CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS
CAMPUS TIMÓTEO

Lorena Campos Rocio

ANÁLISE DAS ÁREAS DE GERENCIAMENTO DE REDES NECESSÁRIAS EM UM AMBIENTE CORPORATIVO: UM ESTUDO DE CASO SOBRE A DETECÇÃO DE INCIDENTES

Timóteo

2018

Lorena Campos Rocio

ANÁLISE DAS ÁREAS DE GERENCIAMENTO DE REDES NECESSÁRIAS EM UM AMBIENTE CORPORATIVO: UM ESTUDO DE CASO SOBRE A DETECÇÃO DE INCIDENTES

Monografia apresentada à Coordenação de Engenharia de Computação do Campus Timóteo do Centro Federal de Educação Tecnológica de Minas Gerais para obtenção do grau de Bacharel em Engenharia de Computação.

Orientador: Prof.Me.Adilson Mendes Ricardo

Timóteo

2018

Lorena Campos Rocio

ANÁLISE DAS ÁREAS DE GERENCIAMENTO DE REDE NECESSÁRIAS EM UM AMBIENTE CORPORATIVO: UM ESTUDO DE CASO SOBRE A DETECÇÃO DE INCIDENTES.

Trabalho de Conclusão de Curso apresentado ao Curso de Engenharia de Computação do Centro Federal de Educação Tecnológica de Minas Gerais, campus Timóteo, como requisito parcial para obtenção do título de Engenheiro de Computação.

Trabalho aprovado. Timóteo, 06 de Dezembro de 2018:

Prof. Me. Adilson Mendes Ricardo
Orientador

Prof. Dr. Elder de Oliveira Rodrigues
Professor Convidado

Prof. Me. Talles Quintão Pessoa
Professor Convidado

Timóteo
2018

Agradecimentos

Agradeço primeiramente a Deus por ter me dado força para superar as dificuldades.

Agradeço aos pais e irmãos pela paciência, compreensão e por incentivarem sempre a continuar neste caminho.

Agradeço ao orientador que sempre esteve disponível a auxiliar e guiar este trabalho para chegar até onde chegou.

Resumo

As redes de computadores estão cada vez mais presentes em empresas de grande, médio e pequeno porte. Para o bom desempenho e continuidade da empresa é fundamental um bom funcionamento da rede, e, para isso, o gerenciamento da mesma é fator extremamente relevante. Este trabalho de pesquisa tem como objetivo oferecer auxílio adequado à equipe de manutenção e suporte dos recursos de rede, propondo implementar sistemas automatizados de gerenciamento de recursos computacionais em um ambiente corporativo, detectando incidentes em ativos. Neste trabalho foi realizado um estudo de caso em uma instituição de ensino superior do Vale do Aço. Esta instituição de ensino superior possui uma rede relativamente rica em número de dispositivos. As áreas de gerência de rede, as ferramentas para o monitoramento de redes e os protocolos que tornam possível esse monitoramento, que são SNMP e MIB, são objetos de estudo e análise neste presente trabalho. O The Dude foi a ferramenta utilizada para identificação da rede e que permitiu a detecção de incidentes. Os resultados foram analisados qualitativamente. Recursos, não existentes para a monitoração do ambiente computacional na instituição onde foi feito o estudo, passaram a integrar um conjunto de elementos de monitoramento relevantes, como o mapa da rede, o registro de eventos que identificam falhas de componentes computacionais e gráficos com informações de serviços, auxiliando a equipe de manutenção e suporte.

Palavras-chave: gerenciamento de redes, SNMP, MIB, detecção de incidentes.

Abstract

Computer networks are increasingly present in companies of large, medium and small size. For the good performance and continuity of the company is fundamental a good functioning of the network, for this, the management of the same is extremely relevant factor. This research work aims to offer adequate support to the maintenance and support team of the network resources, proposing to implement automated management systems of computing resources in an enterprise environment, detecting incidents in assets. In this work, a case study was realized at a higher education institution in Steel Valley. This institution of higher education has a relatively rich network in number of devices. The areas of network management, the tools for monitoring networks and the protocols that make this monitoring possible, that are SNMP and MIB, are objects of study and analysis in this work. The Dude was the tool used to identify the network and that allowed the detection of incidents. The results were analyzed qualitatively. Resources, not existent for the monitoring of the computational environment in the institution where the study was done, started to integrate a set of relevant monitoring elements, as the network map, the register of events that identify computational component failures and graphics with service information, assist the maintenance and support team.

Keywords: network management, SNMP, MIB, incident detection.

Lista de ilustrações

Lista de quadros

Lista de abreviaturas e siglas

CCITT	*International Telephone and Telegraph Consultative Committee* (Comitê Consultivo Internacional de Telefone e Telégrafo)
CMIP	*Common Management Information Protocol* (Protocolo comum de informação de gerenciamento)
CPU	*Central Processing Unit* (Unidade de processamento central)
CSMA/CD	*Carrier Sense Multiple Access with Collision Detection* (Acesso Múltiplo de Detecção de Transportadora com Detecção de Colisão)
DNS	*Domain Name System* (Sistema de Nomes de Domínio)
FTP	*File Transfer Protocol* (Protocolo de transferência de arquivo)
GPL	*General Public License* (Licença Pública Geral)
HD	*Hard Disk* (Disco Rígido)
HTTP	*Hypertext transfer protocol* (Protocolo de Transferência de Hipertexto)
ICMP	*Internet Control Message Protocol* (Protocolo de Mensagens de Controle da Internet)
IETF	*Internet Engineering Task Force* (Força-Tarefa de Engenharia da Internet)
IP	*Internet Protocol* (Protocolo de Internet)
ISO	*International Organization for Standardization* (Organização Internacional de Padronização)
MAC	*Media Access Control* (Controle de Acesso ao Meio)
MIB	*Management Information Base* (Base de Informação de Gestão)
NETBIOS	*Network Basic Input/Output System* (Sistema básico de entrada/saída da rede)
NMS	*Network Management System* (Sistema de Gerenciamento de Rede)
NNTP	*Network News Transfer Protocol* (Protocolo de transferência de notícias de rede)
NOC	*Network Operation Center* (Centro de Operação de Rede)
OID	*Object Identifier* (Identificador de Objeto)
OSI	*Open Systems Interconnection* (Interconexão de sistemas abertos)

PDU	*Protocol Data Unit* (Unidade de dados de protocolo)
POP	*Post Office Protocol* (Protocolo dos correio)
RAM	*Random Access Memory* (Memória de acesso aleatório)
RFC	*Request for Comments* (Pedido de Comentários)
SMTP	*Simple Mail Transfer Protocol* (Protocolo Simples de Transferência de E-mail)
SNMP	*Simple Network Management Protocol* (Protocolo Simples de Gerência de Rede)
WDS	*Windows Deployment Services* (Serviços de Implantação do Windows)

Sumário

1 Introdução

As redes de computadores passaram a fazer parte do cotidiano das pessoas como uma ferramenta que oferece recursos e serviços permitindo maior interação entre os usuários e um consequente aumento de produtividade (CARNIELO; OLIVEIRA et al., 2015).

Inicialmente as redes de computadores foram concebidas como meio para compartilhar dispositivos periféricos tais como impressoras, drivers de alta velocidade, entre outros. Existindo apenas em ambientes acadêmicos, governamentais e algumas empresas de grande porte. Entretanto, a rápida evolução das tecnologias de redes, aliada a grande redução de custos dos recursos computacionais, motivou a proliferação das redes de computadores por todos os segmentos da sociedade(TANEMBAUM, 2011).

Segundo Comer (2016), as redes de computadores têm crescido explosivamente. A comunicação via computador vem se tornando parte essencial da nossa infra-estrutura. Os computadores e as ligações entre eles para comunicação vem aumentando em diversos setores e aspectos dos negócios, incluindo propaganda, produção, planejamento, contabilidade, faturamento, acesso a informação em bibliotecas *on-line* e outros. Em resumo as redes de computadores estão em toda parte e tornaram-se um sistema de comunicação produtivo que alcança corporações, universidades, escritórios governamentais além do uso domiciliar.

1.1 O problema e sua importância

A cada ano as corporações crescem e evoluem tecnologicamente, expandindo também em número e complexidade as aplicações e recursos de hardware. O contínuo crescimento em número e diversidade dos componentes de rede de computadores aumenta a necessidade de gerenciamento, pois o bom funcionamento da corporação depende do funcionamento dos recursos computacionais e da comunicação entre eles.

A redes de computadores possibilitaram a conexão de diferentes hardwares e softwares, responsáveis pelo bom funcionamento das corporações. Além disso, uma industria inteira surgiu para o desenvolvimento de tecnologias de rede, produtos e serviços. Produzindo uma forte demanda por profissionais com conhecimentos sobre redes, para manter o funcionamento destas (COMER, 2016). Neste contexto, entende-se que grande parte dos custos são destinados à manutenção da rede.

Para Fachini (2010), nos dias atuais o monitoramento da infraestrutura computacional, torna-se uma atividade que contribui decisivamente para o funcionamento contínuo dos serviços oferecidos, garantindo que a qualidade desses mantenha-se em níveis satisfatórios pelo maior tempo possível.

Um gerenciamento manual exige uma grande equipe para atender as necessidades de uma rede corporativa e há o risco de apenas estarem consertando erros, demorando para identificar os problemas ao invés de agir de maneira preventiva. Ao alocar tempo para identi-

ficar uma falha, outras falhas poderiam ocorrer e a disponibilidade da rede ou parte dela ficar comprometida, dificultando controlar, analisar e administrar uma rede de forma eficiente e rápida contando apenas com pessoas. "A detecção de incidentes em redes não é uma tarefa simples, principalmente em redes de médio e grande porte, de modo que o papel de detectar e solucionar problemas fica a cargo de funcionários especializados."(MEDEIROS, 2017, p. 8)

Neste contexto, surge as seguintes questões: Como detectar incidentes e suas causas antecipadamente de forma a oferecer a equipe de suporte a possibilidade de ações proativas, visando evitar os incidentes? Como visualizar e analisar os recursos da rede de forma rápida e que auxilie a equipe de suporte, garantindo o funcionamento contínuo dos serviços da rede?

1.2 Justificativa

Uma das características fundamentais para o funcionamento adequado de um ambiente computacional em rede de computadores é a capacidade de ações pró-ativas por parte do corpo técnico responsável. Estas ações envolvem a detecção antecipada dos problemas e/ou possíveis problemas. Segundo Kurose e Ross (2010), o administrador da rede deve estar habilitado a detectar e a reagir a estes incidentes e certamente necessita de ferramentas que auxiliem a monitorar, administrar e controlar a rede.

Devido a constante expansão do uso das redes de computadores, aumentam também os problemas, tais como a indisponibilidade de aplicação e/ou serviço. Diante disso, o monitoramento em tempo real da infraestrutura de rede e seus ativos vem se tornando indispensável na gestão da tecnologia da informação. Esse monitoramento permite obter de modo rápido, preciso e confiável as informações necessárias sobre esses equipamentos, facilitando as tomadas de decisões (BENICIO, 2015).

Fica evidente que ferramentas integradas e automatizadas para o gerenciamento das redes tornaram-se uma necessidade, uma vez que, o gerenciamento manual da rede é insuficiente para resolver todos os problemas que surgem. O estudo e a implementação destas ferramentas, permitindo a otimização e a eficiência do trabalho, é um tema fascinante dentro da complexidade atual das corporações. Este tema, o gerenciamento de redes, ainda não tem a devida penetração nas soluções de conectividade entre os computadores, principalmente para empresas e instituições de pequeno e médio porte, o que faz com que a pesquisa e a busca por soluções eficientes sejam tão relevantes dentro da tecnologia da informação. Este trabalho de pesquisa propõem uma solução de gerenciamento de redes para um ambiente computacional distribuído, mostrando as vantagens e benefícios que os usuários e administradores do ambiente terão.

1.3 Objetivo

1.3.1 Objetivo Principal

O objetivo principal deste trabalho é implementar um sistema de detecção de incidentes em ativos através de uma ferramenta de gerenciamento de redes livre, disponível no

mercado utilizando o protocolo SNMP.

1.3.2 Objetivos Específicos

Os objetivos específicos que estão relacionados ao objetivo principal são:

- analisar as áreas de gerência de redes
- analisar os protocolos SNMP e MIB. Analisar ferramentas de gerenciamento de redes
- investigar os principais parâmetros de gerência visando melhorar a continuidade de serviços computacionais relevantes em um ambiente corporativo.

2 Fundamentação teórica

2.1 Gerenciamento de redes de computadores

Para Kurose e Ross (2010), o gerenciamento de rede permite oferecer, integrar e coordenar elementos de hardware, software e humanos para monitorar, configurar, analisar e controlar os recursos da rede de forma a satisfazer às exigências operacionais, de desempenho e qualidade dos serviços em tempo real. De forma resumida Saito e Madeira (2001), aponta que o gerenciamento de rede pode ser visto como um conjunto de mecanismos operacionais e administrativos necessários para controlar e manter os recursos da rede operando.

"Podemos definir gerenciamento de redes como o monitoramento, teste, configuração e diagnóstico de componentes da rede para atender a um conjunto de exigências definido por uma organização."(FOROUZAN, 2008, p. 873)

Carnielo, Oliveira et al. (2015), afirmam que a tarefa básica que uma gerência de rede deve executar envolve a obtenção de informações da rede, possibilitando um diagnóstico seguro e o encaminhamento de soluções dos problemas. Dentro deste contexto, Olifer e Olifer (2008) menciona sistemas de gerenciamento de redes como um sistema que responde de forma automática, responsável por coletar informações da rede. Estes sistemas são normalmente combinações de hardware e software. Em uma rede pequena é possível usar pequenos programas individuais para gerenciar os dispositivos e a medida que a rede cresce surge o problema relacionado com a combinação de todos utilitários. Para resolver esse problema, surge sistemas integrados de gerenciamento de redes.

2.1.1 Elementos do gerenciamento de redes

Utilizando a analogia de Kurose e Ross (2010), considere que o chefe de uma grande empresa com filiais espalhadas tem a tarefa de controlar o funcionamento destas. Para isso é necessário haver comunicação entre as filiais e a central e coletar informações periodicamente por meio de relatórios. Implícita neste cenário humano existe uma infraestrutura: o chefe, os locais remotos que estão sendo controlados (filiais), os agentes remotos (gerentes das filiais), protocolos de comunicação (modelos de relatórios, normas e dados padronizados), e dados (o conteúdo dos relatórios). A arquitetura de um sistema de gerenciamento de rede é conceitualmente idêntica a essa analogia de uma organização humana, e com o uso de ferramentas/softwares utilizamos termos parecidos para referenciar aos elementos da rede.

“A entidade gerenciadora é uma aplicação que em geral tem um ser humano no circuito e que é executada em uma estação central de gerência de rede na NOC.” (KUROSE; ROSS, 2010, p. 557). NOC (*Network Operation Center* - Centro de Operação de Rede).

