UNIVERSIDADE FEDERAL DO PARÁ
CAMPUS UNIVERSITÁRIO DE CASTANHAL
FACULDADE DE COMPUTAÇÃO
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

KLÉBER ÁLVARES MARTINS

REDES LOCAIS VIRTUAIS: Um estudo de caso

CASTANHAL – PA
2021

KLÉBER ÁLVARES MARTINS

REDES LOCAIS VIRTUAIS: Um estudo de caso

Trabalho apresentado à Universidade Federal do Pará – Campus Castanhal, como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação, sob orientação do Prof. José Jailton Henrique Ferreira Júnior.

CASTANHAL – PA
2021

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD
Sistema de Bibliotecas da Universidade Federal do Pará
Gerada automaticamente pelo módulo Ficat, mediante os dados fornecidos pelo(a) autor(a)

A473r Álvares Martins, Kléber.
REDES LOCAIS VIRTUAIS : Um estudo de caso / Kléber Álvares Martins. — 2021.
49 f. : il. color.

Orientador(a): Prof. Dr. José Jailton Henrique Ferreira Júnior
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal do Pará, Campus Universitário de Castanhal, Faculdade de Sistemas de Informação, Castanhal, 2021.

1. Rede Local Virtual. 2. Rede Virtual. 3. Virtual LAN. 4. Segurança da Informação. I. Título.

CDD 005.7

KLÉBER ÁLVARES MARTINS

REDES LOCAIS VIRTUAIS: Um estudo de caso

Trabalho de Conclusão de curso aprovado em 30 de julho de 2021

Conceito: Bom

Banca Examinadora:

José Jailton Henrique Ferreira Júnior
Orientador – UFPA/ FACOMP

Tássio Costa de Carvalho
Membro da Banca – UFPA/ FACOMP

Thiago Antônio Sidônio Coqueiro
Membro da Banca – UFPA/ FACOMP

CASTANHAL – PA
2021

DEDICATÓRIA

Dedico este trabalho científico a minha família e a todos que de uma forma ou de outra, contribuíram para que esse dia tornasse possível.

AGRADECIMENTO

Agradeço em primeiro lugar a Deus que iluminou o meu caminho durante esta jornada. Agradeço também aos meus filhos, Pedro Ruan e Emilly Kamilly que embora não tivessem conhecimento disto, iluminaram de maneira especial os meus pensamentos, incentivando-me a buscar mais conhecimentos. E não deixando de agradecer de forma grata e grandiosa à minha mãe, Antônia Martins.

“No meio da confusão, encontre a simplicidade. A partir da discórdia, encontre a harmonia. No meio da dificuldade reside a oportunidade.”
Albert Einstein

RESUMO

Uma empresa quer seja pública ou privada, deve ter o cuidado e controle do nível de acesso a rede de computadores. Há diversas aplicações para esse tipo de controle a nível de hardware e software. Nos deteremos, em especial, ao aprofundamento dos conhecimentos referentes à implementação de Redes Locais Virtuais (VLAN's), propondo a segmentação lógica (virtual) em um ambiente físico, a fim de se obter melhor desempenho e segurança em uma estrutura de rede corporativa. Através do estudo de suas diversas características e configurações podemos obter o conhecimento necessário para comparar as diferentes formas de implementação de VLANS e, de certa forma, esta tecnologia que vem se destacando por sua economia, flexibilidade e versatilidade. Descreveremos o uso dessa tecnologia, que associa um conjunto de máquinas ou usuários dispostos na rede, segmentando-os em departamentos ou aplicação, independentemente da localização de seus segmentos físicos. Descrevendo também, os protocolos de redes e VLAN's, os tipos de VLAN's, os equipamentos de interconexão que segmentam e une uma rede a outra, tendo como objetivo geral a segmentação da rede em grupos de usuários, com características de trabalho semelhante, otimizando a transmissão de dados, aumentando a performance e a segurança da rede. Este trabalho culmina em um estudo de caso na Universidade Federal do Pará – Campus Castanhal, evidenciando as razões que justificam a escolha da implementação da tecnologia de VLAN's, e não outra, mostrando cenários antes e após a implementação, analisado o gerenciamento do tráfego de rede, o desempenho e a segurança da informação.

Palavras-chave: Rede Local Virtual. Rede Virtual. Virtual LAN. Segurança da Informação.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

A comunicação entre diversos tipos de equipamentos em uma rede requer um certo nível de segurança. Com a escalabilidade da rede, há uma crescente adição hardwares e softwares que devem ser avaliados, principalmente, no quesito segurança de dados na comunicação entre diversos usuários, para garantir a integridade da informação.

Este trabalho tem como proposta, avaliar o nível de segurança de redes locais virtuais – VLAN, comparando-as com redes locais sem a o uso desta tecnologia, e assim, verificar os possíveis problemas de segurança da informação, sugerindo melhorias a partir de simulações de rede usando a ferramenta Packet Tracer da CISCO. Tendo como ponto de partida, a avaliação da rede em três setores da Universidade Federal do Pará/ Campus Castanhal.

O primeiro setor escolhido foi a Coordenação Geral, onde o coordenador deve usar o computador a nível de gerência na unidade, concentrando toda a decisão política-administrativa. O segundo setor escolhido foi a Secretaria Geral, onde agrupam cinco secretarias de curso: Educação Física, Pedagogia, Letras, Matemática e Computação e, o terceiro setor, o Laboratório de Informática, que dá acesso à internet e a rede local a todos os discentes do compus.

Os setores acima propostos, estão dentro de uma infraestrutura de rede estruturada capaz de conduzir informações de voz, dados, multimídia e vídeo. O problema é que todos os computadores estão compartilhados na rede. Foi identificado a existência de grupos de usuários com as mesmas características de uso, mas sem a separação física dos demais. E, desta forma, um usuário mal-intencionado pode fazer uso de *Sniffer* – um software ou um hardware que permite monitorar o tráfego de rede em tempo real e deste modo, capturar informações sigilosas.

E, como medida de segurança, foi analisado a implementação de switch gerenciáveis com suporte a VLAN, que tem como características o agrupamento de estações de usuários a uma ou mais VLAN's físicas, para se formar um único domínio de difusão ou de broadcast, garantindo a comunicação entre elas, mesmo que façam parte de segmentos físico diferentes.

Neste contexto, é feira uma análise do comportamento da rede e é apontado, em quais cenários é mais vantajoso e eficiente o tráfego de informações na rede, de modo seguro.

1.1 Justificativa

Em uma rede corporativa, onde há diversos usuários conectados, seria um problema ter informações sigilosas em mãos erradas e ter que instaurar uma auditoria para detectar quem acessou a rede indevidamente. O acesso, a divulgação e o tratamento de informação classificada como sigilosa ou pessoal deveriam ficar restritas às pessoas autorizadas. Mas, não é o que acontece em um ambiente compartilhado, onde há muitas possibilidades de invasões de privacidade, caracterizados como crimes cibernéticos.

Como proposta, é feito o agrupamento de um conjunto de máquinas de maneira lógica, através das configurações de switches de nível 3, que suportam VLAN's. Dessa maneira, os grupos de usuários estariam divididos em departamentos e, deste modo, facilitando a gerência da rede.

1.2 Objetivos geral

Propor a implementação de uma segmentação lógica de rede por meio switch gerenciáveis que suportam VLAN's no campus da Universidade Federal do Pará/ Castanhal, em três departamentos ou setores: Coordenação Geral, Secretaria Geral e Laboratório de Informática.

1.3 Objetivos específicos

Diferenciar as melhores soluções para a utilização dos equipamentos de rede e, analisar o estudo de caso, que envolve a segurança da informação em três espaços físicos do Campus Universitário de Castanhal, avaliando-os com o simulador Packet Tracer da CISCO, para evidenciar o funcionamento da rede, e assim, tomar as devidas conclusões de forma assertivas quanto ao tráfego de dados na rede.

1.4 Metodologia de pesquisa

Este trabalho é uma revisão sistemática da literatura, de acordo com a metodologia PICO (participantes, intervenção, contexto e resultados), foi conduzida em três fases: planejamento, condução e por último publicação de resultados.

A metodologia PICO é baseada em evidências que considera o contexto e o delineamento do estudo (CENTRE FOR REVIEWS AND DISSEMINATION, 2008). O quadro 1, apresenta as definições para cada um dos atributos da metodologia PICO.

Quadro 1: Atributos PICO definidos para o mapeamento da pesquisa

População/ Participantes	Aqui está inserida as características e definições relacionadas a redes de computadores com o nível de segurança da informação em publicações relacionadas com o uso de VLAN's.
Intervenção	Este componente abrange o uso de simulador de redes que melhor evidencie as soluções de segurança da informação com a implementação de VLAN.
Contexto	O acesso à informação precisa ser contido em meios compartilhados, evitando que informações sigilosas possam ser usadas de forma ilegítima, causando prejuízos de ordem econômica e estratégica no desenvolvimento institucional.
Resultados	Corresponde ao benefício da análise comparativa, que melhor se adequa ao nível de segurança da informação com baixo custo de investimento.

Fonte: Elaboração própria, 2021

Foi realizado uma revisão sistemática da literatura (RSL) com o objetivo de identificar, selecionar, avaliar os estudos considerados relevantes sobre um tópico de pesquisa. Na fase de planejamento foi conduzida de um modo interativo, com a identificação do objetivo da pesquisa, respondendo a seguinte quentão: Como a literatura tratou ente problema de segurança da informação até então?

A segunda fase é a de condução, cujas as atividades foram a identificações dos estudos primários da literatura, e como estratégia de busca foi usada a *string* ((“*vlan” OR “types of vlan” AND (“traffic safety of network” OR “network security”*)) e, com estes parâmetros aplicados, 115 trabalhos foram retornados.

Um dos critérios de inclusão foi o acesso completo ao conteúdo da base de dados na revisão sistemática encontradas em bases de dados digitais como ACM Digital Library; IEEExplore e Google Scholar. A inclusão foi baseada na identificado procedimentos e técnicas para gerenciamento e implementação de VLAN e estudos que abordam esse tema. O critério de exclusão foi a análise de publicações distintas referentes ao mesmo estudo; estudos que não mencionava o uso de VLAN's.

Aplicando os critérios de seleção dos estudos, foi definido na busca de artigos e textos completos, para assim, extrair e sintetizar os dados, cujo montante foi reduzido para 86 artigos.

E, a terceira fase a de publicação onde foi especificado e formatado o relatório e por último, avaliado.

2 FUNDAMENTAÇÃO TEÓRICA

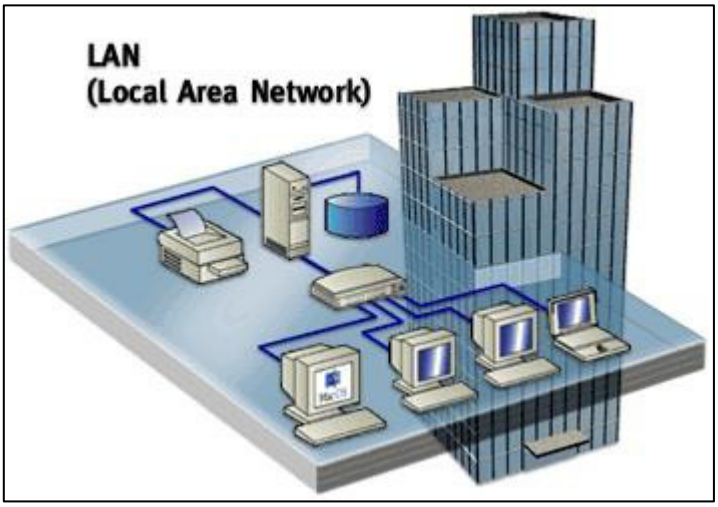
2.1 Classificação das redes (LAN, MAN, WAN)

Com a expansão das redes, foi sentido os problemas desse crescimento acelerado. Muitas das tecnologias criadas foram baseadas em diferentes plataformas de hardware e software que não eram compatíveis, o que dificultou a comunicação entre si, ou seja, o objetivo principal de compartilhar informação e recursos de rede não era atingido. Foi então que as redes foram divididas conforme a classificação LAN, MAN e WAN.

