INSTITUTO FEDERAL DO PARANA

WAMILSON LUIZ CANDIDO

OUTROS TRABALHOS EM:
www.projetoderedes.com.br

GERENCIAMENTO DE REDES

PARANAGUÁ

2011

WAMILSON LUIZ CANDIDO

GERENCIAMENTO DE REDES

Trabalho de Conclusão de Curso apresentado ao Curso de Técnico em Manutenção e Suporte em Informática – Subsequente do Instituto Federal do Paraná – Campus Paranaguá, como requisito parcial de avaliação.

Orientador: Prof. Gil Eduardo de Andrade

PARANAGUÁ

2011

Dedico este trabalho a Deus, a minha esposa Suzani, aos meus filhos Wandryl e Rafael, pela compreensão com relação à minha ausência, por estarem sempre ao meu lado nos momentos difíceis durante o curso, me apoiando, a vocês meu muito obrigado do fundo do coração.

AGRADECIMENTOS

À Deus por ter dado forças para concluir o curso.

Ao Orientador prof. Gil Eduardo de Andrade pelo comprometimento e estando sempre à disposição para sanar as dúvidas.

Ao prof. Emílio Rudolfo Fey Neto, pelo apoio, incentivo e motivação, no momento em que estava prestes a desistir de apresentar o TCC.

Aos meus colegas de sala de aula, que me ajudaram durante o curso.

A todos que me ajudaram diretamente ou indiretamente para a conclusão deste Trabalho de Conclusão de Curso.

RESUMO

O presente trabalho de conclusão de curso está dividido em seções, onde inicio com uma introdução sobre a importância de realizar o gerenciamento de rede dentro da estrutura de uma empresa, onde ele torna-se fundamental para o processo de crescimento. Descrevo sobre a motivação de identificar dificuldades para gerência de redes, justificando que sem um *software* de gerenciamento, o tempo para resolver um problema, pode acarretar em prejuízo financeiro. O objetivo deste trabalho em geral, é compreender o contexto de gerência de redes, com fins específicos de pesquisar técnicas e *software* de gerência de rede. Na seção fundamentação teórica, apresento os conceitos relacionados às pesquisas realizadas para o desenvolvimento do trabalho, apresentando as principais referências bibliográficas consultadas. Realizo uma introdução ao gerenciamento de redes, ressaltando a importância do uso de *software* para realizar o monitoramento da rede. Em seguida, o papel do gerente de redes, onde o objetivo é prevenir e solucionar problemas. Esta tarefa normalmente é realizada por uma equipe (dependendo da estrutura da empresa), onde: o *help desk* é o primeiro a ouvir reclamações dos usuários quando surge um problema; o suporte técnico é o pessoal chamado pela equipe de *help desk* não conseguiu resolver; o operador de rede é o pessoal que mantém o primeiro contato com o problema, gerado pelo sistema; o gerente da equipe de gerência avalia o desempenho da equipe, providencia treinamentos. Continuo o trabalho falando sobre o protocolo *snmp*, que é o responsável por gerenciar redes TCP/IP, o qual facilita a comunicação entre os dispositivos de rede. E um resumo dos componentes básicos do *snmp* e os comandos do *snmp*. Na seção metodologia, descrevo como foi realizado o trabalho de pesquisa, e como foram os testes com os *softwares* de gerenciamento *neteye* e ntop. Em seguida continuando a metodologia, mas na subseção *software* de gerenciamento de rede *neteye*, onde realizo uma introdução e vou explicando os módulos: inventário, segurança, produtividade, monitoramento e desempenho, com exemplos. A outra subseção é o *software* de gerenciamento de rede *ntop*, onde também realizo uma introdução e apresento suas características e suas funcionalidades e gráficos de exemplos. E para finalizar, faço uma análise dos resultados e concluo que de acordo com o crescimento da informática, é necessário

que as empresas optem por realizar gerenciamento de suas redes, para o crescimento da empresa, pois um ambiente bem monitorado tem chance de dar certo.

