UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

ALISSON MADALENA FOGAÇA

UTILIZANDO OS SOFTWARES CACTI E NETEYE NO MONITORAMENTO DE ATIVOS DE REDES

CRICIÚMA

2014

ALISSON MADALENA FOGAÇA

UTILIZANDO OS SOFTWARES CACTI E NETEYE NO MONITORAMENTO DE ATIVOS DE REDES

Trabalho de Conclusão de Curso, apresentado para obtenção do grau de Bacharel no curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC.

Orientador: Prof. MSc. Paulo Martins

CRICIÚMA

2014

ALISSON MADALENA FOGAÇA

UTILIZANDO OS SOFTWARES CACTI E NETEYE NO MONITORAMENTO DE ATIVOS DE REDES

Trabalho de Conclusão de Curso aprovado pela Banca Examinadora para obtenção do Grau de Bacharel, no Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC, com Linha de Pesquisa em Redes de Computadores.

Criciúma, 26 de junho de 2014.

BANCA EXAMINADORA

Prof. Paulo João Martins – Mestre – (UNESC) – Orientador

Prof. Rogério Antônio Casagrande – Mestre – (UNESC)

Prof. Sérgio Coral – Especialista – (UNESC)

AGRADECIMENTOS

Agradeço primeiramente à Deus, por me proporcionar este momento de conquista. Agradeço também ao meu orientador, Mestre Paulo João Martins, por me incentivar e auxiliar ao longo deste projeto, e também aos demais professores do Curso de Ciência da Computação da Unesc.

Aos meus pais Carlos e Lucenir, que sempre me apoiaram nos estudos e nunca me deixaram abandona-los, garantindo que eu chegasse até aqui. À minha irmã Alice que é fonte de inspiração para que eu conseguisse alcançar a conclusão dessa graduação. À minha namorada Gabriela que me incentivou em todos os momentos de dificuldades nesta jornada.

Aos meus amigos e familiares que entenderam as minhas diversas ausências da vida social. Por fim, à todas as pessoas que me ajudaram e me apoiaram ao longo desta caminhada.

“A maneira como você coleta, gerencia e utiliza as informações determina se você vai vencer ou perder.”

Bill Gates

RESUMO

As redes de computadores tornaram-se grandes e complexas com o passar dos tempos, neste caso é importante que haja uma gerência bem definida para garantir que os recursos utilizados estejam sempre disponíveis. Atualmente uma rede de computadores que não há um monitoramento e controle tende a ser prejudicial à sua organização, pois os usuários que a utilizam ficam expostos a instabilidades e insegurança. Porém existem inúmeros softwares capazes de amenizar estes problemas, onde é necessário estudar qual o que melhor se aplica à rede implementada. As aplicações gerenciais necessitam de um protocolo para que as requisições de informações entre servidor e cliente seja entendida e respondida. O protocolo mais utilizado para este é o Simple Network Management Protocol. Com o objetivo de entregar um monitoramento e controle da rede confiáveis ao administrador, este projeto implementa em um único ambiente a utilização dos softwares Cacti e NetEye aplicados à gerencia através do protocolo SNMP. No ambiente foram simulado algumas rotinas ocorridas em uma rede organizacional, onde foi possível realizar um estudo das funcionalidades das ferramentas utilizadas. Através dos estudos realizados foi possível compreender e aplicar os conceitos de redes e de sua gerência, definindo assim uma estrutura de teste capaz de levantar resultados para uma análise e comparação. Estes testes e métricas retornaram resultados que demonstraram que as aplicações são ótimas para a administração, porém existindo diversas funções distintas onde ambas se completam. Concluindo-se que a utilização de ambas em conjunto pode proporcionar ao gerente da rede resultados melhores e mais completos.

Palavras-chave: Redes de computadores. Gerenciamento. Cacti. NetEye. SNMP.

ABSTRACT

The computer network became large and complex over the time. Thereforth, it is very important to have a well-defined management to ensure that used resources be always available. Currently, a computer network that does not have monitoring and control tends to be prejudicial to its organization. That is because the users who use the network are exposed to instability and insecurity. However exist uncountable softwares able of soften these problems, where it is necessary to study what best fits the needsof the implemented network. The management applications require a protocol to assure that the information requests between server and client are understood and answered. The protocol more used to do this is Simple Network Management Protocol. With the goal of delivering a reliable network monitoring and control to the administrator, this project implements in just one environment the use of the softwares Cacti e NetEye. These are used in the management through the SNMP protocol. In the environment was simulated some routines occurring in a organizational network, where it was possible to perform a study of used tools' functionality. Through the performed studies it was possible to understand and apply the network concepts and the management involved, defining a test structure that was able to lift the results towards an analysis and comparison. These tests and metrics returned results demonstrating that these applications are great for administration, although there were several distinct functions where both complemented each other. From that, it was possible to reach the conclusion that the use of both softwares together can provide to the network manager more complete information as better results.

Keywords: Network computer. Management. Cacti. NetEye. SNMP.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

CMIP/CMIS	*Common Management Information Protocol / Common Management Information Service*
GNU	*General Public License*
HEMS	*High-Level Entity management System*
IETF	Internet Engineering Task Force
IP	*Internet Protocol*
ISO	*International Organization for Standardization*
MIB	*Management Information Base*
MIT	*Massachusetts Institute of Technology*
MSDE	*Microsoft SQl Server Desktop Engine*
NMS	*Network Management Systems*
OSI	*Open Systems Interconnection*
PC	*Personal Computer*
PDU	*Protocol Data Unit*
SNMP	*Simple Network Management Protocol*
TCP	*Transmission Control Protocol*
TMN	*Telecommunications Management Network*

SUMÁRIO

1 INTRODUÇÃO

À medida que a tecnologia evolui, a capacidade de coletar, processar e distribuir informações aumenta. Isto segue uma linha de que toda essa demanda cresça ainda mais, sendo inerente que novas e antigas formas de processamento destes dados tornem-se mais aprimoradas. Sendo assim, em uma organização onde o processamento das rotinas era realizado em apenas uma máquina, agora passou a ser feito por uma rede de computadores, nos quais todas as tarefas são divididas entre vários dispositivos de diferentes locais, entretanto estando todos interconectados.

Este foi o início para que a rede de computadores fosse implementada, onde facilitou o alcance de informações que se encontravam em locais distante fisicamente (TORRE, 2001). O termo rede já é algo utilizado antes mesmo das primeiras máquinas existirem, pois este conceito se aplicava em redes de energia, telégrafos, entre outras. Porém a de computadores só foi implantada de fato quando os primeiros computadores pessoais (PC) foram colocados no mercado. Com a junção de todos esses elementos, as redes ganharam novas padronizações e tecnologias, que permitiram uma comunicação melhor e mais otimizada, até mesmo os custos foram amenizados.

Há dois tipos básicos em que as redes podem ser divididas perante a forma que o compartilhamento de dados é realizado, uma chamada de ponto-a-ponto, utilizadas apenas em pequenas redes, e outra chamada cliente/servidor, bastante usada em grandes redes. Dentre alguns componentes que compõe as redes estão as placas de rede, os cabos que são responsáveis pela interligação dessas placas, há as topologias, que se refere à maneira em que as máquinas são interligadas, e diversos outros dispositivos necessários para a comunicação chamados de ativos.

Com o aumento do tráfego de informações e a quantidade de dispositivos em uma rede, a complexidade de gerir todos estes elementos também aumentou, surgindo assim a necessidade de gerenciar e monitorar essas informações. A principal ideia no gerenciamento era o de organizar e amenizar possíveis falhas e defeitos que possam levar a interrupção de serviços e compartilhamentos de informações.

Alguns dos objetivos da gerência de rede são o de realizar um controle e

monitoramento de seus elementos, a fim de garantir os serviços dentro de um padrão aceitável de qualidade. Porém antes da chegada do gerenciamento, os problemas ocorridos na rede eram tratados de maneira manual, ou seja, o administrador analisava o erro, realizava os ajustes necessários no sistema e então reiniciava o software ou hardware. Atualmente este meio manual pode ser substituído por aplicações e conjuntos de ferramentas que auxiliam essa monitoração e controle. Estes softwares apresentam funções que demonstram todas as informações sobre a rede, além possibilitar a execução de grande parte das rotinas administrativas.

Existem alguns modelos de gerenciamento referente à organização de todos os processos que o envolve, onde o FCAPS é o modelo voltado para a estruturação do gerenciamento de computadores. Sendo este é o modelo utilizado neste projeto.

A troca de dados entre as entidades, dispositivos que podem enviar ou receber informações, é realizada a todo momento, porém para que a informação enviada seja compreendida por outra entidade precisa-se que haja um padrão. O termo utilizado para tanto é o protocolo, no qual consiste em uma coleção de regras que controlam a comunicação de todo o tráfego na rede.

A grande complexidade de gerenciamento de uma rede também levou a necessidade de se criar um padrão, onde para este caso foi criado o protocolo *Simple Network Management Protocol* (SNMP). Este protocolo é um conjunto de operações administrativas que podem alterar as informações dos dispositivos, sendo nele onde a grande parte das aplicações de gerenciamento baseiam suas funcionalidades.

Existem inúmeros softwares para gerenciar uma rede, sendo que para a realização deste projeto foram escolhidos dois, o Cacti e o NetEye. A ferramenta NetEye por ser proprietária requer alguns custos para sua aquisição, porém existem versões para testes. Essas aplicações definidas tem capacidades e funcionalidades promissoras para amenizar e controlar os problemas ocasionados em uma rede. Sendo que através de um ambiente propício o estudo de caso realizado procurou explorar estas funções, analisando os resultados obtidos e as técnicas gerenciais utilizadas.

1.1 OBJETIVO GERAL

Analisar e comparar os resultados obtidos durante o gerenciamento e monitoramento dos ativos de redes com o software livre Cacti e o software proprietário NetEye.

1.2 OBJETIVO ESPECÍFICOS

Os objetivos específicos desta pesquisa consistem em:

a) compreender e aplicar os conceitos de redes e sua estrutura;
b) descrever e implementar as técnicas para gerenciar-se uma rede;
c) utilizar as diversas funcionalidades dos softwares Cacti e NetEye na gestão e monitoração de redes;
d) definir e estruturar alguns casos de testes aplicados ao gerenciamento de redes para análise detalhada dos softwares;
e) analisar e comparar os resultados dos procedimentos de testes utilizados.

1.3 JUSTIFICATIVA

As redes de computadores ganharam um poder de processamento e desempenho incríveis em um curto período de tempo, ampliando seus conjuntos de serviços, onde acarretou também em um grande aumento no nível de complexidade e dificuldade de realizar o gerenciamento. Neste crescimento é praticamente normal a ocorrências de falhas e problemas, os motivos são vários como entidades mal configuradas, a utilização de recursos em grande escala ou até mesmo por determinados dispositivos apresentarem defeitos com o tempo.

O impacto de uma dessas falhas pode ser financeiramente grande em casos empresariais, onde aliando-se à uma má gestão na rede, a perca pode se tornar ainda pior, pois quanto maior o tempo em que o problema demora para ser solucionado, maior o tempo em que a mesma ficará limitada ou sem funcionamento.

Para que estes problemas sejam amenizados é preciso que haja o processo de controle de hardware e software, onde é necessária uma pessoa

responsável por configurar, monitorar, dentre outras tarefas em torno das análises das informações de todos os recursos disponíveis. Esses processos garantem que a rede estará com um desempenho seguro e serviços de qualidades dentro de um padrão aceitável.

Existe um modelo para o gerenciamento de redes criado pela *International Organization for Standardization* (ISO), que visa organizar e estruturar as normas e processos que implica a gestão. O modelo é chamado de FCAPS, sendo utilizado neste projeto, onde engloba os conceitos de gerenciamento de desempenho, de falhas, de configuração, de contabilização, e de segurança (SCHAEFER, 2007).

A redes de computadores tornaram-se indispensável para o bom funcionamento das tarefas de uma organização. A boa entrega dos serviços está totalmente associada ao bom monitoramento e controle dos recursos da rede. Para que seja possível realizar o gerenciamento é necessário um grupo de ferramentas. Existe uma grande variedade de aplicações para este fim, e elas reúnem os recursos citados e, quando bem configurados e utilizados, são capazes de realizar todas as atividades para assegurar uma rede em pleno funcionamento, agregando atributos capazes de garantir estabilidade e desempenho.

Analisando o mercado foi encontrado diversos softwares para realizar esta gerencia, porém levando em conta a usabilidade e as possibilidades de monitoramento, foi escolhido a ferramenta livre Cacti pela sua capacidade de geração de gráficos estatísticos e possibilidade de adição de complementos que aumentam sua funcionalidade e a proprietária NetEye, que possui um diferencial no controle e na segurança da rede.

Com a grande quantidade de ferramentas nesta área, a escolha do mais adequado pode ser complicada em algumas situações. Sendo assim através de um estudo de caso dos softwares citados procurou-se levantar as informações de uma instalação e configuração correta, além de apresentar as suas diferentes funcionalidades no gerenciamento da rede.

Através deste estudo será possível auxiliar os administradores a selecionar a ferramenta que melhor se adequa ao seu ambiente utilizado, demonstrando os processos necessárias para a implantação de uma gerência, além de ajudar na resolução dos problemas e dificuldades do monitoramento e controle de uma rede.

1.4 ESTRUTURA DO TRABALHO

O projeto é formado por seis capítulos que apresentam as métricas e etapas realizadas. O primeiro demonstra a introdução para o assunto abordado, o objetivo geral, os objetivos específicos que se buscou alcançar e a justificativa para a realização do projeto.

No segundo capitulo é descrito os conceitos relacionados ao gerenciamento de rede, onde é exposto seu histórico e funcionamento. O terceiro capitulo é dedicado ao protocolo de rede SNMP, elencando suas principais características, as funções de acordo com suas respectivas versões e também posto seu funcionamento.

Já no quarto capítulo é realizado um apanhado geral dos softwares utilizados no projeto, o Cacti e o NetEye. Onde é apresentado informações do desenvolvimento de cada um, suas funcionalidades e os requisitos necessários para suas utilizações.

O quinto relata trabalhos realizados na mesma área que este projeto e seus resultados. No sexto e último capitulo é demonstrado o trabalho desenvolvido, assim como os testes realizados e os resultados obtidos.

2 GERENCIAMENTO DE REDES

As redes de computadores atualmente possuem uma grande diversidade de modelos, de topologias, diferentes equipamentos, meios de transmissão, dentre diversas outras configurações que podem ser aplicadas nas redes. Essa evolução da rede foi realizada durante anos, tudo para melhorar os processos e utilização das redes, permitindo que a comunicação dos dispositivos chegasse a níveis de complexidades muito altos.

Com o objetivo de organizar e estruturar as redes, necessitou-se gerenciar e monitorar toda essas interconexões de computadores, passando por seus hardwares e softwares. A ideia tomou como base o intuito de organizar e amenizar possíveis falhas e defeitos que possam levar a interrupção de serviços e compartilhamentos de informações (KUROSE; ROSS, 2006).

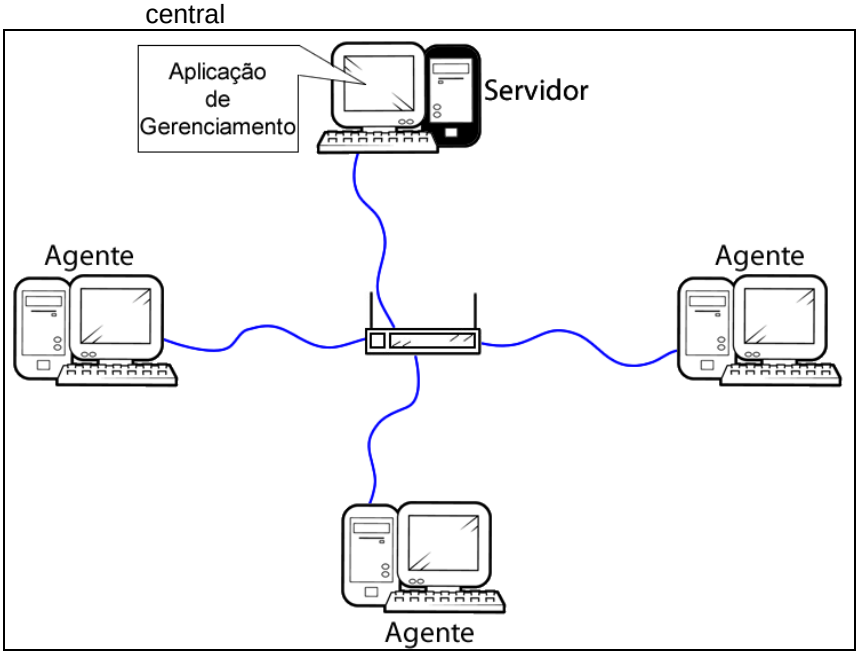
Toda essa complexidade que envolve uma rede de interconexões de entidades, gerenciá-la e monitorá-la garantindo que todos os seus dispositivos estão em execução e em pleno funcionamento pode parecer difícil. Porém através de softwares de gerenciamento adequados e um pouco de conhecimento nas configurações necessárias para uma rede funcionar sem problemas, torna esta tarefa muito mais fácil e simples (MAURA; SCHIMIDT, 2001).

Todavia o gerenciamento da rede sem a utilização de uma ferramenta para isto, pode tornar-se uma escolha pior que a não gerência, pois a busca por uma solução de um determinado problema ocasionado na rede, poderá ocasionar em diversos outros. Por isso o aconselhável é a realização do monitoramento e controle da rede através de softwares focados neste quesito (MOQADI, 2011).

Segundo Stallings (1998, tradução nossa), com a diversificação e a expansão da computação, há grandes quantidades de aplicações e conjuntos de ferramentas para o auxílio na monitoração e controle de uma rede. Estes softwares apresentam funções que demonstram todas as informações sobre a rede, além de possibilidades de executar grande parte das tarefas em relação à gerência.

Na figura 01 é possível observar uma rede pequena com alguns equipamentos conectados e um servidor central, no qual possui uma aplicação de gerência de redes e através dela monitora e controla todas as informações processadas na rede.

Figura 01 - Estrutura de uma rede de computadores com um servidor central



Fonte: Adaptado de Moqad (2011).

A realização desta administração da rede, tem como objetivo analisar o funcionamento inteiro dos dispositivos disponíveis, suas tarefas exercidas, seus processos, sua comunicação, todas as suas tarefas relacionadas a rede. Também proporciona à rede uma boa produtividade, pois não há a preocupação dos usuários em problemas que possam ocasionar em sua rede, pois através do monitoramento bem realizado a tendência é a diminuição significativa dos erros de rede e a resolução rápida dos mesmos (PINHEIRO, 2002).

2.1 HISTÓRICO

O gerenciamento evoluiu paralelamente com a rede de computadores, onde a rede tomou grandes proporções e aumentou seu nível de complexidade, assim obrigatoriamente precisou-se gerenciar e monitorar toda essa interconexão de computadores, passando por seus hardwares e softwares (KUROSE; ROSS, 2006). A ideia tomou como base o intuito de organizar e amenizar possíveis falhas e defeitos que possam levar a interrupção de serviços e compartilhamentos de informações.

O conceito de gerência começo a ser discutido no início da década de 1980, porém ainda não havia uma ideia concreta do como e o que seria implantada para este fim. E enquanto a gerência não saia apenas de uma vaga ideia, a rede de

computadores continuava a ficar mais complicada e de difícil administração (DUARTE, 2005).

Esta dificuldade de gerenciá-la e monitorá-la garantindo que todos os seus dispositivos estão em execução e em pleno funcionamento era muito grande, pois levando em conta as diferentes arquitetura que cada fabricante colocava em seus hardware e software, ficava quase impossível administrar sem que houvesse uma padronização (MAURA; SCHIMIDT, 2001).

Almejando esta padronização, foi criado no final da década de 1980 o protocolo SNMP, no qual possibilitou a comunicação entre todos os dispositivos, mesmo que fossem de diferentes fabricantes (DUARTE, 2005).

Diversas outras opções de protocolos foram criados, dentre alguns destacaram-se o *Hight-Level Entity Management System* (HEMS), o SNMP, o CMOT, dentre outros. Porém padronização necessária só veio a ocorrer no final da década de 1980, quando foi lançado o protocolo SNMP, no qual possibilitou a comunicação entre todos os dispositivos, mesmo que fossem de diferentes fabricantes (DUARTE, 2005).

Este foi o início dos conceitos de gerenciamento de redes de computadores, que ao longo dos anos foi evoluído e ganhando novas funcionalidades que possibilitaram a ela tomar sua total importância em uma implementação de rede. A rede que não possui um sistema de gerenciamento, com certeza está rede está tecnicamente incompleta e sujeita a diversos problemas que possam interromper seu funcionamento.

2.2 ARQUITETURA

A arquitetura do gerenciamento de rede é aplicável indiferente do modelo de rede adotado, onde ela se dividi em quatro importantes elementos. O dispositivo cliente, chamado de agente, o servidor, chamado de gerente, a tabela onde é armazenado as informações dos equipamentos, chamado de *Management Information Base* (MIB), e o padrão utilizado na comunicação, chamado de protocolo de gerenciamento (PINHEIRO, 2002).

Uma arquitetura bem planejada e organizada visa a amenização de problemas, erros e eventos que venham a ocasionar o mal funcionamento da rede ou até a sua paralisação. Pois quando uma rede é bem gerenciada, aumenta sua

segurança, sua integridade dos dados e otimiza todo o trafego gerado através de recursos e serviços (PINHEIRO, 2002).

Os agentes são considerado os dispositivos que estão dispersos na rede que possam ser gerenciados, nos quais executam a aplicação cliente do software de gerenciamento utilizado na rede. Pois é através deste modulo cliente que será possível realizar as funções de monitoração e controle exercidas pelo servidor (ABREU; PIRES, 2013).

Esses agentes são os responsáveis pelo compartilhamento de recursos e informações, e também pela geração de trafego na rede, pois a cada acesso a esses dados compartilhados é gerado um determinado trafego. Não há um limite de agentes, porém cada ferramenta de gerência tem sua própria limitação, cabendo ao administrador analisá-la e estudá-la (ABREU; PIRES, 2013).

Os gerentes são os dispositivos no qual possuem o software de gerência de rede instalado. Sendo estes os responsáveis por administrar todos os equipamentos dispersos pela rede. Essas aplicações possuem diversas funções que são executadas em conjunto com seu equipamento para que o controle da rede possa ser realizado completamente (PINHEIRO, 2002).

O gerente e o agente são os dois únicos elementos da arquitetura da gerência de rede em que o usuário e o administrador terão contato direto. Onde o software gerencial auxiliá-la em todo este uso, evitando assim problemas decorrentes de uma má utilização (MAURA; SCHMIDT, 2001).

A tabela MIB é o local onde é armazenada todas as informações recolhidas através de requisições do gerente. Este local é um banco de dados onde é possível controlar todos os agentes da rede. Todas as informações dos equipamentos da rede podem ser acessada através das ferramentas de gerência da rede na tabela MIB. Onde há as informações dos arquivos e recursos compartilhados na rede. Normalmente esta tabela é utilizada em conjunto com o protocolo SNMP (MAURA; SCHMIDT, 2001).

O protocolo de gerenciamento da rede é o responsável por permitir a realização da comunicação entre os gerentes e os agentes, pois define um padrão no qual essa comunicação acontecerá. O protocolo normalmente utilizado para tanto, é o SNMP, no qual é base das funcionalidades das diversas ferramentas administrativas existentes no mercado (MAURA; SCHMIDT, 2001).

A partir do entendimento dos elementos da estrutura do gerenciamento de rede é possível organizar e implementar uma administração de rede correta. Definindo as aplicações a serem utilizadas, em quais equipamentos as mesmas funcionaram e também os dispositivos agentes que serão gerenciados a partir destas.

2.3 TIPOS

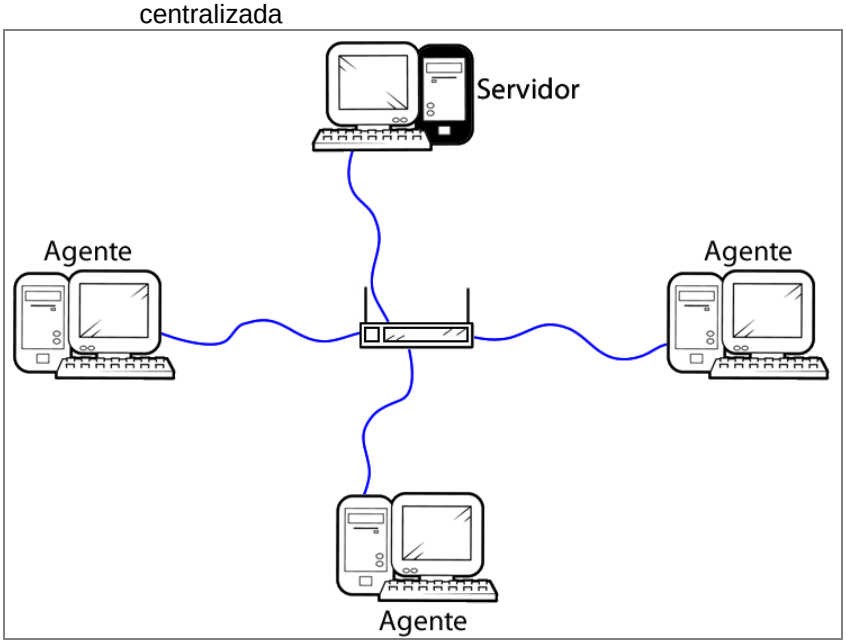
A classificação das redes gerenciadas de acordo com a disposição dos gerentes e agentes na rede, pode ser realizada em basicamente duas, sendo o gerenciamento centralizado e o distribuído. Cada qual possui suas peculiaridades, sendo importante entendê-las para definir a que melhor se aplica na rede implementada (PINHEIRO, 2002).

O funcionamento da gerência centralizada é caracterizada por possuir apenas um gerente na rede toda, onde neste é atribuída todas as funções de monitoração e controle dos agentes distribuídos na rede. O equipamento que possui a aplicação servidora é na qual o administrador da rede poderá exerce as funções gerenciais de rede (OLAVO FILHO, 2013).

Um problema da gerência centralizada é que a medida que a rede cresce a dificuldade de gerenciar todos os seus ativos também aumenta, ficando algumas vezes inviável utilizar este tipo de gerência (MADEIRA, 2012).

A figura 02 demonstra uma rede que possui um gerenciamento centralizado, onde um único servidor controla todas as operações dos dispositivos na rede.

