na camada de acesso para os recursos da rede.

A **Erro! Fonte de referência não encontrada.** abaixo demonstra um modelo de switch de 48 portas Gigas.

Figura 8 - Modelo de Switch Catalyst

Carmona e Hexsel (2005) afirmam que o dispositivo não deve sofrer trepidações durante o funcionamento, sob risco de queda de desempenho. O ideal é que seja utilizada uma prateleira (*patch panels*) especial, onde se possa parafusar o *switch* para evitar trepidações.

O *switch*, assim como a prateleira sobre a qual estiver posicionado, não deve ter contato com paredes ou componentes eletrônicos. Este equipamento, bem como a maioria dos equipamentos eletrônicos, produz calor durante seu funcionamento, portanto, é importante que ele esteja posicionado em um local onde possa ocorrer a dissipação deste calor. O ideal é que sejam mantidos em ambientes com temperatura entre 16º e 18º C.

Os *switches* são mais eficientes que *hubs* em uma rede, pois enviam os dados vindos do computador de origem apenas para o computador de destino. Já o *hub* comum envia os dados para todos os computadores pertencentes à rede, fazendo com que o tráfego da rede seja muito intenso. Portanto, a utilização dos *switches* aumenta o desempenho da rede, diminuindo a ocorrência de erros na transmissão e colisões entre pacotes.

Um *switch* funciona como um nó central de uma rede. Sua função consiste no chaveamento (ou comutação) entre as estações que desejam se comunicar.

Na figura 9 é possível verificar redes interconectadas com um *switch*.

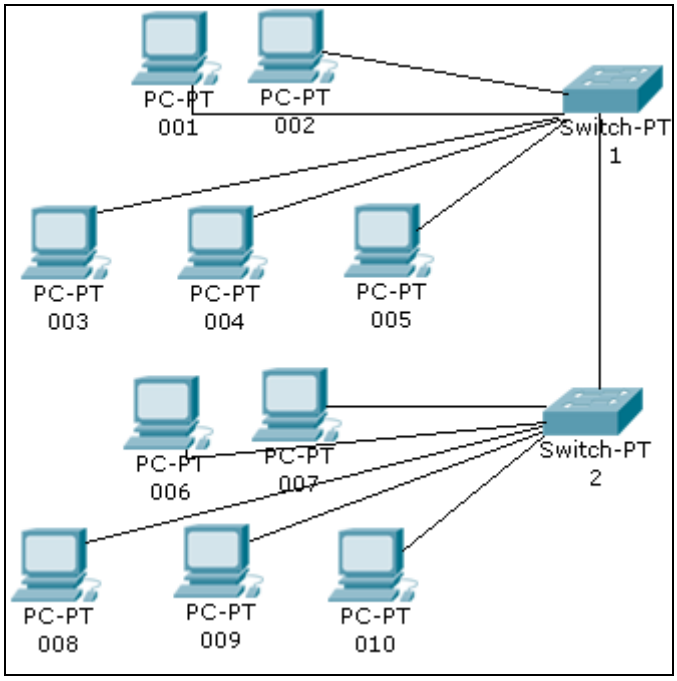

Figura 9 - Redes interligadas por meio de um switch

A partir do momento em que as estações estão ligadas a esse elemento central, há a possibilidade de troca de mensagens entre várias estações

simultaneamente. Dessa forma, as estações podem obter para si taxas efetivas de transmissão bem maiores.

O *switch* possui uma tabela de encaminhamento chamada de tabela CAM (*Content-Addressable Memory*) que contém a associação das máquinas a cada porta do *switch*. Quando uma informação é enviada para uma máquina que não há em sua tabela, o *switch* envia o pacote para todas as máquinas, com exceção da máquina de origem. A partir do momento que essa máquina “responde”, ele armazena em qual porta ela está conectada e passa a se comunicar com ela exclusivamente por meio daquela porta.

Vejamos um exemplo passo a passo de como isso funciona.

Temos um switch de 8 portas em que estão conectadas as máquinas segundo ilustrado na Tabela 2 a seguir:

Tabela 2 - Exemplo de Tabela CAM

Máquinas	MAC	Porta
João	0001	1
Maria	0002	2
Pedro	0003	3
Ronaldo	0004	4
Márcia	0005	5
Paulo	0006	6
Vânia	0007	7
Valério	**0008**	**8**

Quando o switch é inicializado, a tabela CAM está vazia. Então João manda um pacote para Márcia e, neste pacote, constam as informações mostradas na Figura 10:

MAC Origem	*MAC Destino*
0001	0006

Figura 10 - Tabela CAM

O switch envia o pacote para todas as portas (broadcast), já que acabou de ser inicializado e coloca o remetente em sua tabela demonstrado na Figura 11:

MAC	*Porta*
0001	1

Figura 11 - Busca na tabela CAM

Todas as máquinas que não possuem o endereço destino descartam o pacote. Assim, como na Figura 12, Márcia responde:

MAC Origem	*MAC Destino*
0006	0001

Figura 12 - Resposta para o switch

O *switch* encaminha o quadro para a porta 1 (conforme consta em sua tabela) e adiciona as informações de Márcia em sua tabela, conforme a Figura 13.

MAC	*Porta*
0001	1
0006	6

Figura 13 - Tabela CAM completa

Quando João e Márcia precisarem se comunicar novamente, o *switch* não mais enviará o pacote para todas as portas, e sim, somente entre as portas de que eles fazem parte.

3.5.1. Métodos De Encaminhamento

Os métodos de encaminhamento (ou *switching*) fazem parte da lógica dos *switches*, eles contribuem para que o *switch* tenha uma alta taxa de encaminhamento de quadros.

Quanto ao método utilizado pelo *switch* no encaminhamento dos pacotes, podemos ter:

- ***Store-and-forward*** – o *switch* aceita e analisa o pacote inteiro antes de encaminhá-lo para a porta de saída verificando sua integridade. Este método permite que sejam detectados alguns erros, evitando assim sua propagação pela rede;
- ***Cut-through*** – neste método, o *switch* apenas lê os 6 primeiros bytes de dados do pacote e o encaminha. É mais rápido, porém transmite muitos pacotes com erros causados por colisões. É utilizado em redes pequenas.
- ***Adaptative cut-through*** – adaptam-se, transmitindo tanto no modo *store-and-forward* quanto no *cut-through*.

É importante salientar que um switch não bloqueia quadros de broadcast, isso somente será feito por meio de redes locais virtuais (VLAN).

3.6. Redes Virtuais

Muitos são os investimentos em infraestrutura de redes nas grandes organizações empresariais, onde os mesmos vão desde ativos de rede como roteadores e *switches* a dispositivos de rede como computadores e telefones IP. Porém, todo este investimento muitas vezes pode não ser aproveitado totalmente devido à falta de tempo, organização ou conhecimento do administrador de rede.

Muitas vezes nos deparamos com pessoas adquirindo equipamentos pessoais com extremo poder de processamento e funções diversas para a realização de tarefas rotineiras, onde as mesmas acabam não utilizando boa parte dos recursos oferecidos por tal equipamento, assim, subutilizando todos os recursos disponíveis gerando alto custo para a organização em troca de resultados abaixo do esperado.

3.6.1. Modelo Hierárquico

O modelo hierárquico consiste basicamente na divisão de uma rede em camadas, onde cada camada tem suas funções atribuídas para o bom funcionamento da rede. Com essa divisão será possível (CISCO PRESS, 2002):

- Um maior controle onde pode-se definir a quais equipamentos e dispositivos os ativos de cada camada podem se conectar e o que cada um deve processar;
- Problemas podem ser resolvidos mais rapidamente;
- A rede como um todo fica mais organizada, a medida em que a mesma necessita crescer sua escalabilidade se torna fácil;
- A redundância é maior devido as inúmeras alternativas de rotas que um dado pode trafegar assegurando maior estabilidade e um maior desempenho, onde o dado pode passar pelo caminho menos congestionado pelo tráfego da rede;

As camadas utilizadas em um modelo hierárquico são: acesso, distribuição e núcleo. A topologia de uma rede hierárquica deve ser muito bem projetada, objetivando conseguir o melhor desempenho possível em todas as camadas.