Segundo Tanembaum (2003), estações de gerenciamento ou entidade gerenciadora na verdade são computadores que executam um software especial que se comunica com os agentes espalhados pela rede, emitindo comandos e obtendo respostas.

Dispositivos gerenciados são: estação de trabalho, roteador, *hub*, impressora, *switch, modem, Access Point*, e servidores. Podemos gerenciar quaisquer dispositivos que estiverem na rede e que possuem uma comunicação entre eles.

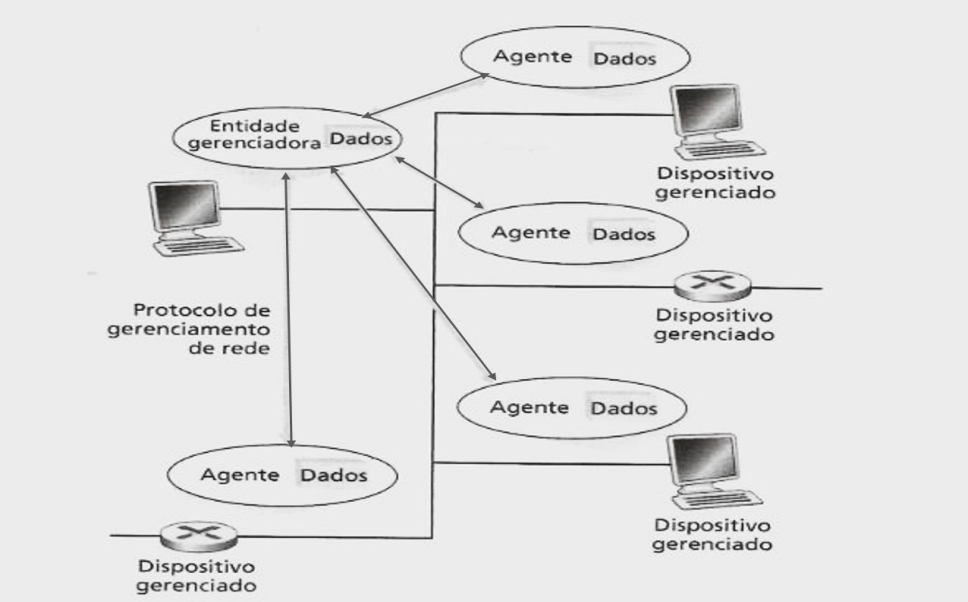
> No interior do dispositivo gerenciado pode haver diversos objetos gerenciados. Estes são, na verdade as peças de hardware propriamente ditas que estão dentro do dispositivo gerenciado (por exemplo, uma placa de interface de rede) e os conjuntos de parâmetros de configuração para as peças de *hardware* e *software* [...] esses objetos gerenciados tem informações associadas a eles que são coletadas dentro uma Base de Informações de Gerenciamento (*Management Information Base* - MIB) (KUROSE; ROSS, 2010, p. 557).

Para Kurose e Ross (2010), o agente de gerenciamento é um processo que ocorre no dispositivo gerenciado, que se comunica com a entidade gerenciadora e que executa ações locais sob o comando e o controle da entidade gerenciadora.

Agente de gerenciamento é um processo executado em um recurso que exporta uma base de dados de gerenciamento (MIB) para que o gerente possa ter acesso aos mesmos. Se comunica com a entidade gerenciadora passando informações da MIB. As informações são passadas através de um protocolo de comunicação ou protocolo de gerenciamento que fornece os mecanismos de comunicação entre o gerente e o agente (CARNIELO; OLIVEIRA et al., 2015).

A Figura 1 exibe uma estrutura básica de comunicação entre os dispositivos gerenciados e a entidade gerenciadora em uma rede. Onde os dispositivos gerenciados se comunicam com a entidade gerenciadora. Como pode ser visto a comunicação é bilateral e feita através de um protocolo de comunicação.

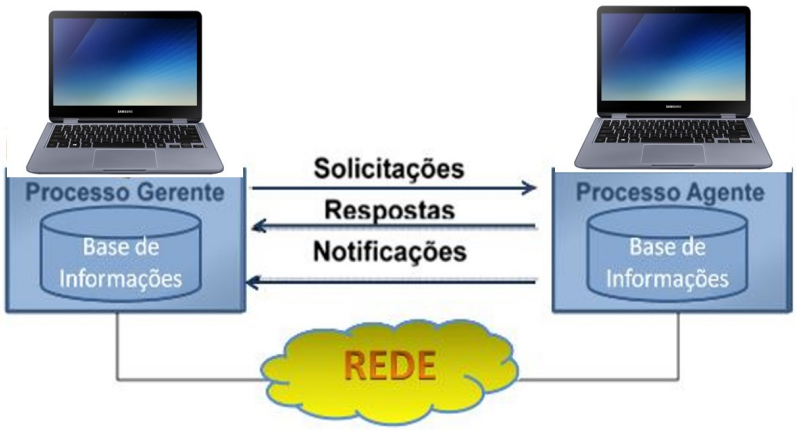
Figura 1 – Infraestrutura básica de gerenciamento de redes



Fonte: (KUROSE; ROSS, 2010)

A Figura 2 mostra de forma simples o modelo de gerenciamento com protocolo, onde o processo gerente faz solicitações/perguntas, o processo agente coleta as informações referentes à solicitação e responde buscando na base de dados. O processo agente pode também enviar notificações (Mensagens-*Trap*), que serão explicadas na seção 2.4.1

Figura 2 – Modelo com protocolo



Fonte: Elaborada pelo autor

2.2 Etapas de gerenciamento

Para Comer (2007), a gerência de redes é dividida em três etapas que se relacionam como na Figura 3. Através da coleta de dados é possível fazer uma análise e diagnóstico, após um diagnóstico é tomada uma ação adequada e coletado novamente os dados após alterações - funcionando em ciclo.

Figura 3 – Esquema das etapas de gerenciamento

Fonte:(COMER, 2007 apud CARNIELO; OLIVEIRA et al., 2015)

A coleta de dados é um processo automático que consiste na monitoração dos recursos gerenciados. O Diagnóstico: consiste na análise realizada a partir dos dados coletados

onde também é realizada a detecção da causa do problema no recurso gerenciado. Uma vez diagnosticado o problema cabe uma ação ou controle sobre o recurso, caso o evento não tenha sido passageiro (COMER, 2007). Neste trabalho vamos utilizar as etapas de coleta de dados e diagnóstico.

2.3 Dividindo em áreas funcionais

Pensando nas diversas tarefas, funções e tipos de monitoramento que um sistema de gerenciamento pode oferecer podemos separar em classes de funcionamento o gerenciamento. Por exemplo: em uma corporação pode-se ter o objetivo de analisar e monitorar determinados aspectos de uma rede – tráfego, mapa da rede, quais portas do *switch* estão sem conexão – enquanto outra corporação ou até mesmo outra parte da corporação pretende analisar e monitorar o estado de componentes dos elementos de rede, como uso de CPU, quantidade de espaço em disco, quantidade de memória RAM dos computadores; quem utiliza mais determinada impressora; atualizações de softwares, etc. Cada ambiente necessita de determinados grupos de funções que podem ser catalogadas em áreas de gerenciamento. Tais áreas definem o que deve ser gerenciado na rede.

2.3.1 Modelo OSI de áreas funcionais

A ISO (International Organization for Standardization) propôs um modelo de gerenciamento OSI (Open Systems Interconnection) que dividiu o gerenciamento em cinco áreas funcionais que são: Gerência de Desempenho, Gerência de Configuração, Gerência de Falhas, Gerência de Contabilidade e Gerência de Segurança. São áreas bem definidas e que reúnem um escopo de funções podendo ter subáreas dentro destas. Não faz parte do escopo deste trabalho de pesquisa a Gerência de Contabilidade e a Gerência de Segurança.

Gerência de Desempenho ou Performance: "mede o comportamento de dispositivos em uma rede, avaliando o desempenho através de seu monitoramento a fim de comprovar e medir o bom funcionamento da rede."(SOUZA,2017 apud BARROSO,2008, p. 25)

A gerência de desempenho avalia o comportamento dos objetos gerenciados e sua eficiência quanto às atividades de comunicação. Preocupa-se com os limites de desempenho dos objetos, permitindo assim alguns ajustes no desempenho para que o mesmo se torne aceitável para o ambiente. Exemplos de itens que devem ser observados: percentual do uso da capacidade de transmissão da rede, o delay-tempo de atraso - do ambiente, possíveis congestionamentos e gargalos na rede (CARNIELO; OLIVEIRA et al., 2015).

Para Forouzan (2008), através da gerência de performance os administradores de rede podem monitorar certas variáveis chaves como *throughput* (números de bits que passam em 1 segundo ou taxa real de transferência).

Gerência de Falhas: Para Olifer e Olifer (2008), inclui a detecção, localização e eliminação de falhas da rede. Expandindo esse conceito Abreu e Pires (2004) afirma que através da gerência de falhas é possível antecipar falhas com uso de rotinas que executam de tempos em tempos determinado pelo gerenciador, também com uso de alarmes, *thresoulds* e *syslog*

–*Thresoulds* é um valor ajustado para advertir o sistema de gerência, quanto a utilização, latência, ou congestionamento. *Syslog* é um padrão para transmissão de mensagem de log ou registro de eventos. A gerência de falhas trabalha com limites (qual limite que um recurso ou dispositivo pode chegar, por exemplo, estabelecer em um computador o valor máximo de memória RAM a ser usado); gerência de eventos (alarmes programados quando os limites forem atingidos, ou algo anormal acontecer.); correlacionamento causa/origem de problemas.

Gerência de Configuração: De acordo com Kurose e Ross (2010), o gerenciamento de configuração permite que um administrador saiba quais as configurações de hardware e software fazem parte da rede. Permitindo identificar os elementos funcionais da rede já na construção de mapas da rede, e as ferramentas de gerência oferecem inventário de *hardware* e *software*. Definindo também valores de limiar para identificação de incidentes, ativação de filtros, configuração de alarmes, e a visualização de *logs*.

A gerência de configuração é responsável pela descoberta, manutenção e monitoração de mudanças da estrutura da rede. As funções básicas desta área são: coleta de informações sobre a configuração, geração de eventos, atribuição de valores iniciais aos parâmetros dos elementos gerenciados, registro de informações e alteração de configuração dos elementos gerenciados (ODA 94 apud BONOMO, 2006).

De forma resumida “O gerenciamento de configuração permite manter atualizadas as informações de *hardware* e *software* de uma rede, incluindo as informações de configurações de todos os equipamentos.” (TELECO, 2017)

2.4 SNMP

2.4.1 Conceituando SNMP

RFC(*Request for Comments*) em português “pedido de comentários” são documentos técnicos criados e mantidos pela IETF (*Internet Engineering Task Force*), instituição que especifica os padrões que serão implementados e utilizados em toda a internet. O papel do RFC é detalhar todos os aspectos do protocolo proposto. O *Simple Network Management Protocol* (SNMP) foi definido e detalhado na RFC 1098 que já foi relançada na RFC 1157 (INTERNET ENGINEERING TASK FORCE, 2006).

“É o protocolo mais utilizado na Internet para gerenciar uma rede, e mesmo apesar de suas limitações em versões iniciais, conseguiu superar o antigo CMIP e se tornar um padrão de fato.” (MEDEIROS, 2017, p. 21)

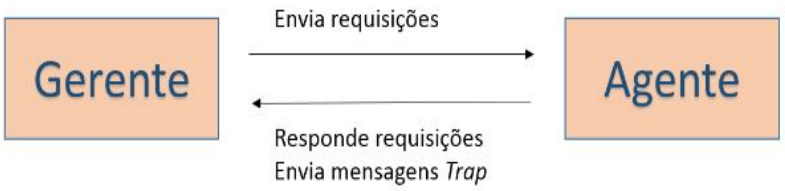
Segundo Comer (2001), o protocolo foi criado para definir exatamente como o um gerente se comunica com um agente. Ele define o formato e tamanho das mensagens.

Segundo Kurose e Ross (2010), o SNMP é usado na forma Comando-Resposta, no qual o gerente envia uma requisição a um agente, que recebe, realiza alguma ação e envia uma resposta ao gerente. A requisição é usada para consultar ou modificar valores de objetos MIB associados a um agente. O SNMP possibilta também Mensagem-*Trap*, ao gerente. As Mensagens-*Trap* são usadas para notificar e alertar o gerente que há uma mudança nos

valores dos objetos MIB. Elas são enviadas esporadicamente ou de tempos em tempos para sem serem requisitadas pelo gerente. Exemplo, se uma interface cair ou quando o congestionamento atingir um nível predefinido em um enlace ou quando ocorrer qualquer outro evento.

A Figura 4 mostra o esquema de comunicação básica entre gerente e agente utilizado pelo SNMP, na forma de comando-resposta, e envio de mensagens *Trap*.

Figura 4 – Comunicação básica entre agente e gerente



Fonte: Elaborada pelo autor

De acordo com as especificações do RFC 1157, em termos de comunicação o protocolo utiliza o datagrama UDP para envio de mensagens, já que “o protocolo UDP necessita de pouco recurso de hardware. Caso não seja possível transportar os dados ele não irá sobrecarregar a rede com tentativas de retransmissão.” (MAURO;SCHMIDT, 2005 apud BARROSO,2008,p. 17). Quanto a transmissão e recebimento de mensagens UDP utiliza a porta 161 e para mensagens-*Trap* utiliza a porta 162 segundo as especificações da RFC 1157 e é obrigatório que todas as implementações do SNMP suportem os cinco PDUs(Unidades de dados do protocolo): *GetRequest-PDU, GetNextRequest-PDU, GetResponse-PDU, SetRequest-PDU e Trap-PDU*.

Segundo Forouzan e Fegan (2008):

Quadro 1 – PDUs (unidades de dados do protocolo)

PDU	Descrição
Get	Coleta uma determinada informação de um elemento de rede
GetNext	É enviado do gerente para agente para recuperar o valor de uma variável. O valor recuperado é do objeto que vem após o ObjectId definido no PDU.
SetRequest	É utilizado para configurar o valor de um objeto gerenciado.
GetResponse	Refere-se a PDU enviada pelo agente ao gerente em resposta a alguma requisição. Ele contém valores das variáveis.
Trap	É enviado do agente ao gerente para relatar um evento, sem ter sido requisitado previamente.

Fonte: Elaborada pelo autor

2.4.2 Versões SNMP e RFCs

O Quadro 2 contém descrições das versões do SNMP de acordo com Bonomo (2006) e Abreu e Pires (2004).

Quadro 2 – Versões do SNMP

Versão	Descrição
Version 1(SNMPv1)	Definida na RFC 1157 [R1157] e é um padrão completo da IETF. A segurança do SNMPv1 baseia-se em comunidades, que são senhas: string de texto puro que permitem que qualquer aplicativo baseado em SNMP, que reconheça a string, tenha acesso a informações de gerenciamento de um dispositivo. Geralmente existem três comunidades: *read-only, read-write e trap*.
Version 2(SNMPv2)	É definida pelas RFCs 1905, 1906 e 1907 pelo IETF. Busca implementar e corrigir algumas deficiências da versão anterior, como: adicionar mais segurança, novas operações, comunicação entre servidores com a função de *manager* e configuração remota via SNMP.
Version 3(SNMPv3)	É a última versão do protocolo a alcançar o status completo da IETF, que inclui suporte para autenticação rigorosa e comunicação privativa entre as entidades gerenciadas.