Figura 02 - Estrutura de uma rede de computadores gerência centralizada



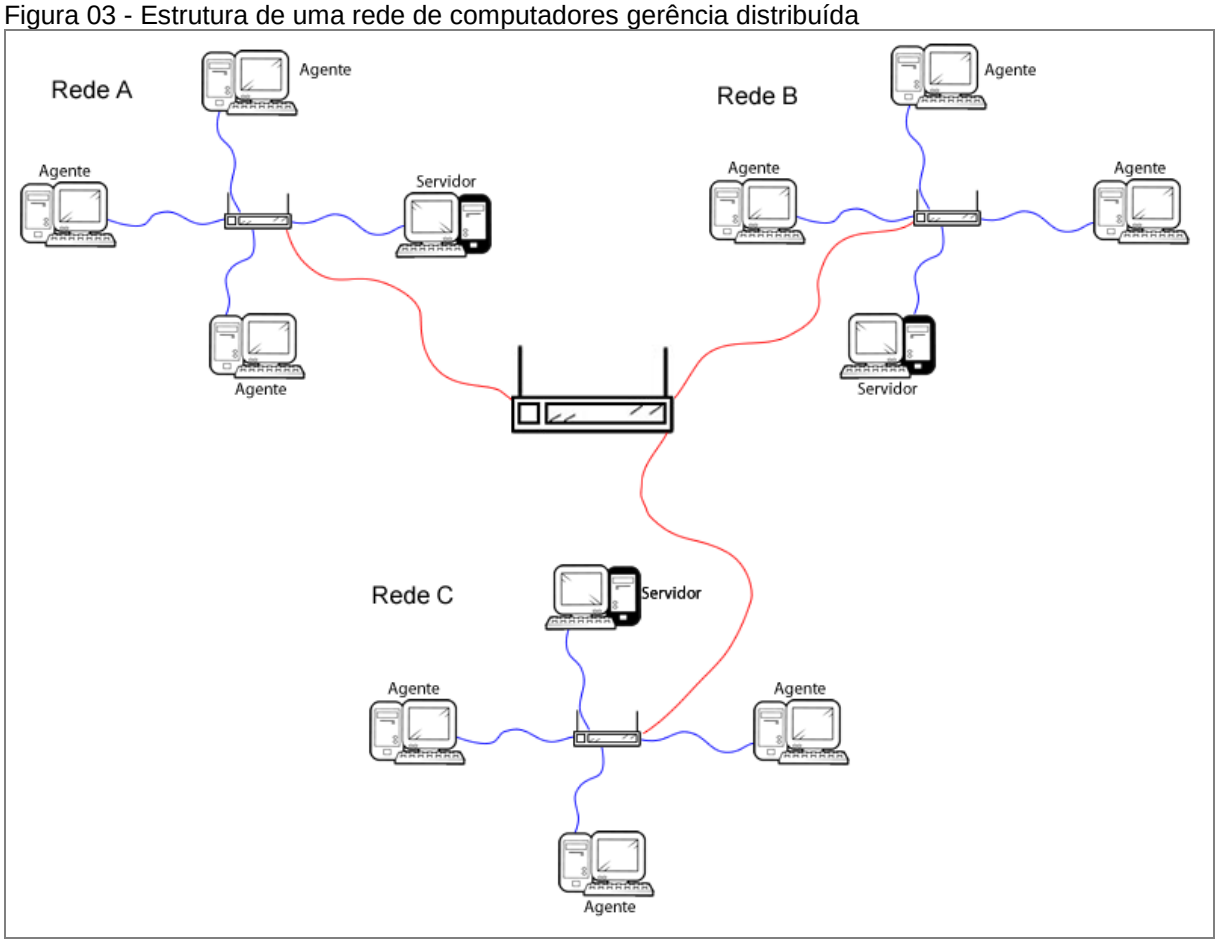
Fonte: Adaptado de Pinheiro (2011).

O modo de gerência distribuído possui o foco de dividir todas as tarefas referentes a administração da rede. Neste tipo de gerência não existe um servidor único e central como no gerenciamento centralizado, mas vários equipamentos que exercem este papel de controle e monitoração (OLAVO FILHO, 2013).

Cada gerente é responsável por um determinado conjunto de dispositivos, onde esta definição pode ser realizada dependendo de sua localização, quantidade de máquinas, dentre outras possibilidades. Portando este conjunto de equipamentos será seu grupo e a sua gerência deverá ser realizada apenas nesses dispositivos (PINHEIRO, 2002).

A figura 03 demonstra uma rede que possui um gerenciamento distribuído, onde vários servidores controlam em conjunto todas as operações dos dispositivos na rede.

Figura 03 - Estrutura de uma rede de computadores gerência distribuída



Fonte: Adaptado de Pinheiro (2011).

O gerenciamento de redes pode ser realizado de várias formas, utilizando softwares diferentes, protocolos distintos, e diversas maneiras de administrá-la, porém é preciso avaliar qual as ferramentas que são aplicáveis a rede gerenciada. É o caso do tipo de gerenciamento a ser utilizado, no qual deve ser avaliado pelo administrador da rede, levando em consideração a quantidade de computadores gerenciáveis que estarão conectados, afim de analisar a sua possibilidade de crescimento. Este planejamento pode evitar diversos dos problemas ocasionados pelo má administração.

2.4 FUNCIONAMENTO

O gerenciamento de rede possui o objetivo de disponibilizar todas as ferramentas necessárias para que o administrador da rede possa exercer as funções de monitoração e controle da rede. Realizando a configuração dos equipamentos, o

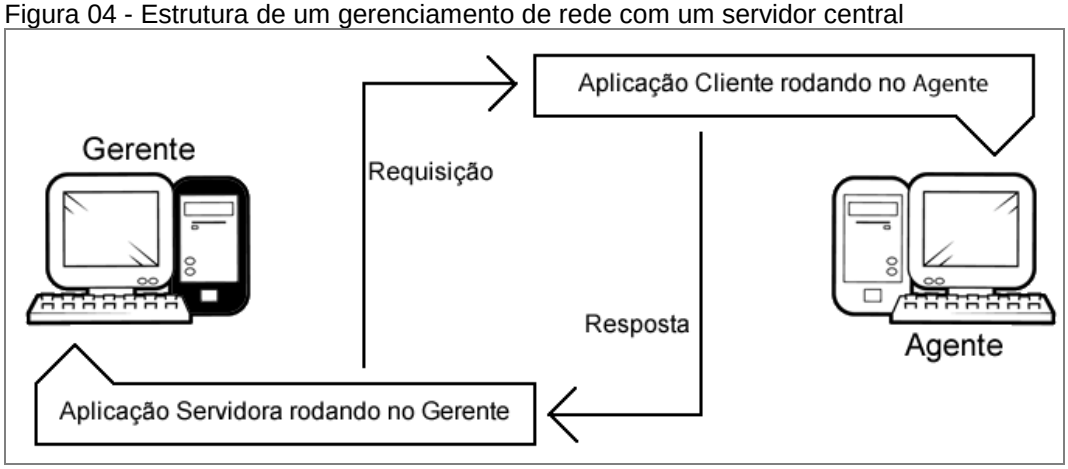
controle do trafego gerado pela rede, a monitoração de falhas e erros, a análise dos recursos, dentre diversas outras tarefas (RIBEIRO; GERK, [s.d]).

Como visto anteriormente a arquitetura da gerência de redes possui quatro elementos, onde através do gerente, do agente, da base MIB e do protocolo é possível colocar em prática os conceitos de uma administração correta. Para um funcionamento correto da rede todos esses elementos precisam funcionar em conjunto (PINHEIRO, 2002).

O administrador de rede é o responsável direto por analisar se todas essas ferramentas da gerenciais estão funcionando de corretamente. Pois qualquer anormalidade em uma das aplicações, poderá ocasionar erros, e o que possuía a função de evitar os problemas na rede, pode torna-se a causa deles (LOPES et al., 2009). Um bom gerenciamento de rede passa por um bom software, evitando assim diversos erros (PINHEIRO, 2010).

A figura 04 demonstra a estrutura de um gerenciamento de rede, com um agente e apenas um gerente centralizado, no qual realiza através de uma aplicação gerencial o controle da rede.

Figura 04 - Estrutura de um gerenciamento de rede com um servidor central



Fonte: Adaptado de Pinheiro (2010).

Ao menos uma máquina na rede deve possuir a tarefa de controlar a rede, este controle é feito através das aplicações gerenciais, onde através de uma interface é possível exerce as funções de administração da rede (LOPES et al, 2009).

Essas tarefas são na maioria das vezes realizadas através do protocolo SNMP, que auxilia na comunicação entre gerente e agente. O protocolo é

configurado na rede com o auxílio dos softwares gerências, pois o mesmo já possui este protocolo em suas funcionalidades (MAURA; SCHMIDT, 2001).

O gerente realiza uma determinada requisição ao agente por meio de sua ferramenta administrativa, o agente recebe está solicitação e analisa também por meio da ferramenta administrativa, porém com o seu modulo cliente, por fim a solicitação é respondida ao gerente. Este comportamento funciona tanto para solicitações de informações quanto para definição das mesmas, onde a comunicação é possível graças ao protocolo gerencial utilizado (LOPES et al, 2009).

A figura 05 apresenta o funcionamento da gerência de rede através de apenas um gerente que realizar uma requisição ao agente.

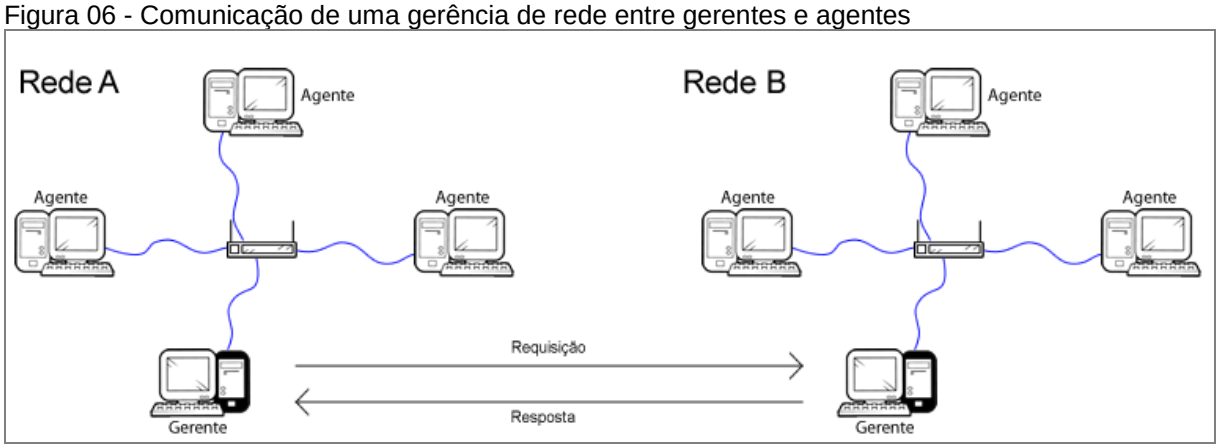
Figura 05 - Comunicação de uma gerência de rede entre gerente e agente

Fonte: Adaptado de Lopes et al. (2009).

O funcionamento também se difere de acordo com o número de gerentes definidos, pois quando existem mais de um servidor monitorando a rede, é preciso realizar a comunicação entre eles. Esta comunicação se faz necessária para que as informações e recursos de dispositivos gerenciados por outro gerentes possam ser acessadas (LOPES et al, 2009).

A figura 06 demonstra o funcionamento da gerência de rede com a utilização de dois servidores, no qual um solicita ao outro uma informação de seu agente.

Figura 06 - Comunicação de uma gerência de rede entre gerentes e agentes



Fonte: Adaptado de Lopes et al(2009).

Este funcionamento descrito é baseado na utilização do protocolo SNMP. O administrador da rede tem a obrigação de verificar se todos esses elementos estão em perfeito funcionamento, pois isto é necessário para que a realização da monitoração e controle da rede sejam seguros e completos.

2.5 MODELOS

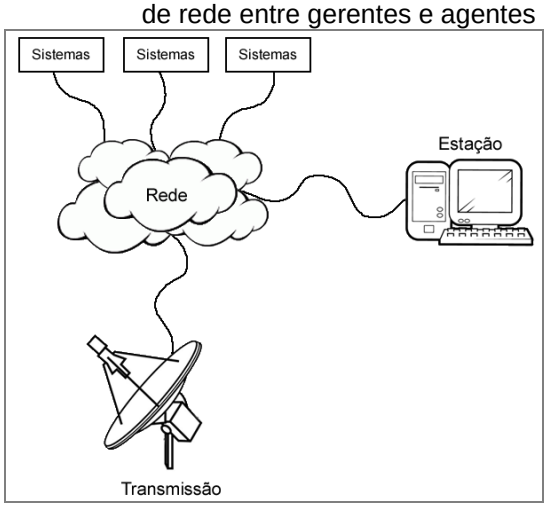
Existem alguns modelos para que o gerenciamento de redes possa ser realizado, dentre eles destacam-se o modelo FCAPS, o modelo *Telecommunications Management Network* (TMN) e o modelo *Common Management Information Protocol / Common Management Information Protocol* (CMIP/CMIS). Estes modelos tem por objetivo estruturar as maneiras de gerenciamento de uma rede, apresentando vários modos de administração (MOQADI, 2011).

O modelo TMN conceitua-se por possuir uma arquitetura estruturada e organizada, onde as aplicações e equipamentos de telecomunicações possam se comunicar e trocar recursos, afim de que o funcionamento em grupo de todos possa ocorrer (SORTICA, 1999).

Este modelo é largamente utilizado em redes de telecomunicações, em funções como o de planejamento, suporte e administração. Sua arquitetura baseia-se em três níveis, o nível físico, de informação e funcional, onde todos esses níveis trabalham em conjunto para que gerência de redes possa ser realizada (SORTICA, 1999).

A imagem 07 demonstra o funcionamento básico do modelo de gerenciamento TMN em uma rede de telecomunicações.

Figura 07 - Comunicação de uma gerência de rede entre gerentes e agentes

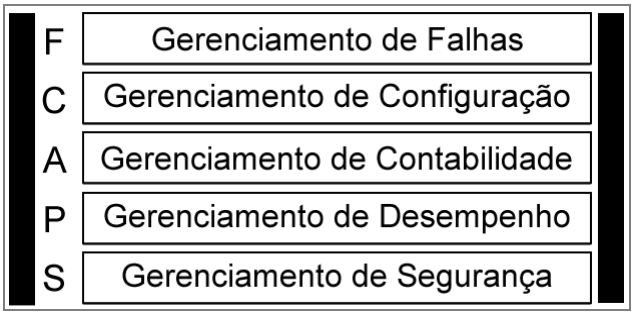


Fonte: Adaptado de Sortica (1999).

O modelo FCAPS foi criado pala *International Organization for Standardization* (ISO) com o objetivo de estruturar as várias situações de gerenciamento em uma rede. Neste modelo a gerência foi dividida em cinco áreas, sendo elas o gerenciamento de falha, de configuração, de contabilidade, de desempenho e de segurança (MOQADI, 2011).

A figura 08 demonstra todos os níveis de gerenciamento aplicáveis ao modelo FCAPS.

Figura 08 - Estrutura de camadas do modelo FCAPS



Fonte: Adaptado de Moqadi (2011).

No gerenciamento de falhas é a busca por falhas e correções, evitando que a rede fique sem trabalhar por muito tempo. Neste gerenciamento a monitoração de todos os equipamentos da rede é a melhor maneira de gerenciamento (MOQADI, 2011).

O gerenciamento de configuração é responsável pelo suporte as definições dos dispositivos, através de manutenções e monitorações de seu

hardware e software. Este gerenciamento é realizado por meio da coleta e análise de dados configuráveis dos equipamentos (MACIEL, 2012).

O gerenciamento de contabilidade é referente a parte burocrática da rede, ou seja, a análise dos acessos dos usuários aos recursos das entidades. Este gerenciamento é realizado através de privilégios entregues aos usuários, onde é possível realizar a limitação de acesso (MACIEL, 2012).

No gerenciamento de desempenho, o objetivo é controlar e analisar o desempenho dos equipamentos da rede. Esta análise é realizada através dos tráfegos gerados na rede, o comportamento e disponibilidade dos dispositivos, a taxa de erros ocorridas, dentre os atrasos da rede, e diversas outros pontos relacionados a otimização da rede (MOQADI, 2011).

O gerenciamento de segurança tem por objetivo garantir a integridade dos dados e seus usuários, controlando as políticas aplicadas a rede. Este gerenciamento é realizado através de monitoração e controle de acesso, analisando o trafego de arquivos e recursos, afim de assegurar a segurança dos mesmos (MACIEL, 2012).

O modelo CMIP/CMIS é um padrão de gerência utilizado, assim como o TMN, por sistemas de telecomunicações, auxiliando em seu planejamento (MENEZES; SILVA, 1998).

Estes são apenas alguns exemplos dos modelos de gerenciamento de que podem ser adotados em uma rede. Porém deve-se analisar o modelo que melhor se aplica a rede que será implementada.

2.6 APLICAÇÕES

No mercado atual existem inúmeras aplicações disponíveis para o gerenciamento de rede. Onde cada qual possui suas funcionalidades especificas, suas vantagens e desvantagens. Essas ferramentas estão em constantes evoluções, pois a medida em que a rede de computadores cresce e ganha novas possibilidades, o meio para monitorá-la também tende a evoluir (MATOS, 2006).

As ferramentas de rede possuem três requisitos mínimos para a classificação, sendo eles a apresentação, que é como as opções dos softwares são dispostas, o gerenciamento, no qual diz respeito a capacidade de execução, e o suporte, sendo em quais sistemas ele pode ser instalado (BARRETO, 2008).

Existem diversas ferramentas no mercado para gerenciar uma rede, alguns exemplos são Nagios, Zabix, OpenNMS, Cacti, NetEye, dentre outras opções existentes no mercado.

A ferramenta Nagios é voltada para a monitoração dos tráfegos da rede gerado através de serviços, onde esses serviços monitorados, podem ser pré configurados através da aplicação. Suas opções e funcionalidades podem ser acessadas diretamente através de um navegador web, onde possibilita configurar e analisar todas as informações referente a rede (NAGIOS, 2013).

O Zabbix é uma ferramenta gratuita que disponibiliza diversas opções de administração de rede como a geração de relatórios, sistema de notificações por e-mail, além de possuir toda as funcionalidades que o protocolo SNMP proporciona (ZABBIX, 2013).

Um outro exemplo de aplicação para a realização do gerenciamento de rede é o HP Open View Network Node Manager, que possibilita o gerenciamento completo de uma rede, mesmo que esta possua centenas de dispositivos conectados e tenha um alto grau de complexidade em suas conexões. Entre suas funcionalidades destacam-se o registro de falhas, alarmes de erros, demonstração clara dos dispositivos na rede, dentre outras (GUTHIERE, 2004).

A aplicação OpenNMS é totalmente gratuita, e se caracteriza pelo funcionamento remoto, pois permite que o administrador acessa os dispositivos remotamente. Utilizando-se do protocolo SNMP, ele permite o recebimento de notificações quando algo anormal ocorrer na rede, onde essas notificações podem ser modificadas conforme necessidade. Existe também as funções de emissão de relatórios apurados acerca da rede gerenciada (OPENNMS, 2013).

Uma outra aplicação gerencial é a ferramenta brasileira Cacic, que foi desenvolvida pela DataPrev. Ele é caracterizado por possui uma espécie de inventário, onde é descrito todos os equipamentos disponíveis na rede, apresentado informações de software, hardware, patrimônio, entre outras numerações e recursos (CACIC, 2013).

O Cacti se destaca por ser um software gratuito e por sua demonstração completa da rede em gráficos estatísticos. Possui funções como a monitoração continua, notificações instantâneas, gerador de relatórios, dentre outras funcionalidades. Todas essas opções podem ser acessadas por meio de uma interface web pelo navegador (CACTI, 2013).

O NetEye é uma ferramenta paga, porém possui versões gratuitas que contém todas as funcionalidades da versão paga, apenas limitando a quantidade de dispositivos a serem gerenciados. Possui várias opções de relatórios, além de proporcionar ao administrador opções de configurações bastante distintas (NETEYE, 2013).

Pode se perceber que há uma enorme variedade de ferramentas disponíveis para administrar uma rede, cabe ao gerente escolher a que melhor se aplicar em sua rede. Pois com a grande concorrência, existe a possibilidade de estudar algumas destas aplicações e selecionar a que possuir funcionalidades que melhor se adéquam ao usuário (MOQADI, 2011).

O administrador da rede deverá analisar o melhor software em quesitos como preço, funcionalidade, otimização, suporte, opções de configurações, e dentre outros pontos que podem fazer a diferença na hora da implementação de uma rede.

3 SNMP

Toda essa complexidade que envolve uma rede de interconexões de entidades, gerenciá-la e monitorá-la garantindo que todos os seus dispositivos estão em execução e em pleno funcionamento pode parecer difícil. Porém através de uma padronização, este processo pode ser facilitado, buscando estabelecer normas que melhoram o trabalho de gestão foi lançado o protocolo SNMP, o protocolo simples de gestão de rede (MAURA; SCHIMIDT, 2001).

Este protocolo possui como principal características o gerenciamento de rede, onde a grande maioria, ou pode se dizer que todas, suas funções são voltadas diretamente para a administração de computadores e equipamentos, ou como é descrito nas especificações do SNMP, uma rede de objetos (RFC, 1990, tradução nossa).

Através do SNMP é possível conseguir as informações de determinados dispositivos através de comandos e pedidos, permitindo assim que o gerente visualize todo o status da rede de uma maneira facilitada, com estatísticas e informações de cada objeto. Dando a possibilidade também de o administrador da rede projetar o aumento gradual de sua rede, dentre outros planos de expansão (MILLER, 1999, tradução nossa).

Existe também a possibilidade de realizar a monitoração do tráfego que é gerado pela rede, além de possuir a função de receber notificações instantâneas de problemas ocasionados nos elementos e meios de transmissão. Desta maneira facilita as tarefas de otimizar o desempenho de uma rede e certificar-se de que a mesma esteja segura (MILLER, 1999, tradução nossa).

O protocolo SNMP também concede a função de observar e analisar todo o histórico de atividades desenvolvidas pela rede, permitindo assim que o administrador saiba de toda e qualquer ameaça que determinada ação poderá ocasionar à sua rede (RFC, 1990, tradução nossa).

Os dispositivos que são utilizados como gerentes nos quais emitem os comandos para a aquisição de informações, simulando um servidor, são denominados gerentes. Já os equipamentos que são os analisados, que recebem os comandos e devolvem as informações solicitadas, simulando um cliente, são denominados agentes (MAURA; SCHIMIDT, 2001).

O termo gerente é utilizado para o programa que é executado no dispositivo de gerenciamento, em quanto o termo agente é usado para a aplicação que é executada no equipamento gerenciado (MAURA; SCHIMIDT, 2001).

O SNMP é um protocolo definido em nível de aplicação, encontrando-se na camada de aplicação. Ele possui uma implementação flexível e fácil, onde toda sua especificação está presente no RFC 1157 (RFC, 1990, tradução nossa).

3.1 HISTÓRICO

O protocolo SNMP veio a ser desenvolvido em 1989, possuindo características de alguns protocolos da época, porém voltado para o monitoramento e controle dos ativos (RFC, 1990, tradução nossa). Sua criação ocorreu de forma a amenizar os problemas do alto grau de complexidade em que as redes se encontravam, pois não havia um padrão (BEHROUZ, 2006).

O SNMP foi desenvolvido por um grupo da *Internet Engineering Task Force* (IETF) com base no protocolo *Simple Gateway Management Protocol* (SGMP), utilizado para monitoração do *Internet Protocol* (IP). O SNMP herdou várias de suas funções, porém foram totalmente alteradas afim de melhorá-las e otimizá-las (RFC, 1990, tradução nossa).

No início do SNMP, sua função era apenas auxiliar a administração de rede até que fosse desenvolvido outro protocolo mais completo. Esses protocolos mais promissores o substituíram pouco tempo depois, porém a ideia não funcionou como previsto e o SNMP continuou sendo o protocolo principal (MILLER, 1999, tradução nossa).

Depois do lançamento oficial do protocolo SNMP, houve diversas alterações e atualizações, a mais importante delas implementada em 1991, porém apenas mais duas versões foram oficialmente publicadas. O SNMPv2 foi lançado em 1993 e recebeu diversas funcionalidades contidas na primeira versão, melhorando-as e corrigindo alguns erro, além de atribuir outras funcionalidades. (RFC, 1996, tradução nossa). A versão SNMPv3 foi a última versão, lançada em 1997, recebeu os processos das duas primeiras, e mais algumas melhorias. Mesmo com todas essas versões lançadas, a versão mais utilizada deste protocolo continua sendo a original (RFC, 1999, tradução nossa).

Apesar de existir muitos usuários em pouco tempo após seu lançamento, apenas na metade de década de 1990, sua utilização se expandiu de maneira promissora. Passou a ser o protocolo gerencial mais utilizado do mercado, servindo de base para diversos outros, além do desenvolvimento de diversas aplicações sobre ele (MILLER, 1999, tradução nossa).

O SNMP sofreu poucas evoluções nos quesitos de funcionalidade, porém todas elas foram melhoradas com o passar dos anos. A grande maioria das ferramentas administrativas utilizam este protocolo como base em seus processos, pois atualmente ele é considerado por muitos como o melhor protocolo voltado para gerência de redes.

3.2 ARQUITETURA

A estrutura do protocolo SNMP é considerada simples, se comparado com outros protocolos. Sua arquitetura pode ser dividida em três grandes grupos de elementos e dispositivos que auxiliam em seu funcionamento. Estes grupos são chamados de *Master Agent*, que são os gerentes, Subagente, considerados os agentes, e por fim o grupo *Management Station*, que são as aplicações que gerência a rede (MILLER, 1999, tradução nossa).

O primeiro grupo é caracterizado pelos elementos gerenciáveis, que consiste nos dispositivos que possuem a aplicação de gerenciamento em execução, chamados de *Managed Devices*. Estas entidades de rede procuram simular o servidor, ou seja, são os gerentes de rede onde o administrador controla todas as informações que trafegam na mesma (MILLER, 1999, tradução nossa).

A conexão do gerente com os demais dispositivos da rede, permite a aquisição de informações, por parte do gerente, estatísticas e configuráveis de qualquer componentes disponível da rede (MILLER, 1999, tradução nossa).

Entre esses componentes que compõe a rede e são suportados pelo protocolo SNMP estão os roteadores, os hubs, as pontes, os computadores, dentre outros diversos dispositivos que são padronizados através dos MIBs (BATES, 2000, tradução nossa).

Os agentes são os elementos que compõe o segundo grupo do protocolo SNMP, que se caracterizam por ser uma aplicação que é executada diretamente em um dispositivo que está conectado à rede em questão. Essa aplicação possibilita a

retirada e envio de informações de determinado dispositivo em que encontra-se, tornando-se a responsável por todos os dados contidos no mesmo (MILLER, 1999, tradução nossa).

Esses dispositivos agentes tem diversas funções importantes para o funcionamento completo do protocolo, onde dentre as principais destaca-se a coleta de informações do objetos gerenciados através de comandos recebidos do gerente (MILLER, 1999, tradução nossa).

Os agentes possuem algumas outras funcionalidades em respostas as solicitações vindas do gerente, como a notificação de eventuais problemas e erros ocasionados na rede, opções de segurança e autenticidade, permitindo uma privacidade adequada, dentre diversas outras funções que auxiliam os administradores de rede (MILLER, 1999, tradução nossa).

O terceiro e último conjunto de dispositivos são conhecidos como sistemas de gerência de redes, denominados *Network Management Systems* (NMS). Esses sistemas são classificados como consoles nos quais permitem, na maioria das vezes em um ambiente visual, realizar comandos com o objetivo de adquirir e definir informações em diversos equipamentos espalhados pela rede.

O protocolo SNMP destaca-se por possuir uma estrutura simplificada e organizada, Pois cada função é bem distribuída e especifica, auxiliando o administrador para uma gerência mais rápida e eficaz (MAURA; SCHMIDT, 2001). Esta arquitetura é otimizada para que a comunicação entre todas as entidades da rede seja realizada de maneira rápida.

3.3 FUNCIONAMENTO

O protocolo SNMP tem a função de implementar a arquitetura de comunicação entre vários elementos, permitindo que cada equipamento seja gerenciado unicamente ou divididos em grupos, afim de obter dados detalhados conforme a necessidade do administrador de rede (RFC, 1990, tradução nossa).

