

UNIVERSIDADE FEDERAL DE SANTA MARIA
COLÉGIO TÉCNICO INDUSTRIAL DE SANTA MARIA
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

Thales Nicolai Tavares

**CTIWIFI - FERRAMENTA PARA MONITORAMENTO DE
REDES SEM FIO**

Santa Maria, RS
2016

CTISM/UFESM,RS

TAVARES, Thales Nicolai

Tecnólogo

2016

Thales Nicolai Tavares

CTIWIFI - FERRAMENTA PARA MONITORAMENTO DE REDES SEM FIO

Trabalho de Conclusão de Curso apresentado ao Curso Superior de Tecnologia em Redes de Computadores da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para a obtenção do grau de **Tecnólogo em Redes de Computadores**.

Orientador: Prof. Me. (UFSM) Renato Preigschadt de Azevedo

Santa Maria, RS

2016

Tavares, Thales Nicolai

CTIWIFI - Ferramenta para monitoramento de redes sem fio / por
Thales Nicolai Tavares. – 2016.

52 f.: il.; 30 cm.

Orientador: Renato Preigschadt de Azevedo

Trabalho de Conclusão de Curso - Universidade Federal de Santa
Maria, Colégio Técnico Industrial de Santa Maria, Curso Superior de
Tecnologia em Redes de Computadores, RS, 2016.

1. Redes de computadores. 2. Monitoramento. 3. Ferramenta.
4. Rede sem fio. I. Azevedo, Renato Preigschadt de. II. CTIWIFI -
Ferramenta para monitoramento de redes sem fio.

Thales Nicolai Tavares

CTIWIFI - FERRAMENTA PARA MONITORAMENTO DE REDES SEM FIO

Trabalho de Conclusão de Curso apresentado ao Curso Superior de Tecnologia em Redes de Computadores da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para a obtenção do grau de **Tecnólogo em Redes de Computadores**.

Aprovado em 06 de dezembro de 2016:

Renato Preigschadt de Azevedo, Me. (UFSM)
(Presidente/Orientador)

Bolívar Menezes da Silva, Tecng. (UFSM)

Rafael Teodósio Pereira, PhD. (UMinho)

Santa Maria, RS

2016

DEDICATÓRIA

Dedico este trabalho a meus pais Vera e Valdir, meus irmãos Ruan, Thomas e minha irmã Cristiane por sempre acreditarem que eu seria capaz.

AGRADECIMENTOS

Em primeiro lugar agradeço aos meus pais Vera da Silva Tavares e Valdir Celio. A. Streck por todo o apoio e incentivo que me deram durante esses anos, aos meus irmãos Ruan Carlo Tavares, Thomas Emanuel Tavares Streck e minha irmã Cristiane Tavares agradeço pelo companheirismo e confiança.

Agradeço a minha namorada Luana Mattiello pela compreensão, atenção, dedicação, e por estar sempre ao meu lado, ajudando e incentivando a passar por esta jornada.

Agradeço ao professor Renato Preigschadt de Azevedo, meu orientador e amigo, pelo apoio, esforço, paciência e confiança que depositou em mim. A ele também agradeço a oportunidade de participação em projeto de iniciação científica.

Agradeço também aos colegas bolsistas da sala 302 pela amizade, churrascos, piadas, brincadeiras e principalmente por estarem sempre dispostos a ajudar. Também agradeço aos professores do curso de Redes de Computadores, pois contribuíram para minha formação.

“O valor de uma coisa depende da maneira como a abordamos mentalmente e não da coisa em si”

(JIGORO KANO)

RESUMO

CTIWIFI - FERRAMENTA PARA MONITORAMENTO DE REDES SEM FIO

AUTOR: THALES NICOLAI TAVARES

ORIENTADOR: RENATO PREIGSCHADT DE AZEVEDO

As redes *Wireless* estão sendo usadas significativamente, de forma a coexistir entre as redes tradicionais que são interligadas através de cabos, sendo assim, se faz necessário o monitoramento aplicado em redes sem fio. Com o monitoramento da rede, pode-se melhorar a qualidade do serviço, tendo em vista aumentar a eficiência e produtividade. Este trabalho descreve uma ferramenta desenvolvida denominada CTIWifi que tem como objetivo auxiliar no monitoramento da rede sem fio. Essa ferramenta apresenta informações compreensíveis da infraestrutura sem fio, como por exemplo, gráficos da quantidade de dispositivos conectados. Esses tipos de gráficos são personalizáveis e interativos, pois, conforme o usuário navega pelo gráfico, o mesmo exibe mais informações. A ferramenta foi desenvolvida na linguagem PHP, junto com a biblioteca Net-SNMP, a qual possui um conjunto de funcionalidades que atuam no protocolo SNMP, o qual tem como propósito monitorar e gerenciar dispositivos de redes. A contribuição da ferramenta proposta é atender o propósito de ter um sistema que monitore e permita a visualização dos dispositivos que se conectam na rede sem fio.

Palavras-chave: Redes de computadores. Monitoramento. Ferramenta. Rede sem fio.

ABSTRACT

CTIWIFI - TOOL FOR MONITORING WIRELESS NETWORKS

AUTHOR: THALES NICOLAI TAVARES

ADVISOR: RENATO PREIGSCHADT DE AZEVEDO

Wireless networks are being used significantly in order to coexist between traditional networks that are interconnected through cables. Therefore, the monitoring applied in wireless networks has been necessary. By monitoring the network, you can improve the quality of service in order to increase efficiency and productivity. This work describes a developed tool, called CTIWifi, that aims to assist in the monitoring of the wireless network. This tool presents understandable wireless infrastructure information, such as graphs of the number of connected devices. These types of charts are customizable and interactive because, as the user browses the chart, it displays more information. The tool was developed in the PHP language, along with the Net-SNMP library, which has a set of functionalities that work on the SNMP protocol, which aims to monitor and manage network devices. The contribution of the proposed tool is to serve the purpose of having a system that monitors and allows the visualization of the devices that connect in the wireless network.

Keywords: Computer network. Monitoring. Tool. Wireless network.

LISTA DE FIGURAS

Figura 2.1 – Coleta informações SNMP	20
Figura 2.2 – Solicitação de objeto gerenciável pelo gerente ao agente	22
Figura 2.3 – Árvore MIB	22
Figura 3.1 – Tela do módulo Dados sobre as Interfaces	29
Figura 3.2 – Tela do módulo Dados da tabela IP ARP	30
Figura 3.3 – Tela do <i>software</i> de monitoramento	31
Figura 4.1 – Gráficos biblioteca Chart.js	35
Figura 4.2 – Diagrama Funcional	36
Figura 4.3 – Arquitetura da Aplicação	37
Figura 4.4 – Classe MostraConectados	37
Figura 4.5 – Classe Banco	38
Figura 4.6 – Modelo ER do banco	39
Figura 4.7 – Gráficos da Interface	40
Figura 5.1 – Tela do Sistema de Máquina Virtual	42
Figura 5.2 – Tela de Login da Aplicação	43
Figura 5.3 – Tela de Busca de Dispositivos.....	43
Figura 5.4 – Tela de Seleção do Protocolo	44
Figura 5.5 – Tela de Dispositivos Encontrados	44
Figura 5.6 – Tela de Configuração de <i>e-mail</i> para Alerta	45
Figura 5.7 – Menu Aplicação	45
Figura 5.8 – Gráficos referente ao <i>Access Point</i> CTISM-SSI-LAB301	46
Figura 5.9 – Gráficos referente ao <i>Access Point</i> CTISM-SSI-LAB-1ANDAR	47
Figura 5.10 – Gráficos referente ao <i>Access Point</i> CTISM-SSI-SEDE-A	47

LISTA DE TABELAS

Tabela 2.1 – Grupos da MIB2	23
Tabela 3.1 – Comparação entre recursos disponíveis	24
Tabela 3.2 – Comparação entre funcionalidades disponíveis	25
Tabela 3.3 – Tabela de comparação	26
Tabela 3.4 – Comparação entre os NMS em análise	27
Tabela 3.5 – Comparação entre as versão do WhatsUp Gold	28

LISTA DE ABREVIATURAS E SIGLAS

ASP	Active Server Pages
CSS	Cascading Style Sheets
DES	Data Encryption Standard
FCAPS	Fault, Configuration, Accounting, Performance, Security
HTML	Hypertext Markup Language
IDS	Intrusion Detection System
IMAP	Internet Message Access Protocol
IP	Internet Protocol
ISO	International Organization for Standardization
LTS	Long Term Support
MAC	Media Access Control
MD5	Message-Digest algorithm 5
MIB	Management Information Base
NMS	Network Management System
OID	Object Identifiers
OAM&P	Operation, administration, maintenance and provisioning
OSI	Open System Interconnection
PDU	Protocol Data Unit
PHP	Hypertext PreProcessor
POP	Post Office Protocol
RFC	Request for Comments
SGBD	Sistema Gerenciador de Banco de Dados
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
TCP	Transmission Control Protocol
VMS	Sistema de Máquina Virtuais

SUMÁRIO

1 INTRODUÇÃO	13
1.1 OBJETIVOS	14
2 GERENCIAMENTO EM REDES DE COMPUTADORES	15
2.1 MONITORAMENTO DE REDES DE COMPUTADORES	15
2.2 PERSPECTIVAS DE GERENCIAMENTO DE REDES	16
2.2.1 FCAPS	16
2.2.1.1 <i>Fault</i>	16
2.2.1.2 <i>Configuration</i>	17
2.2.1.3 <i>Accounting</i>	17
2.2.1.4 <i>Performance</i>	17
2.2.1.5 <i>Security</i>	18
2.2.2 OAM&P	18
2.2.2.1 <i>Operations</i>	18
2.2.2.2 <i>Administration</i>	18
2.2.2.3 <i>Maintenance</i>	18
2.2.2.4 <i>Provisioning</i>	19
2.3 PROTOCOLO SNMP	19
2.3.1 SNMP v1	20
2.3.2 SNMP v2	20
2.3.3 SNMP v3	21
2.3.4 MIB	21
3 TRABALHOS RELACIONADOS	24
4 CTIWIFI - FERRAMENTA PARA MONITORAMENTO DE REDES SEM FIO..	33
4.1 MATERIAIS UTILIZADOS NO DESENVOLVIMENTO	33
4.1.1 PHP	33
4.1.2 Banco de dados MySQL	34
4.1.3 JavaScript	34
4.1.4 Chart.js	34
4.1.5 Apache	35
4.2 MÉTODO DE DESENVOLVIMENTO	36
4.2.1 Módulo de Controle	37
4.2.2 Classe Banco	38
4.2.3 Interface	40
5 EXPERIMENTOS E RESULTADOS	42
6 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS	49
6.1 TRABALHOS PUBLICADOS	50
REFERÊNCIAS	51

1 INTRODUÇÃO

As redes de computadores foram criadas com o propósito inicial de compartilhamento de dados e serviços de dispositivos. De acordo com Kurose e Ross (2010), quando o número de usuários de redes de computadores não era muito grande, a gerência e o monitoramento não eram utilizados. Porém, com o passar do tempo, a rápida evolução das tecnologias de redes foi o fator que contribuiu para a difusão das redes de computadores pelo mundo todo.

Segundo Stallings (1999), as redes de computadores, que não possuem gerenciamento, estão sujeitas a não continuar funcionando por muito tempo. O gerenciamento e monitoramento permitem a construção de uma representação geral e em tempo real do estado da rede para o seu administrador. Isto permite a prevenção e detecção de problemas na infraestrutura das redes de computadores, provendo assim uma operação com maior qualidade.