2.1.1 Redes de Área Local – LAN (Local área Networks)

As redes de abrangência local, designadas de LAN (Local Área Network) são redes de pequena dispersão geográfica que abrange uma área geográfica limitada como escritórios, empresas, ou um conjunto de edifícios muito próximos. Conectando computadores numa mesma sala, prédio ou campus com a finalidade de compartilhar recursos associado aos computadores (ROSS, 2008). Na figura 1, mostra uma rede LAN em uma estrutura predial, conectando diversos computadores, servidores e impressora.

Figura 1: Redes LAN (abrangência local)



Fonte: Fábrica de Software, 2013

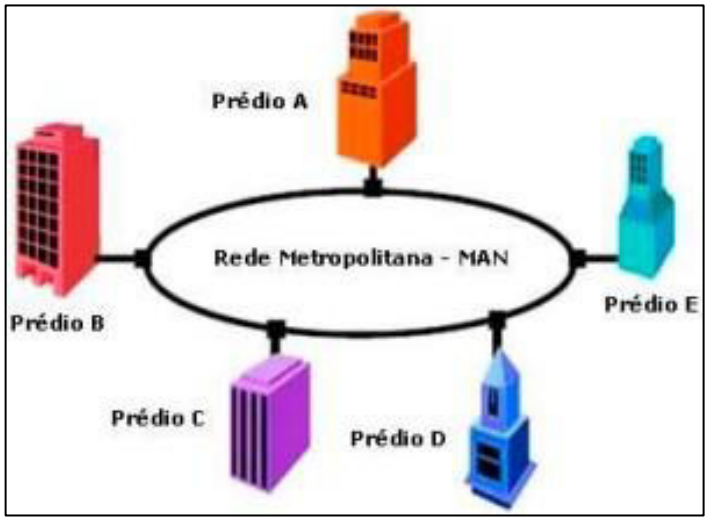
A finalidade principal das LAN's é a troca de dados entre terminais, permitindo também o compartilhamento de recursos de software e hardware. O quesito gestão ou administração de redes, que é uma atividade fundamental que exige do profissional de redes,

conhecimentos técnicos, experiência, e empenho por parte do administrador (BOAVIDA, 2009).

2.1.2 Redes de Área Metropolitana – MAN (Metropolitan Área Networks)

As redes metropolitanas são redes de dimensão média, ocupam aproximadamente o espaço de uma cidade, constituída por uma ou mais redes LANs. Portanto, uma MAN pode abranger um grupo de escritórios vizinhos ou uma cidade inteira e pode ser privada ou pública. Na figura 2 mostra uma rede metropolitana de abrangência a nível de cidade, conectando diversos prédios.

Figura 2: Redes Metropolitanas



Fonte: Fábrica de Software, 2013

2.1.3 Redes de Área Geograficamente Estendida – WAN (Wid Área Networks)

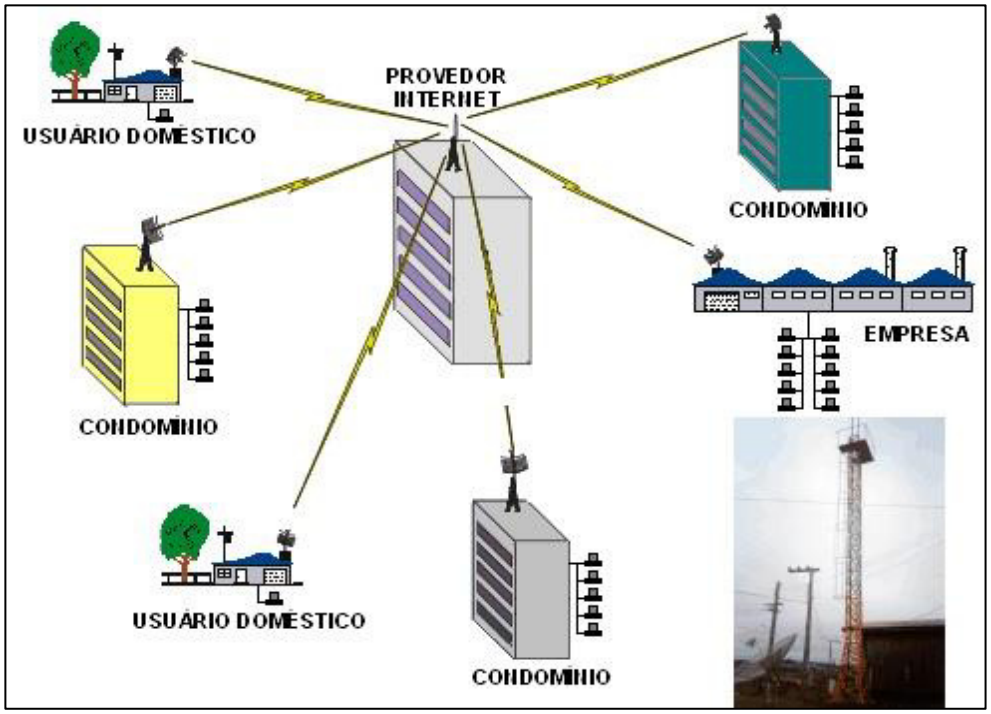
Atualmente a internet é a maior WAN que conhecemos. Em geral as redes geograficamente distribuídas têm conjuntos de servidores, que formam as grandes e variadas sub-redes, tendo como função, o transporte de dados entre os computadores ou dispositivos de rede.

As corporações conseguem um crescimento a nível global, graças a WAN, que conectam as redes de uma vasta área geográfica, permitindo a comunicação a longa distância.

Em resumo, uma rede WAN é uma rede de comunicação de dados que cobre uma área geográfica extensa e que oferece uma transmissão de dados provida por operadoras, como

empresas de telefonia e telecomunicações. Na figura 3, mostra uma rede WAN, que por meio do provedor de internet, consegue prover a comunicação de diversas redes locais em longas distâncias.

Figura 3: Redes WAN (Geograficamente estendida)



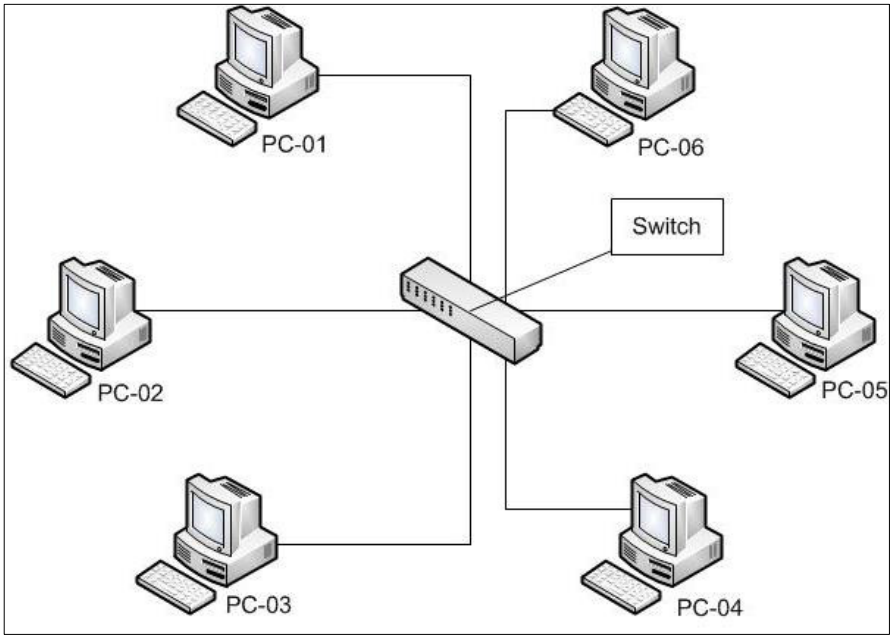
Fonte: Fábrica de Software, 2013

2.2 Topologias de redes

A topologia de redes refere-se ao layout físico dos computadores em uma rede. Os profissionais utilizam esse termo quando querem referir-se ao projeto físico da rede, ou a forma como os computadores e, outros componentes de rede, ficam dispostos no projeto geral de uma rede (ROSS, 2008).

A topologia de rede também descreve como é a estrutura de uma rede, através da qual há o tráfego de informações e, também o modo como os dispositivos estão ligados à mesma e, assim, podem ser descritas fisicamente e logicamente. A topologia física é a verdadeira aparência da rede, como pode ser visto na figura 4, enquanto que a lógica descreve o fluxo dos dados através da mesma (ROSS, 2008).

Figura 4. Topologia de rede em estrela.



Fonte: Elaboração própria (2021).

A instalação física das redes tem sofrido uma forte tendência na direção da utilização de switches, o que fisicamente, corresponde à implantação de uma topologia em estrela, como pode ser visto na figura 4. Essa tendência é explicada, basicamente, pela crescente necessidade de melhorar o gerenciamento e a manutenção nessas instalações (ROSS, 2008).

Em redes locais, a topologia de rede mais usada é a topologia em estrela, onde todas as estações estão interligadas em um equipamento central, numa forma de ligação ponto-a-ponto, que prevê a comunicação no sentido concentrador à estação e vise e versa (DANTAS, 2010).

A topologia de uma rede depende do projeto das operações, da confiabilidade e do seu custo operacional. Ao se planejar uma rede, muitos fatores devem ser considerados, mas o tipo de participação dos nodos[1] é um dos mais importantes (ROSS, 2008).

A topologia de uma rede irá determinar, em parte, o método de acesso utilizado. Métodos de acesso são necessários para regular o acesso a meios físicos compartilhados. Assim, costuma-se associar os métodos de acesso às topologias utilizadas (ROSS, 2008).

O concentrador com o layout em estrela pode implementar a comunicação entre as estações interligadas ao equipamento central de duas maneiras diferentes: por broadcast e na forma comutada ou switched. Na forma broadcast, o computador envia uma mensagem ao

[1] Nodo pode ser fonte ou usuário de recursos, ou ambos (ROSS, 2008).

concentrador que transmite a mensagem para todos os computadores do ambiente. Na técnica conhecida como switched, a mensagem é direcionada diretamente ao computador do destinatário (DANTAS, 2010).

A escolha de uma ou outra topologia irá depender da necessidade e aplicação, lembrando que, este assunto não se esgota por aqui, e que existem outras topologias de redes.

2.3 Arquitetura de rede

A comunicação entre máquinas distintas envolve uma série de detalhes que devem ser cuidadosamente observados para que esta comunicação ocorra de maneira precisa, segura e livre de erros. E para reduzir a complexidade de projeto, a maioria das redes de computadores são estruturadas em camadas ou níveis, onde cada camada desempenha uma função específica dentro do objetivo maior que é a tarefa de comunicação (SECLEN, 2011).

As camadas são construídas umas sobre as outras e cada camada oferece seus serviços para as camadas superiores, protegendo estas dos detalhes de como os serviços oferecidos são de fato implementados. Por exemplo, os comutadores são dispositivos que permitem a ligação entre os elementos de uma rede, que trabalham basicamente nas duas camadas do modelo de referência OSI, camada física e enlace de dados (SECLEN, 2011).

2.4 Modelo de referência TCP/IP

O modelo de referência mais conhecido é o TCP/IP (Transmisson Control Protocol Internet Protocol). Este modelo surgiu da rede ARPANET, que foi uma rede de pesquisa criada pelo Departamento de Defesa do governo americano visando à conexão de inúmeras redes (DANTAS, 2010).

O protocolo TCP/IP é na verdade um conjunto de protocolos também conhecido como pilha de protocolos. Seu nome faz referência a dois protocolos diferentes, o TCP (Transmission Control Protocol) e o IP (Internet Protocol), veja a quadro 1, o modelo de rede baseado no protocolo TCP/ IP.