O funcionamento do SNMP consiste em apenas dois elementos principais, são os gerentes e os agentes. Eles são os responsáveis por administrar as permissões e requisições dos dispositivos (MILLER, 1999, tradução nossa). O funcionamento do agente restringe-se em enviar requisições aos gerentes e responder caso os mesmos tenham o solicitado algo. Por outro lado as tarefas dos

gerentes são a de responder as requisições enviadas pelos agentes, enviar determinadas solicitações caso necessário, e também possuem a função de definir algo a determinados agentes, ou seja, controlá-los de acordo com os processos dos agentes realizados na rede no momento (MAURA; SCHMIDT, 2001).

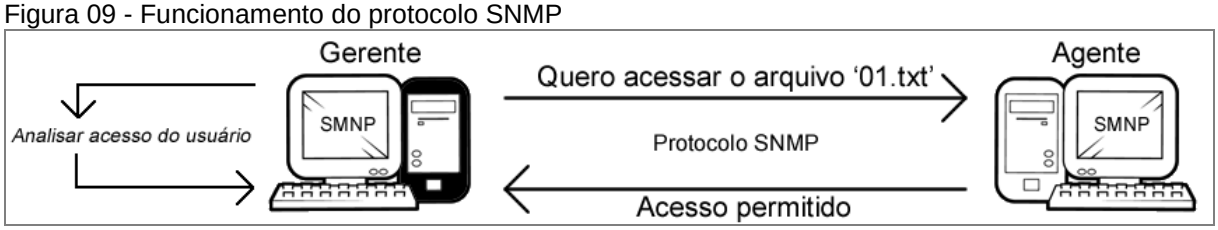
Todas as requisições de acesso à rede e também a determinados dados serão direcionados para os gerentes, que são conhecidos como os servidores. São eles os responsáveis por processar as requisições e enviar uma determinada resposta, possibilitando que o agente prossiga com suas funções ou não, caso sua requisição tenha sido negada (MILLER, 1999, tradução nossa).

Os processos de requisições respostas são realizados através de comandos, nos quais podem ser tratados diretamente por aplicações de gerenciamento de rede que utilizem o protocolo SNMP, sendo assim os usuários não terão contato algum com esta parte um pouco mais complexa do SNMP (MILLER, 1999, tradução nossa).

Os sistemas gerenciais abstraiam ao máximo a complexidade de uma rede e facilitam a utilizam desses comandos. Sendo quase nulo o contato com os protocolos e seus comandos diretamente, onde este contato ocorre somente através de opções e serviços pré-determinados (MILLER, 1999, tradução nossa).

Na figura 09 é possível observar o funcionamento do protocolo SNMP, no qual é exposto a situação em que o agente solicita o acesso a um determinado arquivo e o gerente recebe está solicitação e a trata, enviando-lhe uma resposta positiva de acesso.

Figura 09 - Funcionamento do protocolo SNMP



Fonte: Adaptado de Miller (1999).

Através do SNMP é possível realizar o monitoramento e controle de todos os equipamentos dispersos pela rede. Desde que os mesmos estejam disponíveis e funcionando de acordo com as políticas da rede. Para que esses objeto possa ser totalmente gerenciado e controlado, é necessário estar padronizado em uma

especificação, e possuir a atribuição de um nome ao equipamento, sendo necessariamente único na rede (MAURA; SCHMIDT, 2001).

O nome desta especificação é MIB, que consiste em uma relação de todos os agentes e gerentes que compõem a rede. Incluindo sua localização e diversas informações operacionais (MILLER, 1999, tradução nossa).

Estas relações MIB são de suma importância para que seja possível realizar a padronização dos nomes dos dispositivos disponíveis na rede, assim como quais são suportados gerencialmente. Com isso se defini os comandos em que estes equipamentos serão baseados e um padrão de informação para os mesmos (MILLER, 1999, tradução nossa).

As relações MIB não são especificas de um protocolo, não sendo este o responsável pela sua criação. Deste modo podem ser criadas outros grupos MIB indiferente do protocolo de comunicação utilizado, sendo que a qualquer momento é possível criar e utilizar novos conjuntos de equipamentos MIB (MILLER, 1999, tradução nossa).

A utilização do protocolo SNMP possibilita ao administrador diversas boas possibilidades, porém existe alguns contras em seu funcionamento, como a baixa performance em grandes redes, nas quais existem centenas de equipamentos para serem monitorados. Há também a incapacidade de possuir dois gerentes na rede comunicando-se entre si, mas são problemas que podem ser contornados (RFC, 1990, tradução nossa).

Apesar de possuir diversos processos em seus serviços, o protocolo SNMP possui um funcionamento direto, ou seja, as solicitações são processadas rapidamente e o administrador da rede logo alcança a informação que deseja.

3.4 COMANDOS

O funcionamento do protocolo SNMP se faz através de comandos que podem ser descritos como pacotes enviados do gerente ao agente por meio da rede, ou ao contrário, uma resposta partindo do agente ao gerente (MAURO; SCHMIDT, 2001).

Estes pacotes são divididos em três fragmentos, sendo o primeiro o cabeçalho, onde as informações de emissão são armazenadas, a parte dos dados, onde os comandos encontram-se, e por último as informações de verificação,

utilizadas para analisar se o pacote chegou e está no lugar correto. Eles são utilizados para a aquisição e definição das informações de equipamentos, sendo chamados de *Protocol Data Unit* (PDU) (MAURO; SCHMIDT, 2001).

Entre alguns exemplos destes pacotes se destaca o *Get Request*, que é utilizado para solicitar alguma informação de um determinado dispositivo na rede. Onde estes dispositivos poderão retornar a resposta através de outro comando chamado *Get Response*, no qual permite o envio das informações requisitadas pelo gerente (MAURO; SCHMIDT, 2001).

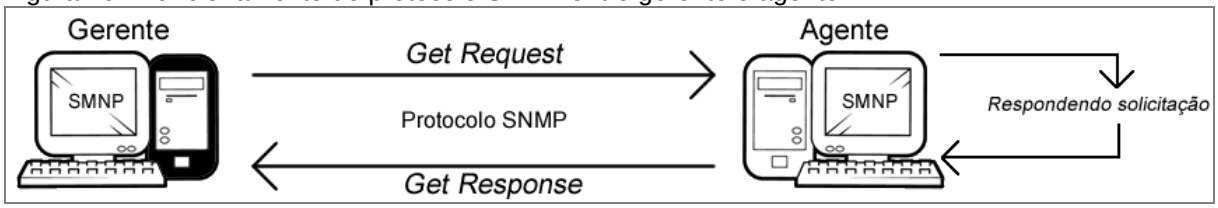
Outro comando que pode ser realizado pelo gerente é o *Get-next Request*, que é semelhante ao anterior, porém este requisita as informações de uma grade de dispositivos conectados ao equipamento em questão (RFC, 1990, tradução nossa).

Para definir alguma informação a algum dispositivo disponível, utiliza-se o comando *Set Request*, no qual atribui qualquer valor determinado a um objeto na rede. Este comando é emitido através da aplicação gerente (RFC, 1990, tradução nossa).

Ainda existe o comando *Trap*, que é utilizado para enviar notificações de algo que ocorreu na rede, desde problemas críticos a eventos que podem ocasionar erros. Essas notificações são enviadas diretamente para o gerente, podendo partir de qualquer equipamento que possui a aplicação agente em execução (RFC, 1990, tradução nossa).

A figura 10 representa um dispositivo executando a aplicação gerente, em que o administrador de rede realiza algumas requisições para outros que possui a aplicação agente em execução.

Figura 10 - Funcionamento do protocolo SNMP entre gerente e agente



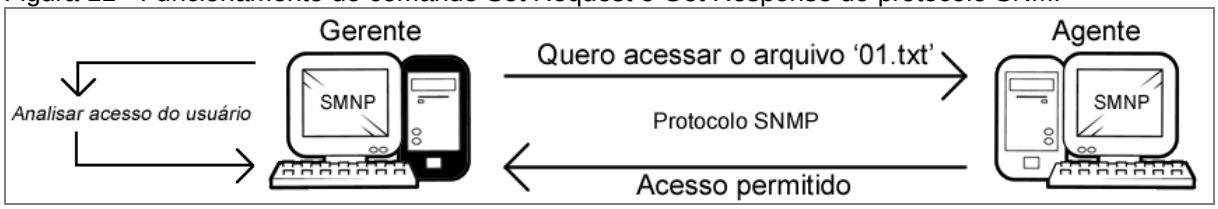
Fonte: Adaptado de Pinheiro (2011).

Analisando a figura 10 observa-se que o administrador envia, através do dispositivo gerente, um comando *Get Request* solicitando para que um determinado equipamento disponível na rede receba a requisição e a responda. O dispositivo

agora utiliza o comando *Get Response* para enviar as informações requisitadas pelo administrador de rede ao dispositivo gerente.

A figura 11 demonstra o gerente definindo determinada informação a um dispositivo.

Figura 11 - Funcionamento do comando Set Request e Get Response do protocolo SNMP

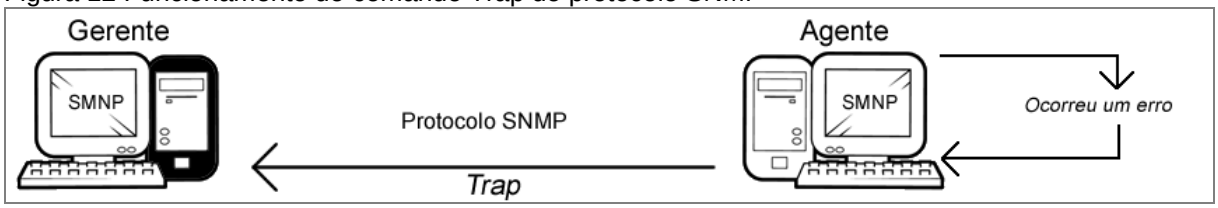


Fonte: Adaptado de Pinheiro (2011).

A figura 11 descreve que quando o administrador de rede define determinado valor a um dispositivo através do comando *Set Request*, o dispositivo defini a informação passada e lhe envia de volta uma resposta de sucesso ou não com o comando *Get Response*.

A figura 12 seguinte simula um evento onde ocorre um determinado erro em um dos equipamentos agentes.

Figura 12 Funcionamento do comando Trap do protocolo SNMP



Fonte: Adaptado de Pinheiro (2011).

A figura 12 demonstra uma situação simples em que um dispositivo da rede rodando a aplicação agente demonstra um erro, sendo que então será enviada uma notificação, por meio do comando *Trap*, para a aplicação gerente que está rodando em outro equipamento. Ao chegar esta notificação o gerente demonstra a mesma ao administrador.

Estas são apenas algumas funcionalidades básicas realizadas através de comandos do console de aplicação do protocolo SNMP, existindo inúmeras outras funções (RFC, 1990, tradução nossa).

Utilizando-se um programa de entrada especifico, esses comandos podem ser realizados de uma maneira muito mais complexa, alcançar novas possibilidades e maneiras mais fáceis de alcançar os dados requerentes.

3.5 VERSÕES

O protocolo SNMP possui apenas três versões oficiais lançadas até o presente momento, sendo que cada atualização está representada e definida por seu respectivo RFC. Suas versões foram lançadas entre os anos de 1991 e 1998, com todas suas características voltadas ao gerenciamento de redes.

A primeira versão do SNMP foi desenvolvido e implementado com o auxílio de diversos programadores espalhados pela comunidade. Houve também a criação de um padrão onde é descrito todos os equipamentos disponíveis na rede, sendo através deste padrão que SNMP realiza a análise de quais dispositivos é possível gerenciar, essa padronização são as conhecidas MIBs (RFC, 1990, tradução nossa).

Neste início do protocolo utilizou-se os conceitos já existentes no funcionamento de rotadores, onde baseou-se boa parte de seus processos e estrutura. Embora tenha sofrido várias alterações o sido diferenciado consideravelmente a cerca dessas organizações de funcionamento contidas nos roteadores (MAURA; SCHMIDT, 2001).

Apesar de ter sido lançada em 1991, diversas atualizações e correções com adição de melhorias de algumas funcionalidades foram lançados logo após sua publicação, obrigando o encerramento desta primeira versão em um curto período de tempo (RFC, 1990, tradução nossa).

A próxima versão foi a SNMPv2 que trouxe basicamente todas as funcionalidades da versão anterior, porém por ser uma versão subsequente trouxe diversas melhorias e também novos processos e funções (MAURA; SCHMIDT, 2001).

Ela foi descrita entre os RFCs 1442 e 1452 e tornou-se a padrão utilizada em abril de 1993, dois anos após o lançamento do SNMPv1 (MAURA; SCHMIDT, 2001).

Dentre várias alterações e melhorias está o aumento considerável dos tipos de dados utilizados, sendo agora possível a utilização de diversos modelos de informações compatíveis com uma variedade de equipamentos e dispositivos que uma rede pode possuir (RFC, 1996, tradução nossa).

Também criou a possibilidade de criar e salvar os históricos de atividades realizadas na rede. Na qual gerou um grande avanço na procura dos motivos que levaram uma determinada rede a parar e sofrer certo erro. Tornando a resolução dos mesmos mais rápidos e seguros, além de se evitar futuros problemas (RFC, 1996, tradução nossa).

Em 1998 foi padronizada a terceira e última versão deste protocolo, o SNMPv3, que foi publicado através das RFCs 2271 a 2275. Nesta versão foram novamente melhoradas consideravelmente as funcionalidades já existentes nas duas primeiras versões e incluídas outras funções e processos a respeito da administração de redes (BATES, 2000).

A segurança sofreu importantes melhorias e a adição de novos módulos e processos que possibilitaram a alteração da forma realizada de autenticação, tornando a integridade das informações mais segura e com um alto nível de privacidade perante aos dados (BATES, 2000). Também foram criados conjuntos de operações relacionadas a administração, onde através de um novo modulo é possível permitir o que certo usuário terá acesso (MILLER, 1999, tradução nossa).

As maiores críticas acerca de cada nova versão lançada, foram de que as funcionalidades de uma não possui compatibilidade com a outra. Isto tornava o uso do SNMP algo complicado para redes que foram atualizadas gradativamente. Algumas atualizações realizadas a partir da terceira versão tentaram corrigir alguns desses problemas e tornar a comunicação entre todas as versões possíveis, porém é algo ainda bem limitado (MILLER, 1999, tradução nossa).

4 SOFTWARES

Os softwares selecionadas para a realização do projeto, Cacti e NetEye, são ferramentas de gerenciamento poderosas na administração e controle da rede, possuindo recursos apurados e diversas opções de configurações.

O Cacti possui ferramentas que proporcionam a visualização dos dados recebidos em gráficos que facilitam o entendimento das informações passadas. A quantidade de possibilidades e funções acabando torando-o um pouco complexo no quesito usabilidade, porém através de sua interface intuitiva é possível utiliza-lo tranquilamente (CACTI, 2013).

Dentre suas funcionalidades destacam-se a possibilidade de obtenção de dados de diferentes equipamentos no mesmo momento, uma avançada configuração de privacidade com um controle total sobre os usuários, gráficos que demonstram estatísticas da rede em tempo real, notificação de problemas instantaneamente, e muitas outras funções disponíveis (CACTI, 2013).

No NetEye é possível controlar e monitorar em tempo real todos os dispositivos, auxiliando e facilitando para o administrador todas as suas tarefas exercidas tanto com relação ao gerenciamento quanto ao suporte (NETEYE, 2013).

Suas funcionalidades que se destacam fazem parte do modulo de monitoramento, onde é possível gerenciar e coletar informações de todas as entidades conectadas. Além da possibilidade de controlar os acessos de usuários aos recursos disponíveis na rede (NETEYE, 2013).

Os dois softwares possuem finitas possibilidades, dentre funções semelhantes e únicas, onde cada um difere através de seus processos de monitoramento. Utilizando toda essas funcionalidades, ambas as ferramentas são uma ótima escolha para implantar o gerenciamento em uma rede.

4.1 CACTI

O Cacti é uma ferramenta livre que auxilia os administradores de rede em suas tarefas gerenciais em uma rede de computadores. Seu objetivo é monitorar e controlar desde redes simples até mais complexas, procurando facilitar essas rotinas administrativas através de suas várias funcionalidades (CACTI, 2013).

Seu desenvolvimento foi realizado pelo grupo de desenvolvedores *The Cacti Group*, onde é mantido atualmente. Sua liberação é sob a licença *General Public License* (GNU), no qual não há custos para a adquirir a ferramenta, porém é possível realizar pequenas doações pelo seu site, ajudando assim no desenvolvimento da software (CACTI, 2013).

Nos fóruns do próprio site do Cacti é possível esclarecer várias das dúvidas acerca da ferramenta, além de adquirir novos conhecimentos sobre a mesma. Pois estes fóruns contam com usuários espalhados por todo o mundo, nos quais também realizam dicas e críticas que ajudam no desenvolvimento e atualizações da aplicação (CACTI, 2013).

Ele se caracteriza na criação de gráficos com as estatísticas de trafego da rede, onde é possível observar e analisar todas as informações dos dispositivos conectados. Estes gráficos são visivelmente claros e demonstram especificamente os dados coletados (CACTI, 2013).

O Cacti permite que as suas funcionalidades sejam acessadas através de uma interface intuitiva, pois a mesma roda em qualquer navegador, pois toda sua interface é orientada à linguagem de programação para web, o PHP (CACTI, 2013).

A figura 13 demonstra a tela inicial da aplicação Cacti através do navegador de web Mozilla Firefox.

Figura 13 - Tela inicial da ferramenta Cacti

Fonte: Do Autor.

A geração dos gráficos é de responsabilidade da ferramenta RRDTool, no qual armazena os dados coletados pelo Cacti em uma banco de dados MySQL, gerando assim, por meio desses dados, os gráficos estatísticos citados (CACTI, 2013).

O Cacti trabalha com o protocolo SNMP no qual permite a comunicação com todos os equipamentos da rede afim de coletar informações sobre os serviços e recursos dos mesmos. Outra característica que se destaca é a possibilidade de utilizar plug-ins para aumentar o nível de gerência e as funcionalidades da ferramenta. Esses plug-ins podem ser encontrados no próprio site, e através da documentação é possível aprender a instala-los sem maiores dificuldades (CACTI, 2013).

4.1.1 Funcionamento

O funcionamento do Cacti pode ser complexo, porém é necessário que haja determinados componentes instalados e devidamente configurados para que as suas funcionalidades possam ser exercidas corretamente. Estes componentes passam pelo banco de dados, por um servidor com suporte à linguagem PHP, pela ferramenta RRDTool e pelo protocolo SNMP (CACTI, 2013).

O banco de dados é o utilizado para armazenar os dados coletados na rede, sendo o MySQL o definido para o funcionamento correto das funcionalidades da aplicação. Para o servidor que suporte à linguagem PHP é aconselhável a utilização do Apache, que dá um bom suporte para esta linguagem (CACTI, 2013).

O ferramenta *Round Robin Database*, ou simplesmente RRDTool, é uma aplicação que gerência o armazenamento de informações referente aos tráfegos gerados em redes de computadores a uma base da dados. Ele foi criado por Tobias Oetiker sob a licença livre GNU (OETIKER, 2013).

O RRDTool deve ser instalada junto com o Cacti para que a maioria de suas funcionalidades possam ser executadas sem problemas, principalmente a geração de gráficos estatísticos. É necessário também a configuração correta do protocolo SNMP para que haja a comunicação entre os equipamentos gerentes e agentes (CACTI, 2013).

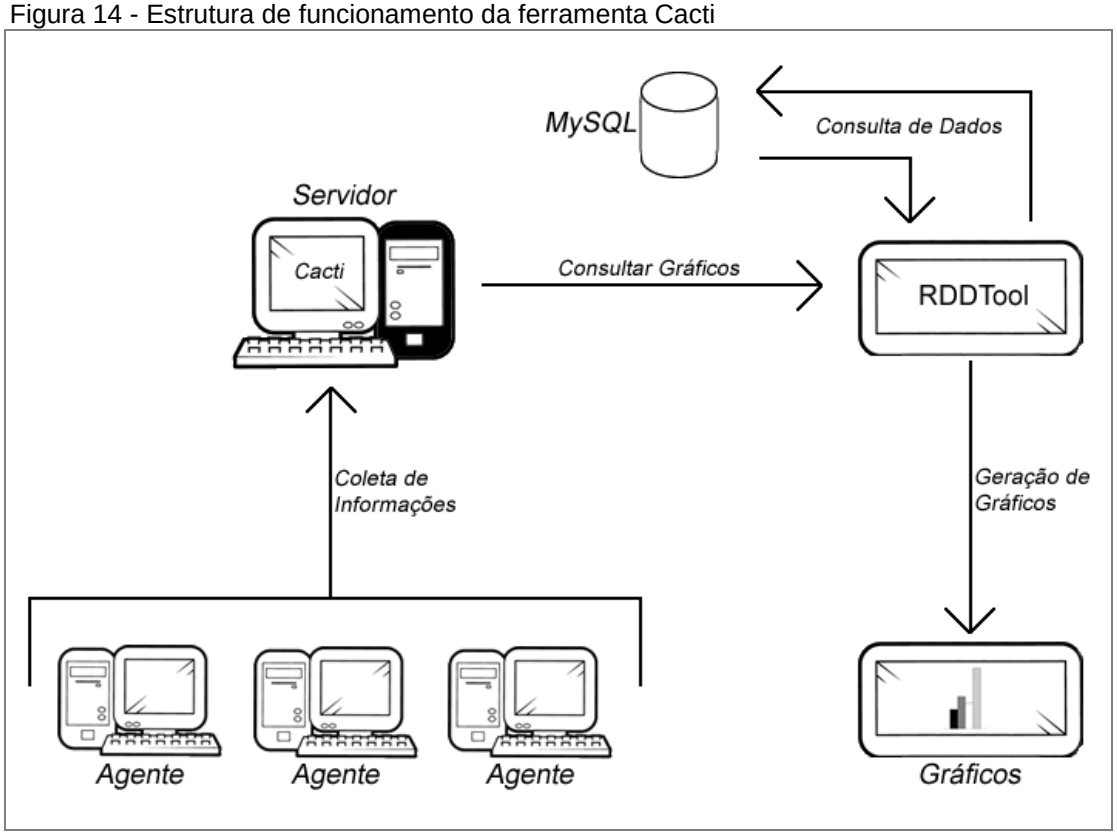
O Cacti é o responsável por coletar todas as informações de tráfegos gerados na rede, seja de acesso a arquivos, recursos, e-mails, dentre outros dados

referentes ao acesso à rede. Essas informações são repassadas através de scripts para a ferramenta RDDTool e então armazenadas no banco de dados, onde então é possível gerar os gráficos (CACTI, 2013).

Os gráficos podem ser classificados e configurados para serem obtidos diariamente, semanalmente, mensalmente e até anualmente, visando a comparação do trafego entre um período e outro.

A figura 14 demonstra o funcionamento de uma rede de computadores gerenciada através do Cacti, onde é apresentado o funcionamento de todos os seus componentes.

Figura 14 - Estrutura de funcionamento da ferramenta Cacti



Fonte: Adaptado de Pinheiro (2010).

Todos os componentes que envolvem o funcionamento do Cacti precisam ser corretamente instalados e configurados, para que assim sejam evitados problemas gerenciais. É necessário também verificar periodicamente a disponibilidade dos mesmos, afim de confirmar que todos estão trabalhando sem falhas e em conjunto.

4.1.2 Requisitos

A implantação de todas as ferramentas do Cacti é possível mesmo através de máquinas com pouca disponibilidade de hardware, pois requer pouco poder de processamento para executa-lo (CACTI, 2013).

Na parte do software é necessário que todos os componentes citados anteriormente estejam instalando e configurados. Sendo eles o banco de dados MySQL, o servidor Apache, a ferramenta RRDTool e o protocolo SNMP (CACTI, 2013).

Os requisitos mínimos para a instalação do banco de dados MySQL sem que haja perca de desempenho são um processador Intel Pentium 500 MHz, 50 MB de memória e espaço de 250 MB em disco (MYSQL, 2013).

As configurações mínimas necessárias para que seja possível executar o servidor Apache são um processador Intel Pentium 500 MHz, 256 MB de memória e espaço de 650 MB em disco (APACHE, 2013).

As configurações necessárias para a instalação do Cacti, onde é possível observar que não é necessário possui uma máquina com grandes configurações para executa-lo, são um processador Intel Pentium 500 MHz, 256 MB de memória e espaço de 500 MB em disco (CACTI, 2013).

Os requerimentos mínimos para que a ferramenta RRDTool não sofra perca de desempenho, onde também é possível observar que não é obrigatório possuir grandes configurações para executa-lo, são um processador Intel 500 MHz, 256 MB de memória e espaço de 650 MB em disco (OETIKER, 2013).

Esses são os requisitos mínimos de software e hardware necessários pra que o Cacti possa ser executado sem que haja perca de funcionalidades. Como observado não há a necessidade de possuir máquinas com um processamento grande, sendo que todas as ferramentas executam nas plataformas Microsoft Windows, Linux e MacOS, porém o mais importante passa a ser a configuração de todos os seus componentes, para que assim todos possam funcionar em conjunto.

4.2 NETEYE

O NetEye é um software proprietário, ou seja, necessita-se de custos para adquiri-lo, ele é totalmente voltado para o gerenciamento de redes de computadores no qual monitora todos os componentes utilizados pelos clientes. Ele foi

desenvolvido em 2006 pela empresa NetEye com o intuito de facilitar o gerenciamento das informações e computadores da rede. A empresa era incubada na Unidade de Desenvolvimento Tecnológico da Universidade do Vale do Rio dos Sinos (UNISINOS) (UNITEC), a incubadora do Parque Tecnológico São Leopoldo. Atualmente a empresa NetEye é especializada no gerenciamento, produtividade e segurança (NETEYE, 2013).

Suas funcionalidades são divididas em cinco módulos, o inventário dos hardwares e softwares, a segurança das informações que trafegam, a produtividade da organização, o monitoramento de todos os dispositivos conectados e desempenho dos mesmos (NETEYE, 2013).

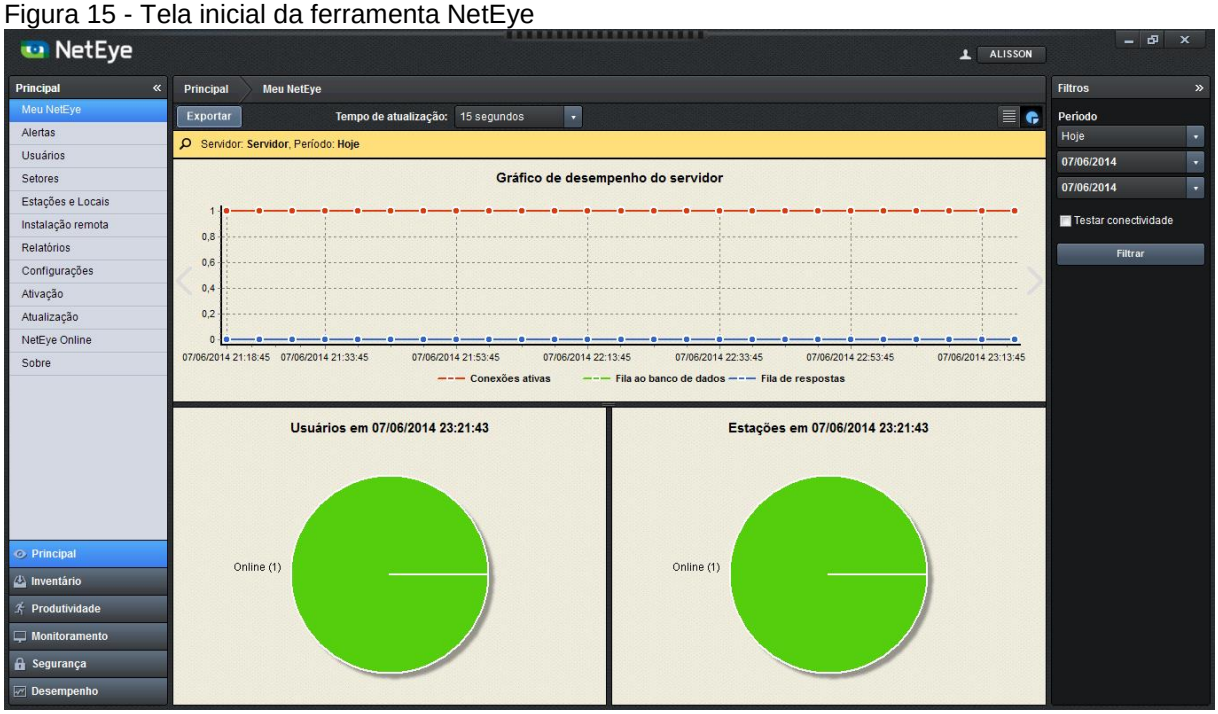
Através de suas funções é possível otimizar a rede em que o mesmo está implantado, também pode proporcionar uma maior agilidade para a gerência e o suporte. Coletando todas as informações dos agentes de forma automática, notificando o administrador ao encontrar um problema (NETEYE, 2013).

