UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO SEMIPRESENCIAL EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

MARCOS CESAR RIBEIRO

PROJETO HIERÁRQUICO DE SEGMENTAÇÃO DE REDES EM UMA CLÍNICA DE ONCOLOGIA APLICANDO BOAS PRÁTICAS DE IMPLEMENTAÇÕES DE REDES

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2020

MARCOS CESAR RIBEIRO

PROJETO HIERÁRQUICO DE SEGMENTAÇÃO DE REDES EM UMA CLÍNICA DE ONCOLOGIA APLICANDO BOAS PRÁTICAS DE IMPLEMENTAÇÕES DE REDES

Monografia de Especialização, apresentada ao Curso de Especialização Semipresencial em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica – DAELN, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. M. Sc. Fabiano Scriptore de Carvalho

CURITIBA
2020

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Câmpus Curitiba

Diretoria de Pesquisa e Pós-Graduação
Departamento Acadêmico de Eletrônica
Curso de Especialização Semipresencial em Configuração e Gerenciamento de Servidores e Equipamentos de Redes

TERMO DE APROVAÇÃO

PROJETO HIERÁRQUICO DE SEGMENTAÇÃO DE REDES EM UMA CLÍNICA DE ONCOLOGIA APLICANDO BOAS PRÁTICAS DE IMPLEMENTAÇÕES DE REDES

por

MARCOS CESAR RIBEIRO

Esta monografia foi apresentada em 13 de Outubro de 2020 como requisito parcial para a obtenção do título de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. M. Sc. Fabiano Scriptore de Carvalho
Orientador

_____
Prof. Dr. Kleber Kendy Horikawa Nabas
Membro titular

_____
Prof. M. Sc. Omero Francisco Bertol
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

Dedico este trabalho a minha esposa e filhas, pela paciência e compreensão nas horas ausentes.

AGRADECIMENTOS

Certamente estes parágrafos não irão atender a todas as pessoas que fizeram parte desta importante fase da minha vida. Portanto, desde já peço desculpas àquelas que não estão presentes entre estas palavras, mas elas podem estar certas de que fazem parte do meu pensamento e de minha gratidão.

Agradeço primeiramente a Deus, aos Professores e a todas as pessoas que contribuíram para elaboração deste trabalho.

Agradeço ao meu orientador Prof. M. Sc. Fabiano Scriptore de Carvalho, pela sabedoria com que me guiou nesta trajetória e pelo aceite desse projeto.

Deixo aqui também o meu agradecimento aos meus colegas de classe pelo companheirismo e pelo conhecimento adquirido nesse período.

A coordenadoria do curso representada pelo Prof. Dr. Kleber Kendy Horikawa Nabas pela disposição, atenção e conhecimento disposto.

Aos demais docentes que colaboraram no desenvolvimento do meu aprendizado e crescimento profissional, sem hesitar em nos transmitir seus conhecimentos.

Deixo também registrado, o reconhecimento a minha família, pois acredito que sem o apoio deles seria muito difícil vencer este desafio.

Enfim, a todos os que por algum motivo contribuíram para a realização desta pesquisa.

Quanto mais aumenta nosso
conhecimento, mais evidente fica nossa
ignorância.

(KENNEDY, John F., 1962)

RESUMO

RIBEIRO, Marcos César. **Projeto hierárquico de segmentação de redes em uma clínica de oncologia aplicando boas práticas de implementações de redes**. 2020. 91 p. Monografia de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2020.

Esta monografia apresenta uma solução para integrar duas redes distintas, que se encontra em uma clínica de Oncologia, ambas em funcionamento, mas em decorrência de obsolescência de hardware, e o gerenciamento das redes sendo executado a parte, sentiu-se a necessidade da integração e buscou-se o estudo de uma solução que atendesse as particularidades de cada uma, ficando assim mais gerível. Após pesquisa e simulação em aplicativo, chegou-se à conclusão de que a implementação da rede segmentada em Redes Virtuais Locais (VLANs) e ambientalizá-las em um único datacenter e domínio, mantendo-o seguro, integro e sem perda de desempenho, seria uma boa prática de implementação. Para isso foram utilizadas tecnologias de protocolos VTP, STP, um servidor DHCP para designar o pool de cada VLAN. Foram desativadas as portas em desuso nos switches, implementada a segurança sticky, senhas seguras (seguindo os critérios de segurança recomendados). A implementação destas técnicas não exigiu um alto investimento financeiro. Por fim a nova topologia proposta segmentada em VLANs atende as necessidades da clínica, nos quesitos segurança, desempenho e eficiência, não comprometendo sua escalabilidade.

Palavras-chave: Segmentação. VLAN. DHCP. ACL.

ABSTRACT

RIBEIRO, Marcos César. **Hierarchical network segmentation project in an oncology clinic applying good practices for network implementations**. 2020. 91 p. Monografia de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2020.

This monograph presents a solution to integrate two different networks, which is found in an Oncology clinic, both in operation, but due to hardware obsolescence, and the management of the networks being carried out separately, the need for integration was felt and we sought to study a solution that would meet the particularities of each one, thus becoming more manageable. After research and application simulation, it was concluded that the implementation of the segmented network in Virtual Local Area Networks (VLANs) and environmentalizing them in a single datacenter and domain, keeping it safe, complete and without loss of performance, would be good implementation practice. For this, VTP, STP protocol technologies, a DHCP server were used to designate the pool for each VLAN. Disused ports on the switches were disabled, sticky security and secure passwords were implemented (following the recommended security criteria). The implementation of these techniques did not require a high financial investment. Finally, the proposed new topology segmented in VLANs meets the clinic's needs, in terms of safety, performance and efficiency, without compromising its scalability.

Keywords: Segmentation. VLAN. DHCP. ACL.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

CO	Conhecimento Organizacional
Gb	Gibabyte
Mbps	Megabits por segundos
Tb	Terabyte

LISTA DE SIGLAS

ARP	*Address Resolution Protocol*
CAM	*Content Address Table*
CSMA/CD	*Carrier Sense, Multiple Access with Collision Detection*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name Server*
ERP	*Enterprise Resource Planning*
IEEE	*Institute of Electrical and Electronic Engineers*
IP	*Internet Protocol*
ISSO	*International Standards Organization*
LACP	*Link Aggregation Control Protocol*
LAN	*Local Area Network*
LLC	*Logical Link Control*
MAC	*Media Access Control*
MSSQL	*Microsoft Structured Query Language*
NVRAM	*Non-Volatile Random Access Memory*
OSI	*Open System Interconnection*
PERC	*PowerEdge RAID Controller*
RAID	*Redundant Array of Independent Disks*
RAM	*Random Access Memory*
SAS	*Serial Attached SCSI*
SCSI	*Small / Computer Systems Interface*
SNMP	*Simple Network Management Protocol*
STP	*Spanning Tree Protocol*
TCP	*Transmission Control Protocol*
TCP/IP	*Transmission Control Protocol over Internet Protocol*
UTP	*Unshielded Twisted Pair*
VLAN	*Virtual Local Access Network*
VLAN-ID	*VLAN (Virtual Local Access Network) Identification*
VTP	*VLAN (Virtual Local Access Network) Trunking Protocol*

SUMÁRIO

1 INTRODUÇÃO

A finalidade desta monografia é apresentar uma solução para a unificação de duas redes distintas, uma utilizada no planejamento e tratamento radioterápicos (FÍSICA) e outra rede corporativa (CLÍNICA). Neste estudo será abordado, os principais aspectos para implementação do projeto de rede segmentada em VLANs, como topologia, hierarquia, protocolos, segurança e segmentação. Ao final é esperado que este trabalho sirva de base teórica na referência para as discussões e entendimento na tomada de decisão sobre a tecnologia abordada e contribuir para um melhor entendimento e concepção das práticas a serem adotadas no planejamento de novas infraestruturas de redes estruturadas e segmentadas.

1.1 PROBLEMA

A presente monografia tem como foco na reestruturação da rede de computadores de uma clínica médica (Oncologia). Atualmente a clínica possui duas redes distintas, a primeira sofre principalmente com a obsolescência de seu servidor, tendo onze anos de uso, falta espaço de armazenamento, dificuldades em reposição de peças (fontes de alimentação, disco rígido, etc.) e de disposição no local (sem refrigeração adequada e redundância na rede elétrica). Os processos executados nesse setor precisam ser precisos, confiáveis e seguros, pois trata de cálculos e definições sobre o melhor local para a aplicação e a quantidade da dosagem radioterápica no paciente. Já a segunda sofre com a constante realocação de equipamentos, dispositivos de terceiros conectados (roteadores Wi-Fi e notebooks) a rede, sem o conhecimento e consentimento do administrador. Muitas vezes a conexão destes dispositivos na rede podem provocar problemas, causando a queda no desempenho da rede e fazendo com que a taxa de transmissão utilizada pelos hosts na rede fique menor. Um outro problema importante relacionado aos equipamentos de terceiros conectados na rede é o comprometimento na segurança das informações, já que estes equipamentos podem estar infectados por algum *ransomware, malware*, vírus de computadores e afins. Existe também a possibilidade de algum usuário instalar um analisador de protocolos (*Sniffer*) para vasculhar os pacotes que estão trafegando pela rede, e procurando por possíveis dados importantes, como por exemplo senhas que são enviadas utilizando

protocolos sem criptografia, como o Telnet, por exemplo. Estes problemas podem levar a um sequestro, corrompimento ou destruição de dados.

Outro problema levantado é o domínio de broadcast único existente na rede atual. Em uma rede com esta configuração, todos os hosts terão conectividades entre si. Isto pode acarretar problemas de segurança e vulnerabilidade de ataques a esse tipo de rede. Nas redes com um único domínio de broadcast, *switches* propagam mensagens de broadcast para todos os seus segmentos causando queda no desempenho da rede (FILIPPETTI, 2019, p. 90).

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Fazer um levantamento da situação topológica atual, da infraestrutura de redes da CLÍNICA e propor uma reestruturação dos projetos de redes física e lógica, com uma topologia unificada, com segmentações a serem implementadas, juntamente, com algumas medidas a serem aplicadas para dificultar o comprometimento da integridade e da segurança das informações, e com isto, melhorar o desempenho da infraestrutura da rede proposta.

1.2.2 Objetivos Específicos

Para atender ao objetivo geral neste trabalho de conclusão de curso de especialização os seguintes objetivos específicos serão abordados:

- Fazer um levantamento da situação atual da infraestrutura da rede da clínica;
- Fazer um projeto de reestruturação física e verificar os elementos de camada 1 (camada física) da rede atual;
- Fazer um projeto de reestruturação lógica da rede, segmentando a rede em VLANs para separar os diversos setores da Clínica;
- Fazer a implementação do projeto físico e lógica na estrutura de redes, unificando as redes atuais em uma única rede segmentada;
- Implementar mecanismos de segurança na rede implementada, para que possa evitar possíveis ataques de invasores;

- Apresentar os benefícios com a reestruturação dos projetos físico e lógica da rede implementada.

1.3 JUSTIFICATIVA

O problema tratado na monografia ocorre em uma Clínica de oncologia que atualmente tem a estrutura dividida em duas redes distintas e a rede não está estruturada corretamente do ponto de vista de desempenho e segurança. A primeira rede de computadores da Clínica é o departamento responsável pelo planejamento do tratamento radioterápico (FÍSICA), onde existem cálculos e planejamento para definir a melhor região para ser aplicada a dosagem de radioterapia nos pacientes com a menor evasividade possível. Esta rede enfrenta problemas em seu servidor, além de ser obsoleto (11 anos) sua disposição não é correta conforme as normas técnicas, não tendo refrigeração e nem redundância elétrica. Existe também a questão de armazenamento de dados, que está no limite e necessita de gerenciamento e monitoramento ativos. Visando a necessidade e a solução para estes problemas, foi almejada a integração com a rede da clínica (CLÍNICA). Esta, por sua vez, apresenta outros problemas como o seu crescimento desordenado, com novos departamentos, trocas constantes na setorização dos equipamentos, além da conexão de outros tipos de equipamentos (roteadores Wi-Fi, notebooks, etc.) em seu parque. Isto leva ao comprometimento da segurança e estabilidade, sendo sujeito a contaminação por pragas virtuais (*ransomware*, *malware*, vírus, *sniffers*, etc.), sequestrando informações, corrompendo arquivos, causando lentidão e em alguns casos a interrupção de serviços. Visto todos os problemas levantados com a infraestrutura de redes atual, é imprescindível um novo projeto físico e lógico da rede, para possível implementação e reestruturação da rede, para que os problemas existentes possam ser minimizados.

Para manter a integridade e segurança da rede FÍSICA e solucionar os problemas da rede CLÍNICA, foram feitos pesquisas e testes no simulador de redes Cisco Packet Tracer, da Cisco Systems. Visto que este simulador permitirá a simulação da infraestrutura de redes que será projetado, será possível fazer os testes e configurações dos equipamentos antes da implementação real, evitando assim qualquer problema na hora da implementação real. O investimento para aplicação dessa solução é considerável em vista de outras soluções encontradas.

1.4 ESTRUTURA DO TRABALHO

Esta monografia de especialização está dividida em quatro capítulos. Neste primeiro capítulo foi introduzido o assunto tema do trabalho, a motivação, os objetivos gerais e específicos, a justificativa e a estrutura geral do trabalho.

O segundo capítulo, aborda o referencial teórico, com os conceitos importantes que irão servir de embasamento para o desenvolvimento do trabalho.

O terceiro capítulo será o desenvolvimento do trabalho, com o projeto físico e lógica da reestruturação da infraestrutura de redes da clínica.

O capítulo quatro apresenta as conclusões e considerações finais da monografia.

2 REFERENCIAL TEÓRICO

Este capítulo aborda os conceitos de redes de computadores, protocolos e equipamentos que servirão de base para o desenvolvimento do trabalho.

2.1 REDES DE COMPUTADORES

O conceito de redes de computadores é central nesta monografia. As redes de computadores são formadas por pelo menos dois equipamentos interligados por um meio de transmissão, que pode ser guiado (cabo UTP, fibra optica) ou não guiado (sem fio). As infraestruturas de redes de computadores funcionam para compartilhar recursos como impressoras, enlaces para a Internet Pública e discos rígidos. Atualmente as redes de computadores se tornaram essenciais nas empresas, facilitando o acesso às informações e agilizando processos. Em relação às redes de computadores, é importante enfatizar que o seu surgimento teve como principal fator a necessidade de diminuição de custos, o aumento da produtividade, a confiabilidade e o compartilhamento de recursos físicos (impressoras) e informações (banco de dados). Também é importante enfatizar que o seu surgimento foi devido ao interesse das pessoas em simplificar suas atividades, compartilhar e buscar informações.

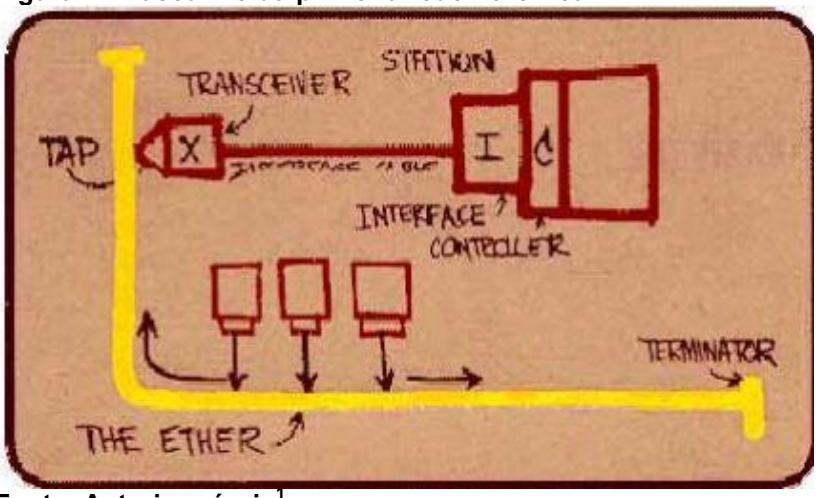
Segundo Tanenbaum e Wetherall (2011, p. 19), se ninguém estivesse interessado em redes de computadores, poucas delas seriam elaboradas. As redes de computadores são elementos essenciais nas empresas e organizações. A necessidade de diminuir custos, aumentar a confiabilidade, disponibilizar o compartilhamento de recursos físicos e informações (banco de dados, sistemas integrados de gestão, etc.) fez surgir a rede de computadores.

Utilizar boas práticas nas implementações de redes pode auxiliar o administrador a ter uma maior gerenciabilidade na estrutura. Atualmente o padrão IEEE 802.3 e suas variantes (Fast Ethernet, Gigabit Ethernet, etc.) estão sendo utilizados para a implementação das redes locais (LANs) das empresas.

2.2 REDE ETHERNET

O seu surgimento deu-se no ano de 1972, em um dos laboratórios da Xerox, através de Robert Metcalfe. O laboratório da Xerox possuía estações compartilhando o mesmo meio de transmissão, um cabo coaxial; a configuração utilizada para esta conexão foi a de barramento com uma taxa de transmissão de 2,94 Mbps. Anteriormente o padrão era conhecido como “Network Alto Aloha”. Robert Metcalfe queria deixar claro que o padrão desenvolvido por ele poderia suportar qualquer computador fora de seus laboratórios. Pode-se verificar na Figura 1 o primeiro rascunho da rede Ethernet, com as interfaces o meio de transmissão e o transceiver interligando as estações ao meio de transmissão. Na implementação do Ethernet havia um único domínio de broadcast e o tipo de rede era interligado via um barramento com cabo coaxial, que conectava todos os hosts em um meio de transmissão comum para todos os computadores na rede.

Figura 1 - Rascunho da primeira rede Ethernet



Fonte: Autoria própria[1]**.**

2.2.1 Padrão IEEE 802.3

A Ethernet nasceu como uma tecnologia proprietária, sendo a Xerox a empresa que detinha todos os direitos sobre a tecnologia. Durante o período de desenvolvimento do Ethernet, somente a Xerox poderia implementar redes com esta tecnologia. Em meados da década de 1980, a tecnologia Ethernet foi enviada para o

[1] Fonte: **Acervo digital**. Programa de Pós-graduação em Tecnologia e Gestão em Educação a Distância. Disponível em: <http://www.ead.ufrpe.br/acervo-digital-eadtec/node/780>. Acesso em: 10 set. 2020.

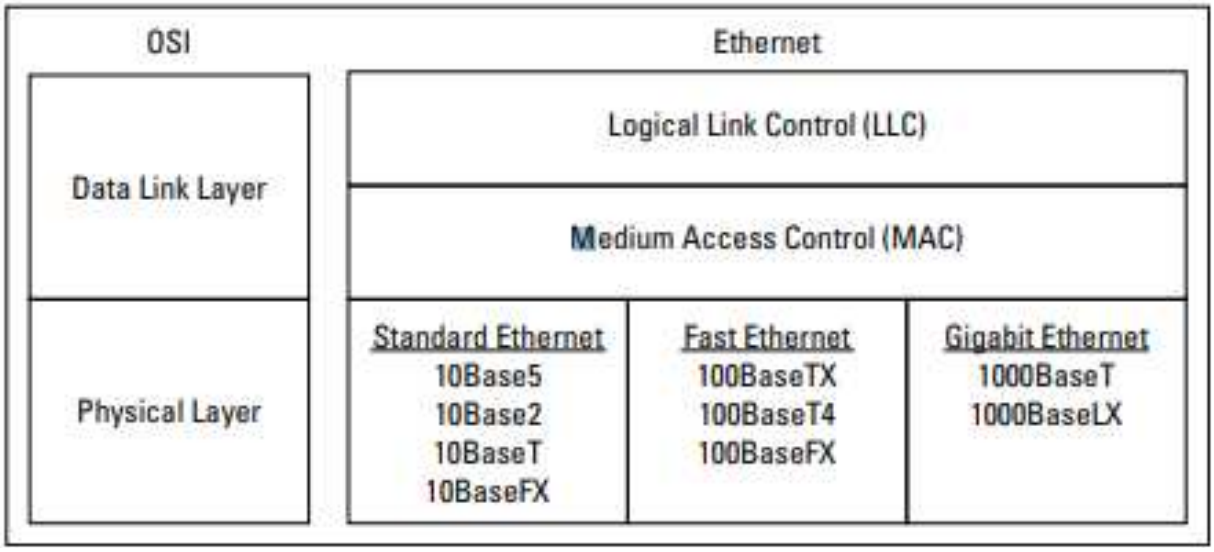
Institute of Electrical and Electronics Engineers (IEEE) para ser padronizada. Com este processo, nasceu o Padrão IEEE 802.3, que determinava um padrão aberto de redes locais que utilizava uma taxa de transmissão de 10Mbps, a princípio em uma rede em barramento, utilizando cabos coaxiais (10base2 e 10base5). A importância da padronização da rede Ethernet é que, a partir daquele momento, qualquer empresa que quisesse fabricar equipamentos com base no padrão IEEE 802.3 poderia fazer, sem ter que pagar royalties para uma determinada empresa. Isto fez com que os preços dos equipamentos, placas de redes, conectores, fossem reduzidos. Uma outra vantagem de se utilizar um padrão aberto é que não existe um único fabricante que disponibiliza os dispositivos/cabos/conectores, etc. Com o decorrer do tempo houve atualizações no padrão IEEE 802.3, e surgiram outros padrões como o IEEE 802.3u (Fast Ethernet), o IEEE 802.3ab (Gigabit Ethernet) e outras variantes. Estes padrões que surgiram disponibilizaram taxas de transmissões mais altas nas conexões de redes (100 Mbps, 1 Gbps) além de utilizar vários tipos de meios de transmissão (cabos de par trançado UTP, fibras ópticas). A importância de definir o padrão IEEE 802.3 no trabalho é porque toda a implementação da reestruturação da rede terá como base este padrão aberto. Todos os switches, roteadores, placas de redes irão utilizar este padrão para a comunicação com os hosts e equipamentos na rede.

O padrão 802.3 usa o conceito de detecção de colisão, chamada *Carrier Sense, Multiple Access with Collision Detection* (CSMA/CD), onde todos os computadores da rede compartilham um mesmo cabo. Ainda segundo ele é o protocolo mais comum para a transmissão de dados na rede. Em geral quando usamos o termo protocolo de rede normalmente estamos nos referindo a protocolos que trabalham nas camadas 3 e 4 do modelo OSI, como o TCP/IP.

A Ethernet opera nas duas primeiras camadas do modelo OSI: Físico e Enlace. No entanto, a Ethernet divide a camada de Enlace em duas camadas separadas, conhecidas como camada *Logical Link Control* (LLC) e *Medium* Camada de controle de acesso (MAC) (LOWE, 2011, p. 34).

A Figura 2 mostra como os vários elementos de Ethernet corresponde ao modelo OSI.

Figura 2 - Os vários elementos de Ethernet



Fonte: Lowe (2011).

2.2.2 Padrão IEEE 802.3u

Segundo Lowe (2011), o padrão IEEE 802.3u comumente chamada de Fast Ethernet, tem a sua taxa de transmissão 10x maior que a taxa de transmissão da tecnologia ethernet padrão (IEEE 802.3), chegando a taxa de transferência de 100 Mbps. A seguir serão apresentadas as três variedades de ethernet:

- **100BaseT4**: esse protocolo permite velocidades de transmissão de 100 Mbps no mesmo cabo UTP das redes 10BaseT. Para fazer isso, o padrão utiliza todos os quatro pares de fios no cabo;
- **100BaseTX**: atualmente é o padrão mais usado para redes locais de computadores (LANs), transmitindo a 100 Mbps em apenas dois pares de cabo metálico de par trançado (UTP). O cabo de par trançado (*Unshielded Twisted Pair Cable*) utiliza um conector RJ-45 e é uma opção mais barata que a implementação utilizando cabos de fibra optica;
- **100BaseFX**: é a versão ethernet rodando a 100 Mbps por segundo utilizando fibra optica, não sendo muito utilizado pelo seu custo e complicações em sua instalação.

2.2.3 Padrão IEEE 802.3ab

O padrão IEEE 802.3ab, comumente chamado de Gigabit Ethernet, pode transmitir até cem vezes mais rápido que a Ethernet original, que utilizava uma taxa de transmissão de 10 Mbps. A implementação de dispositivos que utilizam este padrão é consideravelmente mais caro que a utilização do padrão IEEE 802.3u (Fast Ethernet). Este padrão é utilizado quando o desempenho aprimorado justifica o custo extra.