Um dos fatores que devem ser levados em consideração é o diâmetro da rede, em que deve-se analisar qual o número máximo de dispositivos que um dado pode passar antes de chegar ao seu destino e para evitar ao máximo a latência, esse número deverá ser o menor possível.

3.6.2. Camada De Acesso

A camada de acesso é a responsável por conectar dispositivos finais a rede, como por exemplo, computadores, impressoras, telefones IP, tablets, enfim, dispositivos que podem ter acesso ao restante da rede.

Os equipamentos que fazem parte da camada de acesso basicamente são: *switches*, *bridges*, *hubs*, pontos de rede sem fio (*Access Point*), neste caso equipamentos de rede que proporcionam conectividade aos dispositivos finais da rede, controlando as permissões e gerenciando quais podem ter acesso a rede (CISCO PRESS, 2002).

3.6.3. Camada De Distribuição

Esta camada é responsável pelo recebimento e encaminhamento dos dados recebidos da camada de acesso, assim há o processamento desse dado o encaminhando diretamente para o seu destino controlando o fluxo do tráfego com base nas políticas pré definidas pelo administrador da rede

Nesta camada há o roteamento entre as redes locais virtuais (VLAN), em que por exemplo em uma organização um computador do setor de recursos humanos precisa enviar dados para o setor financeiro, ambos os equipamentos estão em sub-redes separadas, cada um em sua VLAN. A partir do momento que esses dados chegarem na camada de distribuição a mesma fará o roteamento desses dados verificando onde está o destino deste pacote e ao ter essa informação definida, o mesmo irá encaminhar esses dados para a sub-rede certa para que a mesma envie para seu destino (CISCO PRESS, 2002).

Nessa camada trabalham os switches que por sua vez precisam ter um bom desempenho e principalmente uma boa redundância, inibindo ao máximo a possibilidade de instabilidades ou lentidão na rede.

3.6.4. Camada De Núcleo

Esta camada é a responsável pela conexão entre as redes interconectadas da camada de distribuição e acesso a internet, resumidamente essa camada é a responsável pelo processamento e encaminhamento de uma enorme quantidade de dados enviados pela camada de distribuição, exigindo uma conexão com disponibilidade de acordo com as necessidades e uma indispensável redundância.

Lembrando novamente o exemplo citado anteriormente, se caso o computador do setor de recursos humanos não estiver no mesmo domínio de *broadcast* os dados irão ser encaminhados pela camada de núcleo até chegar ao seu destinatário que seria o computador do setor de recursos humanos, além de receber e encaminhar todo o tráfego proveniente da internet. Os ativos de rede pertencentes a essa camada são os *switches* e roteadores.

A topologia abaixo apresentada na Figura 14, é um modelo hierárquico de redes locais onde na camada de núcleo é apresentado dois switches representado o core da rede, quatro switches na camada de distribuição onde estará presente o

servidor VTP e por fim na camada de acesso seis switches estarão inserindo fluxo de dados na rede presente em cada VLAN (CISCO PRESS, 2002).

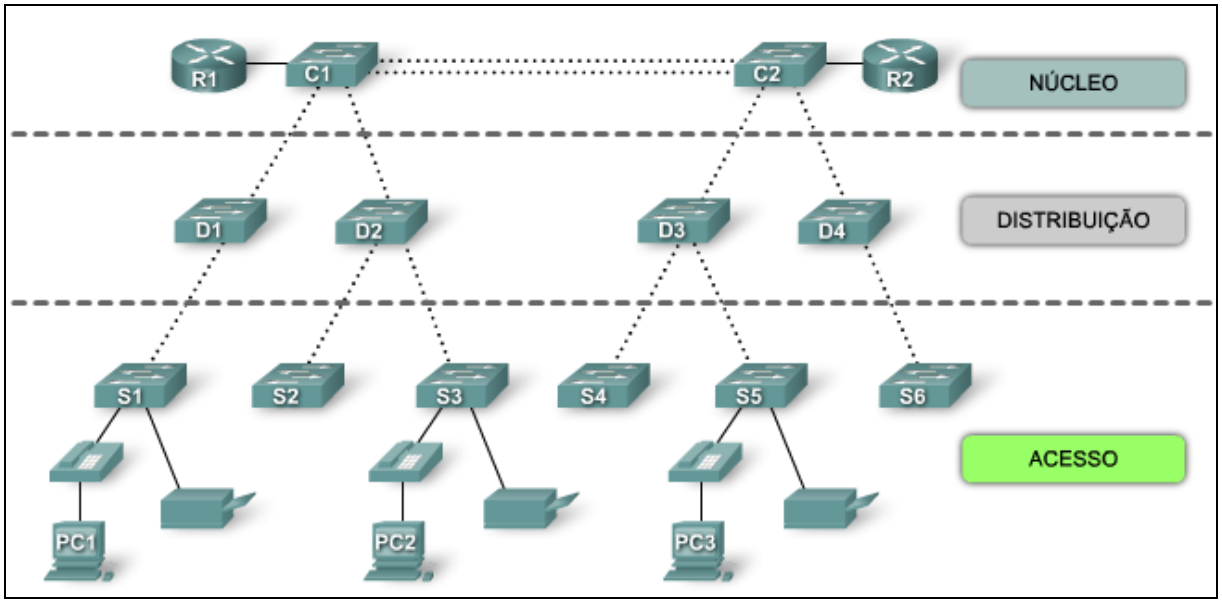

Figura 14 - Modelo Hierárquico de Rede

Fonte: Cisco Press (2002)

3.7. VLAN

Cisco Press (2014) cita que um fator de produtividade que pode se tornar um dos principais em instituições ou empresas, é o desempenho da rede.

Nem sempre uma determinada infraestrutura de uma rede local consegue suprir a demanda computacional de seus usuários. Se isso acontece, uma reestruturação lógica de redes de computadores faz-se necessária, visando aproveitar os recursos pré-existentes e melhorar as atividades gerenciais. Isso é possível por meio da criação de Virtual Local Area Network (VLAN), em outras palavras, a segmentação virtual de redes de computadores. O termo VLAN refere-se à criação de redes locais virtuais em um mesmo dispositivo de rede ou conjunto deles. As VLANs contribuem para reduzir os domínios de colisão em segmentos de redes Ethernet muito extensos, melhorando assim o seu desempenho (IEEE SOCIETY COMPUTER, 2006).

Mattos et al. (2016) acha que a virtualização de redes é fundamental para experimentação de novas arquiteturas para a Internet e também é uma possível solução pluralista para a Internet do futuro.

Para Pillou (2016), VLAN é uma rede local que agrupa conjuntos de máquinas de maneira lógica e não física. Assim, ela acaba se tornando mais flexível quando se trata de gestão da rede utilizando como base um conjunto de normas.

Redes locais podem ser definidas como sistemas de comunicação de dados limitados a uma área geográfica, possuindo altas taxas de transmissão, de acordo com a tecnologia utilizada. Para Gouveia e Magalhães. (2005), uma LAN serve para ligação de vários dispositivos em uma pequena área. Esta área pode ocupar um escritório, edifício ou até mesmo um campus universitário.

Entretanto, alternativamente, diz-se que uma LAN é "um único domínio broadcast". Ou seja, Fragouli, Widmer e Boudec (2008), se referem a isto como um problema de onde cada nó é uma fonte qual transmitirá dados para todos outros nós.

Os domínios de broadcast são tipicamente delimitados por roteadores, já que estes não encaminham quadros deste tipo. Cisco (2011) explica que isso ocorre pois é uma questão de segurança, qual evita um ataque DoS (*Denial of Service*).

As VLANs são uma solução alternativa ao uso de roteadores para conter o tráfego broadcast, já que elas segmentam as redes locais em diferentes domínios dessa natureza.

O termo VLAN (Virtual LAN) refere-se à criação de várias LANs virtuais em uma mesma rede. Dessa forma, pacotes só são recebidos pelos dispositivos pertencentes a uma determinada VLAN.

A Figura 15, demonstra um típico exemplo de VLAN’S.