A aplicação possibilita também o armazenamento de logs de auditoria, estatísticas de uso, além de possuir um modulo de produtividade no qual possibilita ter uma ganho real na produtividade da organização (NETEYE, 2013).

Sua interface é totalmente amigável, podendo ser executada uma determinada função através de menus bem divididos e claros. Caracterizando-se por uma instalação fácil e rápida, a sua configuração é intuitiva, levando o usuário em um passo a passo (NETEYE, 2013).

A figura 15 demonstra a tela inicial da versão 6 da ferramenta NetEye instalada em um computador com o sistema operacional Microsoft Windows 8.

Figura 15 - Tela inicial da ferramenta NetEye



Fonte: Do Autor.

4.2.1 Funcionamento

O funcionamento do NetEye pode ser considerado simples, pois ele não demonstra uma estrutura tão complexa. Onde os componentes que forma esta estrutura são o banco de dados, o *collector*, o *controller*, o *config*, o *client* e o console (NETEYE, 2013).

O banco de dados será onde ficará armazenada as informações de monitoramento dos dispositivos da rede. Pois essas informações são coletadas, processadas e salvas para posteriores consultas (NETEYE, 2013).

O *collector* é um serviço que é executado no servidor, este é o responsável pela coleta das informações dos equipamentos mencionada. A responsabilidade de gravar estes dados no banco de dados também é dele (NETEYE, 2013).

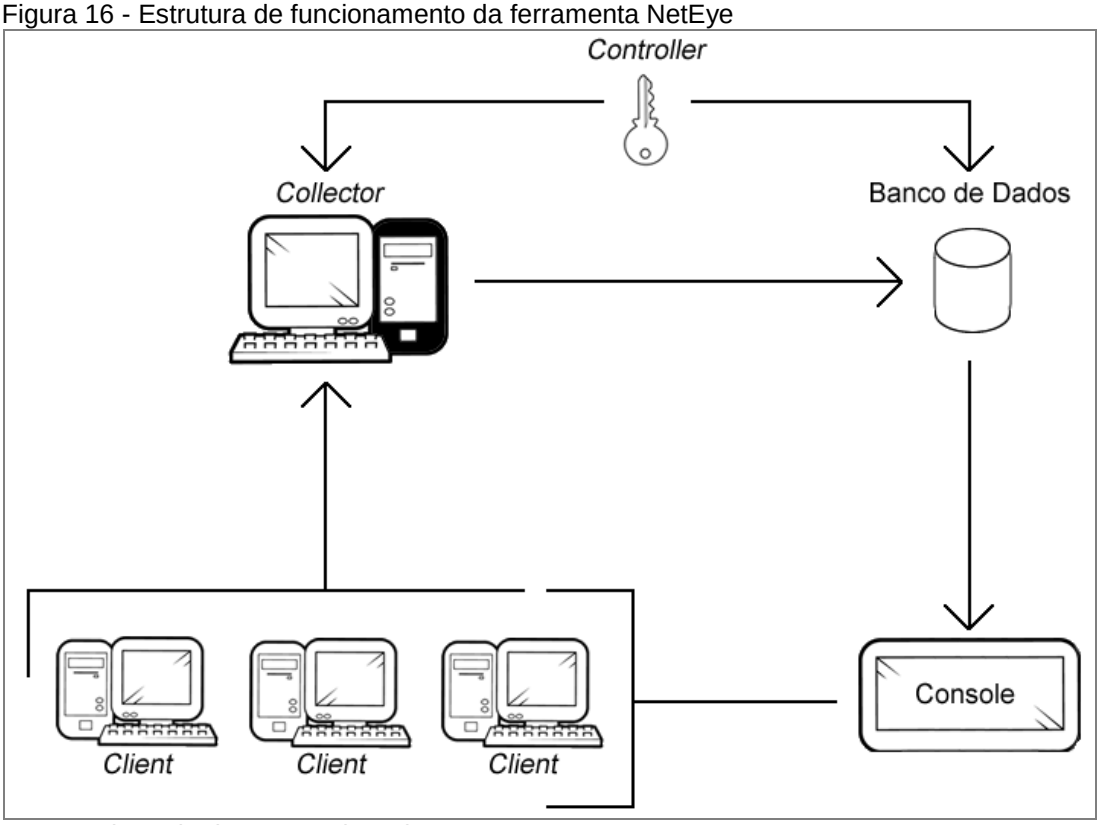
O *config* é um utilitário que é executado em todas máquinas, seja gerente ou agente. Já o *client* é o serviço que é executado no agente, no qual fica responsável por capturar todas as informações de softwares e hardwares do usuário (NETEYE, 2013).

Por fim o console é a ferramenta que permite acessar todos esses dados coletados, onde a visualização dos mesmos pode ser feita através de gráficos,

relatórios, na própria máquina do usuário, dentre outras formas possíveis (NETEYE, 2013).

A figura 16 demonstra o funcionamento do NetEye com todos os seus componentes citados. Onde são demonstradas três máquinas que são gerenciadas através de um servidor central.

Figura 16 - Estrutura de funcionamento da ferramenta NetEye



Fonte: Adaptado de NetEye (2013).

Este são os componentes para que o NetEye possa funcionar corretamente. Sendo que para o gerenciamento por parte da aplicação seja bem feito, é necessário que todas as suas instalações e configurações estejam bem alinhavadas, pois qualquer componente não implantado, poderá ocasionar em um mal funcionamento de uma determinada função.

4.2.1 Requisitos

Os requisitos referentes ao hardware dos equipamentos aqui mencionados serão apenas os mínimos necessários, não levando em conta programas e terceiros que estão em execução simultaneamente com o NetEye (NETEYE, 2013).

Os requisitos computacionais necessários para a instalação do banco de dados são o sistema operacional Microsoft Windows (2000/XP/2003/Vista/7/8), processador de 1,0 GHz, 768 MB de memória e espaço de 1 GB em disco (MICROSOFT, 2013).

Para a instalação pode ser escolhido entre três bancos de dados, o Firebird, o SQL Server e o Microsoft SQL Server Desktop Engine (MSDE). Onde todos funcionam igualmente bem em conjunto com a ferramenta, porém o recomendável pelo próprio programa é o SQL Server (NETEYE, 2013).

Os requisitos computacionais mínimos necessários para a instalação da ferramenta servidora são o sistema operacional Microsoft Windows (2000/XP/2003/Vista/7/8), processador de 1,0 GHz, 768 MB de memória e espaço de 1 MB em disco (NETEYE, 2013).

As máquinas agentes devem possuir uma configuração considerada básica atualmente, sendo o sistema operacional Microsoft Windows, um processador de 166 MHz, apenas 32 MB de memória e espaço de 5 MB em disco (NETEYE, 2013).

Esses são os softwares e hardwares necessários para que o funcionamento do NetEye possa ocorrer de forma correta. Podendo assim o usuário usufruir de todas as funcionalidades disponíveis sem que haja perda de informações ou má funcionamento das mesmas.

5 TRABALHOS CORRELATOS

Durante a realização deste projeto de pesquisa, foi levantado alguns artigos e trabalhos correlacionados ao tema aqui abordado. Os trabalhos foram desenvolvidos como trabalho de conclusão de curso de algumas universidades do país.

Esses trabalhos abordam a análise e implementação de softwares de gerenciamento de redes com o intuito de demostrar a utilização de suas funcionalidades através de um estudo de caso aplicado à um ambiente propicio.

5.1 IMPLEMENTANDO GERENCIAMENTO DE REDES DE COMPUTADORES USANDO NAGIOS E ZABBIX

O projeto implementando gerenciamento de redes de computadores usando Nagios e Zabbix foi realizado por Wagner Ribeiro Junquiera, da Divisão de Tecnologia da Informação da Escola Preparatória de Cadetes do Exército (EsPCEx), e André Luis Boni Déo da Universidade Estadual de Campinas (UNICAMP) (JUNQUEIRA; DÉO, 2010).

Esta pesquisa visou a implementação de um gerenciamento de computadores através da utilização dos softwares Nagios e Zabbix. Onde foi realizada uma análise completa dos mesmos, afim de entender melhor os conceitos do gerenciamento de uma rede por meio de uma ferramenta (JUNQUEIRA; DÉO, 2010).

Seu objetivo principal era a realização da comparação entre os softwares gerenciais. A comparação levou em conta quesitos como a instalação, suporte, configuração, interface, recursos e desempenho dos mesmos. Toda essa documentação e conceitos das ferramentas foram apresentados com base em diversas obras bibliográficas e artigos publicados sobre os mesmos. Além de realizar um estudo de caso mais detalhado com cada aplicação escolhida enfatizando a gerência de redes (JUNQUEIRA; DÉO, 2010).

O estudo de caso realizado foi possível observar que a ferramenta Zabbix é completa nos quesitos de funcionalidades, pois possui todas as funções para a realização da monitoração e controle da rede sem problemas, garantindo a segurança da informação e também o desempenho esperado para a mesma. Por

outro lado a ferramenta Nagios não possui tantas funções como o Zabbix, mas também se mostrou satisfatória dentro de sua proposta, garantindo através de funcionalidades básicas a realização de um gerenciamento correto da rede (JUNQUEIRA; DÉO, 2010).

5.2 UM PROCESSO DE GERÊNCIA PARA REDES DE COMPUTADORES EM AMBIENTE DE SOFTWARE LIVRE

O projeto Um Processo de Gerência para Redes de Computadores em Ambiente de Software Livre foi realizado por Leonardo Kolisnik de Matos na Pontifícia Universidade Católica do Paraná para o curso sequencial de Informática no Gerenciamento de Pequenas e Medias Empresas, na cidade de Curitiba, Paraná (MATOS, 2006).

O trabalho teve como seu objetivo central apresentar a importância do gerenciamento de redes em um ambiente empresarial sem a necessidade de arcar com custos elevados. Onde foram demonstrados alguns softwares livres para a realização deste gerenciamento, com foco nos custos para a implantação destas ferramentas em uma empresa (MATOS, 2006).

Estas ferramentas livres que foram utilizadas para a realização do projeto estão entre as mais conhecidas do mercado, também foi apresentada algumas aplicações proprietárias, sendo apresentada ao todo oito soluções. Estes softwares foram aplicados em uma rede interna empresarial, onde foi possível o estudo dos problemas comuns ocasionados, e então através das ferramentas selecionadas foi possível a identificação e resolução dos problemas (MATOS, 2006).

Os resultados obtidos conseguiram demonstrar que a realização de uma administração na rede em uma empresa é um dos pontos mais crucial para sua produção, pois com uma rede em perfeito funcionamento, os colaboradores puderam trabalhar sem interrupções e prover de todos os recursos compartilhados. Além de que não foi necessário gastar uma alta quantia para que a implantação da gerência fosse bem sucedida. Bastando a utilização de software gratuitos, nos quais possuem as mesmas funcionalidades das aplicações proprietárias (MATOS, 2006).

5.3 ESPECIFICAÇÃO DE UMA PLATAFORMA DE GERENCIAMENTO DE REDES BASEADA NO PROTOCOLO SNMP

O projeto Especificação de uma Plataforma de Gerenciamento de Redes Baseada no Protocolo SNMP foi realizado por Cláudio Barbosa Schmichtemberg na Universidade do Extremo Sul Catarinense (UNESC) para o curso de Ciência da Computação, na cidade de Criciúma, Santa Catarina (SCHMICHTEMBERG, 2009).

O objetivo central da pesquisa foi a de criar uma especificação para um software de gerenciamento que utilizasse como base as funções do protocolo SNMP, e também possuísse uma licença livre. Além de descrever todos os conceitos relacionados à gerência de redes e seus modelos (SCHMICHTEMBERG, 2009).

As plataformas analisadas foram OpenNMS, Nagios, HP Open View Network Node Manager, Tivoli NetView e ZenOSS. As descrições foram realizadas através de bibliografias que puderam servir de base para o entendimento de suas inalações, configurações e sua capacidade funcional no gerenciamento de rede. Sendo que através das ferramentas analisadas é possível manter um bom nível de gerência, onde qualquer das aplicações selecionadas podem auxiliar o administrador da rede nos quesitos de monitoração e controle da mesma (SCHMICHTEMBERG, 2009).

As descrições realizadas no projeto poderá servir de base para o desenvolvimento de um software que possua todas as funcionalidades capazes de manter uma estrutura gerencial, além de otimizar o desempenho da rede, monitorando-a e controlando-a conforme os conceitos de gerência abordados (SCHMICHTEMBERG, 2009).

5.4 GERENCIAMENTO E MONITORAÇÃO DE REDES DE COMPUTADORES UTILIZANDO-SE ZABBIX

O projeto Gerenciamento e Monitoração de Redes de Computador Utilizando-se Zabbix foi realizado por Esley Bonomo em 2006 na Universidade Federal de Lavras para o curso em pós-graduação Lato Sensu em Administração de Redes Linux, na cidade de Lavras, Minas Gerais (BONOMO, 2006).

O trabalho propôs utilizar e analisar todas as funcionalidades da ferramenta gratuita Zabbix, implementando um gerenciamento em uma rede de computadores. Criando soluções para os diversos problemas ocasionados através das funções do software definido (BONOMO, 2006).

Foi realizado um estudo de caso da ferramenta Zabbix em um ambiente corretamente configurado, onde foi possível a utilização de todas as suas funcionalidades, sendo analisado os resultados obtidos (BONOMO, 2006).

A pesquisa demonstrou que o Zabbix é um software que pode tranquilamente assumir o papel principal de gerenciamento de rede. Mostrando-se eficiente nos testes e ambiente em que foi aplicado, resultando em uma ferramenta indispensável no auxílio ao administrador de rede (BONOMO, 2006).

5.5 FERRAMENTAS DE GERÊNCIA DE REDES

O projeto Ferramentas de Gerência de Redes foi realizado por Grasielli Barreto em 2008 no curso de Especialização em Redes de Computadores e Comunicação de Dados para o curso Universidade Estadual de Londrina, na cidade de Londrina, Paraná (BARRETO, 2008).

A pesquisa procurou apresentar os principais conceitos acerca do gerenciamento de redes, abordando sua importância nos quesitos de segurança e integridade das informações. Passando algumas informações técnicas importantes aos administradores de rede (BARRETO, 2008).

As características do protocolo SNMP também foram apresentados, passando por todas as suas versões oficiais lançadas. Além da descrição das informações referente as áreas de gerenciamento do modelo FCAPS e o gerenciamento de rede em redes TCP/IP (BARRETO, 2008).

Os estudos comprovaram que a gerência de rede centralizado é a melhor opção de implantação do gerenciamento. Pois através de uma única máquina é possível analisar as informações de todos os dispositivos disponíveis. Além de que a utilização de uma ferramenta para o auxílio ao administrador é de suma importância, melhorando assim o desempenho e segurança da rede (BARRETO, 2008).

6 GERENCIAMENTO DE ATIVOS DE REDE

Este projeto de pesquisa realizou um estudo completo por meio de casos na utilização dos softwares Cacti e NetEye com enfoque no gerenciamento de rede a fim de analisar os resultados obtidos, buscando a resolução otimizada de problemas cotidianos ocasionados na rede.

Os softwares foram obtidos por meio da Internet, visto que a ferramenta Cacti é gratuita e o NetEye possui uma versão de demonstração completa, apenas restringindo a quantidade de equipamentos monitorados. Na implementação deste trabalho foi realizado em um dos laboratórios de informática da própria universidade a fim de simular um ambiente organizacional e seus problemas, de forma a minimiza-los em uma rede e a auxiliar o administrador em suas tarefas.

6.1 METODOLOGIA

O projeto de pesquisa passou por um levantamento bibliográfico em livros e também junto a Internet em monografias e dissertações. A partir destes foi possível compreender como funciona a gerência de uma rede, bem como as técnicas aplicadas para diagnosticar e administrar a rede e seus ativos.

Os casos de testes foram direcionados a exemplificar alguns problemas ocasionados na rede de uma organização, de forma similar, e não explorando todas as possibilidades, em função da quantidade de informações a serem analisadas. A detecção e a resolução de alguns problemas foi demonstrado por meio do uso dos softwares escolhidos, extraindo alguns resultados de forma a possibilitar algum tipo de análise, com o intuito de ajudar o administrador de rede a diminuir algumas rotinas no gerenciamento de uma rede de computadores.

Os testes foram voltados para as rotinas de utilização da rede, onde foi realizado acessos indevidos à informações e sites, adição e retirada de dispositivos USB e alguns elementos de hardware dos equipamentos, a utilização dos clientes simulando rotinas de utilização e acessos, instalação de softwares e tentativas de burlar as políticas de segurança da rede, dentre outros testes voltados para o monitoramento, controle, segurança e desempenho dos elementos da rede afim de utilizar as ferramentas de gerência.

6.1.1 Definição do Ambiente

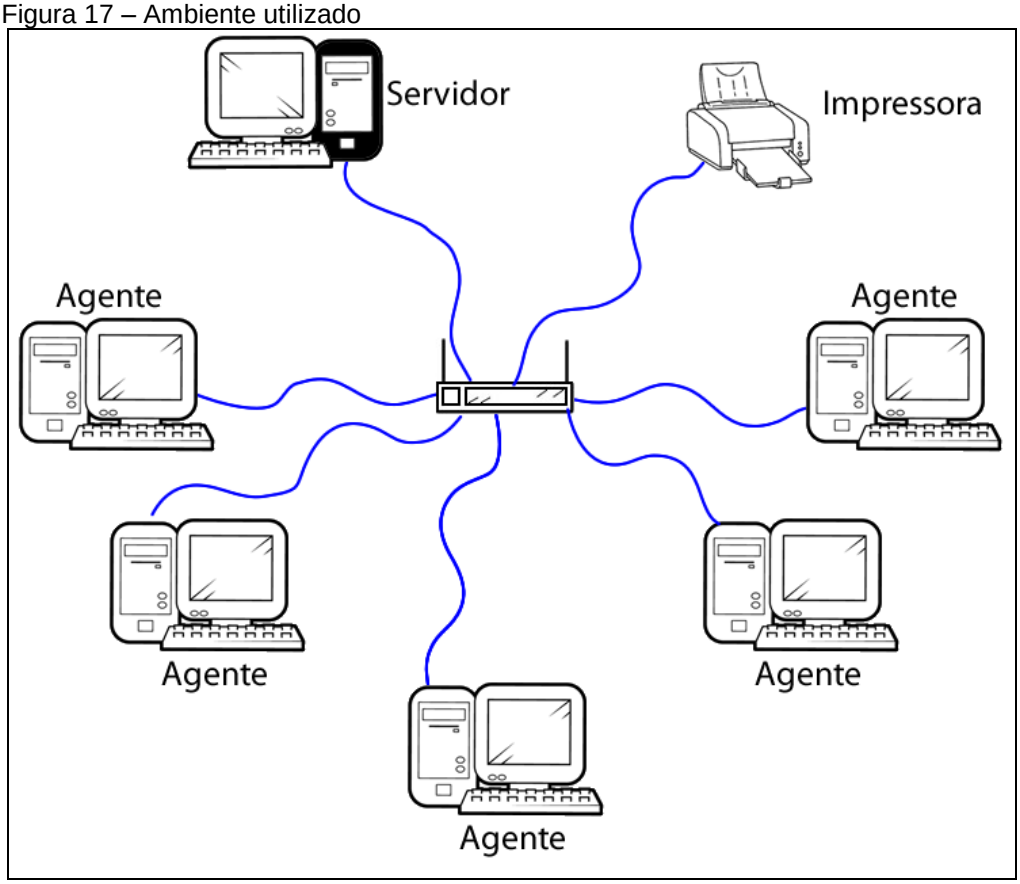
Foram definidos dois ambientes para a realização deste projeto de pesquisa. O primeiro utilizado para implantação da rede e de sua gerência foi um laboratório de informática, foi possível simular uma rede organizacional. Foram utilizados três computadores com plataforma Microsoft Windows 8 rodando a aplicação cliente e utilizado um servidor com a plataforma Linux. O segundo ambiente foi um escritório, com cinco computadores funcionando como agentes, um roteador e uma impressora multifuncional. Um servidor central foi o responsável por rodar a aplicação gerente e possibilitar o compartilhamento dos recursos de todos os equipamentos.

Dentre as seis máquinas agentes selecionadas, dois possuíam o sistema operacional Microsoft Windows 7, um com Microsoft Windows 8 e as outras duas estão com Microsoft Windows XP. O computador servidor estava equipado com o sistema operacional Microsoft Windows 8.

A máquina gerente foi instalado e configurado os softwares Cacti e NetEye, de forma a proporcionar a utilização de acordo com a rede. Sendo que nos outros equipamentos foram instaladas instâncias cliente desses software. A partir daí foi possível obter algumas variáveis da MIB, para análise posterior dos resultados de cada um dos recursos acessados.

A figura 17 demonstra o ambiente de rede utilizado no projeto.

Figura 17 – Ambiente utilizado



Fonte: Do Autor.

Na ferramenta NetEye, os testes possíveis são do inventário, produtividade, monitoramento, segurança e desempenho. Já na ferramenta Cacti, é possível testar o monitoramento e desempenho. Depois de definido o ambiente de monitoração, utilizou-se as ferramentas para captura das informações de gerência, onde foi utilizado *polling* da estação gerente para as estações clientes, pelo protocolo SNMP.

6.2 RESULTADOS OBTIDOS

Nesta etapa, foi realizado o monitoramento de cada uma das estações, por meio dos softwares de gerenciamento Cacti e NetEye.

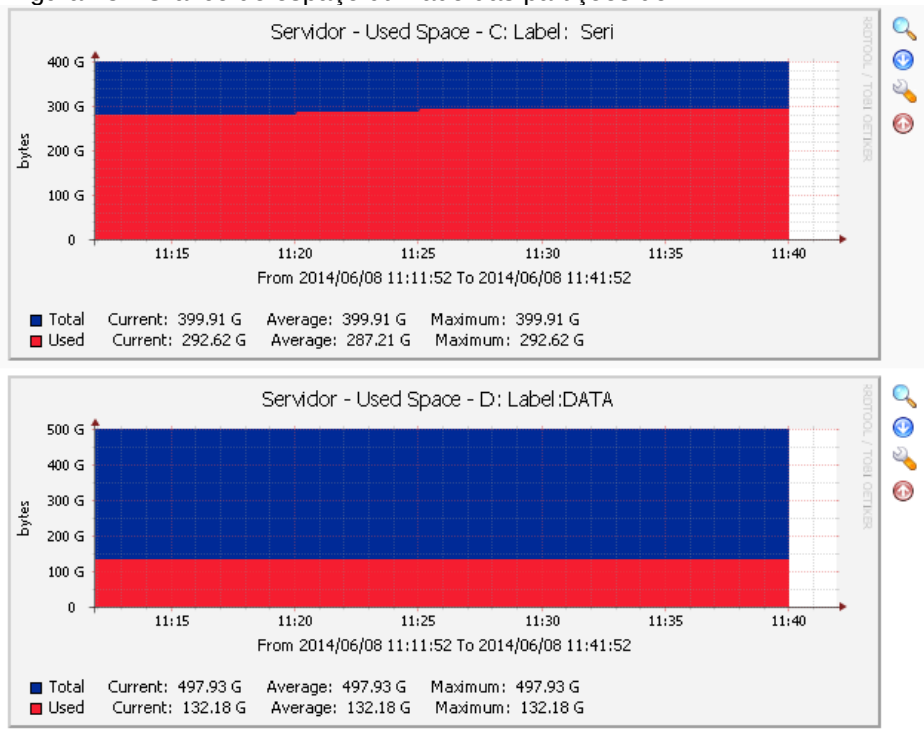
6.2.1 Resultados Obtidos com Cacti

O software Cacti demonstrou ter um grande potencial, porém apresenta grande complexidade na configuração. Os resultados foram satisfatório dentre as tarefas que lhe foram solicitadas.

O teste realizado voltado para a captação de informações referente aos recursos utilizados nas máquinas se mostrou complexo. Por outro lado a forma que os resultados da consulta são demonstrados é um ponto positivo para o Cacti, pois é possível analisar todas as informações de modo a permitir inúmeras possibilidades.

A figura 18 demonstra espaço utilizado e o disponível no HD e suas partições.

Figura 18 - Gráfico de espaço utilizado das partições do HD



Fonte: Do Autor.

Todos gráficos são gerados a partir de um *plugin* com a ferramenta RRDTool, demonstrando os resultados da consulta de forma dinâmica, dando a possibilidade de exportar esse gráfico para o formato PHP.

Mesmo rodando em um servidor Apache local, a aplicação demonstrou um pouco de instabilidade quando usada em plataforma Windows, pois algumas vezes ela não encontrava a solicitação desejada, ou seja, ocorria pequenas quedas do servidor. Porém rodando em ambiente Linux a mesma funcionou com rapidez e sem instabilidades.

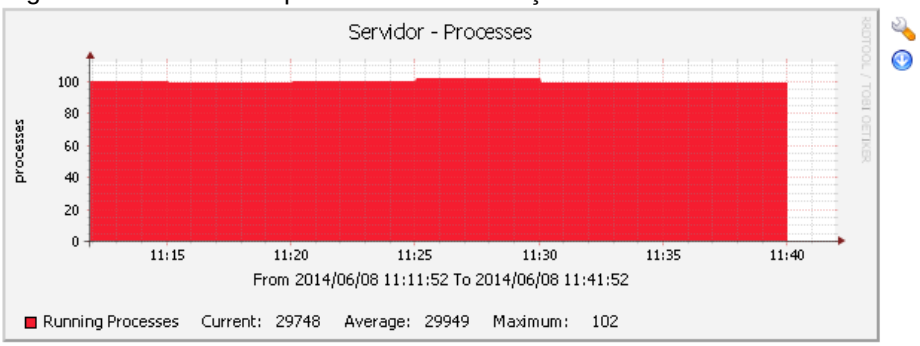
A adição de novos dispositivos para serem monitorados é algo relativamente fácil de se realizar. Pois em poucos minutos é possível adicionar um novo dispositivo e já acessar todas as suas informações. Lembrando é claro de que

é necessário a ativação do protocolo SNMP, visto no apêndice A para plataforma Windows e no B para ambiente Linux.

A velocidade para acesso a todas as funcionalidades foi boa, mesmo com algumas instabilidades de acesso, o sistema se mostrou bem otimizado. Onde a resposta ao clicar em um comando foi realizada em tempo real, principalmente na geração de gráficos onde se exigia um pouco mais de processamento.