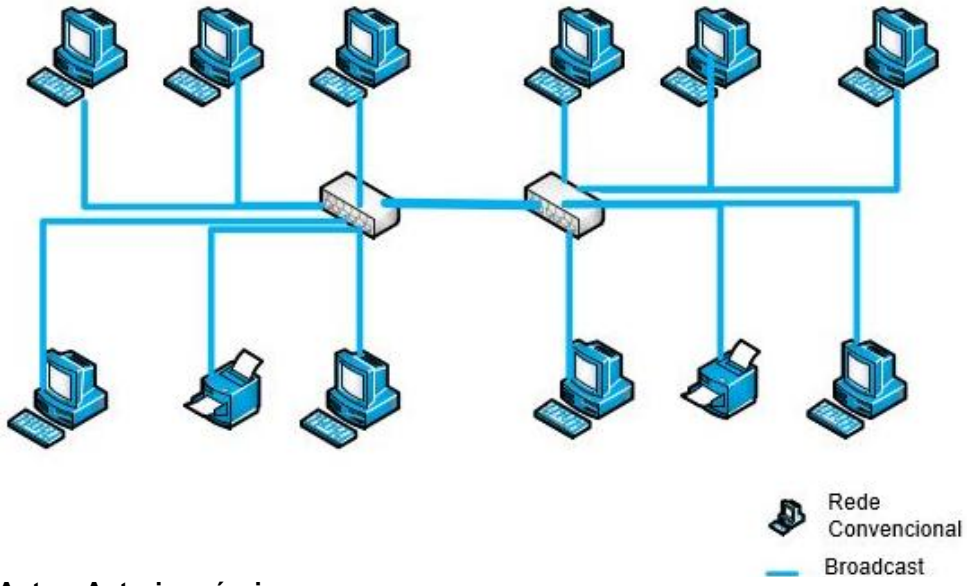
O padrão IEEE 802.3ab é dividido em duas versões:

- **1000BaseT**: pode ser implementado com a utilização de cabos de par trançado não blindado (UTP), sendo melhor sua implementação com a utilização de cabos UTP de categoria 5e ou Categoria 6, porque são mais confiáveis;
- **1000BaseLX**: existe uma grande variedade de cabos de fibra usadas com o padrão IEEE 802.eab (Gigabit Ethernet), mas o mais popular é chamado 1000BaseLX.

2.3 REDES VIRTUAIS LOCAIS (VLANS)

Segundo Filippetti (2019), o surgimento de Redes Locais Virtuais (*Virtual Local Area Network* - VLANs) seria uma resposta a problemas encontrados em uma rede convencional (*Local Area Network* - LAN), como desempenho e segurança. Em referência ao desempenho, pode-se verificar na Figura 3 uma estrutura de redes interligadas por switches e uma rede não segmentada. Todos os dispositivos conectados como computadores, impressoras e outros disseminam uma grande quantidade de pacotes de difusão (*broadcasts*). Quanto maior o número de dispositivos conectados, maior será o atraso no tempo de resposta que implicará no desempenho da rede, causando com isto, lentidão.

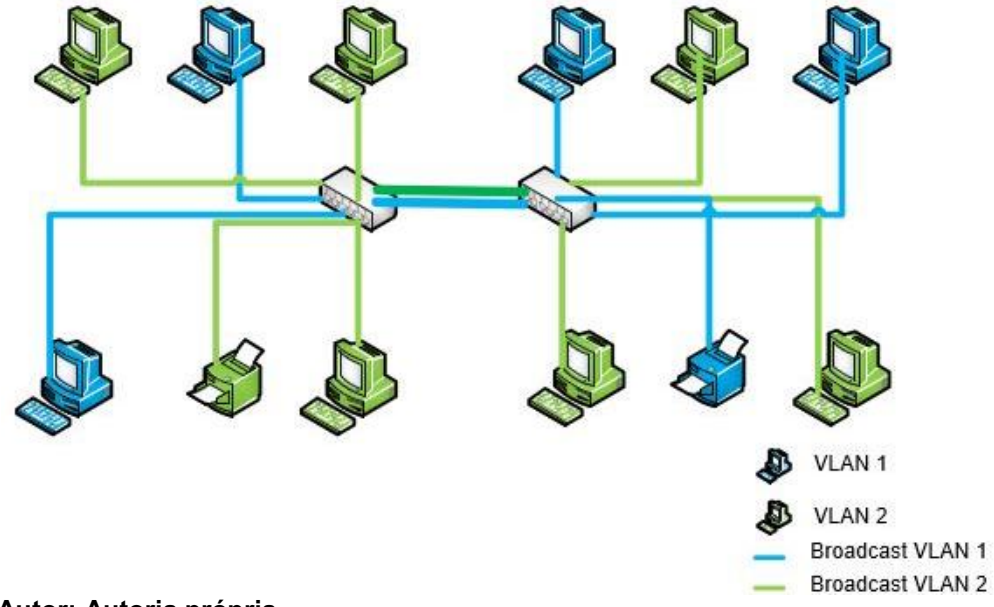
Figura 3 - Rede convencional



Autor: Autoria própria.

Na Figura 4 pode-se verificar a implementação de uma infraestrutura de redes com LANs Virtuais (VLANs). Neste modelo existe um domínio logico de difusão onde os pacotes de broadcast[2] ou multicast[3] ficam contidos na VLAN de origem, não se propagando para as demais LANS Virtuais (VLANs). Uma rede segmentada em VLANs cria vários subdomínios de difusão, diminuindo o tráfego tanto na rede segmentada como na rede organizacional.

Figura 4 - Redes locais virtuais (VLANs)



Autor: Autoria própria.

[2] Broadcast: Envia mensagens para todo os dispositivos conectados a rede.
[3] Multicast: Envia mensagens para alguns ou um grupo de dispositivos a rede.

2.3.1 Classificação de VLANs

As Redes Locais Virtuais (*Virtual Local Area Network* - VLANs) podem ser classificadas de acordo com seu agrupamento e a forma como seus dispositivos serão agrupados. Estes agrupamentos podem seguir um modelo ou uma combinação deles. Nas subseções a seguir serão apresentados três modelos de agrupamentos.

2.3.1.1 Agrupamento por portas

Este tipo de agrupamento por portas não leva em consideração os dispositivos, o sistema ou o usuário conectado a outra extremidade. Neste agrupamento, cada porta ou range de portas no switch é associado a uma ou mais VLANs. Definindo por exemplo que as portas de 2 a 8 de um switch de 24 portas faça parte da “VLAN 10”, enquanto as portas 9,11,15 e 16 pertencem a “VLAN 20”, as demais portas não designadas farão parte da VLAN nativa[4], que pode ser definida pelo administrador.

Barros (2007) indica que no uso desta técnica, a porta é associada a uma determinada VLAN sem levar em conta o utilizador ou o sistema conectado à porta, mesmo que sejam oriundos de edifícios ou pisos diferentes.

2.3.1.2 Agrupamento por endereço físico (MAC)

Nesse método, independentemente de qual porta se conecte o dispositivo ele sempre fara parte da VLAN designada. O administrador irá associar o endereço físico (MAC) do dispositivo a uma VLAN no switch.

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 VLANs, o que, dependendo do tamanho da rede, pode dispender bastante tempo de trabalho. Outra limitação desta solução refere-se a impossibilidade de associar mais de uma VLAN para cada endereço MAC (HAFFERMANN, 2009).

---

[4] Vlan Nativa: é a VLAN que não recebe TAG ao atravessar uma porta tronco, por padrão é a VLAN 1.

2.3.1.3 Agrupamento por endereço IP

Outra forma seria o agrupamento por meio dos seus endereços ou sub-redes IP. Alguns fornecedores de VLANs usam o endereço IP de 32 bits como característica de participação sendo possível determinar a uma VLAN, dispositivos com IP específico (FOROUZAN, 2010, p. 461). Por exemplo, os dispositivos com os blocos de IPs 10.0.0.11,10.0.0.12 e 10.0.0.13 poderiam pertencem à VLAN3. Porém é preciso tomar cuidado com a política de distribuição de IP, tanto de forma manual quanto de reserva atribuída aos endereços físicos no servidor DHCP, que podem ocasionam uma ação extra de trabalho para o gerenciamento dos endereços, esgotando-os e impossibilitando a conexão de novos dispositivos.

2.3.2 Vantagem no Uso de VLANs

Um dos pontos fortes para a sua implementação é o desempenho e a segurança que as VLANs oferecem na implementação da estrutura de redes. Nas subseções a seguir, serão discutidos os principais pontos da utilização de VLANs.

2.3.2.1 Desempenho

Visto que em uma rede comutada, comumente sendo descrita como um domínio de broadcast, todos os quadros de difusão disseminados nela serão enviados a todos os dispositivos conectados, podendo acarretar assim, perda de desempenho neste domínio de broadcast. Com a implementação de VLANs, este domínio de broadcast será segmentado, dividido, e os quadros gerados devem ficar contidos somente na VLAN onde estes quadros forem gerados. Um switch de camada de enlace consegue fazer a comutação por meio do endereço físico (MAC) de destino. Diferente do Hub, que trabalha na camada física, o switch de camada enlace consegue comutar somente para o endereço de destino, não sobrecarregando a rede. Com a implementação de VLANs, os quadros enviados por broadcast também ficarão somente no domínio de broadcast de cada VLAN, fazendo com que menos quadros sejam enviados para as portas do switch.

Quanto maior o número de usuários e dispositivos em uma rede comutada, maior o volume de frames broadcast em trânsito nesta rede e, consequentemente, menor o seu desempenho (FILIPPETTI, 2019, p.89).

2.3.2.2 Segurança

O segundo motivo para sua aplicação é garantir a segurança da rede. Neste caso, cria-se uma barreira onde os quadros devem ficar contidos na VLAN que o originou, mantendo garantia absoluta e evitando problemas entre si. Outro fator importante que deve ser levado em consideração é a ação de um possível invasor da rede, que pode ter acesso a servidores e equipamentos de redes. Se o computador do possível invasor estiver em uma VLAN, ele não poderá acessar equipamentos e servidores de outra VLAN por meio de um switch de camada de enlace. Existe a possibilidade de roteamento entre VLANs por meio de switches multicamadas ou de roteadores. A implementação destes equipamentos faz com que os diferentes departamentos tenham conectividade entre si. O administrador de redes deve levar em conta a aplicação de políticas de segurança nestes equipamentos para evitar que possíveis invasores tenham acesso na rede utilizando mecanismos de segurança. A implementação de VLANs também pode ajudar na segurança em relação à disseminação de um vírus na infraestrutura da rede, pois os quadros enviados ficariam confinados na sua própria VLAN, sem afetar as demais. A criação e utilização de VLANs é importante porque com a segmentação, pode-se ter vários departamentos utilizando um único switch de camada de enlace, e se for utilizado VLANs, pode-se separar estes departamentos por LANs virtuais. Assim, um computador que está conectado ao SwitchA e associado a VLAN 10 não terá acesso direto ao servidor do RH que está na VLAN 20, por meio de um switch de camada 2.

As VLANs fornecem uma medida extra de segurança. Pessoas pertencentes ao mesmo grupo podem enviar mensagens de broadcast com absoluta garantia de que os usuários nos demais grupos não receberão essas mensagens (FOROUZAN, 2010, p. 463).

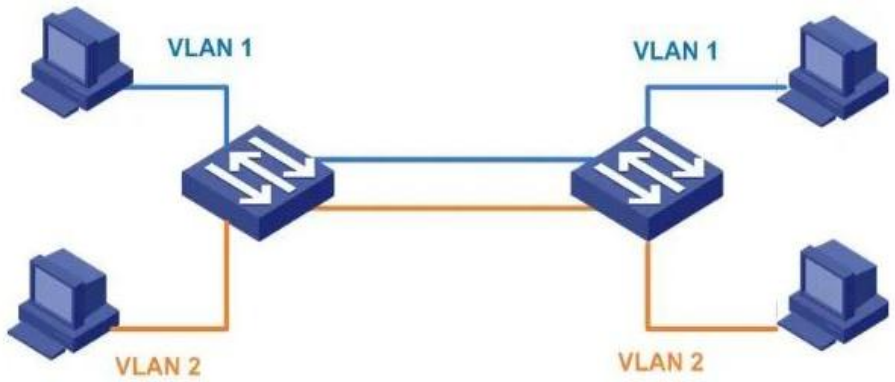
2.4 PROTOCOLOS

2.4.1 Protocolo IEEE 802.1q (dot1q)

No projeto inicial do padrão IEEE 802.3 não existia nenhum campo para indicar as informações de LANs virtuais (VLANs). Isto se deve ao fato de que naquela época as redes funcionavam somente com um único domínio de broadcast. O conceito de VLANs surgiu algum tempo depois, justamente para melhorar o

desempenho e a segurança das redes. Como o quadro do padrão IEEE 802.3 e as suas variantes não sofreu modificação, foi necessário criar um protocolo para incluir um campo no quadro para que fossem definidas informações das VLANs utilizadas. O IEEE 802.1q (Dot1Q) é um protocolo aberto, ou seja, pode ser utilizado por vários fabricantes diferentes, e serve para incluir o campo com a identificação da VLAN (VLAN-ID). Assim, quando é implementado um switch com várias VLANs, e este switch deve se conectar a outro switch por meio de um enlace de tronco, é necessário configurar o protocolo IEEE 802.1q neste enlace, para que seja feita a marcação da identificação da VLAN no quadro que vai ser transferido neste enlace de tronco. Se não fosse utilizada uma interface de tronco, e fosse necessário propagar tráfegos da VLAN para outro switch, seria necessário a passagem de um cabo extra para cada VLAN. O IEEE 802.1q abriu caminho para padronização adicional em outras questões relacionadas a VLANs. Pode-se verificar na Figura 5 como seria sem a utilização do protocolo IEEE 802.1q (dot1q). É possível notar que cada VLAN utiliza uma porta para conexão com o comutador na interligação entre os dois switches (FOROUZAN, 2010, p. 462).

Figura 5 - Sem a utilização do protocolo IEEE 802.1q



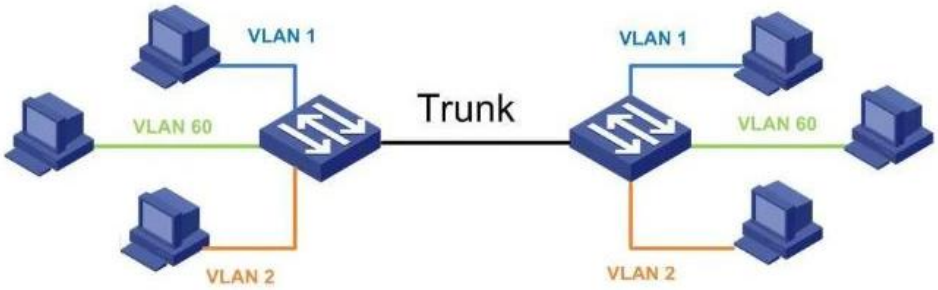
Fonte: Dias (2010).

Como a maioria dos switches tem um número limitado de portas, esta solução inutilizaria várias portas, sendo sua aplicação inviável com muitas VLANs, pois cada VLAN teria que ter um enlace interligando os switches. Já com a implementação do protocolo IEEE 802.1q é utilizado somente um cabo na comunicação entre os switches, marcando cada quadro com o ID de cada VLAN.

O comitê 802 do IEEE enfrentou esse problema em 1995. Depois de muita discussão, ele fez o impensável e mudou o cabeçalho do padrão Ethernet. O novo formato foi publicado no padrão 802.1Q do IEEE, emitido em 1998. O novo formato contém uma tag de VLAN (TANENBAUM; WETHERALL, 2011, p. 130).

A Figura 6 mostra uma topologia utilizando o protocolo IEEE 802.1q (DOT1Q) no qual carrega o tráfego de múltiplas VLANs, quando um quadro da VLAN 60 deve ser enviado de um switch para o outro, o enlace de tronco deve estar configurado com o DOT1q para que a informação da VLAN 60 seja incluída no campo adicional. Na Figura 6 pode-se observar dois quadros, o primeiro será encaminhado para a VLAN default (nativa) que por padrão é a VLAN1, e neste tipo de VLAN não é necessário incluir um campo com o ID da VLAN (sem TAG). O segundo quadro deverá ser incluído o campo de VLAN-ID, para colocar as informações da VLAN que está gerando o quadro (com TAG).

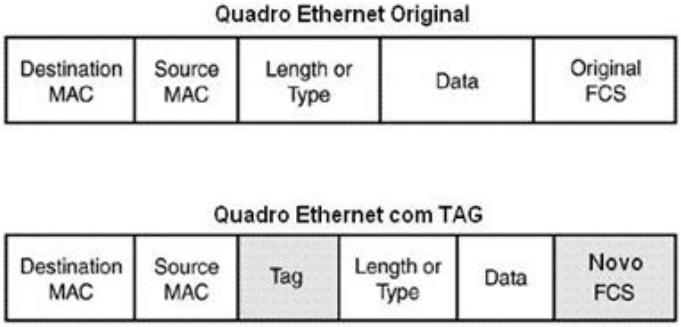
Figura 6 - Com a utilização do protocolo IEEE 802.1q



Fonte: Dias (2010).

A Figura 7 apresenta as subdivisões dentro do campo TAG. Segundo Tanenbaum e Wetherall (2011, p. 218), quando um quadro marcado chega a um switch que reconhece VLANs, o switch utiliza a ID da VLAN como um índice em uma tabela, para descobrir por meio de que portas deve enviar o quadro.

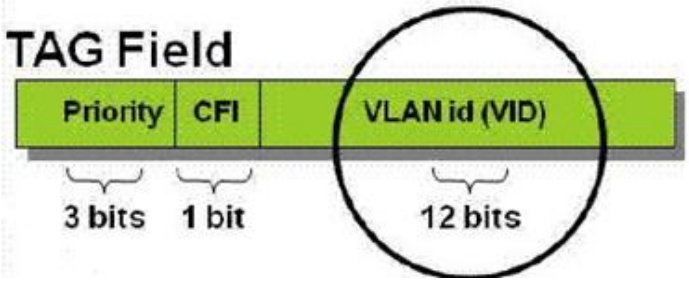
Figura 7 - Quadro IEEE 802.1q



Fonte: Dias (2010).

A Figura 8 mostra as informações do campo incluído no quadro do padrão IEEE 802.3, indicando as informações de VLANs que devem ser inseridas no enlace de tronco, para que seja enviado para o destino correto.

Figura 8 - TAG Field



Fonte: Dias (2010).

Já a comunicação entre os dispositivos conectados no mesmo switch que pertencem a mesma VLAN não são “tagueadas” (*untagged*).

2.4.2 VLAN Trunking Protocol (VTP)

Criado pela Cisco Systems, o *VLAN Trunking Protocol* (VTP) nasceu com a função de gerenciar e manter a consistência de todas as VLANs configuradas em uma rede, mas necessita de um domínio VTP[5] (FILIPPETTI, 2019, p.97).

O VTP reduz a administração em uma rede comutada” (CISCO, 2005). Ele simplifica a configuração das VLANs com vários switches, ficando essas informações centralizadas. Nos switches com suporte a este protocolo, estas informações são difundidas a cada 5 minutos em média. Os dispositivos com suporte ao VLAN Trunking Protocol podem ser configurados de três maneiras:

1. **VTP Server (Servidor):** modo padrão, ativo em todos os switches Cisco. Um switch em modo servidor e capaz de criar, excluir ou modificar VLANs em um domínio VTP (FILIPPETTI, 2019, p. 99).
2. **Modo Client (Cliente):** sugestivo, segundo Filippetti (2019), nesse modo o switch somente recebe informações do servidor VTP e as registra em uma memória não volátil[6], atualizadas essas informações, ele as propaga para seus vizinhos pertencentes ao mesmo domínio VTP.

[5] Domínio VTP: nada mais é do um conjunto de switches que trocarão informações VTP entre si (FILIPPETTI, 2019, p.97).
[6] Memoria não volátil: é um tipo de memória que pode recuperar a informação armazenada mesmo depois de ter sido desligado e ligado novamente.

3. **VTP Transparent (Transparente):** nesse modo as informações apenas seriam retransmitidas, não sofrendo qualquer alteração em suas configurações. Switches operando nesse modo não propagam suas próprias configurações para o domínio VTP (FILIPPETTI, 2019, p. 99).
4. **Modo "Off":** Segundo Filippetti (2019), este modo é semelhante ao modo transparente, mas não encaminha as atualizações VTP recebidas aos seus vizinhos.

Usado para distribuir e sincronizar informações de identificação das VLANs configuradas em toda a rede comutada. As configurações estabelecidas em um único servidor VTP são propagadas através do enlace tronco para todos os switches conectados na rede (TAVARES, 2011).

2.4.3 Spannig Tree Protocol

Esse protocolo normalmente é utilizado em empresas que possuem rotas alternativas para suas redes comutadas, evitando assim o chamado loop de camada 2. Ele permite a ativação e a desativação automática desses caminhos alternativos, fazendo com que os quadros de controle (BPDUs) sejam enviados por estes enlaces de backup, mas os quadros de dados não utilizam estes enlaces enquanto estiverem bloqueados. Caso caminhos redundantes sejam percebidos pelo protocolo, ele atuará elegendo um deles como primário e desativando os caminhos alternativos por meio de bloqueio de interface (FELIPPETTI, 2019, p. 79).

Os loops de camada 2 normalmente são problemáticos para os administradores de redes, porque eles podem parar uma rede inteira, ocasionando lentidão na rede, e mesmo podendo queimar equipamentos por conta da alta carga de quadros que são trocados na rede. A chamada "Tempestade de Broadcast" é o pesadelo dos administradores de redes, podendo fazer com que a rede local fique indisponível. O protocolo *Spanning-Tree* (STP) é um dos protocolos mais importantes para a utilização em redes locais. Uma implementação de LAN sem a previsão do protocolo STP pode ser problemática.

2.4.4 Link Aggregation Control Protocol (LACP)

Segundo a CISCO (2005), o *Link Aggregation Control Protocol* (LACP) empacota links individuais em um único enlace lógico para fornecer muita largura de banda mais alta. É usado para dar a prioridade a portas em uma agregação do link (RETARDAÇÃO). Uma RETARDAÇÃO dinâmica pode ter até 16 portas do mesmo tipo, mas somente 8 portas podem ser ativas ao mesmo tempo. Quando uma RETARDAÇÃO tem mais de 8 portas, o dispositivo usa a prioridade de sistema LACP e a prioridade de porta LACP para determinar que portas se tornam ativas.

A prioridade de sistema LACP está usada para determinar se o dispositivo local ou o dispositivo remoto têm a prioridade. O dispositivo com os controles de valor da baixa prioridade a seleção de porta na RETARDAÇÃO. Se os dispositivos têm a mesma prioridade de sistema LACP os endereços MAC estão comparados. O dispositivo com o mais baixo MAC address é dado o controle. A prioridade de porta LACP é usada para determinar qual 8 portas do dispositivo mais prioritário são ativas na RETARDAÇÃO. As portas com os mais baixos valores de prioridade são ativas.

2.5 MODELO DE REFERÊNCIA OSI

Com o surgimento da rede de computadores, não havia uma padronização de dispositivos e protocolos. Cada fabricante tinha sua tecnologia, topologia e protocolo. Com tantas diferenças e características as redes de computadores tornaram-se incompatíveis, empresas com tecnologias proprietárias que não eram compatíveis com as tecnologias de outros fabricantes. O modelo da camada OSI foi criado com o intuito de se quebrar essa barreira na comunicação de dados e permitir a interoperabilidade, independentemente do fabricante ou sistema utilizado (FILIPPETTI, 2019, p. 37).

Esse modelo se baseia em uma proposta desenvolvida pela ISO (*International Standards Organization*) como um primeiro passo em direção à padronização internacional dos protocolos empregados nas diversas camadas. Ele foi revisto em 1995. O modelo é chamado Modelo de Referência ISO OSI (*Open Systems Interconnection*), pois ele trata da interconexão de sistemas aberto, ou seja,

sistemas que estão abertos à comunicação com outros sistemas (TANENBAUM; WETHERALL, 2011, p .45).

2.5.1 Camadas do Modelo OSI

Segundo Filippetti (2019), cada camada é independente das demais, permitindo que tarefas associadas a uma camada possam ser implementadas ou modificadas sem que a demais tenha que sofrer qualquer tipo de alteração.

Para Morimoto (2008), O modelo OSI tenta explicar o funcionamento da rede, dividindo-a em 7 camadas. Pode-se verificar na Figura 9 as camadas do modelo OSI.

Cada uma delas tem a capacidade de se comunicar com a mesma no computador de destino, ou seja, não é possível para a camada dois ler dados que foram gerados na camada três. Isto origina uma comunicação virtual entre as camadas em computadores diferentes. Cada camada precisa apenas ser capaz de comunicar com as camadas imediatamente superiores e inferiores (DIOGENES, 2004).

Figura 9 - Modelo de referência OSI

Fonte: Pinto (2010).

A Figura 10 a mostra de forma simplificada um resumo das principais funcionalidades e ações de cada camada do modelo OSI.

