UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE INFORMÁTICA
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES

MAICO LOVATTO

GERENCIAMENTO E SEGMENTAÇÃO DE REDES: ESTUDO DE CASO EM EMPRESA DO SETOR ALIMENTÍCIO

TRABALHO DE CONCLUSÃO DE CURSO

PATO BRANCO

2015

MAICO LOVATTO

GERENCIAMENTO E SEGMENTAÇÃO DE REDES: ESTUDO DE CASO EM EMPRESA DO SETOR ALIMENTÍCIO

Trabalho de Conclusão de Curso, apresentado ao II Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Redes, da Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Dr. Fábio Favarim.

PATO BRANCO

2015

TERMO DE APROVAÇÃO

Gerenciamento e Segmentação de Redes: Estudo de Caso em Empresa do Setor Alimentício

por

Maico Lovatto

Esta monografia foi apresentada às 18h30min do dia 23 de outubro de 2015, como requisito parcial para obtenção do título de ESPECIALISTA, no II Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Redes, da Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. O acadêmico foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho **aprovado**.

Banca Examinadora

Prof. Dr. Fábio Favarim
Orientador / UTFPR-PB

Prof. Esp. Rudinei Silvestro
UTFPR-PB

Prof. Dr. Éden Ricardo Dosciatti
UTFPR-PB

Prof. Dr. Fábio Favarim
Coordenador do II Curso de Especialização
em Redes de Computadores

Dedico este trabalho a minha mãe Inês e minha namorada Vanuza, e aos meus familiares, amigos e professores.

AGRADECIMENTOS

Agradeço primeiramente a Deus, sem ele nada seria possível. Agradeço aos meus professores que contribuíram para minha formação, em especial ao meu orientador Prof. Dr. Fábio Favarim, pelo incentivo, e pela ajuda constante no desenvolvimento do trabalho. Agradeço também a minha mãe Inês, e minha namorada Vanuza pelo apoio e por me motivarem a seguir em frente. Obrigado!

RESUMO

LOVATTO, Maico. Gerenciamento e Segmentação de Redes: Estudo de caso em empresa do setor alimentício. 2015. 40f. Monografia (Especialização Semipresencial em Redes de Computadores) – Universidade Tecnológica Federal do Paraná. Pato Branco, 2015.

Atualmente com o crescimento rápido e desordenado das redes de computadores nas empresas, se torna indispensável a segmentação e gerenciamento. O uso de VLANs permite o administrador separar a rede em redes menores, melhorando a segurança, desempenho e principalmente diminuindo o domínio de *broadcast*. Com o objetivo de gerenciamento e segmentação de rede, foi feito um estudo de caso em uma empresa do setor alimentício. A empresa, não possui segmentação de rede, com a rede em um único domínio de *broadcast* e com mais de 300 dispositivos conectados, gerando números excessivos de pacotes *broadcast* na rede capturados pela ferramenta Wireshark. Foi feito a segmentação da rede simulando na ferramenta Cisco Packet Tracer, dividindo a rede em 21 setores da empresa, além de rede para os Servidores, VOIP, Monitoramento e WiFi, totalizando 25 VLANs. As VLANs são configuradas em 8 *switches*, sendo um *switch* de núcleo e os outros *switches* de distribuição. Além da segmentação, o gerenciamento da rede é importante, pois permite ao administrador detectar falhas, monitorar os ativos de rede e detectar intrusos. Neste trabalho foi sugerido e apresentado a ferramenta de gerenciamento The Dude, pela facilidade de configuração e uso. A ferramenta apresenta ao administrador informações importantes para uma rápida solução de possíveis problemas, tornando assim um trabalho proativo e não corretivo.

Palavras-chave: Segmentação de Rede, VLAN, Gerenciamento de Rede.

ABSTRACT

LOVATTO, Maico. Management and network segmentation: Case Study of Company Food Sector. 2015. 40f. Monografia (Especialização Semipresencial em Redes de Computadores) – Universidade Tecnológica Federal do Paraná. Pato Branco, 2015.

Currently the rapid growth and cluttered computer network in companies, becomes indispensable segmentation and management. The use of VLANs allows the administrator to separate a network in networks minor, improving security, performance and especially reducing the domain broadcast. With objective management and network segmentation was made hum case study in a company in the food sector. The company, does not have network segmentation with the network hum single domain transmission and with more than 300 connected devices, generating excessive packet numbers transmitted over the network captured in the Wireshark tool. So it was made one network segmentation simulating the Cisco Packet Tracer tool, the sharing network 21 company sectors, in addition to paragraph network servers, VOIP, Monitoring and Wi-Fi, totaling 25 VLANs. VLANs are configured as 8 switches, being one switch core, and changes distribution. Besides the segmentation, network management is important as it allows administrator by detecting faults, monitor network assets and detect intruders. This work suggested and presented The Dude tool for ease of configuration and use. The tool presents important information when administrator for a quick possible problem solving, being so proactive work and not corrective.

Keywords: Network segmentation, VLAN, Network Management.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

ASN.1 – *Abstract Syntax Notation One*

BER – *Basic Encoding Rules*

CD – Centro de Distribuição

CLI – *Command Line Interface*

CMIP – *Common Management Information Protocol*

CMISE – *Common Managemet Information Service*

CQ – Controle de Qualidade

IEEE – *Istitute of Electric and Electronic Engineer*

IETF – *Internet Engineering Task Force*

IP – *Internet Protocol*

IPX – *Internetwork Packet Exchange*

ISO – *Internacional Organization for Standardization*

LAN – *Local Area Network*

MAC – *Media Access Control*

MIB – *Management Information Base*

OSI – *Open Systems Interconnection*

PCP – Planejamento Controle e Produção

PDU – *Protocol Data Unit*

RFC – *Request for Comments*

RH – Recursos Humanos

SAC – Serviço de Atendimento ao Consumidor

SMI – *Structure of Management Information*

SNMP – Simple Network Management Protocol

TI – Tecnologia e Informação

UDP – *User Datagram Protocol*

VLAN – *Virtual Local Area Network*

VLSM – *Variable Lenght Subnet Mask*

VOIP – *Voice over Internet Protocol*

SUMÁRIO

1. INTRODUÇÃO

Neste capítulo, são abordadas as considerações iniciais, o objetivo geral e os objetivos específicos e por fim os motivos que justificam este trabalho.

1.1. CONSIDERAÇÕES INICIAIS

Atualmente com o crescimento rápido da Internet, o uso de redes de computadores se tornou indispensável em locais com mais de um computador. A Internet abrange todos os ramos da atividade, e empresas buscam utilizá-la, visando lucro, agilidade em tomadas de decisões, agilidade dos serviços prestados, e maior produtividade. Para isso faz-se necessário uso de redes de computadores confiáveis, eficientes, seguras e sempre disponíveis.

Um dos grandes problemas das empresas, são crescimento desordenado da rede, com aumento de equipamentos, computadores e de novos serviços. Esses problemas geram complexidade e complicações no gerenciamento das redes. Muitas delas colocam equipamentos repetidores de sinal, como *switches*, hubs, acarretando cascateamento do sinal, causando o aumento do domínio de *broadcast*. Quanto maior o domínio de *broadcast*, maior perda de informações.

O uso de Redes Locais Virtuais (VLAN – *Virtual Local Area Network*) permite o administrador de rede separar redes em sub-redes, isto é, separar em redes menores, reduzindo o domínio de *broadcast* e consequentemente diminuindo perda de informações. Além disso o uso de VLANs, provê melhor desempenho e mais segurança, por exemplo, separar a rede dos servidores da rede dos usuários garantindo acesso aos servidores apenas a quem de fato necessita.

Contudo, tem-se também a necessidade de gerenciamento da rede, a fim de detectar possíveis falhas, evitando paralisação total ou parcial da rede, monitorando os ativos de rede e também detectando intrusos. Uma rede bem gerenciada permite a um administrador de rede ser proativo, eliminando as manutenções corretivas, onde o problema é reportado por usuários da rede. Além disso o gerenciamento possibilita o administrador de rede agir de forma mais rápida na solução de um problema.

1.2. OBJETIVOS

A seguir são descritos os objetivos do trabalho.

1.2.1. Objetivo Geral

Implementar segmentação e gerenciamento da rede de computadores de uma empresa do setor alimentício.

1.2.2. Objetivos Específicos

Para alcançar o objetivo geral, foram definidos os seguintes objetivos específicos, para o presente trabalho:

- Melhorar o desempenho da rede, com a redução do domínio de *broadcast*;
- Aumentar a segurança da rede, evitando que usuários de um setor possa acessar a rede de outros setores;
- Sugerir e apresentar uma ferramenta de Gerenciamento de rede.

1.3. JUSTIFICATIVA

Geralmente muitas empresas, tem suas redes desorganizadas e sem gerenciamento, fazendo apenas manutenções corretivas, não conseguindo serem proativas em relação a possíveis falhas e problemas. Essas empresas sofrem com problemas de desempenho, tanto no uso da Internet, quanto na geração de relatórios em sistemas locais, geralmente por estar em uma única rede, em um único domínio de *broadcast*.

A segmentação da rede da empresa deixará a rede mais segura, pois computadores e servidores poderão ter seu acesso restrito a apenas um segmento da rede diminuindo as chances de acesso sem permissão a informações confidenciais, além de poder controlar quais dispositivos podem participar de uma VLAN.

O uso de VLANs traz para a empresa redução de custo, por ter menor necessidade das atualizações de rede, o uso mais eficiente da largura de banda e desempenho mais alto, ao dividir a rede em vários grupos de trabalhos, reduz o trafego desnecessário na rede. Além de desempenho e redução de custo, ao dividir a rede em VLANs, diminui o domínio de *broadcast* e melhora a segurança.

A implantação de sistemas de monitoramento do tráfego na rede, assim como de detecção de falhas na rede, possibilita ao administrador da rede reagir rapidamente na resolução do problema detectado.

Deste modo, neste trabalho é apresentado uma proposta de segmentação e gerenciamento da rede de computadores para uma empresa do ramo alimentício, separando em sub-redes os diferentes setores da empresa criando, através do uso de VLANs, que cada sub-rede possa ser monitorado, através de um sistema de monitoramento/gerenciamento.

2. REFERENCIAL TEÓRICO

Este capítulo apresenta os três principais conceitos envolvidos neste trabalho, sendo que a Seção 2.1 apresenta o conceito de segmentação de rede, a Seção 2.2 apresenta os conceitos de VLANs e a Seção 2.3 sobre gerenciamento de rede.

2.1. SEGMENTAÇÃO DE REDE

Segundo Forouzan (2008) dispositivos interligados em um escritório, prédio ou campus, formam uma rede local (LAN – *Local Area Network*), podendo ser muito simples, conectando dois computadores e uma impressora, ou estender para toda a empresa e incluir outros dispositivos.

Conforme Englander (2011) uma LAN conecta computadores e outros dispositivos em uma área localizada relativamente pequena, podendo ser uma sala, edifício, ou edifícios próximos entre si, sendo limitadas em termos de alcance geográfico.

Para Tanenbaum (2011) *broadcast* é o envio de um pacote a todos os destinos simultaneamente. Um método de *broadcasting* não exige recursos especiais da rede, ele permite à origem enviar um pacote específico a cada destino, esse método não só desperdiça largura de banda, mas também exige que a origem tenha uma lista completa de todos os destinos.

Em uma rede não segmentada, computadores, impressoras e outros dispositivos conectados disseminam grande quantidade de pacotes de *broadcast*, seja por falhas na conexão, mau funcionamento de placas de rede, ou até mesmo por protocolos e aplicações na rede local (HAFFERMANN, 2009).

Ao utilizar segmentação de rede com VLANs, é possível diminuir o domínio de *broadcast*, além de outras vantagens como segurança, melhor desempenho, redução de custo, conforme será apresentado na Seção 2.2.