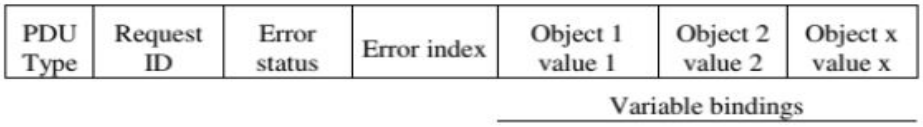
Fonte: Elaborada pelo autor

2.4.3 Formato das mensagens

De acordo com Bonomo (2006) e Abreu e Pires (2004), os pacotes de mensagem do SNMP são divididos em duas partes. A primeira parte contém a versão e o nome da comunidade, a segunda parte contém o PDU (Unidade de dados do protocolo).

A figura 5 mostra de forma simples o formato das PDUs.

Figura 5 – O formato da PDU (*Protocol Data Unit*)



Fonte: (ABREU; PIRES, 2004)

Segundo (ABREU; PIRES, 2004):

- PDU Type – especifica o tipo da PDU transmitida
- Request ID – Associa a requisição SNMP com a resposta
- Error status – Identifica um dos números de erros e o tipo, apenas na resposta

- Error index – Associa um erro com um objeto em particular
- Variable bindings – Representa o campo de dados da PDU SNMPv1, com o objeto e seu valor.

2.5 MIB

Segundo Kurose e Ross (2010), a MIB é um conjunto de objetos que contém todas informações necessárias para o gerenciamento. Pode ser considerada um banco de dados de objetos gerenciados que o agente rastreia. Os objetos são especificados utilizando a construção OBJECT-TYPE (uma identificação do objeto) e são nomeados hierarquicamente. Podemos considerar tais objetos como os recursos que serão monitorados.

"MIB é uma coleção de objetos gerenciados, que contém todas as informações necessárias para a gerência da rede. Os objetos são dispostos em forma hierárquica e reconhecidos por um OID." (MEDEIROS, 2017, p. 22)

A OID é um identificador (número inteiro) ou código que distingue o objeto a ser gerenciado. É uma sequência de inteiros baseada nos nós da árvore da MIB, separados por pontos(.) (COMER, 2001).

De acordo com Forouzan (2008), o SNMP utiliza a representação inteiro-ponto, embora podemos utilizar nome-ponto. Exemplo de representação:

iso.org.dod.internet.mgmt$\Rightarrow 1.3.6.1.2$

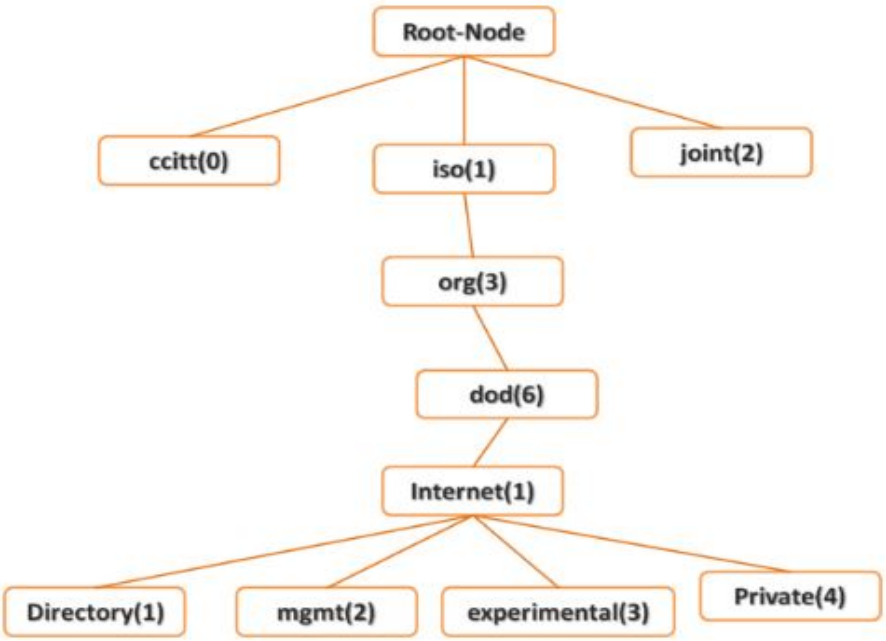
O número representa a identificação do nome representados nos nós da árvore. O caminho da informação se inicia com o nó principal da árvore e vai descendo em profundidade até se chegar na informação que deseja.

A Figura 6 representa parte da árvore MIB, onde os nós são representados por seus respectivos nomes ou números. No primeiro nível da árvore encontram-se os nós que definem 3 subárvores, destinadas aos órgãos responsáveis pela padronização das MIB's. No segundo e terceiro níveis encontram-se os nós que definem os órgãos responsáveis pela administração de uma determinada subárvore. **directory (1):** contém informações sobre o serviço de diretórios OSI; **mgmt (2):** contém informações de gerenciamento de rede, onde se encontra a MIB II; **experimental (3):** contém os objetos que ainda estão sendo pesquisados; **private (4):** contém objetos definidos por outras organizações. (TELECO, 2017)

Sendo o ccitt de responsabilidade do *International Telephone and Telegraph Consultative Committee*; iso da ISO e joint de responsabilidade de ambos.

"A primeira versão da MIB se deu com a RFC 1066. Sua evolução ocorreu quando a RFC 1213 propôs uma segunda MIB, a MIB II. As MIBs existentes são: MIB I, MIB II, MIB experimental, MIB privada. A MIB II, que é a evolução da MIB." (MEDEIROS, 2017, p. 22)

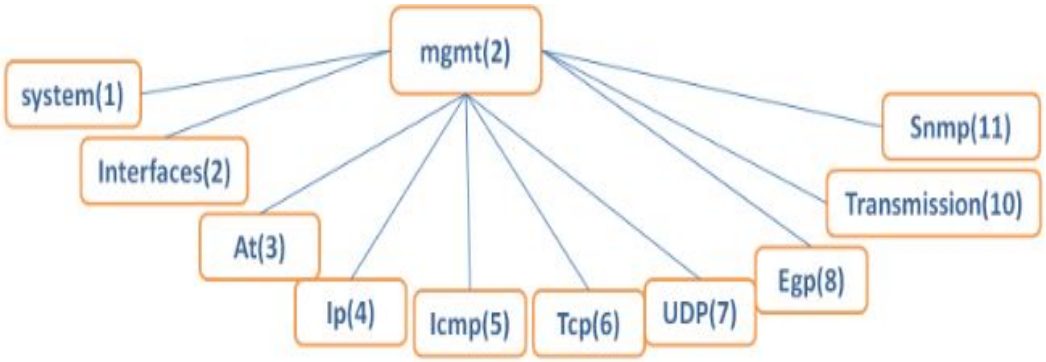
Figura 6 – Árvore MIB



Fonte: Elaborada pelo autor

A Figura 7 ilustra a subárvore do nó (mgmt(2)), a MIB II.

Figura 7 – MIB II



Fonte: Elaborada pelo autor

De acordo com Olifer e Olifer (2008):

- System – Define informações gerais do dispositivo
- Interfaces – Define informações sobre as interfaces de rede (por exemplo, seu número, tipo, taxas de trocas e tamanho mínimo de pacote
- AT – Relação entre endereço físico e endereço de rede

- IP – Dados relacionados ao IP (como endereços de gateway. hosts e estatísticas relacionados aos pacotes IPs)
- ICMP – Define estatísticas do protocolo ICMP
- TCP – Define informações do protocolo TCP e tabela de conexões
- UDP – Define informações do protocolo UDP (como os números de datagramas transmitidos, recebidos e corrompidos)

2.6 Ferramentas de gerência de redes

Durante o atual trabalho de pesquisa foi percebido uma grande variedade de sistemas de gerência de redes no mercado, encontrando também ferramentas livres. Cada uma com um foco em determinadas funcionalidades e diferentes interfaces. A partir disso foram identificadas algumas das ferramentas utilizadas ou estudadas no meio acadêmico, sendo elas: Cacti, Nagios, Zabbix, PRTG, The Dude e SpiceWorks.

"Zabbix é um software, distribuído sob a licença GPL, que monitora um vasto número de parâmetros de rede. Usa um flexível mecanismo de alarmes que permite aos usuários configurar um e-mail para receber um alerta de algum evento."(BONOMO, 2006, p. 14) Possui versões para distribuições Linux: Debian, Red Hat Enterprise Linux, Ubuntu; Windows, FreeBSD e CentOS. De acordo com Bonomo (2006), um dos mais importantes uso do Zabbix, é o monitoramento de desempenho, incluindo, número de processos rodando, disponibilidade de disco, gráficos de tendências para ajudar na identificação de gargalo e outras funcionalidades.

Nagios pode ser executado em sistemas operacionais Linux e Windows. Tanto no Nagios quanto Zabbix as informações sobre as coletas e dados históricos podem ser consultadas via *browser*. "Dentre os fatores que podem ser monitorados pelo Nagios, temos: serviços de rede como SMTP, POP3, HTTP, NNTP, PING, etc; recursos de um elemento como utilização de CPU, espaço em disco e utilização de memória."(BARROSO, 2008, p. 34)

Quanto aos protocolos tem-se: "O protocolo SMTP (Simple Mail Transfer Protocol - Protocolo Simples de Transferência de E-mail) é o protocolo padrão que permite transferir o e-mail de um servidor para outro, em conexão ponto a ponto."(CCMBENCHMARK, 2018). O protocolo POP (Post Office Protocol - Protocolo dos correios) permite recuperar o seu e-mail em um servidor distante (o servidor POP). Ele é necessário para as pessoas não conectadas permanentemente à Internet, para poderem consultar os e-mails recebidos offline (CCMBENCHMARK, 2018). Quanto ao HTTP, este é um protocolo de transmissão de hipertextos, do inglês “hypertext transfer protocol”, é usado para a World Wide Web (www) e define como os servidores devem transferir páginas para os clientes (navegadores) (GALLO; HANCOCK,). Segundo Feather (2006), NNTP é usado para a distribuição, consulta, recuperação e postagem de artigos da Netnews usando um mecanismo confiável baseado em fluxo. Para clientes de leitura de notícias, o NNTP permite a recuperação de artigos de notícias que são armazenados em um banco de dados central, dando aos assinantes a capacidade de selecionar apenas os artigos que deseja ler. O modelo da Netnews fornece indexação, referência cruzada

e expiração de mensagens antigas. NNTP é projetado para eficiente transmissão de artigos da Netnews. Por fim o teste de PING é utilizado para verificar se há comunicação fim a fim, ou seja, entre origem e destino.

O Cacti também é lançado sob a GNU-*General Public License*. É executado no Windows e Linnux sendo uma ferramenta com bastante disponibilidade de gráficos.

Já o PRTG é uma ferramenta paga, executa no Windows, de acordo com o site do fabricante, possui mais de 200 tipos de sensores para todos os serviços comuns de rede, incluindo HTTP, SMTP/POP3 (e-mail), FTP (File Transfer Protocol-protocolo de transferência de arquivo), etc. Sensores são os aspectos que monitora em um dispositivo. Monitora por exemplo o tráfego de uma conexão de rede, uma porta de um switch, a carga da CPU em uma máquina, muitos outros recursos. Os sensores são escolhidos durante o monitoramento e fica a critério do gerenciador.

O SpiceWorks é conjunto de ferramentas divididas que auxiliam na gerência, as ferramentas são: **central de ajuda:** funciona como um um sistema de chamados, onde visualiza os "bilhetes"de atendimento. Gerencia as solicitações de usuário; **monitor de redes:** onde verifica o *status* dos dispositivos, a disponibilidade dos serviços destes; **inventário:** realiza a coleta de detalhes dos dispositivos,permite visualizar por exemplo os softwares instalados e se estão ativados com licença, uso de disco, memória e SO instalado, aviso de erro em impressoras, como pouca tinta e outras funcionalidades. Seus requisitos básicos são: Windows 7, Windows 8, Windows Server 2008 R2 or Windows Server 2012 R2; 1.5 GHz Pentium 4 class processor e 2 GB RAM. É também gratuito.

De acordo com o site da (MIKROTIK,), que fornece o The Dude, ele realiza a descoberta e *layout* da rede de forma automática, descobre qualquer tipo ou marca de dispositivo. Também monitora links e notificações, é de fácil instalação e uso permitindo desenhar seus próprios mapas e adicionar dispositivos personalizados. Suporta monitoramento SNMP, ICMP, DNS e TCP para dispositivos que o suportam, faz também o uso de gráficos e acesso direto a ferramentas de controle remoto para gerenciamento de dispositivos. De forma descentralizada suporta o servidor Dude remoto e o cliente local. O The Dude executa no ambiente do Wine Linux, MacOS e Windows.

2.7 Trabalhos Relacionados

O trabalho de Medeiros (2017) abordou o monitoramento de configurações de switches, que visa detectar incidentes. Neste trabalho foi implementado um sistema com objetivos de capturar informações de configuração dos *switches*, criar uma base de configuração dos *switches* e integrar o sistema com outros sistemas de monitoramento. Onde aponta alguns trabalhos futuros: “indicar todos os switches que conseguem se comunicar através de uma dada Vlan; verificar se os parâmetros (ex: taxa transmissão) nas portas que interconectam dois *switches* estão coerentes; verificar se algum protocolo para lidar com *loops* físicos está configurado nos *switches* onde isso for necessário.”

Carnielo, Oliveira et al. (2015) elabora uma ferramenta via *web* para o monitoramento

descentralizado com o objetivo de facilitar a configuração e monitoração de diferentes serviços necessários em um servidor de rede, tais como: firewall, DHCP, squid/proxy, DNS, e-mail, dentre outros. A ideia deste trabalho é descentralizar o gerenciamento de rede para que coordenadores responsáveis por laboratórios de pesquisa pudessem monitorar separadamente. "A ferramenta foi totalmente desenvolvida com software livre e o acesso ao seu código permite alterações de acordo com as necessidades do usuário."

Almeida e Rohden (2017) apresenta um estudo sobre a utilização do protocolo SNMP na ferramenta ZABBIX, e informa que os resultados obtidos durante os testes foram satisfatórios, mostrando que é possível obter dados de forma automatizada durante longos períodos. Auxiliando o gerente de rede para tomar decisões antecipadamente e prever possíveis falhas ou problemas na rede.

Foi encontrado também o trabalho de dissertação de LEMES (2017) que tem por objetivo analisar soluções *opensource* para gerenciamento de redes de computadores, esboçando características fundamentais das ferramentas. As ferramentas analisadas foram: Nagios e Zabbix,foram analisados alguns critérios para escolha das ferramentas, e discute questões relacionadas ao licenciamento,linguagem de programação que a mesma foi desenvolvida, suporte técnico, interoperabilidade, maturidade, método de armazenamento dentre outros requisitos.