Gerenciamento de redes de computadores é o controle de atividades e monitoramento dos elementos da rede. Através do monitoramento da rede, é possível melhorar a qualidade de serviço, tendo em vista a eficiência e produtividade. A prática de gerenciamento de redes de computadores está tornando-se uma tarefa difícil, especialmente em redes constituídas por muitos dispositivos.

As informações que trafegam em uma rede de computadores precisam ser encaminhadas de modo rápido e seguro. Uma rede de computadores que não possua recursos de gerenciamento está exposta a possíveis problemas de funcionamento, até mesmo de segurança. Estes problemas prejudicarão a produtividade e o legítimo funcionamento da rede, sendo assim, afetando sua integridade e segurança.

A utilização de ferramentas que possibilitam o gerenciamento de redes está se tornando cada vez maior. Levando em consideração que a tarefa de gerenciar uma rede de computadores pode ser composta por um ou mais serviços, trabalhando em conjunto para monitorar as possíveis falhas que comprometam sua integridade.

Para permitir um monitoramento mais eficiente e um maior acesso as informações, foi desenvolvida uma ferramenta de monitoramento com o foco em redes sem fio denominada CTIWifi. Tendo em vista detectar problemas, esta ferramenta busca auxiliar os administradores de redes na tarefa de monitoramento, apresentando gráficos de fácil leitura das informações da infraestrutura sem fio. A ferramenta recebeu este nome em homenagem ao Colégio Técnico Industrial de Santa Maria, onde o curso de Redes de Computadores está vinculado. Essa

ferramenta foi desenvolvida em PHP (*Hypertext PreProcessor*) devido conceitos básicos da linguagem ser de fácil de aprendizagem, além de possuir uma grande quantidade de biblioteca disponível, o que facilita no desenvolvimento de aplicações.

A organização deste trabalho está segmentada em Capítulos. O Capítulo 2 apresenta uma rápida introdução sobre a gerência de redes de computadores, perspectivas de gerenciamento de redes de computadores e protocolo SNMP (*Simple Network Management Protocol*) para gerenciamento de redes, bem como suas versões. O Capítulo 3 apresenta os trabalhos relacionados, que serviram como base para o desenvolvimento deste trabalho. No Capítulo 4 será apresentado o desenvolvimento da ferramenta CTIWifi, e os experimentos realizados na ferramenta desenvolvida são apresentados no Capítulo 5. Por fim, o Capítulo 6 apresenta as considerações finais e as abordagens para trabalhos futuros.

1.1 OBJETIVOS

O monitoramento da rede possibilita melhorar a qualidade de serviço, visando a eficiência e a produtividade, portanto, o presente trabalho tem como objetivo apresentar uma ferramenta de gerenciamento com o foco em redes sem fio. Essa ferramenta apresenta gráficos compreensíveis das informações da infraestrutura sem fio, como por exemplo, a quantidade de dispositivos conectados, auxiliando no gerenciamento e monitoramento de uma infraestrutura *Wireless* de forma dinâmica e interativa, assim buscando trazer uma melhor percepção do estado da rede para o administrador.

Depois de ter a compreensão do assunto relativo a linguagens de programação voltadas para a WEB e monitoramento de redes de computadores, foi desenvolvida uma aplicação com o intuito de auxiliar o gerenciamento e monitoramento da redes *Wireless*.

Com o desenvolvimento da aplicação os seguintes itens poderão ser solucionados:

- Gráficos compreensíveis de informações da infraestrutura sem fio.
- Obter informações atualizadas da quantidade de dispositivos conectados.
- Prover uma interface gráfica, para exibir informações de forma dinâmica.

2 GERENCIAMENTO EM REDES DE COMPUTADORES

Este capítulo tem como objetivo apresentar uma breve revisão sobre o assunto de gerenciamento de redes de computadores, tendo em vista auxiliar o entendimento dos conteúdos presentes na elaboração deste trabalho. A fim de possibilitar um melhor entendimento sobre os assuntos abordados, a Seção 2.1 apresenta uma introdução sobre redes de computadores e monitoramento; na Seção 2.2 são apresentadas perspectivas de gerenciamento como FCAPS (*Fault, Configuration, Accounting, Performance, Security*) na Subseção 2.2.1 e OAM&P (*Operation, administration, maintenance, provisioning*) na Subseção 2.2.2; a Seção 2.3 apresenta o funcionamento do protocolo SNMP, bem como suas versões, as quais são apresentadas nas Subseções 2.3.1, 2.3.2 e 2.3.3; a Subseção 2.3.4 é apresentado o conceito de MIB (*Management Information Base*).

2.1 MONITORAMENTO DE REDES DE COMPUTADORES

Uma rede de computadores é um conjunto de dispositivos que estão ligados de maneira que possibilitem a realização da troca de informações e compartilhamento de recursos. Com o passar dos anos, as redes de computadores se tornaram parte do dia a dia das pessoas, sendo um dos fatores contribuintes para o seu crescimento.

Gerenciar uma rede de computadores é uma tarefa de monitoramento dos elementos ativos da rede, sejam eles *hardware* ou *software* que façam parte da mesma. De acordo com Kurose e Ross (2010), o gerenciamento de rede contém a disponibilização, integração e a coordenação de elementos de *hardware*, *software* e humanos para monitorar, consultar, configurar e controlar os recursos da rede e seus elementos.

Segundo Stallings (1999), um sistema de gerência de rede compreende-se como um conjunto de ferramentas integradas para monitorar e gerenciar uma rede. Esse sistema possui uma interface gráfica, com informações sobre a rede, podendo oferecer também um conjunto de comandos que são utilizados para executar quase todas as tarefas de gerência da rede.

Devido às tecnologias existentes, é possível realizar o monitoramento dos dispositivos em uma rede. Isso ocorre devido às ferramentas e protocolos de gerenciamento onde é possível diminuir essa complexidade, tornando mais simples a tarefa de monitorar os dispositivos existentes na rede. Segundo Dias (2008), os protocolos de monitoramento de rede determinam um

formato para o envio de dados entre os ativos de redes monitorados e as máquinas responsáveis pelo armazenamento de tais informações. Existem protocolos como o SNMP, o qual será abordado na Seção 2.3, que possibilitam que dados dos dispositivos da rede sejam coletados, durante o seu funcionamento. Esses dados não fornecem um diagnóstico pronto da rede, mas são usados no processo que ajudam para a criação de estatísticas do funcionamento da rede.

2.2 PERSPECTIVAS DE GERENCIAMENTO DE REDES

A prática do gerenciamento da rede concede ao administrador uma percepção do que está ocorrendo na rede em tempo de execução, onde lhe é permitido localizar qualquer fato que seja considerado fora do comportamento padrão e que possa afetar o legítimo funcionamento da rede. Para garantir que a rede forneça disponibilidade de serviços e qualidade, é indispensável o gerenciamento de rede.

O conjunto de atividades, métodos e procedimentos relacionados ao gerenciamento podem ser classificados de forma a ser baseada em funcionalidades como o FCAPS, o qual será apresentado na Subseção 2.2.1 ou baseado em operações de rotina como OAM&P, o qual será apresentado na Subseção 2.2.2.

2.2.1 FCAPS

De acordo com Stallings (1999), a preocupação em simplificar e projetar o desenvolvimento de propostas designadas ao gerenciamento de rede, a ISO (*International Organization for Standardization*) apresenta o Modelo de Gerenciamento OSI (*Open System Interconnection*), o qual estabelece áreas funcionais do gerenciamento, sendo elas *Fault*, *Configuration*, *Accounting*, *Performance* e *Security*, as quais são apresentados nas Subseções 2.2.1.1, 2.2.1.2, 2.2.1.3, 2.2.1.4 e 2.2.1.5.

2.2.1.1 *Fault*

O gerenciamento de falhas é encarregado por identificar, isolar e reparar as falhas que podem ocorrer nos dispositivos de rede ou serviços disponibilizados nela. O gerenciamento de falhas está, portanto, interessado no monitoramento da rede para garantir que tudo esteja funcionando regularmente.

Segundo Santos (2015), o gerenciamento de falhas é o conjunto de recursos que pos-

sibilita a detecção, isolamento e correção de condições anormais de operação do ambiente. É um trabalho relevante, visto que o propósito é ter o conhecimento dos problemas antes que os usuários sejam prejudicados e reportem aos administradores.

2.2.1.2 *Configuration*

O gerenciamento de configuração é encarregado pelo registro e manutenção dos parâmetros de configuração dos serviços da rede, tais como informações sobre versões de *software*. Também é responsável pela configuração de dispositivos da rede, seja de forma presencial ou remota.

Ferramentas para configuração são usadas para possibilitar a realização de alterações no funcionamento dos equipamentos. A manutenção de todos os dispositivos de uma rede não é uma tarefa muito simples, necessitando considerar a inclusão, remoção e atualização das informações sobre cada dispositivo. Deste modo, uma boa gerência de configuração para realizar estas atividades deve monitorar todas as mudanças realizadas nos dispositivos.

2.2.1.3 *Accounting*

O gerenciamento de contabilidade é responsável por calcular o uso dos serviços disponibilizados na rede, de forma a definir os custos para os fornecedores de serviços e demais clientes e consumidores. O objetivo dessa gerência é contabilizar as ocorrências que acontecem durante a operação da rede.

A contabilização permite o controle e a cobrança pelo uso dos recursos da rede, ou seja, controla e notifica os usuários sobre os custos dos recursos consumidos. Também podem ser definidos limites de uso dos recursos e tarifação adicional quando ocorre o consumo além do contratado.

2.2.1.4 *Performance*

O gerenciamento de desempenho é o responsável pela verificação das informações sobre aspectos de desempenho dos serviços de rede. Estas informações são utilizadas para certificar que a rede funcione com qualidade para seus respectivos usuários.

As informações coletadas também são utilizadas para identificar possíveis gargalos e congestionamentos na rede. De acordo com Santos (2015), o gerenciamento de desempenho

envolve manter o desempenho da rede em níveis aceitáveis através de verificações e gerência de diversas variáveis ligadas ao desempenho.

2.2.1.5 *Security*

A gerência de segurança é responsável por restringir o acesso à rede e impedir o uso incorreto por parte de seus usuários, de forma intencional ou não. Ela ajuda os administradores na construção de uma rede segura, buscando impedir problemas de segurança de informação. Nesse sentido, envolve o uso de ferramentas IDS (*Intrusion Detection System*), *firewall* entre outros. Entre as funções dessa categoria, pode ser destacada garantir o controle de acesso quanto à prevenção e detecção ataques aos recursos de rede.

2.2.2 **OAM&P**

Conforme Amaro (2010), OAM&P é um modelo de gerência para operações de rotina em ambiente de rede que detecta, diagnostica e corrige falhas, mantendo o funcionamento do sistemas, integrando de forma organizada as funções de *Operations*, *Administration*, *Maintance* e *Provisioning*, as quais são apresentados nas Subseções 2.2.2.1, 2.2.2.2, 2.2.2.3 e 2.2.2.4.

2.2.2.1 *Operations*

As operações são as ações diárias executadas na rede, ou seja, o monitoramento para averiguar o funcionamento correto da rede.

2.2.2.2 *Administration*

A administração abrange o planejamento da rede em longo prazo, dados estatísticos, estratégia e tendências, ou seja, funções de suporte a rede que não envolvem mudanças de configuração.

2.2.2.3 *Maintance*

A manutenção envolve as atividades de atualizações, troca de equipamentos, tarefas que causa a paralisação da rede por determinado tempo, assim sendo necessário um planejamento para não gerar um impacto maior.