2.2. VLAN – REDES LOCAIS VIRTUAIS

Uma das tecnologias que contribuem com a excelência do desempenho da rede é a separação dos grandes domínios de *broadcast* em domínios menores com VLANs, limitando assim o número de dispositivos que participam de *broadcast* (CISCO, 2015).

Para Tanenbaum (2011) as VLANs permitem que a topologia física seja dividida em diferentes topologias lógicas.

Segundo Kurose e Ross (2010), a utilização de VLANs auxilia na solução das seguintes dificuldades:

- Falta de isolamento do tráfego: o tráfego *broadcast* percorre toda a rede, limitar o escopo desse tráfego de *broadcast* aprimoraria o desempenho da LAN. A limitação do tráfego de *broadcast* também é importante por razões de segurança e privacidade, evitando que um grupo de funcionários, por exemplo, analise o tráfego do grupo de gerência.

- Uso ineficiente de comutadores: se uma instituição tivesse 10 grupos, seriam necessários 10 comutadores. Se cada grupo fosse com menos de 10 pessoas, um único comutador de 96 pontos seria suficiente para atender a todos, mas esse comutador não fornece isolamento de tráfego.

- Gerenciamento de usuários: se um funcionário se locomove entre os grupos o cabeamento físico deve ser mudado para conectar o funcionário a um comutador diferente.

Para Cisco (2015) os principais benefícios de usar VLANs são:

- Segurança – Grupos que tem dados confidenciais são separados do restante da rede, diminuindo as chances de acesso sem permissão a informações confidenciais.

- Redução de custo – Menor necessidade das atualizações de rede e uso mais eficiente da largura de banda.

- Melhor desempenho – Dividir a rede em vários grupos de trabalhos lógicos reduz tráfego desnecessário na rede e aumenta o desempenho.

- Atenuação da tempestade de *broadcast* – Dividir a rede em VLANs diminui o número de dispositivos que podem participar de uma situação de descontrole por excesso de *broadcast*.

- Maior eficiência do pessoal de TI (Tecnologia e Informação) – VLANs simplificam o gerenciamento da rede, além da facilidade de identificar a função de uma VLAN, dando a ela um nome apropriado, “Financeiro”, por exemplo.

- Projeto mais simples ou gerenciamento de aplicativo – Simplifica o gerenciamento de um projeto ou trabalho com um aplicativo especializado.

2.2.1. Tipos de VLANs e Tipos de Conexões

Segundo Moraes (2002) as redes locais virtuais podem ser classificadas em:

- **VLANs agrupadas por Portas (Camada 1):** Os membros de uma VLAN podem ser definidos de acordo com as portas do comutador utilizado. É um método muito utilizado na implementação de VLANs, pois a configuração é rápida e simples. A principal desvantagem, é quando um usuário se move para outro local, e conectado em outro *switch*, o administrador da rede deve reconfigurar a VLAN. A Figura 1 mostra que as portas de 1 a 12 pertencem a VLAN 10 e as portas de 13 a 24 pertencem a VLAN 20.

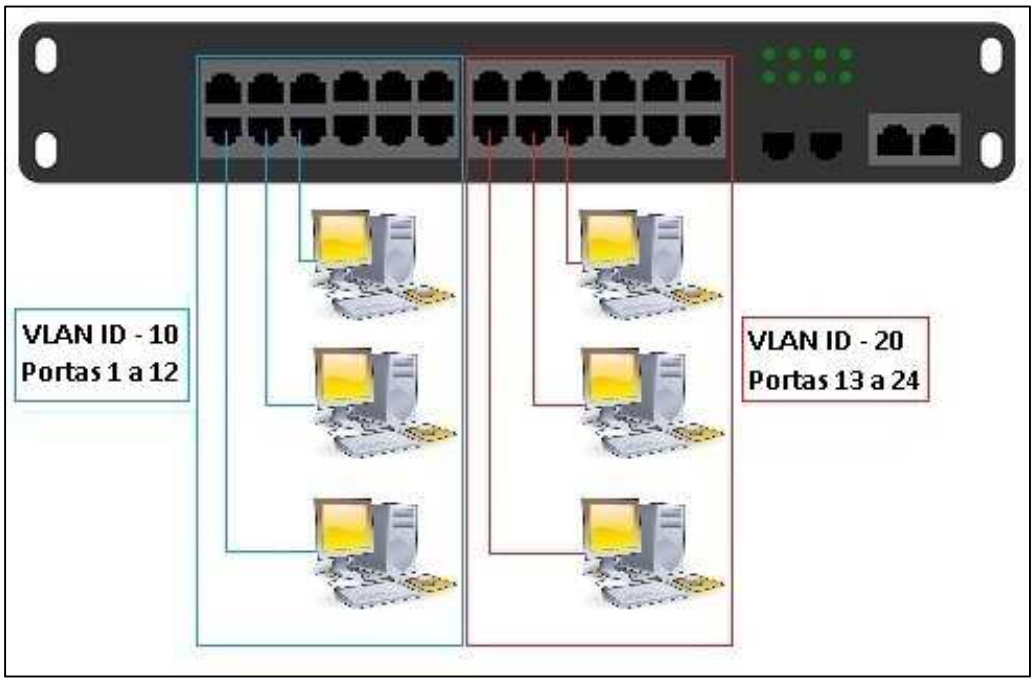

Figura 1. VLAN agrupada por porta
Fonte: Autoria Própria

- **VLANs agrupadas por Endereço MAC (Camada 2):** Os membros de uma VLAN são identificados pelo endereço MAC (*Media Access Control*) do dispositivo. O comutador reconhece o endereço MAC pertencente a cada VLAN. Quando o

dispositivo é movido, não é necessário configurá-lo para que continue pertencendo a mesma VLAN, isso se torna uma vantagem em relação a VLANs agrupadas por portas. O maior problema é que o membro da VLAN deve ser especificado, o administrador de rede não terá uma tarefa simples em redes com milhares de usuários. O Quadro 1 apresenta um exemplo de VLAN agrupada por endereço físico, no qual os dispositivos com endereço MAC 08-00-27-AA-A1-B8, 00-0C-29-A0-BA-13 e E8-D4-E0-A6-9D-93, pertencem às VLANs 10, 20 e 30 respectivamente.

Endereço MAC	08-00-27-AA-A1-B8	00-0C-29-A0-BA-13	E8-D4-E0-A6-9D-93
VLAN	10	20	30

Quadro 1. VLAN agrupada por endereço físico
Fonte: Autoria Própria

- **VLANs agrupadas por Protocolo (Camada 2):** Os membros de uma VLAN por Protocolo, podem ser identificados de acordo com o campo “tipo de protocolo” encontrado no cabeçalho da camada 2. O Quadro 2 apresenta um exemplo de VLAN agrupada por protocolo, no qual os protocolos IPX, IP e NetBios, pertencem às VLANs 10, 20 e 30 respectivamente.

Protocolo	IPX	IP	NetBios
VLAN	10	20	30

Quadro 2. VLAN agrupada por protocolo
Fonte: Autoria Própria

- **VLANs agrupadas por Endereço IP (Camada 3):** Os membros de uma VLAN são determinados pelo endereço IP. Em VLANs por Endereço IP, os usuários podem mover suas estações de trabalho sem reconfigurar os seus endereços de rede. O problema é que o tempo para encaminhamento de pacotes é maior do que utilizando o endereço MAC. O Quadro 3 apresenta um exemplo de VLAN agrupada por endereço IP, no qual os IPs 172.17.10.10, 172.17.20.20 e 172.17.30.30, pertencem às VLANs 10, 20 e 30 respectivamente.

Endereço IP	172.17.10.10	172.17.20.20	172.172.30.30
VLAN	10	20	30

Quadro 3. VLAN agrupada por endereço IP
Fonte: Autoria Própria

- **VLANs agrupadas por Camadas superiores:** Também é possível definir os membros de uma VLAN de acordo com aplicações ou serviços, ou uma combinação destes.

Dispositivos que suportam ou não o padrão IEEE 802.1Q, em uma VLAN podem ser conectados de três maneiras diferentes, de acordo com Moraes (2002) são elas:

- Enlace Tronco (*Trunk Link*): Todos os dispositivos conectados a um enlace deste tipo, devem ter suporte à VLANs.

- Enlace de Acesso (*Access Link*): Conecta um dispositivo sem suporte a VLAN a uma porta de um comutador.

- Enlace Híbrido: Combinação dos dois enlaces anteriores, em um enlace híbrido são conectados tanto dispositivos com suporte a VLANs, quanto os sem.

A Figura 2 mostra um enlace de tronco entre *switches* e um enlace de acesso entre os computadores e o seu respectivo *switch*.

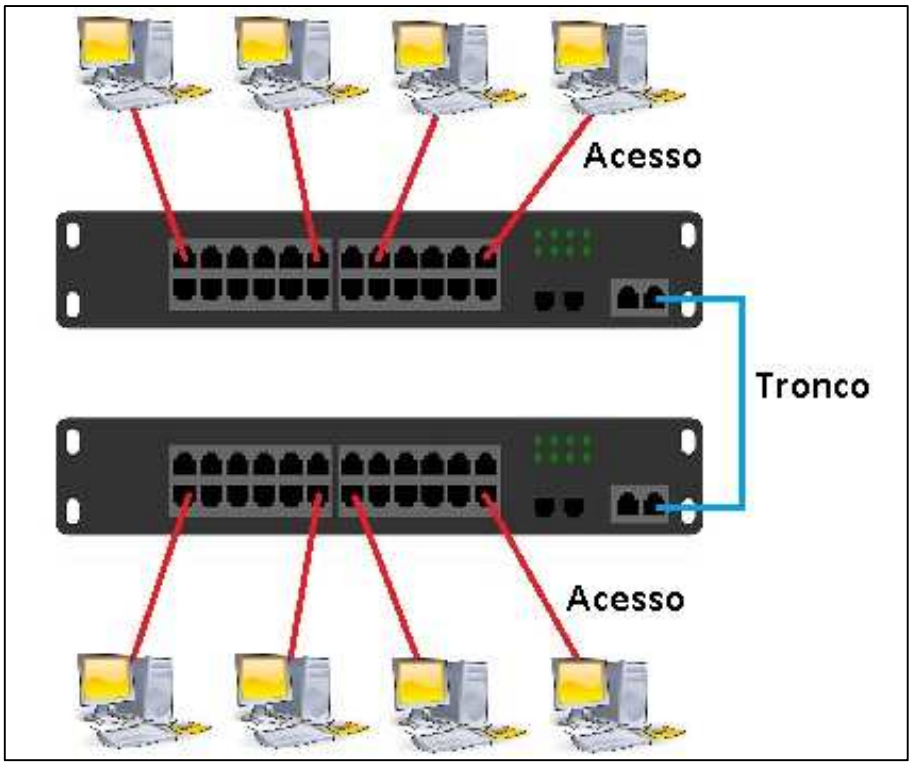

Figura 2. Enlace de rede em modo Tronco e Acesso
Fonte: Autoria Própria

2.3. GERENCIAMENTO DE REDES

Saydam e Magedanz (1996) definiram que gerenciamento de redes é o oferecimento, integração e coordenação de componentes de hardware, software e pessoas, a fim de monitorar, consultar, analisar, configurar, testar, avaliar e controlar os recursos da rede satisfazendo as exigências de qualidade e desempenho com um custo aceitável dentro da organização que a utiliza.

De acordo com Kurose e Ross (2010), mesmo em redes simples, há muitos cenários que o administrador de rede se beneficiará por ter as ferramentas de gerenciamento adequadas, como por exemplo:

- Detecção de falha em uma placa de interface em um hospedeiro ou roteador: Com ferramentas de gerenciamento, uma entidade de rede, pode indicar aos administradores de rede que uma de suas interfaces não está funcionando.