Quadro 1. Modelo TCP/IP.

	Modelo TCP/ IP em Camadas
4	Aplicação
3	Transporte
2	Internet
1	Interface com a Rede

Fonte: Elaboração Própria (2021).

Os modelos de referência TCP/IP e OSI têm muito em comum. Ambos são baseados no conceito de pilha de protocolos independentes e a funcionalidade das camadas é muito semelhante. Por exemplo, em ambos os modelos, camadas de transporte e as demais acima, fornecem o serviço de transporte independente de rede fim a fim, processando pedidos de comunicação, formando o provedor de transporte (DANTAS, 2010).

As camadas acima da de transporte são voltadas para o processamento de pedidos de comunicação. Apesar de terem semelhanças fundamentais, os modelos são muito diferentes. É importante ressaltar que está sendo comparados os modelos de referência, e não as pilhas de protocolos.

2.5 Modelo de referência OSI

Em 1983 a International Organization for Standardization (ISO) concluiu o modelo de referência chamado Open Systems Interconnect (OSI), que descreve as arquiteturas de comunicação de dados (DANTAS, 2010). Veja a quadro 2, o modelo de referência OSI.

Quadro 2. Modelo de referência OSI.

Modelo de referência OSI em camadas	
7	Aplicação
6	Apresentação
5	Sessão
4	Transporte
3	Rede
2	Enlace de Dados
1	Física

Fonte: Elaboração própria (2021).

O modelo OSI divide todas as tarefas relacionadas às redes em sete camadas, conforme mostra a quadro 2. Cada camada é responsável por um subconjunto das funções que devem ser realizadas na rede. Para isso, cada camada tem seus próprios protocolos e manipula uma unidade de dados que é chamada de Unit Protocol Data (Unidade de Dados do Protocolo - PDU). Entenda a PDU como o conjunto de informações, ou o pacote, gerado por uma camada (ROSS, 2008).

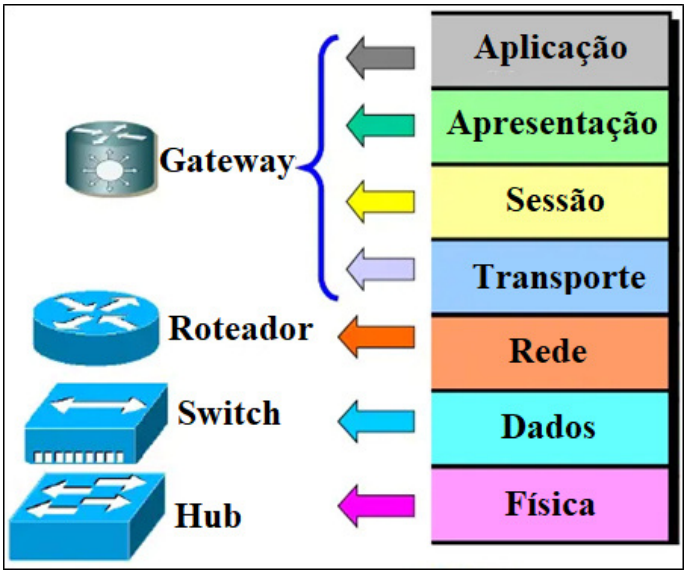
No transmissor, as informações descem da camada 7 até a camada 1 e no receptor elas são recebidas pela camada 1 e sobem até a camada 7. À medida que os dados descem nas camadas, a camada inferior trata os dados recebidos da camada superior como uma caixa preta,

colocando-os no seu campo de dados. Desse modo, a PDU é formada por um campo de dados que corresponde aos dados recebidos da camada superior, acrescido de alguns campos adicionais que são inseridos pela própria camada para que possa realizar suas tarefas. Esses campos adicionais são chamados de cabeçalhos (ROSS, 2008).

Na máquina receptora, à medida que as informações sobem nas camadas, cada camada lê as informações do cabeçalho da sua PDU, processa essas informações, e as retira do pacote passando apenas o conteúdo da parte de dados para a camada superior. O conteúdo desse campo de dados é, evidentemente, a PDU da camada superior (ROSS, 2008).

O modelo OSI, é um padrão para protocolos de rede. E, protocolos nada mais são do que regras de comunicação usadas para conectar dois ou mais computadores. O que o modelo OSI faz é agrupar esses protocolos em grupos específicos, ou camadas para dá suporte a conectividade de diversos equipamentos de redes, como mostra a figura 5. **Gateway** (Aplicação, Apresentação, sessão e transporte; **Roteador** (Redes); **Switch** (Dados) e, **Hub** (Física).

Figura 5: Relação de equipamentos de acordo com o modelo de referência OSI



Fonte: Elaboração própria, 2021

2.5.1 Camada 1 - Física

A primeira camada do modelo OSI é a camada Física, analogamente, a esta camada seria como as estradas, ou seja, o caminho que os pacotes percorrem até chegar ao destino. É na camada física que atuam os dispositivos como hub e os meios de transmissão, como os cabos de rede. Os dados são transmitidos por esses meios e processadas na próxima camada.

2.5.2 Camada 2 - Enlace

A camada de enlace ou ligação funciona como um fiscal. Ela observa se existe algum defeito em sua formatação e controla o fluxo com que os pacotes são enviados.

Se houver algum defeito na camada superior – camada 1, esses erros podem ser corrigidos, para assim, seguir o fluxo dos dados na transmissão a camada seguinte. É nesta camada que é definida as VLAN's, topologias Token ring, ponto-a-ponto, é nesta camada que também funcionam os switches.

2.5.3 Camada 3 – Rede

A camada de rede funciona como uma central de correspondências, é nesta camada que temos o endereçamento IP de origem e destino do pacote. Assim, correspondências precisam ser transportadas para a camada seguinte com esta finalidade sabendo a origem e o destino, e deste modo, precisa da camada seguinte para seguir com o fluxo.

2.5.4 Camada 4 – Transporte

A camada de transporte funciona como estradas e caminhos com que percorrem os dados, analogamente teríamos os caminhões e os carteiros representando-os. Esta camada garante o envio e o recebimento dos pacotes vindos da camada 3. Esta camada lida com a qualidade do serviço, mas para que ocorra o transporte de dados entre os computadores, é necessário que as máquinas consigam se comunicar e, essa é a função da próxima camada.

2.5.5 Camada 5 – Sessão

Esta camada é responsável por estabelecer e encerrar a conexão entre os hosts, é nesta camada que há a sincronização dos hosts. Além de realizar o estabelecimento das sessões, também prover algum suporte a elas, como registro de log e realização de tarefas de segurança.

Os dados ainda precisam ser tratados para serem usados. Como a camada de sessão é responsável por estabelecer a conexão entre os hosts, o tratamento dos dados é de responsabilidade da próxima camada.

2.5.6 Camada 6 – Apresentação

A camada de apresentação é responsável por fazer a tradução para que a próxima camada os use. Nesta camada temos a conversão de códigos para caracteres, a conversão e compactação dos dados, além da criptografia desses dados, caso necessite.

2.5.7 Camada 7 – Aplicação

A camada de aplicação é a última camada usada. Nesta camada temos os programas que garantem a interação humano-computador. Nela, é possível enviar e-mails, transferir arquivos, acessar websites, conectar remotamente em outra máquina, entre outras coisas.

E, para resumir podemos ver as principais atividades do modelo OSI no quadro 3.

Quadro 3: Resumo de atividades do Modelo OSI

CAMADA	**Tipos de atividades**
7 - Aplicação	Desenvolvimento de aplicações Web; Gerenciamento de redes (Ex. aplicações SNMP-based); P2P; VoIP; Web Services; Gerenciamento de serviços de redes (DNS, DHCP, e-mail, etc.); segurança.
6 - Apresentação	Ações relacionadas com a manutenção da semântica das informações transmitidas (Ex. aplicações de registros bancários, utilização de criptografia e compressão de dados).
5 - Sessão	Funcionalidades relacionadas com o estabelecimento de sessões entre diferentes usuários (Ex. browser escalona o uso de rede as diferentes páginas abertas pelo usuários).
4 - Transporte	Gerenciamento de barreira de segurança; criação de protocolos (Ex. protocolo de tempo real para a comunicação de voz).
3 - Rede	Desenvolvimento e gerenciamento de roteadores; endereçamento de dispositivos (IPV4 e IPV6).
2 - Enlace	Projeto e desenvolvimento de projetos (Ex.: ponto de acesso wi-fi, modens e switch)
1 - Física	Projeto e desenvolvimento de meios de comunicação de dados (Ex.: redes sem fio, fibra ótica).

Fonte: Elaboração própria, 2021

2.6 Equipamentos de interligação de redes

Os equipamentos de interligação de rede permitem a ligação de sistemas a uma rede. Interligando vários segmentos dentro da mesma rede e, de redes distintas. A heterogeneidade dos equipamentos é uma das características mais marcantes das redes de hoje. Conhecer os diversos tipos de equipamentos existentes no mercado pode ajudar na tomada de decisão (BOAVIDA, 2009).

Os principais equipamentos de interligação de redes usados nesta pesquisa, permitem a ligação de sistemas terminal à rede são: hubs, switches e roteadores.

2.6.1 Hubs

O hub é um dos equipamentos ativos, muito usados para a interconexão das estações de trabalho, no Modelo OSI, ele atua na camada física, não tem suporte para a identificação do host. O hub tem como característica a formação dentro de seus circuitos, um barramento Ethernet, que permite que todos os computadores conectados a ele se comuniquem e ainda faz a regeneração do sinal digital recebido (MENDES, 2020).

É uma característica do hub transmitir a informação por todas as portas, exceto por aquela que recebeu essa informação (flood), criando assim um único domínio de colisão e diminuindo a performance.

2.6.2 Switches

O switch (ou comutador) atua na camada de enlace do modelo de referência OSI. Ele ao receber um quadro, analisa os endereços MAC, identifica o host de origem e destino e, baseando-se em uma tabela construída de forma dinâmica (tabela de bridging), decide para qual porta enviar o quadro Ethernet (MENDES, 2020).

No switch, a rede não fica vinculada a um único computador no envio de informações. Isso aumenta o desempenho da rede já que a comunicação estará sempre disponível, exceto quando dois ou mais computadores tentam enviar dados simultaneamente à mesma máquina. Essa característica também diminui a ocorrência de erros e colisões de pacotes (DANTAS, 2010).

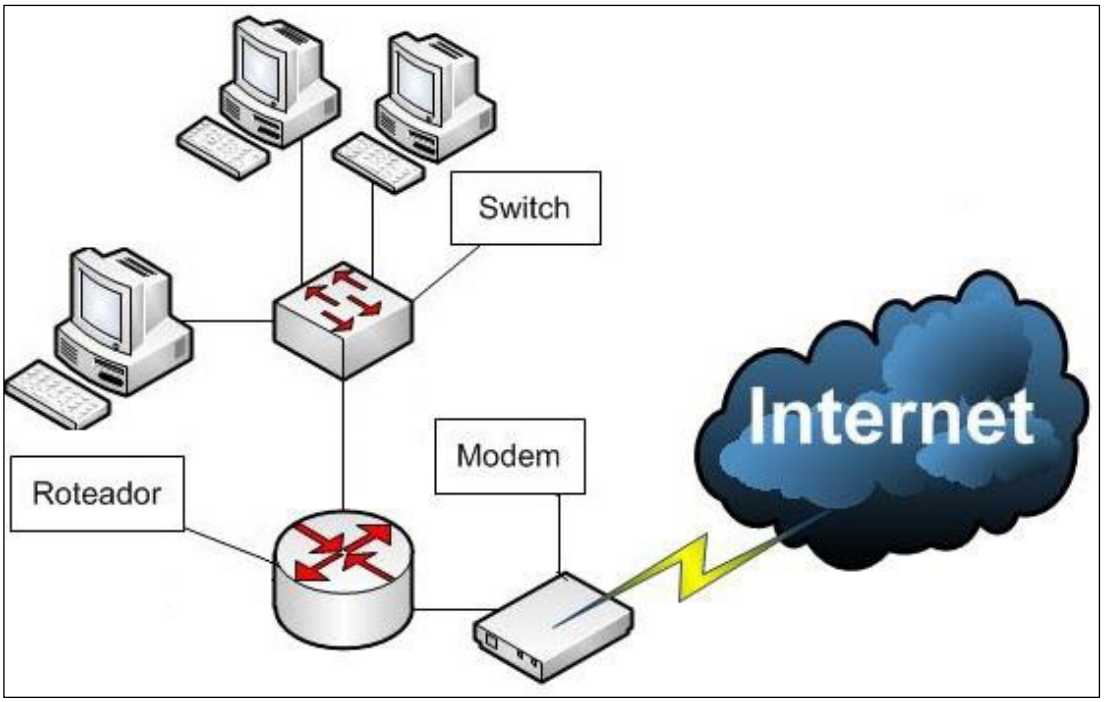
A tabela bridging é construída dinamicamente pelo switch, basta que seja recebido um quadro por uma das portas. Ao receber o quadro, switch extrai o endereço MAC de origem e a VLAN, que serão usados na tabela de bridging. Quando o receptor devolver a requisição ao equipamento origem, o switch analisará o novo quadro e extrairá o endereço MAC e sua VLAN, que também serão armazenados na tabela de bridging (MENDES, 2020).