2.2.2.4 Provisioning

O provisionamento entende-se como a remoção ou criação de serviços, instalações de equipamentos ou configuração de parâmetros na rede para deixá-la funcionando de acordo com o esperado.

2.3 PROTOCOLO SNMP

O SNMP é um protocolo que surgiu no ano de 1988 para suprir à necessidade de um modelo para gerenciar os dispositivos em redes TCP/IP (*Transmission Control Protocol/ Internet Protocol*). Segundo Kurose e Ross (2010), o protocolo SNMP passou por modificações até chegar a versão SNMPv3, a qual foi lançada em abril de 1999 e atualizada em dezembro de 2002.

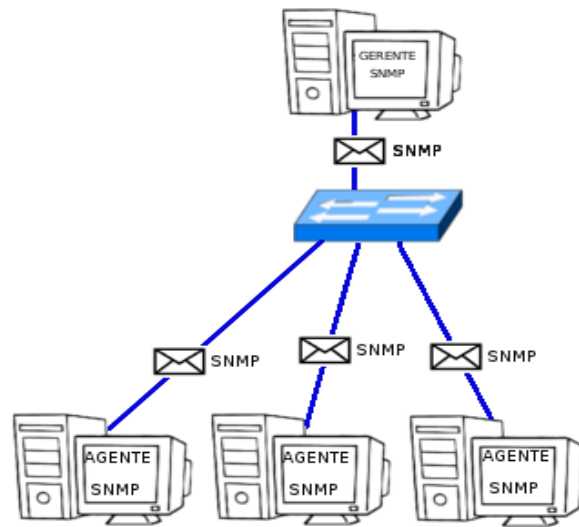
O protocolo SNMP é aplicado para auxiliar o monitoramento e gerenciamento de redes de computadores, com o intuito de simplificar a troca de informações de gerenciamento entre dispositivos de rede. Esse protocolo atua na camada de aplicação, e realiza a troca de mensagens entre os dispositivos da rede e o *software* de monitoramento.

De acordo com Kurose e Ross (2010), o protocolo SNMP foi projetado e oferecido rapidamente em uma época em que a necessidade de gerenciamento de rede começava a ficar indispensável, dessa forma, encontrou uma ampla aceitação. Conforme Kurose e Ross (2010), esse protocolo é a estrutura de gerenciamento de rede mais amplamente usada e disseminada.

Segundo Santos (2015), o SNMP é um protocolo fácil de ser implementado em equipamentos e flexível para aceitar modificações posteriores, visto que possui poucas operações. Os dispositivos monitorados podem ser roteadores, servidores, entre outros dispositivos de redes. O agente é um módulo do *software* de gerenciamento de rede, executado no dispositivo gerenciado. Este agente possui acesso ao estado do dispositivo e transforma essas informações para o formato compatível com o protocolo SNMP.

Conforme Oesterreich (2012), o SNMP segue o modelo Agente - Gerente, o qual um computador funciona como gerente e os demais atuam como agentes. De acordo com Mauro e Schmidt (2005), é possível gerenciar qualquer dispositivo que possibilite a recuperação de informações de SNMP. Um computador pode ser eleito como gerente de rede, o mesmo coleta dados dos demais dispositivos conectados na rede e que são chamados de agentes, como mostra a Figura 2.1.

Figura 2.1: Coleta informações SNMP



Fonte: Acervo pessoal.

2.3.1 SNMP v1

De acordo com Santos (2015), o SNMPv1 é definido na RFC (*Request for Comments*) 1157¹. O SNMPv1 apresenta autenticação baseada em *strings* de comunidades, ou seja, *string* de texto plano, que possibilita que qualquer *sniffer* de rede que reconheça a *string*, consiga tenha acesso a informações de gerenciamento de um dispositivo. A primeira versão do SNMP consiste de cinco PDUs (*Protocol Data Unit*) existentes, sendo elas *GetRequest*, *GetNextRequest*, *GetResponse*, *SetRequest* e *Trap*.

2.3.2 SNMP v2

Em 1993, no intuito de melhorar o SNMP, surgiu a segunda versão do protocolo, chamada de SNMPv2. Segundo Santos (2015), as principais RFC's que definem essa versão são as 3416², 3417³ e 3418⁴. O SNMPv2 traz consigo mais funcionalidades que a primeira versão como novos tipos de dados, melhoramento na recuperação de grandes volumes de dados, melhor desempenho, porém segue usando autenticação baseada nas *strings* de comunidades.

¹ <https://www.ietf.org/rfc/rfc1157.txt>

² <https://tools.ietf.org/rfc/rfc3416.txt>

³ <https://tools.ietf.org/rfc/rfc3417.txt>

⁴ <https://tools.ietf.org/rfc/rfc3418.txt>

Essa versão do protocolo apresenta sete tipos de PDU disponíveis, sendo as cinco da primeira versão com o acréscimo de *GetBulkRequest* e *InformRequest*.

2.3.3 SNMP v3

Em dezembro de 2002 surgiu a terceira versão do protocolo, chamada de SNMPv3. De acordo com Santos (2015), as principais RFC's desta versão são 3410⁵ à 3418⁶ e 2576⁷. De acordo com Péricas (2003), a terceira versão do SNMP apresenta melhorias na segurança, tais como autenticação e privacidade, tão necessárias e exigidas no gerenciamento remoto de redes. Essa versão também traz modificações importantes nos tipos de dados e nos objetos gerenciados, no modelo de segurança. A segurança é conseguida através da introdução de mecanismos de criptografia com o DES (Data Encryption Standard) e de algoritmos de autenticação que podem ser tanto o MD5 (Message-Digest algorithm 5) quanto o SHA (Secure Hash Algorithm).

2.3.4 MIB

A MIB é o conjunto de objetos gerenciados, que procura englobar as informações essenciais para a gerência da rede. A SMI (*Structure of Management Information*) possibilita uma maneira de definir os objetos gerenciados e seus comportamentos.

Um agente dispõe de uma lista de objetos que ele controla. Um possível objeto é a condição operacional, como exemplo, o estado da interface de um computador que pode estar *up* ou *down*. Um objeto gerenciado é a visão abstrata de um recurso real do sistema. Sendo assim, os recursos da rede que devem ser gerenciados são modelados, e as estruturas dos dados decorrentes são os objetos gerenciados.

Podemos pensar em um banco de dados de objetos gerenciados e rastreados pelos agentes, onde qualquer tipo de *status* ou dados estatísticos que podem ser acessados pelo gerente. A MIB é usada para administrar os elementos em uma rede de computadores, que na maior parte das vezes é associadas com o protocolo SNMP, como mostra a Figura 2.2.

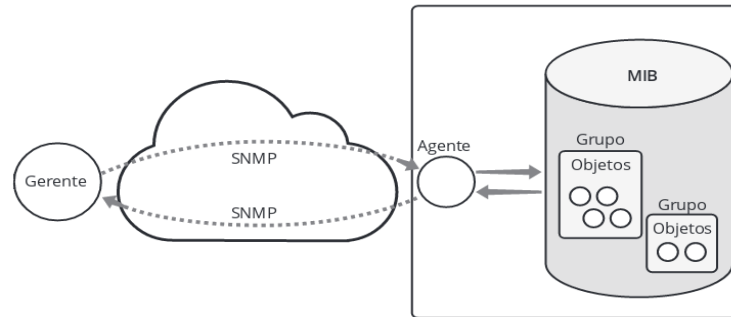
Para Kurose e Ross (2013), a base de informações de gerenciamento é similar a um banco de dados virtual que preserva em seus objetos os dados coletados da rede. As informações são coletadas pelos dispositivos gerenciados ou pelo gerente SNMP.

⁵ <https://www.rfc-editor.org/rfc/rfc3410.txt>

⁶ <https://tools.ietf.org/rfc/rfc3418.txt>

⁷ <https://www.ietf.org/rfc/rfc2576.txt>

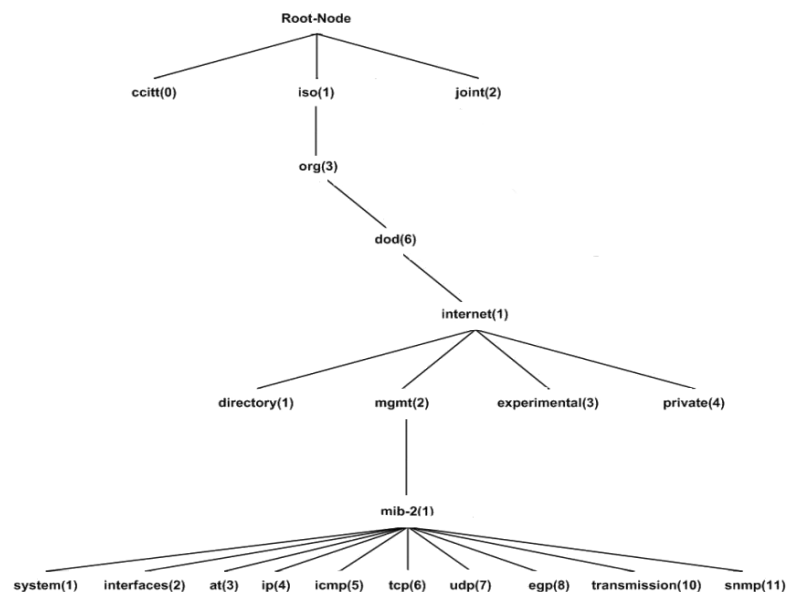
Figura 2.2: Solicitação de objeto gerenciável pelo gerente ao agente



Fonte: (SANTOS, 2015).

As informações estão organizadas na MIB de forma hierárquica, como mostra a Figura 2.3. Segundo Kurose e Ross (2013), somente as folhas da árvore, isto é, os nós das extremidades são os objetos gerenciados. Qualquer objeto representa uma informação capturada do dispositivo, como por exemplo, informações do consumo da rede.

Figura 2.3: Árvore MIB



Fonte: Adaptado de (STALLINGS, 1999).

A hierarquia de uma MIB pode ser compreendida como uma árvore de raiz anônima, possuindo seus galhos distribuídos por diferentes organizações. A camada mais alta das OID

(*Object Identifier*) da MIB é padronizada por diferentes organizações, enquanto a camada mais baixa é alocada em organizações associadas. Essa arquitetura possibilita a gestão em todas as camadas do modelo de referência OSI. Assim as MIBs podem ser estabelecidas para cada área específica de informação e operação, e é possível estender as aplicações e informações monitoradas.

Existem basicamente três tipos de MIB, sendo uma delas chamada de MIB2, a qual foi desenvolvida apenas para gerenciar dispositivos de rede TCP/IP ou que envolvam a rede. Segundo Mauro (2005), a MIB2 é um grupo de gerenciamento importante, por que cada dispositivo com suporte a SNMP também deve aceitar MIB2.

Abaixo da subárvore MIB2 estão os objetos usados para obter informações específicas dos dispositivos da rede. Esses objetos estão divididos em dez grupos, que estão presentes na Tabela 2.1.

Tabela 2.1: Grupos da MIB2

<i>Nome da subárvore</i>	<i>Descrição</i>
system	informações básicas do sistema
interfaces	interfaces de rede
at	tradução de endereços
ip	protocolo ip
icmp	protocolo icmp
tcp	protocolo
udp	protocolo udp
egp	protocolo egp
transmission	meios de transmissão
snmp	protocolo snmp

Fonte: Adaptado de (SILVA, 2005).

3 TRABALHOS RELACIONADOS

Este capítulo apresenta um estudo sobre ferramentas de gerência de redes. Em busca de suporte ao desenvolvimento do trabalho, foram analisados alguns trabalhos nos quais foram utilizados ferramentas de monitoramento e gerenciamento.