- Monitoramento de hospedeiro: O administrador de rede pode verificar se todos os hospedeiros da rede estão ativos e operacionais.

- Monitoramento de tráfego para auxiliar o oferecimento de recursos: O administrador de rede, pode monitorar padrões de tráfego entre as fontes e destinos e perceber que utilizando VLANs, o tráfego pode ser reduzido de maneira significativa, obtendo melhor desempenho e sem custo de novos equipamentos.

- Detecção de mudanças rápidas em tabela de roteamento: A alternância de rotas, pode indicar instabilidades no roteamento ou um roteador mal configurado.

- Detecção de intrusos: O administrador de rede pode detectar a existência de certos tipos de tráfego que são características de ataque à segurança.

Kurose e Ross (2010) descrevem que a ISO (*Internacional Organization for Standardization*) criou um modelo de gerenciamento de rede em um quadro mais estruturado, definindo em cinco áreas de gerenciamento de rede:

1. Gerenciamento de desempenho: O objetivo do gerenciamento de desempenho é quantificar, medir, informar, analisar e controlar o desempenho de componentes da rede (enlaces, roteadores e hospedeiros).

2. Gerenciamento de falhas: O objetivo do gerenciamento de falhas é registrar, detectar e reagir às condições de falha da rede, por exemplo, interrupção de serviços em enlaces, hospedeiros, ou em hardware e software de roteadores.

3. Gerenciamento de configuração: O gerenciamento de configuração permite que o administrador da rede saiba quais dispositivos fazem parte da rede administrada e quais são suas configurações de hardware e software.

4. Gerenciamento de contabilização: O gerenciamento de contabilização permite que o administrador da rede especifique, registre e controle o acesso de usuários e dispositivos aos recursos da rede.

5. Gerenciamento de segurança: O objetivo do gerenciamento de segurança é controlar o acesso aos recursos da rede de acordo com a política de segurança definida.

2.3.1. Arquitetura de Gerenciamento de Rede

Conforme Kurose e Ross (2010) os principais componentes de uma arquitetura de gerenciamento de rede, conforme Figura 3, são:

- Entidade gerenciadora: É ela que controla a coleta, o processamento, a análise e a apresentação de informações de gerenciamento de rede, e é aqui que o administrador interage com os dispositivos de rede.

- Dispositivo gerenciado: É um equipamento de rede que está em uma rede gerenciada, podendo ser um hospedeiro, um roteador, ou uma impressora. Em dispositivo gerenciado pode haver diversos objetos gerenciados, esses objetos têm informações que são coletadas dentro de uma Base de Informações de Gerenciamento (MIB – *Management Information Base*). No dispositivo gerenciado também reside um agente de gerenciamento de rede, responsável por se comunicar com a entidade gerenciadora e executar ações locais no dispositivo, sob o comando e controle da entidade gerenciadora.

- Protocolo de gerenciamento de rede: Este protocolo é executado entre a entidade gerenciadora e o agente de gerenciamento de rede dos dispositivos gerenciados, permitindo investigar o estado desses dispositivos, e executar ações sobre eles mediante seus agentes.

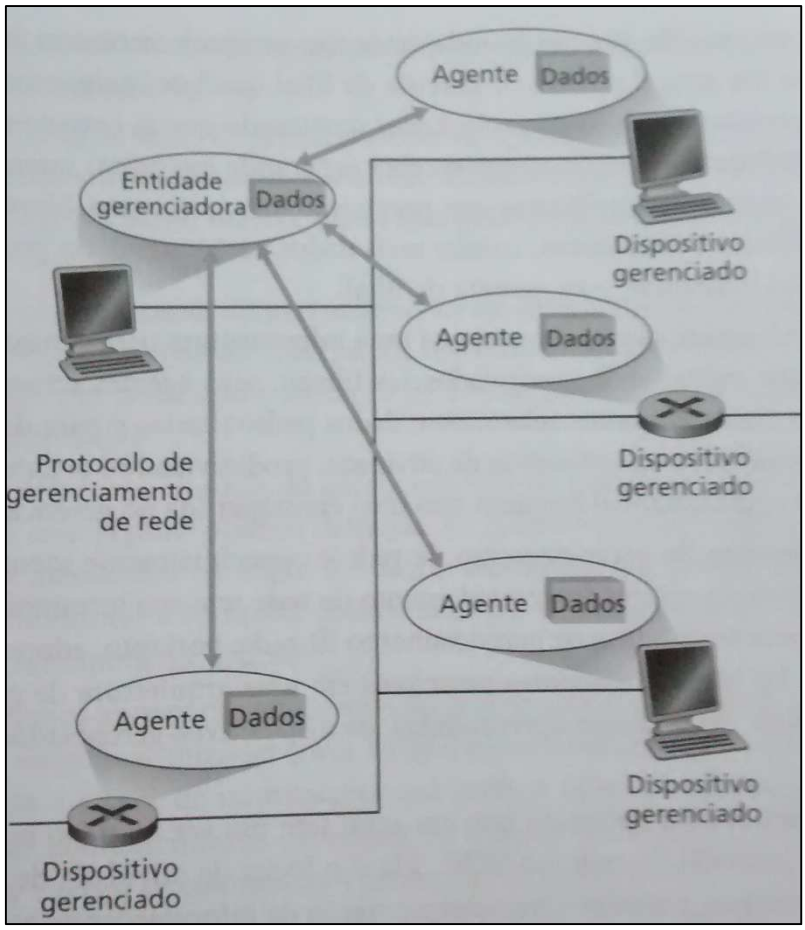

Figura 3. Principais componentes de uma arquitetura de gerenciamento de rede
Fonte: Kurose e Ross (2010)

A estrutura de gerenciamento padrão da Internet é constituída de quatro partes de acordo com Kurose e Ross (2010):

- Definições dos objetos de gerenciamento de redes – conhecidos como objetos MIB. As informações de gerenciamento são representadas como uma coletânea de objetos gerenciados que formam um banco de informações conhecido como MIB. Os objetos MIB definem as informações de gerenciamento mantidas por um dispositivo gerenciado.

- Uma linguagem de definição de dados – conhecida como SMI (*Structure Management Information*). Define os tipos de dados, um modelo de objeto e regras para escrever informações de gerenciamento. Os objetos MIB são especificados nessa linguagem de definição de dados.

- Um protocolo – SNMP (*Simple Network Management Protocol*). O SNMP é usado para transmitir informações e comandos entre uma entidade gerenciadora e um agente que os executa dentro de um dispositivo de rede gerenciado.

- Capacidades de segurança e de administração. Aprimoramento do SNMPv3 em comparação ao SNMPv2.

Para Kurose e Ross (2010), a MIB guarda objetos gerenciados cujos valores refletem o estado atual da rede, esses valores podem ser consultados ou definidos por uma entidade gerenciadora por meio de SNMP.

De acordo com Kurose e Ross (2010), a SMI é a linguagem usada para definir as informações de gerenciamento que contém em uma entidade gerenciada da rede, sendo necessária para assegurar que a sintaxe e a semântica dos dados de gerenciamento de rede sejam bem definidas.

Segundo Kurose e Ross (2010) sobre essa arquitetura de gerenciamento de rede, dois padrões mais importantes surgiram, sendo o OSI (*Open Systems Interconnection*) CMISE/CMIP (*Common Management Information Service/Common Management Information Protocol*) e o SNMP, ambos foram projetados para serem independentes de produtos ou de redes de fabricantes específicos. Hoje o SNMP é a estrutura de gerenciamento de rede mais usada e disseminada.

2.3.2. SNMP – Protocolo Simples de Gerenciamento de Rede

Conforme Farrel (2011) o SNMP (*Simple Network Management Protocol*) é um protocolo cliente-servidor, e em nível de aplicação que pode usar qualquer mecanismo de transporte. Os agentes de gerenciamento se conectam com os dispositivos gerenciados e emitem requisições, e os dispositivos gerenciados retornam respostas.

Para Forouzan (2008) o SNMP usa conceito de gerente e agente, onde, um gerente controla e monitora um conjunto de agentes. O protocolo é projetado no nível de aplicação, para que consiga monitorar dispositivos de diferentes fabricantes e em diferentes redes físicas. O SNMP usa serviços UDP (*User Datagram Protocol*) em duas portas, a porta 161 que é usada pelo agente e a porta 162 usada pelo gerente.

Segundo Forouzan (2008) o gerenciamento por meio do SNMP se fundamenta em três conceitos básicos:

- Um gerente monitora o estado de um agente solicitando informações que refletem o comportamento do agente.

- Um gerente força um agente a realizar uma tarefa reinicializando valores no banco de dados do agente.

- Um agente contribui para o processo de gerenciamento alertando o gerente sobre uma situação anormal.

De acordo com Costa (2008) o SNMP não define um grande número de comandos, e sim apenas duas operações básicas: *fetch*, para obter um valor de um dispositivo, e *store*, para colocar um valor em um dispositivo. Além disso são quatro PDU (*Protocol Data Unit*), são eles:

- GET, usado para recuperar um pedaço de informação de gerenciamento.

- GETNEXT, usado para recuperar sequências de informações de gerenciamento.

- SET, usado para fazer uma mudança no subsistema gerido.

- TRAP, usado para reportar uma notificação ou para outros eventos sobre o subsistema gerido.

Conforme Farrel (2011) existem três versões do SNMP. O SNMPv1 mostrou-se simples em alguns aspectos, não tendo requisições suficientemente capazes e usando o SMIv1 para construir PDUs. Após várias tentativas, a IETF (*Internet Engineering Task Force*) produziu o SMNPv2 e o documento RFC 1901 como protocolo experimental. O SMIv2 foi documentado como RFC 2578 e as mensagens SNMPv2 poder transportar apenas PDUs construídas usando o SMIv2.

O SNMPv1 e o SMPv2 trazem consideráveis preocupações de segurança, não tendo controle de quem na rede tem permissão de realizar operações SNMP e acessar os objetos nesse módulo MIB, ou seja, qualquer usuário na rede será capaz de examinar e modificar os objetos MIB. Assim a terceira versão, o SNMPv3 inclui autenticação criptográfica em nível de aplicação para permitir que usuário sejam autenticados (FARREL, 2011).

De acordo Forouzan (2008), o SNMP define o formato dos pacotes trocados entre um gerente e agente, ele lê e altera o estado dos objetos por pacotes SNMP. O SMI (Estrutura de Informações de Gerenciamento) define as regras de atribuição de nomes a objetos, estabelece tipos de objetos, e mostra como codificar objetos e valores. E por fim

a MIB cria um conjunto de objetos com nomes, tipos e relações entre si para uma entidade a ser gerenciada.

O SNMP usa serviços de dois outros protocolos auxiliares, O MIB que é um conjunto de grupos de objetos que podem ser gerenciados pelo SNMP, e o SMI que atribui nomes a objetos, define tipos de dados que podem ser armazenados em um objeto e codifica os dados. (FOROUZAN, 2008).

Conforme Forouzan (2008) as funções do SMI são: dar nome a objetos, definir o tipo de dados que podem ser armazenados em um objeto, e por fim, mostrar como codificar dados para transmissão através da rede. São três atributos que identificam um objeto:

- Nome: O SMI requer que cada objeto gerenciado tenha um nome exclusivo, ele usa um identificador de objetos, que é um identificador hierárquico com base em uma estrutura em forma de árvore.

- Tipo: É o tipo de dado que pode ser armazenado, o SMI usa as definições padronizadas pelo ASN.1 (*Abstract Syntax Notation One*).

- Método de Codificação: O SMI usa outro padrão, as BER (*Basic Encoding Rules* – Regras de Codificação Básicas), para codificar dados a serem transmitidos através da uma rede. As BER especificam que cada um dos dados seja codificado em um formato de trinca: marca, comprimento e valor.

3. MATERIAIS E MÉTODOS

Este capítulo descreve os materiais e o método utilizado para a realização deste trabalho.