Através da funcionalidade de criação de gráficos do Cacti é possível obter algumas informações como a quantidade de processos que estão sendo executados na máquina, visto na figura 19.

Figura 19 - Gráfico dos processos em execução

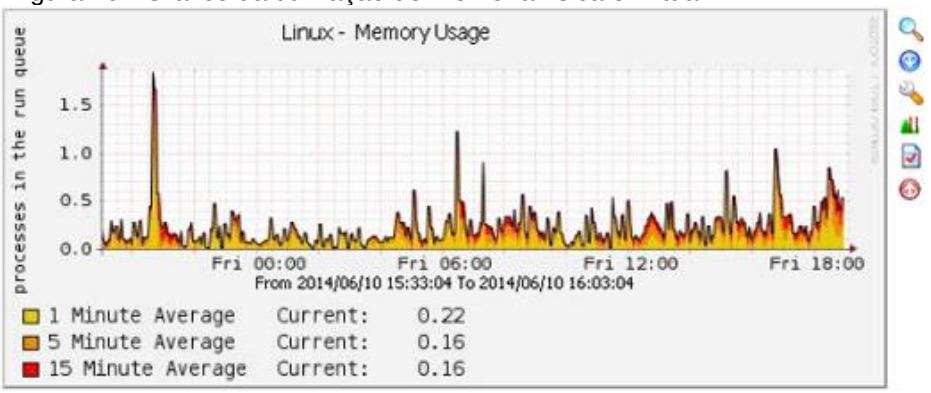


Fonte: Do Autor.

Alguns dos problemas que foram observados na ferramenta, é que nem sempre a opção de gráfico selecionado para computadores com a plataforma Microsoft Windows é a mesma de computadores com Linux.

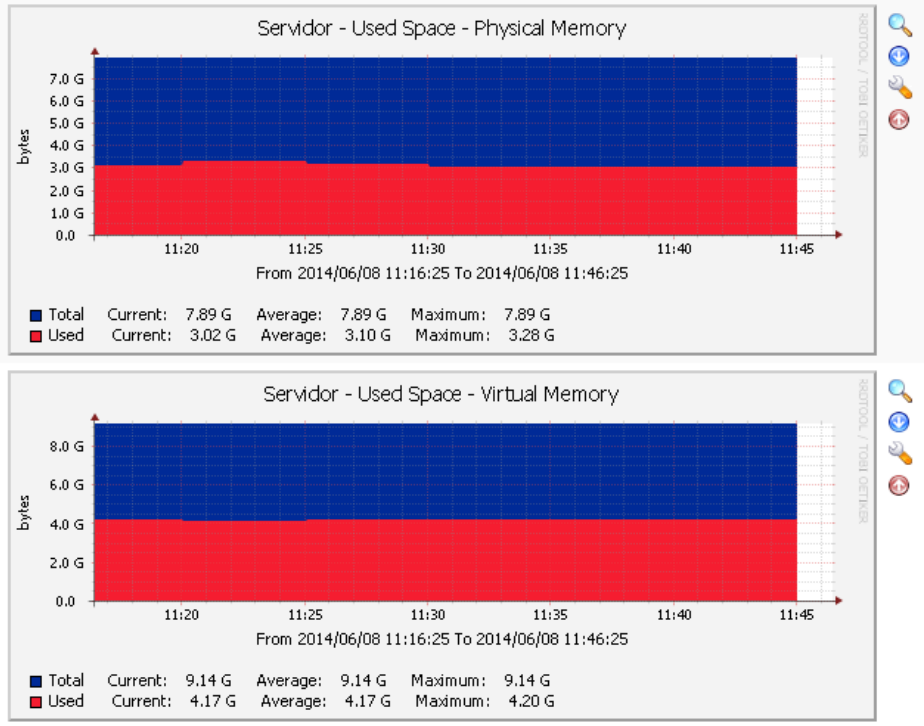
Por exemplo com o Linux é possível observar a memória utilizada em uma opção diferente do Windows. Na figura 20 pode-se observar o gráfico de uma máquina Linux demonstrando a memória utilizada. Já na figura 21 um gráfico que demonstra a memória virtual e física utilizada de uma máquina Windows. Isto porque não é possível utilizar a mesma opção para gerar estes gráficos em ambos os sistemas.

Figura 20 - Gráfico da utilização de memória física e virtual



Fonte: Do Autor.

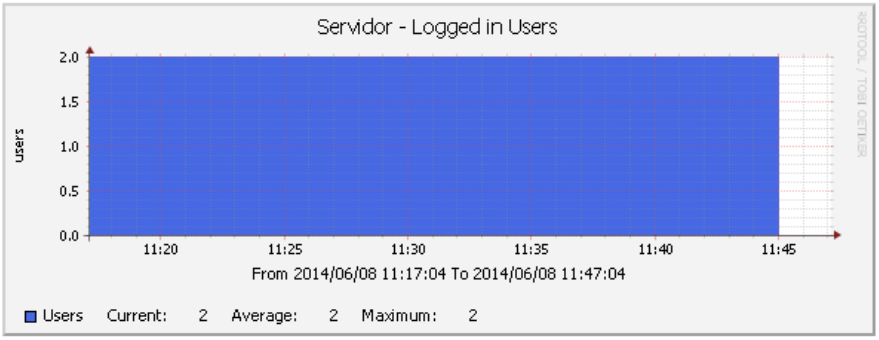
Figura 21 - Gráfico da utilização de memória física e virtual



Fonte: Do Autor.

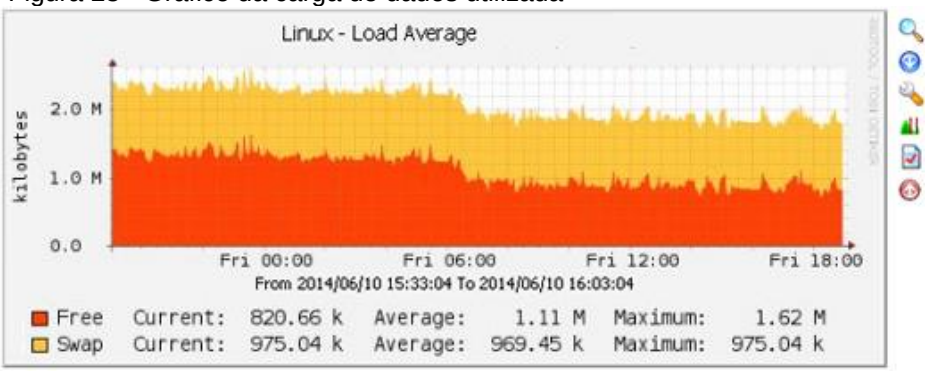
Outras informações possíveis são a possibilidade de analisar quantos usuários estão conectados em uma estação de trabalho e a quantidade de carga de dados utilizada. Nas figuras 22 e 23 são demonstrados estes gráficos respectivamente.

Figura 22 - Gráfico da quantidade de usuários logados



Fonte: Do Autor.

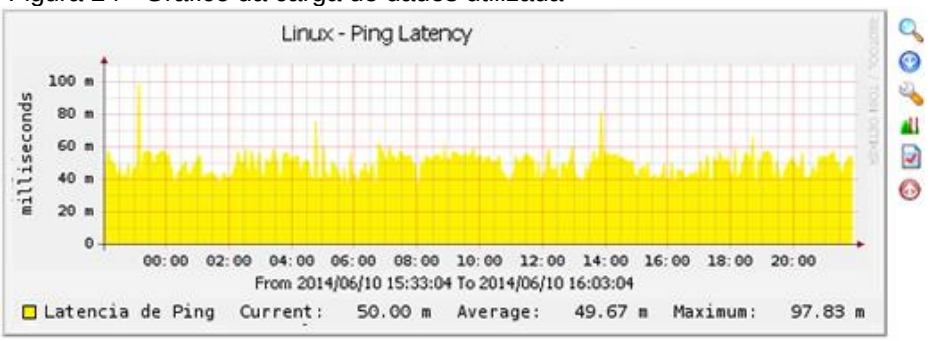
Figura 23 - Gráfico da carga de dados utilizada



Fonte: Do Autor.

Outra análise é o de latência do ping, que apresenta o tempo necessário para obter a resposta da requisição. Porém este gráfico está disponível apenas para máquinas clientes rodando Linux. A figura 24 demonstra este gráfico.

Figura 24 - Gráfico da carga de dados utilizada



Fonte: Do Autor.

O Cacti possui a capacidade de adicionar novas possibilidades e funcionalidades por meio de plugins. A instalação dos complementos pode ser visto no apêndice A.

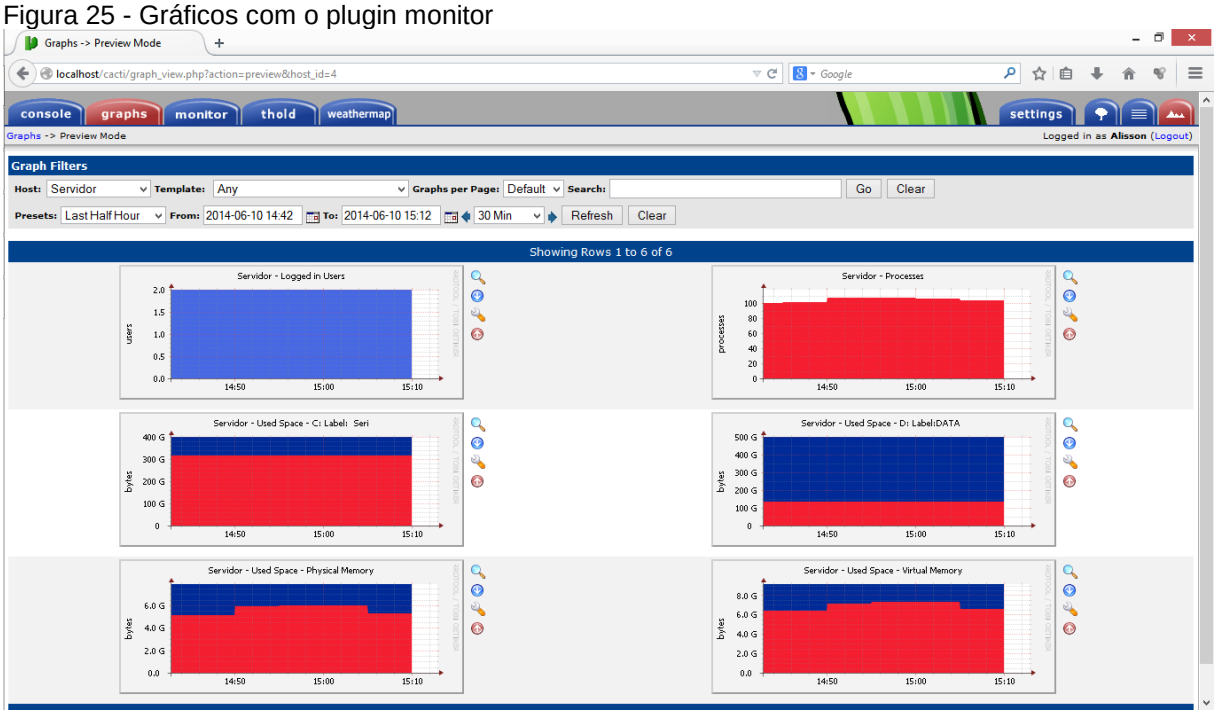
Estes plugins podem ser obtidos no site docs.cacti.net/plugins, onde possui um repositório com todos os disponíveis, nas suas versões mais recentes. É

bom ter cautela com os complementos, pode ocorrer a perda de informação e instabilidade no monitoramento e controle da rede. Por isso, eles são divididos no grupo de desenvolvedores e em usuários da comunidade.

Para a realização foi utilizado três complementos, sendo eles o monitor, thold e weathermap. O monitor é utilizado para ver as estatísticas das entidades com um tempo de atualização menor, demonstrando as falhas e o tempo de resposta. O thold dispara alarmes via e-mail informando determinados acontecimentos na rede. O weathermap possibilita a criação de um mapa para apresentação da estrutura da rede.

O plugin monitor possibilita ver os gráficos gerados com um tempo menor de resposta, interessante para determinadas máquinas que necessitam da captação das informações em menor tempo. Ele foi criado pelos desenvolvedores do Cacti e demonstrou um bom desempenho. A figura 25 demonstra a visualização dos gráficos com este complemento.

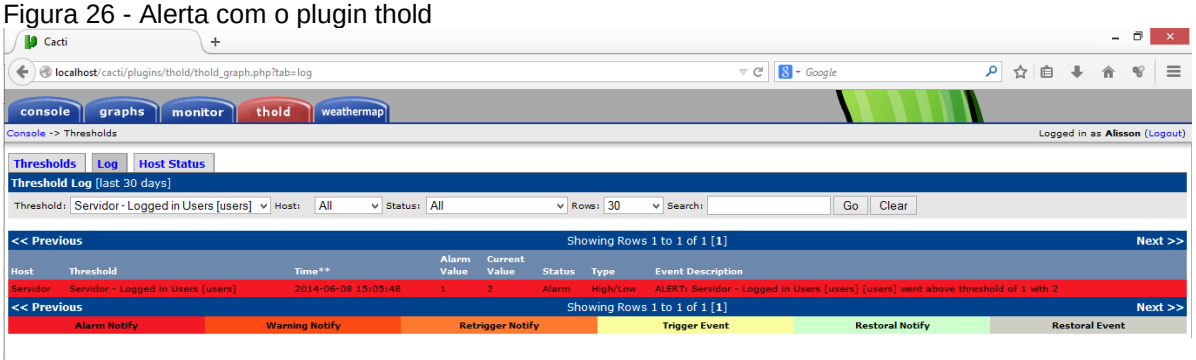
Figura 25 - Gráficos com o plugin monitor



Fonte: Do Autor.

O *thold* permite que o administrador de rede receba os alertas quando por exemplo uma estação de trabalho saia da rede. A figura 26 demonstra a visualização desse alerta quando mais de um usuário utiliza a mesma máquina.

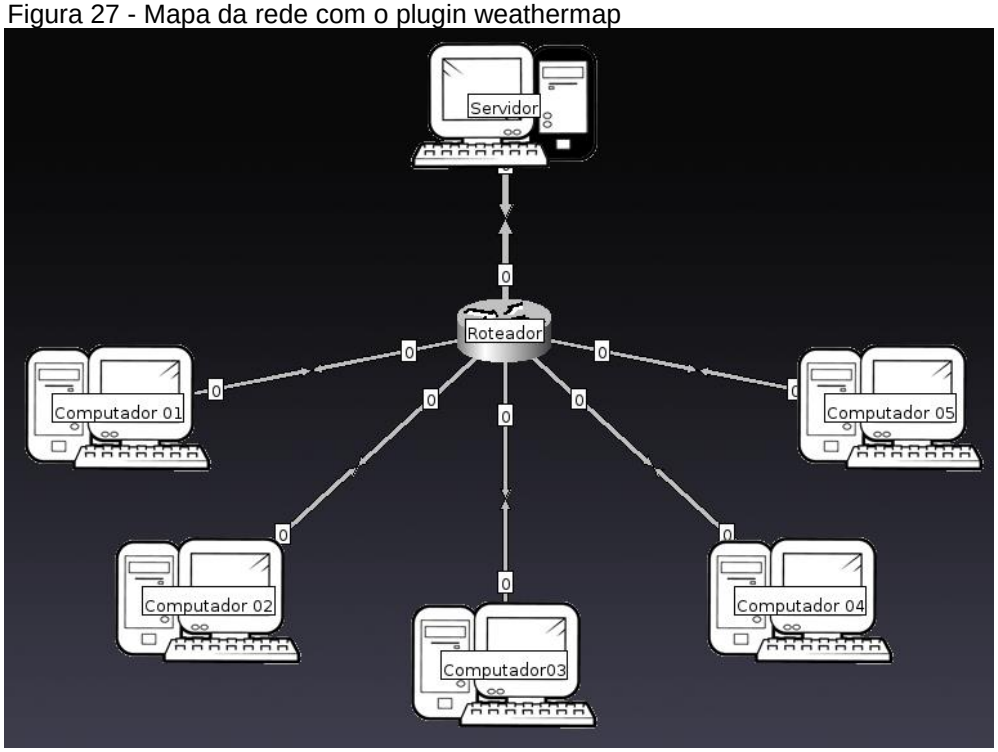
Figura 26 - Alerta com o plugin thold



Fonte: Do Autor.

O complemento *weathermap* possibilita a criação manual da estrutura de rede, assim é possível organizar as conexões, servidores e roteadores disponíveis na rede de forma a auxiliar o administrador a encontrar o dispositivo e seu local físico. Através dele foi criado uma mapa da rede utilizada para testes, vista na figura 27.

Figura 27 - Mapa da rede com o plugin weathermap



Fonte: Do Autor.

Os resultados obtidos com o Cacti demonstraram que a ferramenta entrega as estatísticas da rede de uma maneira gráfica organizada. Onde através dessas informações é possível analisar a real situação da rede e as máquinas que a compõem, monitorando todos os processos e rotinas envolvidos.

6.2.2 Resultados Obtidos com NetEye

Os resultados obtidos através dos testes aplicados no software NetEye foram surpreendentes, demonstrando ser uma ferramenta completa nos quesitos de monitoração e segurança da rede. Seu dinamismo em realizar as tarefas solicitadas atrelado ao desempenho permitiram que a sua utilização fosse satisfatória, mesmo em servidores com pouco poder de hardware houve rapidez nas respostas.

As suas funcionalidades abrangem todas as áreas do modelo FCAPS utilizado, permitindo um gerenciamento completo de todos os processos que envolvem uma rede de computadores.

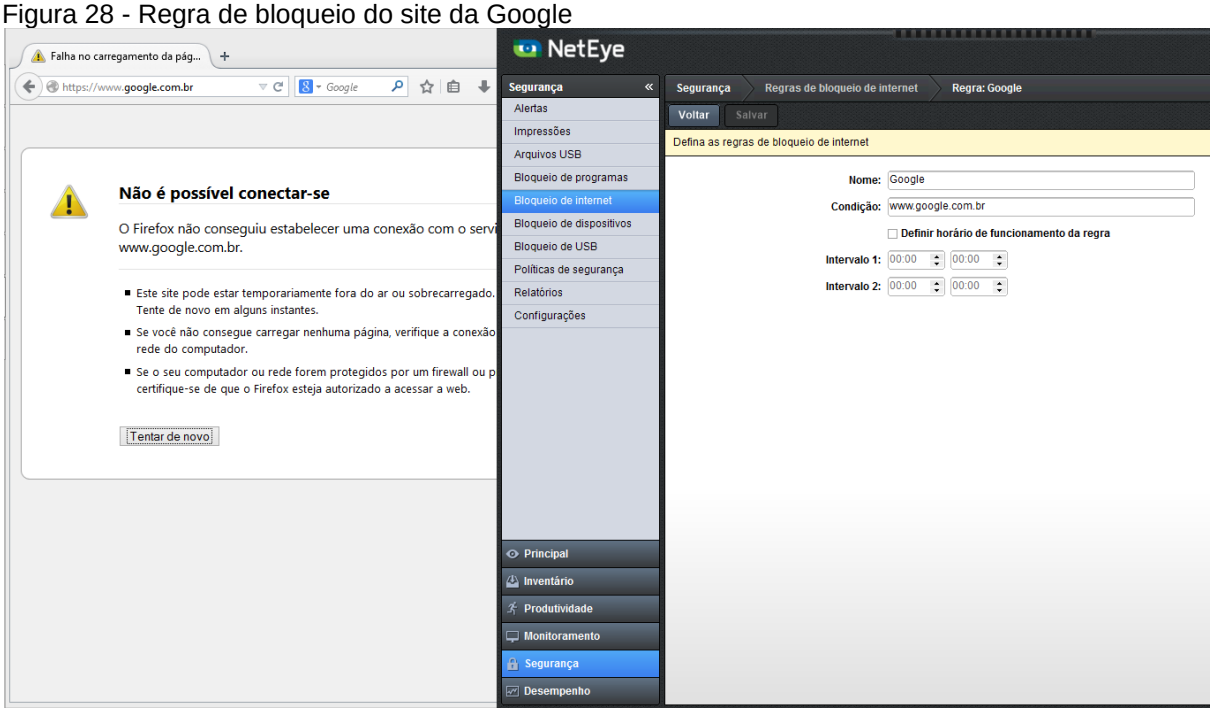
Como é o caso da gerência de segurança, na qual pode ser realizada através do módulo de mesmo nome, onde é possível restringir os acessos de clientes, impossibilitando-os de acessar determinados programas, que são configurados na opção bloqueio de programas. Quando o usuário tentar acessar, será apresentada uma mensagem que o impossibilitará de continuar.

A utilização de dispositivos USB pode ser bloqueada, sendo que desta forma quando o usuário colocar seu dispositivo, nada ocorrerá. Este tipo de bloqueio é essencial em uma empresa, pois 30% dos vírus são causados por dispositivos USB (KASPERSKY, tradução nossa, 2014).

No módulo de produtividade os conceitos do gerenciamento de segurança podem ser aplicados, permitindo que o administrador bloqueie a navegação da estação por meio de palavras, estas são configuradas no menu de segurança bloqueio de Internet.

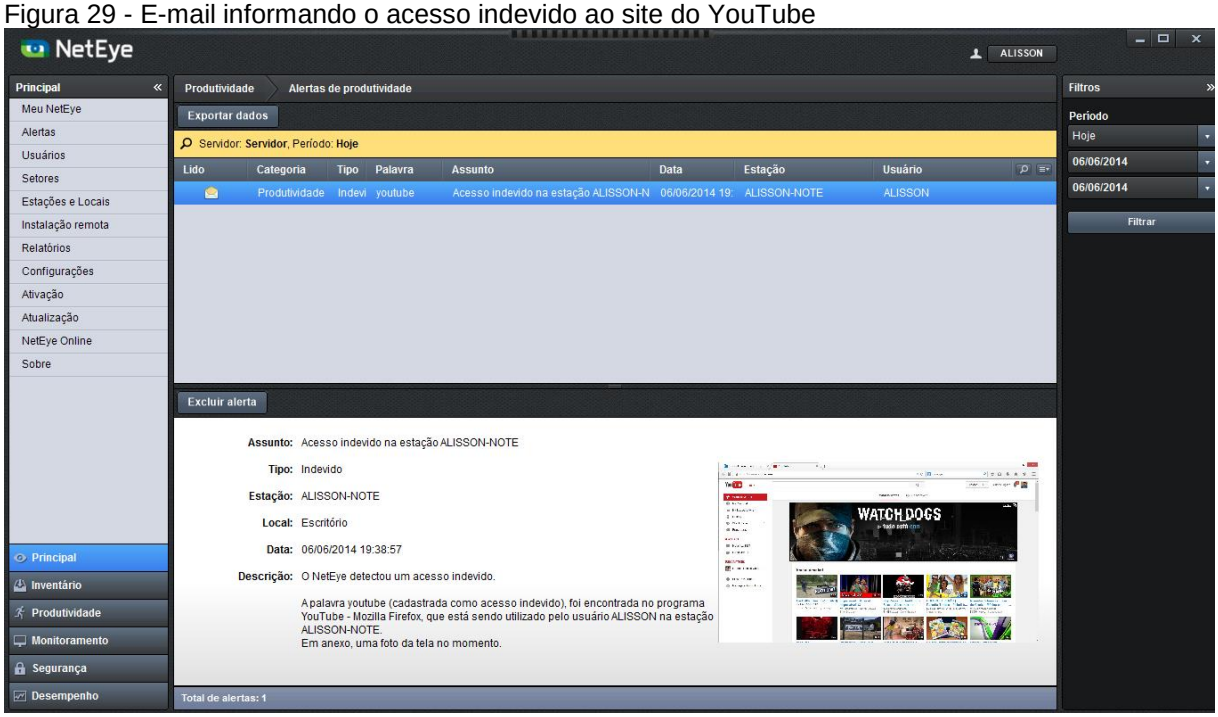
Por exemplo o administrador cadastra o termo youtube, o usuário irá tentar acessar uma página contendo esta palavra e receberá um alerta de bloqueio. Existe a possibilidade de permitir o acesso ao usuário, porém será enviado uma captura de tela do usuário para o administrador.

Figura 28 - Regra de bloqueio do site da Google



Fonte: Do Autor.

Figura 29 - E-mail informando o acesso indevido ao site do YouTube



Fonte: Do Autor.

É possível interromper um processo no modulo de monitoramento. Sendo uma função interessante no caso de um processo diferente do habitual estar executando em uma máquina, podendo ser até mesmo um vírus, o administrador simplesmente o encerra.

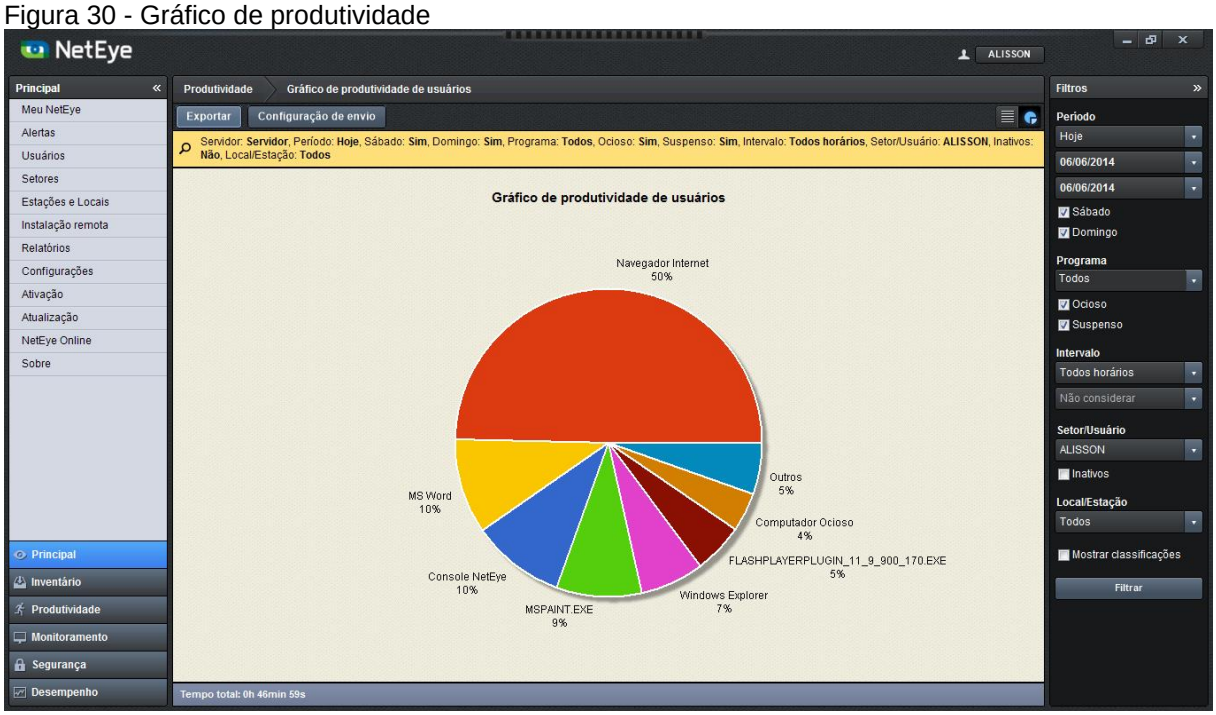
Os conceitos da gerência de contabilidade podem ser utilizados através de três módulos do programa, de segurança, produtividade e monitoramento. Com estes pode se registrar todas as informações dos arquivos utilizados na máquina, acessados pela rede e até mesmo em dispositivos USB conectados. Esses dados podem ser analisados afim de descobrir quais os tipos de arquivos que os clientes mais estão acessando.