2.6.3 Roteadores

Roteadores são comutadores de pacotes do tipo armazena-repassa que transmite pacotes usando endereços da camada de rede (KUROSE, 2010).

É um dispositivo de rede que permite interligar redes distintas. A Internet é composta por inúmeros roteadores interligados entre si. Ao acessar um site qualquer, a requisição trafega por vários roteadores, até chegar ao destinatário e os dados enviados por eles fazem o caminho inverso para chegar ao seu computador veja na figura 6 os equipamentos de interligação de redes (KUROSE, 2010).

Figura 6. Equipamentos de interligação de redes



Fonte: Elaboração própria (2021).

Um roteador pode ser tanto um dispositivo dedicado, no caso dos roteadores de maior porte, quanto um computador com duas ou mais placas de rede rodando um sistema operacional com suporte a esta função (KUROSE, 2010).

Roteadores programáveis vêm sendo utilizado para possibilitar a criação de redes virtuais. Dentre as diversas técnicas empregadas para atribuir programabilidade à rede, a que tem tido maior sucesso no passado recente consiste na criação de regras de fluxos para permitir o particionamento lógico da rede física (BAYS, 2012).

2.7 Segurança de redes

A segurança de redes surge na tentativa de minimizar as vulnerabilidades de sistemas computacionais. Desta forma, para se ter segurança de computadores é preciso prevenir ataques com objetivos definidos por meio de contenção de acessos não autorizados ou usos não autorizados de computadores e redes (MORAES, 2010).

Há diversas analises para se chegar a uma conclusão de sistema realmente seguro. Temos então, que ver se o sistema é seguro, se ele se comporta de maneira que espera que ele o faça, concomitantemente tem que haver um computador que seja confiável, de modo que, você pode depender dele e o software reaja de maneira esperada, possuindo assim, o comportamento que você espera dele (MORAES, 2010).

Há uma série de ações maliciosas, ou ameaças, que podem violar restrições de segurança de sistemas computacionais. Essas ameaças são apresentadas em quatro categorias: divulgação, fraude, disrupção e usurpação (BAYS, 2012).

Divulgação é definida como a obtenção de acesso não autorizado a informações protegidas. Dados sigilosos podem ser erroneamente expostos a entidades não autorizadas, ou adquiridos por atacantes que burlam a segurança de um sistema.

Fraude é caracterizada pela tentativa intencional de iludir outras entidades. Por exemplo, uma entidade maliciosa pode enviar informações falsas ou incorretas a outras, levando-as a acreditar que tais informações são corretas. Identidades falsas podem ser usadas de modo a incriminar outrem ou obter acesso ilegítimo.

Disrupção significa causar a falha ou a degradação de sistemas, afetando negativamente os serviços providos pelos mesmos. Isso pode ser feito por meio da incapacitação direta de um componente do sistema ou dos canais utilizados para transmitir as informações, ou então induzindo o sistema a transmitir informações corrompidas (BAYS, 2012).

Usurpação, por este meio, atacantes podem obter controle não autorizado sobre um sistema. Tal controle não autorizado pode permitir que atacantes acessem dados ou serviços protegidos, de forma ilegítima, ou que adulterem o próprio sistema para causar comportamento incorreto ou malicioso.

2.7.1 Assinatura digital

Para se ter segurança numa transmissão de dados a solução é com a assinatura digital, que é um mecanismo de autenticação que permite ao criador de uma mensagem anexar um código que atue como uma assinatura. A assinatura é formada tomando o hash da mensagem e criptografando-a com a chave privada do criador. A assinatura garante a origem e a integridade da mensagem (STALLINGS, 2007).

2.7.2 Arquitetura de segurança

A arquitetura de segurança enfoca ataques, mecanismos e serviços de segurança. O ataque à segurança seria qualquer ação que comprometa a segurança da informação pertencente a uma organização. O mecanismo de segurança seria um processo, ou mecanismo incorporando a tal processo, que é projetado para detectar ou permitir a recuperação de um ataque à segurança. E, serviço de segurança, seria um serviço de processamento ou comunicação que aumenta a segurança dos sistemas de processamento de dados e as transferências de informação de uma organização (STALLINGS, 2007).

Para poder planejar e implementar um sistema de segurança confiável é aconselhável que os administradores de rede adotem padrões já consagrados no que diz respeito aos requisitos necessários ao tipo de sistema adotado, que melhor se adapte à rede (STALLINGS, 2007).

2.7.3 Sistema de segurança

O sistema de segurança começa com o controle de acesso, onde um sistema pode administrar quais entidades poderão acessar suas funções, e quais permissões cada uma terá. Para conceder direitos de acesso e permissões individuais, entidades devem estar propriamente autenticadas no sistema (BAYS, 2012).

O propósito da autenticação é assegurar que entidades comunicantes são, de fato, as entidades que afirmam ser. O receptor de uma mensagem deve ser capaz de identificar corretamente quem originou a mensagem. E uma entidade não deve ser capaz de usar a identidade de outra, garantindo confidencialidade de dados.

O serviço de integridade de dados tem como propósito garantir que dados armazenados por entidades ou transmitidos por uma rede não serão corrompidos, adulterados ou destruídos. Ataques como duplicação, modificação, reordenamento e reenvio de mensagens devem ser prevenidos (BAYS, 2012).

A disponibilidade de um sistema também é definida como um serviço de segurança. Recursos do sistema devem estar disponíveis no momento em que entidades autorizadas os requisitam, e o sistema deve obedecer a suas especificações de desempenho (BAYS, 2012).

2.7.4 Criptografia

Criptografia é a arte matemática que permite criptografar (cripto=esconder) e descriptografar dados, enquanto que encriptação é um processo de transformação de dados claros em uma forma ilegível, ou seja, encriptado.

O objetivo da criptografia é garantir a privacidade, mantendo a informação escondida para qualquer um que não seja o destinatário da mensagem, mesmo que ele possa ter acesso às informações criptografadas (BAYS, 2012).

Em um ambiente em que recursos físicos são compartilhados entre diversas redes virtuais, há uma série de comportamentos que podem resultar em divulgação indevida de informações.

Ataques de Negação de Serviço é a ameaça mais comum. Durante seu ciclo de vida, redes virtuais podem sofrer ataques que visam causar ruptura de serviços. Tais ataques podem se originar dentro da própria rede virtual, ou então de fontes externas.

Sobrecarga de recursos físicos, atributos como a capacidade de CPU e o limite de largura de banda devem ser levados em consideração em operações de implantação ou gerência de redes virtuais. A sobrecarga de recursos físicos pode causar a degradação do desempenho da rede. Tal degradação causa congestionamento e perda de pacotes (BAYS, 2012).

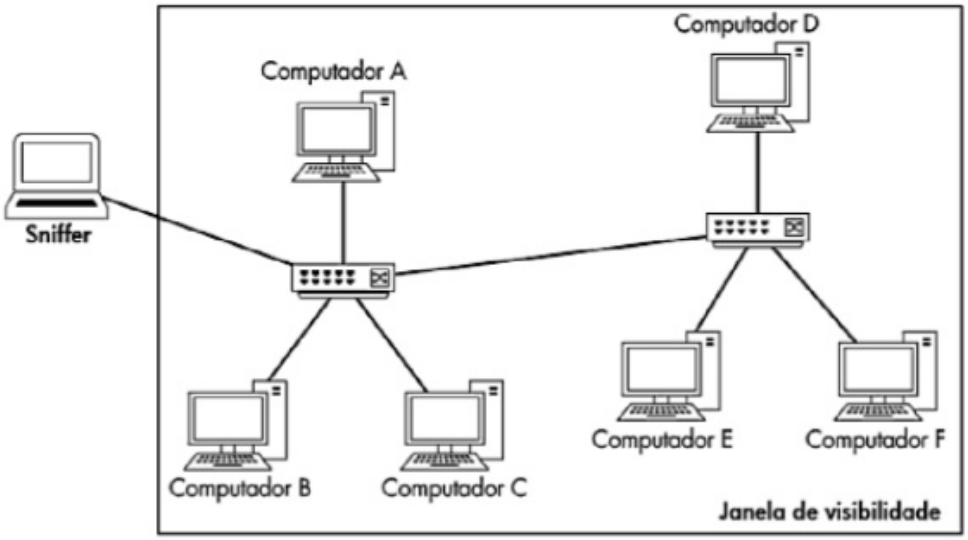
O isolamento e a distribuição adequada de recursos físicos entre redes virtuais são essenciais para manter o ambiente de virtualização de redes operando adequadamente. Isso inclui assegurar que os requisitos mínimos de cada rede serão cumpridos, bem como proibir que redes consumam recursos além do que lhes é permitido (BAYS, 2012).

2.8 Sniffers nos hubs

Segundo (SANDERS, 2017), é um sonho para qualquer profissional de análise de pacotes, ter sniffing instalados em uma rede com hub. Isso porque o tráfego por meio de um hub passa por todas as portas conectadas a esse equipamento, bastando conectar um sniffer de pacotes a uma porta vazia do hub é possível filtrar tudo que trafega na rede.

No contexto da segurança de rede, os sniffers são aplicativos usados para interceptar ou roubar dados, capturando o tráfego de rede. Os dados não criptografados estão sujeitos a interceptação, se não houver uma política de segura de rede bem definida. Na figura, temos uma rede com hub, onde oferece uma visibilidade ilimitada de acessos não autorizados.

Figura 7: Sniffing em uma rede com hub oferece uma janela de visibilidade ilimitada

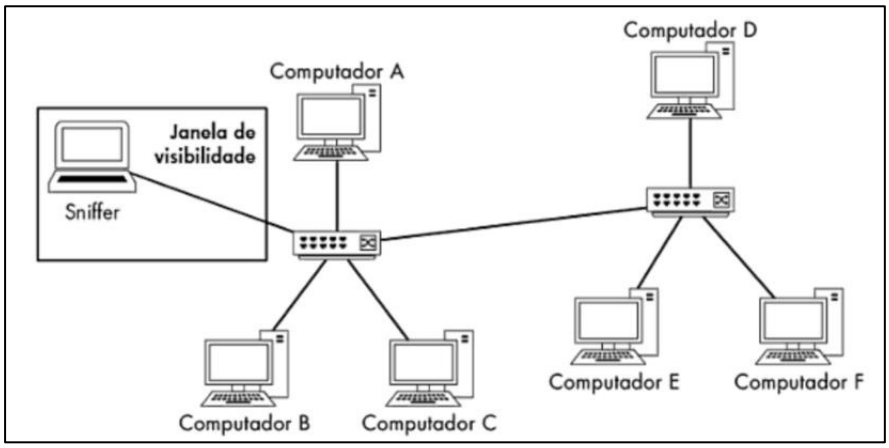


Fonte: (SANDERS, 2017)

2.8.1 Sniffers em ambientes com switches

Os switches são dispositivos muito usados em conexões de redes modernas. Oferecem maior eficiência no tráfego de dados, permitem a comunicação full-duplex, o que significa que as máquinas podem enviar e receber dados simultaneamente (SANDERS, 2017). Mas, estão sujeitos a ataques de acessos não autorizados. Na figura 8, mostra um sniffer conectado em um dos switches, possibilitando a filtragem de pacotes na rede, limitada a porta a qual está conectada.