3.1. MATERIAIS

Para o desenvolvimento deste projeto foram utilizadas as ferramentas Cisco Packet Tracer (Versão *Student*), Wireshark (Versão 1.12.7) e The Dude (Versão 3.6).

3.1.1. Cisco Packet Tracer

Cisco Packet Tracer é uma ferramenta de simulação de configuração de rede, utilizada para o ensino, desenvolvida pela Cisco. Nesta ferramenta é possível simular uma rede real e criar novos cenários, situações e configurações. A ferramenta tem uma interface simples conforme Figura 4, e contém vários dispositivos para a simulação, como roteadores, *switches*, hubs, computadores, etc.

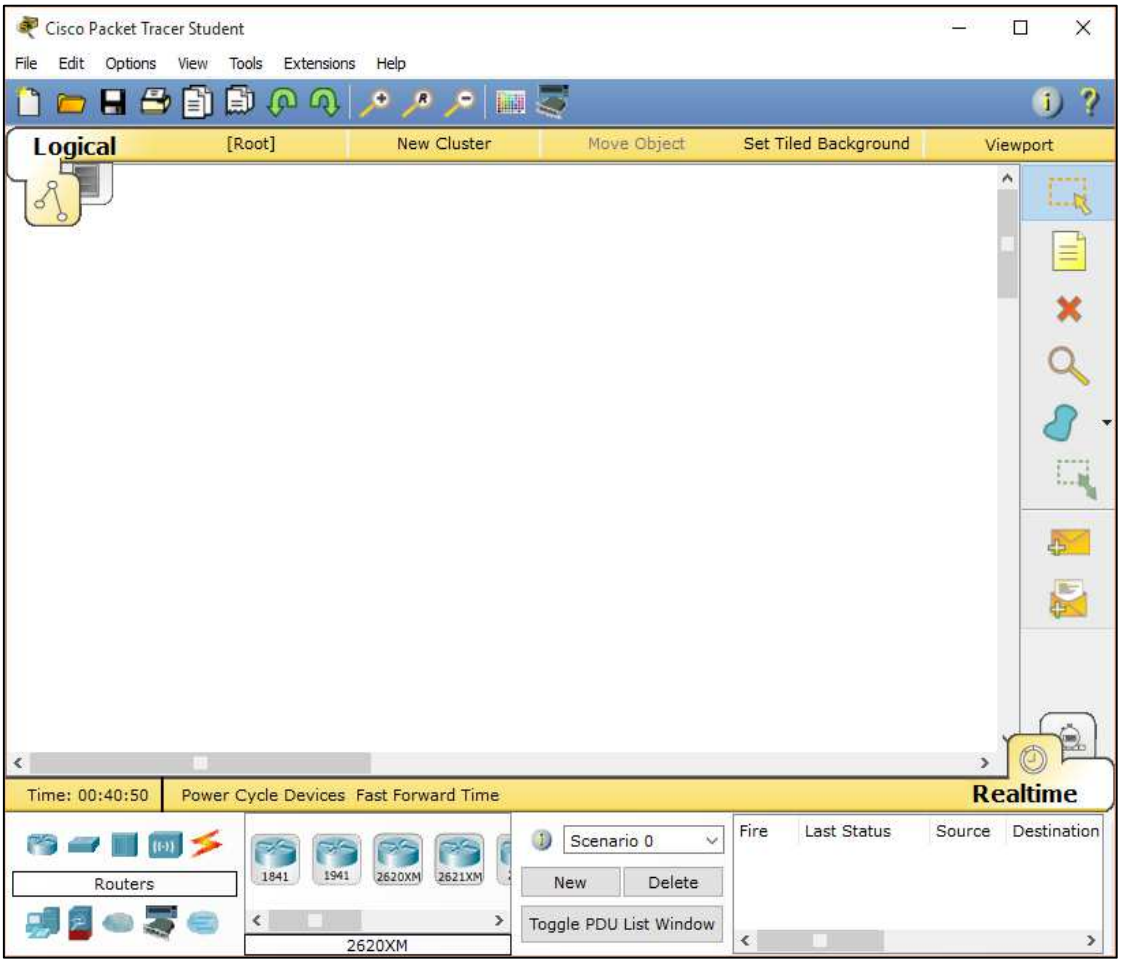

Figura 4. Cisco Packet Tracer Student
Fonte: Autoria Própria

Neste trabalho, a ferramenta Cisco Packet Trace, foi utilizada para montar a rede atual da empresa. Também foi utilizada para montar a rede proposta para empresa, para isso foi utilizado o *switch* Cisco Catalyst 2960, no qual tem gerenciamento baseado em *Web* e na CLI (*Command Line Interface*).

3.1.2. Wireshark

O Wireshark é uma ferramenta que analisa o tráfego de rede, sendo possível saber tudo que passa pela rede. A ferramenta contém um conjunto de recursos, sendo os principais, captura ao vivo do tráfego e multi-plataforma, A Figura 5 apresenta a interface da ferramenta Wireshark.

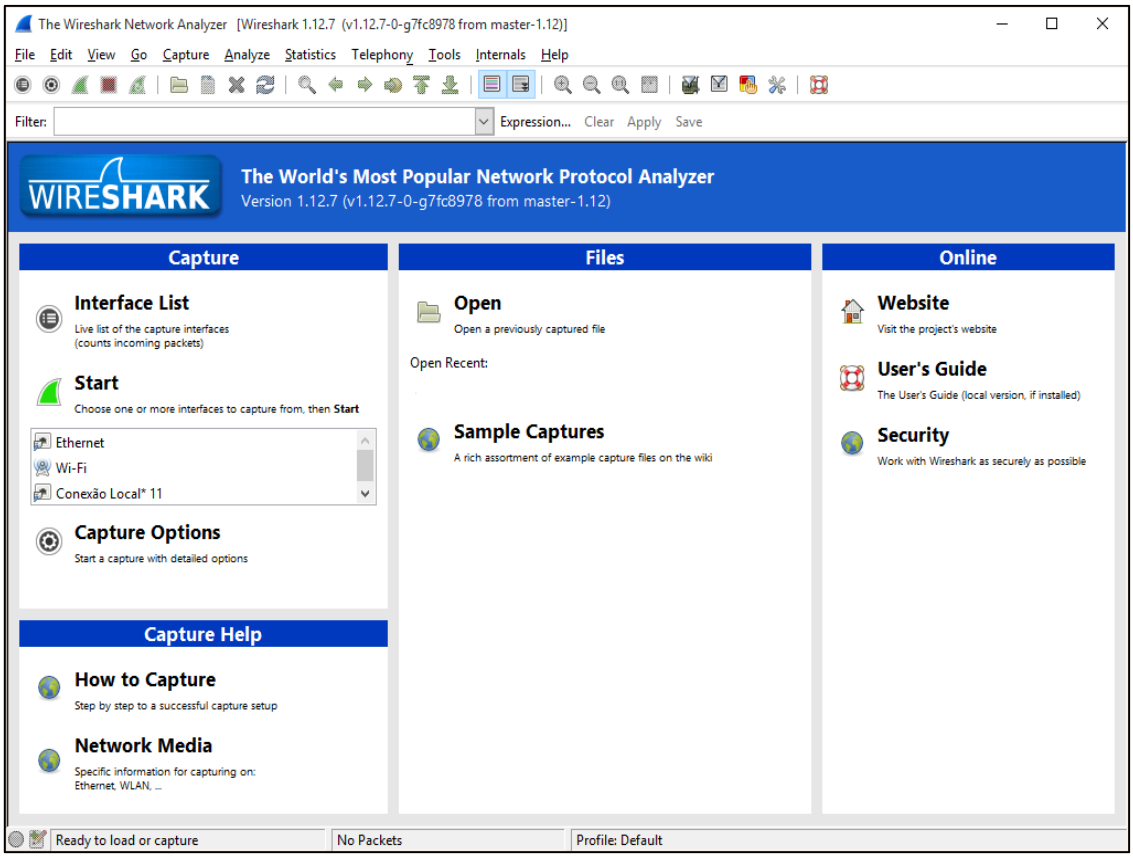

Figura 5. Wireshark
Fonte: Autoria Própria

Neste trabalho, a ferramenta Wireshark foi utilizada para captura de pacotes e análise da rede atual da empresa, gerando assim gráficos do comportamento da rede. Sendo possível também filtrar os pacotes *broadcast*, dos pacotes capturados.

3.1.3. The Dude

O software The Dude foi desenvolvido pela MikroTik para gerenciamento da rede. Este software possibilita verificar todos os dispositivos dentro da rede, controlar os serviços desses dispositivos e alertar caso algum serviço venha a apresentar problemas, além de desenhar o mapa da rede. A Figura 6 apresenta a interface do software The Dude.

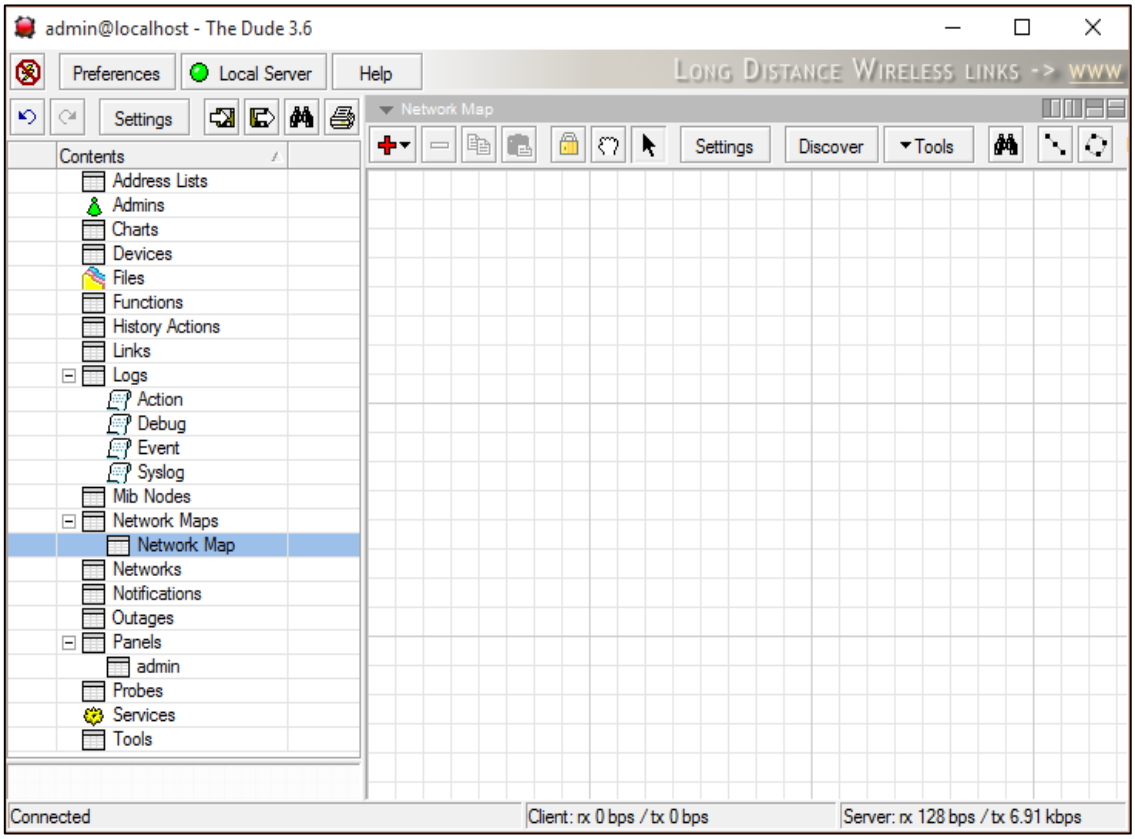

Figura 6. The Dude
Fonte: Autoria Própria

3.2. MÉTODOS

A primeira etapa para o desenvolvimento do trabalho foi o levantamento bibliográfico sobre redes locais virtuais e gerenciamento de redes.