A impressão de documentos pode ser monitorada, onde é registrado todos os arquivos enviados para a impressora e a suas quantidades de folhas. Com esta função é possível diminuir o consumo de tinta evitando gastos com a impressão de documentos desnecessários.

O processo de produtividade permite que o gerente observe todas as aplicações que foi e está sendo utilizada em determinada estação. Demonstrando em um gráfico a porcentagem do tempo que o computador está ligado gasto em cada programa e também o tempo em que o sistema ficou ocioso.

A figura 30 demonstra o gráfico de estatística de utilização do sistema por parte do usuário.

Figura 30 - Gráfico de produtividade



Fonte: Do Autor.

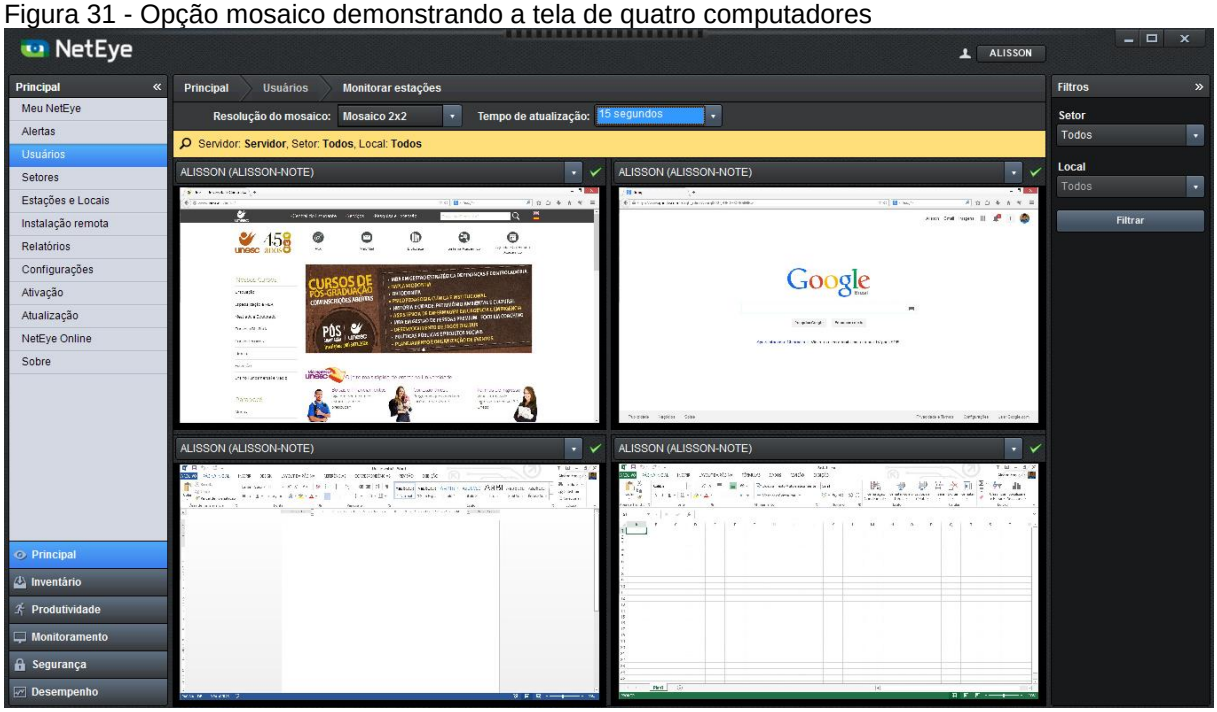
Está funcionalidade é um grande diferencial na ferramenta, pois permite de forma prática e intuitiva a visualização de todas as informações a respeito da utilização da máquina pelo cliente, gerando uma análise da produtividade.

O acompanhamento das informações pode ser feito também com as estações off-line, sendo está uma opção configurável para cada cliente. Assim mesmo quando o usuário não está conectado à rede, é registrado os seus dados e enviados posteriormente para o gerente.

O monitoramento pode ser realizado por meio do acompanhamento da tela do usuário, onde escolher por capturas de telas atualizadas em um período configurável ou em tempo real com a opção de acesso remoto. Sendo interessante para analisar esporadicamente a utilização da máquina por parte dos usuários.

Existe a possibilidade de observar até 20 telas ao mesmo tempo por meio da opção chamada de mosaico, como demonstra a figura 31.

Figura 31 - Opção mosaico demonstrando a tela de quatro computadores



Fonte: Do Autor.

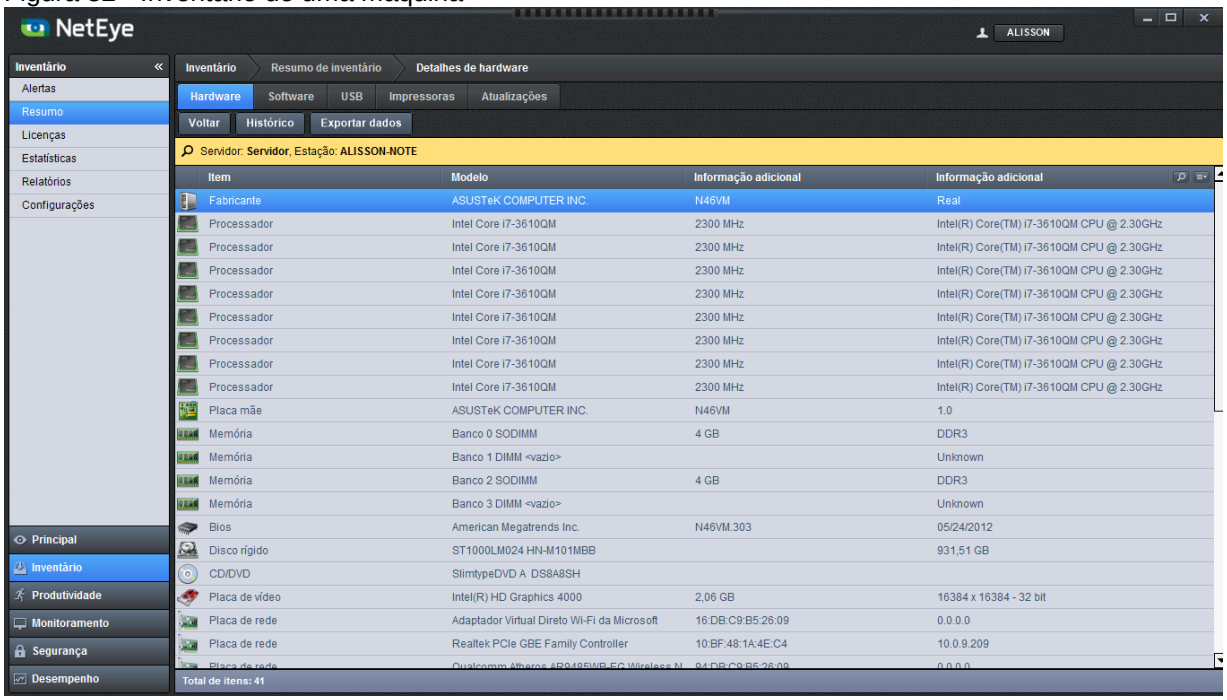
Os discos rígidos das estações podem ser acessados diretamente do NetEye, seja para realizar uma transferência de arquivos ou apenas para monitorar seu conteúdo. Há ainda a função de enviar mensagens de alertas para os usuários informando-os de algo.

O gerenciamento de falhas na rede funcionado através da opção de receber alertas quando uma máquina saiu da rede por problemas técnicos. Desta maneira o administrador não precisa se preocupar em ficar monitorando todas as máquinas de forma a garantir que todas estão conectadas e em funcionamento, pois o mesmo será notificado automaticamente.

A gerência de configuração inicia com a funcionalidade do inventário, onde é possível realizar um levantamento de todos os softwares, hardwares, USB, impressoras e atualizações dos softwares instalados.

A figura 32 apresenta o inventário de uma máquina da rede.

Figura 32 - Inventário de uma máquina



Fonte: Do Autor.

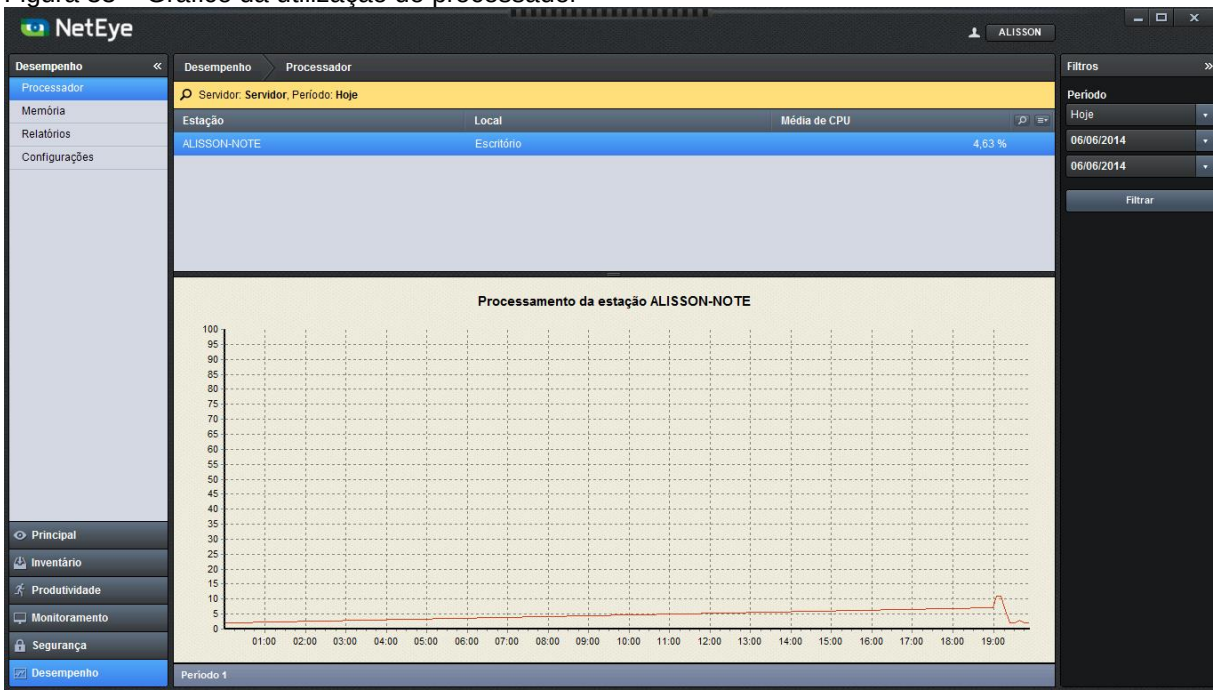
Está funcionalidade é importante, de forma a obter todas as informações dos periféricos de um dado equipamento específico. Sendo possível controlar quais foram removidos ou adicionados, sem que o administrador necessite abrir o equipamento e nem esteja no local do equipamento.

O resumo de softwares permite listar todos os programas instalados e analisar se suas licenças estão em dia, evitando assim que softwares ilegais sejam utilizados em máquinas da rede. É possível realizar um levantamento até dos dispositivos USB utilizados.

O inventário do NetEye notifica o gerente da rede caso houver uma determinada alteração em um computador. Por exemplo, uma estação possui dois pentes de memória, porém por algum motivo u m desses pentes é retirado da máquina. O administrador receberá um alerta informando de que tal máquina sofreu uma mudança de hardware, neste caso a memória.

O módulo de desempenho é quem cuida da gerência de desempenho da rede, onde é possível registrar todo um histórico de utilização da memória e da CPU. Isto permite analisar se o computador não está sobrecarregado com os processos do cotidiano e quando que deverá ser realizado uma atualização em seu hardware.

Figura 33 – Gráfico da utilização do processador



Fonte: Do Autor.

As informações de desempenho permitem que as estações de trabalho sejam comparadas, afim de observar se todas elas estão com um mesmo padrão de processamento. Esta funcionalidade auxilia no mapeamento dos recursos utilizados pelo computador na rede.

Por meio de um registro do histórico de manutenção e mudanças nos computadores, é possível analisar quando determinado hardware foi alterado. Estes registros são importantes para avaliar uma alteração futura da rede.

Um de seus problemas é a demora para instalação, pois somente através do instalador próprio é realizado o download da ferramenta.

Outro ponto negativo na instalação é a necessidade de utilizar o banco de dados Microsoft SQL Server 2008 ou superior, pois trata-se de um banco muito robusto. Porém caso o computador não possua instalado, o próprio instalador do NetEye baixa e o instala, deixando totalmente configurado para a utilização do programa.

Os testes realizados com o NetEye retornaram um bom resultado, entregando ao administrador uma plataforma que o auxilia a tomar as decisões a respeito de sua rede. Possibilitando diminuir os gastos que normalmente envolvem essas interconexões, além de permitir controlar todos os serviços e recursos que nela são executados e planejar um possível crescimento.

Para os testes com o monitoramento dos dispositivos foi realizada a utilização das estações de trabalho gerando uma carga de acesso a sites, e em seguida a geração de um relatório, para ser posteriormente analisado pelo administrador da rede.

Foram criadas situações para que fosse possível utilizar o acesso remoto das máquinas, e também o acompanhamento via captura de tela. Esses testes tiveram como objetivo o monitoramento dos clientes analisando o que os mesmos estão acessando e usando.

Realizaram-se diversas impressões de documentos para que fosse possível monitorar a utilização da impressora e seu gasto. Onde analisou-se a quantidade de arquivos que foram impressos e também a quantidade de páginas.

Por fim foi instalado alguns programas para observar se era possível obter as informações de instalação em tempo real. Onde também foram executados determinados processos e programas para que fosse possível a geração de relatórios e gráficos demonstrando toda está utilização por parte do usuário.

Os testes de segurança realizados buscaram garantir que os usuários não realizassem acessos não autorizados e o uso indevido de determinados recursos, Utilizando as ferramentas gerenciais para que os usuários seguissem obrigatoriamente todas as políticas adotadas pelo administrador de rede.

Nestes testes foram realizados acessos a sites indevidos para que fosse possível avaliar as funcionalidades de bloqueio e alertas enviados pelos programas. Garantindo que o acesso à Internet seja feito apenas dentro do que a rede permite.

Utilizou-se diversos softwares ilícitos que possuem a funcionalidade de burlar a rede e seus bloqueios. Um desses programas é o Tor, no qual permite que a Internet seja acessada de maneira anônima, sendo possível burlar o bloqueio de uma rede. Estes testes foram realizados para que a eficiência de bloqueio das ferramentas fosse verificada.

Foram realizados testes de bloqueio de USB, onde não permite que o usuário utilize esses dispositivos. Assim como o bloqueio de drivers de CD, bluetooth

e outros dispositivos. Também foi analisado a aplicação de regras onde o usuário tentava desativar determinado processos através do gerenciador de tarefas.

A aplicação destes testes tem por objetivo criar uma carga de resultados que foram analisados para definir a eficácia dos programas em garantir a segurança da rede.

Foi realizado o teste de desempenho, onde a primeira etapa deste teste será a instalação e configuração das aplicações, onde será instalado todo os seus conjuntos de ferramentas necessárias. Neste quesito foi levado em conta a complexidade e o tempo levado para que o sistema esteja totalmente pronto para ser utilizado. Porém aqui não será considerado o tempo de instalação e ativação do protocolo SNMP, visto que as aplicações concorrentes também necessitam de tal protocolo para seu funcionamento, desconsiderando assim este tempo.

Outro ponto em que o sistema possuirá um foco é a usabilidade, onde serão consideradas as facilidades de entrar no sistema, o tempo gasto para procurar e encontrar determinada funcionalidade e a dificuldade de utilização dela. Sendo avaliado a interface, levando em consideração pontos como a demonstração e separação das informações na tela e a iteratividade da aplicação com o usuário.

A usabilidade pode se dividir em dois pontos, pois o desempenho terá total relação com a usabilidade da ferramenta. Para analisar o desempenho observou-se os tempos de resposta para as requisições em um servidor com configurações avançadas. Sendo memória RAM de 8GB, HD de 1TB, processador Intel Core i7 e sistema operacional Microsoft Windows 8.

Também foi utilizado servidores com configurações intermediárias e limitadas. Através destes outros servidores as aplicações foram instaladas e configuradas a fim de observar possíveis travamentos e lentidões ao executar as tarefas propostas. As configurações desta máquina foram de 2GB de memória RAM, 250GB de HD, processador Intel Dual Core e sistema operacional Microsoft Windows 7. Já as configurações do computador de menor porte foram de 1GB de memória RAM, 10GB de HD, processador Intel Celeron e sistema operacional Microsoft Windows XP.

6.2.3 Monitoramento dos Softwares em Conjunto

A pesquisa levantou e utilizou as funcionalidades dos softwares Cacti e NetEye com enfoque no gerenciamento de rede afim de analisar os resultados obtidos, buscando observar a aplicações em alguns dos problemas ocasionados em uma rede. A intenção é utilizar os dois softwares em conjunto, ou seja, levantar as funcionalidades de um que completam o que falta no outro. Para tanto, foi analisado os resultados obtidos com o estudo de caso e observado em quais quesitos ambos se destacam, demonstrando as áreas de atuação de cada software. Assim conclui-se que utilizados em conjunto tem-se um gerenciamento mais qualitativo e abrangente.

As duas ferramentas não são capazes de se comunicar e trocar informações entre si, porém é possível utilizar ambas em conjunto afim de melhorar a gerencia da rede. Além de que o funcionamento de uma não atrapalha o da outra, fazendo com que as duas possam ser utilizadas em uma mesma rede sem maiores problemas.

A tabela 1 comparar determinadas funcionalidades de cada ferramenta.

Tabela 1 – Comparação de funcionalidades entre Cacti e Netye.

Funcionalidade	Cacti	NetEye
Monitoramento	X	X
Controle		X
Contabilidade	X	X
Segurança		X
Desempenho	X	X
Gráficos estatísticos	X	
Adição de funcionalidades (plugins)	X	
Gratuito	X	
Alertas	X	X
Inventário		X

Fonte: Do Autor.

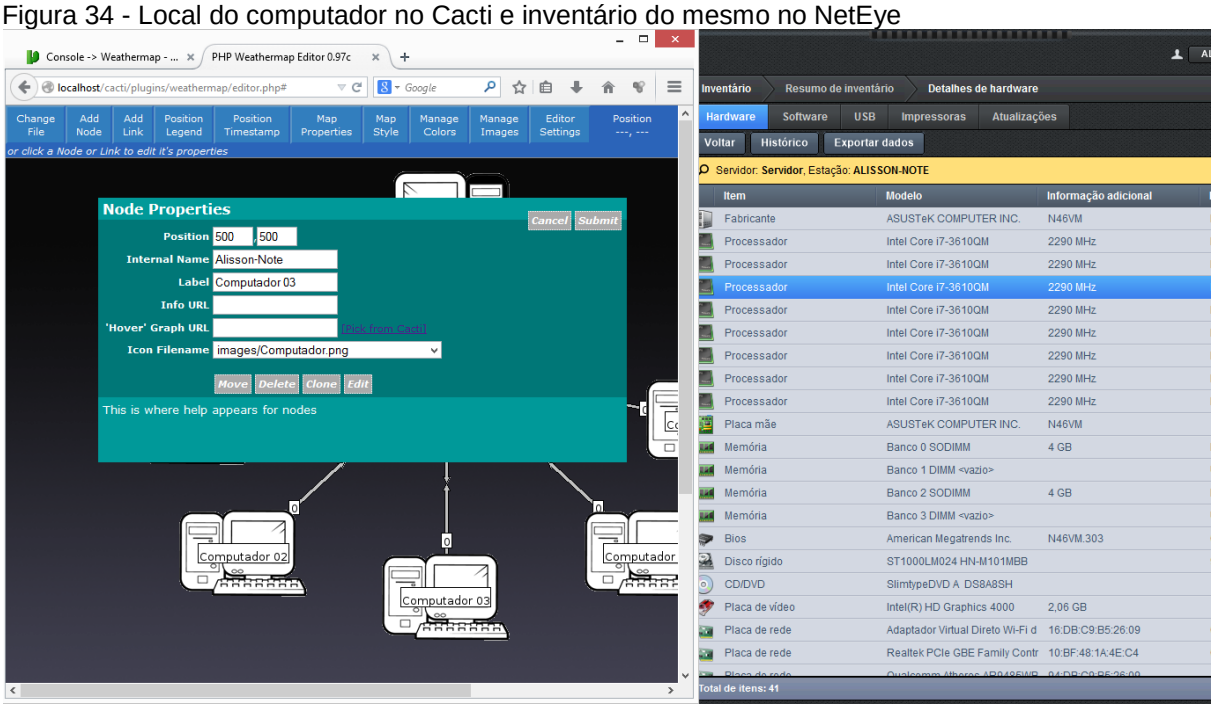
Os resultados demonstraram que a utilização de uma pode ser capaz de satisfazer as rotinas administrativas, porém ao juntar as funcionalidades particulares de cada uma pode levar a administração da rede a outros níveis, além de facilitar a gerência.

No emprego das duas ferramentas existem diversas funções que podem ser utilizadas em conjunto para que o gerente possa ter informações mais confiáveis e consistentes.

Por exemplo, utilizar a funcionalidade de criação do mapa da rede para observar onde determinado computador se encontra e através do módulo de inventário do NetEye, olhar as configurações de hardware desta mesma máquina. Assim é possível encontrar o setor e local físico em que a máquina se encontra, sabendo se as configurações de hardware estão atualizadas para seu ambiente.

Na figura 34 é possível observar o local em que o computador se encontra no Cacti e seu inventário através do NetEye.

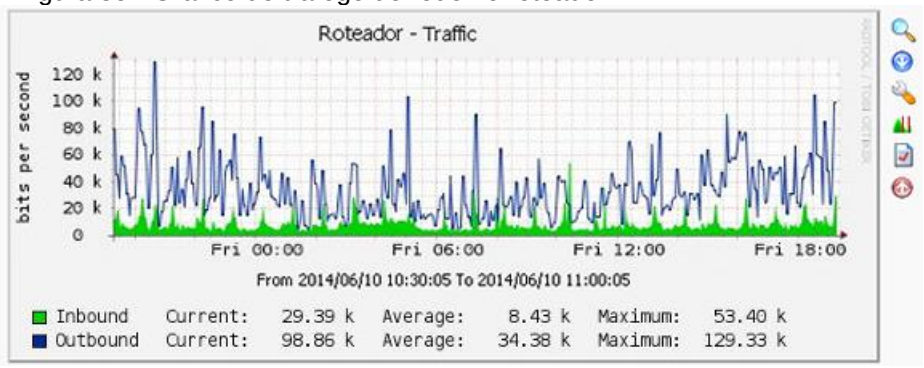
Figura 34 - Local do computador no Cacti e inventário do mesmo no NetEye



Fonte: Do Autor.

A utilização do Cacti também é importante para o monitoramento de roteadores, sabendo através de gráficos o tráfego da rede. Na figura 35 é possível observar este gráfico que apresenta a quantidade de informações trafegadas na rede através do roteador.

Figura 35 - Gráfico de tráfego de rede no roteador



Fonte: Do Autor.

O NetEye é permite realizar o monitoramento off-line das máquinas, ou seja, quando a máquina não estiver na rede a mesma registrará as informações e quando conectada na rede novamente enviará estas informações para o servidor. Sendo que através do plugin thold do Cacti é possível receber o alerta em tempo real de que este computador saiu da rede, deixando o administrador informado, quando a mesma se reconectar na rede será possível saber se ela saiu da rede ou foi apenas desligada.

A viabilidade de adição de plugins no Cacti é importante, pois sempre existe a possibilidade de adicionar novas funcionalidades que contemplem ainda mais a administração da rede.

Toda essa capacidade pode ser aliada ainda ao poder de controle do NetEye, sendo que através dele é possível garantir que os usuários sigam todas as políticas aplicadas a rede como citado anteriormente. Evitando acessos indevidos e possibilitando uma segurança adequada da rede.

A aplicação NetEye disponibiliza todas as suas documentações e guias em seu site oficial, mesmo sendo proprietário. Já o Cacti por ser aberto, acaba existindo diversos meios para acesso a essas informações.

Por fim os dois softwares demonstraram seu potencial e suas falhas, onde concluiu-se que quando utilizadas em conjunto pode se ter novas possibilidades administrativas, além de que ao captar as mesmas informações com as duas, pode se garantir a consistência dos dados.

7 CONCLUSÃO

Os estudos de casos aplicados auxiliaram no entendimento das técnicas gerenciais e de implementação de uma rede. Foi possível observar a importância de um planejamento com base na infraestrutura disponível para garantir que a rede possua uma organização gerencial capaz de administrar todas as suas rotinas.

As informações monitoradas e recolhidas por meio dos softwares foram capazes de abranger inúmeras rotinas da rede. Sendo que elas serviram para passar ao gerente um panorama geral, onde através de todos esses dados ele poderá tomar as melhores decisões para o funcionamento da sua rede.

A implantação de softwares para realizar o gerenciamento de redes se faz necessário para que seja possível controlar todas as entidades garantindo uma organização e qualidade. Essas aplicações garantem a amenização dos problemas ocorridos e do tempo gasto em busca de suas soluções. A gerência realizada demonstrou que as ferramentas são de suma importância para que a rede possa ter uma consistência no quesito administrativo e também usual.

O Cacti apresentou um grande potencial no monitoramento da rede demonstrando as informações através de gráficos, onde foi possível observar as informações de memória, disco, CPU, dentre outras. Utilizando tudo isso em conjunto com a sua capacidade de adição de *plugins* suas funcionalidades podem ser elevadas e melhores aproveitadas.

O NetEye por outro lado apresentou um resultado ainda melhor em quesitos como controle e segurança da rede, sendo capaz de impedir e controlar os acessos dos usuários. Através de seu módulo inventário é possível realizar um levantamento completo de todo o hardware disponível nas estações da rede, possibilitando ao administrador um planejamento futuro da rede.

Através dos resultados obtidos foi possível observar que apesar das duas ferramentas serem bem completas e capazes de monitorar e controlar diversas informações na rede, as funcionalidades de ambas podem se completar. A utilização em conjunto permite que o administrador possa analisar os dados das estações de uma maneira mais completa.

O gerenciamento de rede está constante evolução, partindo deste princípio como sugestão para estudos futuros ficam o de realizar estudos através de novas ferramentas e a possibilidade de integração com as citadas neste trabalho,

assim como o desenvolvimento de novos plugins para o Cacti com o intuito de otimizar as rotinas administrativas da rede.

REFERÊNCIAS

ABREU, Fabiano; PIRES, Herbert. **Gerência de Redes.** Disponível em: <http://www.midiacom.uff.br/~debora/redes1/pdf/trab042/SNMP.pdf>. Acesso em: 23 de setembro de 2013.

BARRETO, Grasielli. **Ferramentas de Gerência de Redes**. Paraná: Universidade Estadual de Londrina, 2008. Disponível em: <www2.dc.uel.br/nourau/document/?down=736> Acesso em: 28 de abril de 2013.

BEHROUZ, A. Forouzan. **Comunicação de Dados e Redes de Computadores**. 3. ed. São Paulo: Bookman, 2006.

BONOMO, Esley. **Gerenciamento e Monitoração de Computadores Utilizando-se Zabbix.** Paranaguá: Universidade Federal de Lavras, 2006. Disponível em: < http://www.ginux.ufla.br/files/mono-EsleyBonomo.pdf> Acesso em: 28 de abril de 2013.