Palavras-chave: Gerenciamento de rede. Monitoramento. Software. Trabalho.

LISTA DE FIGURAS

LISTA DE TABELAS

Lista de abreviaturas, símbolos e siglas

SNMP	*Simple Network Management Protocol*
NMS	*Network-Management Systems*
RFC	*Request for Comments*
IETF	*Internet Engineering Task Force*
DES	*Data Encryption Standard*
MD5	*Message-Digest algorithm*
MIB	*Management Information Base*
UDP	*User Datagram Protocol*
BER	*Basic Encoding Rules*
ARP	*Address Resolution Protocol*
IP	*Internet Protocol*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
TCP/IP	*Transmission Control Protocol/Internet Protocol*

SUMÁRIO

1 INTRODUÇÃO

O Gerenciamento de Rede é essencial dentro da estrutura de uma empresa, ainda mais se o ambiente de Tecnologia de Informação for grande e complexo. Desta forma, é necessário no dia-a-dia um *software* de gerenciamento de rede, que possa nos ajudar a detectar problemas quando eles ocorrem e solucioná-los o mais rápido possível.

Gerenciar uma rede sem o auxílio de software adequado, torna-se uma tarefa muito difícil e que provavelmente não se obterá um resultado com boa qualidade, ou até mesmo, com ferramentas inadequadas, as quais não nos dêem uma visão dos principais elementos da rede. Desta forma, quando não estamos bem instrumentados, não somos capazes de descobrir problemas e por conseqüência, não seremos capazes de solucioná-los, fazendo com que o objetivo principal, que é manter o bom funcionamento da rede, não seja alcançado.

Dentro deste contexto, COSTA (2008, p.Introdução) afirma:

> Ter um ambiente mapeado e monitorado é fundamental para o processo de crescimento de uma empresa, já está mais do que comprovado que com um ambiente de T.I bem planejado seu negócio tem mais chances de dar certo, mesmo para as empresas em que o principal foco seja T.I, pois todos dependem hoje da internet e dos serviços que ela disponibiliza.

A gerência de rede, tem a finalidade de verificar e controlar as informações da rede geradas por softwares de gerenciamento, as quais deverão ser analisadas e se necessário, tomar as devidas providências, para o bom andamento da rede.

1.1 MOTIVAÇÃO

Identificar as dificuldades existentes para gerência de redes no contexto dos administradores iniciantes e encontrar soluções que auxiliem no gerenciamento, com relação a identificação dos possíveis problemas em uma rede sem o auxílio de um *software.*

1.2 JUSTIFICATIVA

O trabalho proposto analisa *softwares* de gerenciamento de rede, visto que o não conhecimento de técnicas adequadas, que permitam encontrar e analisar os possíveis problemas em uma rede de computadores acarreta em uma demora excessiva para diagnosticá-los e resolvê-los. Sendo assim, como conseqüência para a empresa, tem-se prejuízos financeiros devido a equipamentos parados por dispositivos defeituosos.

1.3 OBJETIVO GERAL

Este documento tem como objetivo geral compreender o contexto de gerência de redes, levantando informações sobre o monitoramento e controle dos dispositivos que a compõem.

1.4 OBJETIVO ESPECÍFICO

- ✓ Pesquisar técnicas de gerenciamento de redes.
- ✓ Identificar requisitos mínimos necessários para obter uma gerência de rede satisfatória.
- ✓ Identificar *software* que atendam requisitos mínimos para gerência de uma rede.
- ✓ Analisar e demonstrar os procedimentos necessários para instalação e configuração dos *softwares*.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são apresentados os conceitos relacionados às pesquisas realizadas para o desenvolvimento do trabalho proposto.

Dentre as referências consultadas para realização do trabalho de conclusão de curso sobre gerenciamento de rede, podemos destacar os seguintes: Melhores práticas de gerência de redes de computadores dos autores SUAVE; LOPES; NICOLLETTI, (2003), Ambiente de rede monitorado com nagios e cacti do autor COSTA (2008), Redes de computadores do autor TANEMBAUM (1997), e o trabalho exemplar sobre Simple Network Management Protocol, realizado pela UFRJ no site < http://www.gta.ufrj.br/grad/10_1/snmp/versoes.htm>.