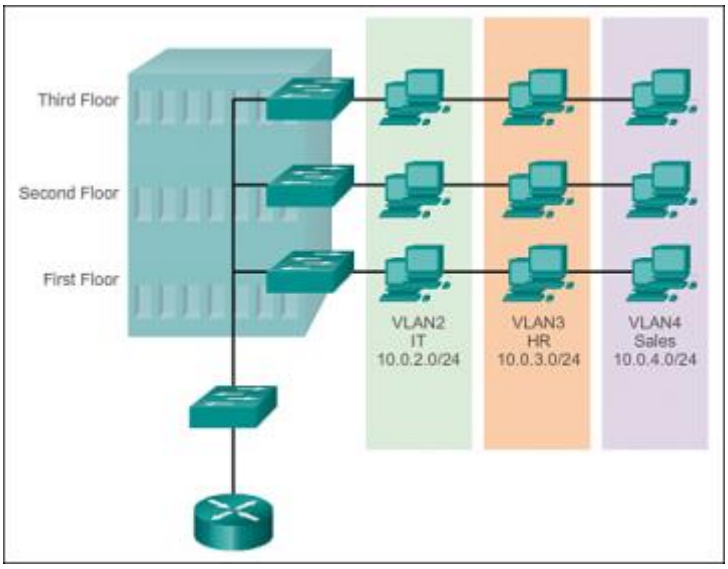

Figura 15 - Exemplo de VLAN'S

Fonte: Cisco (2011)

Como se pode perceber na figura anterior, as máquinas que pertencem a uma mesma VLAN não precisam necessariamente estar no mesmo ambiente.

As VLANs proporcionam uma alta flexibilidade a uma rede local. Isso é ideal para ambientes corporativos, onde a todo o momento ocorrem mudanças de empregados, reestruturações internas, aumento do número de usuários, entre outras situações.

As VLANs podem ser classificadas de acordo com sua base:

- VLANs baseadas em portas: os membros de uma VLAN podem ser definidos de acordo com a porta à qual estão conectados, conforme a Tabela 3 abaixo:

Tabela 3 - Exemplo de conexão dos membros de uma VLAN

Portas	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
VLAN	**0**	**0**	**0**	**1**	**2**	**2**	**2**	**0**	**1**	**1**

Fonte: Autoria Própria

3.7.1. Benefícios

Os benefícios proporcionados pela implantação de redes virtuais são inúmeros, dentre os quais pode-se citar (CISCO PRESS, 2014):

1- Controle do tráfego *broadcast*

As VLANs apresentam um desempenho superior às tradicionais redes locais, principalmente devido ao controle do tráfego *broadcast*.

Tempestades de quadros *broadcast* (*broadcast storms*) podem ser causadas por mau funcionamento de placas de interface de rede, conexões de cabos mal feitas e aplicações ou protocolos que geram esse tipo de tráfego, entre outros.

2- Segmentação lógica da rede

Como visto anteriormente, redes virtuais podem ser criadas com base na organização setorial de uma empresa. Cada VLAN pode ser associada a um departamento ou grupo de trabalho, mesmo que seus membros estejam fisicamente distantes. Isso proporciona uma segmentação lógica da rede.

3- Redução de custos e facilidade de gerenciamento

Grande parte do custo de uma rede se deve ao fato da inclusão e da movimentação de usuários dela. Cada vez que um usuário se movimenta é necessário um novo cabeamento, um novo endereçamento para estação de trabalho e uma nova configuração de repetidores e roteadores.

Já em uma VLAN, a adição e movimentação de usuários podem ser feitas remotamente pelo administrador da rede (da sua própria estação), sem a necessidade de modificações físicas, proporcionando uma alta flexibilidade.

4- Maior segurança

As redes locais virtuais limitam o tráfego a domínios específicos proporcionando mais segurança a estes.

O tráfego em uma VLAN não pode ser "escutado" por membros de outra rede virtual, já que estas não se comunicam sem que haja um dispositivo de rede desempenhando a função de roteador entre elas. Dessa forma, o acesso a servidores que não estejam na mesma VLAN é restrito, criando assim "domínios de segurança no acesso a recursos".

3.7.2. Função Trunk

A função trunk é utilizada para configurar portas e adicionar VLANs à lista permitida.

A capacidade do *trunking* depende do *hardware*. Alguns switches ajustam automaticamente as ligações das portas ao trunk. Para que uma porta se ajuste para se tornar uma porta trunk, dependerá da modalidade e do tipo do trunk especificado para essa porta.

Para que o trunk seja ajustado a portas rápidas é necessário que as portas estejam no mesmo domínio de VTP (*VLAN trunking protocol*).

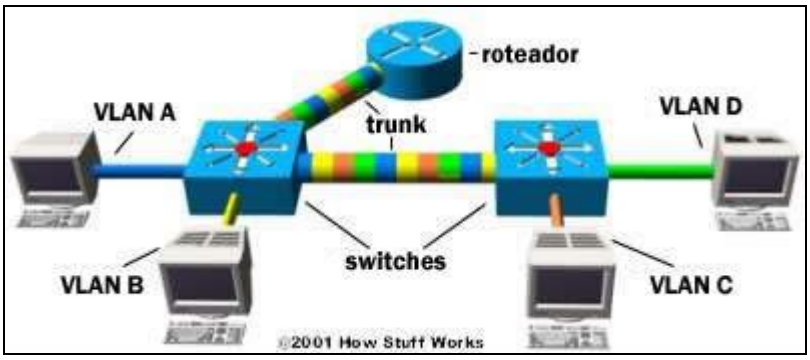

Figura 16 - Exemplo de trunk

Fonte: How Stuff Works (2001)

Na Figura 16 acima, é demonstrado um exemplo de trunk, onde as VLANs A e B enviam informações por uma mesma porta ao roteador e ao switch. O mesmo acontece com as VLANs C e D que utilizam trunking do segundo para o primeiro switch e do primeiro switch para o roteador.

As VLANs podem se comunicar entre si por meio da conexão trunking entre os dois switches utilizando o roteador. Por exemplo, dados do computador na VLAN A que precisam chegar a um computador na VLAN B (ou VLAN C ou VLAN D) devem trafegar do switch para o roteador e novamente para o switch. Devido ao aprendizado automático e ao trunking, as máquinas e o roteador entendem que eles estão no mesmo segmento físico.

3.7.3. VTP Domain

O protocolo VTP (*Vlan Trunking Protocol*) simplifica a configuração de uma VLAN em uma rede com vários switches garantindo um método mais fácil para a manutenção de uma configuração em toda a rede.

Segundo Véstias (2005), este protocolo faz a gestão de VLANs automaticamente, permitindo assim, que o administrador de rede consiga adicionar, remover e alterar a configuração de VLAN em qualquer switch desde que pertençam ao mesmo domínio e tenham ligação partilhada.

Tal protocolo é utilizado para distribuir e sincronizar informações de identificação das VLANs configuradas em toda a rede. As configurações estabelecidas em um único servidor VTP são propagadas através do enlace trunk para todos os switches conectados na rede.

Os anúncios VTP são transmitidos para todo o domínio de gerenciamento a cada 5 minutos ou sempre que ocorrer uma alteração nas configurações de VLANs.

O switch está no estado do *no-management-domain* até que seja configurado um *Domain Name*. Quando no estado de *no-management-domain*, o switch não emite nenhuma propagação de VTP mesmo se as mudanças ocorrerem à configuração local da VLAN.

A seguir, alguns modos de configuração de VTP:

- *Server*: é um switch utilizado para efetuar alterações à configuração da VLAN;
- *Client*: recebe as alterações de um servidor VTP. Não se pode alterar as configurações da VLAN neste modo de configuração;
- *Transparent*: Não recebe informação de configuração de outros switches. As alterações efetuadas neste modo apenas serão aplicadas no switch atual.

3.7.4. Roteamento Entre As VLANs

Quando duas máquinas participam de VLANs diferentes, mesmo que estejam conectadas ao mesmo comutador, elas não podem mais realizar uma entrega direta de pacotes entre elas. A razão é simples.

Antes, quando ambas as máquinas faziam parte da mesma VLAN, elas participavam do mesmo domínio de difusão. Assim, uma requisição ARP, que é um quadro de difusão, sempre atingia a outra máquina.

Mas, quando elas são separadas em VLANs distintas, uma requisição ARP de uma máquina não atinge mais a outra máquina, pois elas não mais compartilham o mesmo domínio de difusão. Sendo assim, para cruzar VLANs é necessário usar roteamento.