Figura 8: Janela de visibilidade em uma rede com switches é limitada a porta a qual está conectada



Fonte: (SANDERS, 2017)

2.9 Modos de funcionamento de um comutador

O comutador estará no estado de encaminhamento, quando um usuário da rede envia um novo quadro, e este passa pelo comutador, o quadro é armazenado em uma tabela de roteamento do próprio comutador. E, todavia, que um quadro novo aparece o comutador analisa o endereço de destino e procura na tabela de endereços interno para escolher a porta por onde deve passar o encaminhamento, há outros tipos de encaminhamentos que são descritos no quadro 4. (SECLEN, 2011).

Quadro 4: Tipos de encaminhamentos em um switch

Unicast	É quando o quadro é encaminhado para única porta.
Multicast	É quando o quadro é encaminhado a um conjunto de portas.
Floading	É quando o quadro é encaminhado por todas as portas exceto a porta de entrada do quadro. Acontece quando o comutador não encontra o endereço de destino na tabela de endereços.
broadcast	É um tipo de endereço *multicast*. Quando um quadro é encaminhado por todas as portas exceto a porta de entrada do quadro.
Filtering	Filtragem de quadros. Sua função é restringir o encaminhamento de quadros que passam pelo comutador.

Fonte: Elaboração própria, 2021

O correto funcionamento do comutador está atrelado à tabela de endereço MAC. Esta tabela relaciona o endereço MAC com as físicas do comutador. O comutador precisa estar sempre armazenando endereços, e se por algum motivo, nunca mais apagar, a pesquisa de endereços na tabela demoraria muito. A solução foi apagar os endereços que não estão ativos, e só fica ativo se existir quadros na tabela de endereço de origem, desta forma o comutador estará no estado de envelhecimento constante (SECLEM, 2011).

2.9.1 Padronização de VLAN

IEEE 802.1D é o padrão para redes virtuais sobre Ethernet, que descreve as operações de comutadores interligados. Além disso, contêm uma descrição da tabela de endereços do comutador, os mecanismos de filtro e encaminhamento de quadros. Esta é uma tecnologia de redes virtuais que permite separar a conectividade lógica da conectividade física. (SECLEN, 2011).

2.9.2 Quadro ethernet

Um quadro Ethernet é definido pela norma IEEE 802.3, no caso do quadro Ethernet padrão, e pela norma IEEE 802.1Q, para os quadros com etiquetas VLAN (SECLEN 2011).

O quadro 5, mostra as funcionalidades de cada campo quadro Ethernet com etiqueta VLAN.

Quadro 5. Funcionalidades do quadro Ethernet com etiqueta VLAN.

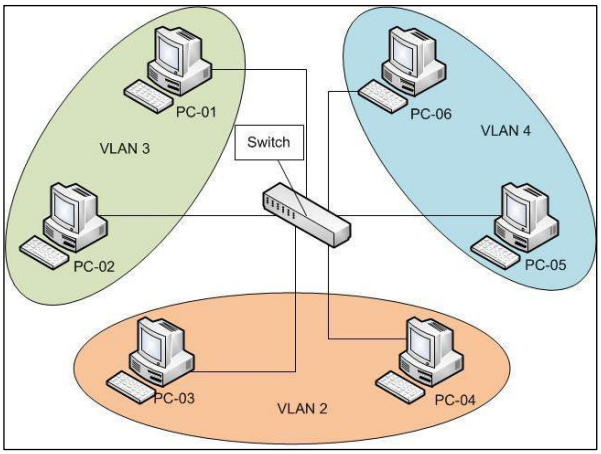
As funcionalidades do quadro Ethernet com etiqueta VLAN	
Preâmbulo	Padrão alternado de ‘0’ e ‘1’ sincroniza receptores com os quadros recebidos
FSD	Byte responsável pelo início do quadro
DA	Especifica o endereço de destino do quadro, *multcast* ou *broadcast*.
AS	Especifica o endereço físico MAC de quem enviou o quadro.
LENGTH/ TYPE	Indica o tamanho do quadro.
VLAN Identifie	A VLAN de 12 bits permite a construção de no máximo 4096 VLAN’s.
Dados	Tamanho do quadro 46 a 1500 bytes, no máximo.
FCS	Responsável por seqüenciar o tamanho de verificação do quadro.
VLAN *Protocol* ID	É globalmente atribuído e reservado o campo *EthernetType* como o valor 0x8100.
Priority	Responsável por estabelecer prioridades que vão de 0 a 7, este campo nos permite ter classes de serviços *Ethernet*.
CFI	Este campo é usado nos casos de encapsulamento de dados, nos quadros *token-Ring*.

Fonte: Elaboração própria (2021).

2.9.3 VLAN (Virtual Local Area Network)

VLAN ou *Virtual LAN* é uma facilidade de operação numa rede comutada. Esta facilidade permite que o administrador da rede a configure como sendo uma única entidade interligada. Todavia, é assegurada aos usuários a conectividade e privacidade que é esperada como se houvessem múltiplas redes separadas, como pode ser visto na figura 9, um exemplo de VLAN (DANTAS, 2010).

Figura 9. Exemplo de VLAN.



Fonte: Elaboração própria (2021).

As VLANs permitem a segmentação das redes físicas, sendo que a comunicação entre máquinas de VLANs diferentes terão que passar obrigatoriamente por um roteador ou outro equipamento capaz de realizar o encaminhamento, que será responsável por encaminhar o tráfego entre redes distintas.

O *switch*, equipamento central, dividiu a rede nas VLAN's 2, 3 e 4. Se não for configurado o switch, todos os computadores estarão conectados a VLAN 1. Na figura 9, a VLAN 2 está compartilhando o acesso com os PC-03 e PC-04; a VLAN 3 com os PC-01 e PC-02; a VLAN 4 com os PC-05 e PC-06, respectivamente.

Pode se ativar VLAN's em algumas portas de diferentes *switches*, fazendo com que estas se comportem como redes separadas, sendo assim, todos os pacotes provenientes de dispositivos membros de uma VLAN somente serão encaminhados para as portas dos *switches* pertencentes a mesma VLAN.

Em uma configuração básica, computadores de uma VLAN não podem se comunicar com computadores de outra VLAN, da mesma forma como redes locais diferentes não podem se comunicar. Assim também como nas redes locais, nas VLAN's devem ser usados dispositivos roteadores para proporcionar a interconectividade entre estas.

3 IDENTIFICAÇÃO DE VLAN

AS VLAN'S VID (*VLAN Identifier* ou Identificador de VLAN) podem ser identificadas de acordo com o código VID para a identificação das VLAN's. Os segmentos que possuem o mesmo VID pertencem à mesma VLAN. De alguma forma os switches devem reconhecer os VID's de cada quadro recebido, veja na quadro 6, algumas das identificações do código VID (DANTAS, 2010).

Quadro 6. Identificação de VLAN (VID).

VID	**Significado/Uso**
0x0-00	*NullnVLAN* ID. Indica que o tag não contém informação VID, apenas informação de prioridade. Assim, é conhecido como *Priority Tagged Frame*. Uma ponte VLAN somente enviará este quadro depois de classificar um TCI apropriado na porta de saída ou retirar a VLAN Tag retransmitindo o quadro sem informação de tag.
0x0-01	Valor padrão de porta VLAN usado para classificação por uma *bridge*. O valor pode ser trocado por gerenciamento baseado por porta.
0xF-FF	Reservado

Fonte: Adaptado de DANTAS (2010).

Todos os quadros enviados pela rede são rotulados com o ID da VLAN a qual pertencem que são processados por roteadores habilitados e então encaminhados conforme, as VLAN's são identificadas em porta, endereço MAC e protocolos (BAYS, 2010).

A virtualização de redes consiste no compartilhamento de dispositivos físicos reais como roteadores e comutadores, entre diferentes redes virtuais. Nas redes virtuais os roteadores e enlaces virtuais comportam-se como equipamentos físicos dedicados. No entanto, em termos práticos, os mesmos compartilham os recursos físicos com roteadores e enlaces de outras redes virtuais.

Ao longo dos anos, diferentes métodos para criação de redes virtuais têm sido usados. Abordagens típicas incluem VLAN's e VPN's (Virtual Private Networks). Mais recentemente, Monitores de Máquinas Virtuais e dispositivos de rede programáveis são empregados para criar roteadores e enlaces virtuais sobre dispositivos e canais de comunicação físicos (BAYS, 2012).

3.1 VLAN baseado em portas

As VLAN's baseada em portas também são conhecidas como VLAN briding. Neste tipo, cada porta recebe uma ou mais VID's, fazendo com que todos os terminais que estiverem conectados na mesma porta pertençam à mesma VLAN (DANTAS, 2010).

As portas de um switch podem ser configuradas nos modos Access (acesso) e Trunk (tronco). No modo Access pode pertencer somente a uma VLAN. E no modo Trunk pode pertencer a muitas VLAN's (DANTAS, 2010).

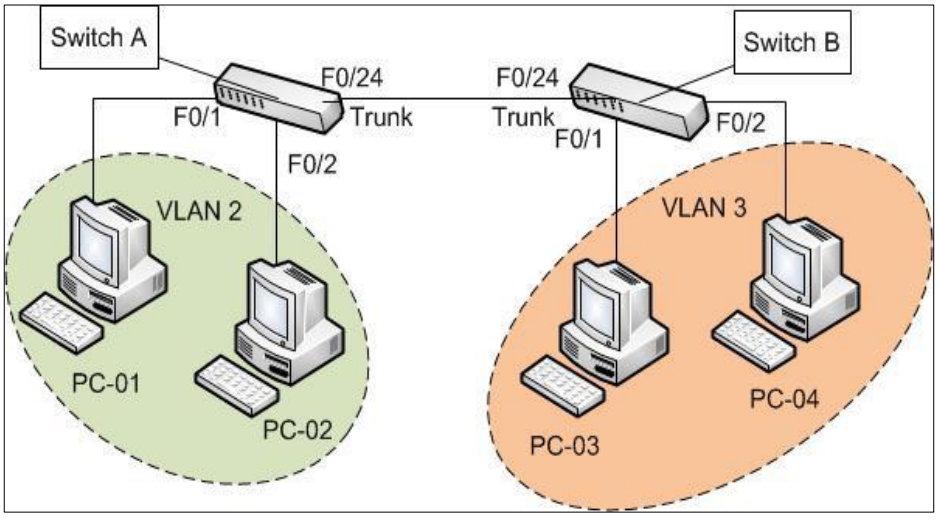
A identificação das VLAN's em um enlace configurado no modo Trunk é feita através dos métodos de marcação de quadros. Neste modelo de funcionamento todos os dispositivos interconectados devem ter suporte à identificação de membros e dos formatos de quadros de VLAN's. Dispositivos de rede que não suportem o reconhecimento de VLAN's não propagarão tráfego deste tipo, descartando os quadros, interrompendo ou impedindo a comunicação dos dispositivos interligados. (DANTAS, 2010).

As portas dos dispositivos de rede podem ser configuradas, além do modo Tronco, no modo Access, que ao contrário do trunk, restringe o enlace ao trafegar pacotes de uma única VLAN por meio de configuração prévia (DANTAS, 2010).