A segunda etapa foi feito um levantamento da rede atual da empresa simulando na ferramenta Cisco Packet Tracer, e feitos testes utilizando a ferramenta Wireshark, medindo a quantidade de pacotes *broadcast* que são enviados na rede.

A terceira etapa, foi feito estudo e definição da segmentação da rede, e a simulação e implementação no Cisco Packet Tracer, utilizando os equipamentos que o mesmo disponibiliza.

A quarta etapa foi a configuração dos equipamentos, disponibilizados pelo Cisco Packet Tracer.

A última etapa foi a apresentação do software de gerenciamento The Dude.

4. RESULTADOS E DISCUSSÃO

4.1. REDE DE DADOS ATUAL DA EMPRESA

O crescimento constante da empresa, faz com que mais dispositivos sejam conectados na rede, causando crescimento desordenado da infraestrutura dos ativos e passivos de rede, além disso, muitos equipamentos não conseguem suportar o crescimento por serem obsoletos, causando problemas e lentidão.

Atualmente a rede não é segmentada e possui um único domínio de *broadcast* com mais de 300 dispositivos conectados. A Figura 7 mostra como está a rede atual, em que o *switch* principal, conecta o Bloco_1, Bloco_2, Bloco_3, Fabrica_1, Fabrica_2, Fabrica_3 e Logística.

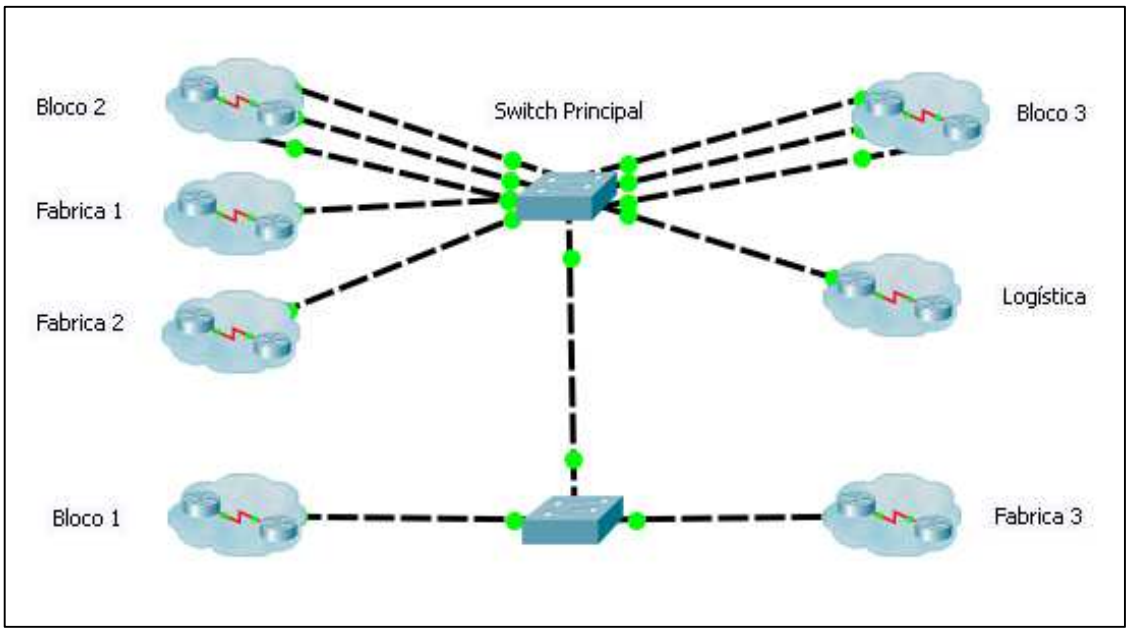

Figura 7. Distribuição do *switch* principal
Fonte: Autoria Própria

A Figura 8 mostra como está organizado o Bloco_1, dividido em três setores, Compras com sete computadores, RH (Recursos Humanos) com vinte computadores e duas impressoras, e Recepção com três computadores e uma impressora, todos conectados em dois *switches*, no qual o primeiro com conexão com um *switch* que está conectado ao *switch* principal.

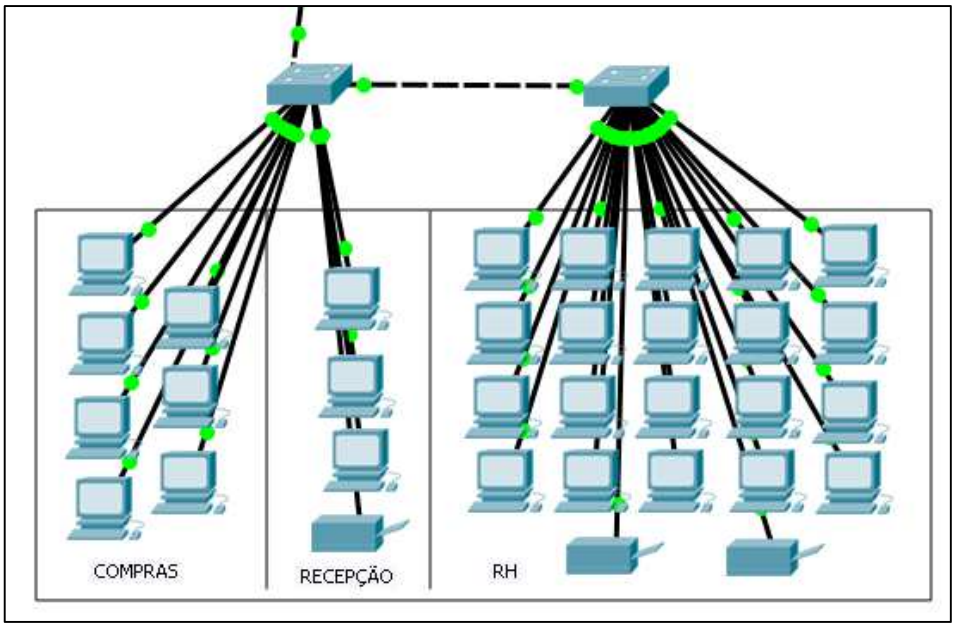

Figura 8. Bloco_1
Fonte: Autoria Própria

O Bloco_2 está dividido também em três setores conforme Figura 9, Vendas com trinta computadores, quatro notebooks e uma impressora conectados em dois *switches*, um deles conectado ao *switch* principal. Uma sala do setor de TI (Tecnologia e Informação), com sete computadores e alguns notebooks, ambos conectados a um *switch* e esse ao *switch* principal. E outra sala do setor de Recepção com três computadores e uma impressora, também conectados a um *switch* e esse ao *switch* principal.

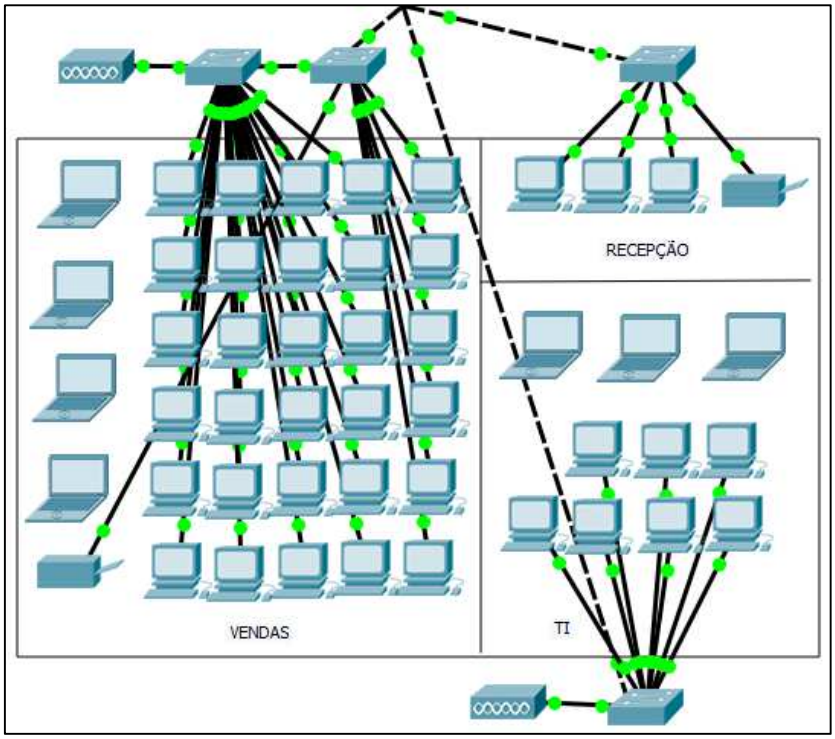

Figura 9. Bloco_2
Fonte: Autoria Própria

No Bloco_3, encontra-se os setores de Contabilidade com dezesseis computadores, Financeiro com quatorze computadores e duas impressoras, SAC (Serviço de Atendimento ao Consumidor) com quatro computadores, Jurídico com dois computadores, um notebook e uma impressora, uma segunda sala de Vendas com oito computadores, e outra sala de TI com nove computadores e um notebook. O Bloco_3 contém ainda uma sala com duas impressoras, dois notebooks, um computador, e quatro *switches* sendo três deles conectado no *switch* principal conforme mostra Figura 10.

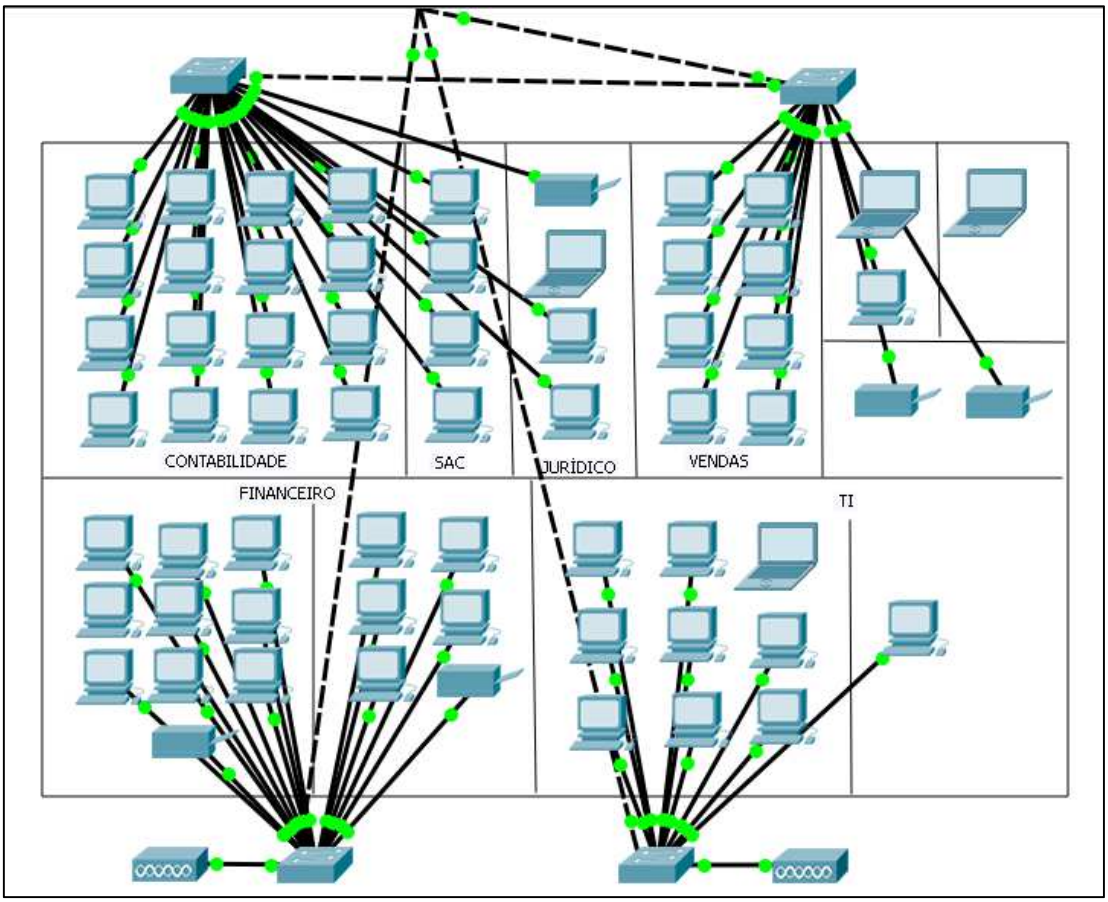

Figura 10. Bloco_3
Fonte: Autoria Própria

A Figura 11 mostra a Fabrica_1 e sua divisão, com os setores Supervisão, CQ (Controle e Qualidade), PCP (Planejamento e Controle de Produção), Engenharia, Desenvolvimento de Embalagens, Segurança do Trabalho, Laboratório, Oficina e Produção. Na Fabrica_1, tem seis *switches*, no qual apenas um está conectado ao *switch* principal, e mais de 75 equipamentos conectados.