O próprio comutador pode fazer o roteamento de nível 3. Os chamados comutadores nível 3 ou *routers* incluem roteador embutido para os protocolos IP, IPv6 e IPX.

O fato de muitos comutadores serem capazes de realizar o roteamento em nível de rede não significa que se pode aposentar os roteadores. Eles ainda são muito utilizados por várias razões. Dentre elas, citamos:

- Aproveitar bons roteadores existentes;
- Roteadores são mais conhecidos pelos administradores de redes, facilitando a configuração e a operação dos mesmos;
- Roteadores possuem portas de rede de longa distância – comutadores nível 3 normalmente só possuem portas de rede local;
- Roteadores dão suporte a múltiplos protocolos de rede (IP, X25, IPX etc.) e de roteamento dinâmico (RIP I/II, OSPF, BGP etc.) – comutadores nível 3 normalmente somente dão suporte a poucos protocolos de rede (IP e IPX) e de roteamento dinâmico (RIP I/II e OSPF

A Figura 17 estará exemplificando um ambiente de roteamento entre VLANs:

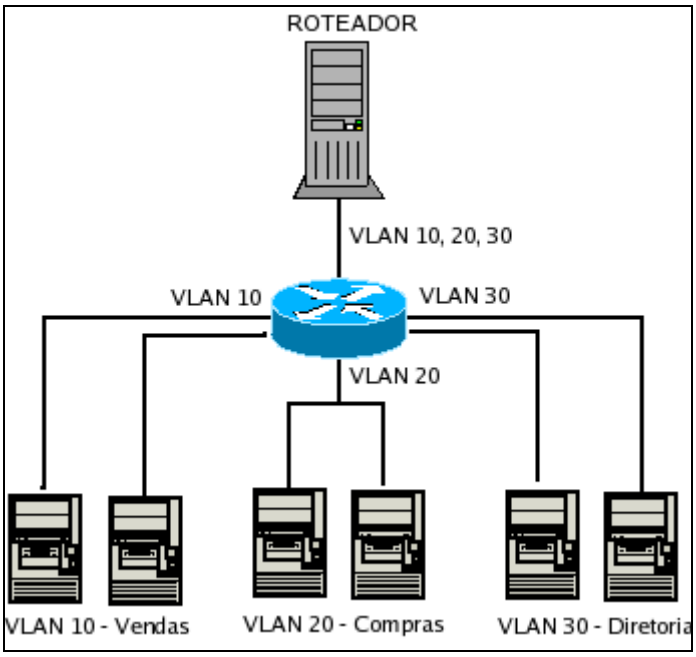

Figura 17 - Roteamento entre VLANs

Fonte: Comer (1998)

Cram101 (2015) aponta que na rede de computadores, encapsulamento é um método de criação de protocolos de comunicação modulares em que as funções logicamente separadas na rede são abstraídas de suas estruturas subjacentes pela inclusão ou ocultação de informação dentro de objetos de nível superior.

De acordo com Comer (1998), encapsulamento é uma técnica usada por protocolos em camadas, na qual um protocolo de nível mais baixo aceita uma mensagem de um protocolo de nível mais alto e a coloca na parte de dados do quadro de nível mais baixo.

Com o encapsulamento, os quadros transportados em uma rede física têm uma seqüência de cabeçalhos, na qual o primeiro deles vem do quadro da rede física, o próximo, do protocolo de Internet, o seguinte, do protocolo de transporte e assim por diante.

Dot1Q foi criado pelo IEEE para ser padrão de interoperabilidade entre equipamentos de diversos fabricantes. O método insere um novo campo específico no quadro Ethernet, e depois recalcula seu FCS (*Frame check Sequence*). Sendo assim, não é realizado um novo encapsulamento, como o antigo ISL.

3.7.5. Desempenho e Segurança

Apresentando um desempenho maior, as VLANs são superiores as redes locais, devido principalmente, a seu tráfico de broadcast.

Segundo um estudo de WYKRET (2009), concluiu-se que grande parte de todo o tráfego na rede é desnecessário. Como forma de segmentação lógica das redes, a implementação das VLANs obteve um resultado significativo no tráfego total da rede. A redução em alguns situações foi de aproximadamente 70%. Isso acaba se tornando possível, pois as VLANs tem a capacidade de reduzir o envio dos pacotes para endereços diferentes do destinatário.

Para maior segurança dos dados, as VLANs limitam o tráfego dos mesmos a domínios específicos. Ou seja, o tráfego de dados em uma VLAN acabam não sendo “escutados” por outras VLANs, a não ser que, haja um dispositivo de rede desempenhando uma função de roteamento entre essas redes virtuais. Criando assim, um ambiente mais restrito e seguro.

Sendo uma das características que mais é levada em conta durante a implementação de VLANs segundo Frinhani (2005), a segurança, permite que dispositivos localizados em diferentes segmentos físicos e em uma mesma VLAN, possam vir a se comunicar sem que outros dispositivos vizinhos tenham acesso.

Uma organização pode, por exemplo, separar seus setores em VLAN. Baseado na afirmação anterior, caso em uma organização existisse um setor por exemplo, de engenharia, este poderia ter sua própria VLAN em que todos os computadores e periféricos da camada de acesso correspondentes a esse setor fariam parte dessa VLAN, tornando essa, uma sub-rede separada das demais podendo ou não deixar os dados isolados do resto da rede mesmo que tenha outro setor com outra VLAN utilizando o mesmo switch. Nesse método, a segurança se torna maior, pois as políticas de segurança podem ser aplicadas de acordo com a VLAN desejada e, como já mencionado, os custos diminuem devido ao melhor aproveitamento do equipamento, o desempenho aumenta devido ao crescimento do número de domínios de broadcast e também por causa da diminuição do tráfego desnecessário na rede.

3.7.6. Port Security

Um switch que não contém a segurança de porta configurada deixa uma enorme brecha para possíveis ataques, roubo de informações sigilosas ou até infecção da rede com vírus ou pragas do tipo. Todas as portas do switch devem ser protegidas. A segurança de porta pode ser configurada de três formas (CISCO PRESS, 2002):

- **Endereços MAC seguros estáticos:** No modo estático é necessário entrar na configuração de cada porta e atribuir o endereço MAC do equipamento a porta para que o mesmo possa se conectar;
- **Endereços MAC seguros dinâmicos:** enquanto isso no modo dinâmico ao invés de configurar o endereço MAC, é configurado o número máximo de endereços MAC que a porta pode aprender, porém nesse caso, ao se reiniciar o switch essas configurações são perdidas;
- **Endereços MAC seguros fixos:** No modo fixo o método é o mesmo do modo dinâmico, porém essas informações são armazenadas no switch, e mesmo reiniciando o mesmo elas permanecem;

Caso haja alguma situação em que o número máximo de endereços MAC seja ultrapassado ou um endereço que não está na tabela tente se conectar ou até mesmo um endereço configurado em uma porta tente se conectar a outra porta, será entendido como uma violação de segurança. Essa violação pode ter três configurações de ações a serem tomadas, esses modos de violação são (CISCO PRESS, 2002):

- **Proteger:** neste modo, caso o número de endereços MAC aprendidos pela porta ultrapasse o limite estipulado a porta do switch simplesmente para de encaminhar tráfego, sem enviar mensagem de erro e sem desativar a porta;
- **Restringir:** no modo restringir a regra é a mesma porém nesse modo uma mensagem *syslog* é enviada acusando a violação;
- **Desligamento:** enquanto que no modo desligamento a regra também é a mesma, mas além da mensagem de *syslog* a porta é desativada;

3.7.7. QoS (Quality of Service)

A rede de uma comunicação é um dos principais constituintes de qualquer organização bem sucedida. Estas redes transportam uma infinidade de aplicações e dados, incluindo vídeos de alta qualidade e dados que são sensíveis a latência de uma rede, como por exemplo um vídeo ao vivo (CISCO, 2016). Através dessa afirmação é possível notar a importância do transporte desses dados, e para garantir uma boa qualidade para gerenciar os recurso de uma rede, é empregado o QoS (*Quality of Service* – Qualidade de serviço).