O livro sobre Melhores práticas para gerência de redes de computadores, é excelente, é indicado para administradores de redes com ou sem experiência, onde por exemplo, é realizada uma citação de STALLINGS (1998) por SUAVE; LOPES; NICOLLETTI, (2003), o seguinte: O objetivo da Gerência de Redes é monitorar e controlar os elementos da rede (sejam eles físicos ou lógicos), assegurando um certo nível de qualidade de serviço. Para realizar esta tarefa, os gerentes de redes são geralmente auxiliados por um sistema de gerência de redes. Um sistema de gerência de rede pode ser definido como uma coleção de ferramentas integradas para a monitoração e controle da rede. Este sistema oferece uma interface única, com informações sobre a rede e pode oferecer também um conjunto poderoso e amigável de comandos que são usados para executar quase todas as tarefas da gerência da rede.

Nesta citação, já é resumido o que é gerenciamento de rede, vindo de encontro com o objetivo deste trabalho.

Para desenvolver a seção 2.1 e 2.2, utilizei como referência os livros de SUAVE; LOPES; NICOLLETTI, (2003), e COSTA (2008), onde realizei citações destes autores enriquecendo este trabalho. Na seção 2.3, as referências, foi a de COSTA (2008), e o site da UFRJ <http://www.gta.ufrj.br/grad/10_1/snmp/versoes.htm>.

Onde estas referência explicam com detalhes o que é o protocolo SNMP, tornando uma leitura clara e de fácil entendimento sobre o assunto abordado.

Na seção 2.4, utilizei como referência para desenvolvimento, COMER (2006), para explicar sobre componentes básicos do snmp.

E por último na seção 2.5 comandos do snmp, me referenciei pelo livro de TANEMBAUM (1997).

2.1 INTRODUÇÃO AO GERENCIAMENTO DE REDES

Podemos imaginar uma rede sem monitoramento, onde existe um servidor de dados, várias estações de trabalho, e de repente nessa rede os usuários começam a reclamar de lentidão excessiva. É chamado um técnico para verificar o problema, o qual encontra um ambiente sem *software* de gerenciamento de rede. Então, o técnico, começará a realizar testes (tentativa e erro), substituindo *switches*, placa de rede do servidor, verificar problemas de vírus, etc., ou seja , vai perder muito tempo até chegar realmente ao problema que está causando a lentidão de toda a rede.

> O objetivo da Gerência de Redes é monitorar e controlar os elementos da rede (sejam eles físicos ou lógicos), assegurando um certo nível de qualidade de serviço. Para realizar esta tarefa, os gerentes de redes são geralmente auxiliados por um sistema de gerência de redes. Um sistema de gerência de rede pode ser definido como uma coleção de ferramentas integradas para a monitoração e controle da rede. Este sistema oferece uma interface única, com informações sobre a rede e pode oferecer também um conjunto poderoso e amigável de comandos que são usados para executar quase todas as tarefas da gerência da rede. Citado acima. (Stallings, 1998 citado por SUAVE; LOPES; NICOLLETTI, 2003).

Através dos *softwares* de gerenciamento é possível checar a todo momento, como está o funcionamento da rede. É possível sermos alertados por email ou SMS quando por exemplo, ocorrer algum problema no servidor, como queda de algum serviço essencial. Desta forma, o administrador da rede poderá corrigir o problema, até mesmo, antes de ser notado pelos usuários.