CACTI. **Cacti - The Complete RRDTool based Graphing Solution.** 2013. Disponível em: <http://www.cacti.net/>. Acesso em: 27 de abril de 2013.

CACTI. **O que é o Cacti?.** Disponível em: <http://openmaniak.com/pt/cacti.php>. Acesso em: 28 de abril de 2013.

DUARTE, Jean. Relatório **Técnico de Meios de Transmissão.** Disponível em: <http://187.7.106.13/nataniel/Turmas_T3_T4/Conectividade/Trabalhos/MT_T3/JEAN_LUIGI_DUARTE%20%281%29.pdf>. Acesso em: 03 de setembro de 2013.

DUARTE, Lianna. **Gerência de Redes e Software Livre: Uso do Nagios.** Disponível em: <http://www.faete.edu.br/revista/ArtigoLiannaFSA.pdf>. Acesso em: 07 de setembro de 2013.
Editora Ciência Moderna Ltda., 2008.

FILHO, Olavo. **Gerenciamento e Monitoramento de Redes I: Análise de Desempenho.** Disponível em: <http://www.teleco.com.br/tutoriais/tutorialgmredes1/default.asp>. Acesso em: 23 de setembro de 2013.

ISO. **Internet Society Brasil**. Disponível em: <http://www.isoc.org.br/>. Acesso em: 23 de setembro de 2013.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet.** 3. ed. São Paulo: Pearson, 2005.

MACIEL, Luis. **Modelo de Gerência: FCAPS.** Disponível em: <www.trabalhosfeitos.com/ensaios/Modelo-De-Gerenciamento-Fcaps/40151422.html>. Acesso em: 23 de setembro de 2013.

MATOS, Leonardo K. **Um Processo de Gerência para Redes de Computadores em Ambientes de Software Livre.** Curitiba: Pontifícia Universidade Católica do Paraná, 2006. Disponível em: <http://www.bibliotecavirtual.celepar.pr.gov.br/arquivos/File/MonografiaseArtigos/Monografia_Leonardo_GerênciadeRedes.pdf> Acesso em: 28 de abril de 2013

MAURO, Douglas R.; SCHMIDT, Kevin J. **SNMP Essencial**. 1. ed. O'Reilly, 2001.

MENEZES, Elionildo; SILVA, Pedro. **Gerenciamento de Redes: Estudos de Procotolos.** Disponível em: <http://www.di.ufpe.br/~flash/ais98/gerrede/gerrede.html>. Acesso em: 23 de setembro de 2013.

MILLER, Mark. **Managing Internetworks with SNMP.** ed. 3. Chicago: M&T Books, 1999.

MOQADI, Kanan; SILVA, Verônica. **Uso de Ferramentas de Gerência de Rede para Análise de Desempenho de uma Rede Local**. Disponível em: <http://www.ulbra.inf.br/joomla/images/documentos/TCCs/2011_02/PROJETO_RC_KANAN_ALI_ABDULLA_MOQADI.pdf>. Acesso em: 07 de setembro de 2013.

MORIMOTO, C. E. **Servidores Linux: guia prático**. 2. ed. Porto Alegre: Sul Editores, 2009.

MORIMOTO, Carlos E. **Redes: Guia Completo.** 3. ed. Porto Alegre: Sul Editores, 2008.

NETEYE. **NetEye**. 2013. Disponível em: <http://www.neteye.com.br/en/>. Acesso em: 27 de abril de 2013.

OETIKER, T**. RRDtool - Logging and Graphing**. Disponível em: <http://oss.oetiker.ch/rrdtool/doc/rrdtool.en.html>. Acesso em: 27 de abril de 2013.

PINHEIRO, Marcos. **Gerenciamento de Redes - SNMP, RMON e CACTI.** Disponível em: <http://www.metropoledigital.ufrn.br/aulas_avancado/web/disciplinas/rede_comp/aula_15.html>. Acesso em: 03 de setembro de 2013.

PINHEIRO, Ricardo. **O Protocolo SNMP**. Disponível em: <http://www.mundotibrasil.com.br/o-protocolo-snmp/>. Acesso em: 03 de setembro de 2013.

RFC. **A Simple Network Management Protocol (SNMP).** Disponível em: <www.rfc-base.org/txt/rfc-1157.txt>. Acesso em: 23 de setembro de 2013.

RFC. **Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2).** Disponível em: <www.rfc-base.org/txt/rfc-1907.txt>. Acesso em: 23 de setembro de 2013.

RFC. **User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).** Disponível em: <http://www.ietf.org/rfc/rfc2574.txt>. Acesso em: 23 de setembro de 2013.

SCHAEFER, Charles V. **System of Systems Management: A Network Management Approach**. Disponível em: <http://www.boardmansauser.com/downloads/2007GorodGoveSauserBoardmanIEEE.pdf>. Acesso em: 28 de abril de 2013.

SCHMICHTEMBERG, Claudio. **Especificação de uma Plataforma de Gerenciamento de Redes Baseada no Protocolo SNMP**. Universidade do Extremo Sul Catarinense, 2009.

SORTICA, Eduardo. **Redes de Telecomunicações TMN e Gerência Integrada de Redes e Serviços.** ed. 2. Sortz, 2007.

STALLINGS, William. **SNMP, SNMPv2, SNMPv3, AND RMON 1 and 2.** 3. ed. Addison-Wesley, 1998.

APÊNDICE(S)

APÊNDICE A – Habilitar e configurar o protocolo SNMP no Windows 7/8

No sistema operacional Microsoft Windows 7/8 o protocolo SNMP vem desabilitado por padrão, para ativa-lo basta seguis os passos abaixo.

1. Abra o Painel de Controle.
2. Entre em Programas > Desinstalar um programa.
3. Clique em Ativar ou desativar recursos do Windows.
4. Na listagem de recursos que abrirá, procure por Protocolo SNMP.
5. Selecione-o e clique em OK.
6. Aguarde o mesmo ser instalado.

O protocolo SNMP já estará instalado corretamente. Agora vamos configurar para que aceite requisições de computadores na rede.

1. Abra o Painel de Controle do Windows.
2. Entre em Sistema e Segurança > Ferramentas Administrativas
3. Acesse Serviços e procure nas listagem de serviços por Serviço SNMP.
4. Selecione-o e acesse a guia Segurança.
5. Em Nome de comunidade aceitos adicione a public clicando em Adicionar.
6. Selecione também a opção Aceitar pacotes SNMP de qualquer host.
7. Retorne para guia Geral e clique em Parar.
8. Depois clique em Iniciar.

Pronto, o protocolo SNMP já está habilitado e configurado para ser utilizado.

APÊNDICE B – Habilitar e configurar o protocolo SNMP no Linux

Em algumas distribuições do sistema operacional Linux o protocolo SNMP vem desabilitado por padrão, para ativa-lo basta seguis os passos abaixo.

1. Abra o terminal de comandos do Linux e digite os comandos abaixo:

apt-get update

apt-get install snmpd

2. Execute o comando abaixo para abrir o arquivo de configurações do SNMP.

cd /etc/snmp/

cp snmpd.conf snmpd.conf.original

vi snmpd.conf

3. No arquivo que abriu mantenha somente as linhas de configuração abaixo:

rocommunity public 127.0.0.1

rocommunity public 186.233.144.4

rocommunity public 186.233.144.5

4. Agora execute o comando abaixo para reiniciar o serviço SNMP:

/etc/init.d/snmpd restart

Pronto, o protocolo SNMP já está habilitado e configurado para ser utilizado.

APÊNDICE C – Instalando o Cacti

Siga os passos abaixo para instalar o Cacti e suas aplicações:

1. Execute o arquivo Setup Cacti 0.8.8a.exe como administrador.
2. Na primeira tela clique em Next.
3. Na próxima tela aceite os temos de licença e clique em Next.
4. Na próxima tela selecione o servidor web que o programa utiliza-la. Neste caso selecione o Apache e clique em Next.
5. Na próxima tela você pode selecionar alguns plugins para serem pré instalados junto. Neste selecione apenas a opção Cact Dependencies e clique em Next.
6. Na próxima tela será solicitado para escolher o local onde o Cacti e suas aplicações serão instaladas. Neste caso deixaremos a sua escolha.
7. Na última tela clique em Install e aguarde todos os aplicativos serem instalados.
8. Agora acesse seu navegador web e acesse localhost/cacti e utilize o usuário cacti e a senha cactipw.

O Cacti está pronto para ser utilizado. Agora adicionaremos os plugins.

1. Copie as pastas
2. Acessa a opção Configuration > Plugin Management.
3. Procure o nome do plugin desejado na lista e clique no botão azul.
4. Agora clique no botão verde.

Pronto, o plugin está instalado em seu Cacti.

APÊNDICE D – Instalando o NetEye

Siga os passos abaixo para instalar o NetEye e suas aplicações:

1. Execute o arquivo Setup NetEye 6.exe como administrador.
2. Na primeira tela clique em Avançar.
3. Na próxima tela aceite os termos de licença e clique em Avançar.
4. Na próxima tela será solicitado para escolher o local onde o NetEye será instalado. Neste caso deixaremos a sua escolha.
5. Na próxima tela será solicitado para escolher o banco de dados que o programa utilizará. Neste caso selecione a primeira opção e clique em Avançar.
6. Na próxima tela será onde você definirá as configurações do servidor. Altere apenas o campo Código do Collector caso necessário. Clique em Avançar.
7. Na próxima tela deixe a primeira opção selecionada e clique em Avançar.
8. Na próxima tela será demonstrado o caminho onde a instalação do cliente estará disponível. Apenas clique em Avançar.
9. Na próxima tela selecione como será o acesso dos clientes. Escolha pelo nome do computador ou pelo IP.
10. Na próxima tela deixe a primeira opção selecionada e clique em Avançar.
11. Na duas próxima telas apenas clique em Avançar.
12. Na última tela clique em Instalar.
13. Aguarde todas as aplicações serem instaladas e abra o console NetEye.
14. Selecione a opção na qual não possua o código de ativação e clique em Avançar.
15. Agora será solicitado um e-mail para que o link de ativação seja enviado. Digite as suas informações e clique em Avançar.
16. Acesse o e-mail enviado pelo NetEye, copie o código de ativação e cole em seu respectivo campo na janela. Clique em Avançar.

Pronto, o NetEye está instalado. Agora instalaremos a instancia cliente.

1. Acesse a máquina servidora e entre na pasta compartilhada chamada NetEye.

2. Agora execute como administrador o arquivo Instala.bat e aguarde todos os processos serem executados.

Pronto, a instância cliente do NetEye está instalado.

APÊNDICE E – Artigo

Utilizando os Softwares Cacti e NetEye no Monitoramento de Ativos de Redes

Alisson M. Fogaça[1], Paulo J. Martins[1]

[1]Ciência da Computação - Universidade do Extremo Sul Catarinense (UNESC)
Av. Universitária, 1105 – Bairro Universitária – Criciúma – SC - Brasil

alisson_fogassa@hotmail.com, pjm@unesc.net

Abstract. *The computer network became large and complex over the time. Thereforth, it is very important to have a well-defined management to ensure that used resources be always available. With the goal of delivering a reliable network monitoring and control to the administrator, this project implements in just one environment the use of the softwares Cacti e NetEye These are used in the management through the Simple Network Management Protocol. n the environment was simulated some routines occurring in a organizational network, where it was possible to perform a study of used tools' functionality. These tests and metrics returned results demonstrating that these applications are great for administration, although there were several distinct functions where both complemented each other. From that, it was possible to reach the conclusion that the use of both softwares together can provide to the network manager more complete information as better results.*

Resumo. *As redes de computadores tornaram-se grandes e complexas com o passar dos tempos, neste caso é importante que haja uma gerência bem definida para garantir que os recursos utilizados estejam sempre disponíveis. Com o objetivo de entregar um monitoramento e controle da rede confiáveis ao administrador, este projeto implementa em um único ambiente a utilização dos softwares Cacti e NetEye aplicados à gerencia através do protocolo Simple Network Management Protocol. No ambiente foram simuladas algumas rotinas ocorridas em uma rede organizacional, onde foi possível realizar um estudo das funcionalidades das ferramentas utilizadas. Os testes e métricas retornaram resultados que demonstraram que as aplicações são ótimas para a administração, porém existindo diversas funções distintas que podem se completam. Concluindo-se que a utilização de ambas em conjunto pode proporcionar ao gerente da rede resultados melhores e mais completos.*

1. Introdução

À medida que a tecnologia evolui, a capacidade de coletar, processar e distribuir informações aumenta. Isto segue uma linha de que toda essa demanda cresça ainda mais, sendo inerente que novas e antigas formas de processamento destes dados tornem-se mais aprimoradas. Sendo assim, em uma organização onde o processamento das rotinas era realizado em apenas uma máquina, agora passou a ser feito por uma rede de computadores, nos quais todas as tarefas são divididas entre vários dispositivos de diferentes locais, entretanto estando todos interconectados.

Este foi o início para que a rede de computadores fosse implementada, onde facilitou o alcance de informações que se encontravam em locais distante fisicamente (TORRE, 2001). O termo rede já é algo utilizado antes mesmo das primeiras máquinas existirem, pois este

conceito se aplicava em redes de energia, telégrafos, entre outras. Porém a de computadores só foi implantada de fato quando os primeiros computadores pessoais (PC) foram colocados no mercado. Com a junção de todos esses elementos, as redes ganharam novas padronizações e tecnologias, que permitiram uma comunicação melhor e mais otimizada, até mesmo os custos foram amenizados.

Há dois tipos básicos em que as redes podem ser divididas perante a forma que o compartilhamento de dados é realizado, uma chamada de ponto-a-ponto, utilizadas apenas em pequenas redes, e outra chamada cliente/servidor, bastante usada em grandes redes. Dentre alguns componentes que compõe as redes estão as placas de rede, os cabos que são responsáveis pela interligação dessas placas, há as topologias, que se refere à maneira em que as máquinas são interligadas, e diversos outros dispositivos necessários para a comunicação chamados de ativos.

Com o aumento do tráfego de informações e a quantidade de dispositivos em uma rede, a complexidade de gerir todos estes elementos também aumentou, surgindo assim a necessidade de gerenciar e monitorar essas informações. A principal ideia no gerenciamento era o de organizar e amenizar possíveis falhas e defeitos que possam levar a interrupção de serviços e compartilhamentos de informações.

Alguns dos objetivos da gerência de rede são o de realizar um controle e monitoramento de seus elementos, a fim de garantir os serviços dentro de um padrão aceitável de qualidade. Porém antes da chegada do gerenciamento, os problemas ocorridos na rede eram tratados de maneira manual, ou seja, o administrador analisava o erro, realizava os ajustes necessários no sistema e então reiniciava o software ou hardware. Atualmente este meio manual pode ser substituído por aplicações e conjuntos de ferramentas que auxiliam essa monitoração e controle. Estes softwares apresentam funções que demonstram todas as informações sobre a rede, além possibilitar a execução de grande parte das rotinas administrativas.

Existem alguns modelos de gerenciamento referente à organização de todos os processos que o envolve, onde o FCAPS é o modelo voltado para a estruturação do gerenciamento de computadores. Sendo este é o modelo utilizado neste projeto.

A troca de dados entre as entidades, dispositivos que podem enviar ou receber informações, é realizada a todo momento, porém para que a informação enviada seja compreendida por outra entidade precisa-se que haja um padrão. O termo utilizado para tanto é o protocolo, no qual consiste em uma coleção de regras que controlam a comunicação de todo o tráfego na rede.

A grande complexidade de gerenciamento de uma rede também levou a necessidade de se criar um padrão, onde para este caso foi criado o protocolo Simple Network Management Protocol (SNMP). Este protocolo é um conjunto de operações administrativas que podem alterar as informações dos dispositivos, sendo nele onde a grande parte das aplicações de gerenciamento baseiam suas funcionalidades.

Existem inúmeros softwares para gerenciar uma rede, sendo que para a realização deste projeto foram escolhidos dois, o Cacti e o NetEye. A ferramenta NetEye por ser proprietária requer alguns custos para sua aquisição, porém existem versões para testes. Essas aplicações definidas tem capacidades e funcionalidades promissoras para amenizar e controlar os problemas ocasionados em uma rede. Sendo que através de um ambiente propício o estudo de caso realizado procurou explorar estas funções, analisando os resultados obtidos e as técnicas gerenciais utilizadas.

2. Gerenciamento de Redes

As redes de computadores atualmente possuem uma grande diversidade de modelos, de topologias, diferentes equipamentos, meios de transmissão, dentre diversas outras configurações que podem ser aplicadas nas redes. Essa evolução da rede foi realizada durante anos, tudo para melhorar os processos e utilização das redes, permitindo que a comunicação dos dispositivos chegasse a níveis de complexidades muito altos.

Com o objetivo de organizar e estruturar as redes, necessitou-se gerenciar e monitorar toda essas interconexões de computadores, passando por seus hardwares e softwares. A ideia tomou como base o intuito de organizar e amenizar possíveis falhas e defeitos que possam levar a interrupção de serviços e compartilhamentos de informações (KUROSE; ROSS, 2006).

Toda essa complexidade que envolve uma rede de interconexões de entidades, gerenciá-la e monitorá-la garantindo que todos os seus dispositivos estão em execução e em pleno funcionamento pode parecer difícil. Porém através de softwares de gerenciamento adequados e um pouco de conhecimento nas configurações necessárias para uma rede funcionar sem problemas, torna esta tarefa muito mais fácil e simples (MAURA; SCHIMIDT, 2001).

Todavia o gerenciamento da rede sem a utilização de uma ferramenta para isto, pode tornar-se uma escolha pior que a não gerência, pois a busca por uma solução de um determinado problema ocasionado na rede, poderá ocasionar em diversos outros. Por isso o aconselhável é a realização do monitoramento e controle da rede através de softwares focados neste quesito (MOQADI, 2011).

Segundo Stallings (1998, tradução nossa), com a diversificação e a expansão da computação, há grandes quantidades de aplicações e conjuntos de ferramentas para o auxílio na monitoração e controle de uma rede. Estes softwares apresentam funções que demonstram todas as informações sobre a rede, além de possibilidades de executar grande parte das tarefas em relação à gerência.

Na figura 01 é possível observar uma rede pequena com alguns equipamentos conectados e um servidor central, no qual possui uma aplicação de gerência de redes e através dela monitora e controla todas as informações processadas na rede.

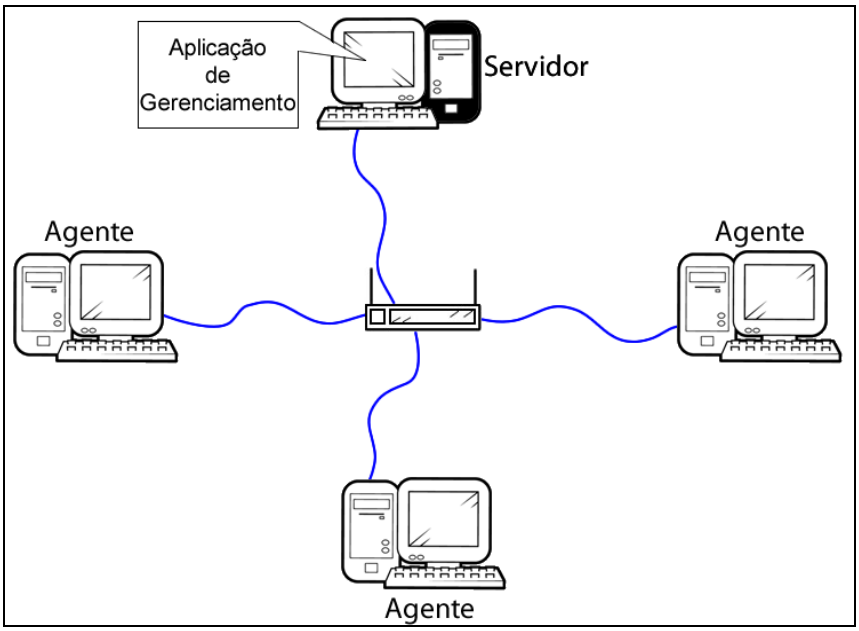


Figura 1. Estrutura de uma rede de computadores com um servidor central.

A realização desta administração da rede, tem como objetivo analisar o funcionamento inteiro dos dispositivos disponíveis, suas tarefas exercidas, seus processos, sua comunicação, todas as suas tarefas relacionadas a rede. Também proporciona à rede uma boa produtividade, pois não há a preocupação dos usuários em problemas que possam ocasionar em sua rede, pois através do monitoramento bem realizado a tendência é a diminuição significativa dos erros de rede e a resolução rápida dos mesmos (PINHEIRO, 2002).

3. SNMP

Toda essa complexidade que envolve uma rede de interconexões de entidades, gerenciá-la e monitorá-la garantindo que todos os seus dispositivos estão em execução e em pleno funcionamento pode parecer difícil. Porém através de uma padronização, este processo pode ser facilitado, buscando estabelecer normas que melhoram o trabalho de gestão foi lançado o protocolo SNMP, o protocolo simples de gestão de rede (MAURA; SCHIMIDT, 2001).

Este protocolo possui como principal características o gerenciamento de rede, onde a grande maioria, ou pode se dizer que todas, suas funções são voltadas diretamente para a administração de computadores e equipamentos, ou como é descrito nas especificações do SNMP, uma rede de objetos (RFC, 1990, tradução nossa).

Através do SNMP é possível conseguir as informações de determinados dispositivos através de comandos e pedidos, permitindo assim que o gerente visualize todo o status da rede de uma maneira facilitada, com estatísticas e informações de cada objeto. Dando a possibilidade também de o administrador da rede projetar o aumento gradual de sua rede, dentre outros planos de expansão (MILLER, 1999, tradução nossa).

Existe também a possibilidade de realizar a monitoração do tráfego que é gerado pela rede, além de possuir a função de receber notificações instantâneas de problemas ocasionados nos elementos e meios de transmissão. Desta maneira facilita as tarefas de otimizar o desempenho de uma rede e certificar-se de que a mesma esteja segura (MILLER, 1999, tradução nossa).

O protocolo SNMP também concede a função de observar e analisar todo o histórico de atividades desenvolvidas pela rede, permitindo assim que o administrador saiba de toda e

qualquer ameaça que determinada ação poderá ocasionar à sua rede (RFC, 1990, tradução nossa).

Os dispositivos que são utilizados como gerentes nos quais emitem os comandos para a aquisição de informações, simulando um servidor, são denominados gerentes. Já os equipamentos que são os analisados, que recebem os comandos e devolvem as informações solicitadas, simulando um cliente, são denominados agentes (MAURA; SCHIMIDT, 2001).

O termo gerente é utilizado para o programa que é executado no dispositivo de gerenciamento, em quanto o termo agente é usado para a aplicação que é executada no equipamento gerenciado (MAURA; SCHIMIDT, 2001).

O SNMP é um protocolo definido em nível de aplicação, encontrando-se na camada de aplicação. Ele possui uma implementação flexível e fácil, onde toda sua especificação está presente no RFC 1157 (RFC, 1990, tradução nossa).

4. Softwares

Os softwares selecionadas para a realização do projeto, Cacti e NetEye, são ferramentas de gerenciamento poderosas na administração e controle da rede, possuindo recursos apurados e diversas opções de configurações.

O Cacti possui ferramentas que proporcionam a visualização dos dados recebidos em gráficos que facilitam o entendimento das informações passadas. A quantidade de possibilidades e funções acabando torando-o um pouco complexo no quesito usabilidade, porém através de sua interface intuitiva é possível utiliza-lo tranquilamente (CACTI, 2013).

Dentre suas funcionalidades destacam-se a possibilidade de obtenção de dados de diferentes equipamentos no mesmo momento, uma avançada configuração de privacidade com um controle total sobre os usuários, gráficos que demonstram estatísticas da rede em tempo real, notificação de problemas instantaneamente, e muitas outras funções disponíveis (CACTI, 2013).

No NetEye é possível controlar e monitorar em tempo real todos os dispositivos, auxiliando e facilitando para o administrador todas as suas tarefas exercidas tanto com relação ao gerenciamento quanto ao suporte (NETEYE, 2013).

Suas funcionalidades que se destacam fazem parte do modulo de monitoramento, onde é possível gerenciar e coletar informações de todas as entidades conectadas. Além da possibilidade de controlar os acessos de usuários aos recursos disponíveis na rede (NETEYE, 2013).

Os dois softwares possuem finitas possibilidades, dentre funções semelhantes e únicas, onde cada um difere através de seus processos de monitoramento. Utilizando toda essas funcionalidades, ambas as ferramentas são uma ótima escolha para implantar o gerenciamento em uma rede.

4.1. Cacti

O Cacti é uma ferramenta livre que auxilia os administradores de rede em suas tarefas gerenciais em uma rede de computadores. Seu objetivo é monitorar e controlar desde redes simples até mais complexas, procurando facilitar essas rotinas administrativas através de suas várias funcionalidades (CACTI, 2013).

Seu desenvolvimento foi realizado pelo grupo de desenvolvedores The Cacti Group, onde é mantido atualmente. Sua liberação é sob a licença General Public License (GNU), no qual não

há custos para a adquirir a ferramenta, porém é possível realizar pequenas doações pelo seu site, ajudando assim no desenvolvimento da software (CACTI, 2013).

Nos fóruns do próprio site do Cacti é possível esclarecer várias das dúvidas acerca da ferramenta, além de adquirir novos conhecimentos sobre a mesma. Pois estes fóruns contam com usuários espalhados por todo o mundo, nos quais também realizam dicas e críticas que ajudam no desenvolvimento e atualizações da aplicação (CACTI, 2013).

Ele se caracteriza na criação de gráficos com as estatísticas de trafego da rede, onde é possível observar e analisar todas as informações dos dispositivos conectados. Estes gráficos são visivelmente claros e demonstram especificamente os dados coletados (CACTI, 2013).

O Cacti permite que as suas funcionalidades sejam acessadas através de uma interface intuitiva, pois a mesma roda em qualquer navegador, pois toda sua interface é orientada à linguagem de programação para web, o PHP (CACTI, 2013).

A geração dos gráficos é de responsabilidade da ferramenta RRDTool, no qual armazena os dados coletados pelo Cacti em uma banco de dados MySQL, gerando assim, por meio desses dados, os gráficos estatísticos citados (CACTI, 2013).

O Cacti trabalha com o protocolo SNMP no qual permite a comunicação com todos os equipamentos da rede afim de coletar informações sobre os serviços e recursos dos mesmos. Outra característica que se destaca é a possibilidade de utilizar plug-ins para aumentar o nível de gerência e as funcionalidades da ferramenta. Esses plug-ins podem ser encontrados no próprio site, e através da documentação é possível aprender a instala-los sem maiores dificuldades (CACTI, 2013).

4.2. NetEye

O NetEye é um software proprietário, ou seja, necessita-se de custos para adquiri-lo, ele é totalmente voltado para o gerenciamento de redes de computadores no qual monitora todos os componentes utilizados pelos clientes. Ele foi desenvolvido em 2006 pela empresa NetEye com o intuito de facilitar o gerenciamento das informações e computadores da rede. A empresa era incubada na Unidade de Desenvolvimento Tecnológico da Universidade do Vale do Rio dos Sinos (UNISINOS) (UNITEC), a incubadora do Parque Tecnológico São Leopoldo. Atualmente a empresa NetEye é especializada no gerenciamento, produtividade e segurança (NETEYE, 2013).

Suas funcionalidades são divididas em cinco módulos, o inventário dos hardwares e softwares, a segurança das informações que trafegam, a produtividade da organização, o monitoramento de todos os dispositivos conectados e desempenho dos mesmos (NETEYE, 2013).