Para Cisco (2016), o QoS é um conjunto de técnicas para gerenciamento de recursos na rede, ou seja, são recursos que irão gerir o *delay*, largura de banda, parâmetros perdidos de pacotes, entre outros. Com isso, as redes acabam oferecendo serviços seguros, previsíveis, mensuráveis.

4. ESTUDO DE CASO

É demonstrado neste item, o estudo de caso realizado no decorrer deste trabalho. O estudo de caso foi realizado na topologia já existente de uma empresa de implementos rodoviários localizada na região. Por questões de sigilo, a empresa não permitiu a identificação neste trabalho.

As principais questões que foram levantadas na empresa, foram a: possibilidade de vazar dados de projetos (o que poderia gerar um grande prejuízo) e a demora em que esses dados eram trafegados pela rede.

4.1. Gerador De Tráfego JPERF (Java Performance And Scalability Testing)

O JPERF é uma ferramenta de software livre, do tipo cliente / servidor desenvolvida pelo *National Laboratory for Applied Network Research* (NLANR). Com este software é possível analisar textualmente e graficamente a medição do *throughput* da rede de pacotes TCP ou UDP, que é a taxa de dados transferidos de um cliente para um servidor na rede.

Para realizar as medições, o JPERF envia pacotes do cliente para o servidor, estes pacotes são enviados diretamente da memória do cliente para a memória do servidor, minimizando ao máximo as limitações de hardware. Ao final de cada geração de tráfego, é gerado um relatório em texto com os intervalos, dados transferidos ou perdidos e largura da banda. É gerado também, um gráfico baseado nos dados do relatório em texto.

Nas Figuras 18 e 19, é possível visualizar a forma que o software JPERF representa os relatórios.

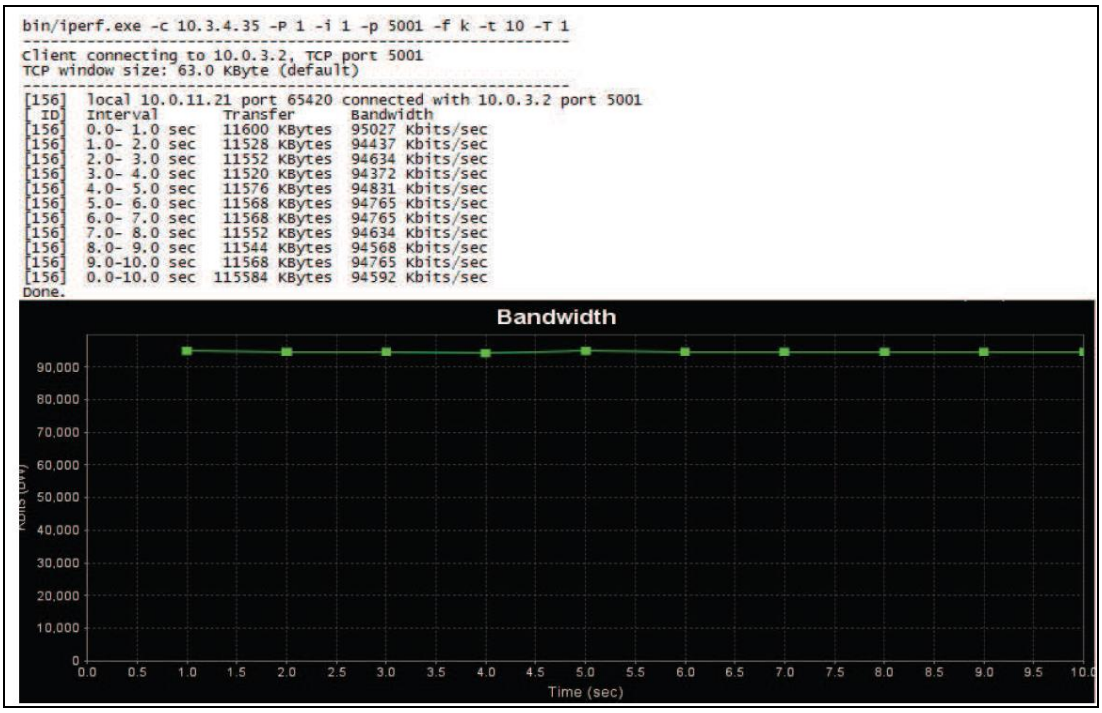

Figura 18 - Relatório Bandwidth Cliente JPERF

Fonte: Autoria Própria

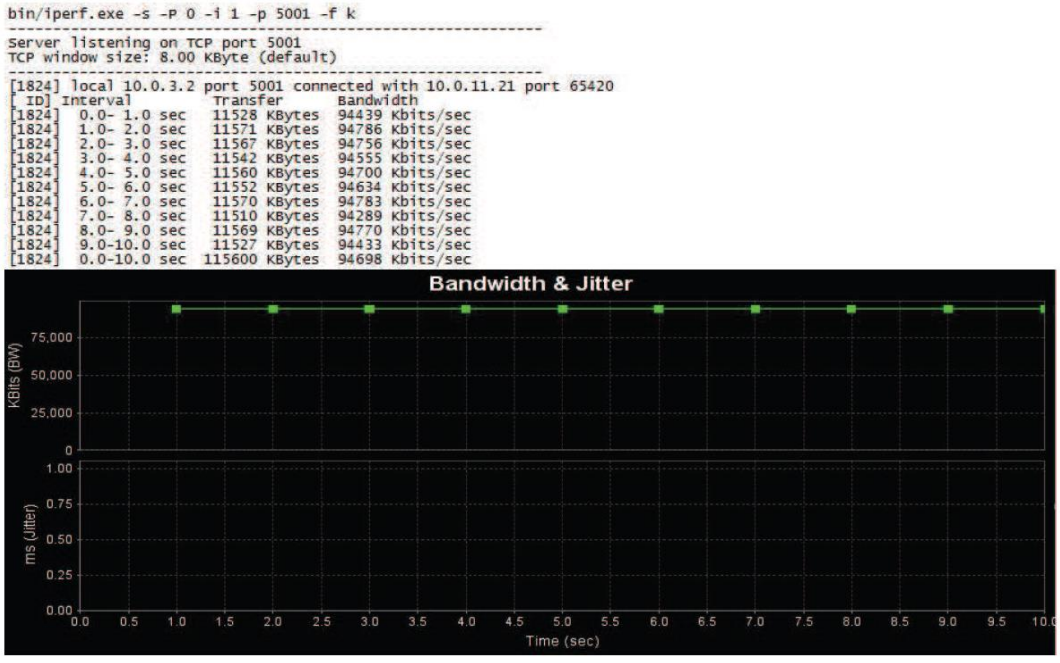

Figura 19 - Relatório Bandwidth Servidor JPERF

Fonte: Autoria Própria

A Figura 20 apresenta a topologia de uma rede existente anteriormente na empresa mencionada no início, onde os switches estão estruturados em cascata formando uma rede plana para todos os dispositivos.