Figura 10 - Resumo das camadas OSI

Camada	Descrição
Físico	Esta camada pega os quadros enviados pela camada de enlace e os transforma em sinais compatíveis com o meio por onde os dados deverão ser transmitidos.
Enlace de Dados	A camada de enlace pega os pacotes de dados recebidos da camada de rede e os transforma em quadros que trafegarão pela rede, adicionando informações como o endereço da placa de rede de origem, o endereço da placa de rede de destino, os dados de controle, os dados em si e a checagem de redundância cíclica (CRC).
Rede	É responsável pelo endereçamento dos pacotes, convertendo endereços lógicos em endereços físicos, de forma que os pacotes consigam chegar corretamente ao destino.
Transporte	Esta camada é responsável por pegar os dados enviados pela camada de sessão e dividi-los em pacotes que serão transmitidos à camada de rede.
Sessão	A camada de sessão permite que duas aplicações em computadores diferentes estabeleçam uma sessão de comunicação.
Apresentação	A camada de apresentação converte o formato do dado recebido pela camada de aplicação em um formato comum a ser usado na transmissão desse dado.
Aplicação	A camada de aplicação faz a interface entre o protocolo de comunicação e o aplicativo que pediu ou receberá a informação através da rede.

Fonte: Alencar (2010, p. 28).

2.5.2 Protocolos do Modelo de Referência OSI

A Figura 11 apresenta onde atua cada protocolo nas camadas do modelo de referência OSI.

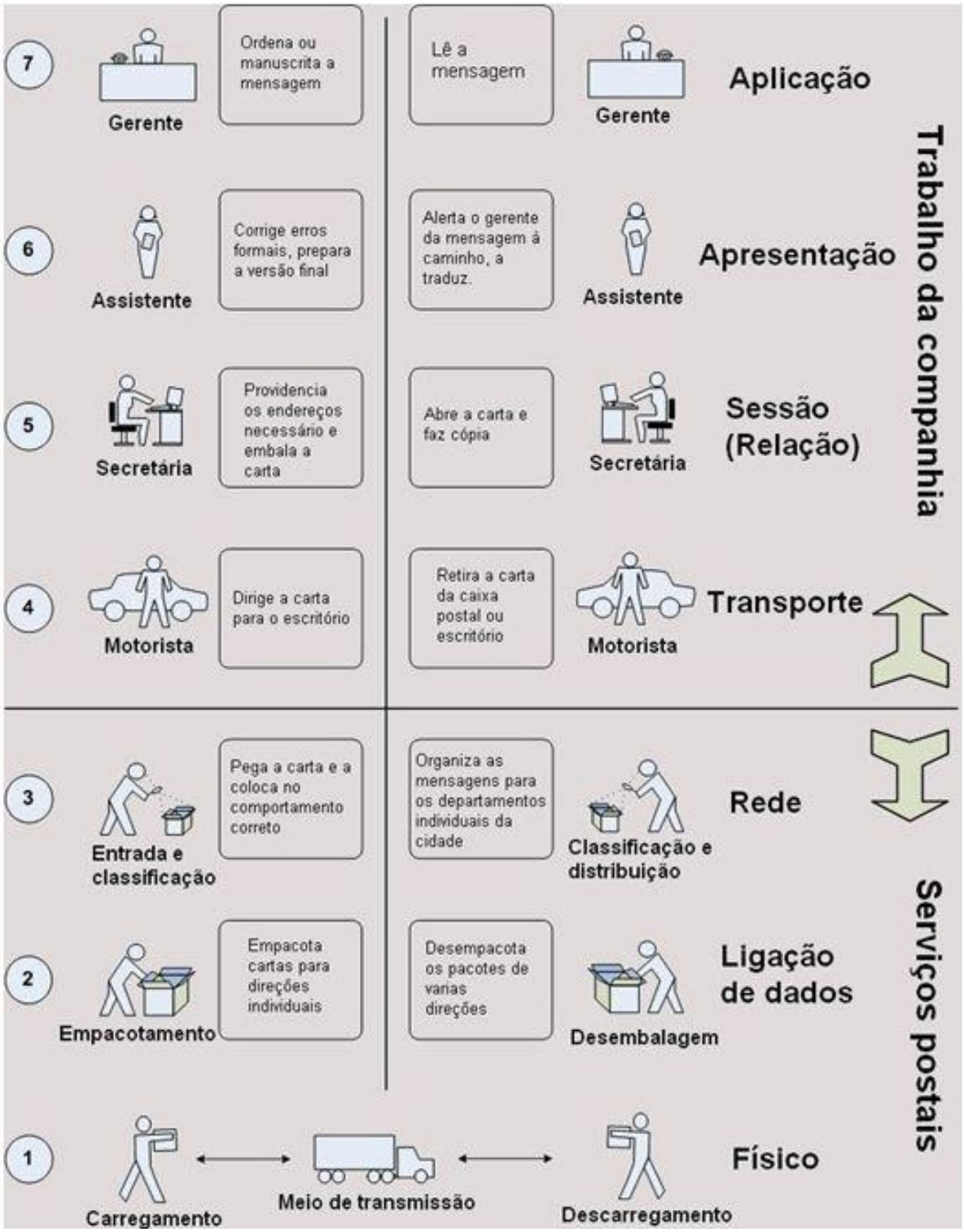
Figura 11 - Protocolos do modelo de referência OSI

Fonte: Pinto (2010).

2.5.3 Analogia do Modelo OSI

A Figura 12, ilustra o processo de envio e recebimento de dados, seguindo uma analogia como se fosse enviada uma carta.

Figura 12 - OSI e o paralelo com a comunicação por carta



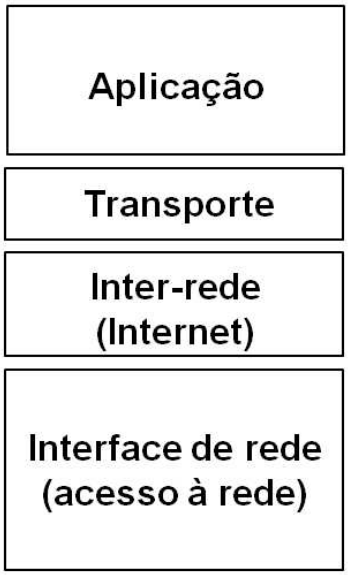
Fonte: Pinto (2010).

2.6 PILHA DE PROTOCOLOS TCP/IP

Segundo Filippetti (2019), este modelo não foi planejado e a Internet Pública não existiria caso o conjunto de protocolos e aplicações TCP/IP não tivessem sido criados. A pilha de protocolos TCP/IP surgiu para dar suporte a um conjunto de protocolos que já haviam sido criados sob demanda do Departamento de Defesa Americano (DoD). Este conjunto de protocolos foi desenvolvido bem antes do modelo OSI e foi definido pela primeira vez em 1974. Robert Kahn[7] desenvolveu o protocolo TCP e Vint Cerf[8] iniciou o desenvolvimento do protocolo IP. A pilha de protocolos TCP/IP, é definido como a pilha de protocolos padrões para todos os computadores atualmente (KUROSE; ROSS, 2014, p. 170).

Segundo Dantas (2002), o modelo de referência mais conhecido é o TCP/IP (*Transmisson Control Protocol / Internet Protocol*). A camada de aplicação do modelo TCP/IP corresponde às três superiores camadas do modelo OSI, ou seja Sessão, Apresentação e Aplicação (LOWE, 2011, p. 35). O Modelo TCP/IP é dividido em 4 camadas, e suas camadas são análogas as camadas do modelo OSI, mas com uma diferença, no TCP/IP houve uma fusão das 3 camadas superiores definidas pelo modelo OSI. A Figura 13 mostra as camadas da pilha de protocolos TCP/IP.

Figura 13 - Camadas no modelo TCP/IP



Fonte: Autoria própria.

[7] Robert Elliot Kahn, informático estadunidense.
[8] Vint Cerf: Abreviação de Vinton Gray Cerf, matemático e informático estadunidense.

A Figura 14 apresenta a funcionalidade e responsabilidade de cada camada no modelo TCP/IP.

Figura 14 - Funcionalidades de cada camada TCP/IP

Camada	Descrição
Interface de rede (acesso à rede)	Esta camada, de acesso à rede, é a primeira do modelo TCP/IP, sua função é dar suporte à camada de rede, através dos serviços de acesso físico e lógico ao meio físico.
Inter-rede (Internet)	O nível inter-rede (Internet) é o responsável pelo envio dos datagramas de um computador qualquer para o outro computador, independente de suas localizações na rede.
Transporte	A camada de transporte é responsável por prover suporte à camada de aplicação de maneira confiável (ou não), independente dos serviços oferecidos pelas camadas de interface de rede e inter-rede.
Aplicação	A quarta camada do modelo TCP/IP é denominada de camada de aplicação. Nesta camada, estão os protocolos que dão suporte às aplicações dos usuários.

Fonte: Alencar (2010, p. 29).

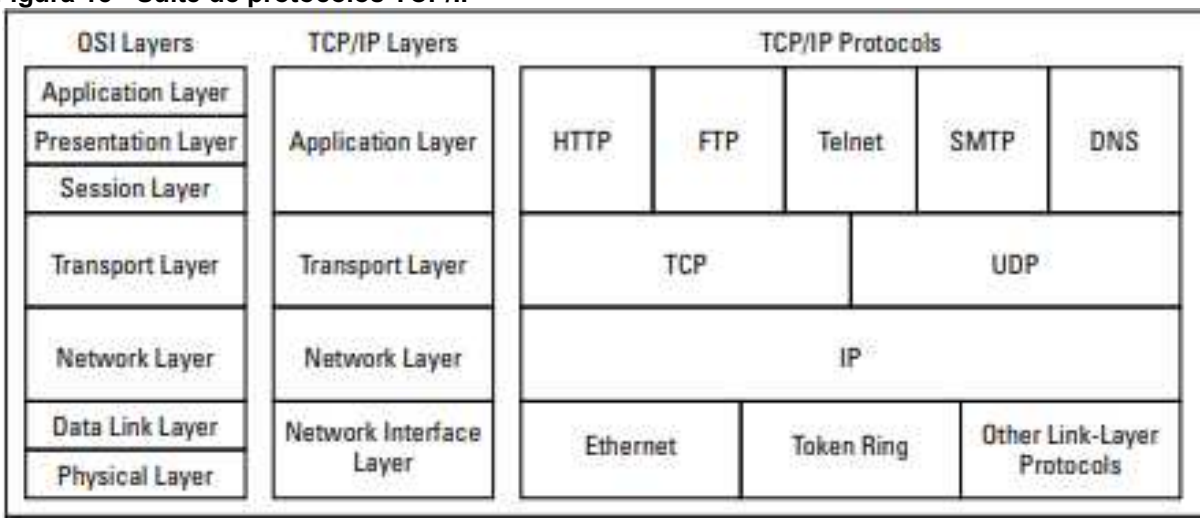
2.6.1 Suíte de Protocolos TCP/IP

Segundo Lowe (2011), a Internet Pública não é constituída unicamente de um protocolo, mas sim de um conjunto inteiro de protocolos relacionados. Muitos protocolos podem ser usados nesse nível. Alguns dos mais populares são HTTP, FTP, Telnet, SMTP, DNS e SNMP[9].

A Figura 15 mostra como o modelo TCP/IP corresponde com o modelo OSI e de alguns dos principais protocolos TCP/IP se encaixam no modelo. Como observado, a camada mais baixa do modelo, a camada de interface de rede (Network Interface Layer), corresponde ás camadas de enlace físico *(Physical Layer)* e de dados *(Data Link Layer)* do modelo OSI.

[9] SNMP: Protocolo de Gerenciamento de Rede, sendo possível através dele monitorar a funcionalidade dos dispositivos (computadores, roteadores,etc).

Figura 15 - Suíte de protocolos TCP/IP

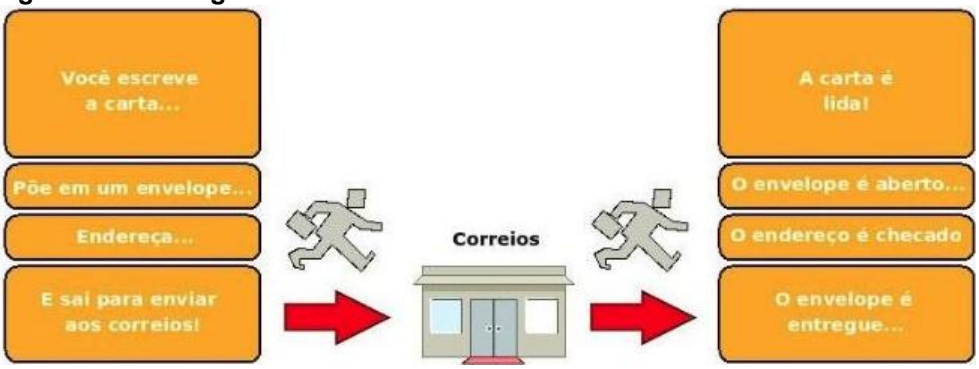


Fonte: Lowe (2011).

2.6.2 Analogia do TCP/IP

A Figura 16 ilustra o processo de envio e recebimento de dados, seguindo uma analogia do envio de uma carta.

Figura 16 - Analogia TCP/IP correios



Fonte: Autoria própria.

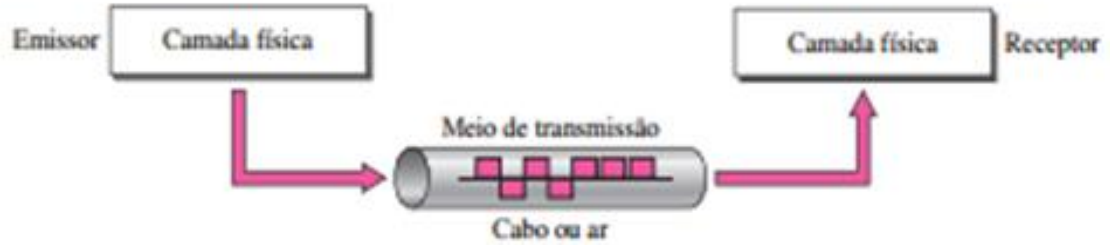
2.7 EQUIPAMENTOS DE REDE

2.7.1 Meios de Transmissão

O objetivo da camada física é a transmissão de um fluxo de bits de um dispositivo para outro. Existem vários meios físicos para realizar a transmissão, e cada um tem o seu próprio nicho em termos de largura de banda, retardo, custo e facilidade na instalação de manutenção. São divididos em duas categorias: os meios guiados, que utilizam fios de cobre e fibras ópticas, e os meios não guiados, com transmissão por ondas de rádio e os raios laser transmitidos pelo ar.

Segundo Forouzan (2010), um meio de transmissão, em termos gerais, pode ser definido como qualquer coisa capaz de transportar informações de uma origem a um destino. Por exemplo, o meio de transmissão para duas pessoas conversando durante um jantar é o ar que também pode ser usado para transmitir uma mensagem por meio de sinais de fumaça ou um código de sinais. Para uma mensagem escrita, o meio de transmissão poderia ser um carteiro, um caminhão ou um avião. A Figura 17 denota o que poderíamos classificar como meio de transmissão, o que faz o transporte entre o emissor e o receptor.

Figura 17 - Meio de transmissão e a camada física



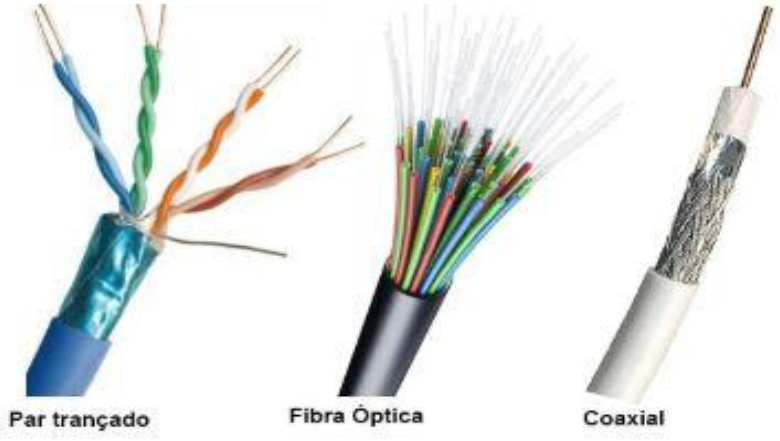
Fonte: Forouzan (2010).

Para Kurose e Ross (2014), os meios físicos se enquadram em duas categorias: meios guiados e meios não guiados. Nos meios guiados, as ondas são dirigidas ao longo de um meio sólido, tal como um cabo de fibra ótica, um par de fios de cobre trançado ou um cabo coaxial. Nos meios não guiados, as ondas se propagam na atmosfera e no espaço, como é o caso de uma LAN sem fio ou de um canal digital de satélite.

Meios de transmissão guiados – a Figura 18 mostra os meios de transmissão que comumente utilizam cabeamento, meios que basicamente são definidos em categorias que utilizam fios de cobre (par trançado e coaxial) e ópticos (fibras ópticas).

Entre os meios de transmissão guiados, que são aqueles que requerem um condutor físico para interligar um dispositivo a outro, tem-se: cabo de par trançado, cabo coaxial e cabo de fibra óptica. Um sinal trafegando por qualquer um desses meios é direcionado e contido por limites físicos do meio. Cabos de par trançado e coaxiais usam condutores metálicos (cobre) que aceitam e transportam sinais na forma de corrente elétrica. A fibra óptica é um cabo que aceita e transporta sinais na forma de luz (FOROUZAN, 2010, p. 192).

Figura 18 - Meios de transmissão



Fonte: Autoria própria.

Meios não guiados**, p**ara Forouzan (2010), os meios não guiados transportam ondas eletromagnéticas sem o uso de um condutor físico. Esse tipo de comunicação é, muitas vezes, conhecido com comunicação sem fio. Os sinais são normalmente transmitidos pelo espaço livre e, portanto, ficam disponíveis a qualquer um que tenha um dispositivo capaz de recebe-los. Exemplos seriam as ondas de rádio, micro-ondas[10], infravermelho[11], bluetooth[12], etc.

2.7.2 Placas de Rede

Para Morimoto (2008), o primeiro componente de uma rede é justamente a placa de rede. Além de funcionar como um meio de comunicação, a placa de rede desempenha várias funções essenciais, como a verificação da integridade dos dados recebidos e a correção de erros. O papel principal das placas de rede Ethernet é receber os quadros enviados pela camada de Controle de Acesso ao Meio e transmitir os dados através do cabeamento da rede (TORRES, 2001, p. 286).

Quanto a taxa de transmissão, temos placas Ethernet variando de 10 Mbps a 10 Gbps. A Figura 19, apresenta uma placa Ethernet para transmissão de dados a 10 Gbps, utilizam conectores GBIC ou cabo SFP+ *Direct Attached Twin Axial Cabling up to 10m.*

---

[10] Micro-ondas: são ondas eletromagnéticas com comprimentos de onda que variam de 1 a 300 GHz.

[11] Infravermelho: Frequências que vão dos 300GHz aos 400 THz, usada para comunicação de curta distância (FOROUZAN,2010).

[12] Bluetooth: é um protocolo padrão de comunicação primariamente projetado para baixo consumo de energia com baixo alcance.

Figura 19 - Placa rede Intel X520-da2 10gb E10gsfpsr Sfp + 2 Gbic 10gb

Fonte: Autoria própria.

Para computadores domésticos, geralmente é utilizado uma placa de rede integrada de baixo custo, porque são usados apenas para conectar um usuário a rede. No entanto em um servidor deve-se utilizar um NIC de alta qualidade como Intel, SMC ou 3COM, e com uma velocidade de transferência alta, pois os servidores são conectados a muitos usuários em uma rede.

2.7.3 Switch

O switch é um elemento concentrador interligando dispositivos (computadores, servidores, cartão ponto, SmartTVs, etc) na rede e faz o que é chamado de comutação de quadros. Ele recebe os pacotes do padrão IEEE 802.3 já encapsulados dos hosts que contem informação do endereço MAC de origem e o endereço MAC de destino e, ao contrário do HUB, encaminha estes pacotes diretamente ao destino pois possui internamente uma tabela de comutação MAC contendo o endereço (MAC) do dispositivo e em qual porta ele está conectado. Switches são rápidos e eficientes porque não analisam informações pertinentes a camada de rede, concentrando-se apenas nas informações presentes no cabeçalho dos frames (FELIPPETTI, 2019, p. 73).

Segundo Lowe (2011), um switch é simplesmente um tipo de hub mais sofisticado. O custo dos switches diminuíra drasticamente nos últimos anos, e a maioria das novas redes são construídas com switches em vez de hubs. Se um administrador de redes administra uma rede mais antiga que utiliza hubs ao invés de switches, este administrador pode ter problemas de segurança e desempenho nesta

rede, visto que estes equipamentos trabalham na camada física enviando as informações para todas as portas. O switch de camada de enlace, ao invés de enviar para todas as portas, faz a comutação e encaminha somente para a máquina de destino. Atualmente somente redes legadas utilizam hubs, por conta dos problemas de desempenho e segurança.

Os switches são usados para conectar dispositivos de rede em encaminhar dados de uma porta a outra com base em informações obtidas a partir dos pacotes a serem transmitidos (LOWE, 2011, p. 50).

A Figura 20 mostra um switch CISCO Catalyst 9200 Series com 24 portas Gigabit, 4 uplinks fixos SFP+ de 10 Gigabit, fontes de alimentação redundantes e garantia vitalícia limitada aprimorada (CISCO, 2005).

Figura 20 - Switch Cisco Catalyst 9200 Series

Fonte: Autoria própria.

Os switches também podem ser conectados a outros switches, permitindo assim a ampliação do total de número de pontos conectados na rede. A essa conexão dá-se o nome de cascading, ou cascateamento de switches. Assim, cada switch cascateado cria um entroncamento distinto em uma rede hierárquica.

2.7.3.1 Switch de camada de enlace (Layer 2)

Os modelos de switches de camada de enlace fazem a comutação dos quadros do padrão IEEE 802.3 (Ethernet) e as suas variantes, fazendo com que estes quadros sejam enviados da origem ao destino, utilizando para isto o endereço de 48 bits utilizado nas chamadas *Network Interface Card* (NIC), ou placas de redes. Estes endereços são controlados pelo IEEE que fornecem aos fabricantes de equipamentos de redes blocos de endereços MAC. Esta comutação é feita nas LANs e atuam somente no mesmo domínio de broadcast. Assim, um switch de camada de enlace não pode fazer o roteamento entre as VLANs, somente irá fazer a comutação entre os hosts da mesma VLAN. Um switch de camada de enlace armazena os endereços MAC aprendidos por meio do processo de *backard lerarning* e associa cada porta em sua tabela de comutação (*Content Address Table* - CAM).

Estes switches geralmente são utilizados na camada de acesso do modelo hierárquico para interligar os dispositivos finais (PCs, Telefones, impressoras, etc). São equipamentos mais baratos que os switches multicamadas, que além da comutação de camada 2, podem realizar roteamento de camada 3, interligando as VLANs.

A Figura 21 apresenta uma tabela CAM de um switch camada de enlace e pode-se observar que cada porta está ligada a um endereço MAC. Quando uma das portas é trocada, ele processa e reescreva a sua tabela CAM. Quando o switch recebe um quadro e o destino deste quadro está na tabela CAM, ele encaminha para a porta de destino. Quando o switch recebe um quadro e o endereço MAC de destino não está na tabela CAM, o switch encaminha o quadro para todas as portas, menos para a porta de origem.

Figura 21 - Tabela CAM switch L2

Porta	Endereço MAC
1	A4:50:46:66:5B:8B
2	78:8A:20:66:E7:30
3	78:8A:20:C5:5C:2F
4	FC:EC:DA:44:7B:E3
5	E8:DE:27:07:55:B9
20	70:AF:24:7C:DA:62
23	CC:61:E5:6B:55:CD
34	64:27:37:CE:9C:3B

Fonte: Autoria própria.

2.7.3.2 Switch multicamada (Layer 3)

Os switches multicamadas possuem todas as funcionalidades de um switch de camada de enlace e incorporam a função de roteamento (camada de rede), além da compreensão de vários protocolos existentes. Trabalhando diretamente onde ficam localizados os protocolos TCP/IP do modelo OSI, são capazes de entender tanto os endereços físicos como os endereços lógicos independentemente da versão do protocolo IPv4 ou versão IPv6.

Uma das grandes vantagens de um switch multicamada é a possibilidade de fazer o tráfego fluir entre duas ou mais VLANs distintas. Se o host de origem e o de destino não estiverem dentro de uma mesma subrede ou VLAN, os pacotes deverão ser encaminhados baseados na informação de endereço IP da camada de rede (camada 3) do modelo OSI.

Switches multicamadas podem funcionar como roteadores tradicionais conectando vários switches de camada de enlace e fornece conectividade inter-VLAN. Em tais casos, não existe nenhuma funcionalidade deste tipo em switches de Camada de enlace. Este conceito pode ser ilustrado pela colocação de um switch multicamada entre a camada de um switch de camada de enlace e o roteador (CHANG; HUANG, 2013).

Além das funcionalidades de roteamento, switches multicamadas empregam balanceamento de carga e podem distribuir o tráfego sobre todas as suas portas de rede que possuem a mesma distância a partir do endereço de destino. O balanceamento de carga aumenta a utilização de segmentos de rede, aumentando assim a largura de banda efetiva. A comutação em camada 3 efetua o balanceamento de carga baseado no destino e origem dos pacotes IP (3COM, 2013).