Portas configuradas em modo Acesso também não reconhecem quadros com marcação IEEE 802.1Q e descartam todo conteúdo deste tipo que chega. A comunicação entre dois dispositivos com suporte à VLAN também só ocorre quando as portas que os conectam estiverem configuradas de maneira adequada.

Na figura 10 mostra a configuração no modo Access. O switch A conecta os PC-01 e PC-02 nas portas F0/1 e F0/2, e estes só podem comunicar-se entre si na VLAN 2. No switch B conecta os PC-03 e PC-04 nas portas F0/1 e F0/2, e estes só podem comunicar-se entre si na VLAN 3. Para que as duas VLAN's possam comunicar-se, elas precisam de uma configuração, por exemplo, na porta F0/24 para o modo Trunk, e assim, troca informações entre os dois switches.

Figura 10. VLAN baseada em porta.



Fonte: Elaboração própria (2021).

Com as VLAN’s, basta realizar a configuração dos comutadores e roteadores para que, em determinadas portas, seja permitido o tráfego de pacotes da VLAN a qual o equipamento pertencia anteriormente, o que evita perda de tempo com deslocamentos e instalações, proporcionando uma alta flexibilidade.

3.2 VLAN baseado em endereço MAC

As VLAN's baseadas em endereço MAC funcionam mantendo uma lista no switch, que contém o endereço MAC de cada máquina que está conectada a ele, fazendo com que extraia o endereço MAC dos pacotes recebidos e procure em sua lista para qual terminal deverá ser encaminhado, veja quadro 7, exemplo de implementação de VLAN usando endereço MAC (DANTAS, 2010).

Quadro 7. Exemplo de implementação de VLAN usando endereço MAC.

Segmentação de rede usando endereço MAC para atribuição de VLAN			
Endereço MAC	00:50:04:64:2B:24	01:50:0F:F8:2F:37	00:04:DF:C8:72:A7
VLAN	1	2	1

Fonte: Elaboração própria (2021).

Ao invés de portas do switch as VLAN’s são associadas ao endereço MAC. Neste tipo de configuração, não há necessidade do switch ser reconfigurado toda vez que a estação do usuário for conectada a uma porta diferente. Esta implementação é útil quando, nas mudanças de departamentos, os usuários costumam levar suas estações de trabalho. A grande desvantagem deste método é associar entidades VLAN a cada endereço MAC encontrado, tornando-se muito onerosa no caso de redes muito grandes (DANTAS, 2010).

3.3 VLAN baseado em protocolos

As VLAN’s funcionam agrupando diversos protocolos diferentes. Os comutadores verificam cada pacote para identificar a qual rede virtual o pacote está associado por meio do protocolo usado. Um exemplo de virtualização de redes baseada em protocolos são as próprias VLAN’s, pois elas consistem em partições lógicas sobre uma única rede subjacente (BAYS, 2012).

3.4 Vantagens na implementação de VLAN'S

As VLAN's proporcionam um método de criação de redes lógicas independentes, que segmentam a rede global em pequenos domínios lógicos, suportados na mesma rede física. Desse modo, segue algumas vantagens com a implementação de VLAN's (DANTAS, 2010).

3.4.1 Flexibilidade da rede

Um novo usuário poderá ser adicionado à VLAN independentemente de sua localização física na rede (DANTAS, 2010).

3.4.2 Gerenciamento da rede

Em uma rede, quando é necessário mudar um computador de um lugar para outro, é necessário executar uma série de procedimentos, desde lançamento de novo cabeamento, até configuração de rotas e regras para que o equipamento permaneça na mesma rede ligada anteriormente. Com as VLAN's, basta realizar a configuração dos comutadores e roteadores para que, em determinadas portas, seja permitido o tráfego de pacotes da VLAN a qual o equipamento pertencia anteriormente, o que evita perda de tempo com deslocamentos e instalações, proporcionando uma alta flexibilidade (DANTAS, 2010).

Os equipamentos que suportam o uso de VLAN's também possuem funções de monitoramento de tráfego e comporta a ativação/desativação de portas permitindo que o administrador bloqueie portas que apresentem qualquer problema ou impedir que pessoas, inadvertidamente, conectem equipamentos em determinada rede virtual (DANTAS, 2010).

3.4.3 Controle do tráfego broadcast

Em redes não segmentada, computadores, impressoras e outros dispositivos conectados disseminam uma grande quantidade de pacotes de difusão, seja por falhas na conexão dos cabos, mau funcionamento de placas de rede, ou até mesmo por protocolos e aplicações que geram este tipo de tráfego, podendo causar atraso no tempo de resposta e lentidão na rede local.

Em uma rede segmentada com VLAN's cria vários subdomínios de difusão, diminuindo o tráfego de mensagens, tanto na rede segmentada como na rede da organização em geral (DANTAS, 2010).

3.4.4 Aumento de nível de segurança

Coma a segmentação da rede em domínios lógicos menores, pode dificultar o acesso de possíveis atacantes que não fazem parte desse domínio.

Um só switch com VLAN consegue suportar múltiplos domínios de broadcast e necessita apenas uma configuração de interface de ligação entre o switch e o roteador (DANTAS, 2010).

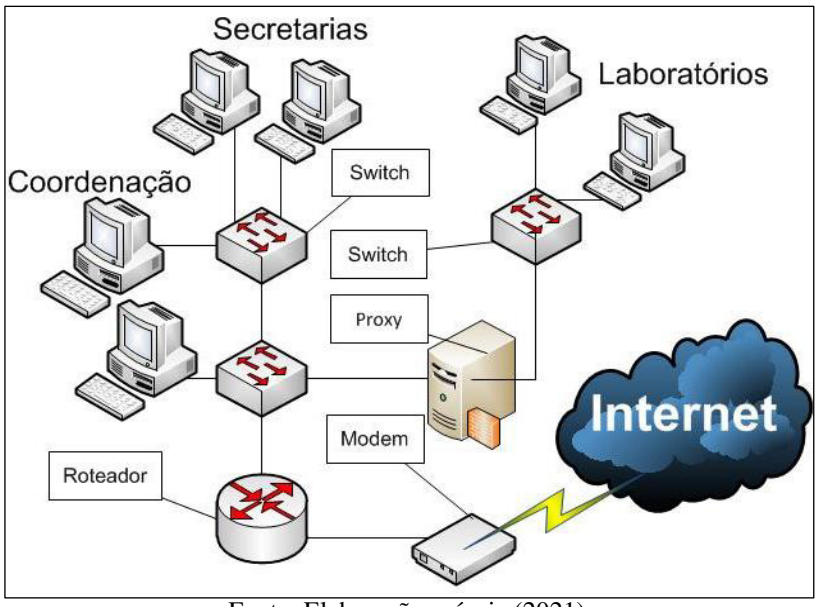
4 ESTUDO DE CASO

A Universidade Federal do Pará/ Campus Castanhal está localizada na região Nordeste do Estado do Pará. E, é um dos doze campi da UFPA, que vem se desenvolvendo com a interiorização da Universidade no Estado.

Este é um trabalho que tem como proposta avaliar o nível de segurança da informação com a virtualização de rede com VLAN's, verificando o comportamento da rede, especificamente em três setores: Coordenação Geral, Secretaria Geral e Laboratório de Informática. Estes setores ou departamentos, fazem parte de uma infraestrutura de rede estruturada, o tráfego da informação na rede, usando *sniffers* como ferramenta de filtragens de pacotes.

A figura 11, mostra a rede antes do uso de VLAN's. Todos os usuários pertenciam ao mesmo domínio de broadcast, ou seja, a rede compartilhava o mesmo canal de comunicação, apesar de ter diversos equipamentos de interconexão de rede, o que veio provocando lentidão na transmissão de dados, além da falta de segurança dos dados.

Figura 11. Cenário da rede da UFPA/ Castanhal sem VLAN.



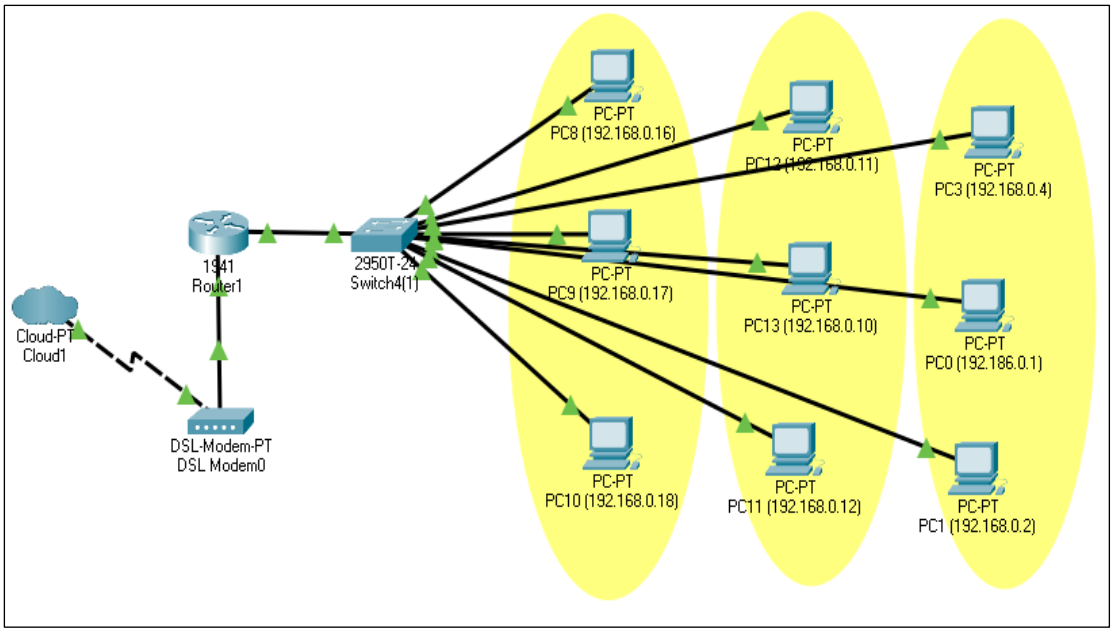
Fonte: Elaboração própria (2021).

Em uma LAN comum, quando é necessário mudar um computador de um edifício para outro, é necessário executar uma série de procedimentos, desde lançamento de novo cabeamento, até configuração de rotas e regras para que o equipamento permaneça na mesma rede ligada anteriormente.

Usado a ferramenta Packet Tracer, foi possível avaliar o funcionamento da rede em dois momentos. O primeiro, com todos os computadores conectados em rede, sem a separação por departamentos. A segunda, fazendo a separação por departamentos configuradas por meio de switches com suporte a VLAN's.

A figura 12, mostra a rede não segmentada, mas com características em comum onde os usuários pertencem a um determinado grupo com as mesma afinidades. Na figura 13, será mostrada a ideia de segmentação lógica, como proposta para diminuir os problemas relacionadas à falha de segurança e lentidão na transmissão de dados.