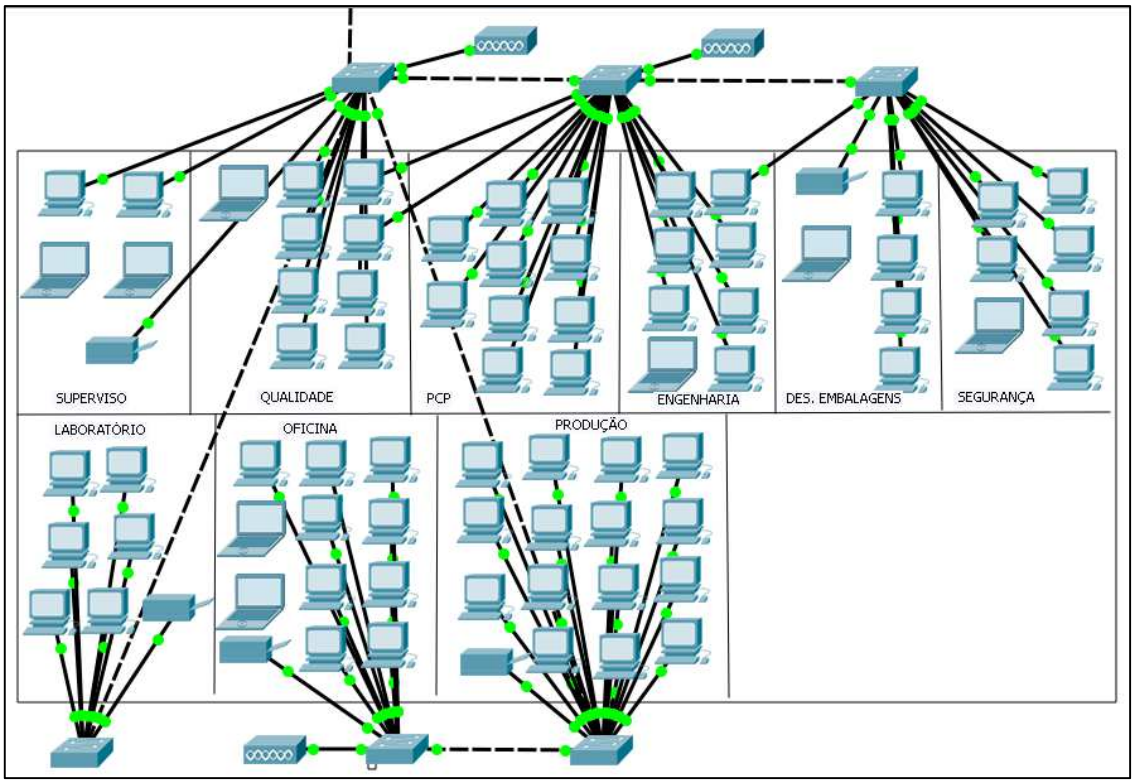

Figura 11. Fabrica_1
Fonte: Autoria Própria

A Figura 12 mostra como está organizado a Fabrica_2 e Fabrica_3, ambas as fabricas tem um *switch* cada conectados ao *switch* principal, e o setor Produção. A Fabrica_3 contém um setor a mais, o setor Restaurante. Com o total de doze equipamentos conectados.

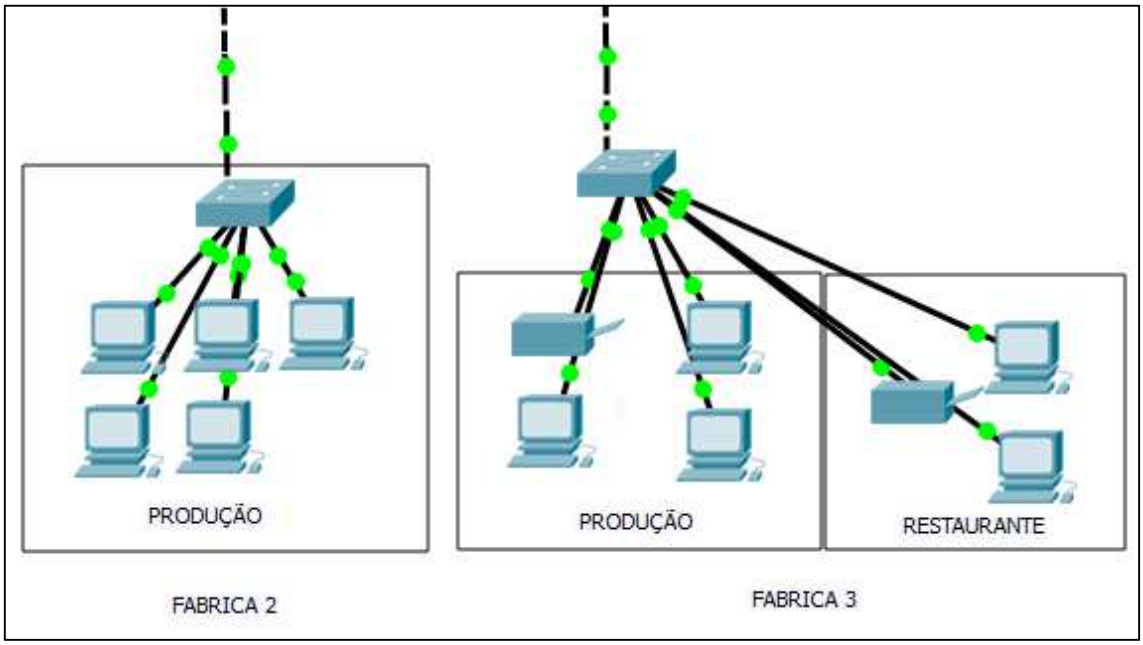

Figura 12. Fabrica_2 e Fabrica_3
Fonte: Autoria Própria

A Logística está organizada conforme Figura 13, onde o setor de Logística contém vinte computadores e três impressoras, e o setor CD (Centro de Distribuição) contém seis computadores e uma impressora, ambos conectados a dois *switches*, no qual um está conectado ao *switch* principal.

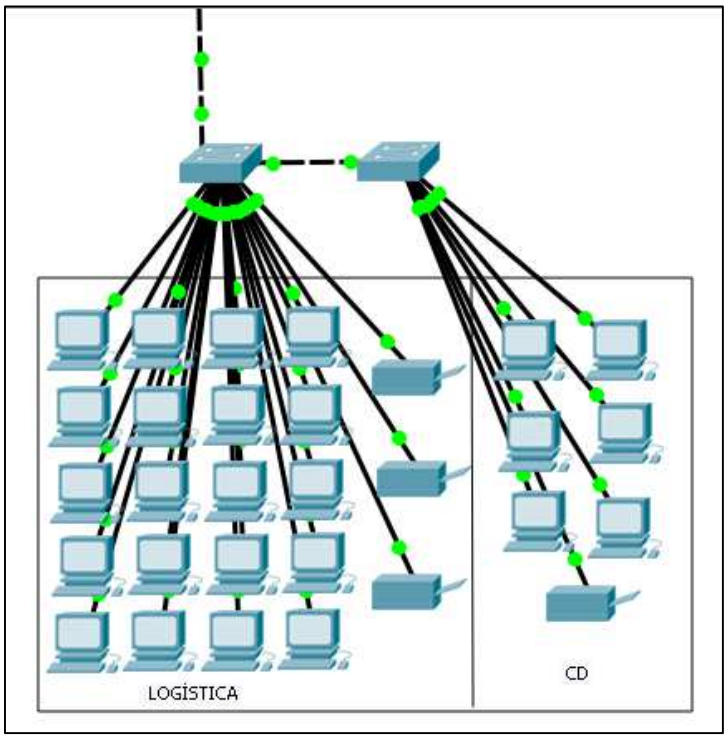

Figura 13. Logística
Fonte: Autoria Própria

A Figura 14 mostra a quantidade de pacotes que trafega em duas horas. Foi utilizado a ferramenta Wireshark para a captura de pacotes, em um computador localizado no setor de TI, a captura foi feita no período da tarde em horário de expediente. Na imagem o eixo *x* é a quantidade de pacotes e o eixo *y* é o tempo em minutos.

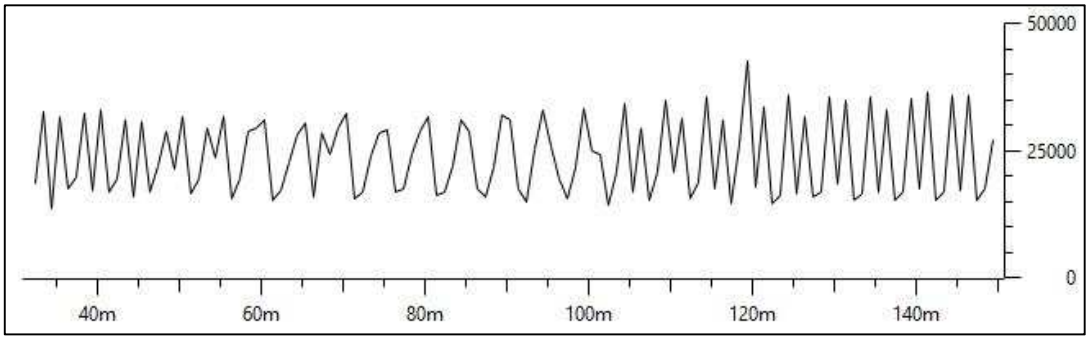

Figura 14. Tráfego de pacotes
Fonte: Autoria Própria

Através da captura, foi feito filtro dos pacotes *broadcast*. A Figura 15 apresenta o gráfico do tráfego de *broadcast* da rede atual da empresa.

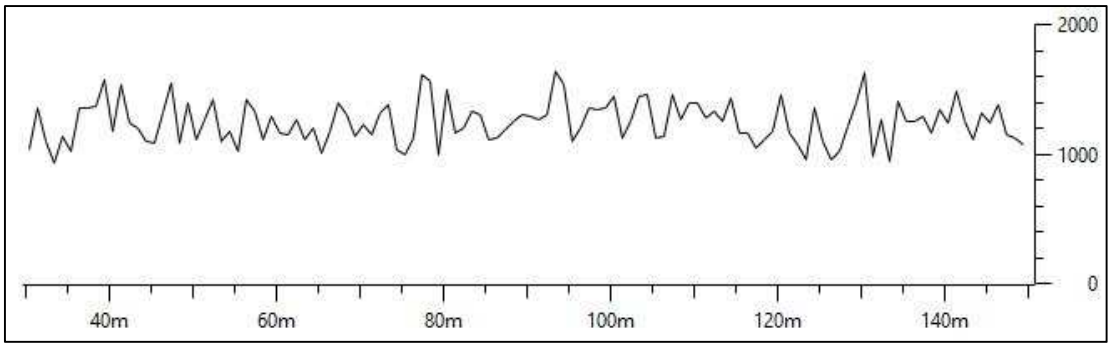

Figura 15. Tráfego *broadcast*
Fonte: Autoria Própria

Na imagem o eixo *x* é a quantidade de pacotes e o eixo *y* é o tempo em minutos.