Dentro deste contexto, SUAVE; LOPES; NICOLLETTI, (2003, p.17) afirma:

> A arquitetura geral dos sistemas de gerência de redes apresenta quatro componentes básicos: elementos gerenciados, estações de gerência, protocolos de gerência e informações de gerência. A seguir falaremos um pouco sobre cada um deles:
>
> - os **elementos gerenciados** possuem um *software* especial chamado **agente**. Este *software* permite que o equipamento seja monitorado e controlado através de uma ou mais estações de gerência;
>
> - em um sistema de gerência de redes deve haver pelo menos uma **estação de gerência**. Em sistemas de gerência distribuídos existem duas ou mais estações de gerência. Em sistemas centralizados – mais comuns –

existe apenas uma. Chamamos de **gerente** o *software* da estação de gerência que conversa diretamente com os agentes nos elementos gerenciados, seja com o objetivo de monitorá-los, seja com o objetivo de controlá-los. A estação de gerência oferece uma interface através da qual usuários autorizados podem gerenciar a rede;

- para que a troca de informações entre gerente e agentes seja possível é necessário que eles falem o mesmo idioma. O idioma que eles falam é um **protocolo de gerência**. Este protocolo permite operações de monitoramento (leitura) e controle (escrita);

- gerentes e agentes podem trocar informações, mas não qualquer tipo de informação. As **informações de gerência** definem os dados que podem ser referenciados em operações do protocolo de gerência, isto é, dados sobre os quais gerente e agente conversam.

Podemos observar na figura 01, a estrutura geral de elementos de uma solução de gerência, onde temos: roteadores, comutadores, repetidores, impressoras, servidores e estações de trabalho. A estação de gerência deve obter informações de gerência destes agentes usando o protocolo SNMP, ver seção 4.