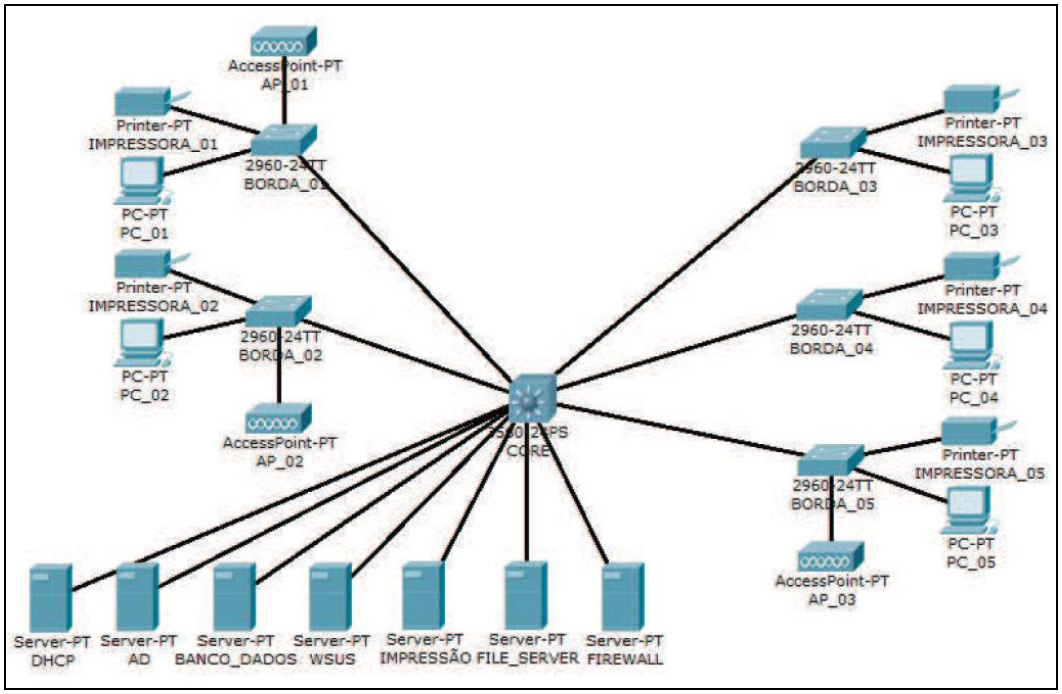

Figura 20 - Antiga topologia da Rede

Fonte: Autoria Própria

Como pode ser observado anteriormente na Figura 20, o *switch* CORE do modelo CISCO 3750X, considerado o núcleo da rede, onde estão conectados os *switches* do modelo CISCO 2960 BORDA_Ol, BORDA_02, BORDA_03, BORDA 04 e BORDA 05 e todos os servidores, sendo eles: DHCP, AD, BANCO=DADOS, WSUS, IMPRESSÃO, FILE_SERVER e FIREWALL. Os switches BORDA 01 e BORDA 02 se encontram em um andar do prédio e os switches BORDA_03, BORDA -04 e BORDA -05 se encontram em outro andar. A largura de banda dos enlaces entre os *switches* CORE e os de acesso dos equipamentos controlados são de 1 Gbps e a largura de banda entre os switches de acesso dos equipamentos não controlados e dispositivos finais são de 100 Mbps.

Na Tabela 4, é apresentado o plano de IPs que estava sendo utilizado anteriormente, onde estavam conectados todos os dispositivos, independentemente de sua importância ou aplicação.

Tabela 4 - Plano de numeração antigo

IP REDE	IP BROADCAST	MÁSCARA	RANGE ENDEREÇOS ÚTEIS	RANGE IP – FIXO	RANGE IP – DHCP
192.168.0.0	192.168.0.255	255.255.255.0	192.168.01 – 254	192.168.0.1 - 40	192.168.0.41 – 254

Fonte: Autoria Própria

Com a utilização deste plano de IPs teremos apenas um domínio de *broadcast*. O range de IP fixo é utilizado para dispositivos como servidores, impressoras, *switches* e pontos de acesso. O range de IP - DHCP é utilizado para os microcomputadores e notebooks que são inseridos na rede.

Quando há apenas um domínio de *broadcast*, temos também um problema de segurança, pois todos os dispositivos se "enxergam" sem restrições.

Na Tabela 5, estarão sendo apresentadas as medições geradas pelo software JPERF. O teste foi efetuado entre um CLIENTE / SERVIDOR onde foi utilizada uma estação de trabalho da engenharia (PC-03) e o servidor de arquivos da companhia (FILE-SERVER), que foi disparado do cliente para o servidor 10 pacotes TCP em um intervalo de 10 segundos.

Tabela 5 - Resultado da transferência

DESCRIÇÃO DO TESTE	ORIGEM	DESTINO	TEMPO	DADOS TRANSFERIDOS	LARGURA DE BANDA
TESTE_01	PC-03	FILE-SERVER	10 seg.	93368 KB	76371 Kbps

Fonte: Autoria Própria

Como pode ser visto, em um período de 10 segundos foi transferido uma média de 93368 Kbytes com uma largura de banda de 76371 Kbps. Este resultado será comparado com os testes que serão realizados após as alterações da rede.

Na topologia apresentada na Figura 17, foi utilizado o modelo Hierárquico de Rede, onde é possível visualizar quatro camadas numeradas de 1 até 4.

A camada 1 é a camada do Core, onde se encontrarão todos os switches e roteadores de alto desempenho e disponibilidade. Neste caso foram utilizados dois switches do modelo CISCO 3750X empilhados entre si para garantir sua redundância.

A camada 2 é a camada de acesso de equipamentos controlados, onde se encontram os servidores. Nesta camada foram utilizados switches do modelo CISCO 2960.

A camada 3 e 4 são as camadas de acesso de equipamentos não controlados, onde se encontram os *switches* do modelo CISCO 2960 que serão conectados aos dispositivos finais com os microcomputadores, telefones, impressoras, notebooks e pontos de acesso.

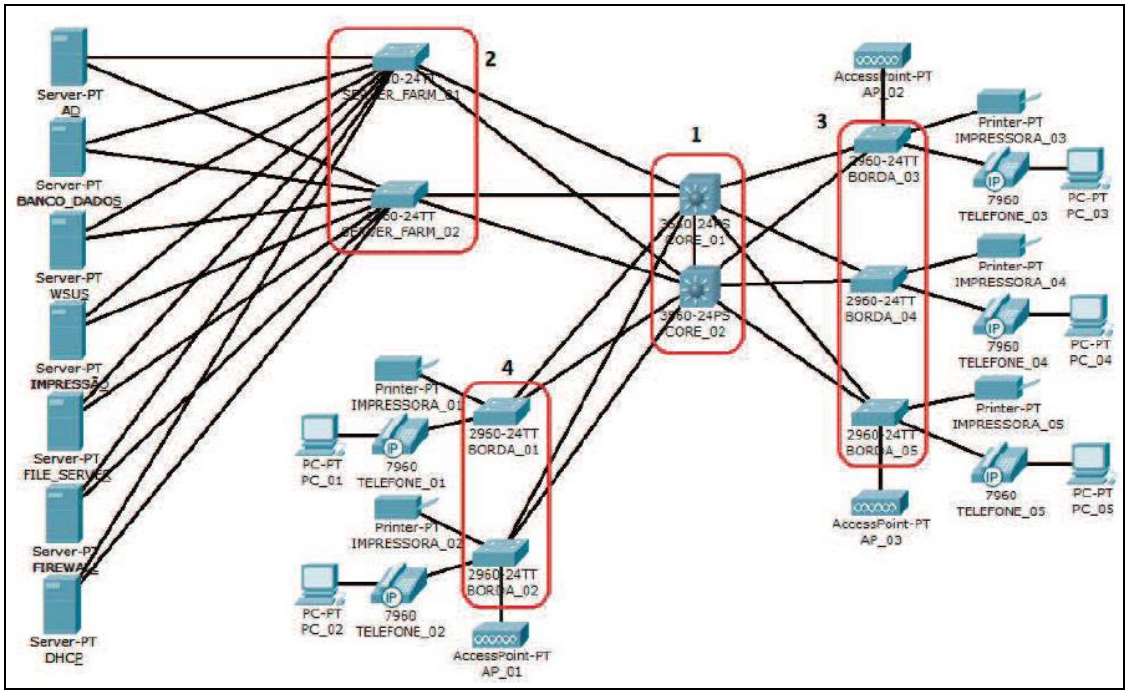

Figura 21 - Topologia segundo Modelo Hierárquico de redes

Fonte: Autoria Própria

Com o objetivo de evitar que alguma falha desabilite as aplicações de missão crítica da rede, será utilizada redundância entre as quatro camadas apresentadas na Figura 21.

O switch de acesso BORDA_01 está conectado aos dois switches CORE_Ol e CORE_02, que estão conectados aos *switches* de servidores SERVER -FARM -01 e SERVER_FARM_02. Estes dois, que por sua vez, estão conectados a uma placa de rede de cada servidor. A largura de banda dos enlaces entre o *switches* CORE e os de acesso dos equipamentos controlados são de 1 Gbps e a largura de banda

entre os *switches* de acesso dos equipamentos não controlados e dispositivos finais são de 100 Mbps.