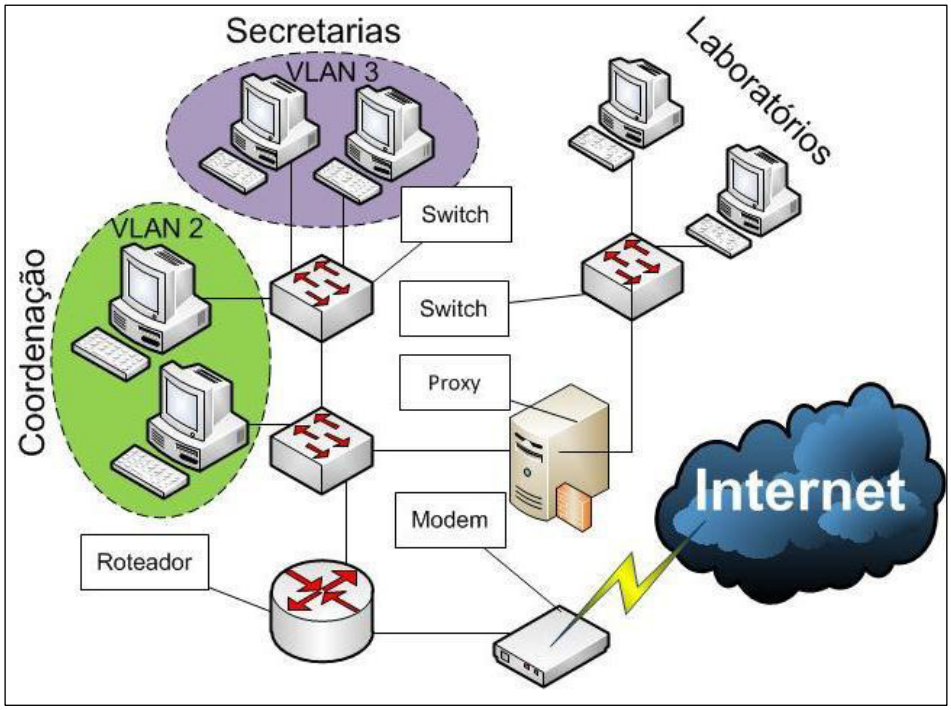
Figura 12. Simulação de Rede com a ferramenta Packet Tracer



Fonte: Elaboração própria (2021).

A figura 13, mostra a implementação de VLAN's. A coordenação passa a pertencer a VLAN 2, as secretarias a VLAN 3, e quanto ao laboratório, não está em nenhuma VLAN, (posteriormente pertencerá a VLAN 4). Neste momento, o laboratório de informática possui um servidor proxy, que é um computador intermediário que fica entre o computador dos usuários e a Internet, que pode ser usado para registrar o uso da internet e/ ou bloquear o acesso a um determinado site.

Figura 13: Layout do laboratório de informática com servidor proxy

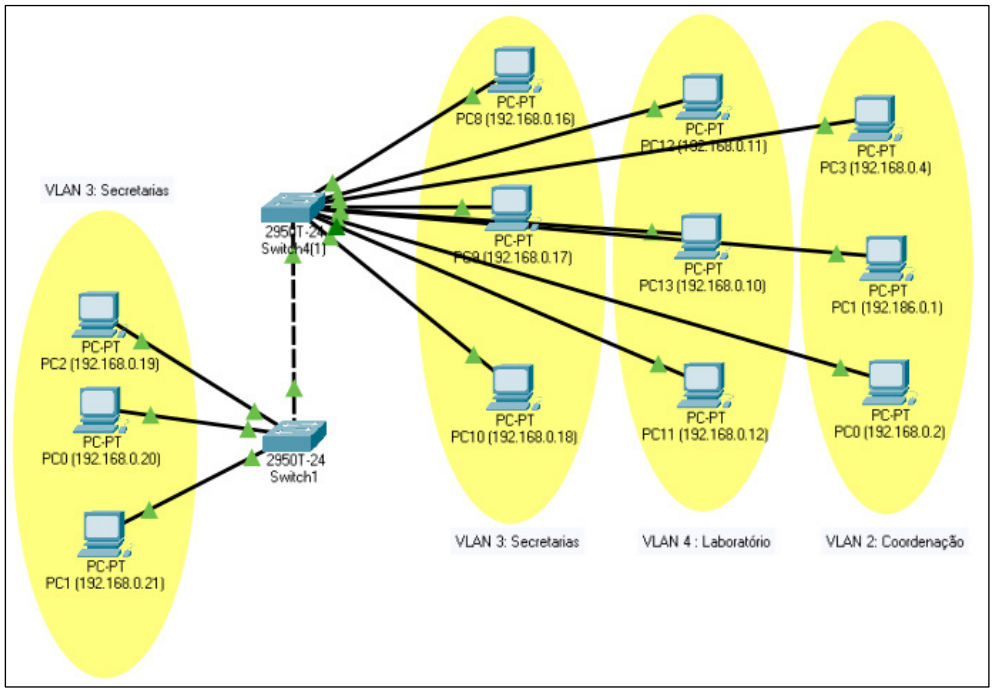


Fonte: Elaboração própria, 2021

O laboratório de informática passou a incorporar a estrutura de atendimento da xerox, com isso, houve a substituição de todos os computadores. E, deste modo, o servidor proxy foi desativado. E, partir de então, o laboratório passou a fazer parte da rede como o todo.

Diversos usuários acessando a rede do laboratório, gerou uma sobre carga, aumentando o fluxo de dados da rede. E, como alternativa, foi a inclusão do laboratório de informática em uma VLAN, para assim, limitar o acesso a sua respectiva VLAN.

Figura 14. Cenário da rede da UFPA/ Castanhal com VLAN.



Fonte: Elaboração própria (2021)

O gerenciamento da rede com a configuração de switches com suporte a VLAN, agrupa os usuários independentemente da topologia de rede, dessa maneira, um grupo de usuário ou departamento pode acessar dados compartilhados com seus respectivos departamentos, garantindo a integridade da informação.

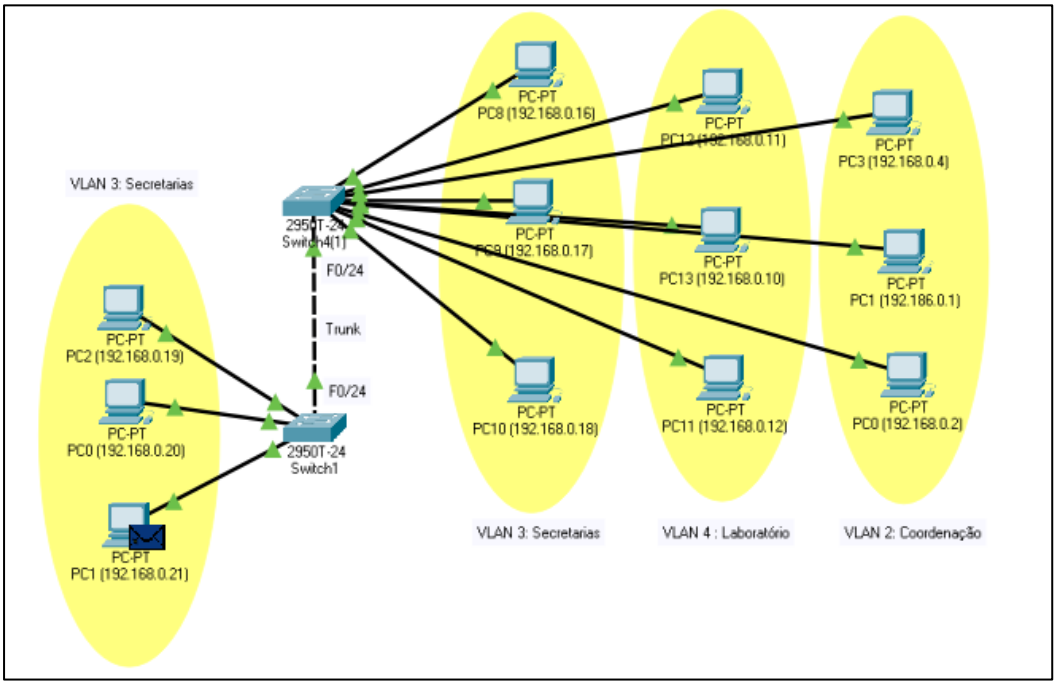
A VLAN é uma tecnologia para segmentar as redes virtualmente, uma função reconhecida pela maioria dos switches gerenciáveis. Isso pode ser feito dividindo-se os usuários da rede em grupos lógicos como é visto na figura 13. Apenas os usuários de um grupo específico podem trocar dados ou acessar determinados recursos da rede, que no caso, da UFPA/ Campus Castanhal, segmenta um ou mais usuários dos demais da rede, ganhando mais segurança e aumentando a performance na transmissão de dados.

Se um usuário compartilha dados em uma VLAN, apenas os usuários localizados nessa VLAN poderão acessar os dados compartilhados. Embora todos os computadores estejam em funcionamento no mesmo switch foram criados grupos diferentes, separadas por VLAN's. Dessa maneira, os participantes de um grupo, ou VLAN, conectados entre si, sem restrições.

Na simulação de rede, foi usado o simulador Packet Tracer – um programa que permite simular a rede, sendo possível adicionar tanto equipamentos de rede, como também computadores e periféricos, passível de configurações como em situações reais.

Na figura 15, mostra a rede segmentada nas VLAN 2: Coordenação, VLAN 3: Secretaria, VLAN 4: Laboratório. Por padrão todos computadores ficam alocados na VLAN 1 no switch.

Figura 15: Encaminhamento de pacotes ICMP

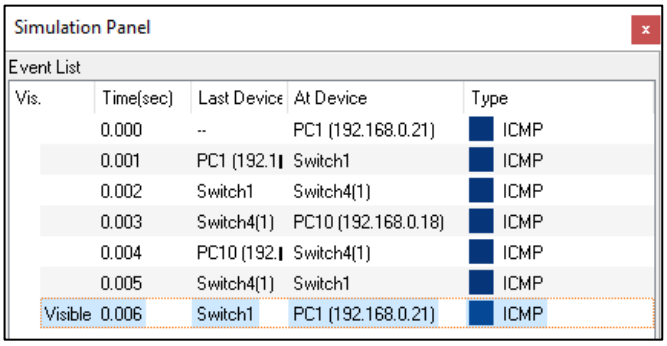


Fonte: Elaboração própria, 2021

Simulando a escalabilidade da rede, com a expansão de mais equipamento, configuradas na mesma VLAN, foi realizada o envio de pacotes de dados na rede, usando o protocolo ICMP, de acordo com a figura 15, e deste modo, foi possível fechar a comunicação entre computadores pertentes à mesma VLAN.

A simulação se comportou de maneira esperada, computadores de mesma VLAN, houve o encaminhamento e a recepção de dados. Mas, em VLAN distinta, a comunicação falhou.

Figura 15: Simulação de encaminhamento de pacotes ICMP

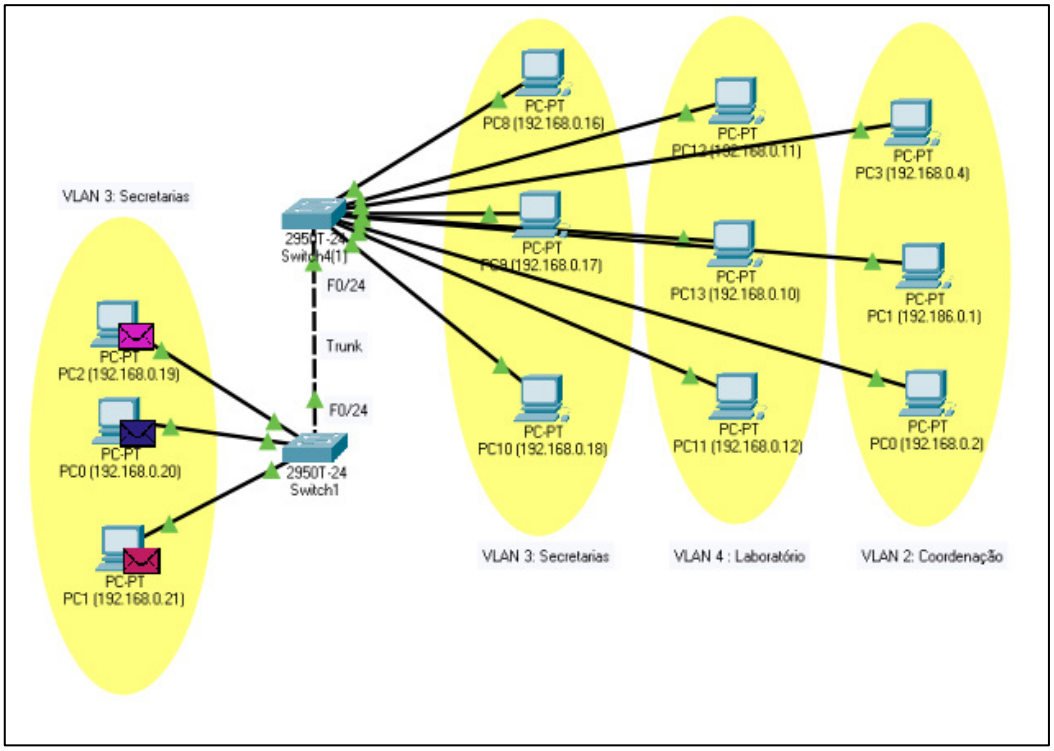


Fonte: Elaboração própria, 2021

Com as VLAN's também reduz o tráfego de broadcast e aumento de segurança, já que os dispositivos de uma VLAN só podem se comunicar com outros dispositivos na mesma VLAN. Além disso, as VLAN's ajudam no controle do tráfego e aumentam a eficiência da rede, por que cada VLAN pode ser organizada para conter somente aqueles dispositivos necessários para se comunicar com outra VLAN (DANTAS, 2010).