4.2. PROPOSTA DE SEGMENTAÇÃO DA REDE LÓGICA

As VLANs foram divididas por setores da empresa, o Quadro 4 apresenta, o número, o nome, o número de dispositivos, faixa de IP e a máscara de cada VLAN.

ID	Nome	Nº de Disp	Rede/Prefixo	Faixa de IP	Máscara
2	Servidores	-	172.17.0.0/23	172.17.0.1 - 172.17.1.254	255.255.254.0
3	VOIP	-	172.17.2.0/23	172.17.2.1 - 172.17.3.254	255.255.254.0
4	Monitoramento	-	172.17.4.0/23	172.17.4.1 - 172.17.5.254	255.255.254.0
5	WiFi	-	172.17.6.0/23	172.17.6.1 - 172.17.7.254	255.255.254.0
100	Vendas	43	172.17.8.0/26	172.17.8.1 - 172.17.8.62	255.255.255.192
101	Producao	25	172.17.8.64/27	172.17.8.65 - 172.17.8.94	255.255.255.224
102	RH	22	172.17.8.96/27	172.17.8.97 - 172.17.8.126	255.255.255.224
103	Contabilidade	21	172.17.8.128/27	172.17.8.129 - 172.17.8.158	255.255.255.224
104	Logistica	20	172.17.8.160/27	172.17.8.161 - 172.17.8.190	255.255.255.224
105	Financeiro	16	172.17.8.192/27	172.17.8.193 - 172.17.8.222	255.255.255.224
106	TI	16	172.17.8.224/27	172.17.8.225 - 172.17.8.254	255.255.255.224
107	Oficina	11	172.17.9.0/27	172.17.9.1 - 172.17.9.30	255.255.255.224
108	PCP	10	172.17.9.32/27	172.17.9.33 - 172.17.9.62	255.255.255.224
109	Compras	8	172.17.9.64/28	172.17.9.65 - 172.17.9.78	255.255.255.240
110	CQ	8	172.17.9.80/28	172.17.9.81 - 172.17.9.94	255.255.255.240
111	Engenharia	8	172.17.9.96/28	172.17.9.97 - 172.17.9.110	255.255.255.240
112	Laboratorio	7	172.17.9.112/28	172.17.9.113 - 172.17.9.126	255.255.255.240
113	Recepcao	7	172.17.9.128/28	172.17.9.129 - 172.17.9.142	255.255.255.240
114	CD	7	172.17.9.144/28	172.17.9.145 - 172.17.9.158	255.255.255.240
115	Supervisao	6	172.17.9.160/28	172.17.9.161 - 172.17.9.174	255.255.255.240
116	Segurança	6	172.17.9.176/28	172.17.9.177 - 172.17.9.190	255.255.255.240
117	Embalagens	5	172.17.9.192/28	172.17.9.193 - 172.17.9.206	255.255.255.240
118	Juridico	4	172.17.9.208/28	172.17.9.209 - 172.17.9.222	255.255.255.240
119	SAC	4	172.17.9.224/28	172.17.9.225 - 172.17.9.238	255.255.255.240
120	Restaurante	3	172.17.9.240/28	172.17.9.241 - 172.17.9.238	255.255.255.240

Quadro 4. VLANs
Fonte: Autoria Própria

Foi utilizado o VLSM (*Variable Length Subnet Mask*) para o cálculo das sub-redes, e para evitar o desperdício de IPs. Optou-se pela segmentação de uma rede local virtual agrupada por porta, devido a facilidade na configuração e por ser mais simples em relação às outras opções, pois a rede possui um número de dispositivos conectados considerável.

As VLANs Servidores, VOIP, WiFi e Monitoramento (câmeras e catracas), por ter quantidades de dispositivos consideravelmente alto, ficaram com prefixo /23, tendo a possibilidade de conectar 510 dispositivos.

Para a VLANs Vendas com o maior número de dispositivos, 43 no total, o prefixo /26 podendo conectar 62 dispositivos. As VLANs Produção, RH, Contabilidade, Logística, Financeiro, TI, Oficina, PCP, ambos com aproximadamente 25 dispositivos ficaram com o prefixo /27, com possibilidade de 30 dispositivos conectados.

Por fim as VLANs Compras, CQ, Engenharia, Laboratório, Recepção, CD, Supervisão, Segurança, Embalagens, Jurídico, SAC e Restaurante, com número de dispositivos reduzidos, ficaram com o prefixo /28 com possibilidade de 14 dispositivos conectados.

4.3. PROPOSTA DE IMPLEMENTAÇÃO

Nesta seção é apresentado como foi realizada a implementação da segmentação da rede lógica, conforme Quadro 4, utilizando *switches* Cisco da ferramenta Cisco Packet Tracer.

Para a implementação será necessário um *switch* de núcleo, e sete *switches* para distribuição, nos quais ficará um *switch* para o Bloco_1, um para o Bloco_2, um para Bloco_3, um para Fabrica_1, um para Fabrica_2, um para Fabrica_3 e um *switch* para Logística, conforme Figura 16.

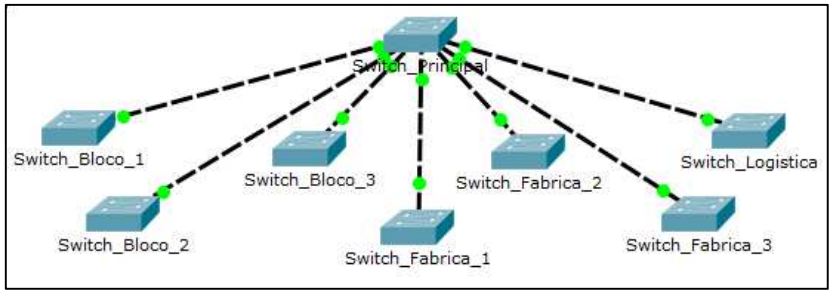

Figura 16. Separação de *Switches*
Fonte: Autoria Própria

Será necessário fazer a criação de todas as VLANs no *switch* de núcleo que foi nomeado *Switch*_Principal. O Quadro 5, mostra os comandos necessários para a criação das VLANs projetadas.

```
Switch_Principal(config)#vlan 2
Switch_Principal(config-vlan)#name Servidores
Switch_Principal(config-vlan)#vlan 3
Switch_Principal(config-vlan)#name VOIP
Switch_Principal(config-vlan)#vlan 4
Switch_Principal(config-vlan)#name Monitoramento
Switch_Principal(config-vlan)#vlan 5
Switch_Principal(config-vlan)#name WiFi
Switch_Principal(config-vlan)#vlan 100
Switch_Principal(config-vlan)#name Vendas
Switch_Principal(config-vlan)#vlan 101
Switch_Principal(config-vlan)#name Producao
Switch_Principal(config-vlan)#vlan 102
Switch_Principal(config-vlan)#name RH
Switch_Principal(config-vlan)#vlan 103
Switch_Principal(config-vlan)#name Contabilidade
Switch_Principal(config-vlan)#vlan 104
Switch_Principal(config-vlan)#name Logistica
Switch_Principal(config-vlan)#vlan 105
Switch_Principal(config-vlan)#name Finaceiro
Switch_Principal(config-vlan)#vlan 106
Switch_Principal(config-vlan)#name TI
Switch_Principal(config-vlan)#vlan 107
Switch_Principal(config-vlan)#name Oficina
Switch_Principal(config-vlan)#vlan 108
Switch_Principal(config-vlan)#name PCP
Switch_Principal(config-vlan)#vlan 109
Switch_Principal(config-vlan)#name Compras
Switch_Principal(config-vlan)#vlan 110
Switch_Principal(config-vlan)#name CQ
Switch_Principal(config-vlan)#vlan 111
Switch_Principal(config-vlan)#name Engenharia
Switch_Principal(config-vlan)#vlan 112
Switch_Principal(config-vlan)#name Laboratorio
Switch_Principal(config-vlan)#vlan 113
Switch_Principal(config-vlan)#name Recepcao
Switch_Principal(config-vlan)#vlan 114
Switch_Principal(config-vlan)#name CD
Switch_Principal(config-vlan)#vlan 115
Switch_Principal(config-vlan)#name Supervisao
Switch_Principal(config-vlan)#vlan 116
Switch_Principal(config-vlan)#name Seguranca
Switch_Principal(config-vlan)#vlan 117
Switch_Principal(config-vlan)#name Embalagens
Switch_Principal(config-vlan)#vlan 118
Switch_Principal(config-vlan)#name Juridico
Switch_Principal(config-vlan)#vlan 119
Switch_Principal(config-vlan)#name SAC
Switch_Principal(config-vlan)#vlan 120
Switch_Principal(config-vlan)#name Restaurante
```

Quadro 5. VLANs no *Switch*_Principal
Fonte: Autoria Própria

Nos *switches* de distribuição somente são criadas as VLANs necessárias, ou seja, conforme os comandos do Quadro 6. O *switch* que ficará no Bloco_1, receberá o nome de *Switch*_Bloco_1, e serão criadas as VLANs Compras, Recepção e RH. O *switch* que ficará no Bloco_2, receberá o nome de *Switch*_Bloco_2, e serão criadas as VLANs Vendas, TI e Recepção.

```
Switch_Bloco_1(config)#vlan 102
Switch_Bloco_1(config-vlan)#name RH
Switch_Bloco_1(config-vlan)#vlan 109
Switch_Bloco_1(config-vlan)#name Compras
Switch_Bloco_1(config-vlan)#vlan 113
Switch_Bloco_1(config-vlan)#name Recepcao
```

```
Switch_Bloco_2(config)#vlan 100
Switch_Bloco_2(config-vlan)#name Vendas
Switch_Bloco_2(config-vlan)#vlan 106
Switch_Bloco_2(config-vlan)#name TI
Switch_Bloco_2(config-vlan)#vlan 113
Switch_Bloco_2(config-vlan)#name Recepcao
```

Quadro 6. VLANs *Switch*_Bloco_1 e *Switch*_Bloco_2
Fonte: Autoria Própria

Conforme os comandos do Quadro 7, o *switch* que ficará no Bloco_3, receberá o nome de *Switch*_Bloco_3, e serão criadas as VLANs Contabilidade, Financeiro, Jurídico, Vendas e TI. O *switch* que ficará na Fabrica_1, receberá o nome de *Switch*_Fabrica_1, e serão criadas as VLANs Supervisão, Qualidade, PCP, Engenharia, Embalagens, Segurança, Laboratório, Oficina e Produção.

```
Switch_Bloco_3(config)#vlan 100
Switch_Bloco_3(config-vlan)#name Vendas
Switch_Bloco_3(config-vlan)#vlan 103
Switch_Bloco_3(config-vlan)#name Contabilidade
Switch_Bloco_3(config-vlan)#vlan 105
Switch_Bloco_3(config-vlan)#name Financeiro
Switch_Bloco_3(config-vlan)#vlan 106
Switch_Bloco_3(config-vlan)#name TI
Switch_Bloco_3(config-vlan)#vlan 118
Switch_Bloco_3(config-vlan)#name Juridico
```

```
Switch_Fabrica_1(config)#vlan 101
Switch_Fabrica_1(config-vlan)#name Producao
Switch_Fabrica_1(config-vlan)#vlan 107
Switch_Fabrica_1(config-vlan)#name Oficina
Switch_Fabrica_1(config-vlan)#vlan 110
Switch_Fabrica_1(config-vlan)#name CQ
Switch_Fabrica_1(config-vlan)#vlan 111
Switch_Fabrica_1(config-vlan)#name Engenharia
Switch_Fabrica_1(config-vlan)#vlan 112
Switch_Fabrica_1(config-vlan)#name Laboratorio
Switch_Fabrica_1(config-vlan)#vlan 115
Switch_Fabrica_1(config-vlan)#name Supervisao
Switch_Fabrica_1(config-vlan)#vlan 116
Switch_Fabrica_1(config-vlan)#name Seguranca
Switch_Fabrica_1(config-vlan)#vlan 117
Switch_Fabrica_1(config-vlan)#name Embalagens
```