3 Ferramenta e metodologia

Este trabalho é uma pesquisa de caráter exploratório com estudo de caso em uma instituição de ensino no Vale do Aço. O trabalho foi realizado durante o período de estágio nesta. As análises dos resultados são qualitativas e se restringem a detecção de incidentes. A análise para a solução dos possíveis problemas ou erros encontrados não fazem parte do escopo deste trabalho de pesquisa.

3.1 Parâmetros de gerência

Como visto na seção 2.3.1 a gerência de redes é bastante abrangente, analisando diversos recursos e como o foco deste trabalho é detecção de incidentes, foram escolhidos previamente alguns parâmetros de gerência para diminuir o escopo e chegar ao objetivo.

Os seguintes parâmetros foram escolhidos: obter informações de portas dos *switches*; mapa da rede; funcionamento dos serviços em servidores; verificação de serviços críticos como DNS; verificação da disponibilidade de impressoras; quantidade de ativos conectados nos períodos de maior uso; verificação da taxa de envio e recebimento dos principais *links*, verificação de taxa de envio e recebimento de pacotes em *switches* e servidores.

3.2 Ferramenta Investigada e utilizada: The Dude

A escolha da ferramenta levou em conta a facilidade de instalação, pois é necessário apenas o aplicativo em extensão .exe, utilizado no Windows (sistema operacional utilizado no ambiente de teste). Possui fácil visualização das telas, alternando rapidamente entre mapa da rede ou tela de *Syslog* por exemplo e permite acesso remoto para visualizar a rede. Levou em conta também a facilidade de configuração dos parâmetros além de ser oferecida gratuitamente pela Mikrotik. O The Dude atende a escala de rede de médio porte, utilizada no ambiente de teste. Já existe uma gama de materiais a respeito das outras ferramentas citadas no capítulo 2, seção: 2.6, mas a ferramenta utilizada ainda é pouco estudada em meios acadêmicos.

O *software* The Dude, uma importante ferramenta para o monitoramento e mapeamento da rede, oferece diversas funcionalidades como lista de endereços, lista de administradores de rede, gráficos, acesso aos principais dispositivos, histórico, informações de *links*, registro de atividades, mapa da rede, oferece também acesso remoto a ferramenta, entre outros. O The Dude realiza a autodescoberta de rede, varre uma faixa de endereços IP para verificar quais dispositivos estão conectados, podendo exibir inicialmente o nome, endereço MAC e IP do dispositivo. O *software* prepara automaticamente o mapa da rede e permite desenhar os seus próprios mapas ou organizar, podendo ser executado em ambiente Windows, MacOS e Linux, exibe as atualizações e monitoramento da rede em tempo real e excelente tempo de resposta (SOUZA; LIMA, 2016).

3.3 Ambiente de teste

O ambiente de teste é uma das unidades de uma grande instituição de ensino no Vale do Aço. A instituição possui duas redes: acadêmica e administrativa. O ambiente possui:

- 240 computadores na rede acadêmica e 60 na rede administrativa;
- 14 impressoras;
- A rede acadêmica possui 2 servidores: o servidor de arquivos e o de DNS;
- A rede administrativa possui 4 servidores: o de DNS, o de arquivos, o de impressão, e o WDS que possui imagens de instalação contendo, por exemplo, aplicações, configurações e *updates* para serem utilizados nos processo de instalação do Windows nos computadores das redes;
- O ambiente possui 13 *switches*, gerenciáveis e não gerenciáveis, variando em número de portas;
- Contém 5 *acces point* e *routers* nos setores.

A rede acadêmica é composta por computadores para uso dos alunos em laboratórios e para professores em sala de aula. A rede administrativa contém computadores e impressoras para uso dos funcionários. Os equipamentos são de diferentes marcas, modelos, e arquiteturas. As redes se distinguem em número de equipamentos, domínio de rede, políticas de serviços e aplicações (sofwtares instalados), ambas com rede *Wireless*.

O ambiente foi propício pois conta com uma grande quantidade de equipamentos na rede (computadores, impressoras, *switches*, servidores, *access point* e roteadores).

A instituição de ensino possui um setor de TI com técnicos e estagiários responsáveis pelo suporte aos usuários, realizando manutenção das redes e dos computadores. No ambiente do setor possui: 2 computadores conectados ao domínio da rede acadêmica e 2 computadores conectados ao domínio da rede administrativa.

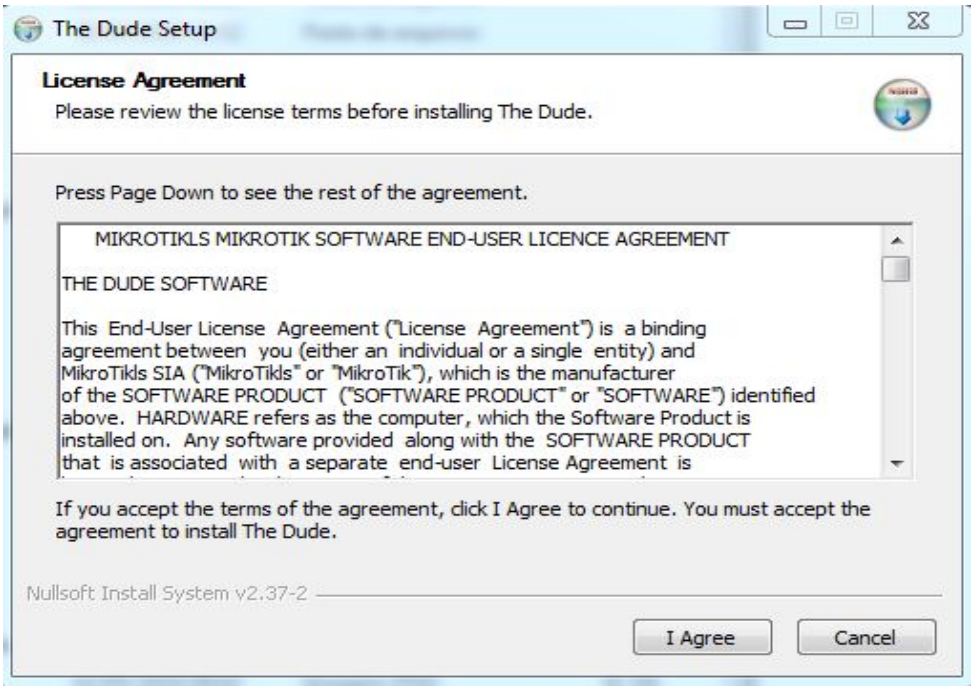
3.3.1 Instalação da ferramenta

O The Dude foi instalado em dois computadores diferentes, um conectado à rede acadêmica e outro à administrativa com as seguintes características:

- Sistema Operacional Windows 8.1 Professional;
- arquitetura de 64 bits;
- 4 Gbytes de RAM;
- processador Intel Core i3 3.2GHZ.

A Figura 8 é a tela inicial da instalação do The Dude, com os termos do acordo. Basta aceitar e ir para os próximos passos. É uma instalação fácil e rápida.

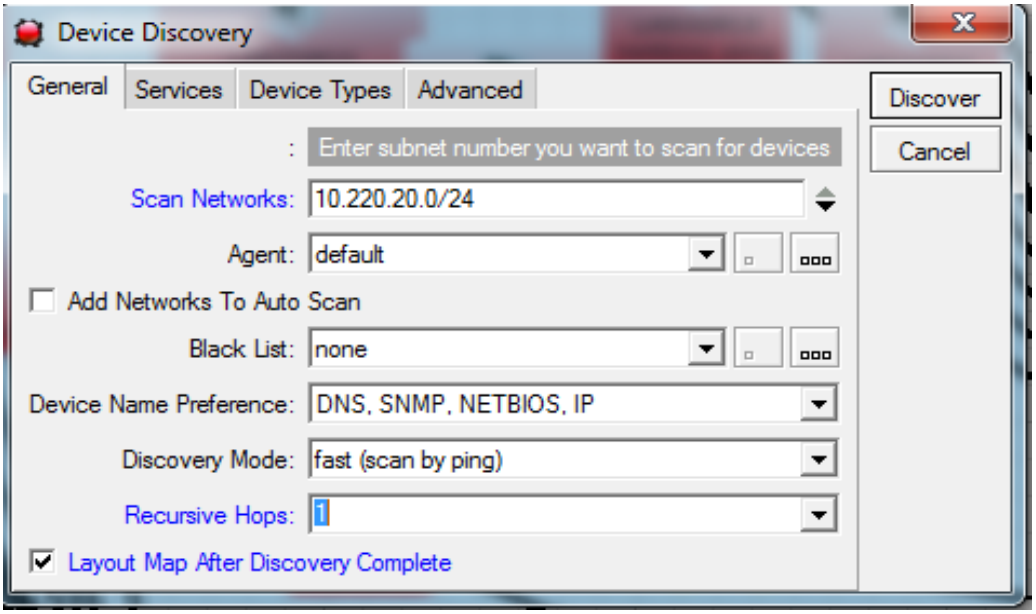
Figura 8 – Instalação Etapa-1



Fonte: Elaborada pelo autor

Na Figura 9 a ferramenta detecta automaticamente a faixa de IP da rede: 10.220.20.0/24.

Figura 9 – Instalação Etapa-2



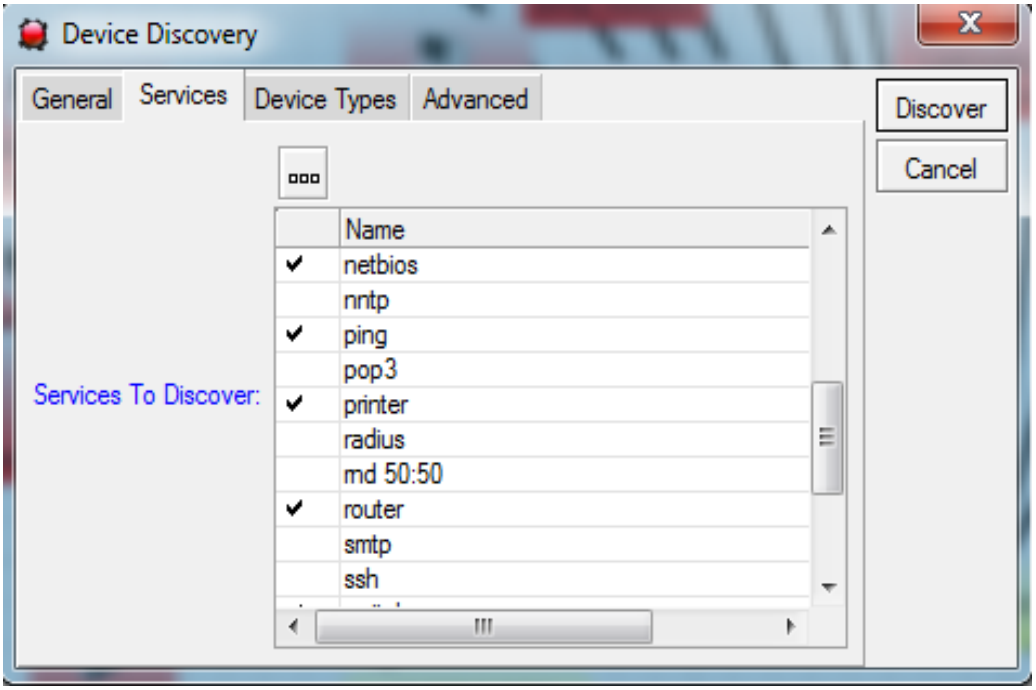
Fonte: Elaborada pelo autor

O campo **agente** especifica se a instalação é **default** ou **server**, a opção server é utilizada quando será instalada depois um cliente remoto. O campo **recursive hops** determina

quantos saltos serão verificados, no caso de haver alguns dispositivos de rede detectados conectados a mais de uma rede, continue a verificação da rede à qual esses dispositivos estão conectados. Foi marcada a opção de gerar automaticamente o mapa depois de descobrir a rede. O campo **services** especifica quais serviços deseja monitorar. Os serviços escolhidos estão relacionados ao parâmetros citados na sessão 3.1. São eles: ping (verificar comunicação fim a fim), HTTP (Protocolo de Transferência de Hipertexto), NETBIOS (Sistema básico de entrada/saída da rede), *printer* (verifica serviço de impressão) , *router*, DNS (Sistema de Nomes de Domínio), *switch*.

A Figura 10 mostra que existem outros serviços a serem monitorados, como NNTP, POP3, CPU, FTP, e outros.

Figura 10 – Serviços monitorados

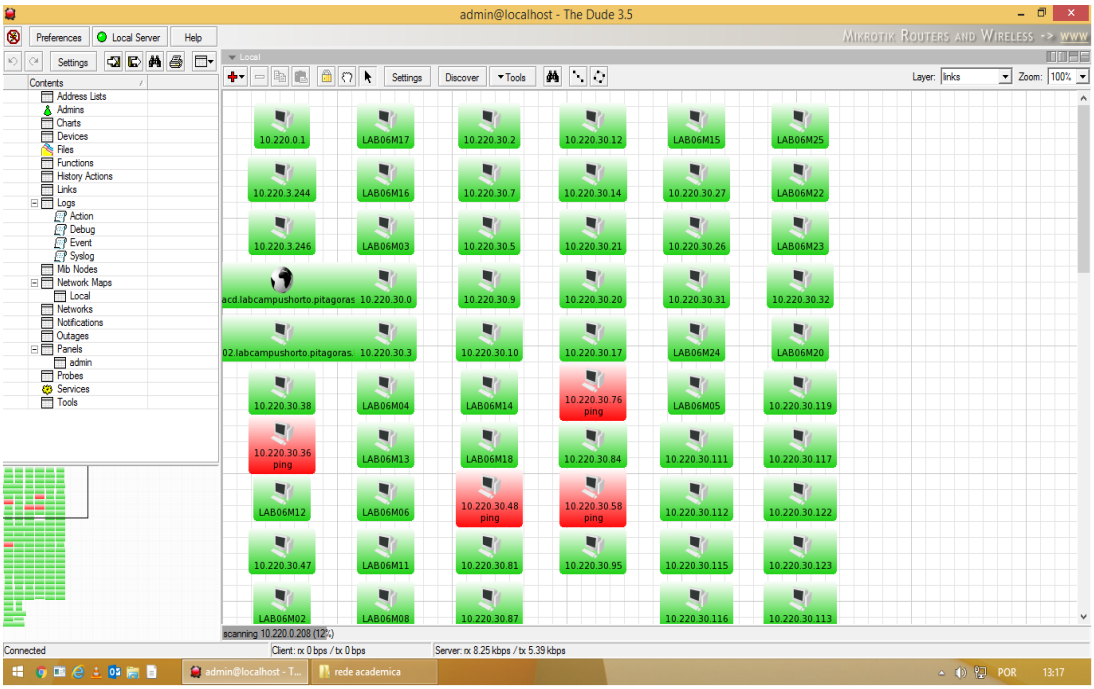


Fonte: Elaborada pelo autor

3.3.2 Descoberta da rede

Depois de instalar e definir inicialmente alguns parâmetros o The Dude escaneia a rede fazendo uma varredura na faixa de IPs. A Figura 11 mostra o *scaner* inicial da rede acadêmica, onde ele detecta aos poucos todos os dispositivos conectados nela. A figura 11 mostra que a ferramenta descobre a rede e identifica os dispositivos pelo nome ou IP, sendo representados pela cor verde os que estão ativos e vermelho os que desconectaram, exibindo no canto inferior a barra de porcentagem aproximada do escaneamento. No canto esquerdo da tela do The Dude é exibido o menu por onde pode alternar as telas principais, exibindo por exemplo, o mapa da rede ou notificações, ou registro de eventos (*syslog*), lista de todos dispositivos, objetos da árvore MIB, e outras funções.