De acordo com a 3COM (2013), os roteadores tradicionais, uma vez que são componentes fundamentais de redes corporativas, tornaram-se um grande obstáculo à migração para redes de próxima geração. Porém é interessante notar que um switch multicamada faz tudo o que um roteador tradicional faz:

- Determina o caminho do encaminhamento com base nas informações da camada 3;
- Valida a integridade da camada 3 por meio da soma de verificação do dataframe;
- Verifica a validade de pacotes e efetua atualizações sobre eles;
- Processa e responde a todas as informações da opção;
- Efetua atualizações estatísticas encaminhamento do protocolo Management Information Base (MIB);
- Aplica controles de segurança, se necessário.

2.7.4 Roteadores

Segundo Morimoto (2008), os roteadores servem para interligar duas redes separadas. Usando roteadores é possível interligar redes diferentes, mesmo que situadas em países ou mesmo continentes diferentes. Eles também são programados para determinar o melhor caminho a seguir, dependendo do tipo de roteamento que o administrador de redes irá utilizar para fazer as configurações de

roteamento na rede. Assim, o protocolo de roteamento RIP irá utilizar o menor número de saltos (*hops*) como métrica principal. Outros protocolos de roteamento irão utilizar diferentes tipos de métricas para alcançar a rede de destino. O protocolo de roteamento OSPF, é um protocolo do tipo Link-state que utiliza um custo relacionado à largura de banda, e vai calcular o melhor caminho verificando a largura de banda entre a origem e o destino.

A internet Pública é uma rede mundial formada por várias sub-redes interligadas por roteadores. Todos os usuários de um pequeno provedor, por exemplo, podem ser conectados à Internet Pública por meio de um roteador. Para acessar uma página do Gmail.com por exemplo, o pacote irá atravessar vários roteadores, até chegar no servidor do Google, que está hospedando o serviço do Gmail para os usuários. Se não houver muitos pacotes sendo trafegados na rede, o serviço será carregado rapidamente. Porém, se houver algum congestionamento no caminho escolhido talvez demore vários segundos, ou mesmo minutos (MORIMOTO, 2008, p. 34).

Segundo Edwards e Bramante (2009), os roteadores, diferentemente dos switches, possuem como funcionalidade principal a capacidade de conectar dois tipos distintos de redes. Os roteadores suportam muitos protocolos e padrões que permitem maior flexibilidade na sua implementação.

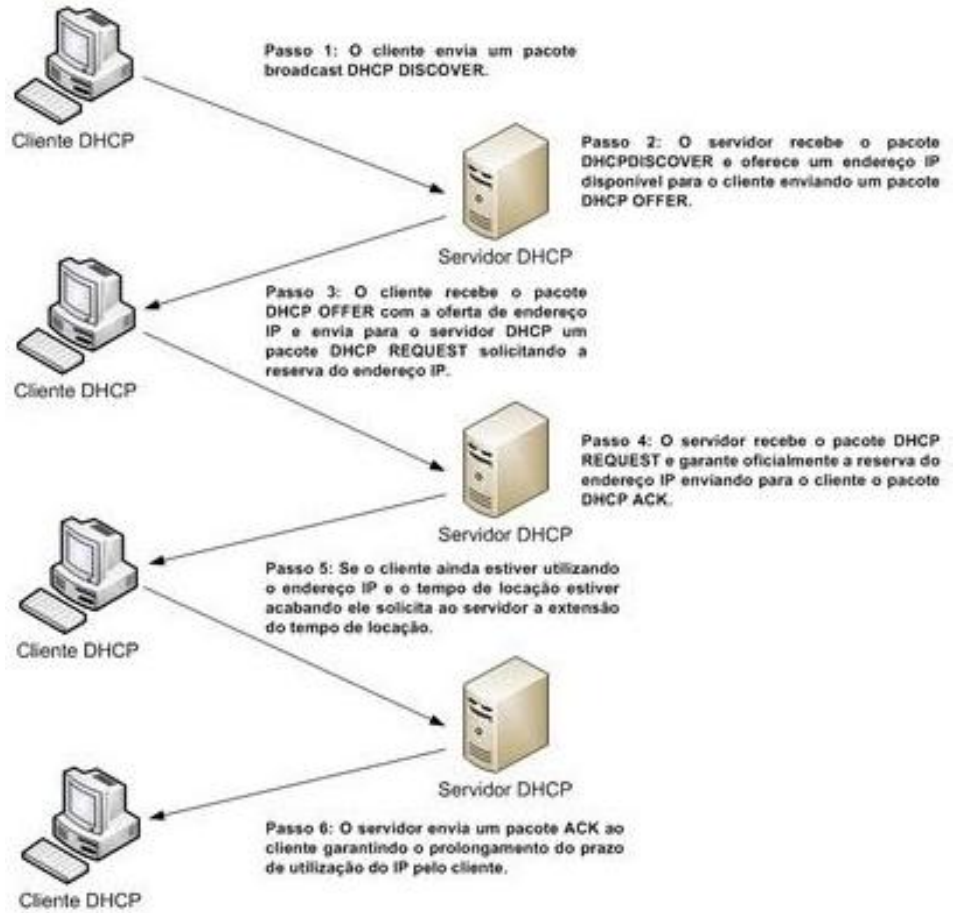
Assim como outros equipamentos de redes, os roteadores existem em diversos tamanhos e capacidades. Pode-se utilizar um roteador para uma pequena ou média empresa, onde a capacidade de roteamento e interfaces são limitados. Estes roteadores podem utilizar os principais protocolos existentes. Existem também os roteadores de grande porte, com muitos slots, fontes redundantes, interfaces de fibra optica, e muitas outras opções a mais na utilização. Estes roteadores podem custas centenas de milhares de reais, mas para as empresas de grande porte e as operadoras de Telecomunicações, o investimento neste tipo de equipamento tende a vale a pena. Não importa o tamanho e a capacidade do roteador, todos eles têm a mesma finalidade: rotear pacotes entre redes diferentes.

2.8 SERVIÇOS

2.8.1 Servidor DHCP

Em uma rede de computadores baseada no protocolo TCP/IP, todo dispositivo deve possuir um endereço IP próprio. O servidor de DHCP fornece esse endereço de forma automática, além de outras informações como gateways, servidor de nomes, servidores wins e servidores proxy. Um servidor DHCP pode ser um computador localizado na rede TCP/IP. Todos os sistemas operacionais de servidores modernos têm um servidor DHCP embutido, não necessariamente ser totalmente dedicado, a menos que a rede seja muita grande. Segundo Lowe (2011), muitos roteadores multifuncionais também possuem servidores DHCP embutidos. Então, para não sobrecarregar um dos servidores de rede com a função DHCP, é possível ativar o servidor DHCP interno do roteador. A Figura 22 mostra como o dispositivo cliente faz para se obter um endereço IP.

Figura 22 - Funcionamento servidor DHCP



Fonte: Autoria própria.

Criado em 1993, o serviço DHCP permite a configuração dinâmica de elementos conectados a uma rede, via concessão de endereços IP e máscara de rede, default gateway (roteador padrão), endereço IP de um ou mais servidores DNS e algumas outras opções (FELIPPETTI, 2019, p. 114).

Sem o uso de um servidor DHCP, o administrador da rede e a sua equipe teriam que configurar, manualmente, as propriedades do protocolo TCP/IP em cada dispositivo de rede(hosts). Com o uso do DHCP esta tarefa pode ser completamente automatizada.

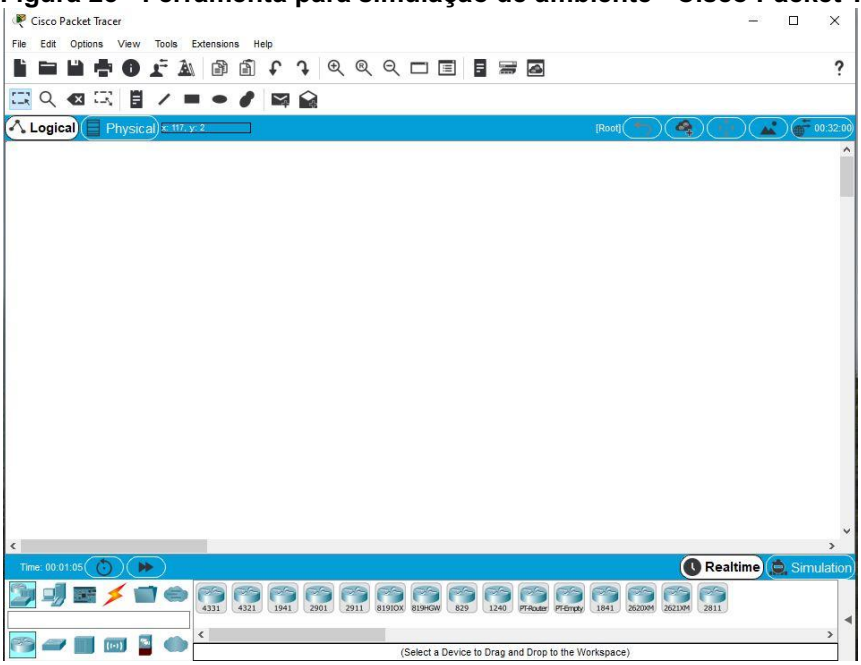
Em uma rede com centenas ou até mesmo milhares de estações de trabalho, configurar o TCP/IP manualmente, em cada estação de trabalho é uma tarefa bastante trabalhosa, que envolve tempo e exige uma equipe técnica para executar este trabalho. Além disso, sempre que houver mudanças em algum dos parâmetros de configuração (como por exemplo uma mudança no número IP do servidor DNS), a reconfiguração terá que ser feita manualmenteem todas as estações de trabalho da rede. Por exemplo, imaginar que o númeroIP do *default gateway* teve que ser alterado devido a uma reestruturação da rede. Neste caso a equipe de suporte teria que ir de computador em computador, alterando as propriedades do protocolo TCP/IP, para informar o novo número IP do *default Gateway*, isto é, alterando o número IP antigo do *default gateway* para o novo número.

2.9 APLICATIVOS

2.9.1 Cisco Packet Tracer

Essa é uma ferramenta muito utilizada por uma gama de profissionais, docentes e discentes no mundo. Esse aplicativo simula um ambiente de rede como em um laboratório, possibilitando inúmeras situações e configurações com dispositivos (roteadores, firewall, switches, etc.) Cisco. A Figura 23 apresenta a tela inicial do aplicativo. Este software será utilizado na monografia para a implementação das infraestruturas de redes que serão propostas para que a Clínica tenha uma estrutura de redes organizada e bem estruturada. Será uma ferramenta essencial para moldar a futura estrutura da rede.

Figura 23 - Ferramenta para simulação de ambiente - Cisco Packet Tracer



Autor: Autoria própria.

2.10 LISTA DE CONTROLE DE ACESSO (ACL)

A Lista de controle de acesso (ACL) contém uma lista de regras “instruções” a serem executadas sobre determinada ação de um protocolo ou a endereçamento. São geralmente aplicadas pelos administradores a fim de filtrar determinado tráfego, seja ele na entrada (IN) ou saída (OUT), seguindo um protocolo de execução, a lista sequencial de regras é executada de cima para baixo, uma linha por vez. Todas suas validações são feitas a partir da camada 3 do modelo OSI.

Dentro de um mesmo elemento, podemos ter várias listas de acesso criadas, porém, elas apenas serão utilizadas se associadas a alguns objetos (interface) ou serviço (NAT). Segundo Filippetti (2019, p. 419), as ACLs podem ser usadas para:

- Permitir ou negar um fluxo de pacotes baseado em sua origem, destino e ou protocol ou aplicação;
- Proteger o acesso a elementos críticos ou a redes/sub-redes inteiras;
- Determinar quais fluxos de dados serão submetidos a algum tipo de tratamento adicional (NAT ou roteamento);
- Identificar e bloquear tráfegos nocivos originados externa ou internamente;
- Apenas monitorar o tráfego com determinadas características e armazenar as informações coletadas em arquivos.

Segundo Filippetti (2019), existem basicamente dois tipos de acls: a) standard (padrão); e b) extended (estendidas). A diferença se baseia em como são analisados os pacotes durante o processo de filtragem:

- São sempre processadas de cima para baixo em ordem sequencial;
- Um pacote é comparado com as condições impostas pela ACLS até encontrar uma correspondência;
- Assim que encontrar uma ACLS correspondente, nenhuma comparação adicional será feita para esse pacote;
- A interface irá agir com base na condição de correspondência. Existem duas ações possíveis; permitir e negar;
- Cada ACL tem uma declaração de negação padrão no final dela.
- Se a condição de permissão corresponder, o pacote poderá passar da interface;
- Se a condição de negação corresponder, o pacote será destruído imediatamente;
- Se um pacote não atender a nenhuma condição, ele será destruído (pela última condição de negação);
- ACL vazio permitirá todo o tráfego por padrão. A condição de negação implícita não funcionará com ACL vazia;
- A condição implícita (última negação padrão) funcionaria apenas se o ACL tiver pelo menos uma condição definida pelo usuário;
- O ACL pode filtrar apenas o tráfego que passa da interface. Ele não pode filtrar o tráfego originado do roteador ao qual foi aplicado;
- A ACL padrão pode filtrar apenas o endereço IP de origem;
- ACL padrão deve ser colocado próximo aos dispositivos de destino;
- A ACL estendida deve ser colocada perto dos dispositivos de origem;
- Cada ACL precisa de um número ou nome exclusivo;
- Pode-se ter apenas uma ACL aplicada a uma interface em cada direção; entrada e saída.

Segundo a CISCO uma das habilidades mais importante seria que o administrador de redes, domina-se ACLs, com isso permitindo ou negando um trafego em especifico.

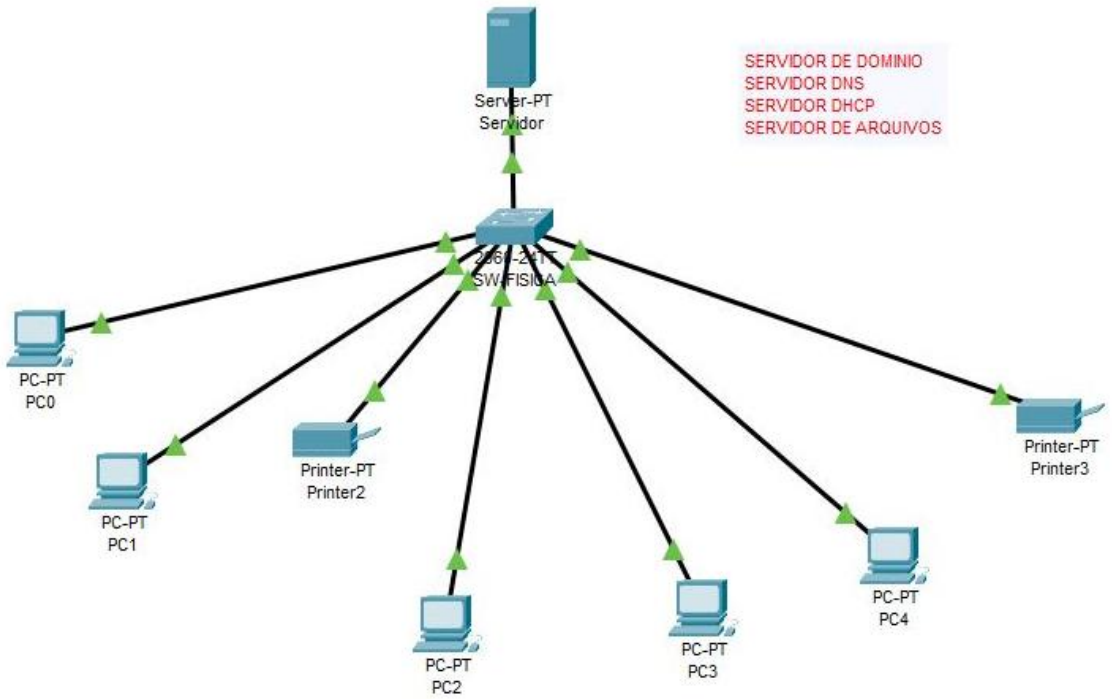
3 DESENVOLVIMENTO

3.1 REDE FISICA ATUAL

3.1.1 Topologia Física

A Figura 24 apresenta a topologia atual da rede FÍSICA, possui 1 switch gerenciável de 16 portas da DELL, uma unidade de backup externo com dois disco de 1Tb em raid1, 5 Workstations (HP e DELL) e duas impressoras com suporte a impressão no formato A3 e um servidor de domínio primário com funções de DHCP e DNS.

Figura 24 - Topologia atual rede Física



Autor: Autoria própria.

3.1.1.1 Servidor

Atualmente a rede da FÍSICA, possuí um servidor um Servidor DELL PowerEdge 1900 com processador Intel Xeon X5365, 4 Gb de memória RAM uma controladora DELL SAS 5/ir com 2 discos SAS de 600Gb 15k em RAID 1. Apresenta sistema operacional Windows 2012 R2 server com funções de servidor de domínio primário, DHCP, DNS e servidor de arquivos.

3.1.1.2 Backup

O Sistema de Backup é executado pelo *software* da Veeam (*Veeam Backup Essential*) em duas etapas uma sendo executado localmente em unidade externa com discos em RAID 1 e outra sendo executada na nuvem em um servidor de hospedagem da Alhambra EIDOS.

3.1.1.3 Workstations

Os profissionais da área utilizam Workstation tanto da HP como da Dell, foram padronizadas com as seguintes configurações de hardware: disco de 1Tb, 16 Gb de memória RAM e utilizam processadores da Intel core i5 e core i7, com monitores de com resolução Full HD e display de LED.

3.1.1.4 Switch

O Switch pode ser usado em projetos futuros, sendo de camada de enlace (camada 2), com 16 portas Gigabit ethernet, gerenciável.

3.1.1.5 Meios de transmissão

O cabo de par trançado (UTP) categoria 5e é o meio de transmissão utilizado como padrão para a interligação dos dispositivos e os equipamentos de redes na infraestrutura de rede. Este tipo de meio de transmissão tem um bom custo/benefício, visto que a conectorização é barata, o cabo tem um preço acessível e a taxa de erros de bits em uma rede local (LAN) com a utilização do cabo UTP é baixa. Os enlaces podem ser feitos com uma distância máxima de 100 metros, sendo que além deste comprimento, haverá uma atenuação no enlace. Como a interligação dos equipamentos finais e dos dispositivos de redes em uma rede local (LAN) normalmente não é maior do que a distância máxima que o UTP utiliza, é possível interligar estes equipamentos utilizando este tipo de cabeamento.

3.1.2 Principais Problemas

O Servidor está defasado, com mais de onze anos de uso. Existem dificuldades em encontrar peças de reposição (como fontes de alimentação e HDs), pouco espaço de armazenamento, localização do servidor em ambiente sem controle de refrigeração, rede elétrica sem redundancia e sem previsão para

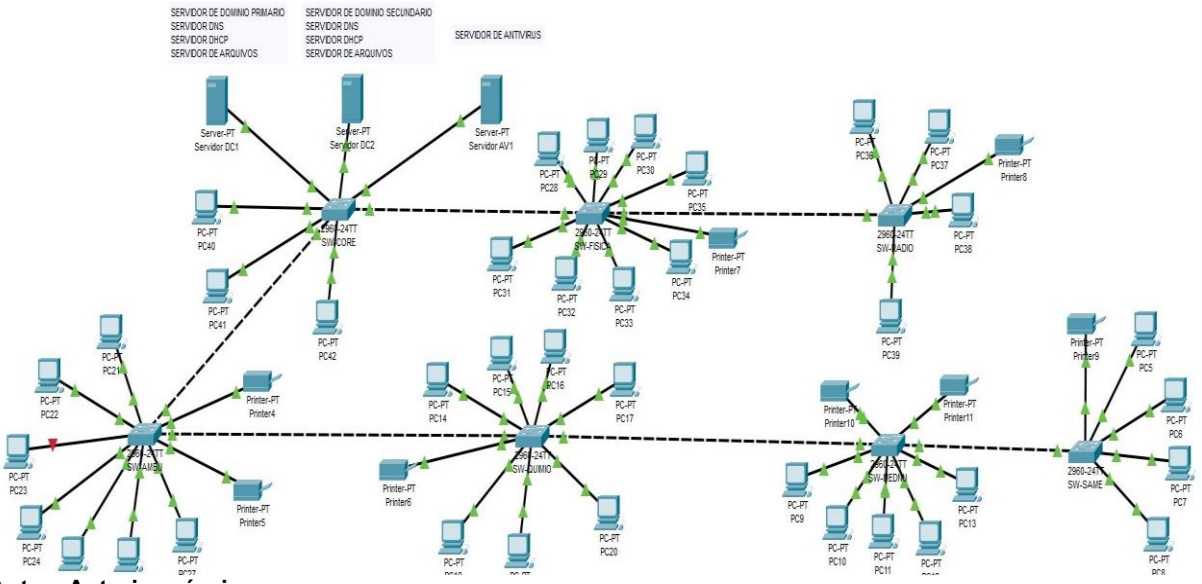
investimentos futuros. São alguns dos fatores que justificam a necessidade de atualização do ambiente.

3.2 REDE CLÍNICA ATUAL

3.2.1 Topologia Fisica

A Figura 25 detalha a topologia atual da rede CLÍNICA, que é dividida em vários departamentos e setores, compartilham a mesma infraestrutura, gerando lentidão na transferência de aquivos de imagem de pacientes para os servidores. É utilizado somente um range de endereçamento IP, que são distribuídos por um servidor DHCP. Possui também um servidor de Antivirus que necessita de constante comunicação com a rede. Ambos geram constantes tráfegos de broadcast na rede. Esta topologia é sucetivel a falhas, pois não existe qualquer redundância de dispositivos essenciais.

Figura 25 - Topologia atual rede Clínica



Autor: Autoria própria.

3.2.1.1 Servidores

A rede CLÍNICA possui três servidores localizados no Data Center, sendo o controlador de domínio principal, o controlador secundário e o servidor para gerenciamento do antivírus, tanto das estações como dos servidores.

A configuração de *Hardware* do servidor principal é um servidor Rack DELL R540 Xeon 4210, 32 Gb de memória RAM, com duas fontes de alimentação redundantes de 750w, 4 discos de 2 TB SAS 10K em RAID 10, uma controladora DELL PERC H740P e possui 2 discos de 600 Gb SAS 10K para o Sistema Operacional Windows Server 2019. Executa as funções de servidor DHCP, DNS primário, Banco de dados MSSQL para o sistema ERP, servidor de arquivos e uma máquina virtual HYPER-V com backup do servidor de antivírus.

O servidor de domínio secundário apresenta a seguinte configuração: HP Proliant ML 110 Gen 9 Xeon em Torre,16 Gb de memória RAM, 2 discos de 1 Tb SATA em RAID 1, sistema operacional Windows 2012 R2. Executa as funções de servidor DHCP secundário e DNS secundário.

O servidor de Antivírus é um dos servidores mais simples, sua configuração e um HP Proliant ML 310e Gen 8 v2 Xeon E3-1220 v3, com 8 Gb de memória RAM, 2 discos de 500 GB SATA 7200 RPM, com Sistema Operacional Windows Server 2012 R2. Utiliza o Kaspersky Security Center versão 12, que propaga para a estações a versão 14 do EndPoint e nos servidores a versão Kaspersky Security for Windows Server 10.1.2.996.

3.2.1.2 Backup

O sistema de *Backup* também utiliza o *software* citado no subitem 3.1.2, seguindo a mesma simétrica, mas com armazenado local em dispositivos diferentes.

3.2.1.3 Switches

Os switches dispersados pela CLÍNICA são de camada de enlace gerenciáveis, sendo compostos por switches de 24 e 48 portas Gigabits, com portas SFP para a conexão de *uplinks*.

3.2.1.4 Meios de transmissão

Os meios de transmissão utilizam o cabo de par trançado não blindado (UTP) com as categorias 5e e 6 para interconectar os switches. Não está sendo utilizado a conexão por meio de cabos de fibra óptica pois a distância máxima ainda permite a utilização de cabos de cobre par trançado.

3.2.2 Principais Problemas

O fator principal que onera essa topologia é sua unicidade em broadcast. Outro fator é a dificuldade do administrador de rede em controlar os dispositivos conectados, comprometendo gradativamente a segurança e a estabilidade da rede CLÍNICA, pois trazem consigo *softwares* maliciosos ou pragas virtuais (vírus, *worms*, *malware*, *ransomware*) e por último a necessidade de se implementar uma rede wi-fi tanto para os dispositivos de visitantes e colaboradores, enquadrando na questão de dispositivos de terceiros.