Colocando fisicamente os cabos redundantes nos *switches* é necessário configurarmos o RSTP (*Rapid Spanning Tree Protocol*) para que os *switches* eliminem os *loops*. A opção pela escolha do RSTP foi feita por ter um tempo menor de convergência quando comparado ao STP (*Spanning Tree Protocol*). Os *trunks* são as interconexões de um switch ao outro onde são transferidos os dados e as informações de VLANs. Neste trabalho todos os *trunks* foram feitos entre as portas de 1 Gbps.

Como já foi dito anteriormente, com a utilização de VLANs podem-se criar vários domínios de broadcast e colocar cada dispositivo em domínios distintos, podendo ser roteados para outras VLANs ou não. Sendo assim, neste trabalho foi criado uma VLAN para gerência dos ativos, uma para os servidores, uma para impressoras, uma para access points com acesso para visitantes, uma para telefonia e uma para cada departamento ou grupo de trabalho. Em todos os *access points* foram criados SSIDs para todos os departamentos, inclusive para o acesso visitante. Por medida de segurança a VLAN default dos switches será desativada conforme apresentado na Tabela 6.

Tabela 6 - Plano de numeração novo

ID	DESCRIÇÃO	IP REDE	IP BROADCAST	MÁSCARA	RANGE END. ÚTEIS	GATEWAY (VLAN)	RANGE IP (FIXO)	RANGE IP (DHCP)	STATUS
1	PADRÃO	-	-	-	-	-	-	-	INATIVA
2	GERÊNCIA_ SWITCHES	10.0.2.0	10.0.2.31	255.255.255.224	10.0.2.1 – 30	10.0.2.30	10.0.2.1 - 29	-	ATIVA
3	SERVIDORES	10.0.3.0	10.0.3.31	255.255.255.224	10.0.3.1 – 30	10.0.3.30	10.0.3.1 – 29	-	ATIVA
4	IMPRESSORAS	10.0.4.0	10.0.4.31	255.255.255.224	10.0.4.1 – 30	10.0.4.30	10.0.4.1 – 29	-	ATIVA
5	AP_VISITANTES	10.0.5.0	10.0.5.127	255.255.255.128	10.0.5.1 – 126	10.0.5.126	10.0.5.1 – 20	10.0.5.21 – 125	ATIVA
11	TI	10.0.0.11.0	10.0.11.63	255.255.255.192	10.0.11.1 – 62	10.0.11.62	10.0.11.1 – 10	10.0.11.11 – 61	ATIVA
12	RH	10.0.0.12.0	10.0.12.63	255.255.255.192	10.0.12.1 – 62	10.0.12.62	10.0.12.1 – 10	10.0.12.11 – 61	ATIVA
13	DP	10.0.0.13.0	10.0.13.63	255.255.255.192	10.0.13.1 – 62	10.0.13.62	10.0.13.1 – 10	10.0.13.11 – 61	ATIVA
14	COMERCIAL	10.0.0.14.0	10.0.14.63	255.255.255.192	10.0.14.1 – 62	10.0.14.62	10.0.14.1 – 10	10.0.14.11 – 61	ATIVA
15	JURIDICO	10.0.0.15.0	10.0.15.63	255.255.255.192	10.0.15.1 – 62	10.0.15.62	10.0.15.1 – 10	10.0.15.11 – 61	ATIVA
16	FINANCEIRO	10.0.0.16.0	10.0.16.63	255.255.255.192	10.0.16.1 – 62	10.0.16.62	10.0.16.1 – 10	10.0.16.11 – 61	ATIVA
17	CONTABILIDADE	10.0.0.17.0	10.0.17.63	255.255.255.192	10.0.17.1 – 62	10.0.17.62	10.0.17.1 – 10	10.0.17.11 – 61	ATIVA
18	ADMINISTRAÇÃO	10.0.0.18.0	10.0.18.63	255.255.255.192	10.0.18.1 – 62	10.0.18.62	10.0.18.1 – 10	10.0.18.11 – 61	ATIVA
19	COMPRAS	10.0.0.19.0	10.0.19.63	255.255.255.192	10.0.19.1 – 62	10.0.19.62	10.0.19.1 – 10	10.0.19.11 – 61	ATIVA
20	REUNIÃO	10.0.0.20.0	10.0.20.63	255.255.255.192	10.0.20.1 - 62	10.0.20.62	10.0.20.1 – 10	10.0.20.11 – 61	ATIVA
21	RECEPÇÃO	10.0.0.21.0	10.0.21.63	255.255.255.192	10.0.21.1 – 62	10.0.21.62	10.0.21.1 – 10	10.0.21.11 – 61	ATIVA
22	ENG_E_ORCAMENTO	10.0.0.22.0	10.0.22.63	255.255.255.192	10.0.22.1 – 62	10.0.22.62	10.0.22.1 – 10	10.0.22.11 – 61	ATIVA
23	LICITACAO	10.0.0.23.0	10.0.23.63	255.255.255.192	10.0.23.1 – 62	10.0.23.62	10.0.23.1 – 10	10.0.23.11 – 1961	ATIVA
24	PLANEJAMENTO	10.0.0.24.0	10.0.24.63	255.255.255.192	10.0.24.1 – 62	10.0.24.62	10.0.24.1 – 10	10.0.24.11 – 61	ATIVA
101	TELEFONIA_01	10.0.0.101.0	10.0.101.63	255.255.255.0	10.0.101.1 – 254	10.0.101.254	10.0.101.1 – 10	10.0.101.11 – 253	ATIVA

Fonte: Autoria Própria

Para que não seja necessário criar as VLANs em todos os switches, foi configurado no CORE da rede, o VTP *server* e, em todos as bordas foi configurado o

VTP cliente, onde é feita a replicação das VLANs do CORE para as bordas automaticamente, passando pelos *trunks* criados.

Para uma melhor visualização e comparação dos testes executados, serão mostrados o teste na rede anterior às mudanças e na rede atual que serão apresentados na Tabela 7 depois das especificações do TESTE_02 e TESTE_03.

Abaixo é apresentado informações detalhadas sobre o TESTE_02:

- Equipamento de Origem: PC-03 pertencente à VLAN 22 (engenharia e orçamento);
- Equipamento de Destino: FILE_SERVER pertencente à VLAN 3;
- Rota traçada: PC_03 > TELEFONE_03 > BORDA_03 > CORE_01 > SERVER_FARM_01 > FILE_SERVER.

Abaixo é apresentado informações detalhadas sobre o TESTE_03:

- Equipamento de Origem: PC-02 pertencente à VLAN 11 (TI);
- Equipamento de Destino: PC-03 pertencente à VLAN 22 (engenharia e orçamento);
- Rota traçada: PC_02 > TELEFONE_02 > BORDA_02 > CORE_01 > BORDA_03 > TELEFONE_03 > PC_03.

Tabela 7 - Informações detalhadas sobre os testes

DESCRIÇÃO DO TESTE	VLAN ORIGEM	VLAN DESTINO	TEMPO	DADOS TRANSFERIDOS	LARGURA DE BANDA
TESTE 01	DEFAULT	DEFAULT	10 seg.	93368 KB	76371 Kbps
TESTE 02	22	3	10 seg.	115584 KB	94592 Kbps
TESTE 03	11	22	10 seg.	114584 KB	93848 Kbps

Fonte: Autoria Própria

Os testes consistiram em disparar do cliente para o servidor 10 pacotes TCP em um intervalo de 10 segundos, para medir o tráfego entre eles, levando em consideração a quantidade de dados transferidos, a largura de banda e o tempo.

5. CONCLUSÃO

Com o crescimento e aumento da complexidade das redes, uma solução simples e fácil de organizar uma rede logicamente é aplicar o uso de VLANs. Como tem sido visto no dia a dia, cada vez mais as tecnologias vêm convergindo para as redes, por exemplo, a telefonia IP que se não for implantada sobre uma boa segmentação da rede pode ter seu desempenho comprometido.

Baseado nos estudos e testes realizados é apresentado que parte do tráfego da rede de computadores é desnecessário, mas com a segmentação da rede com o uso de VLANs e outras tecnologias trabalhando simultaneamente o tráfego foi reduzido e o mais interessante é que isso ocorreu com praticamente o dobro de equipamentos conectados à rede.