Através de suas funções é possível otimizar a rede em que o mesmo está implantado, também pode proporcionar uma maior agilidade para a gerência e o suporte. Coletando todas as informações dos agentes de forma automática, notificando o administrador ao encontrar um problema (NETEYE, 2013).

A aplicação possibilita também o armazenamento de logs de auditoria, estatísticas de uso, além de possuir um modulo de produtividade no qual possibilita ter uma ganho real na produtividade da organização (NETEYE, 2013).

Sua interface é totalmente amigável, podendo ser executada uma determinada função através de menus bem divididos e claros. Caracterizando-se por uma instalação fácil e rápida, a sua configuração é intuitiva, levando o usuário em um passo a passo (NETEYE, 2013).

5. Gerenciamento de Ativos de Redes

Este projeto de pesquisa realizou um estudo completo por meio de casos na utilização dos softwares Cacti e NetEye com enfoque no gerenciamento de rede a fim de analisar os resultados obtidos, buscando a resolução otimizada de problemas cotidianos ocasionados na rede.

Os softwares foram obtidos por meio da Internet, visto que a ferramenta Cacti é gratuita e o NetEye possui uma versão de demonstração completa, apenas restringindo a quantidade de equipamentos monitorados. Na implementação deste trabalho foi realizado em um dos laboratórios de informática da própria universidade a fim de simular um ambiente organizacional e seus problemas, de forma a minimiza-los em uma rede e a auxiliar o administrador em suas tarefas.

5.1. Metodologia

O projeto de pesquisa passou por um levantamento bibliográfico em livros e também junto a Internet em monografias e dissertações. A partir destes foi possível compreender como funciona a gerência de uma rede, bem como as técnicas aplicadas para diagnosticar e administrar a rede e seus ativos.

Os casos de testes foram direcionados a exemplificar alguns problemas ocasionados na rede de uma organização, de forma similar, e não explorando todas as possibilidades, em função da quantidade de informações a serem analisadas. A detecção e a resolução de alguns problemas foi demonstrado por meio do uso dos softwares escolhidos, extraindo alguns resultados de forma a possibilitar algum tipo de análise, com o intuito de ajudar o administrador de rede a diminuir algumas rotinas no gerenciamento de uma rede de computadores.

Os testes foram voltados para as rotinas de utilização da rede, onde foi realizado acessos indevidos à informações e sites, adição e retirada de dispositivos USB e alguns elementos de hardware dos equipamentos, a utilização dos clientes simulando rotinas de utilização e acessos, instalação de softwares e tentativas de burlar as políticas de segurança da rede, dentre outros testes voltados para o monitoramento, controle, segurança e desempenho dos elementos da rede afim de utilizar as ferramentas de gerência.

6. Resultados Obtidos

Os testes aplicados no monitoramento de cada uma das estações, por meio dos softwares de gerenciamento Cacti e NetEye, gerou um volume de resultados, onde os mesmos foram analisados e documentados.

6.1. Resultados Obtidos com Cacti

O software Cacti demonstrou ter um grande potencial, porém apresenta grande complexidade na configuração. Os resultados foram satisfatório dentre as tarefas que lhe foram solicitadas.

O teste realizado voltado para a captação de informações referente aos recursos utilizados nas máquinas se mostrou complexo. Por outro lado a forma que os resultados da consulta são demonstrados é um ponto positivo para o Cacti, pois é possível analisar todas as informações de modo a permitir inúmeras possibilidades.

Todos gráficos são gerados a partir de um plugin com a ferramenta RRDTool, demonstrando os resultados da consulta de forma dinâmica, dando a possibilidade de exportar esse gráfico para o formato PHP.

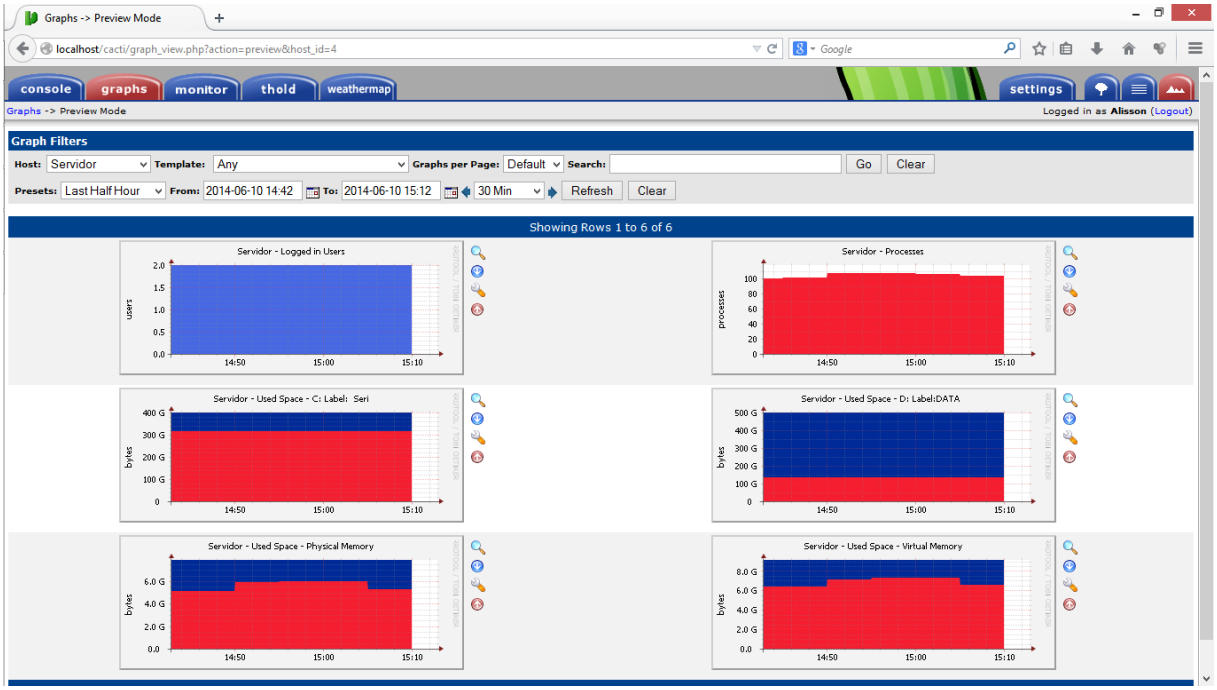


Figure 2. Gráficos gerados com o Cacti.

Mesmo rodando em um servidor Apache local, a aplicação demonstrou um pouco de instabilidade quando usada em plataforma Windows, pois algumas vezes ela não encontrava a solicitação desejada, ou seja, ocorria pequenas quedas do servidor. Porém rodando em ambiente Linux a mesma funcionou com rapidez e sem instabilidades.

A adição de novos dispositivos para serem monitorados é algo relativamente fácil de se realizar. Pois em poucos minutos é possível adicionar um novo dispositivo e já acessar todas as suas informações. Lembrando é claro de queé necessário a ativação do protocolo SNMP, visto no apêndice A para plataforma Windows e no B para ambiente Linux.

A velocidade para acesso a todas as funcionalidades foi boa, mesmo com algumas instabilidades de acesso, o sistema se mostrou bem otimizado. Onde a resposta ao clicar em um comando foi realizada em tempo real, principalmente na geração de gráficos onde se exigia um pouco mais de processamento.

Os resultados obtidos com o Cacti demonstraram que a ferramenta entrega as estatísticas da rede de uma maneira gráfica organizada. Onde através dessas informações é possível analisar a real situação da rede e as máquinas que a compõem, monitorando todos os processos e rotinas envolvidos.

6.2. Resultados Obtidos com NetEye

Os resultados obtidos através dos testes aplicados no software NetEye foram surpreendentes, demonstrando ser uma ferramenta completa nos quesitos de monitoração e segurança da rede. Seu dinamismo em realizar as tarefas solicitadas atrelado ao desempenho permitiram que a sua utilização fosse satisfatória, mesmo em servidores com pouco poder de hardware houve rapidez nas respostas.

As suas funcionalidades abrangem todas as áreas do modelo FCAPS utilizado, permitindo um gerenciamento completo de todos os processos que envolvem uma rede de computadores.

Como é o caso da gerência de segurança, na qual pode ser realizada através do módulo de mesmo nome, onde é possível restringir os acessos de clientes, impossibilitando-os de acessar

determinados programas, que são configurados na opção bloqueio de programas. Quando o usuário tentar acessar, será apresentada uma mensagem que o impossibilitará de continuar.

No módulo de produtividade os conceitos do gerenciamento de segurança podem ser aplicados, permitindo que o administrador bloqueie a navegação da estação por meio de palavras, estas são configuradas no menu de segurança bloqueio de Internet.

Os conceitos da gerência de contabilidade podem ser utilizados através de três módulos do programa, de segurança, produtividade e monitoramento. Com estes pode se registrar todas as informações dos arquivos utilizados na máquina, acessados pela rede e até mesmo em dispositivos USB conectados. Esses dados podem ser analisados afim de descobrir quais os tipos de arquivos que os clientes mais estão acessando.

O processo de produtividade permite que o gerente observe todas as aplicações que foi e está sendo utilizada em determinada estação. Demonstrando em um gráfico a porcentagem do tempo que o computador está ligado gasto em cada programa e também o tempo em que o sistema ficou ocioso.

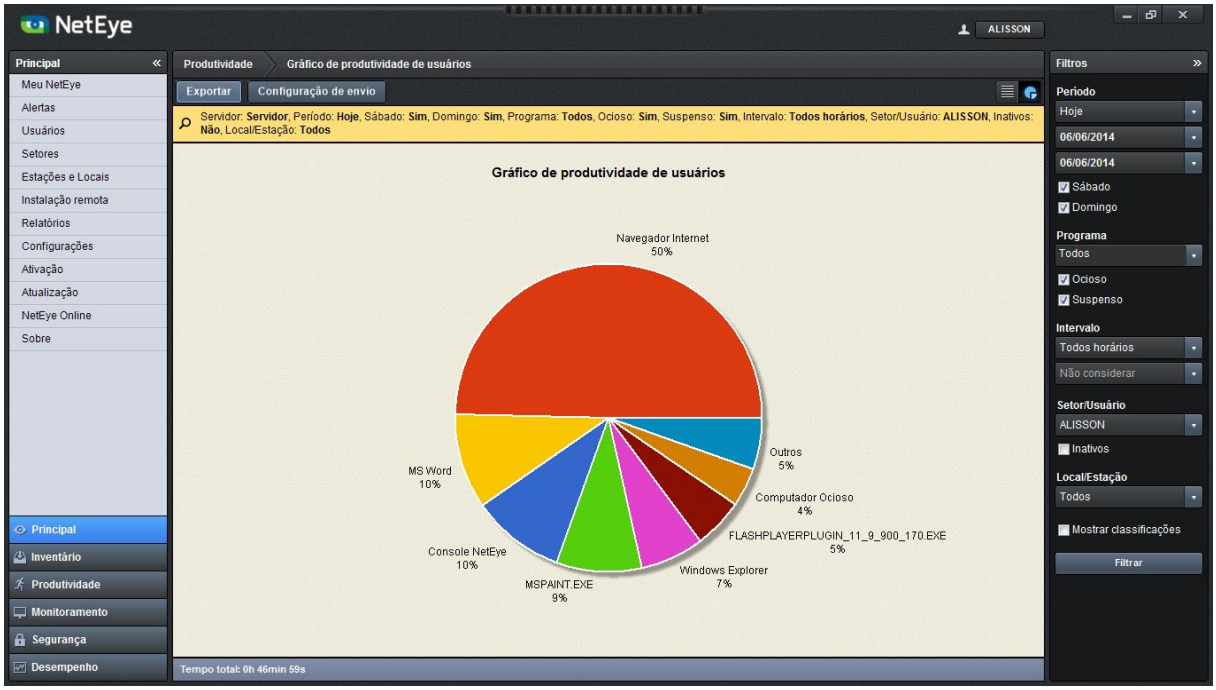


Figure 3. Gráfico de estatística de utilização do sistema por parte do usuário.

Está funcionalidade é um grande diferencial na ferramenta, pois permite de forma prática e intuitiva a visualização de todas as informações a respeito da utilização da máquina pelo cliente, gerando uma análise da produtividade.

O monitoramento pode ser realizado por meio do acompanhamento da tela do usuário, onde escolher por capturas de telas atualizadas em um período configurável ou em tempo real com a opção de acesso remoto. Sendo interessante para analisar esporadicamente a utilização da máquina por parte dos usuários.

O gerenciamento de falhas na rede funcionado através da opção de receber alertas quando uma máquina saiu da rede por problemas técnicos. Desta maneira o administrador não precisa se preocupar em ficar monitorando todas as máquinas de forma a garantir que todas estão conectadas e em funcionamento, pois o mesmo será notificado automaticamente.

A gerência de configuração inicia com a funcionalidade do inventário, onde é possível realizar um levantamento de todos os softwares, hardwares, USB, impressoras e atualizações dos softwares instalados.

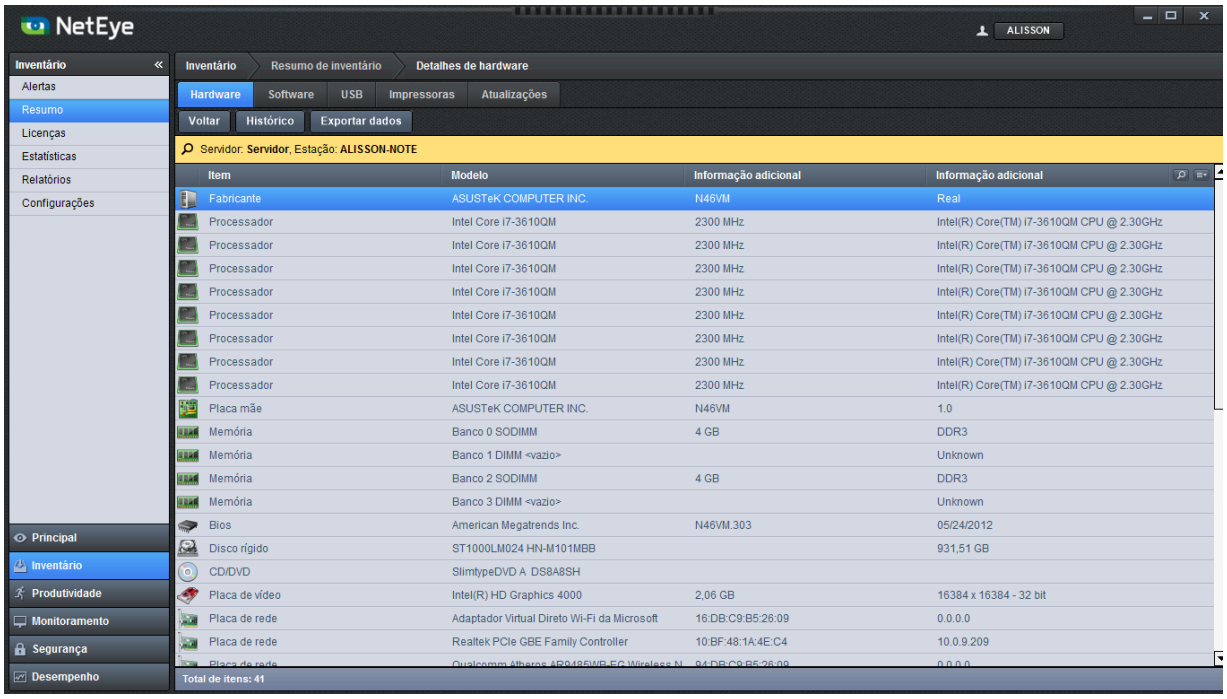


Figure 4. Inventário de uma máquina.

Está funcionalidade é importante, de forma a obter todas as informações dos periféricos de um dado equipamento específico. Sendo possível controlar quais foram removidos ou adicionados, sem que o administrador necessite abrir o equipamento e nem esteja no local do equipamento.

O módulo de desempenho é quem cuida da gerência de desempenho da rede, onde é possível registrar todo um histórico de utilização da memória e da CPU. Isto permite analisar se o computador não está sobrecarregado com os processos do cotidiano e quando que deverá ser realizado uma atualização em seu hardware.

Um de seus problemas é a demora para instalação, pois somente através do instalador próprio é realizado o download da ferramenta.

Outro ponto negativo na instalação é a necessidade de utilizar o banco de dados Microsoft SQL Server 2008 ou superior, pois trata-se de um banco muito robusto. Porém caso o computador não possua instalado, o próprio instalador do NetEye baixa e o instala, deixando totalmente configurado para a utilização do programa.

Os testes realizados com o NetEye retornaram um bom resultado, entregando ao administrador uma plataforma que o auxilia a tomar as decisões a respeito de sua rede. Possibilitando diminuir os gastos que normalmente envolvem essas interconexões, além de permitir controlar todos os serviços e recursos que nela são executados e planejar um possível crescimento.

6.3. Aspectos de Integração dos Softwares

A pesquisa levantou e utilizou as funcionalidades dos softwares Cacti e NetEye com enfoque no gerenciamento de rede afim de analisar os resultados obtidos, buscando observar a aplicações em alguns dos problemas ocasionados em uma rede. A intenção é utilizar os dois

softwares em conjunto, ou seja, levantar as funcionalidades de um que completam o que falta no outro. Para tanto, foi analisado os resultados obtidos com o estudo de caso e observado em quais quesitos ambos se destacam, demonstrando as áreas de atuação de cada software. Assim conclui-se que utilizados em conjunto tem-se um gerenciamento mais qualitativo e abrangente.

As duas ferramentas não são capazes de se comunicar e trocar informações entre si, porém é possível utilizar ambas em conjunto afim de melhorar a gerencia da rede. Além de que o funcionamento de uma não atrapalha o da outra, fazendo com que as duas possam ser utilizadas em uma mesma rede sem maiores problemas.

Funcionalidade	Cacti	NetEye
Monitoramento	X	X
Controle		X
Contabilidade	X	X
Segurança		X
Desempenho	X	X
Gráficos estatísticos	X	
Adição de funcionalidades (plugins)	X	
Gratuito	X	
Alertas	X	X
Inventário		X

Tabela 1. Comparação de funcionalidade entre Cacti e NetEye.

Os resultados demonstraram que a utilização de uma pode ser capaz de satisfazer as rotinas administrativas, porém ao juntar as funcionalidades particulares de cada uma pode levar a administração da rede a outros níveis, além de facilitar a gerência.

No emprego das duas ferramentas existem diversas funções que podem ser utilizadas em conjunto para que o gerente possa ter informações mais confiáveis e consistentes.

A viabilidade de adição de plugins no Cacti é importante, pois sempre existe a possibilidade de adicionar novas funcionalidades que contemplem ainda mais a administração da rede.

Toda essa capacidade pode ser aliada ainda ao poder de controle do NetEye, sendo que através dele é possível garantir que os usuários sigam todas as políticas aplicadas a rede como citado anteriormente. Evitando acessos indevidos e possibilitando uma segurança adequada da rede.

A aplicação NetEye disponibiliza todas as suas documentações e guias em seu site oficial, mesmo sendo proprietário. Já o Cacti por ser aberto, acaba existindo diversos meios para acesso a essas informações.

Por fim os dois softwares demonstraram seu potencial e suas falhas, onde concluiu-se que quando utilizadas em conjunto pode se ter novas possibilidades administrativas, além de que ao captar as mesmas informações com as duas, pode se garantir a consistência dos dados.

7. Conclusão

Os estudos de casos aplicados auxiliaram no entendimento das técnicas gerenciais e de implementação de uma rede. Foi possível observar a importância de um planejamento com base na infraestrutura disponível para garantir que a rede possua uma organização gerencial capaz de administrar todas as suas rotinas.

As informações monitoradas e recolhidas por meio dos softwares foram capazes de abranger inúmeras rotinas da rede. Sendo que elas serviram para passar ao gerente um panorama geral, onde através de todos esses dados ele poderá tomar as melhores decisões para o funcionamento da sua rede.

A implantação de softwares para realizar o gerenciamento de redes se faz necessário para que seja possível controlar todas as entidades garantindo uma organização e qualidade. Essas aplicações garantem a amenização dos problemas ocorridos e do tempo gasto em busca de suas soluções. A gerência realizada demonstrou que as ferramentas são de suma importância para que a rede possa ter uma consistência no quesito administrativo e também usual.

O Cacti apresentou um grande potencial no monitoramento da rede demonstrando as informações através de gráficos, onde foi possível observar as informações de memória, disco, CPU, dentre outras. Utilizando tudo isso em conjunto com a sua capacidade de adição de plugins suas funcionalidades podem ser elevadas e melhores aproveitadas.

O NetEye por outro lado apresentou um resultado ainda melhor em quesitos como controle e segurança da rede, sendo capaz de impedir e controlar os acessos dos usuários. Através de seu módulo inventário é possível realizar um levantamento completo de todo o hardware disponível nas estações da rede, possibilitando ao administrador um planejamento futuro da rede.

Através dos resultados obtidos foi possível observar que apesar das duas ferramentas serem bem completas e capazes de monitorar e controlar diversas informações na rede, as funcionalidades de ambas podem se completar. A utilização em conjunto permite que o administrador possa analisar os dados das estações de uma maneira mais completa.

O gerenciamento de rede está constante evolução, partindo deste princípio como sugestão para estudos futuros ficam o de realizar estudos através de novas ferramentas e a possibilidade de integração com as citadas neste trabalho, assim como o desenvolvimento de novos plugins para o Cacti com o intuito de otimizar as rotinas administrativas da rede.

Referências

ABREU, Fabiano; PIRES, Herbert. **Gerência de Redes.** Disponível em: <http://www.midiacom.uff.br/~debora/redes1/pdf/trab042/SNMP.pdf>. Acesso em: 23 de setembro de 2013.

BARRETO, Grasielli. **Ferramentas de Gerência de Redes**. Paraná: Universidade Estadual de Londrina, 2008. Disponível em: <www2.dc.uel.br/nourau/document/?down=736> Acesso em: 28 de abril de 2013.

BEHROUZ, A. Forouzan. **Comunicação de Dados e Redes de Computadores**. 3. ed. São Paulo: Bookman, 2006.

BONOMO, Esley. **Gerenciamento e Monitoração de Computadores Utilizando-se Zabbix.** Paranaguá: Universidade Federal de Lavras, 2006. Disponível em: < http://www.ginux.ufla.br/files/mono-EsleyBonomo.pdf> Acesso em: 28 de abril de 2013.

CACTI. **Cacti - The Complete RRDTool based Graphing Solution.** 2013. Disponível em:

<http://www.cacti.net/>. Acesso em: 27 de abril de 2013.

CACTI. **O que é o Cacti?.** Disponível em: <http://openmaniak.com/pt/cacti.php>. Acesso em: 28 de abril de 2013.

DUARTE, Jean. Relatório **Técnico de Meios de Transmissão.** Disponível em: <http://187.7.106.13/nataniel/Turmas_T3_T4/Conectividade/Trabalhos/MT_T3/JEAN_LUIGI_DUARTE%20%281%29.pdf>. Acesso em: 03 de setembro de 2013.

DUARTE, Lianna. **Gerência de Redes e Software Livre: Uso do Nagios.** Disponível em: <http://www.faete.edu.br/revista/ArtigoLiannaFSA.pdf>. Acesso em: 07 de setembro de 2013.

Editora Ciência Moderna Ltda., 2008.

FILHO, Olavo. **Gerenciamento e Monitoramento de Redes I: Análise de Desempenho.** Disponível em: <http://www.teleco.com.br/tutoriais/tutorialgmredes1/default.asp>. Acesso em: 23 de setembro de 2013.

ISO. **Internet Society Brasil**. Disponível em: <http://www.isoc.org.br/>. Acesso em: 23 de setembro de 2013.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet.** 3. ed. São Paulo: Pearson, 2005.

MACIEL, Luis. **Modelo de Gerência: FCAPS.** Disponível em: <www.trabalhosfeitos.com/ensaios/Modelo-De-Gerenciamento-Fcaps/40151422.html>. Acesso em: 23 de setembro de 2013.

MATOS, Leonardo K. **Um Processo de Gerência para Redes de Computadores em Ambientes de Software Livre.** Curitiba: Pontifícia Universidade Católica do Paraná, 2006. Disponível em: <http://www.bibliotecavirtual.celepar.pr.gov.br/arquivos/File/MonografiaseArtigos/Monografia_Leonardo_GerênciadeRedes.pdf> Acesso em: 28 de abril de 2013

MAURO, Douglas R.; SCHMIDT, Kevin J. **SNMP Essencial**. 1. ed. O'Reilly, 2001.

MENEZES, Elionildo; SILVA, Pedro. **Gerenciamento de Redes: Estudos de Procotolos.** Disponível em: <http://www.di.ufpe.br/~flash/ais98/gerrede/gerrede.html>. Acesso em: 23 de setembro de 2013.

MILLER, Mark. **Managing Internetworks with SNMP.** ed. 3. Chicago: M&T Books, 1999.

MOQADI, Kanan; SILVA, Verônica. **Uso de Ferramentas de Gerência de Rede para Análise de Desempenho de uma Rede Local**. Disponível em: <http://www.ulbra.inf.br/joomla/images/documentos/TCCs/2011_02/PROJETO_RC_KANAN_ALI_ABDULLA_MOQADI.pdf>. Acesso em: 07 de setembro de 2013.

MORIMOTO, C. E. **Servidores Linux: guia prático**. 2. ed. Porto Alegre: Sul Editores, 2009.

MORIMOTO, Carlos E. **Redes: Guia Completo.** 3. ed. Porto Alegre: Sul Editores, 2008.

NETEYE. **NetEye**. 2013. Disponível em: <http://www.neteye.com.br/en/>. Acesso em: 27 de abril de 2013.

OETIKER, T**. RRDtool - Logging and Graphing**. Disponível em: <http://oss.oetiker.ch/rrdtool/doc/rrdtool.en.html>. Acesso em: 27 de abril de 2013.

PINHEIRO, Marcos. **Gerenciamento de Redes - SNMP, RMON e CACTI.** Disponível em: <http://www.metropoledigital.ufrn.br/aulas_avancado/web/disciplinas/rede_comp/aula_15.ht

ml>. Acesso em: 03 de setembro de 2013.

PINHEIRO, Ricardo. **O Protocolo SNMP**. Disponível em: <http://www.mundotibrasil.com.br/o-protocolo-snmp/>. Acesso em: 03 de setembro de 2013.

RFC. **A Simple Network Management Protocol (SNMP).** Disponível em: <www.rfc-base.org/txt/rfc-1157.txt>. Acesso em: 23 de setembro de 2013.

RFC. **Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2).** Disponível em: <www.rfc-base.org/txt/rfc-1907.txt>. Acesso em: 23 de setembro de 2013.

RFC. **User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).** Disponível em: <http://www.ietf.org/rfc/rfc2574.txt>. Acesso em: 23 de setembro de 2013.

SCHAEFER, Charles V. **System of Systems Management: A Network Management Approach**. Disponível em: <http://www.boardmansauser.com/downloads/2007GorodGoveSauserBoardmanIEEE.pdf>. Acesso em: 28 de abril de 2013.

SCHMICHTEMBERG, Claudio. **Especificação de uma Plataforma de Gerenciamento de Redes Baseada no Protocolo SNMP**. Universidade do Extremo Sul Catarinense, 2009.

SORTICA, Eduardo. **Redes de Telecomunicações TMN e Gerência Integrada de Redes e Serviços.** ed. 2. Sortz, 2007.

STALLINGS, William. **SNMP, SNMPv2, SNMPv3, AND RMON 1 and 2.** 3. ed. Addison-Wesley, 1998.