3.3 REDE CLÍNICA PROPOSTA

3.3.1 Topologia Lógica

3.3.1.1 VLANs

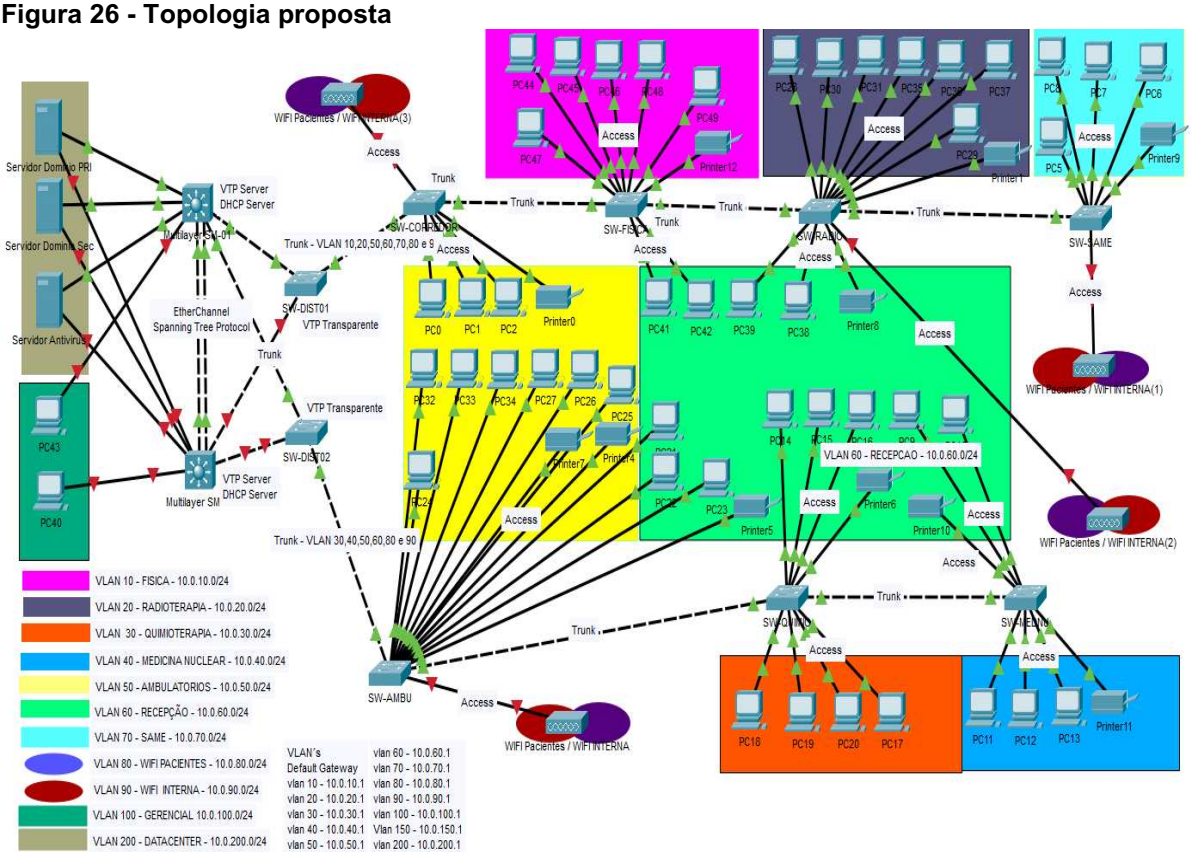
A organização lógica da CLINICA já organizado em setores (Fisica, Radioterapia, Quimioterapia, Medicina Nuclear, Ambulatórios, Recepção, Same, Wifi Visitantes, Wifi Interno, Gerenciamento e Data Center). Foram criadas VLANs para cada um dos setores propostos (Tabela 1). As VLANs possuem os seguintes Ids (numerações): 10,20,30,40,50,60,70,80,90,100 e 200 (Figura 26) e a nomeação será referente aos setores qual pertencem (FISICA, RADIOTERAPIA, QUIMIOTERAPIA, MEDICINA NUCLEAR, AMBULATORIOS, RECEPÇÃO, SAME, WIFI-VISITANTES, WIFI-INTERNO, GERENCIAMENTO E DATACENTER). Todos os switches devem receber endereços IPs, e devem ser associados a VLAN 100 para gerenciamento remoto, caso seja necessário. Seguindo as condutas de boas práticas na implementação de redes, o administrador de rede deve constatar que todos os segmentos estão devidamente configurados para evitar problemas relacionados a propagação de um segmento em outro.

Tabela 1 - VLAN's aplicadas e endereçamento

ID	Nome	Endereço	Máscara de Sub-redes	Gateway
1	NATIVA	10.0.0.0	255.255.255.0	10.0.0.254
10	FISICA	10.0.10.0	255.255.255.0	10.0.10.1
20	RADIOTERAPIA	10.0.20.0	255.255.255.0	10.0.20.1
30	QUIMIOTERAPIA	10.0.30.0	255.255.255.0	10.0.30.1
40	MEDICINA NUCLEAR	10.0.40.0	255.255.255.0	10.0.40.1
50	AMBULATORIOS	10.0.50.0	255.255.255.0	10.0.50.1
60	RECEPCAO	10.0.60.0	255.255.255.0	10.0.60.1
70	SAME	10.0.70.0	255.255.255.0	10.0.70.1
80	WIFI-VISITANTES	10.0.80.0	255.255.255.0	10.0.80.1
90	WIFI-INTERNA	10.0.90.0	255.255.255.0	10.0.90.1
100	GERENCIAMENTO	10.0.100.0	255.255.255.0	10.0.100.1
200	DATA CENTER	10.0.200.0	255.255.255.0	10.0.200.1

Autor: Autoria própria.

Figura 26 - Topologia proposta



Autor: Autoria própria.

3.3.1.2 Endereçamento IP

Em um ambiente de simulação, foi utilizado um bloco de endereçamento falso de rede privada (RFC 1918) Classe A. Foi utilizado o bloco 10.0.0.0 (e algumas sub-redes 10.0, 20.0, 30.0, 40.0, 50.0, 60.0, 70.0, 80.0, 90.0, 100.0 e 200.0). Todas as subredes utilizarão máscaras notação CIDR /24.

3.3.2 Investimento

Depois de analisar toda a infraestrutura de rede, visto que para um melhor desempenho é necessário a utilização de equipamentos mais modernos e eficientes, e sabendo-se que pela tecnologia e a robustez, pode-se ter um alto custo, para a implementação deste projeto, será necessário a aquisição de dois switches 24 portas gigabit ethernet multicamada.

3.3.3 Vantagens

Aplicando esta topologia, cada VLAN poderá utilizar até 254 dispositivos. A VLAN de gerenciamento terá acesso irrestrito ao datacenter, aos switches e as demais VLANs. A rede da FISICA será incorporada na VLAN 10 (FÍSICA), mantendo sua integridade, seus usuários e os arquivos serão migrados para o domínio existente da CLÍNICA. Com isto, não apresentará mais problemas de armazenamento e sua gerencia será de responsabilidade da CLÍNICA.

3.3.4 Escalabilidade

Em relação à escalabilidade, a rede proposta permitirá uma maior escalabilidade, permitindo que a rede cresça conforme a necessidade do administrador de redes. Pode-se verificar, por exemplo, o caso da VLAN 60, recepção na topologia proposta. É possível notar que os equipamentos estão dispostos em vários switches, mas fazem parte da mesma VLAN 60 (recepção). Nada impede também a ampliação da CLÍNICA, simplesmente criando uma nova VLAN ou adicionando dispositivos a uma VLAN existente.

3.3.5 Desempenho

Nesta topologia, o problema apresentado anteriormente referente ao trafego de *broadcast* que fica confinado na VLAN onde trafegam, evitando assim o congestionamento de quadros. Também o fato de diminuir o número de dispositivos que compartilham o mesmo canal logico melhora o tempo de resposta.

3.3.6 Segurança

A segurança é um dos principais motivos para implementação de VLANs, e seu uso permite que dispositivos em diferentes segmentos físicos em uma mesma VLAN, possam trocar informações sem que seus vizinhos tenham acesso às elas. A aplicação de segurança na infraestrutura da rede também pode evitar que pessoas mal-intencionadas, busquem capturar informações pela disseminação de pragas virtuais (vírus, *worms*, *malware*, *ransomware*, etc) ou através de *sniffers*, capturem ou sequestrem informações que possam ser interessantes para o invasor.

3.3.6.1 Segurança em portas

Segundo FELIPPETTI, os switches possuem uma série de mecanismos para evitar que usuários conectem dispositivos não autorizados, sem o conhecimento do administrador de rede. Segundo ele até 132 endereços MAC podem ser associados a uma interface de um switch, ou seja, um usuário qualquer pode trazer um *access-point* (AP) Wi-Fi e conecta-lo ao seu ponto de rede e pronto: a rede estará disponível a todos que se conectem a esse AP. Uma forma de limitar isso é usando os recursos de "*port-security*" disponíveis no IOS.

3.3.6.2 Desativando portas

Este é uma forma bem compreensível para se evitar a conexão de dispositivos sem o conhecimento e consentimento do administrador da rede. Seu método de aplicação é muito simples. Esse método foi aplicado em todos os switches multicamadas do projeto, bloqueando assim conexões suspeitas.

3.3.6.3 Seguranças sticky

A segurança sticky permite limitar a quantidade de dispositivos que podem ser conectados em uma determinada porta por meio do seu endereço físico (MAC). Esta limitação é aplicada pelo administrador da rede, permitindo somente os dispositivos legitimados por ele. Os demais dispositivos teriam o acesso recusado. Essa configuração é aplicada geralmente nos switches de camada de acesso.

3.3.6.4 Senhas seguras

Como pratica na prevenção de alterações nos equipamentos (switches) diretamente e sem o conhecimento do administrador de rede, adotou-se a

implementação de senhas seguras nos equipamentos. Para tal seguiu-se o padrão comumente utilizado que seria:

- ter no minimo 8 caracteres;
- ter no minimo 1 letras maiúsculas;
- ter no minimo 1 letra minúscula;
- ter no minimo 1 número.

Aconselha-se tambem a não utilizar a mesma senha para equipamentos diferentes. Apresentar um aviso legal de uso restrito, ativar a criptografia nos dispositivos para todas as senhas geradas. Sugere-se a utilização do protocolo SSH (Secure Shell), pois fornece uma conexão mais segura e criptografada. Não se recomenda a utilização do protocolo Telnet, pois não apresenta criptografia e uma conexão segura.

3.3.7 DHCP

Os responsáveis pela distribuição de endereços IPs nas VLANs serão os Switches multicamadas (SM01/SM02).

3.3.7.1 Pools DHCP

A Tabela 2 apresenta os pools DHCP que fora atribuído a cada VLAN. Para cada VLANs ficou determinado uma quantidade de 244 hosts e uma faixa de reserva de 10 IPs, ficou determinado que o gateway de cada VLAN seria o primeiro IP da rede VLAN e como servidor DNS primário o IP 10.0.200.1 e DNS secundário 10.0.200.2, os servidores ficarão na VLAN 200, mas o recomendado é deixá-los com endereço IP fixo.

Tabela 2 - Pools DHCP

Pool	Rede	DNS	Gateway	Faixa Excluida
RedeVlan10	10.0.10.0/24	10.0.200.1 -10.0.200.2	10.0.10.1	10.0.10.1-10.0.10.10
RedeVlan20	10.0.20.0/24	10.0.200.1 – 10.0.200.2	10.0.20.1	10.0.20.1-10.0.20.10
RedeVlan30	10.0.30.0/24	10.0.200.1 – 10.0.200.2	10.0.30.1	10.0.30.1-10.0.30.10
RedeVlan40	10.0.40.0/24	10.0.200.1 – 10.0.200.2	10.0.40.1	10.0.40.1-10.0.40.10
RedeVlan50	10.0.50.0/24	10.0.200.1 – 10.0.200.2	10.0.50.1	10.0.50.1-10.0.50.10
RedeVlan60	10.0.60.0/24	10.0.200.1 – 10.0.200.2	10.0.60.1	10.0.60.1-10.0.60.10
RedeVlan70	10.0.70.0/24	10.0.200.1 – 10.0.200.2	10.0.70.1	10.0.70.1-10.0.70.10
RedeVlan80	10.0.80.0/24	10.0.200.1 – 10.0.200.2	10.0.80.1	10.0.80.1-10.0.80.10
RedeVlan90	10.0.90.0/24	10.0.200.1 – 10.0.200.2	10.0.90.1	10.0.90.1-10.0.90.10
RedeVlan100	10.0.100.0/24	10.0.200.1 – 10.0.200.2	10.0.100.1	10.0.90.1-10.0.90.10
RedeVlan200	10.0.200.0/24	10.0.200.1 – 10.0.200.2	10.0.200.1	10.0.90.6-10.0.90.254

Autor: Autoria própria.

3.3.8 Redes de Gerenciamento

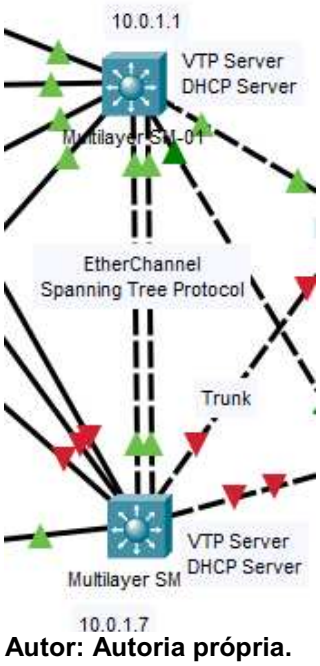
Determinado que a VLAN 100 será a rede responsável por todo o gerenciamento da infra. Essa terá acesso exclusivo a todos os switches e suas configurações, será responsável pela liberação, bloqueio e atribuições de VLANs as portas.

3.3.9 Switches

Os switches serão acessados somente para os computadores alocados na VLAN 100, todas as portas em desuso serão desabilitadas e será aplicado a politica de segurança *port-security sticks* onde será registrado o MAC ADDRESS do dispositivo conectado. Será possível o seu gerenciamento através de conexão remota pelo protocolo SSH (porta 22), com usuário (tecnico) e senha local (Clinica2020).

Os switches multicamadas (SM-01/SM-02) serão responsáveis pela propagação dos endereços IPs na rede, que tambem irão conter todas as ACLs e informações da VLANs existente (VTP Server). Haverá uma redundância entre eles através de uma porta EtherChannel/LACP (Figura 27) portas 23 e 24, onde no SM01 está habilitado no modo ativo e no SM-02 no modo passivo, em ambos os swiches está habilitado o protocolo *Spanning Tree* para as portas 23 e 24.

Figura 27 - Switches multicamadas



Autor: Autoria própria.

3.3.10 Topologia Física

Na Topologia da física atualmente existem dois switches de camada 3 que trabalham em redundância e estão ligados diretamente ao datacenter e aos demais switches por meio de cabo de par trançado Cat6, com uma taxa de transmissão de 1000 Mbps (1 Gbps). Também nesses switches está configurado o servidor VTP, contendo as informações de todas as VLANs existentes, os roteamentos e as regras de acesso.

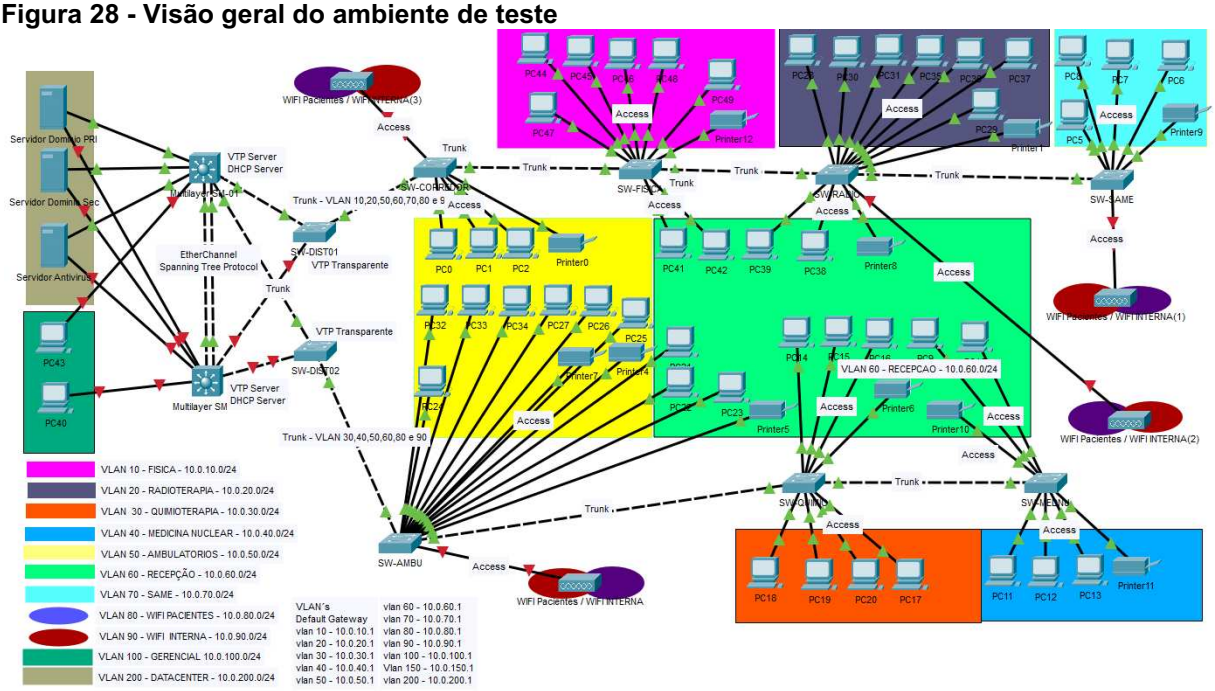
Os demais switches de distribuição e de bordas estarão conectados aos dispositivos exceto aos switches L3 por cabo UTP Cat5e, com uma taxa de transmissão de até 1000 Mbps (1 Gbps) e modo VTP Cliente ativo. Os switches pertencem a rede nativa e com endereçamento de IPs fixados, onde seu acesso é feito somente pela rede gerencial por meio de console SSH ou dashboard HTTPS.

3.4 AMBIENTE DE TESTES

3.4.1 Packet Tracer

Antes da apresentação da proposta, fizemos configurações em um simulador que permite simular um ambiente completo de rede, o Cisco Packet Tracer versão 7.3.0838 de 64 bits. Neste ambiente (Figura 28) foram feitas as configurações necessárias como VTP (server, transparente e cliente), foram criadas todas as VLans sugeridas, foram aplicadas as regras de ACLs e foram feitos os testes de intrusão e redundância. Neste ambiente também pode-se identificar as possíveis dificuldades que possam surgir e estes problemas podem ser corrigidos, para que não comprometa no momento da implantação.

Figura 28 - Visão geral do ambiente de teste



Autor: Autoria própria.

O Cisco Packet Tracer pode ser utilizado tanto no sistema operacional Windows (versões Desktops e Servers), distribuições Linux que usam a plataforma Debian (Ubuntu, Fedora, etc), macOS e dispositivos moveis (IOS e Android). O ambiente de simulação tem suporte aos seguintes equipamentos (Roteadores, Comutadores, *Host*, Concentradores, *Bridges*, *Wireless Access Points*, Roteadores Wireless, *Clouds* e *DSL/Cable modems*) e aos protocolos (Figura 29) comumente mais utilizados entre outros, também possui uma variedade de meios de conexões para interconectar esses dispositivos.

Figura 29 - Protocolos Packet Tracer

Categoria	Protocolos
LAN	Ethernet (incluindo CSMA/CD*), 802.11 wireless (conhecida como Wi-Fi)*
Comutadores (switch):	VLANs, 802.1q, trunking[EN], VTP, DTP, STP*, RSTP, switch multicamadas[EN], EtherChannel[EN]
TCP/IP:	HTTP, DHCP, DHCPv6, Telnet, SSH, TFTP, DNS, TCP*, UDP, IP, IPv6, ICMP, ICMPv6, ARP, IPv6 ND[EN]
Roteamento:	estático[EN], rota padrão, RIPv1, RIPv2, EIGRP, OSPF (simples e múltiplo), roteamento inter-VLAN
WAN:	HDLC, PPP, Frame Relay*
Outros:	ACLs (padrão, estendido e nominal), CDP, NAT (estático, dinâmico e overload), NATv6, Sniffer

Fonte: Autoria própria[13].

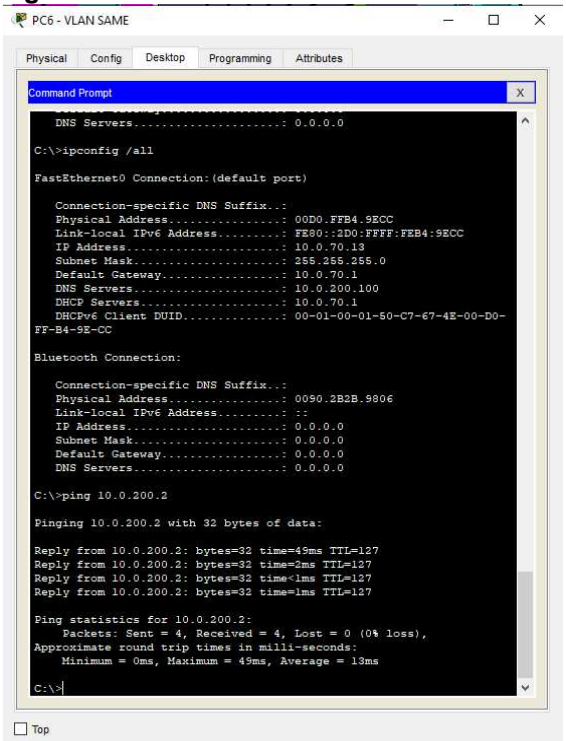
[13] Fonte: **Packet Tracer**. Wikipédia, A enciclopédia livre. Disponível em: <https://pt.wikipedia.org/wiki/Packet_Tracer#Protocolos>. Acesso em: 20 set. 2020.

3.4.1.1 Teste geral de conectividade

A infraestrutura apresentada ainda na Figura 28, apresenta detalhes físicos e lógicos da proposta de segmentação. Os equipamentos intermediários são compostos por nove switches de camada de enlace gerenciaveis de 24 portas: SW-DIST01 (Apêndice C), SW-DIST02 (Apêndice D), SW-CORREDOR (Apêndice E), SW-FISICA (Apêndice F), SW-RADIO (Apêndice G), SW-SAME (Apêndice H), SW-AMBU (Apêndice I), SW-QUIMIO (Apêndice J) e SW-MEDNU (Apêndice K), dois switches multicamadas (SM-01/SM-02) e 4 *access point* com suporte a VLANs. Infelizmente não foi possível simular a implementação de VLANs na rede wireless porque o Cisco Packet Tracer não tem suporte dos dispositivos wireless com VLANs.

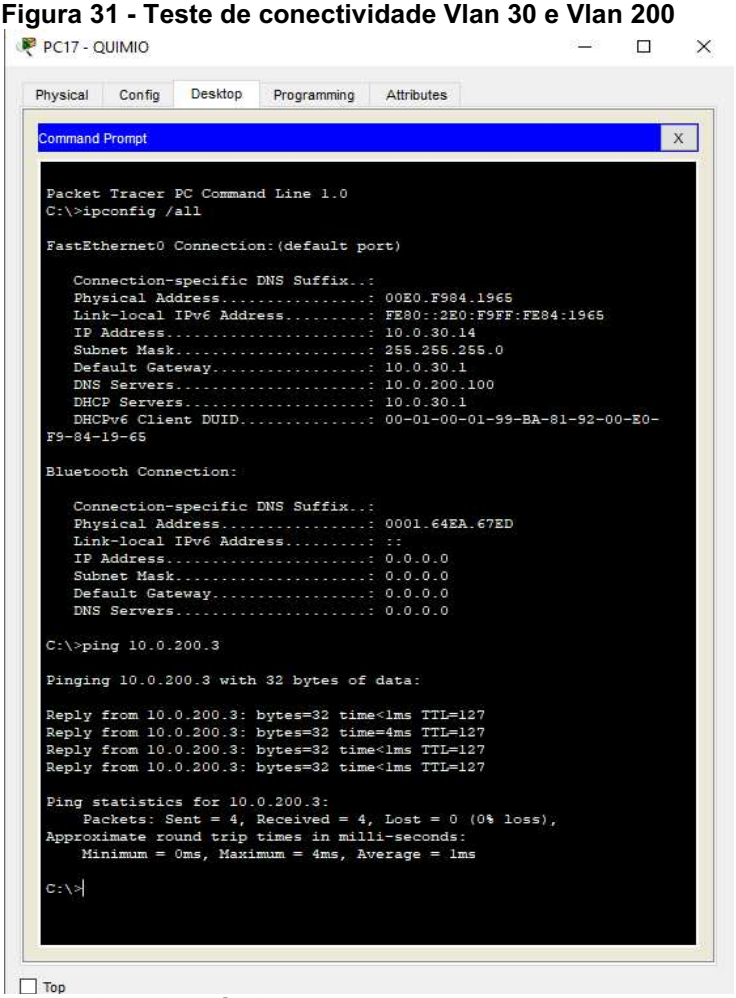
Nessa primeira etapa, foram feitos testes de conectividade, representado na Figura 30 com o comando ping, entre um computador utilizado na Vlan 70 – SAME (10.0.70.13) com o servidor de domínio primário (10.0.200.2) da Vlan 200 – DATA CENTER. Seguindo o mesmo padrão de testes com o comando ping, foi testado também a conectividade entre a Vlan 30 – QUIMIOTERAPIA (10.0.30.14) e o servidor de domínio secundário (10.0.200.3) da Vlan 200 – DATA CENTER, representado na Figura 31. Em ambos os testes fora obtido sucesso de conectividade.