Como foi apresentado, foram criadas várias VLANs representando grupos de trabalho ou departamentos. Com isso foi ganho um aumento da capacidade da rede e melhoria do tráfego de broadcast, pois a separando a rede em grupos de trabalho ou departamentos menores diminuiu o tráfego da rede toda. Segmentando a rede podemos também ter uma organização e facilidade na administração, pois fica muito mais fácil de visualizar a rede como um todo e também de se trocar a VLAN de cada usuário em caso de mudança de posto de trabalho.

Outra grande vantagem do uso de VLANs é que não é necessário termos um switch separado para cada grupo de trabalho ou departamento, pois as VLANs permitem que vários grupos possam trabalhar em um mesmo switch, mas em redes virtuais separadas. Isso faz com que o número de equipamentos seja reduzido, agrupando os departamentos em um mesmo switch.

Mesmo os grupos de trabalho ou departamentos estando num mesmo *switch* é possível ter um ganho de segurança, pois os equipamentos de uma VLAN não são capazes de capturar o tráfego de outra VLAN.

Importante também, destacar que o emprego de VLANs é possível ser feito em qualquer marca de *switches* a única restrição é que o equipamento seja gerenciável.

Novas tecnologias sempre irão surgir devido à demanda e crescimento que temos nas redes, mas é fato que o conceito de VLAN se consolidou nos dias atuais.

5.1. Trabalhos Futuros

Pode-se optar em um melhoramento da segurança da rede, visto que o principal foco deste trabalho era a performance. Para isso, seria interessante algumas outras técnicas como encriptação de dados, entre outros. Também, seria interessante a verificação da aplicação de alguns cenários específicos, para visualizar se há uma possiblidade de vazamentos dos dados trafegados pela rede.

Outra ponto que vale a pena verifica, é realização de testes na rede em vários momentos do dia, pois a latência de uma rede pode variar bastante de acordo com seu uso.

6. REFERÊNCIAS BIBLIOGRÁFICAS

BONAVENTURE, Olivier. **Computer Networking : Principles, Protocols and Practice**. Louvain-la-neuve: The Saylor Foundation, 2011. 282 p.

CRAM101. **Network+ Guide to Networks: Computer science, Computer networking.** 6. ed. Estados Unidos: Cram101 Textbook Reviews, 2015. 133 p. Disponível em: <https://books.google.com.br/books/about/Network+_Guide_to_Networks.html?id=2UHMAwAAQBAJ&redir_esc=y>. Acesso em: 19 maio 2016.

CISCO PRESS. **Cisco Ccna - Guia de Certificação do Exame Ccna Cisco Ccna - Guia de Certificação do Exame Ccna.**Estados Unidos: Cisco Press, 2002

CISCO PRESS. **Cisco Networking Academy's Introduction to VLANs**. 2014. Disponível em: <http://www.ciscopress.com/articles/article.asp?p=2181837&seqNum=4>. Acesso em: 19 maio 2016.

CISCO. **Quality of Service (QoS).** Disponível em: <http://www.cisco.com/c/en/us/products/ios-nx-os-software/quality-of-service-qos/index.html>. Acesso em: 14 jun. 2016.

CISCO. **Configure InterVLAN Routing on Layer 3 Switches**. 2016. Disponível em: <http://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html>. Acesso em: 19 maio 2016.

CISCO PRESS. **Construindo Redes Cisco Escaláveis.** Estados Unidos: Cisco Press, 2002. 820 p

CISCO PRESS. **Diagnosticando Redes - Cisco Internetwork Troubleshooting Diagnosticando Redes - Cisco Internetwork Troubleshooting.** Estados Unidos: Cisco Press, 2002.

CISCO PRESS. **Projeto de Interconexão de Redes - Cisco Internetwork Design.** Estados Unidos: Cisco Press, 2002. 636 p.

CARTHERN, Chris et al. Data Link Layer. In: CARTHERN, Chris et al. **Cisco Networks: Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA**. Nova Iorque: Apress, 2015. p. 35-48.

FOROUZAN, Behrouz A.; MOSHARRAF, Firouz. **Redes de Computadores: Uma Abordagem Top-Down**. Porto Alegre: Mcgraw-hill, 2012. 928 p.

FRAGOULI, Christina; WIDMER, Jörg; BOUDEC, Jean-yves Le. **Efficient Broadcasting Using Network Coding**. Ieee: ACM TRANSACTIONS ON NETWORKING, Lausanne, p.450-463, abr. 2008.

FRINHANI, Rafael de Magalhães Dias. **Projeto de re-estruturação do gerenciamento e otimização da rede computacional da Universidade Federal de Lavras**. 2005. 123 f. TCC (Graduação) - Curso de Ciência da Computação, Universidade Federal de Lavras, Lavras, 2005.

Gouveia, J.; Magalhães, A. (2005). **Redes de Computadores**. R. D. Estefânia, 138, R/C Dto., 1049-057 LISBOA: FCA - Editora de Informática, Lda.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **About ISO**. 2016. Disponível em: <http://www.iso.org/iso/home/about.htm>. Acesso em: 16 maio 2016.

JUNG, Edson Venicius; PELLIS, Ricardo Rafael. **Aplicando segurança em redes locais através de gerenciamento de ativos de rede**. 2013. Disponível em: <http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS11/Ricardo Rafael Pellis _ TCC Ricardo Pellis.pdf>. Acesso em: 19 maio 2016.

MATTOS, Diogo M. F. et al. **Uma Rede de Testes Interuniversitária com Técnicas de Virtualização Híbridas**. Disponível em: <http://gta.ufrj.br/ftp/gta/TechReports/MMC12.pdf>. Acesso em: 19 maio 2016.

PEICEVIC, Antun. **CCENT ICND1 100-101 Cert Guide**. Estados Unidos: Geek University Press, 2016

PILLOU, Jean-françois. **VLAN - Redes virtuais**. Disponível em: <http://br.ccm.net/contents/289-vlan-redes-virtuais>. Acesso em: 19 maio 2016.

PINHEIRO, José Mauricio Santos. **OSI: Um Modelo de Referência**. 2008. Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_osi_um_modelo_de_referencia.php>. Acesso em: 19 maio 2016.

ROSÁRIO, J.M. **Princípios de Mecatrônica**. São Paulo: Prentice Hall, 2005.

SOARES, Luiz Fernando Gomes; SOUZA, Guido Lemos de; COLCHER, Sérgio. **Redes de Computadores: das Lans, Mans e Wans às Redes ATM**. 2. ed. Rio de Janeiro: Campus, 1995. 740 p.

STRATA. **The Data Encapsulation Process**. Disponível em: <http://strata.ccilearning.com/Lesson3NetworkingandInternetworking/TheDataEncapsulationProcess/tabid/733/language/en-CA/Default.aspx>. Acesso em: 19 maio 2016.

TANENBAUM, Andrew S. **Redes de Computadores**. 4. ed. Rio de Janeiro: Campus, 2003.

TANENBAUM, Andrew S.; WETHERALL, David J.. **COMPUTER NETWORKS**. 5. ed. Seattle: Pearson, 2011. 933 p.

TIWARI, Anamika et al. **Data Link Layer**. International Journal Of Engineering Technology & Management Research.Jabalpur, p. 143-146. fev. 2013

TORRES, Gabriel. **Redes de Computadores Curso Completo**. Rio de Janeiro: Axcel Books, 2001. 688 p.

TORRES, Gabriel. **O Modelo de Referência OSI para os Protocolos de Rede**. 2007. Disponível em: <http://www.clubedohardware.com.br/artigos/o-modelo-de-referencia-osi-para-protocolos-de-rede/1349>. Acesso em: 19 maio 2016.

VÉSTIAS, M. (2005). **Redes Cisco para Profissionais**. R. D. Estefânia, 183, R/C Dto., 1049-057 LISBOA: FCA - Editora de informática, Lda.

WYKRET, Thiago Floriano. **Segmentação Virtual de Redes de Computadores**. 2009. 106 f. TCC (Graduação) - Curso de Ciência da Computação, Universidade Federal de Lavras, Lavras, 2009.

ZIMMERMANN, Hubert. **OSI Reference Model-The ISO Model of Architecture for Open Systems Interconnection**. Ieee Transactions On Communications, Rocquencourt, v. 4, n. 28, p.425-432, abr. 1980.