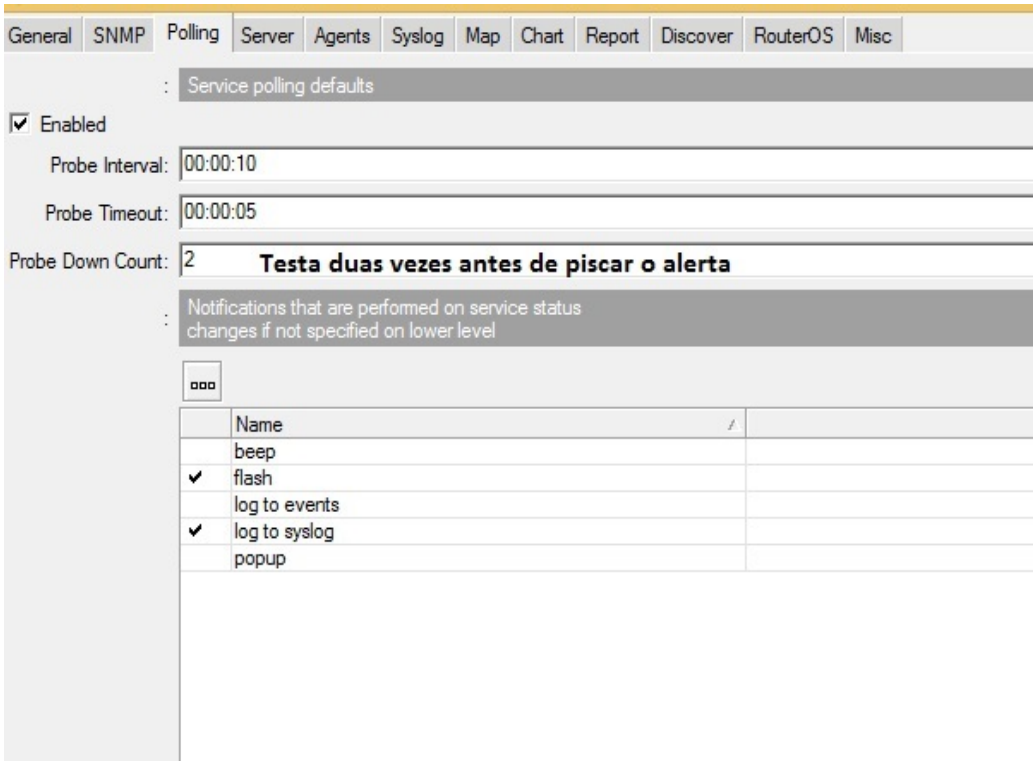
Figura 11 – Descoberta da rede acadêmica



Fonte: Elaborada pelo autor

Na Figura 12 pode ser visualizado a aba ***Polling*** (Amostragem) o ***Probe Interval*** onde se configura o Intervalo de testes, que foi colocado de 10 em 10 segundos, significa que de 10 em 10 segundos o The Dude vai realizar o teste de PING. ***Probe Timout*** define o tempo que irá continuar testando mesmo que tenha expirado o tempo de resposta. Foi configurado em 5 segundos. O campo ***Probe Down Count*** estabelece quantas tentativas são necessárias depois que o equipamento estiver *offline* para identificar como desconectado. Além disso existe o campo ***Notifications*** onde pode-se escolher como receberá as notificações, neste caso foram escolhidas o *flash* que é um alerta na tela da ferramenta onde o ícone do dispositivo altera de cor e gera o efeito de piscar, e *log to syslog* que exibe mensagem de *log* ou registro de eventos.

Figura 12 – Configurações de monitoramento



Fonte: Elaborada pelo autor

4 Resultados

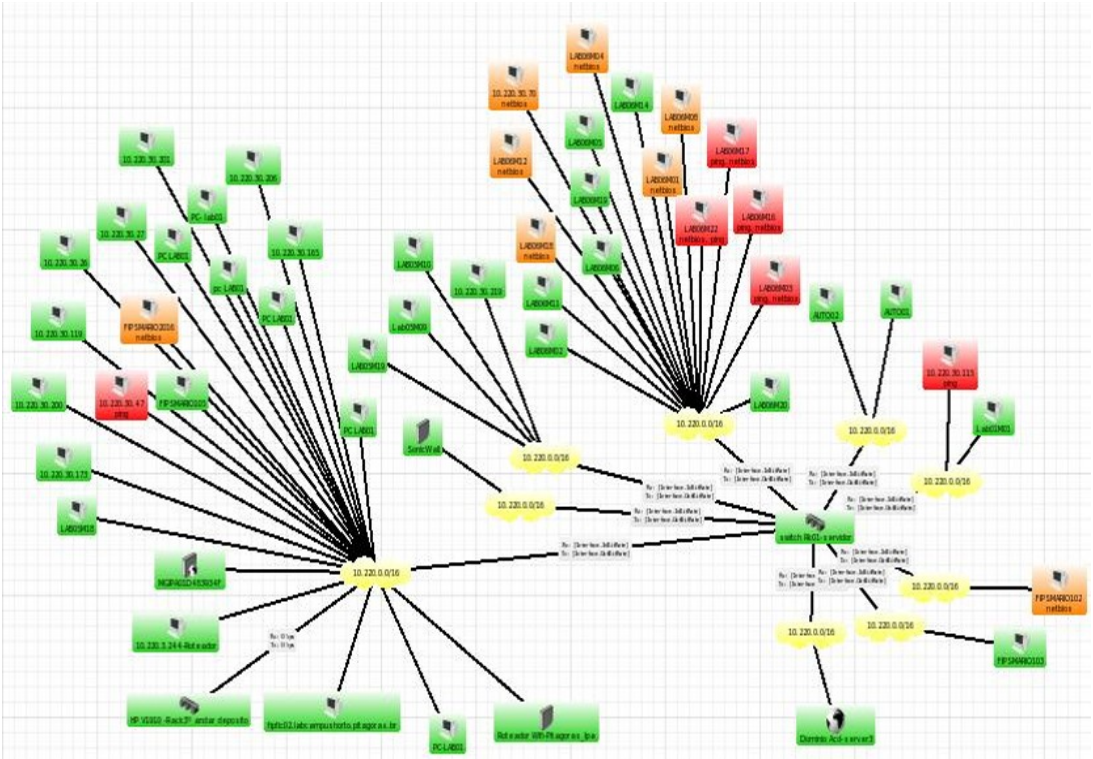
4.1 Mapa das redes

As Figuras 13 e 14 mostram o mapa das redes. O mapa da rede é o elemento de monitoramento essencial, pois permite a visualização rápida dos dispositivos. Os mapas foram reduzidos contendo dispositivos essenciais para o funcionamento da rede (*switches, routers, sonicwall* servidores e impressoras).

Alguns dispositivos estão no mapa apenas para efeito de uma pequena amostragem, computadores de funcionários e laboratórios/sala de aula. Tendo em vista que os mapas contém pequena parte da rede para satisfazer os parâmetros descritos na 3.1.

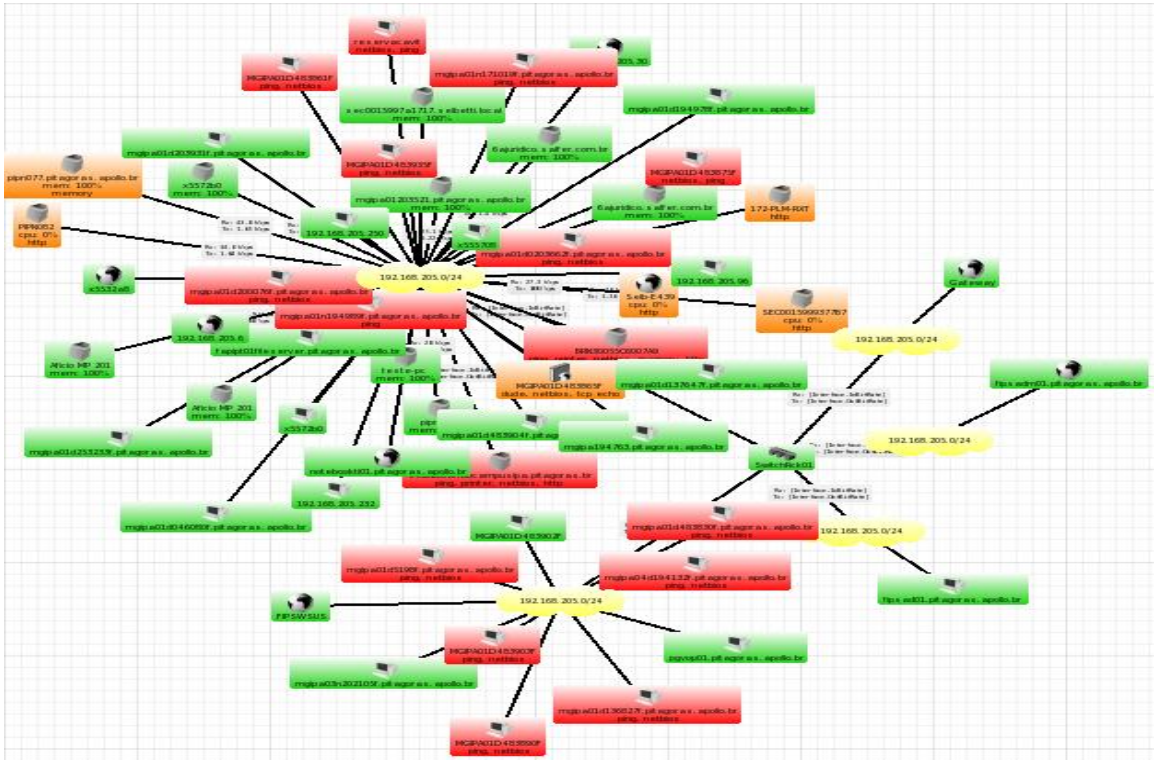
A ferramenta identifica e mostra o tipo de dispositivo encontrado, se é computador, *switch*, impressora, *Web server* ou *router*. Também identifica os celulares que estão na rede *Wireless*, porém captura apenas o IP e MAC (Media Access Control) - Controle de Acesso ao Meio, endereço físico e único, que é associado à interface de comunicação.

Figura 13 – Mapa da rede acadêmica



Fonte: Elaborada pelo autor

Figura 14 – Mapa da rede administrativa



Fonte: Elaborada pelo autor

No The Dude a cor verde nos dispositivos indica que os serviços estão ativos (*status* "ok"), a cor vermelha indica que houve perda de conexão ou outros serviços estão inativos, e a cor laranja indica que a conexão está caindo ou serviços estão lentos (estado intermediário entre o verde e vermelho).

4.2 Rede acadêmica

De acordo com os parâmetros citados na seção 3.1, pôde-se coletar várias informações importantes da rede, como: taxa de recebimento e envio de *links, status* de serviços como DNS, quantidade de ativos em período de maior uso, disponibilidade de impressoras, mapa da rede e informações de portas dos *switches*.

4.2.1 Dispositivos conectados

Na rede acadêmica (utilizada por professores e alunos) da faculdade, foi percebido que o horário de maior uso era durante o período noturno, que de fato possui mais cursos e aulas em funcionamento. O The Dude escaneou cerca de 2000 dispositivos conectados (a maior parte era na rede *Wireless*). Este dado é relevante pois auxilia na análise de sobrecarga de dispositivos conectados, pois se houver um número muito maior que este de dispositivos conectados pode haver congestionamento e ocasionar a lentidão do uso de Internet por exemplo. Para haver expansão ou aumento da rede em nível de *hardware* por exemplo, depende do

quanto a estrutura suporta e como tem funcionado com o tamanho atual, a fim de evitar uma sobrecarga.

4.2.2 Syslog: monitorando conexão de dispositivos

Um problema comum detectado na Instituição, conforme informação da sua equipe de manutenção e suporte, é o mal funcionamento de computadores devido ao não desligamento destes após o uso no final da noite. Para explicar melhor: os usuários utilizavam os computadores e muitas vezes deixavam ligados após o uso, durante toda a noite, e é comum um computador ficar muito lento quando está a muito tempo ligado ocasionando o aquecimento da CPU. Através do The Dude foi constatado que vários computadores continuavam conectados de um dia para outro. Essa verificação foi feita com o *syslog*. A Figura 15 mostra parte das informações do *syslog*, capturadas em um dia aleatório, depois do horário das aulas acabarem (22 horas). Foi percebido que alguns endereços IPs de computadores ainda estavam conectados. A tela de *syslog* mostrou o serviço de Ping nos dispositivos. Podemos perceber por exemplo que os IPs : 10.220.30.23, 10.220.30.116, 10.220.30.92 estavam conectados depois do horário de término das aulas (22:00 horas). A figura 15 mostra apenas parte da tela de *syslog*.