Na figura 16, mostra o envio de pacotes ICMP, para toda rede, mas é recepcionada por apenas, na VLAN correspondente. E, os dados encaminhados pelos computadores que iniciam a comunicação, não chega a disseminar na rede, falhando o encaminhamento de forma imediata.

Figura 16: Momento de envio de pacotes ICMP

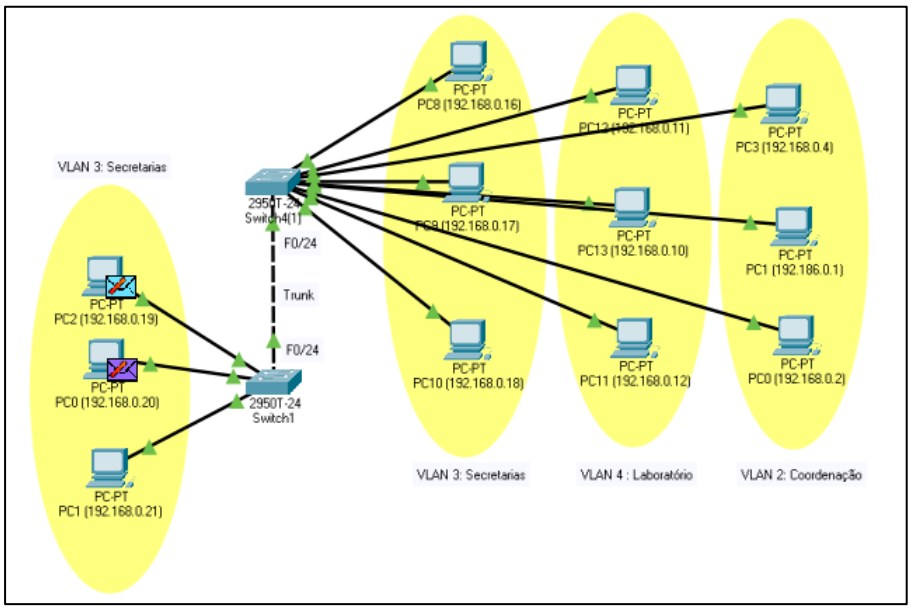


Fonte: Elaboração própria, 2021

Pensando na escalabilidade de um sistema, o modelo de rede com VLAN adapta-se muito, pois permite que equipamento em diferentes switches possam comunicar-se com suas respectivas VLAN's, sem a necessidade de mexer na infraestrutura presente. Com isso, a Universidade Federal do Pará pode economizar recursos públicos.

Na figura 17, mostra o descarte do pacote ICMP sendo descartado na rede, e aceito no computador que encaminhou o pacote.

Figura 17: O pacote ICMP é negado nos outros enquanto no receptor é aceito



Fonte: Elaboração própria, 2021

4.1 Desempenho da rede

Com a implementação de VLAN's, é criado uma rede lógica, que aumenta o controle de tráfego da rede, diminuir o alcance de disseminação de pacotes de difusão broadcast, melhorando assim o desempenho e a segurança da rede, pois os domínios de broadcast e multicast são direcionados a VLAN de onde originou, evitando assim sobrecarga da rede.

4.2 Redução de custo

O custo maior da rede deve-se à adaptação dos equipamentos aos utilizadores, compra de novos equipamentos, ajuste do cabeamento, entre outros. Muitas vezes, cada movimentação requer uma nova configuração de repetidores e roteadores, nova passagem de cabos e um novo endereçamento de rede.

Usando VLAN a configuração ou reconfiguração de redes é realizada através switches gerenciáveis, desta forma, a configuração de uma VLAN não requer o deslocamento ou conexão física dos equipamentos da rede. Dessa maneira, a Universidade Federal do Pará / Campus Castanhal economiza na reestruturação da rede de forma lógica, pois em vez de refazer a rede, a mesma permanece com todo o cabeamento estruturado, bastando adquirir os switches gerenciável com suporte a VLAN.

E assim, consegue diminuir os custos associados à uma rede local com grande número de estações, e realizar uma segmentação lógica, de maneira que seja possível endereçar os quadros enviados para novos domínios de broadcast.

5 CONCLUSÃO

A principal característica atribuída ao uso de redes locais virtuais é a possibilidade de se agrupar estações de usuários a uma ou mais Lans físicas para se formar um único domínio de difusão ou broadcast, garantindo a comunicação entre elas, mesmo que façam parte de segmentos físicos diferentes. Além desta, existem outras características importantes quando se avalia o uso de VLAN's.

Em uma rede não segmentada, computadores, impressoras e outros dispositivos conectados disseminam uma grande quantidade de pacotes de difusão, seja por falhas na conexão dos cabos, mau funcionamento de placas de rede, ou até mesmo por protocolos e aplicações que geram este tipo de tráfego, podendo causar atraso no tempo de resposta e lentidão na rede local.

As redes locais podem ser classificadas de acordo com seu agrupamento, isto é, reunindo os dispositivos que farão parte das mesmas VLANS. Estes agrupamentos podem ser definidos por intermédio das portas do comutador, pelos endereços físicos das interfaces de rede, endereço IP dos clientes, protocolos e também por uma combinação de alguns destes.

Como o agrupamento leva em conta apenas as portas do switch, não são considerados os dispositivos, utilizador ou sistema conectado à outra ponta. Outra forma de agrupamento de Vlans se faz através do endereço físico das interfaces de rede dos dispositivos. Neste método, o administrador de redes associa um endereço MAC de um dispositivo a uma determinada VLAN no switch. Assim os dispositivos podem ser movidos para qualquer localização, dentro da organização, que continuarão a fazer parte da mesma rede virtual, sem qualquer reconfiguração posterior.

Talvez um dos maiores inconvenientes desta modalidade de agrupamento é o fato de que, antes de se colocar em operação, devem-se cadastrar todos os endereços MAC dos dispositivos que serão conectados no switch e associá-los a suas respectivas VLAN's, o que, dependendo do tamanho da rede, pode dispender bastante tempo de trabalho. Outra limitação desta solução referese a impossibilidade de associar mais de uma VLAN para cada endereço MAC.

No modelo de VLANS, existe um domínio lógico de difusão por onde os pacotes de broadcast ou multicast são contidos e não se propagam a outras redes virtuais. Assim uma rede segmentada com Vlans cria vários subdomínios de difusão, diminuindo o tráfego de mensagens de difusão tanto na rede segmentada como na rede da organização em geral.

Com a implementação de Vlan na Universidade Federal Pará/ Campus Castanhal houve a melhora da performance, pois os broadcasts e multicasts são confinados a VLAN onde trafegam evitando congestionamentos. Outra característica é o fato de diminuir o número de estações que compartilham o mesmo canal lógico diminuindo o tempo de acesso.

A implantação de redes virtuais pode ser aplicada de acordo com grupos de trabalhos ou setores mesmo que estes grupos estejam em localizações físicas distintas, garantindo assim a segmentação lógica da rede. No exemplo do Campus Castanhal o departamento pode pertencer a uma VLAN diferente do restante da organização a fim de proteger informações sigilosas. Em outra situação, um setor que gera muito tráfego de rede pode fazer parte de outra VLAN a fim de melhorar o desempenho da rede de modo geral.

Outro quesito é a segurança, uma das características que mais é levada em conta quando se implementa VLAN's, permitindo que dispositivos localizados em diferentes segmentos físicos e em uma mesma VLAN possam se comunicar sem que dispositivos fisicamente vizinhos tenham acesso.

Os pacotes transmitidos são normalmente entregues somente ao endereço de destino dificultando a interceptação dos mesmos. Quando se trata de tráfego entre VLAN's, os pacotes são submetidos a um roteador, que possui diversas funcionalidades de filtragem, segurança e prioridade, antes de chegarem a seu suposto destino, criando assim domínios de segurança para acesso a recursos da rede.

O uso de comutadores combinado com VLAN's pode tornar a implementação mais atrativa se considerada a questão financeira. Usando-se VLAN's as migrações e reconfigurações são realizadas em nível de software, através da console de gerenciamento dos switches.

Contudo, com a segmentação da rede, os funcionários da UFPA/ Campus Castanhal demonstraram mais motivados ao trabalho, pois a rede tornou-se mais confiável, segura e eficaz.

6 REFERÊNCIAS

BAYS, L.R. et al. Segurança de Redes Virtuais: Fundamentos, Tecnologias e Tendências. In: XXX SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS, 264., 2012, Ouro Preto. **Anais**... Ouro Preto: SBRC 2012. p.59-93.

BOAVIDA, F., BERNARDES, M., VAPI, P. **Administração de Redes Informáticas.** Lisboa: FCA Editora, 2009.

CONCEIÇÃO, Miguel Alexandre Santos Gomes da. **Administração de uma infraestrutura informática ao nível de segurança e rede**. 2020. Tese de Doutorado. Universidade de Coimbra.

DANTAS, M. Redes de Comunicação e Computadores: abordagem quantitativa. Florianópolis: Visual Books, 2010.

DUARTE, Pedro José Mendes Nunes. **Ambiente virtual de redes orientado ao treino e educação**. 2019. Tese de Doutorado.

Kitchenham, B. e Charters, S. (2007) Guidelines for Performing Systematic Literature Reviews in Software Engineering. Relatório Técnico, EBSE 2007-001, Relatório Conjunto da Universidade Keele e da Universidade Durham.

KUROSE, J. F. **Redes de Computadores e a Internet: Uma abordagem top-down**, 5ª Ed. São Paulo: Pearson Education, 2010.

M. Smirnov, N. Spiricheva and V. Smirnova, "Network Sniffer for Time Tracking," 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), 2020, pp. 0471-0474, doi: 10.1109/USBEREIT48449.2020.9117635.
MENDES, Douglas Rocha. **Redes de computadores: teoria e prática**. Novatec Editora, 2020.
MORAES, A. F. D. **Segurança em Redes - Fundamentos**. São Paulo: Editora Érica, 2010.
ROSS, J. **Redes de Computadores**. 1ª Ed. Rio de Janeiro, RJ: Antenna Edições Técnicas, 2008.

SANDERS, Chris. **Análise de pacotes na prática: Usando Wireshark para solucionar problemas de rede do mundo real**. Novatec Editora, 2017.

SECLEN, J. L. T. **Projeto, Verificação Funcional e Síntese de Módulos Funcionais para um Comutador Gigabit Ethernet** - Porto Alegre, BR-RS, 2011. 128 f. Dissertação (Mestrado em Microeletrônica) - Universidade Federal do Rio Grande do Sul. Programa de Pós-Graduação em Microeletrônica, Porto Alegre, BR-RS, 2011.
STALLINGS, W. Criptografia e Segurança de Redes: Princípios e Práticas, 4ª Ed. São Paulo: Editora Peason, 2007.

TANENBAUM, A. S. **Redes de computadores**, 5ª Ed. São Paulo: Pearson Education, 2011.