Figura 30 - Teste de conectividade Vlan 70 e a Vlan 200



Autor: Autoria própria.

Figura 31 - Teste de conectividade Vlan 30 e Vlan 200

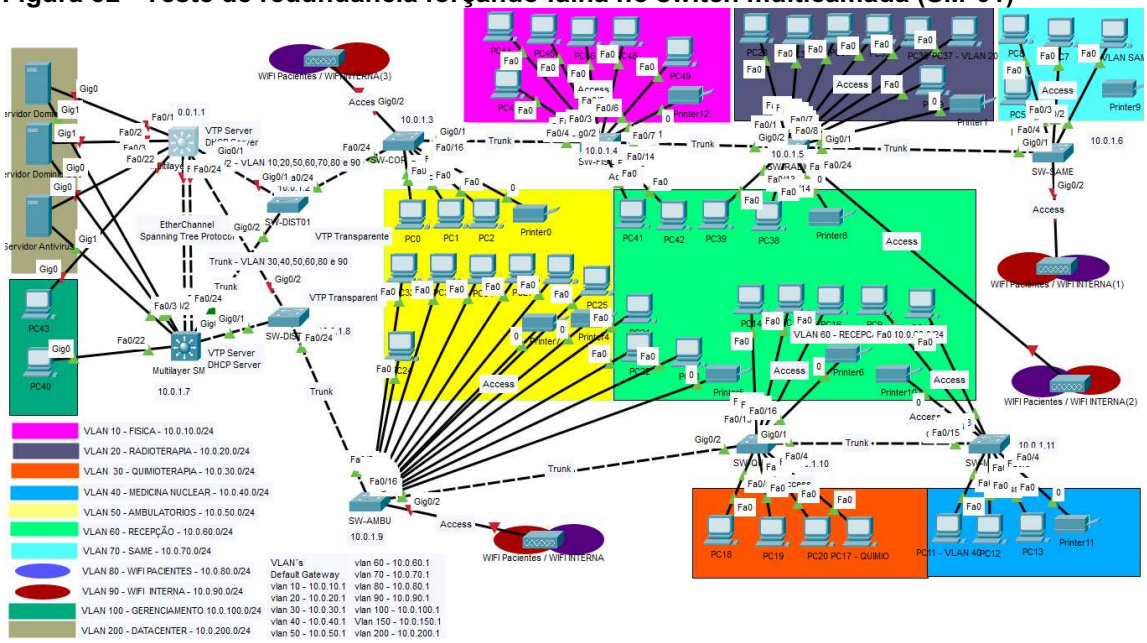


Autor: Autoria própria.

3.4.1.2 Teste geral de interruptabilidade

A proposta do modelo trás consigo a ideia de redundância no uso da rede, fazendo com que a mesma fique ineterrupta. Para simular uma falha, foi desativado o switch multicamada 1 (SM-01 – Apêndice A) (Figura 32), sendo assim todo o trafego de rede foi redirecionado para o switch multicamada 2 (SM-01 – Apêndice B). Esse teste objetivou simular a falha em um dos switches no ambiente que possa a ocorrer por ocasiões variadas.

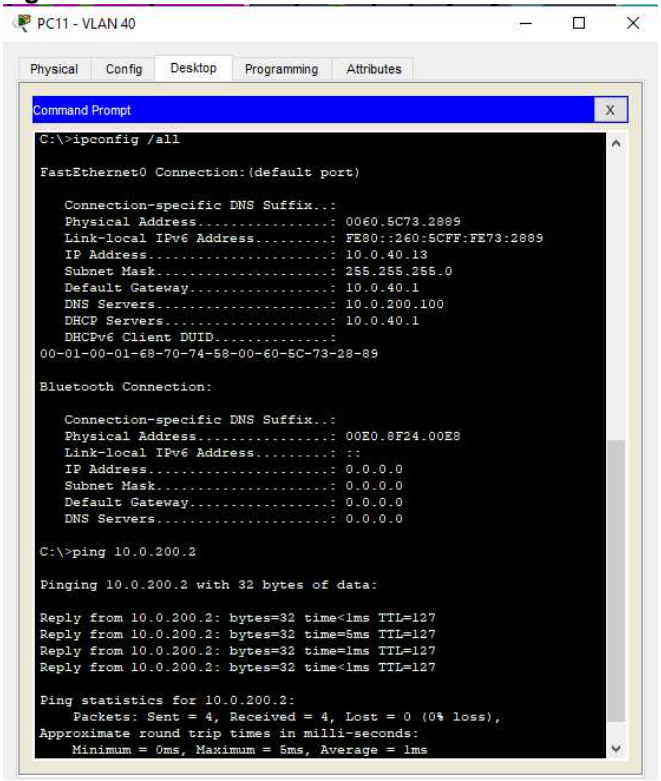
Figura 32 - Teste de redundância forçando falha no switch multicamada (SM-01)



Autor: Autoria própria.

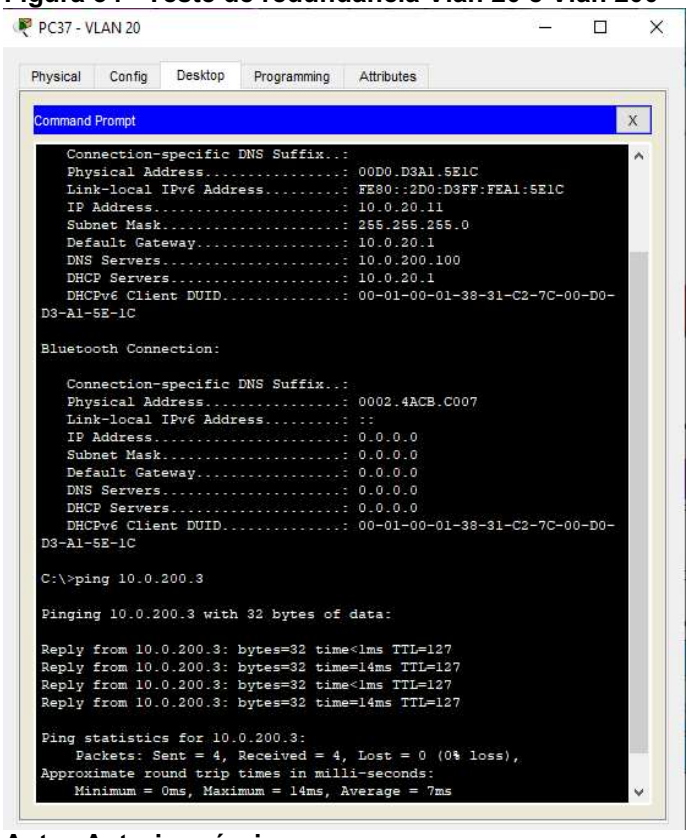
Para estes testes foi utilizado um computador na Vlan 40 (10.0.40.13) com o servidor de domínio primário na Vlan 200 (10.0.200.2) e o computador na Vlan 20 (10.0.20.11) com o servidor de antivírus na Vlan 200 (10.0.200.3), representados na Figura 33 e Figura 34 respectivamente.

Figura 33 - Teste de redundância Vlan 40 e Vlan 200



Autor: Autoria própria.

Figura 34 - Teste de redundância Vlan 20 e Vlan 200



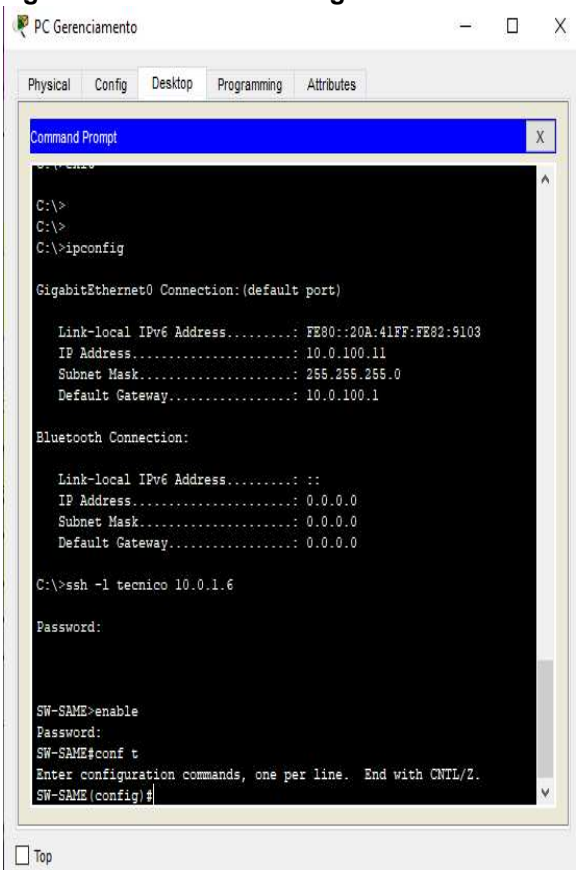
Autor:Autoria própria.

3.4.1.3 Teste de acesso remoto – rede de gerenciamento

No modelo adotado pela CLINICA, comumente necessitam a liberação de acesso a um novo dispositivo na rede, seja ele temporário ou permanente. Para isto é necessário ter acesso a estes dispositivos. Os computadores alocados na rede de gerenciamento (VLAN100) terão acesso remoto por meio de uma conexão SSH através de usuário local cadastrado nos dispositivos (técnico) e credenciais para este acesso (Clinica2020). Esses dispositivos estão configurados na VLAN 1 (10.0.0.0), VLAN padrão dos switches para gerenciamento.

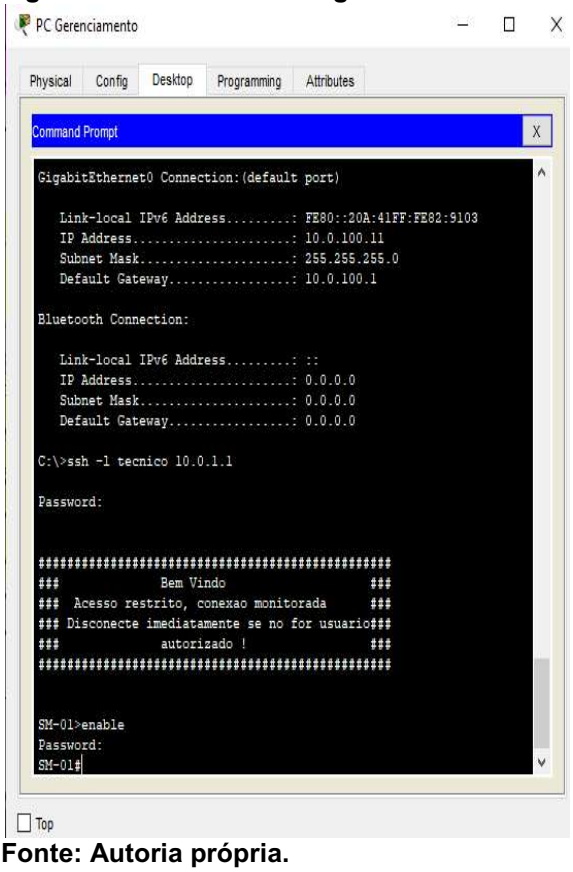
Foi testado a conectividade com o switch de camada de enlace (SW-SAME) e o switch multicamada (SM-01) representados nas Figuras 35 e 36. Utilizando a conexão SSH em ambas tentativas se obteve êxito.

Figura 35 - Conectivicade gerenciamento ao switch (SW-SAME)



Fonte: Autoria própria.

Figura 36 - Conectividade gerenciamento ao switch (SM-01)

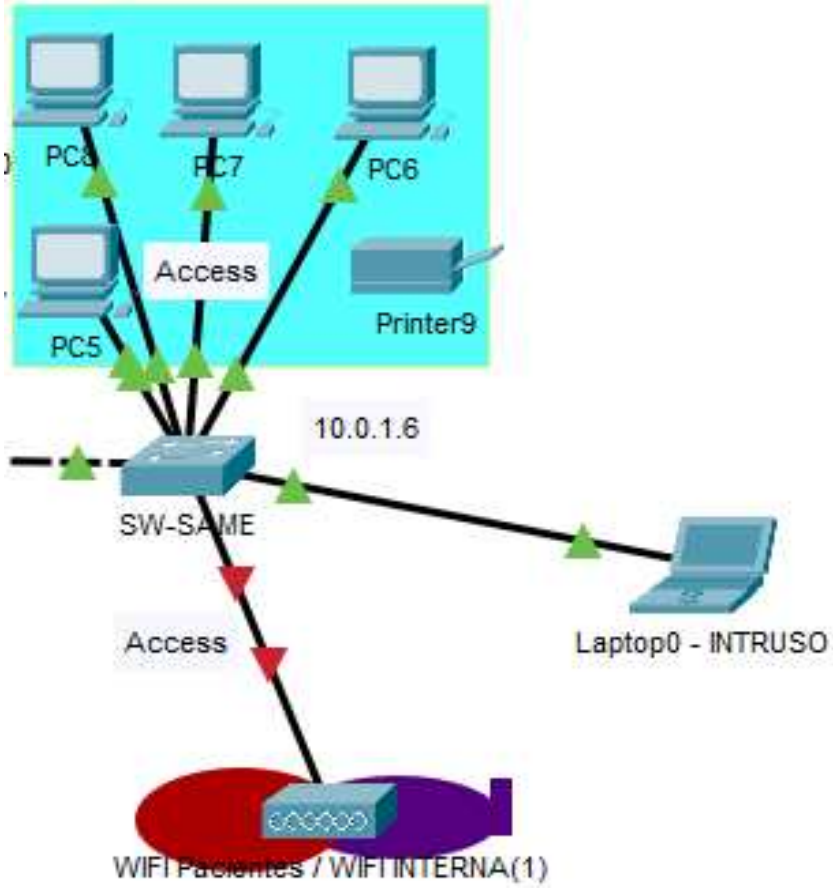


Fonte: Autoria própria.

3.4.1.4 Teste de segurança de portas

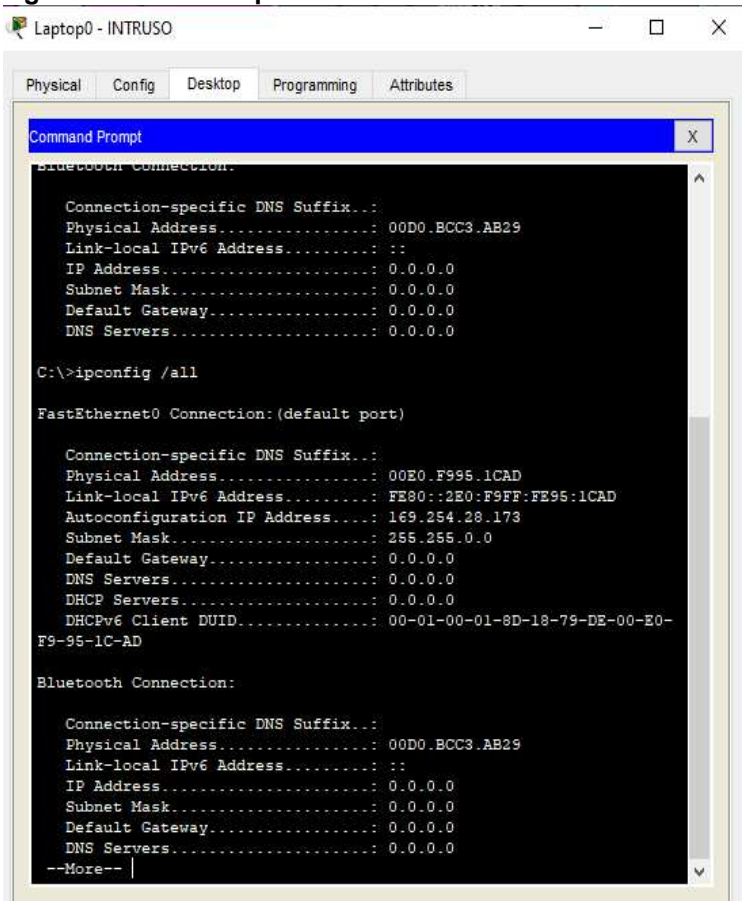
Para a realização desse teste fora utilizado um Laptop (Figura 37), onde plugando o mesmo em uma das portas livres do switch (SW-SAME) (Figura 38), o mesmo não obteve sucesso. Em outra tentativa, fora desconectado a impressora e na tentativa da utilização dessa porta que esta ativa (Figura 39), novamente não se obteve sucesso, pois em todos os switches foram aplicados as boas praticas de segurança que consiste em desabilitar as portas que não são utilizadas e aplicação da segurança *port-security* stick e port-security MAC, onde consiste em atrelar um determinado dispositivo a determinada porta. Seguindo as boas práticas o *Port-Security* não deve ser configurado em conjunto com os seguintes recursos: 802.1x, SPAN(Espelhamento) e EtherChannel.

Figura 37 - Tentativa de acesso não autorizado



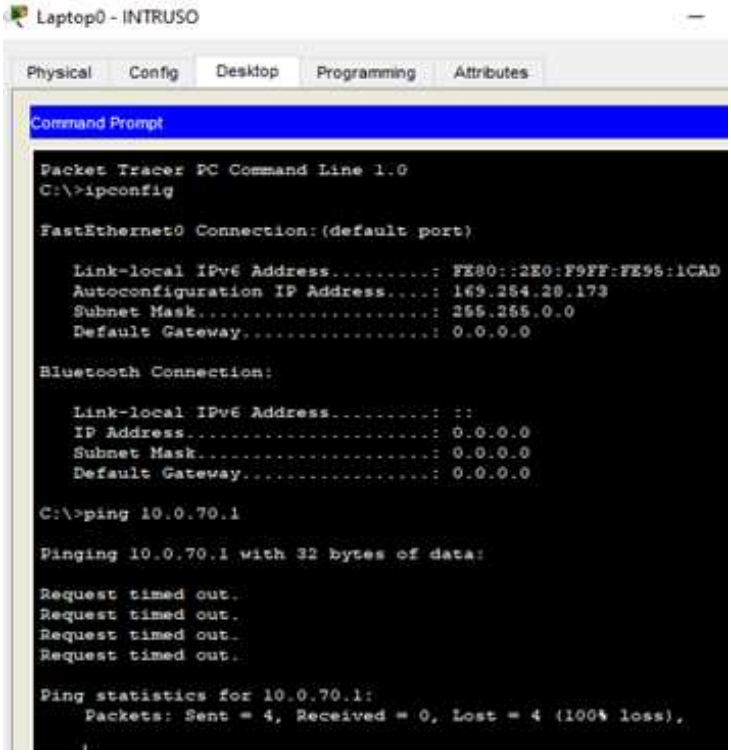
Autor: Autoria própria.

Figura 38 - Intruso / porta desabilitada



Autor: Autoria própria.

Figura 39 - Intruso / porta da impressora



Autor: Autoria própria.

4 CONCLUSÃO

O projeto e simulação da infraestrutura de redes da presente monografia teve o objetivo de aplicar as boas técnicas de implementação na rede atual. Após a simulação deste ambiente no simulador de redes Cisco Packet Tracer, chegou-se à conclusão que os equipamentos sugeridos e adotados atendem as necessidades da CLÍNICA, podendo ser implementados na topologia organizacional escolhida.

Como a escolha de implementação de alguns equipamentos de redes supera atualmente as necessidades da CLÍNICA, foi mantido a sua implementação pensando futuramente na necessidade da implementação de um software de gerenciamento e monitoramento, como por exemplo o Zabbix, que habilitando o protocolo SNMP nos servidores e switches, poderá ser utilizado na gerência da rede, pois irá receber informações preciosas sobre o funcionamento dos dispositivos de rede e irá ajudar o administrador da rede em suas decisões preventivas e corretivas.

O que tange a questões de segurança, o ambiente simulado se mostrou muito seguro, os problemas de broadcast foram solucionados e quanto as questões da conexão de equipamentos de terceiros, agora somente com permissão e conhecimento do administrador de rede. O administrador precisa sempre estar atendo as novas tecnologias evasivas e corretivas.

Em relação ao conhecimento das técnicas e práticas implementadas na simulação da infraestrutura de redes, o curso de especialização forneceu conhecimentos suficientes para a aplicação e reestruturação da infraestrutura de redes escolhida.

Como trabalhos futuros, indico a implementação de um sistema de gerência utilizando SNMP no sistema atual, para que o administrador de redes possa verificar mais rapidamente os possíveis erros e problemas que a rede possa ter.

REFERÊNCIAS

3COM. **Layer 3 switching - An introduction.** Disponível em: <http://www.zwaga.com/info/net/netwerk/pdf/Layer3Switching.pdf>. Acesso em: 06 ago. 2020.

ALENCAR, M. A. dos S. **Fundamentos e redes de computadores**. Manaus: Universidade Federal do Amazonas, Centro de Educação Tecnológica do Amazonas (CETAM), 2010. Disponível em: <http://pronatec.ifpr.edu.br/wp-content/uploads/2012/07/Instalador_e_Reparador_de_Redes_de_Computadores.pdf >. Acesso em: 05 ago. 2020.

BARROS, O. S. **Segurança de redes locais com a implementação de VLANs**. Universidade Jean Piaget de Cabo Verde, 2007.

CHANG, G.; HUANG, M. **Introduction to layer 2/3 switches**. Disponível em: <ftp://ftp.dlink.es/Switch/Miscellaneous/Manuali%20Tecnici%20comuni%20PDF/Switch-Layer3_1-8-01.pdf>. Acesso em: 29 ago. 2020.

CISCO. **Visão geral do TCP/IP**. Copyright© 1992-2020 Cisco, documento publicado em: 10 ago. 2005. Disponível em: <https://www.cisco.com/c/pt_br/support/docs/ip/routing-information-protocol-rip/13769-5.html#tcp>. Acesso em: 05 jul. 2020.

DANTAS, M. **Tecnologias de redes de comunicação e computadores**. Rio do Sul: Axcel Books, 2002.

DIAS, D. **VLan – Trunk utilizando 802.1q (dot1q). 2012**. Blog Comutadores, post publicado em: 15 out. 2010. Disponível em: <https://www.comutadores.com.br/vlan-trunk-utilizando-802-1q-dot1q/>. Acesso em: 29 jun. 2020.

DIOGENES**,** Y. **Certificação Cisco.** Rio de Janeiro: Axcel Books, 2004.

EDWARDS, J.; BRAMANTE, R. **Networking - Self teaching guide**.1. ed. Indianapolis: Wiley, 2009.

FILIPPETTI, M. A. **CCNA 6.0**: Guia Completo de Estudo**.** 2. ed. Rio de Janeiro: Alta Books, 2019.

FOROUZAN, B. A. **Comunicação de dados e rede de computadores.** 4. ed. Porto Alegre: AMGH Editora, 2010.

HAFFERMANN, L. **Segmentação de redes com VLAN**. Pós Graduação em Redes e Segurança de Sistemas. Pontifícia Universidade Católica do Paraná (PUC PR). Curitiba, 2009. Disponível em: <https://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Leonardo%20Haffermann%20-%20Artigo.pdf>. Acesso em: 15 set. 2020.

KUROSE, J. F.; ROSS, K. W. **Rede de computadores e a internet:** Uma Abordagem Top Down. 6. ed. São Paulo: Pearson, 2014.

LOWE, D. **Networking all-in-one for dummies**. 4. ed. Indianapolis: Wiley, 2011.

MORIMOTO, C. E. **Redes**: guia prático**.** Porto Alegre: Sul Editores, 2008.

PINTO, P. **Redes – Sabe o que é o modelo OSI?** Copyright© Pplware.com, artigo publicado em: 15 set. 2010. Disponível em: <https://pplware.sapo.pt/tutoriais/networking/redes-sabe-o-que-e-o-modelo-osi/>. Acesso em: 20 ago. 2020.

TANENBAUM, A. S.; WETHERALL, D. J. **Rede de computadores.** 5. ed. São Paulo: Pearson, 2011.

TAVARES, A. C. **VTP (LAN Trunk Protocol (VTP) – Estudo de caso**. O Curso CCNA da DlteC do Brasil, artigo publicado em 22 dez. 2011. Disponível em: <http://www.dltec.com.br/blog/cisco/vtp-vlan-trunk-protocol-estudo-de-caso-curso-ccna/>. Acesso em: 28 jun. 2020.

TORRES, G. **Redes de computadores**. 1. ed. Rio de Janeiro: Axcel Books do Brasil Editora, 2001.