Figura 15 – Tela de syslog

Syslog

Time	Address	Event
Feb/19 21:36:00	10.220.30.201	Service ping on 10.220.30.201 is now down (timeout)
Feb/19 21:36:07	10.220.30.201	Service ping on 10.220.30.201 is now up (ok)
Feb/19 21:36:40	10.220.30.201	Service ping on 10.220.30.201 is now down (timeout)
Feb/19 21:36:55	10.220.30.201	Service ping on 10.220.30.201 is now up (ok)
Feb/19 21:36:56	10.220.30.116	Service ping on LAB05M10 is now down (timeout)
Feb/19 21:42:28	10.220.41.129	Service netbios on FIPSMARIO105 is now down (timeout)
Feb/19 21:42:30	10.220.41.129	Service ping on FIPSMARIO105 is now down (timeout)
Feb/19 21:52:45	10.220.30.23	Service ping on LAB06M03 is now up (ok)
Feb/19 21:53:26	10.220.30.73	Service netbios on LAB06M20 is now down (timeout)
Feb/19 21:54:19	10.220.30.23	Service ping on LAB06M03 is now down (timeout)
Feb/19 21:55:29	10.220.30.23	Service ping on LAB06M03 is now up (ok)
Feb/19 21:56:19	10.220.30.23	Service ping on LAB06M03 is now down (timeout)
Feb/19 21:56:57	10.220.30.23	Service ping on LAB06M03 is now up (ok)
Feb/19 21:58:08	10.220.30.96	Service netbios on LAB06M11 is now down (timeout)
Feb/19 21:58:49	10.220.30.23	Service ping on LAB06M03 is now down (timeout)
Feb/19 21:59:48	10.220.30.23	Service ping on LAB06M03 is now up (ok)
Feb/19 22:00:19	10.220.30.23	Service ping on LAB06M03 is now down (timeout)
Feb/19 22:01:07	10.220.30.23	Service ping on LAB06M03 is now up (ok)
Feb/19 22:02:19	10.220.30.23	Service ping on LAB06M03 is now down (timeout)
Feb/19 22:02:26	10.220.30.23	Service ping on LAB06M03 is now up (ok)
Feb/19 22:02:36	10.220.30.146	Service netbios on LAB06M05 is now down (timeout)
Feb/19 22:02:49	10.220.30.23	Service ping on LAB06M03 is now down (timeout)
Feb/19 22:02:56	10.220.30.23	Service ping on LAB06M03 is now up (ok)
Feb/19 22:03:49	10.220.30.23	Service ping on LAB06M03 is now down (timeout)
Feb/19 22:04:06	10.220.30.23	Service ping on LAB06M03 is now up (ok)
Feb/19 22:04:29	10.220.30.23	Service ping on LAB06M03 is now down (timeout)
Feb/19 22:05:04	10.220.30.23	Service ping on LAB06M03 is now up (ok)
Feb/19 22:10:19	10.220.30.23	Service ping on LAB06M03 is now down (timeout)
Feb/19 22:10:26	10.220.30.92	Service netbios on LAB06M06 is now down (timeout)
Feb/19 22:10:56	10.220.31.65	Service netbios on LAB06M19 is now down (timeout)
Feb/19 22:10:58	10.220.30.23	Service ping on LAB06M03 is now up (ok)
Feb/19 22:11:45	10.220.30.92	Service ping on LAB06M06 is now down (timeout)
Feb/19 22:11:51	10.220.30.116	Service ping on LAB05M10 is now up (ok)
Feb/19 22:12:11	10.220.30.92	Service netbios on LAB06M06 is now up (ok)
Feb/19 22:12:36	10.220.30.92	Service netbios on LAB06M06 is now down (timeout)
Feb/19 22:13:12	10.220.30.92	Service ping on LAB06M06 is now up (ok)
Feb/19 22:13:21	10.220.30.92	Service netbios on LAB06M06 is now up (ok)

Fonte: Elaborada pelo autor

Por meio dos resultados obtidos pelo presente trabalho de pesquisa, que foram repassados para a equipe de suporte e manutenção, tomou-se a decisão de criar uma política de

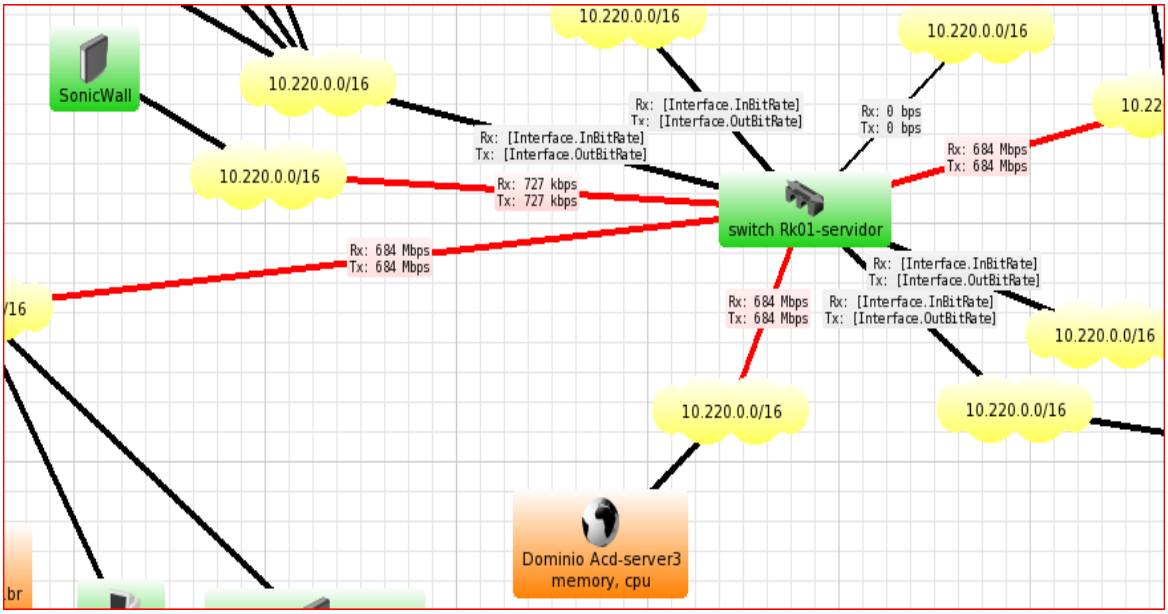
grupo no domínio da rede para desligar os computadores automaticamente as 23 horas. Com isso não houve mais o problema de aquecimento dos computadores e mal funcionamento, não sendo mais solicitado pelos usuários a equipe de suporte por este motivo.

4.2.3 Monitorando Links

De acordo com Forouzan (2008), o desempenho da rede depende de vários fatores, um deles é o controle de congestionamento que envolve medição de dois fatores: atraso e *throughput*.

Na tela do mapa da rede é possível identificar os links e as faixas de velocidade em que operam, a espessura do link mostra se é Ethernet (10 Mbit/s), Fast Ethernet (100 Mbit/s), GigaEthernet (1 Gbit/s) ou Wireless. Monitorando os links é possível verificar a taxa de envio (Tx) e de recebimento (Rx) em tempo real como mostrado na Figura 16.

Figura 16 – Velocidade de Links



Fonte: Elaborada pelo autor

Quanto maior a espessura do *link* maior a velocidade em que opera. O The Dude identifica *links* em vermelho como *link full*, apesar de no manual do The Dude não especificar o que significa este termo, foi pesquisado em outras fontes e no fórum da Mikrotik, que o termo indica que a taxa de envio Tx é a mesma de recebimento Rx. É muito importante monitorar as velocidades dos links em tempo real, pois é através deles que os dados são transportados. Monitorando estes é possível verificar congestionamento, ou se o link "caiu".

Os resultados do *throughput* (números de bits que passam em 1 segundo ou taxa real de transferência) do *link* que conecta ao SonicWall, por exemplo, é relevante, pois trata-se dos dados coletados de um router e serviço de *firewall* para proteger a rede. Este dispositvo é responsável pelo acesso a rede externa (Internet) e pela proteção da rede interna. Quando o *link* conectado a ele cai, toda a faculdade fica sem acesso a Internet. Foi bastante útil este

monitoramento, pois permite conhecer a causa do problema, exemplo, ao perceber lentidão do serviço de Internet como um todo, basta verificar o *link* com SonicWall, se houver problema com link significa que as decisões tomadas pela equipe de suporte e manutenção devem ser sobre o SonicWall.

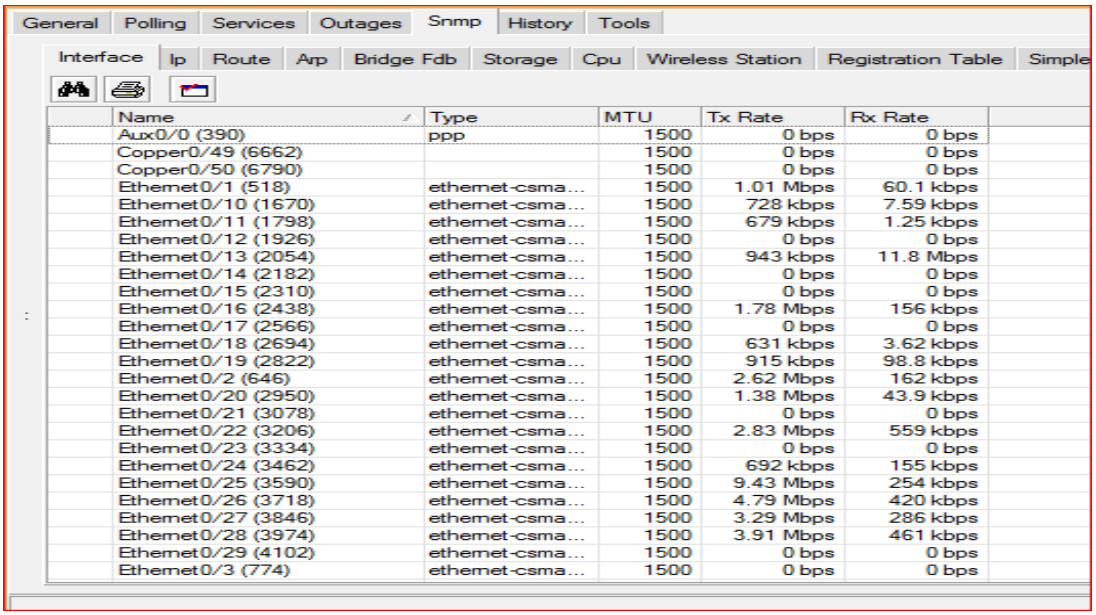
Não existe um valor exato de referência para taxa de transmissão dos links pois depende de diversos fatores da rede. No entanto, os valores obtidos no monitoramento devem ser analisados pela equipe de manutenção e suporte.

Throughput pode ser definido como número de pacotes que passam em um link. Quando a carga está abaixo da capacidade da rede, o *throughput* aumenta e quando a cargar atinge a capacidade da rede, o *throughput* diminui, a razão disso é o descarte de pacotes por parte de roteadores. As filas ficam cheias e tem que retransmitir pacotes usando mecanismo de time-out. Causando a lentidão ou congestionamento (FOROUZAN, 2008).

4.2.4 Monitorando Switches

Um monitoramento importante são as portas do *switches*, como visto na Figura 17.

Figura 17 – Portas conectadas



Name	Type	MTU	Tx Rate	Rx Rate
Aux0/0 (390)	ppp	1500	0 bps	0 bps
Copper0/49 (6662)		1500	0 bps	0 bps
Copper0/50 (6790)		1500	0 bps	0 bps
Ethernet0/1 (518)	ethernet-csma...	1500	1.01 Mbps	60.1 kbps
Ethernet0/10 (1670)	ethernet-csma...	1500	728 kbps	7.59 kbps
Ethernet0/11 (1798)	ethernet-csma...	1500	679 kbps	1.25 kbps
Ethernet0/12 (1926)	ethernet-csma...	1500	0 bps	0 bps
Ethernet0/13 (2054)	ethernet-csma...	1500	943 kbps	11.8 Mbps
Ethernet0/14 (2182)	ethernet-csma...	1500	0 bps	0 bps
Ethernet0/15 (2310)	ethernet-csma...	1500	0 bps	0 bps
Ethernet0/16 (2438)	ethernet-csma...	1500	1.78 Mbps	156 kbps
Ethernet0/17 (2566)	ethernet-csma...	1500	0 bps	0 bps
Ethernet0/18 (2694)	ethernet-csma...	1500	631 kbps	3.62 kbps
Ethernet0/19 (2822)	ethernet-csma...	1500	915 kbps	98.8 kbps
Ethernet0/2 (646)	ethernet-csma...	1500	2.62 Mbps	162 kbps
Ethernet0/20 (2950)	ethernet-csma...	1500	1.38 Mbps	43.9 kbps
Ethernet0/21 (3078)	ethernet-csma...	1500	0 bps	0 bps
Ethernet0/22 (3206)	ethernet-csma...	1500	2.83 Mbps	559 kbps
Ethernet0/23 (3334)	ethernet-csma...	1500	0 bps	0 bps
Ethernet0/24 (3462)	ethernet-csma...	1500	692 kbps	155 kbps
Ethernet0/25 (3590)	ethernet-csma...	1500	9.43 Mbps	254 kbps
Ethernet0/26 (3718)	ethernet-csma...	1500	4.79 Mbps	420 kbps
Ethernet0/27 (3846)	ethernet-csma...	1500	3.29 Mbps	286 kbps
Ethernet0/28 (3974)	ethernet-csma...	1500	3.91 Mbps	461 kbps
Ethernet0/29 (4102)	ethernet-csma...	1500	0 bps	0 bps
Ethernet0/3 (774)	ethernet-csma...	1500	0 bps	0 bps

Fonte: Elaborada pelo autor

A aba de Interface exibe o número da porta, tipo de protocolo de gerenciamento de tráfego (CSMA/CD) e a taxa de transporte e recebimento de dados no momento. Podemos identificar portas inativas, por exemplo, como as portas com velocidade sempre zero de envio e recebimento. Na aba ARP exibe o IP e o MAC do dispositivo conectado, na aba Bridge Fdb exibe o número da porta e o MAC conectado.

Um problema que foi resolvido com o auxílio deste monitoramento foi o melhor mapeamento da rede. Vários *switches* não eram gerenciáveis, sendo assim não era possível visualizá-los como *switches* no mapa e apenas como dispositivo comum. Verificando fisica-

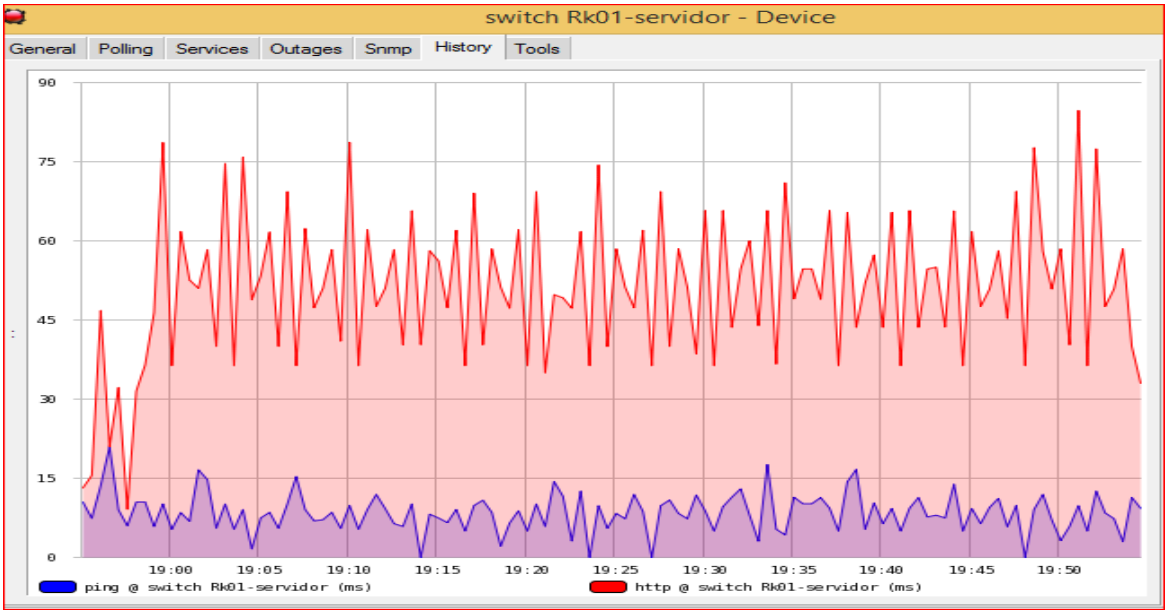
mente no dispositivo o seu MAC, era possível verificar em qual porta estava conectado em outro *switch* utilizando o The Dude, pois mesmo em um ambiente corporativo e que tenta seguir padrões, muitas vezes vários dispositivos não estavam identificados no local físico correto. Um problema comum que contatou no ambiente de teste era um dispositivo ter sua conexão trocada fisicamente de porta no *switch* sem fazer as devidas modificações na lista de identificações, gerando como consequência um longo tempo para corrigir incidentes ou até mesmo provocando outros. Por isso a importância de obter estas informações dos *switches*.