O trabalho apresentado por Santos (2016), tem como objetivo analisar os gráficos e relatórios diversos gerados pelas ferramentas, a fim de fazer um comparativo das ferramentas Cacti e Zabbix.

O autor deste trabalho simula um ambiente de monitoramento em que foram utilizadas seis máquinas virtuais, sendo que três dessas máquinas foram utilizada no Cacti e três máquinas foram utilizadas no Zabbix, assim foi realizada a instalação dos *softwares* Cacti e Zabbix. O primeiro passo foi realizar o *download* dos pacotes de instalação pela internet, e o segundo passo foi a instalação e configurações dos *softwares*.

Santos (2016), após a implementação e testes, traz uma comparação dos recursos disponíveis em cada ferramenta, os quais são apresentadas na Tabela 3.1.

Tabela 3.1: Comparação entre recursos disponíveis

Cacti	Zabbix
CPU usage	CPU jumps
CPU utilization	CPU load
Load usage	CPU utilization
Load average	Disk space usage
Logged in users	Memory usage
Memory usage	Network traffic on eth0
Ping Latency	Network traffic on eth2
Traffic (bits/sec)	Swap usage
	Value cache effectiveness
	Zabbix cache usage, % free
	Zabbix data gathering process busy
	Zabbix internal process busy
	Zabbix server performance

Fonte: Adaptado de (SANTOS; MARTINS, 2016).

Na Tabela 3.2, é apresentada uma comparação das funcionalidades disponíveis em cada ferramenta, coletadas durante os testes nas ferramentas Cacti e Zabbix.

Tabela 3.2: Comparação entre funcionalidades disponíveis

Funcionalidade	Cacti	Zabbix
CPU jumps	Não	Sim
CPU load	Sim	Não
CPU usage	Sim	Não
CPU utilization	Sim	Sim
Disk space usage	Não	Sim
Load average	Sim	Não
Load usage	Sim	Não
Logged in users	Sim	Não
Memory usage	Sim	Sim
Network traffic on eth0	Não	Sim
Network traffic on eth2	Não	Sim
Ping Latency	Sim	Não
Swap usage	Não	Sim
Traffic (bits/sec)	Sim	Não
Value cache effectiveness	Não	Sim
Zabbix cache usage, % free	Não	Sim
Zabbix data gathering process busy %	Não	Sim
Zabbix internal process busy %	Não	Sim
Zabbix server performance	Não	Sim

Fonte: Adaptado de (SANTOS; MARTINS, 2016).

Santos (2016), conclui o trabalho descrevendo que as ferramentas implantadas e configuradas comprovam ser eficientes e eficazes aos objetivos apresentados no trabalho. Análise e testes podem ser utilizados por administradores de empresas, universitários e interessados na área de redes de computadores. As informações ajudam na verificação ativas dos dispositivos e componentes, estados das máquinas e configuração do equipamento. Com os resultados obtidos através de análises e testes, o autor conclui que as informações contidas nas ferramentas ajudam a obter uma boa visualização e um melhor desempenho da rede analisada.

O trabalho realizado por Mohr (2012) analisa alguns critérios que são considerados essenciais para uma ferramenta de monitoramento. Neste trabalho foram escolhidas três ferramentas de código aberto, sendo elas Zabbix, Nagios e Zenoss. Esse trabalho também tem como objetivo identificar oportunidades de melhorias nessas ferramentas, pois todas as ferramentas são de códigos aberto.

Outro critério de escolha foi a procura por ferramentas com propósitos levemente dife-

rentes. O Nagios foi escolhido por ser uma ferramenta voltada a usuários mais avançados, por usar muito pouco a interface gráfica e facilitar o desenvolvimento de *plugins*. Já o Zenoss é altamente voltado para a interface gráfica e compatibilidade com *plugins* já existentes. O Zabbix é uma mescla das outras duas, com potencial para ser a mais completa entre as três.

De acordo com Mohr (2012), foram realizadas comparações de uma série de conceitos escolhidos para as ferramentas. O objetivo principal aqui é identificar pontos fracos e pontos fortes de cada uma delas. De forma a simplificar a visualização dos resultados, o autor apresenta um *ranking* da ferramenta com melhor performance em cada um dos resultados, sendo que cada ferramenta foi dada uma nota de 1 a 3, sendo 1 a pior ferramenta para aquele quesito e 3 a melhor ferramenta. A Tabela 3.3, traz o resultado da comparação final entre as ferramentas e todos os critérios avaliados.

Tabela 3.3: Tabela de comparação

	Zabbix	Nagios	Zenoss
Documentação e Disponibilidade	3	2	1
Código Fonte	2	3	1
Fóruns	1	3	2
Suporte	3	2	1
Instalação	2	3	1
Interface com Usuário	3	1	2
Criação de Monitores	3	2	1
Estado dos Monitores	3	2	1
Gráficos de Análise	3	1	2
Relatórios	2	1	3
Usabilidade Geral	1	2	2
Capacidade	1	3	2
Compatibilidade	1	2	2
Alertas	2	3	1
Escalabilidade	3	1	2
Configuração e Personalização	2	1	3

Fonte:(MOHR, 2012).

Observando a Tabela 3.3, é possível identificar que a ferramenta Zabbix se mostrou a mais completa. Essa ferramenta é uma combinação de interface gráfica apropriada com importantes funcionalidades. Em segundo lugar na avaliação fica a ferramenta Nagios. O autor conclui que ela é uma ferramenta adaptável, apesar de exigir um usuário mais avançado que não

precise utilizar tanto a interface gráfica.

O Zenoss ficou na última colocação. Apesar de sua interface gráfica extremamente poderosa, essa ferramenta se mostrou inferior às outras justamente por causa da dificuldade de uso, pois se mostrou extremamente complicado de instalar e configurar.

Mohr (2012), conclui o trabalho falando que durante esse estudo, foi possível observar claramente o foco que cada uma das ferramentas recebeu em seu desenvolvimento. O Nagios foi uma ferramenta que mostrou ser facilmente adaptável e melhorada, por sua facilidade de receber novos *plugins*. Inclusive o desenvolvimento desses *plugins* é bastante facilitado por uma grande comunidade ativa.

O trabalho desenvolvido por Garcia (2012), desenvolveu uma ferramenta para apoiar à gestão da infraestrutura de comunicações do Aeroporto Francisco Sá Carneiro. Para a elaboração desse trabalho, o autor realizou uma comparação entre o NMS (*Network Management System*) *WhatsUp Gold*, *Enterasys NetSight*, *Hp OpenView* e *Nagios*. De modo a ajudar a compreender as principais diferenças entre os *softwares* anteriormente mencionados, podemos nos fundamentar nas informações ilustradas na Tabela 3.4, que o autor apresenta em seu trabalho.

Tabela 3.4: Comparação entre os NMS em análise

<i>Software</i>	<i>Auto - Descoberta</i>	<i>Plugins</i>	<i>Alertas</i>	<i>Licença Livre</i>	<i>Mapas</i>	<i>Mib's Externas</i>	<i>Vários Fabricantes</i>
<i>WhatsUp Gold</i>	V	V	V	X	V	V	V
<i>Enterasys NetSight</i>	V	X	V	X	V	V	V
<i>Hp OpenView</i>	V	V	V	X	V	V	V
<i>Nagios</i>	X	V	V	V	V	V	V

Fonte: Adaptado de (GARCIA, 2012).

O autor do trabalho ressalta que um mesmo *software* possui diferentes versões à disposição do cliente, sendo normalmente a principal diferença entre elas o número de equipamentos a monitorar. No caso do *WhatsUp Gold*, existem várias licenças dentro da mesma versão, dependendo sempre do número de elementos presentes na rede. Na Tabela 3.5, podemos encontrar as principais diferenças entre as três versões disponíveis.

Tabela 3.5: Comparação entre as versão do WhatsUp Gold

Funcionalidades	Standard	Premium	Distributed
WEB UI, Windows Console & Acesso móvel	V	V	V
Centro de alertas	V	V	V
Base de dados SQL integrada	V	V	V
Monitoramento de desempenho	V	V	V
Suporte a Jscript ouVBscript	V	V	V
Monitoramento de rede e criação de gráficos em tempo real	X	V	V
Aplicação de monitoramento WMI	X	V	V
Monitoramento de hardware com recurso a MIBs	X	V	V
Monitoramento de servidores Unix e recursos SSH	X	V	V
Monitoramento dos pontos de rede Wireless (WAP)	X	V	V
Monitores ativos ou passivos já pré-configurados	X	V	V
Transmissão de dados (HTTP/HTTPS/FTP)	X	V	V
Serviços de monitoramento remoto	X	X	V

Fonte: Adaptado de (GARCIA, 2012).

Como podemos analisar através da Tabela 3.5, a versão *Standard* suporta as funcionalidades básicas para qualquer *software* NMS. No entanto, o autor apresenta a principal diferença entre as versões *Premium* e *Distributed*. Nota-se que a versão *Distributed* suporta a possibilidade de monitoramento dos equipamentos remotamente de qualquer ponto, sem necessariamente fazer parte da mesma rede monitorada pelo administrador.

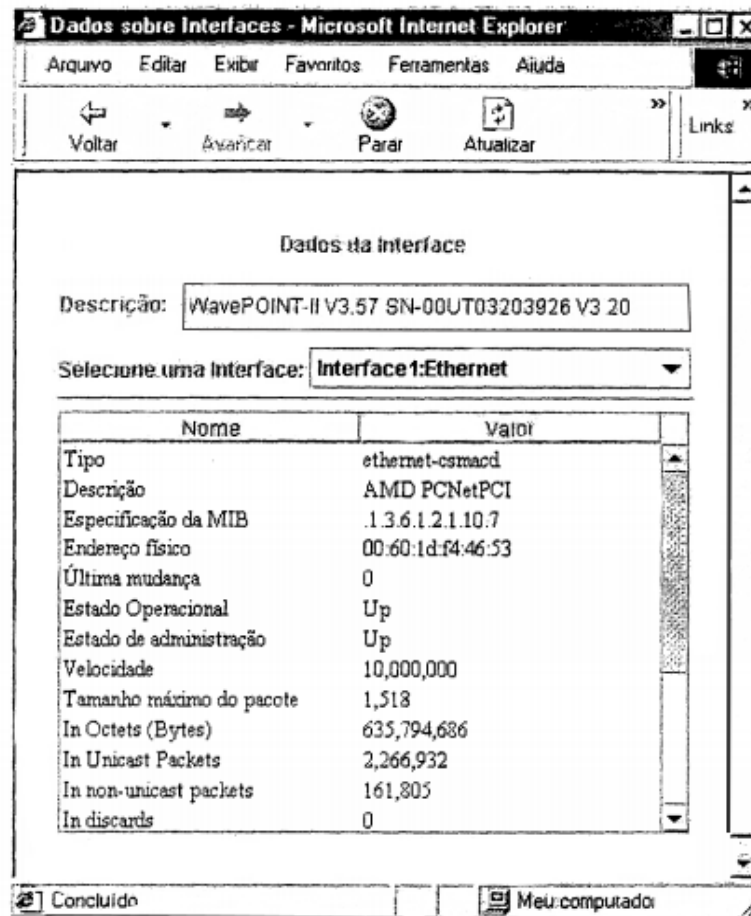
O trabalho desenvolvido por Pisching (2001), apresenta uma análise da possibilidade e a necessidade de implementação de um aplicativo para o monitoramento de redes *Wireless*, aplicadas ao provimento de serviços de internet. Neste trabalho é utilizado o protocolo de gerência SNMP para obtenção de dados sobre as condições da rede, a linguagem de programação Java para o desenvolvimento do aplicativo, e o serviço WEB para permitir a interface com o usuário final.