APÊNDICE A: SWITCH MULTICAMADA 1

Nomeação de Dispositivo
Switch#enable
Switch#configure terminal
Switch(config)#hostname SM-01
Habilitando Roteamento
SM-01(config)#ip routing
SM-01(config)#interface fa 0/1
SM-01(config-if)#no switchport
SM-01(config-if)#ip address 10.0.0.254 255.255.255.0
SM-01(config-if)#no shut
SM-01(config-if)#exit
VLAN de Gerênciamento
SM-01(config)#int vlan 1
SM-01(config-if)#ip address 10.0.1.1 255.255.255.0
SM-01(config-if)#no shut
SM-01(config-if)#exit
SM-01(config)#ip default-gateway 10.0.1.1
Configurações de VLANs
SM-01(config)#vlan 10
SM-01(config-vlan)#name FISICA
SM-01(config-vlan)#int vlan 10
SM-01(config-if)#ip address 10.0.10.1 255.255.255.0
SM-01(config-if)#ip helper-address 10.0.0.1
SM-01(config-if)#no shut
SM-01(config)#vlan 20
SM-01(config-vlan)#name RADIOTERAPIA
SM-01(config-vlan)#int vlan 20
SM-01(config-if)#ip address 10.0.20.1 255.255.255.0
SM-01(config-if)#ip helper-address 10.0.0.1
SM-01(config-if)#no shut
SM-01(config)#vlan 30
SM-01(config-vlan)#name QUIMIOTERAPIA
SM-01(config-vlan)#int vlan 30
SM-01(config-if)#ip address 10.0.30.1 255.255.255.0
SM-01(config-if)#ip helper-address 10.0.0.1
SM-01(config-if)#no shut
SM-01(config)#vlan 40
SM-01(config-vlan)#name MEDICINA-NUCLEAR
SM-01(config-vlan)#int vlan 40
SM-01(config-if)#ip address 10.0.40.1 255.255.255.0
SM-01(config-if)#ip helper-address 10.0.0.1
SM-01(config)#vlan 50
SM-01(config-vlan)#name AMBULATORIOS
SM-01(config-vlan)#int vlan 50
SM-01(config-if)#ip address 10.0.50.1 255.255.255.0
SM-01(config-if)#ip helper-address 10.0.0.1
SM-01(config)#vlan 60
SM-01(config-vlan)#name RECEPCAO
SM-01(config-vlan)#int vlan 60
SM-01(config-if)#ip address 10.0.60.1 255.255.255.0
SM-01(config-if)#ip helper-address 10.0.0.1
SM-01(config)#vlan 70
SM-01(config-vlan)#name SAME
SM-01(config-vlan)#int vlan 70
SM-01(config-if)#ip address 10.0.70.1 255.255.255.0
SM-01(config-if)#ip helper-address 10.0.0.1
SM-01(config)#vlan 80

```
SM-01(config-vlan)#name WIFI-VISITANTES
SM-01(config-vlan)#int vlan 80
SM-01(config-if)#ip address 10.0.80.1 255.255.255.0
SM-01(config-if)#ip helper-address 10.0.0.1
SM-01(config)#vlan 90
SM-01(config-vlan)#name WIFI-INTERNA
SM-01(config-vlan)#int vlan 90
SM-01(config-if)#ip address 10.0.90.1 255.255.255.0
SM-01(config-if)#ip helper-address 10.0.0.1
SM-01(config)#vlan 100
SM-01(config-vlan)#name DISPOSITIVOS
SM-01(config-vlan)#int vlan 100
SM-01(config-if)#ip address 10.0.100.1 255.255.255.0
SM-01(config-if)#ip helper-address 10.0.0.1
SM-01(config)#int gigabitEthernet 0/1
SM-01(config-if)#switchport trunk encapsulation dot1q
SM-01(config-if)#switchport mode trunk
SM-01(config-if)#switchport trunk allowed vlan 1,10,20,50,60,70
SM-01(config)#int gigabitEthernet 0/2
SM-01(config-if)#switchport trunk encapsulation dot1q
SM-01(config-if)#switchport mode trunk
SM-01(config-if)#switchport trunk allowed vlan 1,30,40,50,60
SM-01(config-if)#exit
```

Configurando modo VTP

```
SM-01(config)#vtp mode server
SM-01(config)#vtp domain clinica.interno.local
SM-01(config)#vtp pass Cl1n1c@2020
```

Configuração do STP

```
SM-01(config)#spanning-tree vlan 10,20,30,40,50,60,70,80,90,100 root primary
```

Desativação de Portas Ociosas

```
SM-01(config)#interface range fastEthernet 0/4-22
SM-01(config-if-range)#shut
SM-01(config-if-range)#exit
```

Configuração do EtherChannel/LACP

```
SM-01(config)#interface range FastEthernet 0/23-24
SM-01(config-if-range)#channel-group 1 mode active
SM-01(config-if-range)#exit
```

Configuração de Acesso Remoto SSH

```
SM-01(config)#enable secret Clinica2020
SM-01(config)#ip domain-name clinica.interno.local
SM-01(config)#crypto key generate rsa <1024>
SM-01(config)#username tecnico priv 0 secret Clinica2020
SM-01(config)#line vty 0 4
SM-01(config-line)#login local
SM-01(config-line)#transport input ssh
SM-01(config-line)#exit
```

Configuração dos pools DHCP

```
SM-01(config)#ip dhcp pool RedeVlan10
SM-01(dhcp-config)#network 10.0.10.0 255.255.255.0
SM-01(dhcp-config)#default-router 10.0.10.1
SM-01(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
SM-01(dhcp-config)#ip dhcp pool RedeVlan20
SM-01(dhcp-config)#network 10.0.20.0 255.255.255.0
SM-01(dhcp-config)#default-router 10.0.20.1
SM-01(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
SM-01(dhcp-config)#ip dhcp pool RedeVlan30
SM-01(dhcp-config)#network 10.0.30.0 255.255.255.0
SM-01(dhcp-config)#default-router 10.0.30.1
SM-01(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
SM-01(dhcp-config)#ip dhcp pool RedeVlan40
```

```
SM-01(dhcp-config)#network 10.0.40.0 255.255.255.0
SM-01(dhcp-config)#default-router 10.0.40.1
SM-01(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
SM-01(dhcp-config)#ip dhcp pool RedeVlan50
SM-01(dhcp-config)#network 10.0.50.0 255.255.255.0
SM-01(dhcp-config)#default-router 10.0.50.1
SM-01(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
SM-01(dhcp-config)#ip dhcp pool RedeVlan60
SM-01(dhcp-config)#network 10.0.60.0 255.255.255.0
SM-01(dhcp-config)#default-router 10.0.60.1
SM-01(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
SM-01(dhcp-config)#ip dhcp pool RedeVlan70
SM-01(dhcp-config)#network 10.0.70.0 255.255.255.0
SM-01(dhcp-config)#default-router 10.0.70.1
SM-01(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
SM-01(dhcp-config)#ip dhcp pool RedeVlan80
SM-01(dhcp-config)#network 10.0.80.0 255.255.255.0
SM-01(dhcp-config)#default-router 10.0.80.1
SM-01(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
SM-01(dhcp-config)#ip dhcp pool RedeVlan90
SM-01(dhcp-config)#network 10.0.90.0 255.255.255.0
SM-01(dhcp-config)#default-router 10.0.90.1
SM-01(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
SM-01(dhcp-config)#ip dhcp pool RedeVlan100
SM-01(dhcp-config)#network 10.0.100.0 255.255.255.0
SM-01(dhcp-config)#default-router 10.0.100.1
SM-01(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
SM-01(dhcp-config)#ip dhcp pool RedeVlan200
SM-01(dhcp-config)#network 10.0.200.0 255.255.255.0
SM-01(dhcp-config)#default-router 10.0.200.1
SM-01(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
```

Reservas de IPs

```
SM-01(dhcp-config)#host 10.0.200.2 255.255.255.0
SM-01(dhcp-config)#hardware-address
SM-01(dhcp-config)#client-name SRV-DC01
SM-01(dhcp-config)#host 10.0.200.3 255.255.255.0
SM-01(dhcp-config)#hardware-address
SM-01(dhcp-config)#client-name SRV-DC02
SM-01(dhcp-config)#host 10.0.200.4 255.255.255.0
SM-01(dhcp-config)#hardware-address
SM-01(dhcp-config)#client-name SRV-Antivirus
SM-01(dhcp-config)#exit
```

Faixa de Ips Excluidos do Range DHCP

```
SM-01(config)#ip dhcp excluded-address 10.0.10.1 10.0.10.10
SM-01(config)#ip dhcp excluded-address 10.0.20.1 10.0.20.10
SM-01(config)#ip dhcp excluded-address 10.0.30.1 10.0.30.10
SM-01(config)#ip dhcp excluded-address 10.0.40.1 10.0.40.10
SM-01(config)#ip dhcp excluded-address 10.0.50.1 10.0.50.10
SM-01(config)#ip dhcp excluded-address 10.0.60.1 10.0.60.10
SM-01(config)#ip dhcp excluded-address 10.0.70.1 10.0.70.10
SM-01(config)#ip dhcp excluded-address 10.0.80.1 10.0.80.10
SM-01(config)#ip dhcp excluded-address 10.0.90.1 10.0.90.10
SM-01(config)#ip dhcp excluded-address 10.0.100.1 10.0.100.10
SM-01(config)#ip dhcp excluded-address 10.0.200.6 10.0.200.254
SM-01(config)#exit
```

APÊNDICE B: SWITCH MULTICAMADA 2

Nomeação de Dispositivo
Switch#enable
Switch#configure terminal
Switch(config)#hostname SM-02
Habilitando Roteamento
SM-02(config)#ip routing
SM-02(config)#interface fa 0/1
SM-02(config-if)#no switchport
SM-02(config-if)#ip address 10.0.0.254 255.255.255.0
SM-02(config-if)#no shut
SM-02(config-if)#exit
Vlan de Gerênciamento
SM-02(config)#int vlan 1
SM-02(config-if)#ip address 10.0.1.7 255.255.255.0
SM-02(config-if)#no shut
SM-02(config-if)#exit
SM-02(config)#ip default-gateway 10.0.1.1
Configurações de VLANs
SM-02(config)#vlan 10
SM-02(config-vlan)#name FISICA
SM-02(config-vlan)#int vlan 10
SM-02(config-if)#ip address 10.0.10.1 255.255.255.0
SM-02(config-if)#ip helper-address 10.0.0.1
SM-02(config-if)#no shut
SM-02(config)#vlan 20
SM-02(config-vlan)#name RADIOTERAPIA
SM-02(config-vlan)#int vlan 20
SM-02(config-if)#ip address 10.0.20.1 255.255.255.0
SM-02(config-if)#ip helper-address 10.0.0.1
SM-02(config-if)#no shut
SM-02(config)#vlan 30
SM-02(config-vlan)#name QUIMIOTERAPIA
SM-02(config-vlan)#int vlan 30
SM-02(config-if)#ip address 10.0.30.1 255.255.255.0
SM-02(config-if)#ip helper-address 10.0.0.1
SM-02(config-if)#no shut
SM-02(config)#vlan 40
SM-02(config-vlan)#name MEDICINA-NUCLEAR
SM-02(config-vlan)#int vlan 40
SM-02(config-if)#ip address 10.0.40.1 255.255.255.0
SM-02(config-if)#ip helper-address 10.0.0.1
SM-02(config)#vlan 50
SM-02(config-vlan)#name AMBULATORIOS
SM-02(config-vlan)#int vlan 50
SM-02(config-if)#ip address 10.0.50.1 255.255.255.0
SM-02(config-if)#ip helper-address 10.0.0.1
SM-02(config)#vlan 60
SM-02(config-vlan)#name RECEPCAO
SM-02(config-vlan)#int vlan 60
SM-02(config-if)#ip address 10.0.60.1 255.255.255.0
SM-02(config-if)#ip helper-address 10.0.0.1
SM-02(config)#vlan 70
SM-02(config-vlan)#name SAME
SM-02(config-vlan)#int vlan 70
SM-02(config-if)#ip address 10.0.70.1 255.255.255.0
SM-02(config-if)#ip helper-address 10.0.0.1
SM-02(config)#vlan 80

```
SM-02(config-vlan)#name WIFI-VISITANTES
SM-02(config-vlan)#int vlan 80
SM-02(config-if)#ip address 10.0.80.1 255.255.255.0
SM-02(config-if)#ip helper-address 10.0.0.1
SM-02(config)#vlan 90
SM-02(config-vlan)#name WIFI-INTERNA
SM-02(config-vlan)#int vlan 90
SM-02(config-if)#ip address 10.0.90.1 255.255.255.0
SM-02(config-if)#ip helper-address 10.0.0.1
SM-02(config)#vlan 100
SM-02(config-vlan)#name DISPOSITIVOS
SM-02(config-vlan)#int vlan 100
SM-02(config-if)#ip address 10.0.100.1 255.255.255.0
SM-02(config-if)#ip helper-address 10.0.0.1
SM-02(config)#int gigabitEthernet 0/1
SM-02(config-if)#switchport trunk encapsulation dot1q
SM-02(config-if)#switchport mode trunk
SM-02(config-if)#switchport trunk allowed vlan 30,40,50,60
SM-02(config)#int gigabitEthernet 0/2
SM-02(config-if)#switchport trunk encapsulation dot1q
SM-02(config-if)#switchport mode trunk
SM-02(config-if)#switchport trunk allowed vlan 10,20,50,60,70
SM-02(config-if)#exit
```

Configurando modo VTP

```
SM-02(config)#vtp mode server
SM-02(config)#vtp domain clinica.interno.local
SM-02(config)#vtp pass Cl1n1c@2020
```

Configuração do STP

```
SM-02(config)#spanning-tree vlan 10,20,30,40,50,60,70,80,90,100 root primary
```

Desativação de Portas Ociosas

```
SM-02(config)#interface range fastEthernet 0/4-22
SM-02(config-if-range)#shut
SM-02(config-if-range)#exit
```

Configuração do EtherChannel/LACP

```
SM-02(config)#interface range FastEthernet 0/23-24
SM-02(config-if-range)#channel-group 1 mode passive
SM-02(config-if-range)#exit
```

Configuração de Acesso Remoto SSH

```
SM-02(config)#enable secret Clinica2020
SM-02(config)#ip domain-name clinica.interno.local
SM-02(config)#crypto key generate rsa <1024>
SM-02(config)#username tecnico priv 0 secret Clinica2020
SM-02(config)#line vty 0 4
SM-02(config-line)#login local
SM-02(config-line)#transport input ssh
SM-02(config-line)#exit
```

Configuração dos pools DHCP

```
SM-02(config)#ip dhcp pool RedeVlan10
SM-02(dhcp-config)#network 10.0.10.0 255.255.255.0
SM-02(dhcp-config)#default-router 10.0.10.1
SM-02(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
SM-02(dhcp-config)#ip dhcp pool RedeVlan20
SM-02(dhcp-config)#network 10.0.20.0 255.255.255.0
SM-02(dhcp-config)#default-router 10.0.20.1
SM-02(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
SM-02(dhcp-config)#ip dhcp pool RedeVlan30
SM-02(dhcp-config)#network 10.0.30.0 255.255.255.0
SM-02(dhcp-config)#default-router 10.0.30.1
SM-02(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
SM-02(dhcp-config)#ip dhcp pool RedeVlan40
```

```
SM-02(dhcp-config)#network 10.0.40.0 255.255.255.0
SM-02(dhcp-config)#default-router 10.0.40.1
SM-02(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
SM-02(dhcp-config)#ip dhcp pool RedeVlan50
SM-02(dhcp-config)#network 10.0.50.0 255.255.255.0
SM-02(dhcp-config)#default-router 10.0.50.1
SM-02(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
SM-02(dhcp-config)#ip dhcp pool RedeVlan60
SM-02(dhcp-config)#network 10.0.60.0 255.255.255.0
SM-02(dhcp-config)#default-router 10.0.60.1
SM-02(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
SM-02(dhcp-config)#ip dhcp pool RedeVlan70
SM-02(dhcp-config)#network 10.0.70.0 255.255.255.0
SM-02(dhcp-config)#default-router 10.0.70.1
SM-02(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
SM-02(dhcp-config)#ip dhcp pool RedeVlan80
SM-02(dhcp-config)#network 10.0.80.0 255.255.255.0
SM-02(dhcp-config)#default-router 10.0.80.1
SM-02(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
SM-02(dhcp-config)#ip dhcp pool RedeVlan90
SM-02(dhcp-config)#network 10.0.90.0 255.255.255.0
SM-02(dhcp-config)#default-router 10.0.90.1
SM-02(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
SM-02(dhcp-config)#ip dhcp pool RedeVlan100
SM-02(dhcp-config)#network 10.0.100.0 255.255.255.0
SM-02(dhcp-config)#default-router 10.0.100.1
SM-02(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
SM-02(dhcp-config)#ip dhcp pool RedeVlan200
SM-02(dhcp-config)#network 10.0.200.0 255.255.255.0
SM-02(dhcp-config)#default-router 10.0.200.1
SM-02(dhcp-config)#dns-server 10.0.200.2 10.0.200.3
```

Reservas de IPs

```
SM-02(dhcp-config)#host 10.0.200.2 255.255.255.0
SM-02(dhcp-config)#hardware-address
SM-02(dhcp-config)#client-name SRV-dc01
SM-02(dhcp-config)#host 10.0.200.3 255.255.255.0
SM-02(dhcp-config)#hardware-address
SM-02(dhcp-config)#client-name SRV-DC02
SM-02(dhcp-config)#host 10.0.200.4 255.255.255.0
SM-02(dhcp-config)#hardware-address
SM-02(dhcp-config)#client-name SRV-Antivirus
SM-02(dhcp-config)#exit
```

Faixa de Ips Excluidos do Range DHCP

```
SM-02(config)#ip dhcp excluded-address 10.0.10.1 10.0.10.10
SM-02(config)#ip dhcp excluded-address 10.0.20.1 10.0.20.10
SM-02(config)#ip dhcp excluded-address 10.0.30.1 10.0.30.10
SM-02(config)#ip dhcp excluded-address 10.0.40.1 10.0.40.10
SM-02(config)#ip dhcp excluded-address 10.0.50.1 10.0.50.10
SM-02(config)#ip dhcp excluded-address 10.0.60.1 10.0.60.10
SM-02(config)#ip dhcp excluded-address 10.0.70.1 10.0.70.10
SM-02(config)#ip dhcp excluded-address 10.0.80.1 10.0.80.10
SM-02(config)#ip dhcp excluded-address 10.0.90.1 10.0.90.10
SM-02(config)#ip dhcp excluded-address 10.0.100.1 10.0.100.10
SM-02(config)#ip dhcp excluded-address 10.0.200.6 10.0.200.254
SM-02(config)#exit
```

APÊNDICE C: SWITCH DE DISTRIBUIÇÃO 01

Nomeação do Dispositivo
Switch>enable
Switch#conf t
Switch(config)#hostname SW-DIST01
Vlan de Gerênciamento
SW-DIST01((config)#int vlan 1
SW-DIST01 (config-if)#ip address 10.0.1.2 255.255.255.0
SW-DIST01 (config-if)#no shut
SW-DIST01 (config-if)#exit
SW-DIST01 (config)#ip default-gateway 10.0.1.1
Configuração Truncamento de Portas
SW-DIST01(config)#int gigabitEthernet 0/1
SW-DIST01(config-if)#switchport mode trunk
SW-DIST01(config-if)#no shut
SW-DIST01(config-if)#exit
SW-DIST01(config)#int fastEthernet 0/24
SW-DIST01(config-if)#switchport mode trunk
SW-DIST01(config-if)#no shut
SW-DIST01(config-if)#exit
Configuração modo VTP
SW-DIST01(config)#vtp mode transparent
Desativação de Portas Ociosa
SW-DIST01(config)#int range fa 0/1-23
SW-DIST01(config-if-range)#shut
SW-DIST01(config-if-range)#exit
Configuração de Acesso Remoto SSH
SW-DIST01(config)#enable secret Clinica2020
SW-DIST01(config)#ip domain-name clinica.interno.local
SW-DIST01(config)#crypto key generate rsa <1024>
SW-DIST01(config)#username tecnico priv 0 secret Clinica2020
SW-DIST01(config)#line vty 0 4
SW-DIST01(config-line)#login local
SW-DIST01(config-line)#transport input ssh
SW-DIST01(config-line)#end

APÊNDICE D: SWITCH DE DISTRIBUIÇÃO 02

Nomeação do Dispositivo
Switch>enable
Switch#conf t
Switch(config)#hostname SW-DIST02
Vlan de Gerênciamento
SW-DIST02(config)#int vlan 1
SW-DIST02(config-if)#ip address 10.0.1.8 255.255.255.0
SM-DIST02(config-if)#no shut
SM-DIST02(config-if)#exit
SM-DIST02(config)#ip default-gateway 10.0.1.1
Configuração modo VTP
SW-DIST02(config)#vtp mode transparente
Configuração Truncamento de Portas
SW-DIST02(config)#interface gigabitEthernet 0/2
SW-DIST02(config-if)#switchport mode trunk
SW-DIST02(config-if)#no shut
SW-DIST02(config-if)#exit
SW-DIST02(config)#int fastEthernet 0/24
SW-DIST02(config-if)#switchport mode trunk
SW-DIST02(config-if)#no shut
SW-DIST02(config-if)#exit
Desativação de Portas Ociosa
SW-DIST02(config)#int range fastEthernet 0/1-23
SW-DIST02(config-if-range)#shut
SW-DIST02(config-if-range)#end
Configuração de Acesso Remoto SSH
SW-DIST02(config)#enable secret Clinica2020
SW-DIST02(config)#ip domain-name clinica.interno.local
SW-DIST02(config)#crypto key generate rsa <1024>
SW-DIST02(config)#username tecnico priv 0 secret Clinica2020
SW-DIST02(config)#line vty 0 4
SW-DIST02(config-line)#login local
SW-DIST02(config-line)#transport input ssh
SW-DIST02(config-line)#end

APÊNDICE E: SWITCH CORREDOR

Nomeação do Dispositivo
Switch>enable
Switch#conf t
Switch(config)#hostname SW-CORREDOR
Vlan de Gerênciamento
SW-CORREDOR(config)#int vlan 1
SW-CORREDOR(config-if)#ip address 10.0.1.3 255.255.255.0
SW-CORREDOR(config-if)#no shut
SW-CORREDOR(config-if)#exit
SW-CORREDOR(config)#ip default-gateway 10.0.1.1
Configuração Truncamento de Portas
SW-CORREDOR(config)#int fastEthernet 0/24
SW-CORREDOR(config-if)#switchport mode trunk
SW-CORREDOR(config-if)#no shut
SW-CORREDOR(config-if)#exit
SW-CORREDOR(config)#int gigabitEthernet 0/1
SW-CORREDOR(config-if)#switchport mode trunk
SW-CORREDOR(config-if)#no shut
SW-CORREDOR(config-if)#exit
Configuração Modo VTP
SW-CORREDOR(config)#vtp mode client
SW-CORREDOR(config)#vtp domain clinica.interno.local
SW-CORREDOR(config)#vtp pass Cl1n1c@2020
Desativação de Portas Ociosa
SW-CORREDOR(config)#int range fastEthernet 0/1-23
SW-CORREDOR(config-if-range)#shut
SW-CORREDOR(config-if-range)#exit
SW-CORREDOR(config)#int gigabitEthernet 0/2
SW-CORREDOR(config-if)#shut
SW-CORREDOR(config-if)#exit
Configuração de Segurança e Portas de Acesso
SW-CORREDOR(config)#int range fastEthernet 0/13-16
SW-CORREDOR(config-if-range)#switchport mode access
SW-CORREDOR(config-if-range)#switchport access vlan 50
SW-CORREDOR(config-if-range)#switchport port-security
SW-CORREDOR(config-if-range)#switchport port-security maximum 1
SW-CORREDOR(config-if-range)#switchport port-security violation restrict
SW-CORREDOR(config-if-range)#no shut
SW-CORREDOR(config-if-range)#exit
SW-CORREDOR(config)#int fastEthernet 0/13
SW-CORREDOR(config-if)#switchport port-security mac-address 0001.647B.24CB
SW-CORREDOR(config-if)#exit
SW-CORREDOR(config)#int fastEthernet 0/14
SW-CORREDOR(config-if)#switchport port-security mac-address 00D0.5868.9408
SW-CORREDOR(config-if)#exit
SW-CORREDOR(config)#int fastEthernet 0/15
SW-CORREDOR(config-if)#switchport port-security mac-address 0090.0C49.616B
SW-CORREDOR(config-if)#exit
SW-CORREDOR(config)#int fastEthernet 0/16
SW-CORREDOR(config-if)#switchport port-security mac-address 0002.4A71.037B
SW-CORREDOR(config-if)#exit