No ambiente de teste houve a oportunidade de presenciar a perda de conexão em um laboratório inteiro de informática, e também em um andar inteiro. Foi verificado que os cabos estavam corretamente ligados, porém o incidente devia-se aos *switches* dos respectivos locais estarem com portas importantes queimadas. A ação da equipe de suporte e manutenção, diante do diagnóstico apresentado, fez a substituição. O The Dude gerou alertas sobre o *status* destes *switches* que tornou possível identificar a real causa do incidente.

Para atender os parâmetros de gerência foram monitorados os serviços de PING e HTTP. O PING é essencial pois mostra o tempo de resposta de conexão do dispositivo na rede e o HTTP mostra o tempo de resposta da comunicação de transferência de Hipertexto, utilizado na navegação Web.

As Figuras 18 e 19 exibem o histórico do Ping e HTTP em um dos *switches* principais que fazem a distribuição da rede. O histórico é de um dia aleatório.

Figura 18 – Histórico Ping e HTTP-switch

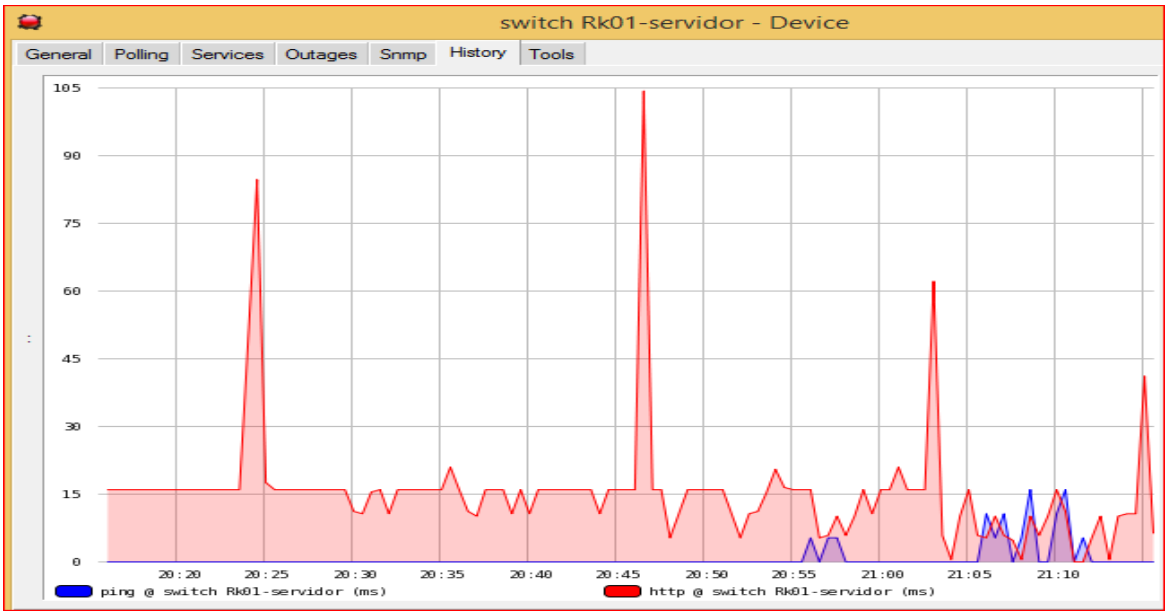


Fonte: Elaborada pelo autor

A linha em azul mostra em milissegundos o serviço de PING, relativamente baixo, portanto um tempo de resposta rápido, quanto menor o tempo em ms, mais rápida a resposta.

A análise dos valores exibidos é um tema complexo que deve ser estudado com mais detalhes. O objetivo dos resultados coletados neste presente trabalho de pesquisa não é anali-

Figura 19 – Histórico Ping e HTTP-switch



Fonte: Elaborada pelo autor

sar os valores coletados e sim mostrar que o monitoramento com a ferramenta permite coletar tais dados em tempo real, de forma a identificar falhas no momento do incidente. Para uma análise dos valores é necessário estudo de valores de referência e da estrutura da rede.

Em Brito (2013), informa que não existe um valor único de referência de tempo de resposta para todas as redes e mostra alguns valores aceitáveis em algumas tecnologias. Em redes locais cabeadas, por exemplo, é tolerável uma latência de até 30ms e recomendado 10ms. Para link com internet é ideal até 50ms. Mas tais valores dependem da finalidade e estrutura da rede para avaliar se realmente estão aceitáveis ou não.

A linha em vermelho mostra o serviço HTTP com alguns picos e tempo em milissegundo mais alto no horário de 19:00 as 19:50 conforme a Figura 18, que coincide com o horário de maior utilização da internet tanto no domínio acadêmico quanto administrativo. Através do monitoramento destes serviços é possível analisar a conexão com o *switch*, se está ativa e se está lenta ou não, podendo concluir também se o tráfego de HTTP está ativo, e o tempo de resposta, ou seja se o *switch* está conseguindo distribuir dados da internet.

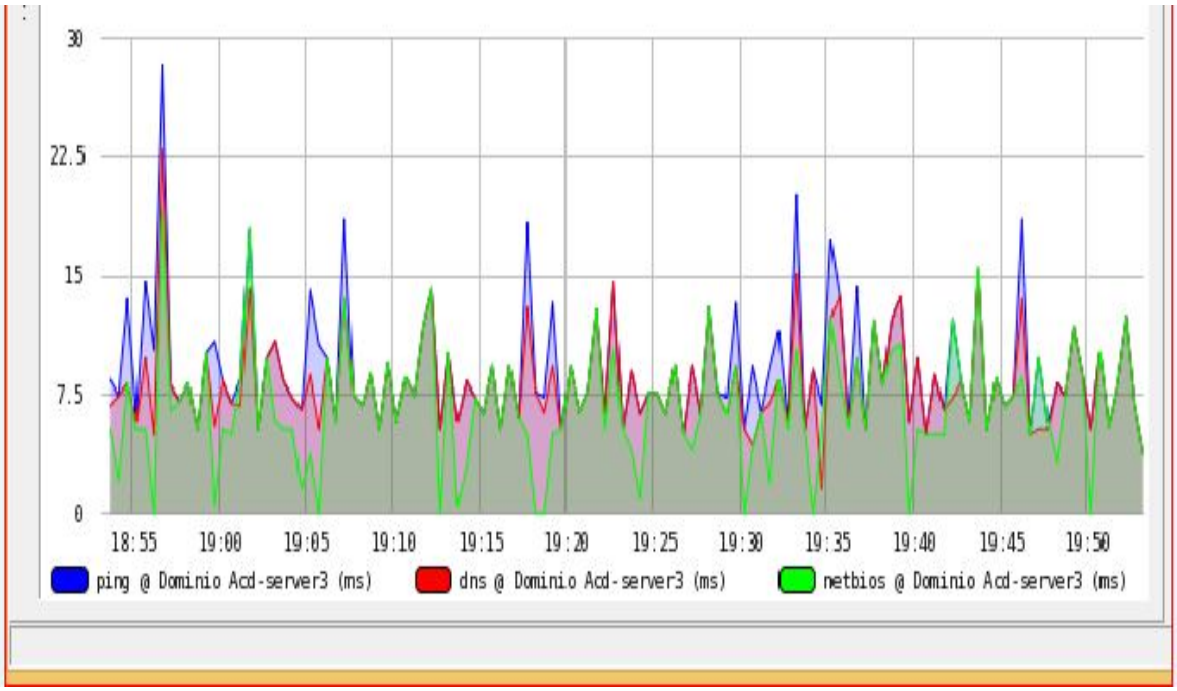
4.2.5 Monitorando servidor

Foram também monitorados os servidores. A Figura 20 mostra o histórico dos serviços monitorados em um servidor de domínio de rede.

As linhas de PING e DNS, que estão nas cores azul e vermelho respectivamente. O PING mostra o tempo de resposta de conexão do dispositivo na rede, o DNS mostra o tempo de resposta do serviço que gerencia o domínio da rede (que permite os usuários fazerem *login* nos computadores, gerencia as políticas de grupos e outros). Podendo observar que estavam com tempo de resposta em milissegundos relativamente rápido. Ambos abaixo de 22

milisegundos, com pouca variação entre os picos. A linha na cor verde refere-se ao serviço de NetBIOS. De acordo com Symantec (2017), NetBIOS é um protocolo de entrada/saída básico da rede que permite que aplicativos em computadores separados comuniquem-se através de uma rede local, utilizando o Windows. É importante o monitoramento deste serviço pois muitas vezes fez-se necessário acessar computadores da rede remotamente, principalmente os servidores, além do próprio serviço de login dos usuários. O gráfico mostra que todos os três serviços monitorados tinham o tempo de resposta baixo.

Figura 20 – Histórico Server DNS



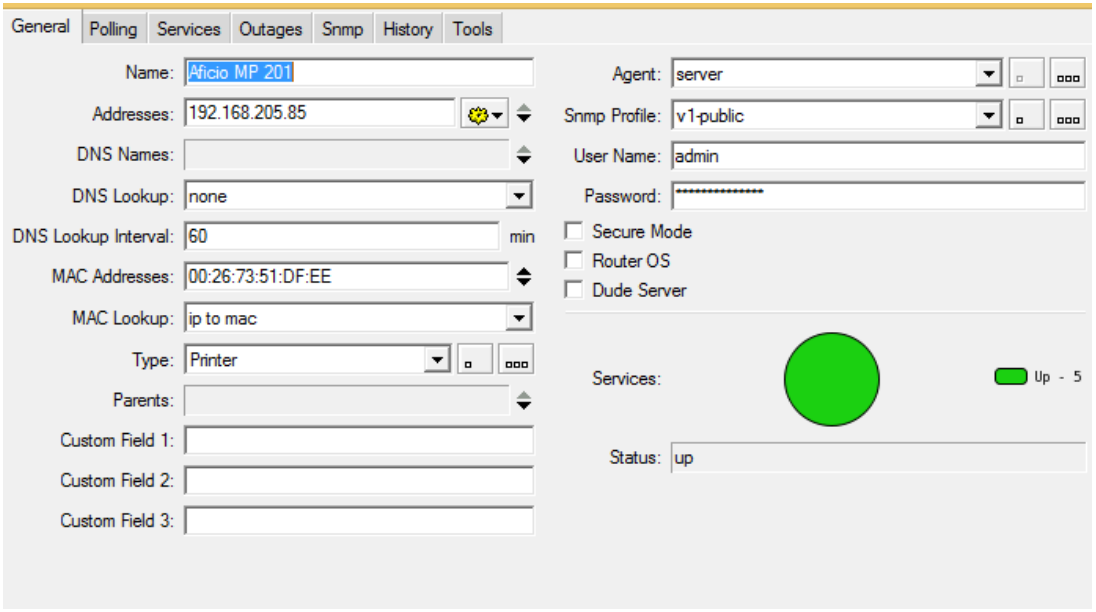
Fonte: Elaborada pelo autor

4.3 Rede administrativa

4.3.1 Monitorando Impressoras

Conforme informação da equipe de suporte e manutenção, grande parte dos chamados abertos solicitando a equipe de suporte era referente às impressoras, seja por falta de toner, papel atolado, ou falta de comunicação com servidor, e assim o serviço de impressão parava. Diante dessa informação foi feito o monitoramento das impressoras. A Figura 21 mostra a tela de propriedades de uma impressora capturada pelo The Dude. Identificando o IP, MAC e nome. É possível alterar o nome colocando uma descrição do setor onde se encontra, para melhor identificação. Como visto na figura é possível visualizar se os serviços da impressora estão ativos, a imagem mostra que o gráfico está verde (ativo), logo a impressora está conectada e sem problemas de impressão. O serviço "*printer*", indica se a impressora está imprimindo ou não. Sendo feito o monitoramento e analisando os dados, é possível identificar se a impressora parou de imprimir devido a falha de conexão ou por outro motivo, ao identificar a causa é tomada a decisão cabível para resolver.

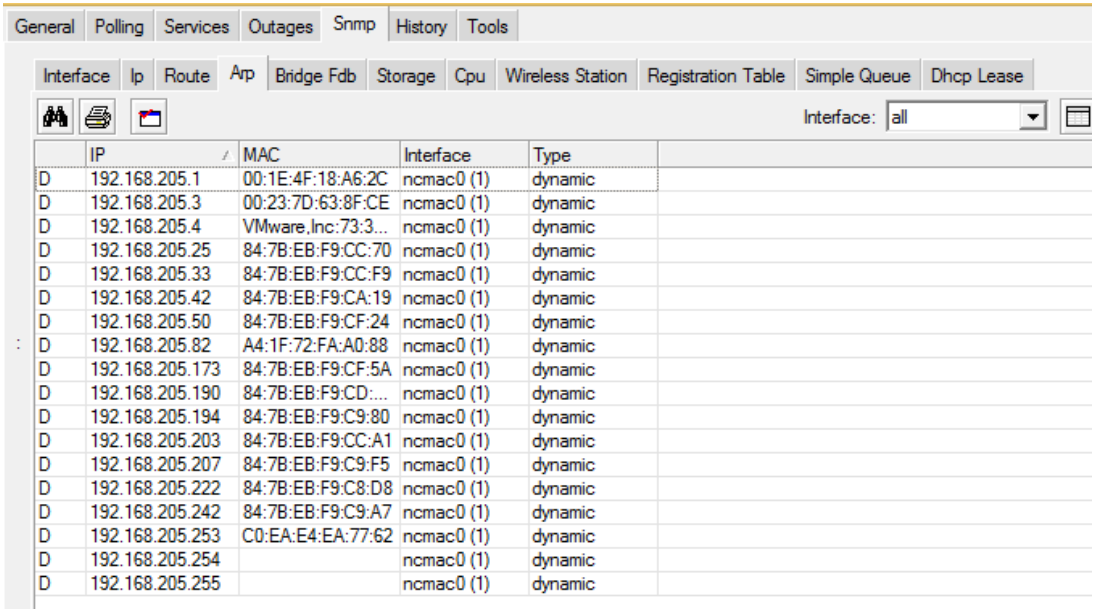
Figura 21 – Propriedades da impressora



Fonte: Elaborada pelo autor

Em tempo real é possível verificar também a tabela com os IPs de computadores que estão acessando a impressora, verificando a tabela ARP. A Figura 22 mostra a tabela ARP (Address Resolution Protocol - Protocolo de Resolução de Endereços) de uma impressora.