O autor descreve que o estudo efetuado no ambiente de transmissão sem fio, o elemento *Wireless Bridge* (WavePOINT-II) foi pesquisado, e neste foi identificado o suporte a gerência de redes via SNMP. Segundo Pisching (2001), este equipamento é o principal elemento para a comunicação sem fio, o qual faz a ligação entre a base de transmissão e as estações remotas no cenário de seu trabalho. O autor percebe neste equipamento a necessidade de monitoramento a fim de permitir controlar o seu funcionamento.

As interfaces desenvolvidas neste trabalho estão divididas em módulos, e cada um de-

les possui um objetivo específico. As interfaces desenvolvidas permitem este monitoramento, através da WEB, como mostra a Figura 3.1, a qual apresenta informações sobre as interfaces de rede.

Figura 3.1: Tela do módulo Dados sobre as Interfaces



Fonte: (PISCHING, 2001).

As interfaces desenvolvidas neste trabalho permitem o monitoramento através da WEB, como foi apresentado na Figura 3.1, que demonstra a interface do módulo “*Dados sobre Interface*”, a qual apresenta ao administrador as informações sobre as interfaces da entidade gerenciada. Como pode-se observar, são listadas as interfaces identificadas, e, quando uma delas é selecionada em particular, são apresentadas diversas informações coletadas sobre a interface.

Outra funcionalidade desta ferramenta é o módulo “*Dados da tabela IP ARP*”, con-

forme mostra a Figura 3.2, a qual apresenta uma simples tabela que segundo o autor, onde cada linha corresponde a uma interface física do sistema. As informações em cada linha fornecem um mapeamento do endereço de rede para endereço físico.

Figura 3.2: Tela do módulo Dados da tabela IP ARP

Dados TCP/UDP - Microsoft Internet Explorer

Arquivo Editar Exibir Favoritos Ferramentas Ajuda

Voltar Avançar Parar Atualizar Página inicial Pesquisar Links

Tabela IP ARP

Interface	End Físico	Endereço IP	Media Type
2	00:e0:2d:83:9e:52	192.168.2.1	dynamic(3)

Fonte: (PISCHING, 2001).

Conforme Pisching (2001), com os valores coletados e apresentados através das interfaces implementadas, o autor chegou à conclusão de que o administrador de uma rede sem fio pode tomar decisões sobre seus equipamentos *Wireless*, quando estes apresentarem algum resultado inadequado.

No trabalho proposto por Santos (2011), é apresentado um *software* de monitoramento para roteadores *Wireless*, onde o mesmo utiliza-se do protocolo SNMP para realizar a comu-

nicação com roteadores que tenham o *firmware DD-WRT* ou *OpenWrt*. Se os roteadores da rede a ser monitorada tenham o *firmware DD-WRT* ou *OpenWrt* e possua o serviço de SNMP habilitado, a ferramenta desenvolvida pode se conectar a estes equipamentos e ler informações como taxa de utilização de uma determinada interface, endereço MAC (*Media Access Control*) das interfaces, quantidade de usuários conectados a este roteador, entre outras.

Através das informações obtidas nesta ferramenta o administrador da rede pode identificar, por exemplo, qual ponto de acesso está sendo mais utilizado e se este ponto está sobrecarregado. As informações apresentadas na ferramenta são distribuídas na tela em três seções, sendo uma com informações do roteador, outra com informações das interfaces do roteador, sendo possível navegar pelas interfaces e por fim uma seção com informações dos clientes *Wireless* conectados, também com possibilidade de escolher de qual cliente se deseja mostrar as informações, como mostra a Figura 3.3.

Figura 3.3: Tela do *software* de monitoramento



Fonte: (SANTOS, 2011).

A ferramenta de monitoramento foi elaborada em linguagem de programação C++. Para o seu desenvolvimento foi usada uma versão *Trial* do Borland C++ Builder. O Borland C++

Builder dispõe uma série de componentes para as mais diversas finalidades. Para a comunicação SNMP com os roteadores foi usado o componente TidSNMP para deixar transparente ao programador toda a troca de mensagens do protocolo até que se consiga executar uma operação SNMP.

O autor do trabalho afirma que o *software* precisa de melhorias para se tornar um sistema de larga utilização, porém o que foi implementado até então prova que este sistema como um todo pode ser muito útil.

Existem diversas ferramentas de acordo com os trabalhos relacionados, como vemos os trabalhos de Santos (2016), Mohr (2012) e Garcia (2012) apresentam comparações entre ferramentas já conhecidas. A comparação dessas ferramentas mostram que algumas possuem funcionalidades conforme o tipo de licença, também podemos notar que algumas ferramentas não possui suporte a monitoramento de rede sem fio. Já os trabalhos apresentados por Pisching (2001) e Santos (2011), são ferramentas desenvolvidas para o monitoramento voltado para redes sem fio. Porém as ferramentas desenvolvidas, não possuem gráficos compreensíveis de informações da rede sem fio.

Os trabalhos apresentados, possuem em comum a intenção de apoiar e incentivar a utilização de ferramentas de gerenciamento e monitoramento de redes. Por este motivo, este trabalho apresenta a ferramenta CTIWifi, a qual irá auxiliar o monitoramento de redes *Wireless*.

4 CTIWIFI - FERRAMENTA PARA MONITORAMENTO DE REDES SEM FIO

O presente capítulo apresenta o processo de desenvolvimento da ferramenta para monitoramento de redes sem fio, a qual auxilia o administrador de rede na análise do comportamento da rede sem fio. A fim de possibilitar um melhor entendimento sobre os assuntos abordados, a Seção 4.1 apresenta uma breve introdução das tecnologias utilizadas para o desenvolvimento da aplicação; na Seção 4.2 é apresentado o desenvolvimento da aplicação, sendo ela divididas em módulo de controle, banco de dados e interfaces que são apresentadas nas Subseção 4.2.1, 4.2.2 e 4.2.3.

4.1 MATERIAIS UTILIZADOS NO DESENVOLVIMENTO

Esta Seção tem o intuito de apresentar uma introdução sobre as tecnologias utilizadas para o desenvolvimento do presente trabalho, tendo em vista auxiliar no entendimento.

4.1.1 PHP

O PHP é uma linguagem de *script*, utilizada no *back-end*⁸ para o desenvolvimento de aplicações presentes e atuantes no lado do servidor, capazes de gerar conteúdo dinâmico na WEB. Segundo Dall (2015), essa linguagem foi desenvolvida em 1994 por Rasmus Lerdorf. Atualmente encontra-se na versão 7.0.13 lançada em 10 de novembro de 2016⁹.

O PHP foi inicialmente desenvolvido como uma linguagem de *script* estruturada, mas com o decorrer do tempo novos recursos foram sendo acrescentados com o intuito de torná-lo uma linguagem orientada a objetos. De acordo com Dall (2015), a orientação a objetos é um paradigma que representa toda uma filosofia para construção de sistemas. Por tanto, a partir da versão 4 da linguagem, existe a possibilidade de se utilizar classes e objetos.

O PHP tem como uma das suas características o suporte a bancos de dados, como MySQL¹⁰, Oracle¹¹, PostgreSQL¹² entre outros. Além disso, tem suporte a serviços através de protocolos como IMAP (*Internet Message Access Protocol*), SNMP, POP3 (*Post Office Pro-*

⁸ Back-end é a parte que fica por trás da interface, aonde fica a lógica e são implementadas as rotinas, regras de negócio, validação, interação com o banco de dados e etc.

⁹ <https://secure.php.net/downloads.php>

¹⁰ MySQL é um banco de dados relacional de código aberto que foi desenvolvido pela empresa sueca MySQL.

¹¹ Oracle é um banco de dados relacional oferecido atualmente pela Oracle Corporation.

¹² PostgreSQL é um banco de dados objeto relacional desenvolvido na Universidade da Califórnia em Berkeley.

tocol) entre outros.

4.1.2 Banco de dados MySQL

Um sistema de banco de dados é uma maneira de guardar dados, para que posteriormente informações possam ser recuperadas e utilizadas conforme a necessidade. Sendo assim, pode-se definir banco de dados como uma coleção de dados, representando algum tipo de informação.

O SGBD (*Sistema Gerenciador de Banco de Dados*) é um *software* que contém recursos capaz de utilizar as informações do banco de dados e interagir com o usuário. Segundo Date (2004), o primeiro SGBD comercial surgiu no final de 1960.

O MySQL é um SGBD *open source*, que utiliza a linguagem SQL (*Structured Query Language*). Segundo Suehring (2002), a linguagem SQL foi desenvolvida na década de 80 por David Axmark, Allan Larsson e Michael Monty Widenius, e nos dias de hoje é amplamente utilizada.

4.1.3 JavaScript

JavaScript é uma linguagem de programação interpretada disponível nos navegadores de internet. A linguagem JavaScript oferece uma série de recursos, possibilitando assim o desenvolvimento WEB *front-end*¹³.

A linguagem JavaScript foi desenvolvida em 1995 por Brendan Eichpermite. A linguagem permite modificar e integrar, de forma dinâmica, o conteúdo e a aparência dos vários elementos que compõem o documento.

4.1.4 Chart.js

A biblioteca Chart.js é uma biblioteca em JavaScript que auxilia na criação de gráficos utilizando apenas HTML (*Hypertext Markup Language*), CSS (*Cascading Style Sheets*) e JavaScript para renderizar os gráficos utilizando o elemento do *Canvas* do HTML5. De acordo com Neto (2013), essa biblioteca é extremamente leve e não possui dependências. Essa biblioteca possui tipos diferentes para gráficos, como mostra a Figura 4.1, entre os tradicionais como barra e *pizza*, além de possuir suporte responsivo.

¹³ Front-end é a parte responsável da visualização para o usuário na camada final que é exibido no navegador como interfaces, layouts, cores, etc.

Figura 4.1: Gráficos biblioteca Chart.js



Fonte: (NETO, 2013).

A Figura 4.1 apresenta o gráfico de linhas que exibe informações como uma série de pontos ligados por uma linha, ele é aplicado para a visualização de dados sob intervalos de tempo. O gráfico de barras podem ser plotadas verticalmente ou horizontalmente, e possuem tamanhos proporcionais aos valores que representam. No gráfico de radar serve para comparar valores agregados de várias séries de dados. O gráfico polar exibe uma sequência como um conjunto de pontos reunidos por categoria em um círculo de 360 graus, tendo seus valores representados pelo comprimento do ponto. No gráfico de pizza os dados de valor são exibidos como porcentagem de um todo e as categorias são representadas por fatias individuais. O gráfico de rosca é semelhante ao gráfico de pizza, mas pode conter mais de uma sequência.

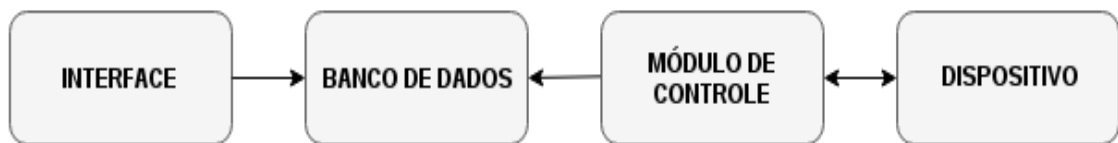
4.1.5 Apache

O Apache é um servidor WEB popular e teve sua primeira versão desenvolvida em 1995 por Rob McCool, sendo multiplataforma. O Apache encontra-se na versão 2.4.17 lançada no dia 13 de outubro de 2015, que através de módulos é capaz de executar código em PHP, Perl, Shell Script e até em ASP (*Active Server Pages*).