Configuração de Acesso Remoto SSH

```
SW-CORREDOR(config)#enable secret Clinica2020
SW-CORREDOR(config)#ip domain-name clinica.interno.local
SW-CORREDOR(config)#crypto key generate rsa <1024>
SW-CORREDOR(config)#username tecnico priv 0 secret Clinica2020
SW-CORREDOR(config)#line vty 0 4
SW-CORREDOR(config-line)#login local
SW-CORREDOR(config-line)#transport input ssh
SW-CORREDOR(config-line)#end
```

APÊNDICE F: SWITCH FISICA

Nomeação do Dispositivo
Switch>enable
Switch#conf t
Switch(config)#hostname SW-FISICA
Vlan de Gerênciamento
SW-FISICA(config)#int vlan 1
SW-FISICA(config-if)#ip address 10.0.1.4 255.255.255.0
SW-FISICA(config-if)#no shut
SW-FISICA(config-if)#exit
SW-FISICA(config)#ip default-gateway 10.0.1.1
Configuração modo VTP
SW-FISICA(config)#vtp mode client
SW-FISICA(config)#vtp domain clinica.interno.local
SW-FISICA(config)#vtp pass Cl1n1c@2020
Configuração Truncamento de Portas
SW-FISICA(config)#int gigabitEthernet 0/1
SW-FISICA(config-if)#switchport mode trunk
SW-FISICA(config-if)#no shut
SW-FISICA(config-if)#int gigabitEthernet 0/2
SW-FISICA(config-if)#switchport mode trunk
SW-FISICA(config-if)#no shut
SW-FISICA(config-if)#exit
Desativação de Portas Ociosas
SW-FISICA(config)#int range fastEthernet 0/8-12
SW-FISICA(config-if-range)#shut
SW-FISICA(config-if-range)#exit
SW-FISICA(config)#int range fastEthernet 0/15-24
SW-FISICA(config-if-range)#shut
SW-FISICA(config-if-range)#exit
Configuração de Segurança e Portas de Acesso
SW-FISICA(config)#int range fastEthernet 0/1-7
SW-FISICA(config-if-range)#switchport mode access
SW-FISICA(config-if-range)#switchport access vlan 10
SW-FISICA(config-if-range)#switchport port-security
SW-FISICA(config-if-range)#switchport port-security maximum 1
SW-FISICA(config-if-range)#switchport port-security violation restrict
SW-FISICA(config-if-range)#no shut
SW-FISICA(config-if-range)#exit
SW-FISICA(config)#int range fastEthernet 0/13-14
SW-FISICA(config-if-range)#switchport mode access
SW-FISICA(config-if-range)#switchport access vlan 60
SW-FISICA(config-if-range)#switchport port-security
SW-FISICA(config-if-range)#switchport port-security maximum 1
SW-FISICA(config-if-range)#switchport port-security violation restrict
SW-FISICA(config-if-range)#no shut
SW-FISICA(config-if-range)#exit
SW-FISICA(config)#int fastEthernet 0/1
SW-FISICA(config-if)#switchport port-security mac-address 000B.BEA7.0037
SW-FISICA(config)#int fastEthernet 0/2
SW-FISICA(config-if)#switchport port-security mac-address 0001.64C9.C599
SW-FISICA(config)#int fastEthernet 0/3
SW-FISICA(config-if)#switchport port-security mac-address 0001.4215.6CDD
SW-FISICA(config)#int fastEthernet 0/4
SW-FISICA(config-if)#switchport port-security mac-address 0001.C7B0.5985
SW-FISICA(config)#int fastEthernet 0/5
SW-FISICA(config-if)#switchport port-security mac-address 000B.BE25.93E2
SW-FISICA(config-if)#int fastEthernet 0/6

```
SW-FISICA(config-if)#switchport port-security mac-address 0030.F289.E7B9
SW-FISICA(config)#int fastEthernet 0/7
SW-FISICA(config-if)#switchport port-security mac-address 000A.F365.5CBB
SW-FISICA(config)#int fastEthernet 0/13
SW-FISICA(config-if)#switchport port-security mac-address 0030.A385.402E
SW-FISICA(config)#int fastEthernet 0/14
SW-FISICA(config-if)#switchport port-security mac-address 0004.9A94.5D19
SW-FISICA(config-if)#exit
```

Configuração de Acesso Remoto SSH

```
SW-FISICA(config)#enable secret Clinica2020
SW-FISICA(config)#ip domain-name clinica.interno.local
SW-FISICA(config)#crypto key generate rsa <1024>
SW-FISICA(config)#username tecnico priv 0 secret Clinica2020
SW-FISICA(config)#line vty 0 4
SW-FISICA(config-line)#login local
SW-FISICA(config-line)#transport input ssh
SW-FISICA(config-line)#end
```

APÊNDICE G: SWITCH RADIO

Nomeação do Dispositivo
Switch>enable
Switch#conf t
Switch(config)#hostname SW-RADIO
Vlan de Gerênciamento
SW-RADIO(config)#int vlan 1
SW-RADIO(config-if)#ip address 10.0.1.5 255.255.255.0
SW-RADIO(config-if)#no shut
SW-RADIO(config-if)#exit
SW-RADIO(config)#ip default-gateway 10.0.1.1
Configuração modo VTP
SW-RADIO(config)#vtp mode client
SW-RADIO(config)#vtp domain clinica.interno.local
SW-RADIO(config)#vtp pass Cl1n1c@2020
Configuração Truncamento de Portas
SW-RADIO(config)#int gigabitEthernet 0/1
SW-RADIO(config-if)#switchport mode trunk
SW-RADIO(config-if)#no shut
SW-RADIO(config-if)#exit
SW-RADIO(config)#interface gigabitEthernet 0/2
SW-RADIO(config-if)#switchport mode trunk
SW-RADIO(config-if)#no shut
SW-RADIO(config-if)#exit
Desativação de Portas Ociosas
SW-RADIO(config)#int range fastEthernet 0/9-12
SW-RADIO(config-if-range)#shut
SW-RADIO(config-if-range)#exit
SW-RADIO(config)#int range fastEthernet 0/16-24
SW-RADIO(config-if-range)#shut
SW-RADIO(config-if-range)#exit
Configuração de Segurança e Portas de Acesso
SW-RADIO(config)#int range fastEthernet 0/1-8
SW-RADIO(config-if-range)#switchport mode access
SW-RADIO(config-if-range)#switchport access vlan 20
SW-RADIO(config-if-range)#no shut
SW-RADIO(config-if-range)#switchport port-security
SW-RADIO(config-if-range)#switchport port-security maximum 1
SW-RADIO(config-if-range)#switchport port-security violation restrict
SW-RADIO(config-if-range)#exit
SW-RADIO(config)#int range fastEthernet 0/13-15
SW-RADIO(config-if-range)#switchport mode access
SW-RADIO(config-if-range)#switchport access vlan 60
SW-RADIO(config-if-range)#no shut
SW-RADIO(config-if-range)#switchport port-security
SW-RADIO(config-if-range)#switchport port-security maximum 1
SW-RADIO(config-if-range)#switchport port-security violation restrict
SW-RADIO(config-if-range)#end
SW-RADIO(config)#in fastEthernet 0/1
SW-RADIO(config-if)#switchport port-security mac-address 0090.0C43.D9C5
SW-RADIO(config)#in fastEthernet 0/2
SW-RADIO(config-if)#switchport port-security mac-address 0006.2A46.80A5
SW-RADIO(config)#in fastEthernet 0/3
SW-RADIO(config-if)#switchport port-security mac-address 0000.0C08.5522
SW-RADIO(config)#in fastEthernet 0/4
SW-RADIO(config-if)#switchport port-security mac-address 0006.2A54.3698
SW-RADIO(config)#in fastEthernet 0/5
SW-RADIO(config-if)#switchport port-security mac-address 0040.0B78.485C

```
SW-RADIO(config)#in fastEthernet 0/6
SW-RADIO(config-if)#switchport port-security mac-address 0040.0BCE.6DA0
SW-RADIO(config)#in fastEthernet 0/7
SW-RADIO(config-if)#switchport port-security mac-address 00D0.D3A1.5E1C
SW-RADIO(config)#in fastEthernet 0/8
SW-RADIO(config-if)#switchport port-security mac-address 0050.0FE5.2171
SW-RADIO(config)#in fastEthernet 0/13
SW-RADIO(config-if)#switchport port-security mac-address 0001.64C5.D5E8
SW-RADIO(config)#in fastEthernet 0/14
SW-RADIO(config-if)#switchport port-security mac-address 000A.F368.0607
SW-RADIO(config)#in fastEthernet 0/15
SW-RADIO(config-if)#switchport port-security mac-address 00E0.F99B.4537
SW-RADIO(config)#exit
```

Configuração de Acesso Remoto SSH

```
SW-RADIO(config)#enable secret Clinica2020
SW-RADIO(config)#ip domain-name clinica.interno.local
SW-RADIO(config)#crypto key generate rsa <1024>
SW-RADIO(config)#username tecnico priv 0 secret Clinica2020
SW-RADIO(config)#line vty 0 4
SW-RADIO(config-line)#login local
SW-RADIO(config-line)#transport input ssh
SW-RADIO(config-line)#end
```

APÊNDICE H: SWITCH SAME

Nomeação do Dispositivo
Switch>enable
Switch>conf t
Switch(config)#hostname SW-SAME
Vlan de Gerênciamento
SW-SAME(config)#int vlan 1
SW-SAME(config-if)#ip address 10.0.1.6 255.255.255.0
SW-SAME(config-if)#no shut
SW-SAME(config-if)#exit
SW-SAME(config)#ip default-gateway 10.0.1.1
Configuração modo VTP
SW-SAME(config)#vtp mode client
SW-SAME(config)#vtp domain clinica.interno.local
SW-SAME(config)#vtp pass Cl1n1c@2020
Configuração Truncamento de Portas
SW-SAME(config)#int gigabitEthernet 0/1
SW-SAME(config-if)#switchport mode trunk
SW-SAME(config-if)#no shut
SW-SAME(config-if)#exit
Desativação de Portas Ociosas
SW-SAME(config)#int range fastEthernet 0/6-24
SW-SAME(config-if-range)#shut
SW-SAME(config-if-range)#exit
SW-SAME(config)#int gigabitEthernet 0/2
SW-SAME(config-if)#shut
SW-SAME(config-if)#exit
Configuração de Segurança e Portas de Acesso
SW-SAME(config)#int range fastEthernet 0/1-5
SW-SAME(config-if-range)#switchport mode access
SW-SAME(config-if-range)#switchport access vlan 70
SW-SAME(config-if-range)#switchport port-security
SW-SAME(config-if-range)#switchport port-security maximum 1
SW-SAME(config-if-range)#switchport port-security violation restrict
SW-SAME(config-if-range)#no shut
SW-SAME(config-if-range)#exit
SW-SAME(config)#int fastEthernet 0/1
SW-SAME(config-if)#switchport port-security mac-address 00D0.970B.D95B
SW-SAME(config)#int fastEthernet 0/2
SW-SAME(config-if)#switchport port-security mac-address 00D0.FFB4.9ECC
SW-SAME(config)#int fastEthernet 0/3
SW-SAME(config-if)#switchport port-security mac-address 0030.F24D.B8B7
SW-SAME(config)#int fastEthernet 0/4
SW-SAME(config-if)#switchport port-security mac-address 0009.7C02.C15E
SW-SAME(config)#int fastEthernet 0/5
SW-SAME(config-if)#switchport port-security mac-address 0002.1631.6805
SW-SAME(config-if)#exit
Configuração de Acesso Remoto SSH
SW-SAME(config)#enable secret Clinica2020
SW-SAME(config)#ip domain-name clinica.interno.local
SW-SAME(config)#crypto key generate rsa <1024>
SW-SAME(config)#username tecnico priv 0 secret Clinica2020
SW-SAME(config)#line vty 0 4
SW-SAME(config-line)#login local
SW-SAME(config-line)#transport input ssh
SW-SAME(config-line)#end

APÊNDICE I: SWITCH AMBU

Nomeação do Dispositivo
Switch#enable
Switch#conf t
Switch(config)#hostname SW-AMBU
Vlan de Gerênciamento
SW-AMBU(config)#int vlan 1
SW-AMBU(config-if)#ip address 10.0.1.9 255.255.255.0
SW-AMBU(config-if)#no shut
SW-AMBU(config-if)#exit
SW-AMBU(config)#ip default-gateway 10.0.1.1
Configuração modo VTP
SW-AMBU(config)#vtp mode client
SW-AMBU(config)#vtp domain clinica.interno.local
SW-AMBU(config)#vtp pass Cl1n1c@2020
Configuração Truncamento de Portas
SW-AMBU(config)#interface fastEthernet 0/24
SW-AMBU(config-if)#switchport mode trunk
SW-AMBU(config-if)#no shut
SW-AMBU(config-if)#exit
SW-AMBU(config)#interface gigabitEthernet 0/1
SW-AMBU(config-if)#switchport mode trunk
SW-AMBU(config-if)#no shut
SW-AMBU(config-if)#exit
Desativação de Portas Ociosas
SW-AMBU(config)#interface gigabitEthernet 0/2
SW-AMBU(config-if)#shut
SW-AMBU(config)#interface range fastEthernet 0/10-12
SW-AMBU(config-if-range)#shut
SW-AMBU(config-if-range)#exit
SW-AMBU(config)#interface range fastEthernet 0/17-23
SW-AMBU(config-if-range)#shut
SW-AMBU(config-if-range)#exit
Configuração de Segurança e Portas de Acesso
SW-AMBU(config)#interface range fastEthernet 0/1-9
SW-AMBU(config-if-range)#switchport mode access
SW-AMBU(config-if-range)#switchport access vlan 50
SW-AMBU(config-if-range)#no shut
SW-AMBU(config-if-range)#switchport port-security
SW-AMBU(config-if-range)#switchport port-security maximum 1
SW-AMBU(config-if-range)#switchport port-security violation restrict
SW-AMBU(config-if-range)#exit
SW-AMBU(config)#interface range fastEthernet 0/13-16
SW-AMBU(config-if-range)#switchport mode access
SW-AMBU(config-if-range)#switchport access vlan 60
SW-AMBU(config-if-range)#no shut
SW-AMBU(config-if-range)#switchport port-security
SW-AMBU(config-if-range)#switchport port-security maximum 1
SW-AMBU(config-if-range)#switchport port-security violation restrict
SW-AMBU(config-if-range)#exit
SW-AMBU(config)#int fastEthernet 0/1
SW-AMBU(config-if)#switchport port-security mac-address 0030.A340.1591
SW-AMBU(config)#int fastEthernet 0/2
SW-AMBU(config-if)#switchport port-security mac-address 00E0.F9B6.59A1
SW-AMBU(config)#int fastEthernet 0/3
SW-AMBU(config-if)#switchport port-security mac-address 0004.9A14.3B0E
SW-AMBU(config)#int fastEthernet 0/4
SW-AMBU(config-if)#switchport port-security mac-address 000A.416A.0C57

```
SW-AMBU(config)#int fastEthernet 0/5
SW-AMBU(config-if)#switchport port-security mac-address 0001.4266.0CC7
SW-AMBU(config)#int fastEthernet 0/6
SW-AMBU(config-if)#switchport port-security mac-address 000D.BD37.12E3
SW-AMBU(config)#int fastEthernet 0/7
SW-AMBU(config-if)#switchport port-security mac-address 0050.0F67.0B1D
SW-AMBU(config)#int fastEthernet 0/8
SW-AMBU(config-if)#switchport port-security mac-address 00D0.D3B0.EB80
SW-AMBU(config)#int fastEthernet 0/9
SW-AMBU(config-if)#switchport port-security mac-address 0050.0F02.2E73
SW-AMBU(config)#int fastEthernet 0/13
SW-AMBU(config-if)#switchport port-security mac-address 0004.9A2E.9E66
SW-AMBU(config)#int fastEthernet 0/14
SW-AMBU(config-if)#switchport port-security mac-address 00E0.F744.8D90
SW-AMBU(config)#int fastEthernet 0/15
SW-AMBU(config-if)#switchport port-security mac-address 0060.5C7C.DB7C
SW-AMBU(config)#int fastEthernet 0/16
SW-AMBU(config-if)#switchport port-security mac-address 0001.63EA.D212
SW-AMBU(config-if-range)#exit
```

Configuração de Acesso Remoto SSH

```
SW-AMBU(config)#enable secret Clinica2020
SW-AMBU(config)#ip domain-name clinica.interno.local
SW-AMBU(config)#crypto key generate rsa <1024>
SW-AMBU(config)#username tecnico priv 0 secret Clinica2020
SW-AMBU(config)#line vty 0 4
SW-AMBU(config-line)#login local
SW-AMBU(config-line)#transport input ssh
SW-AMBU(config-line)#end
```

APÊNDICE J: SWITCH QUIMIO

Nomeação do Dispositivo
Switch>enable
Switch#conf t
Switch(config)#hostname SW-QUIMIO
Vlan de Gerênciamento
SW-QUIMIO(config)#int vlan 1
SW-QUIMIO(config-if)#ip address 10.0.1.10 255.255.255.0
SW-QUIMIO(config-if)#no shut
SW-QUIMIO(config-if)#exit
SW-QUIMIO(config)#ip default-gateway 10.0.1.1
Configuração modo VTP
SW-QUIMIO(config)#vtp mode client
SW-QUIMIO(config)#vtp domain clinica.interno.local
SW-QUIMIO(config)#vtp pass Cl1n1c@2020
Configuração Truncamento de Portas
SW-QUIMIO(config)#interface gigabitEthernet 0/1
SW-QUIMIO(config-if)#switchport mode trunk
SW-QUIMIO(config-if)#no shut
SW-QUIMIO(config-if)#exit
SW-QUIMIO(config)#interface gigabitEthernet 0/2
SW-QUIMIO(config-if)#switchport mode trunk
SW-QUIMIO(config-if)#no shut
SW-QUIMIO(config-if)#exit
Desativação de Portas Ociosas
SW-QUIMIO(config)#interface range fastEthernet 0/5-12
SW-QUIMIO(config-if-range)#shut
SW-QUIMIO(config-if-range)#exit
SW-QUIMIO(config)#interface range fastEthernet 0/17-24
SW-QUIMIO(config-if-range)#shut
SW-QUIMIO(config-if-range)#exit
Configuração de Segurança e Portas de Acesso
SW-QUIMIO(config)#interface range fastEthernet 0/1-4
SW-QUIMIO(config-if-range)#switchport mode access
SW-QUIMIO(config-if-range)#switchport access vlan 30
SW-QUIMIO(config-if-range)#no shut
SW-QUIMIO(config-if-range)#switchport port-security
SW-QUIMIO(config-if-range)#switchport port-security maximum 1
SW-QUIMIO(config-if-range)#switchport port-security violation restrict
SW-QUIMIO(config-if-range)#exit
SW-QUIMIO(config)#interface range fastEthernet 0/13-16
SW-QUIMIO(config-if-range)#switchport mode access
SW-QUIMIO(config-if-range)#switchport access vlan 60
SW-QUIMIO(config-if-range)#no shut
SW-QUIMIO(config-if-range)#switchport port-security
SW-QUIMIO(config-if-range)#switchport port-security maximum 1
SW-QUIMIO(config-if-range)#switchport port-security violation restrict
SW-QUIMIO(config)#exit
SW-QUIMIO(config)#int fastEthernet 0/1
SW-QUIMIO(config-if)#switchport port-security mac-address 0010.1189.2587
SW-QUIMIO(config-if)#int fastEthernet 0/2
SW-QUIMIO(config-if)#switchport port-security mac-address 0060.7042.E1EC
SW-QUIMIO(config-if)#int fastEthernet 0/3
SW-QUIMIO(config-if)#switchport port-security mac-address 000B.BEC7.CC98
SW-QUIMIO(config-if)#int fastEthernet 0/4
SW-QUIMIO(config-if)#switchport port-security mac-address 00E0.F984.1965
SW-QUIMIO(config-if)#int fastEthernet 0/13
SW-QUIMIO(config-if)#switchport port-security mac-address 0001.C708.01E2

```
SW-QUIMIO(config-if)#int fastEthernet 0/14
SW-QUIMIO(config-if)#switchport port-security mac-address 0002.1779.7715
Found duplicate mac-address 0002.1779.7715.
SW-QUIMIO(config-if)#int fastEthernet 0/15
SW-QUIMIO(config-if)#switchport port-security mac-address 00D0.9785.B4E7
SW-QUIMIO(config-if)#int fastEthernet 0/16
SW-QUIMIO(config-if)#switchport port-security mac-address 0001.4396.3B74
SW-QUIMIO(config-if)#exit
```

Configuração de Acesso Remoto SSH

```
SW-QUIMIO(config)#enable secret Clinica2020
SW-QUIMIO(config)#ip domain-name clinica.interno.local
SW-QUIMIO(config)#crypto key generate rsa <1024>
SW-QUIMIO(config)#username tecnico priv 0 secret Clinica2020
SW-QUIMIO(config)#line vty 0 4
SW-QUIMIO(config-line)#login local
SW-QUIMIO(config-line)#transport input ssh
SW-QUIMIO(config-line)#end
```

APÊNDICE K: SWITCH MEDNU

Nomeação do Dispositivo
Switch>enable
Switch#conf t
Switch(config)#hostname SW-MEDNU
Vlan de Gerênciamento
SW-MEDNU(config)#int vlan 1
SW-MEDNU(config-if)#ip address 10.0.1.11 255.255.255.0
SW-MEDNU(config-if)#no shut
SW-MEDNU(config-if)#exit
SW-MEDNU(config)#ip default-gateway 10.0.1.1
Configuração modo VTP
SW-MEDNU(config)#vtp mode client
SW-MEDNU(config)#vtp domain clinica.interno.local
SW-MEDNU(config)#vtp pass Cl1n1c@2020
Configuração Truncamento de Portas
SW-MEDNU(config)#interface gigabitEthernet 0/2
SW-MEDNU(config-if)#switchport mode trunk
SW-MEDNU(config-if)#no shut
SW-MEDNU(config-if)#exit
Desativação de Portas Ociosas
SW-MEDNU(config)#interface gigabitEthernet 0/1
SW-MEDNU(config-if)#shut
SW-MEDNU(config)#interface range fastEthernet 0/5-12
SW-MEDNU(config-if-range)#shut
SW-MEDNU(config-if-range)#exit
SW-MEDNU(config)#interface range fastEthernet 0/16-24
SW-MEDNU(config-if-range)#shut
SW-MEDNU(config-if-range)#exit
Configuração de Segurança e Portas de Acesso
SW-MEDNU(config)#interface range fastEthernet 0/1-4
SW-MEDNU(config-if-range)#switchport mode access
SW-MEDNU(config-if-range)#switchport access vlan 40
SW-MEDNU(config-if-range)#no shut
SW-MEDNU(config-if-range)#switchport port-security
SW-MEDNU(config-if-range)#switchport port-security maximum 1
SW-MEDNU(config-if-range)#switchport port-security violation restrict
SW-MEDNU(config-if-range)#exit
SW-MEDNU(config)#interface range fastEthernet 0/13-15
SW-MEDNU(config-if-range)#switchport mode access
SW-MEDNU(config-if-range)#switchport access vlan 60
SW-MEDNU(config-if-range)#no shut
SW-MEDNU(config-if-range)#switchport port-security
SW-MEDNU(config-if-range)#switchport port-security maximum 1
SW-MEDNU(config-if-range)#switchport port-security violation restrict
SW-MEDNU(config-if-range)#exit
SW-MEDNU(config)#int fastEthernet 0/1
SW-MEDNU(config-if)#switchport port-security mac-address 0060.5C73.2889
SW-MEDNU(config-if)#int fastEthernet 0/2
SW-MEDNU(config-if)#switchport port-security mac-address 0001.96EA.6CA6
SW-MEDNU(config-if)#int fastEthernet 0/3
SW-MEDNU(config-if)#switchport port-security mac-address 0030.A347.B384
SW-MEDNU(config-if)#int fastEthernet 0/4
SW-MEDNU(config-if)#switchport port-security mac-address 00D0.BCC9.2227
SW-MEDNU(config-if)#int fastEthernet 0/13
SW-MEDNU(config-if)#switchport port-security mac-address 00E0.F9C9.63E5
SW-MEDNU(config-if)#int fastEthernet 0/14
SW-MEDNU(config-if)#switchport port-security mac-address 0030.A386.794D

```
SW-MEDNU(config-if)#int fastEthernet 0/15
SW-MEDNU(config-if)#switchport port-security mac-address 0090.0CAE.D2B9
SW-MEDNU(config-if)#exit
```

Configuração de Acesso Remoto SSH

```
SW-MEDNU(config)#enable secret Clinica2020
SW-MEDNU(config)#ip domain-name clinica.interno.local
SW-MEDNU(config)#crypto key generate rsa <1024>
SW-MEDNU(config)#username tecnico priv 0 secret Clinica2020
SW-MEDNU(config)#line vty 0 4
SW-MEDNU(config-line)#login local
SW-MEDNU(config-line)#transport input ssh
SW-MEDNU(config-line)#end
```