Quadro 7. VLANs *Switch*_Bloco_3 e *Switch*_Fabrica_1
Fonte: Autoria Própria

O Quadro 8 apresenta os comandos do *switch* que ficará na Fabrica_2, e o *switch* que ficará na Fabrica_3, ambos receberão os nomes de *Switch*_Fabrica_2 e *Switch*_Fabrica_3 respectivamente, e será criada a VLAN Produção em cada um deles, e a VLAN Restaurante somente no *Switch*_Fabrica_3.

```
Switch_Fabrica_2(config)#vlan 101
Switch_Fabrica_2(config-vlan)#name Producao
```

```
Switch_Fabrica_3(config)#vlan 101
Switch_Fabrica_3(config-vlan)#name Producao
Switch_Fabrica_3(config-vlan)#vlan 120
Switch_Fabrica_3(config-vlan)#name Restaurante
```

Quadro 8. VLANs *Switch*_Fabrica_2 e *Switch*_Fabrica_3
Fonte: Autoria Própria

E por fim o Quadro 9 apresenta os comandos do *switch* que ficará na Logística, com o nome de *Switch*_Logistica, e serão criadas as VLANs Logística e CD.

```
Switch_Logistica(config)#vlan 104
Switch_Logistica(config-vlan)#name Logistica
Switch_Logistica(config-vlan)#vlan 114
Switch_Logistica(config-vlan)#name CD
```

Quadro 9. VLANs *Switch*_Logistica
Fonte: Autoria Própria

Além disso, deve-se criar um tronco em cada *switch* de distribuição com o *switch* núcleo (*Switch*_Principal) para que as VLANs sejam transportadas. A Figura 17 mostra como ficará a organização dos *switches* e VLANs, onde os computadores, representa as VLANs de cada *switch*.

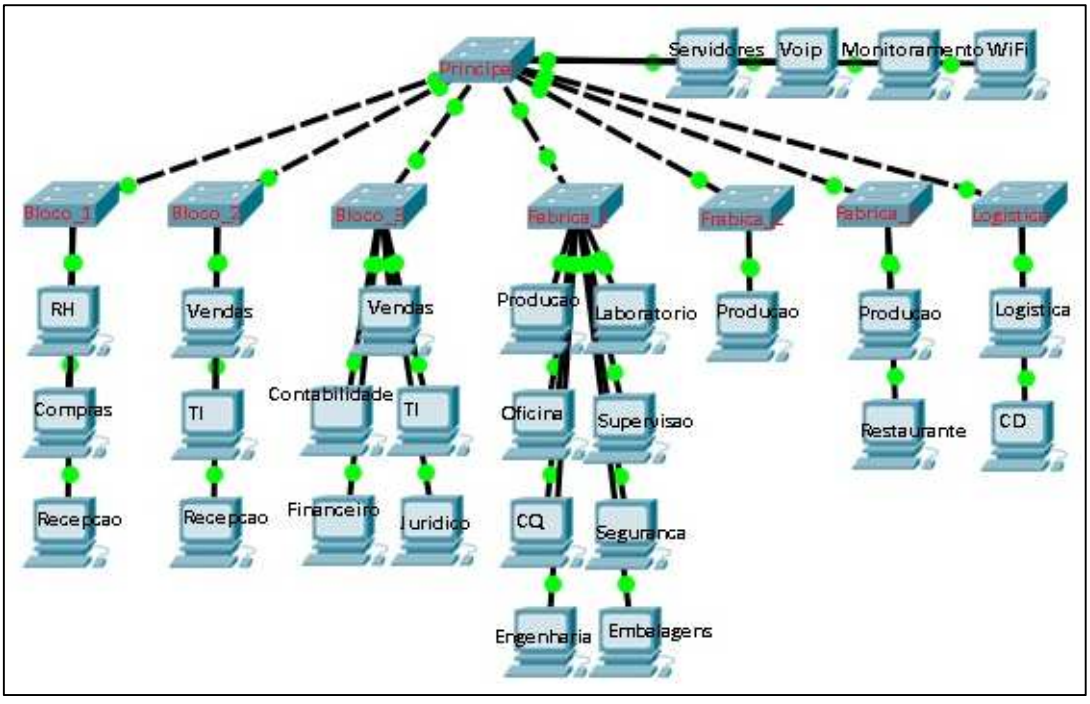

Figura 17. Organização *switches* e VLANs
Fonte: Autoria Própria

4.4. MONITORAMENTO DA REDE

Para auxiliar na manutenção da rede e fornecer informações do estado da rede, sugere-se a instalação de um software de monitoramento, visto que atualmente a manutenção é corretiva, ou seja, o problema é informado por um usuário, acarretando atrasos na solução do mesmo. Para isso foi utilizado o software The Dude, para obter informações do estado da rede, e tornar a equipe responsável proativa e ágil, em soluções de problemas relacionados a rede, além da facilidade de configuração e uso.

O software The Dude é desenvolvido pela empresa Mikrotik para monitorar e gerenciar a rede, possibilita verificar todos os dispositivos dentro da rede, controlar os serviços desses dispositivos e alertar caso algum serviço apresentar problemas, além de desenhar o mapa da rede. O *download* do software pode ser feito no site da Mikrotik pelo endereço http://www.mikrotik.com/thedude, e sua instalação é simples, basta aceitar o termo de licença, escolher os componentes e escolher o locar em que deseja instalar (MIKROTIK, 2015).

Para monitorar dispositivos da rede, basta utilizar a opção de adicionar o mesmo, colocando o número de IP, ou utilizando a opção de “descoberta”, no qual o software irá pesquisar na rede inteira e detectar os dispositivos conectados conforme Figura 18.

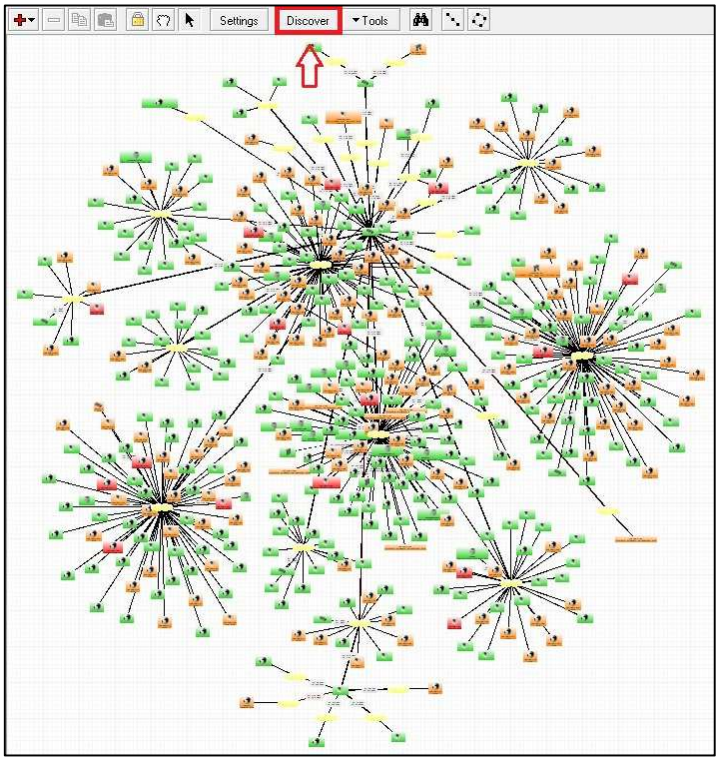

Figura 18. Descoberta de Rede
Fonte: Autoria Própria

O software The Dude utiliza o modelo de gerenciamento SNMP, permitindo monitorar e gerar alertas dos equipamentos gerenciados, independente de fabricantes, apenas com o requisito do dispositivo suportar o SNMP.

Depois de implementado as VLANs na empresa, é possível fazer o gerenciamento e monitoramento das mesmas, assim o administrador de rede terá informações para agir de maneira proativa e encontrar soluções mais rapidamente.

5. CONCLUSÃO

Este trabalho possibilitou apresentar a implementação da segmentação e monitoramento da rede de uma empresa. Utilizando-se do referencial teórico juntamente com o estudo de caso realizado em uma empresa do setor alimentício, foi possível organizar a rede segmentando através da VLANs.

O uso de VLANs possibilitou uma melhor organização da rede, foi criada uma VLAN para cada setor da empresa. Possibilitou também a melhoria na performance e segurança pois evita que usuários de um setor possa acessar a rede de outros setores. E por fim possibilitou diminuir o domínio de *broadcast*, fazendo com que cada setor fique em domínios separados, desfazendo assim, um único domínio de *broadcast*.

A facilidade de configuração e uso do software The Dude, além da apresentação visual das informações, torna-se a ferramenta de gerenciamento importante para a rede, no qual o administrador de rede pode ser proativo, podendo identificar problemas, e agir de forma mais rápida na solução.

Por ser uma rede considerável grande, e não sendo possível a paralisação total da rede para a configuração e implementação, a segmentação da rede foi simulada no Cisco Packet Tracer.

Pode-se concluir que com a segmentação de rede, juntamente com o gerenciamento dos dispositivos dessa rede, é essencial para o bom funcionamento, melhor performance e maior segurança, fazendo com que os administradores de rede tenham maior facilidade nas soluções de problemas, bem como menor números de problemas de rede.

5.1. TRABALHOS FUTUROS

Com a segmentação implementada pode-se perceber a possibilidade de melhorias. A seguir algumas sugestões para trabalhos futuros:

- Contingência do *switch* Principal e nos *switches* de distribuição;
- Utilização de roteador ou *switch* camada três para a comunicação entre VLANs, quando necessário;
- Organização da estrutura física em conjunto com a segmentação (cabeamento, racks, etc).

6. REFERÊNCIAS

CISCO. **CCNA EXPLORATION 4.0.** 2015. Disponível em http://www.pb.utfpr.edu.br/redes/cisco/. Acesso em 19 de agosto de 2015.

COSTA, Felipe. **Ambiente de Redes Monitorado com Nagios e Cacti.** 2008.

ENGLANDER, Irv. **A arquitetura de hardware computacional, software de sistema e comunicação em rede: uma abordagem da tecnologia da informação.** 2011.

FARREL, Adrian. **A Internet e seus protocolos: uma análise comparativa.** 2005.

FOROUZAN, Behrouz A. **Comunicação de dados e rede de computadores.** 2008.

HAFFERMAN, Leonardo. **Segmentação de Redes com VLAN.** 2009. Disponível em http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Leonardo%20Haffermann%20-%20Artigo.pdf. Acesso em 17 de agosto de 2015.

KUROSE, James F. **Redes de computadores e a Internet: uma abordagem top-down.** 2010.

MIKROTIK. **Mikrotik Routers and Wireless**. 2015. Disponível em http://www.mikrotik.com/thedude. Acesso em 14 de setembro de 2015.

MORAES, Igor M. **VLANs – Redes Locais Virtuais.** 2002. Disponível em http://www.gta.ufrj.br/grad/02_2/vlans/. Acesso em 21 de agosto de 2015.

SAYDAM, T; MAGEDANZ, T. **From Networks and Network Management into Service and Service Management, Journal of Networks and System Management.** 1996.

TANENBAUM, Andrew S. **Redes de computadores.** 2011.

WIRESHARK. **Wireshark.** 2015. Disponível em http://www.wireshark.org/. Acesso em 2 de setembro de 2015.