4.2 MÉTODO DE DESENVOLVIMENTO

O funcionamento da aplicação é apresentando em blocos ligados entre si que representam, por sua vez, os módulos da arquitetura funcional da aplicação e a transferência da informação por ela tratada, como mostra a Figura 4.2.

Figura 4.2: Diagrama Funcional



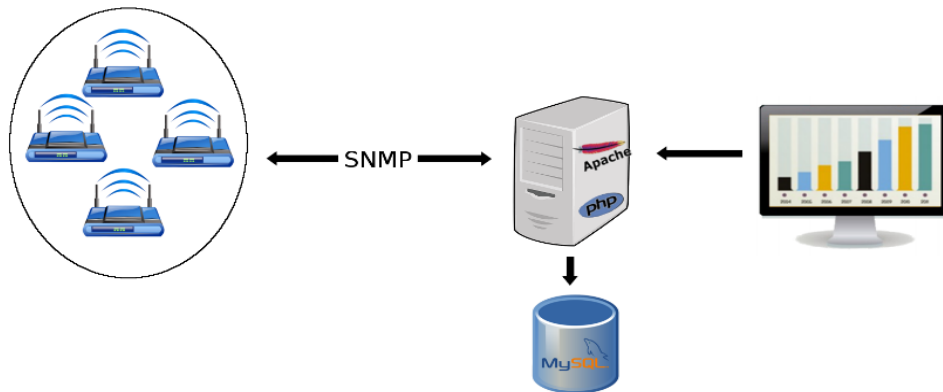
Fonte: Acervo pessoal.

Em termos gerais, podemos descrever os módulos da seguinte forma:

- **Interface:** Representação gráfica da informação manipulada pela aplicação e que permite a utilização desta por parte do utilizador, nela foram utilizadas as linguagens JavaScript, HTML5 e CSS.
- **Banco de Dados:** Responsável por guardar a informação e retorná-la quando solicitada por parte da interface.
- **Módulo de Controle:** Responsável por executar as ações de obtenção da informação do dispositivo e tratar para posteriormente ser armazenada. Neste módulo foi utilizado a linguagem de programação PHP.
- **Dispositivos:** Elementos da rede a serem monitorados pela aplicação.

No que diz respeito à arquitetura na qual se dispõe o funcionamento da aplicação, está pode ser ilustrada pela Figura 4.3. Como se pode verificar, os dispositivos monitorados estão ligados através da rede, onde se executam os módulos de controle e armazenamento. A informação recolhida e tratada, enviada e armazenadas em uma base de dados no servidor, onde todos os pedidos de dados são solicitados pela interface, através do servidor WEB.

Figura 4.3: Arquitetura da Aplicação



Fonte: Acervo pessoal.

4.2.1 Módulo de Controle

Para realização da tarefa de coletar e armazenar as informações dos *Access Points*, foi criada uma classe denominada *MostraConectados* que possui dois métodos, sendo eles chamados de *conectadosShow* e *salvaConectados*, como mostra a Figura 4.4. Esses métodos serão responsáveis por realizar busca e armazenamento das informações.

Figura 4.4: Classe MostraConectados



Fonte: Acervo pessoal.

O método *conectadosShow*, que é responsável por realizar a busca das informações, recebe como entrada uma lista contendo os endereços IP's dos roteadores sem fio. Logo após é

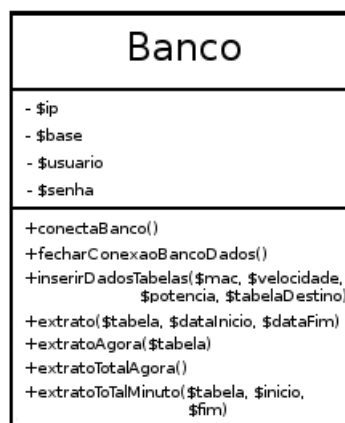
percorrido todos os equipamentos e são consultados os sensores relevantes em busca de informação da quantidade de usuários conectados, bem como velocidade e potência. Após coletar as informações, é realizado o processo de tratamento e depois enviado para armazenamento no banco de dados.

Para realizar o armazenamento das informações, após receber o devido tratamento é executado o outro método existente nessa classe chamado de *salvaConectados*. Esse método recebe a informação de qual a tabela do banco de dados deve ser armazenada, e com o auxílio de outro método pertencente a classe *banco* é executada a tarefa de armazenamento das informações, para uso futuro.

4.2.2 Classe Banco

Para realizar o armazenamento dos dados coletados, bem como recuperá-los, foi desenvolvida uma classe que é responsável por manipular o banco de dados. A classe *Banco*, possui métodos para realizar conexão com o banco, inserção, consulta, através de uma consulta *SQL* e método para finalizar a conexão, como mostra a Figura 4.5. Esta classe possui alguns atributos, as quais contém informação sobre o endereço do banco de dados, bem como a base de dados e informações para autenticação.

Figura 4.5: Classe Banco

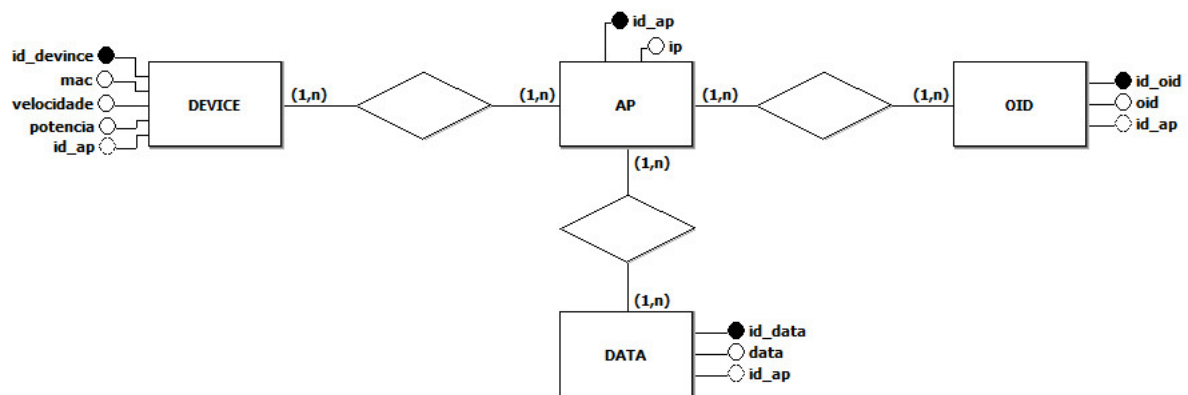


Fonte: Acervo pessoal.

O método *conectaBanco* é o responsável por estabelecer a conexão com o banco de

dados. Esse método é utilizado quando ocorre alguma forma de manipulação das tabelas do banco de dados apresentada na Figura 4.6. O método *inserirDadosTabelas* é utilizado para realizar a tarefa de salvar os dados tratados na classe *MostraConectados*. Para inserir os dados na tabela *DEVICE*, o método recebe como parâmetros, as informações como MAC, velocidade, potência.

Figura 4.6: Modelo ER do banco



Fonte: Acervo pessoal.

Para realizar a busca das informações existentes no banco de dados, são utilizados os métodos *extrato*, *extratoAgora*, *extratoTotalAgora*. Estes métodos realizam a busca das informações desejadas, conforme o gráfico que se deseja. O método *extrato* é utilizado para buscar no banco de dados a quantidade de dispositivos conectados, e esse método necessita que seja passado argumentos para ele, informando em qual tabela fará a busca e o período de início e fim.

Para saber a quantidade de dispositivos conectados atualmente em um *Access Point*, é necessário a utilização do método *extratoAgora*. Esse método é informado em qual tabela devesse realizar a busca da quantidade de dispositivos que estejam conectados, sendo assim, trazendo a informação da quantidade de dispositivos conectados em um determinado *Access Point*. Para saber a quantidade de dispositivos conectados por minuto, é utilizado o método *extratoTotalMinuto*, o qual possibilita ter um conhecimento da quantidade máxima por minuto conectado.

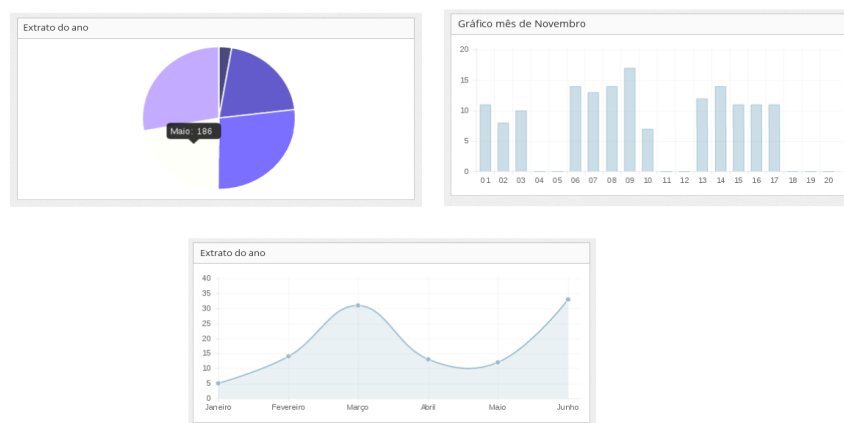
Para que seja possível informar a quantidade de dispositivos conectados em toda a rede, é utilizado o método *extratoTotalAgora*. Esse método tem a função de fazer uma busca no banco de dados da quantidade total dos dispositivos conectados, ou seja, fará uma pesquisa em todas as tabelas e retornará um somatório dos resultados obtidos.

4.2.3 Interface

A interface gráfica é quem permite mostrar ao administrador da rede as informações coletadas. Para essa etapa foi desenvolvido arquivos com a estrutura de uma página HTML5 necessários para a criação dos gráficos de forma a ser genéricos, ou seja, de forma que possam se adaptar conforme as informações coletadas do banco de dados. Neste módulo foi usado a biblioteca Chart.JS, que permite a visualização de dados através de gráficos diversos e interativos. A biblioteca utiliza elemento *canvas* do HTML5 para desenhar esses gráficos em uma página WEB.

Para gerar os gráficos, é realizado o acesso a classe *Banco* e seus métodos. Através da chamada desses métodos, o *script* contido no arquivo que gera os gráficos realiza uma consulta na tabela que foi passada. Após a consulta é gerado o gráfico e exibido na tela, como mostra a Figura 4.7.

Figura 4.7: Gráficos da Interface



Fonte: Acervo pessoal.

Os gráficos exibem a quantidade de dispositivos conectados nos *Access Point*, a Figura

4.7 apresenta os gráficos de pizza e linha, os quais exibem a quantidade de dispositivos por ano que acessam a rede *Wireless*. Outro gráfico apresentado na figura é o gráfico de barra, o qual mostra a quantidade de dispositivos que conectaram durante o mês de novembro.

5 EXPERIMENTOS E RESULTADOS

Para realizar o teste da ferramenta *CTIWifi*, foi monitorada a rede *Wireless* disponibilizada pelo Colégio Técnico Industrial de Santa Maria, onde a ferramenta foi inserida em uma máquina virtual do VMS (sistema de máquina virtuais), disponibilizada pela instituição. Este sistema busca auxiliar no ensino das diversas disciplinas ministradas neste ambiente estudantil, buscando auxiliar nas atividades empregadas. Essa máquina virtual possui o sistema operacional Ubuntu 12.04.1 LTS (*Long Term Support*), onde foi instalado um servidor WEB Apache, o qual foi hospedada as páginas PHP desenvolvidas.