Figura 22 – Tabela ARP-impressora



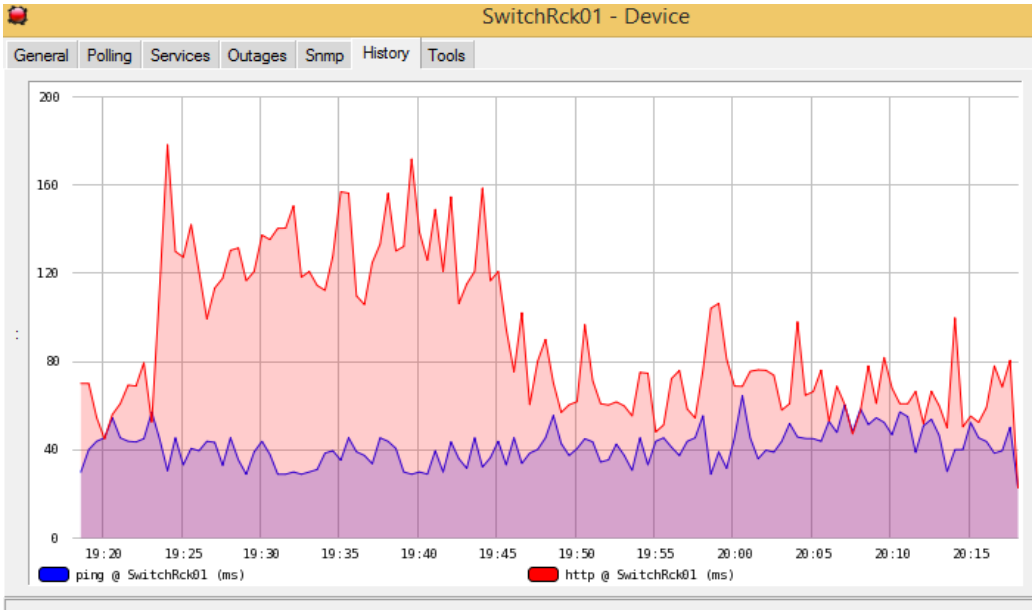
	IP	MAC	Interface	Type
D	192.168.205.1	00:1E:4F:18:A6:2C	ncmac0 (1)	dynamic
D	192.168.205.3	00:23:7D:63:8F:CE	ncmac0 (1)	dynamic
D	192.168.205.4	VMware,Inc:73:3...	ncmac0 (1)	dynamic
D	192.168.205.25	84:7B:EB:F9:CC:70	ncmac0 (1)	dynamic
D	192.168.205.33	84:7B:EB:F9:CC:F9	ncmac0 (1)	dynamic
D	192.168.205.42	84:7B:EB:F9:CA:19	ncmac0 (1)	dynamic
D	192.168.205.50	84:7B:EB:F9:CF:24	ncmac0 (1)	dynamic
D	192.168.205.82	A4:1F:72:FA:A0:88	ncmac0 (1)	dynamic
D	192.168.205.173	84:7B:EB:F9:CF:5A	ncmac0 (1)	dynamic
D	192.168.205.190	84:7B:EB:F9:CD:...	ncmac0 (1)	dynamic
D	192.168.205.194	84:7B:EB:F9:C9:80	ncmac0 (1)	dynamic
D	192.168.205.203	84:7B:EB:F9:CC:A1	ncmac0 (1)	dynamic
D	192.168.205.207	84:7B:EB:F9:C9:F5	ncmac0 (1)	dynamic
D	192.168.205.222	84:7B:EB:F9:C8:D8	ncmac0 (1)	dynamic
D	192.168.205.242	84:7B:EB:F9:C9:A7	ncmac0 (1)	dynamic
D	192.168.205.253	C0:EA:E4:EA:77:62	ncmac0 (1)	dynamic
D	192.168.205.254		ncmac0 (1)	dynamic
D	192.168.205.255		ncmac0 (1)	dynamic

Fonte: Elaborada pelo autor

4.3.2 Monitorando switch

Foi feito também o monitoramento dos *switches*. A Figura 23 mostra o histórico de Ping e HTTP de um dos *switches* principais, que fazem a distribuição da rede para demais setores da faculdade.

Figura 23 – Histórico switch principal



Fonte: Elaborada pelo autor

O gráfico acima apenas comprova que o serviço HTTP opera com maior tempo em ms (milissegundos) em determinados horários, que possivelmente é devido a maior quantidade de acesso, já que o Ping continua na mesma média, e de fato o período de maior utilização dos serviços Web é no período noturno. Durante o estágio foi percebido que entre as 19:00 e 20:00 horas os funcionários utilizavam muito mais os sistemas e serviços Web do que em outros horários, e o gráfico demonstra isso. O ambiente de teste não possuía nenhum sistema de gerenciamento de redes, portanto a análise dos dados foi feita de forma qualitativa, e tomando como partida alguns problemas encontrados no ambiente e como o sistema implementado foi capaz de auxiliar. A partir do auxílio da ferramenta foi possível monitorar serviços e dispositvos a fim de prever incidentes e tomar decisões que diminuíram ou eliminaram incidentes.

5 Conclusão

“As palavras fogem quando precisamos delas e sobram quando não pretendemos usá-las.”
Carlos Drummond de Andrade

A justificativa para o presente trabalho de pesquisa foi oferecer auxílio adequado à equipe de suporte e manutenção da rede, a partir da necessidade de se implementar sistemas automatizados de gerenciamento de redes em um ambiente corporativo. Este trabalho de pesquisa fez uma análise do ambiente da rede de uma grande instituição de ensino superior do Vale do Aço com o objetivo de propor um sistema com configurações e parâmetros que se adaptam a sua necessidade, conforme informações da equipe de suporte e manutenção. A partir deste trabalho foi possível visualizar, na prática, o funcionamento de ferramentas de gerência de redes e os benefícios que elas oferecem, tornando possível a prevenção e identificação de incidentes. Foram identificadas características potencialmente comuns aos ambientes corporativos, que possuem suas particularidades e necessidades específicas, e os resultados obtidos partiram de uma análise qualitativa após a implementação da ferramenta no ambiente de teste. Levou-se em conta as limitações das políticas de gerenciamento da instituição, e as restrições à alguns acessos.

A utilização das ferramentas de gerenciamento de redes, em qualquer ambiente corporativo, é fundamental para o bom funcionamento dos recursos computacionais, mantendo a organização e prevenindo incidentes. O estudo e análise das áreas de gerência de rede, dos protocolos, das ferramentas e dos parâmetros de gerenciamento de software e hardware que garantem os serviços de rede conduziram ao uso da ferramenta The Dude. Tudo isso tornou possível a tomada de decisões para diminuir ou eliminar alguns incidentes, como mostrado no Capítulo 4, melhorando a organização das informações para a equipe de suporte. A partir dos resultados foi possível analisar as causas de incidentes e criar uma política de grupo de desligamento automático dos computadores, mapear e identificar problemas em *switches*, monitorar a conexão de impressoras, além de links importantes que estabelecem a conexão com a Internet e o *status* de serviços essenciais como DNS e outros.

O presente trabalho de pesquisa apresentou algumas limitações para uma análise mais aprofundada de alguns serviços, devido a restrições de comunicação dos dispositivos em função da política local da corporação. Contudo, foi possível à equipe de suporte e manutenção analisar informações básicas e mais urgentes ou necessárias para o ambiente de teste.

Sendo assim, este trabalho de pesquisa conseguiu cumprir os objetivos estipulados que foram: implementar uma ferramenta de gerenciamento de redes utilizando o protocolo SNMP, para detectar possíveis incidentes no ambiente de teste; analisar as áreas de gerência de redes, que auxiliam na análise do que é necessário monitorar; analisar os protocolos e ferramentas que tornam possível o gerenciamento automatizado e por fim investigar princi-

pais parâmetros de gerência que visam melhorar a continuidade de serviços computacionais relevantes em um ambiente corporativo.

5.1 Trabalhos futuros

Como trabalhos futuros o estudo de outras configurações da ferramenta que atendam outras áreas de gerência de redes ou outros aspectos das áreas abordadas neste trabalho, podemos citar, por exemplo: a verificação de limites da utilização de recursos, verificação de usuários e grupos com acesso aos recursos, coleta de informações sobre a utilização, verificação de outros serviços em servidores e monitoramento de uso de discos, tendo em vista que estes são apenas alguns dos possíveis itens a serem estudados.

Referências

ABREU, F. R.; PIRES, H. D. Gerencia de redes. *Trabalho apresentado na Disciplina de Redes de Computadores I, Departamento de Engenharia de Telecomunicações, Universidade Federal Fluminense. Disponível em:< http://www. midiacom. uff. br/˜ debora/redes1/pdf/trab042/SNMP. pdf>. Acesso em*, v. 16, 2004. Citado nas páginas 18 e 21.

ALMEIDA, D. R.; ROHDEN, R. B. Utilizando o protocolo snmp para gerenciar ativos de rede no zabbix. *I Seminário de Pesquisa Científica e Tecnológica*, v. 1, n. 1, 2017. Citado na página 26.

BARROSO, D. M. *Gerência de redes de computadores: Serviços, Espaço em Disco e Falhas nos Agentes via SNMP*. 2008. Dissertação (B.S. thesis) — Faculdade de Tecnologia e Ciências Sociais Aplicadas, 2008. Citado na página 24.

BENICIO, W. E. P. Monitoramento e gerenciamento de redes utilizando zabbix. *Trabalho apresentado ao Curso de Análise e Desenvolvimento de Sistemas do Instituto Federal como requisito para obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas*, 2015. Citado na página 13.

BONOMO, E. *Gerenciamento e monitoração de redes de computadores utilizando-se Zabbix*. 2006. Dissertação (B.S. thesis) — Universidade Federal de Lavras, 2006. Citado nas páginas 21 e 24.

BRITO, S. H. B. *Interpretação dos Resultados do Ping*. 2013. Disponível em: <http://labcisco.blogspot.com/2013/05/interpretacao-dos-resultados-do-ping.html>. Acesso em: 13 agos. 2018. Citado na página 39.

CARNIELO, A.; OLIVEIRA, S. A. de et al. Gerenciamento descentralizado de rede com software livre. *Anais SULCOMP*, v. 7, 2015. Citado nas páginas 12, 15, 16, 17, 18 e 25.

CCMBENCHMARK. *Os protocolos de serviço de mensagens: SMTP, POP3 e IMAP4*. 2018. Disponível em: <https://br.ccm.net/contents/282-os-protocolos-de-servico-de-mensagens-smtp-pop3-e-imap4#>. Acesso em: 02 abr. 2018. Citado na página 24.

COMER, D. E. *Redes de Computadores e Internet 2 Ed.* São Paulo, Brasil: Bookman, 2001. Citado nas páginas 19 e 22.

COMER, D. E. *Redes de Computadores E Internet 4 Ed.* São Paulo, Brasil: Bookman, 2007. Citado nas páginas 17 e 18.

COMER, D. E. *Redes de Computadores E Internet 6 Ed.* São Paulo, Brasil: Bookman, 2016. Citado na página 12.

FACHINI, T. Implementação da ferramenta zabbix para monitoramento reativo. Canoas, RS, 2010. Disponível em: <http://memoria.rnp.br/newsgen/9901/rmon.html#inicio>. Acesso em: 08 Agos. 2017. Citado na página 12.

FEATHER, C. D. Network news transfer protocol (nntp). 2006. Disponível em: <https://tools.ietf.org/html/rfc3977>. Acesso em: 02 abr. 2018. Citado na página 24.

FOROUZAN, B. A. *Comunicação de dados e redes de computadores*. 4. ed. São Paulo, Brasil: AMGH Editora, 2008. Citado nas páginas 15, 18, 22, 36 e 37.

FOROUZAN, B. A.; FEGAN, S. C. *Protocolo TCP/IP*. 3. ed. São Paulo, Brasil: McGraw-Hill Companies, 2008. Citado na página 20.

GALLO, M. A.; HANCOCK, W. S. *Comunicação entre computadores e tecnologias de rede*. [S.l.: s.n.]. Citado na página 24.

INTERNET ENGINEERING TASK FORCE. Rfcs. 2006. Disponível em: <https://www.ietf.org/standards/rfcs>. Acesso em: 02 abr. 2018. Citado na página 19.

KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a Internet. Uma abordagem Top-Down*. 5. ed. São Paulo, Brasil: Pearson Addison Wesley, 2010. Citado nas páginas 13, 15, 16, 19 e 22.

LEMES, A. S. P. Análise de soluções abertas de gerenciamento de redes em relação ao padrão fcaps (itu-t m. 3400) de gerenciamento de redes. *Projetos e Dissertações em Sistemas de Informação e Gestão do Conhecimento*, v. 5, n. 2, 2017. Citado na página 26.

MEDEIROS, S. T. d. *Sistema de detecção automatizada de incidentes de redes decorrentes das mudanças nas configurações dos switches*. 2017. Dissertação (B.S. thesis) — Universidade Federal do Rio Grande do Norte, 2017. Citado nas páginas 13, 19, 22 e 25.

MIKROTIK. *The Dude*. Disponível em: <https://www.mikrotik.com/thedude>. Acesso em: 30 Agos.2018. Citado na página 25.

OLIFER, N.; OLIFER, V. *Redes de computadores: princípios, tecnologias e protocolos para o projeto de redes*. [S.l.]: LTC, GEN, 2008. Citado nas páginas 15, 18 e 23.

SAITO, J. T.; MADEIRA, E. Um modelo de gerenciamento de redes de telecomunicações utilizando a plataforma corba. In: *Simpósio Brasileiro de Redes de Computadores*. [s.n.], 2001. v. 20, p. 01. Disponível em: <http://www.lbd.dcc.ufmg.br/colecoes/sbrc/2001/009.pdf>. Acesso em: 05 Out. 2017. Citado na página 15.

SOUZA, A. V. de; LIMA, A. M. de. Implantação e gestão de rede wireless com hardware e software mikrotik. *Revista Científica da UNESC*, v. 14, n. 1, p. 70–81, 2016. Citado na página 27.

SYMANTEC. *NetBIOS*. 2017. Disponível em: <https://www.symantec.com/pt/br/security_response/glossary/define.jsp?letter=n&word=netbios>. Acesso em: 05 Jun. 2018. Citado na página 40.

TANEMBAUM, A. S. *Redes de computadores*. 4. ed. Rio De Janeiro, Brasil: Pearson Education, Inc, 2003. Citado na página 15.

TANEMBAUM, A. S. *Redes de computadores*. 5. ed. Rio De Janeiro, Brasil: Pearson Education, Inc, 2011. Citado na página 12.

TELECO. *Modelo TMN: Áreas Funcionais e Niveis de Gerência*. 2017. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialmodelotmn/pagina_4.asp>. Acesso em: 08 Agos. 2017. Citado nas páginas 19 e 22.