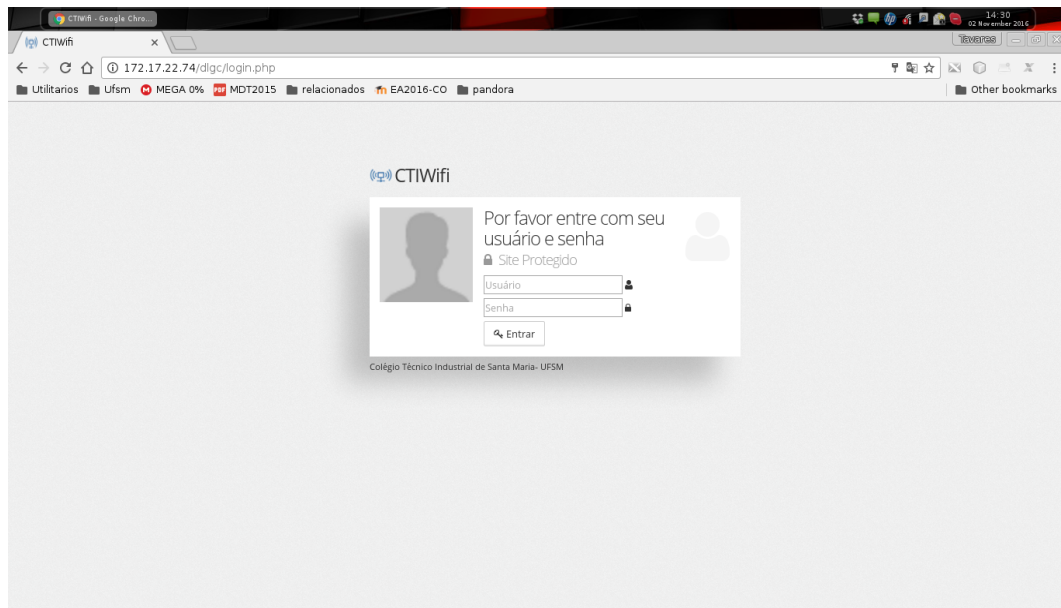
Figura 5.1: Tela do Sistema de Máquina Virtual



Fonte: Acervo pessoal.

No momento em que tentamos acessar o endereço da ferramenta através de um navegador de internet, surge a página de início de sessão solicitando um usuário e senha válidos para acesso a ferramenta, como mostra a Figura 5.2. Será necessário informar as credenciais de acesso para poder utilizar a aplicação, essas credenciais serão verificadas encontram-se presente no banco de dados.

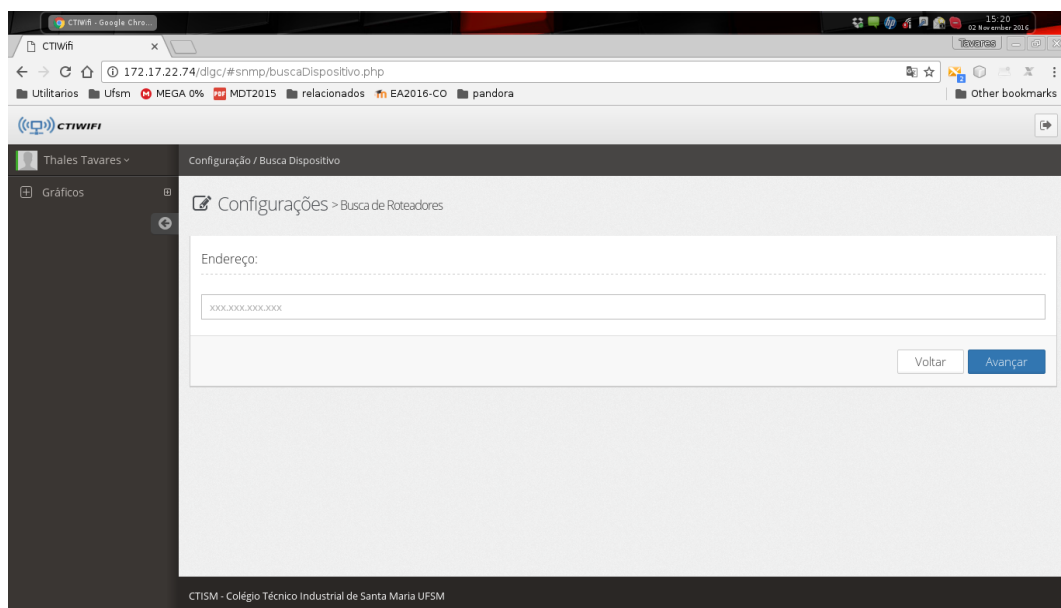
Figura 5.2: Tela de Login da Aplicação



Fonte: Acervo pessoal.

Após se autenticar-se na ferramenta, pode ser realizada a busca dos *Access Point* que serão monitorados pela ferramenta, como mostra a Figura 5.3. Para realizar a busca do dispositivos, foi informado a faixa de endereço IP dos dispositivo.

Figura 5.3: Tela de Busca de Dispositivos



Fonte: Acervo pessoal.

Será necessário informar a versão do protocolo SNMP que está sendo utilizado nos dispositivos, como mostra a Figura 5.4. No caso da rede *Wireless* do Colégio Técnico Industrial de Santa Maria, foi selecionado a segunda versão do protocolo SNMP e informado a *string* de comunidade *public*, a qual é utilizada nos dispositivos da rede.

Figura 5.4: Tela de Seleção do Protocolo

Fonte: Acervo pessoal.

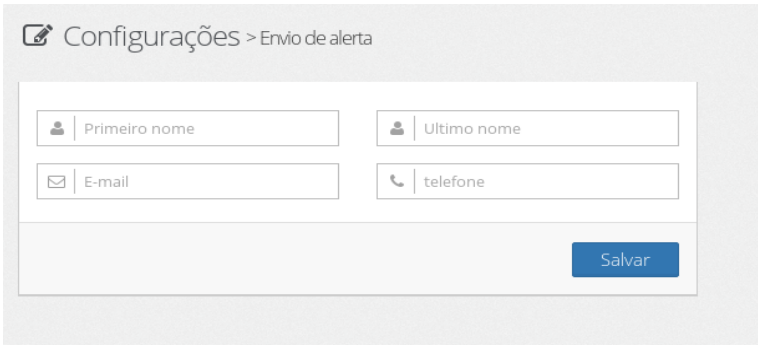
Logo após ser realizada a busca dos *Access Point* a serem monitorados, é retornado uma tela com os dispositivos encontrados dentro da faixa de endereço IP informada anteriormente, conforme a Figura 5.5. A tela apresentada informações o nome cadastrado no dispositivo, endereço IP, local cadastrado no dispositivo e o fabricante.

Figura 5.5: Tela de Dispositivos Encontrados

Fonte: Acervo pessoal.

O administrador da rede deve selecionar os dispositivos que serão monitorados. Isso permite evitar que a ferramenta insira algum dispositivo desnecessário. Logo após selecionar os dispositivos, o administrador deve informar qual a quantidade total de dispositivos conectados em cada *Access Point*, sendo que essas informações serão armazenadas no banco de dados. O próximo passo é configurar o *e-mail* que receberá as notificações de alertas, como mostra a Figura 5.6.

Figura 5.6: Tela de Configuração de *e-mail* para Alerta

A imagem mostra a interface de configuração de e-mail para alertas. No topo, há uma barra de título com o ícone de uma caneta e o texto "Configurações > Envio de alerta". Abaixo, há um formulário com quatro campos de entrada: "Primeiro nome", "Último nome", "E-mail" (com ícone de envelope) e "telefone" (com ícone de telefone). Um botão azul com o texto "Salvar" está localizado no canto inferior direito do formulário.

Fonte: Acervo pessoal.

Ao terminar as configurações, a ferramenta constrói um menu na parte lateral onde se apresentam os equipamentos monitorados na rede, como mostra a Figura 5.7. Esse menu é montado pela ferramenta a partir das informações que foram armazenadas no banco de dados anteriormente, quando foi realizado a busca dos dispositivos.

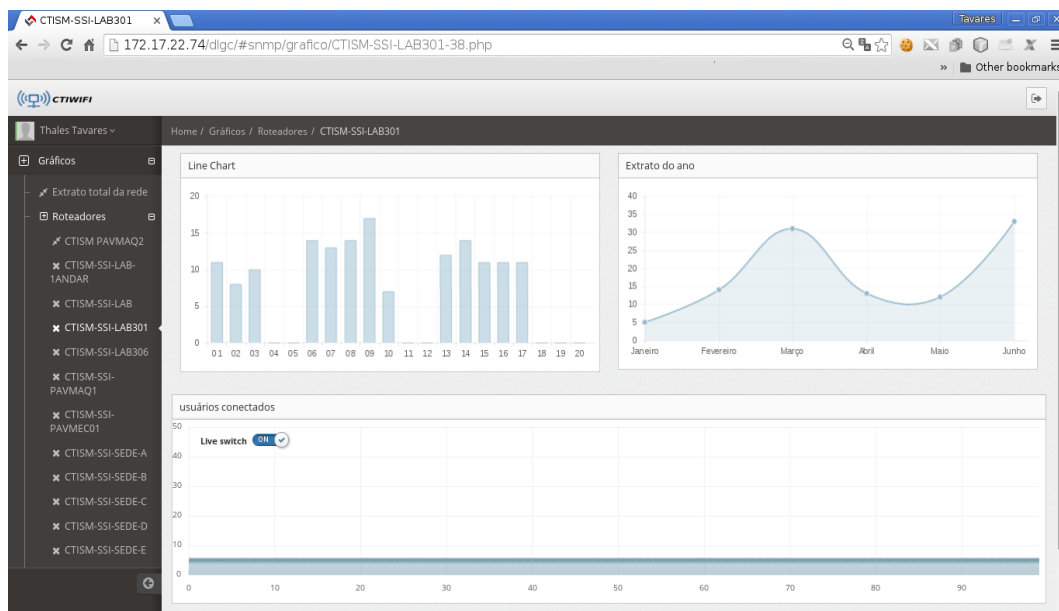
Figura 5.7: Menu Aplicação



Fonte: Acervo pessoal.

Com a ferramenta configurada, os gráficos da quantidade de usuário conectados na rede sem fio começa a ser gerados pela aplicação. Os gráficos exibem informações sobre a quantidade de dispositivos conectado durante os dias do mês corrente, um gráfico mostrando o histórico do ano corrente, como mostra a Figura 5.8. O gráfico que fica abaixo dos citados anteriormente é um gráfico que mostra a quantidade de dispositivos conectados naquele *Access Point*, sendo atualizado constantemente. Através do menu que encontra-se na lateral da interface, tem-se a possibilidade de escolher qual *Access Point* deseja exibir os gráficos.

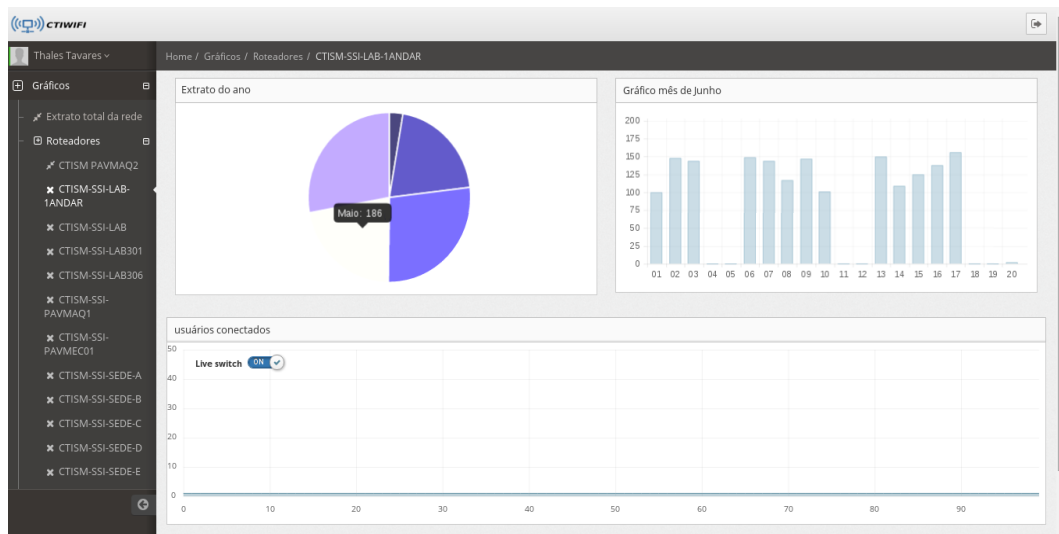
Figura 5.8: Gráficos referente ao *Access Point* CTISM-SSI-LAB301



Fonte: Acervo pessoal.

Os gráficos exibidos na figura acima referem-se aos dispositivos que conectaram no *Access Point* CTISM-SSI-LAB301. Para cada *Access Point* é gerado um modo de visualização diferente ou desejado, isso fica a cargo do administrador da rede e da ferramenta, como mostra a Figura 5.9, que exibe as informações do *Access Point* CTISM-SSI-LAB-1ANDAR. A ferramenta *CTIWifi* permite, além de uma visualização segmentada, o gráfico que mostra a quantidade de dispositivos totais conectados. Este gráfico possui atualizações constantes, buscando ter uma precisão exata da quantidade de dispositivos conectados.

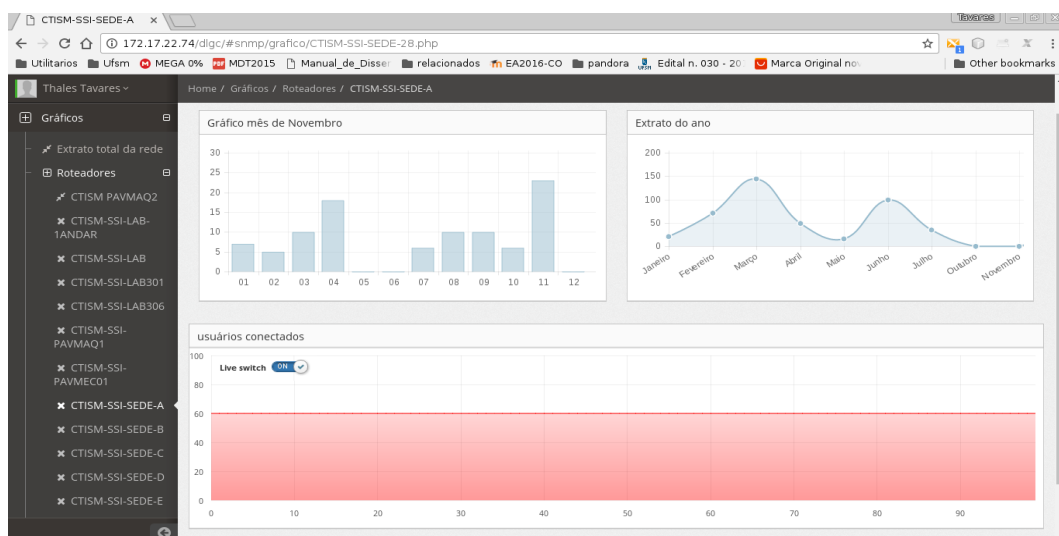
Figura 5.9: Gráficos referente ao *Access Point* CTISM-SSI-LAB-1ANDAR



Fonte: Acervo pessoal.

Quando a quantidade de usuário conectados em um *Acess Point* está acima do configurado, o gráfico de usuário conectados troca sua cor para vermelho. Vemos na Figura 5.10, que a troca da cor do gráfico é para mostrar ao administrador de rede que o *Access Point* CTISM-SSI-SEDE-A esta com a quantidade de usuários conectados acima do configurado.

Figura 5.10: Gráficos referente ao *Access Point* CTISM-SSI-SEDE-A



Fonte: Acervo pessoal.

O gráfico altera sua cor para vermelho quando ultrapassa a quantidade de usuário conectados. Quando isso ocorre, é enviado um *e-mail* de alerta para o endereço de contato configurado anteriormente na ferramenta. Essa medida é tomada para que tenha uma garantia maior que o administrador da rede seja informado do ocorrido, para que não seja preciso estar em frente a ferramenta durante todo o tempo.

6 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

O gerenciamento de redes de computadores é uma área que requer trabalho e dedicação, tanto para visão acadêmica como empresarial. Devido a sua grande granularidade, essa área é composta vários protocolos, inúmeras maneiras de se monitorar dispositivos, vários serviços e *softwares* que podem auxiliar o administrador de redes.

Com o crescimento das redes de computadores sem fio, um sistema de gerenciamento de redes torna-se cada vez mais indispensável. Possuir as informações corretas, possibilita aos administradores de rede tomar decisões coerente e em tempo hábil, minimizando assim indisponibilidade de equipamentos ou serviço.

A proposta apresentada neste trabalho demonstrou resultados satisfatórios, considerando que atendeu ao objetivo proposto. Através da implementação da ferramenta de monitoramento, constatou-se que a solução proposta é viável e que sua utilização pode auxiliar os administradores de redes.

Com as informações coletadas e apresentadas através da ferramenta desenvolvida, chega-se à conclusão que a utilização da mesma pode dar ao administrador da rede informações importantes. Com essas informações, o administrador pode tomar decisões sobre seus equipamentos *Wireless* quando estes apresentarem algum resultado inadequado. Estas decisões poderão ser tomadas, através da análise dos dados referentes a quantidade de dispositivos presentes na rede, locais em que estão. Sendo assim, o administrador pode realizar uma ação proativa, como por exemplo, aumento de capacidade ou área de cobertura em determinados pontos da rede. Essas decisões que serão tomadas, serão com base nas informações apresentadas pela ferramenta.

Como proposta de trabalhos futuro poderá ser implementadas novas funcionalidades, como por exemplo, descoberta automática de novos *Access Point* através da verificação de rede. Sendo que hoje a busca de dispositivos é realizada manualmente no momento da configuração da ferramenta. Outra sugestão é integração da ferramenta com o servidor de autenticação RADIUS, para que seja possível identificar os usuários conectados por *Access Point*. Também será melhorado o aspecto da escolha do protocolo SNMP, o qual será realizada a descoberta automática da versão protocolo utilizada pelo dispositivo.

6.1 TRABALHOS PUBLICADOS

Durante o desenvolvimento dessa monografia, foram publicados artigos nos eventos da 14ª Escola Regional de Redes de Computadores, VIII Congresso Sul Brasileiro de Computação, 31ª Jornada Acadêmica e VII Encontro Anual de Tecnologia da Informação. É importante ressaltar que essa monografia foi desenvolvida como parte do trabalho de um grupo de pesquisa, coordenado pelo Professor Renato Preigschadt de Azevedo.

Abaixo, seguem as referências, contendo os autores e o evento no qual os artigos foram publicados:

- TAVARES, T. N.; FISCHER, I. A. ; AZEVEDO, R. P. . CTIWIFI - Sistema de monitoramento para redes sem fio. In: 14ª Escola Regional de Redes de Computadores, 2016, Porto Alegre - RS. Escola Regional de Redes de Computadores, 2016. v. 14. p. 139-146.
- FISCHER, I. A. ; TAVARES, T. N. ; AZEVEDO, R. P. . Desenvolvimento de uma solução para redes sem fio por intermédio de um controlador central. In: VIII Congresso Sul Brasileiro de Computação, 2016, Criciúma-SC. Congresso Sul Brasileiro de Computação, 2016. v. 8.
- TAVARES, T. N.; FISCHER, I. A. ; PREUSS, J. O. ; AZEVEDO, R. P. . Ferramenta para monitoramento de redes wifi. In: 31ª Jornada Acadêmica Integrada - UFSM, 2016, Santa Maria - RS. 31ª Jornada Acadêmica Integrada - UFSM, 2016.
- TAVARES, T. N.; FISCHER, I. A. ; DUARTE, F. ; AZEVEDO, R. P. . Desenvolvimento de uma ferramenta para monitoramento de dispositivos em rede sem fio. In: VII Encontro Anual de Tecnologia da Informação - EATI, 2016, Frederico Westphalen - RS. Encontro Anual de Tecnologia da Informação - EATI, 2016. v. 7. p. 171-176.

REFERÊNCIAS

- AMARO, M. S. **Gerenciando Redes e Servidores com Nagios**. Campinas, SP: Universidade de Pernambuco, 2010.
- DALL’OGLIO, P. **PHP Programando com Orientação a Objetos 3ª Edição**. 3 ed..ed. [S.l.]: Novatec Editora, 2015.
- DATE, C. **Introdução a sistemas de bancos de dados**. [S.l.]: Campus, 2004.
- DIAS, H. d. L. **A importância do monitoramento de ativos de redes**: um estudo de caso com o sistema cacic. Recife, PE: Universidade de Pernambuco, 2008.
- GARCIA, J. N. **Aplicação para gestão de activos de rede do aeroporto de Porto**. Porto, PT: Instituto Superior de Engenharia do Porto, 2012.
- KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet**: uma abordagem top-down. Trad. 5 ed..ed. São Paulo, SP: Pearson, 2010.
- KUROSE, J. F.; ROSS, K. W. **Computer networking**: a top-down approach. always learning. 6 ed..ed. [S.l.]: Pearson, 2013.
- MAURO, D.; SCHMIDT, K. **Essential SNMP**. 2.ed. [S.l.]: O’Reilly Media, 2005.
- MOHR, R. F. **Análise de Ferramentas de Monitoração de Código Aberto**. Porto Alegre, RS: Universidade Federal do Rio Grande do Sul, 2012.
- NETO, O. P. M. **Análise de bibliotecas para geração de gráficos na web**. Porto Alegre, RS: Universidade Federal do Rio Grande do Sul, 2013.
- OESTERREICH, O. **Um estudo sobre as técnicas para monitoramento de redes de computadores utilizando a ferramenta Nagios**. Santiago, RS: Universidade Regional Integrada do Alto Uruguai e das Missões, 2012.
- PISCHING, M. A. **Uma aplicação Java-SNMP para Monitoramento de Redes Sem Fio**. Florianópolis, SC: Universidade Federal de Santa Catarina, 2001.
- PÉRICAS, F. **Redes De Computadores**: conselhos e a arquitetura internet. 1.ed. [S.l.]: EDI-FURB, 2003.

SANTOS, C. J. M. d. **Sistema de monitoramento para redes sem fio**. Curitiba, PR: Universidade Tecnológica Federal do Paraná, 2011.

SANTOS, L. N. dos; MARTINS, H. P. Comparativo das funcionalidades das ferramentas open-source Zabbix e Cacti. **Caderno de Estudos Tecnológicos**, [S.l.], v.4, n.1, 2016.

SANTOS, M. T. **Gerência de Redes de Computadores**. 2.ed. Rio de Janeiro, RJ: RNP/ESR, 2015.

SILVA, J. M. A. d. **Construção de Agentes SNMP em Ambientes Linux**. Lavras, MG: Universidade Federal de Lavras, 2005.

STALLINGS, W. **SNMP, SNMPv2, SNMPv3, and RMON 1 and 2**. 3.ed. [S.l.]: Addison-Wesley, 1999.

SUEHRING, S. **MYSQL - A BÍBLIA**. [S.l.]: CAMPUS, 2002.