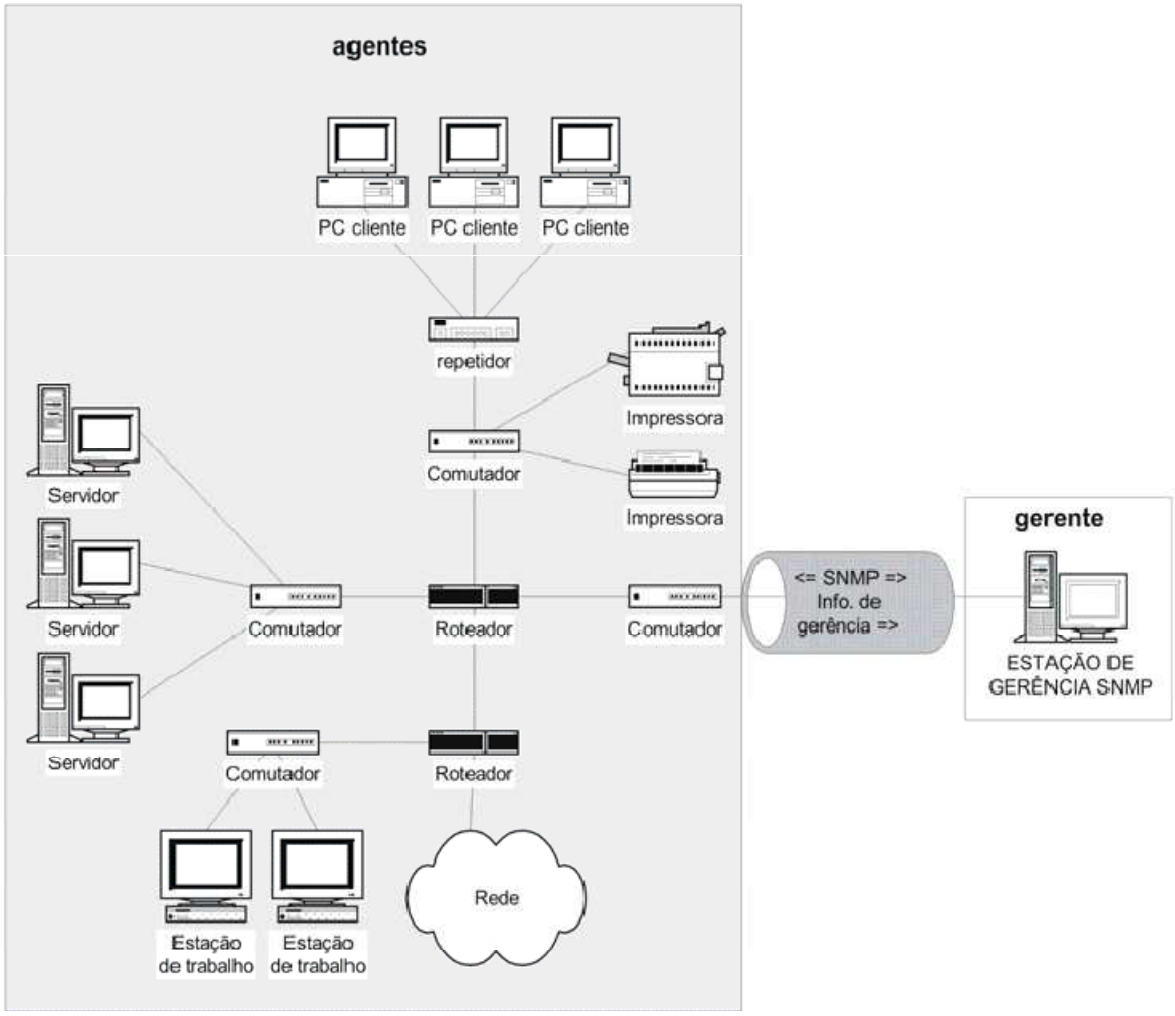


Figura.01 - Estrutura geral de elementos de uma solução de gerência

Dentro deste contexto, COSTA (2008, p.21) afirma:

> O programa gerente da rede é a entidade responsável pelo monitoramento e controle dos sistemas de hardware e software que compõem a rede, e o seu trabalho consiste em detectar e corrigir problemas que causem ineficiência (ou impossibilidade) na comunicação e eliminar as condições que poderão levar a que o problema volte a surgir.

Podemos também, através de softwares, realizar o monitoramento de todas as estações da rede, para avaliar a produtividade da equipe de trabalho. De acordo com a empresa Web@Work, realizou uma pesquisa sobre utilização da Internet no mundo, nos mostram que 97% dos funcionários entrevistados admitem navegar em sites pessoais. Há um alto índice de atividades, as quais não estão relacionadas às funções de trabalho, causando baixa produtividade, e prejuízos para a empresa.

2.2 O PAPEL DO GERENTE DE REDES

Dentro deste contexto, SUAVE; LOPES; NICOLLETTI, (2003, p.19) afirma:

> Um dos objetivos da gerência de redes é prevenir e solucionar problemas na rede. Geralmente esta tarefa é realizada por uma equipe. Não existe uma regra rígida sobre os profissionais que fazem parte desta equipe. Cada organização tem autonomia para criar seu próprio time de gerência de redes de acordo com suas conveniências. Porém, é comum que nesta equipe existam profissionais que executem quatro tarefas distintas: o pessoal do *help desk*, a equipe de suporte técnico, o operador da rede e o gerente da equipe de gerência.

Equipes de Gerência:

- ✓ ***Help desk*** – quando o usuário está enfrentando algum problema relacionado à tecnologia de informação, é solicitado auxílio do *help desk*, o qual estará colhendo informações do usuário para que se possa resolver o problema.

- ✓ **Suporte Técnico** – é o pessoal chamado pelo equipe do *help desk* quando não foi solucionado o problema do usuário. É este pessoal responsável pela manutenção dos equipamentos da rede, pela configuração e operação da rede. Este pessoal precisa possuir conhecimentos técnicos.

- ✓ **Operador de rede** – é o pessoal que mantém o primeiro contato com o problema, o qual é gerado pelo sistema através de alarme na tela, ou, através de email, SMS, etc. O operador tentará resolver o problema, se não conseguir resolver, encaminhará para a equipe de suporte técnico.

- ✓ **Gerente da equipe de gerência** – O gerente tem conhecimento de rede , mas não no nível de um técnico. O gerente avalia o desempenho da equipe de suporte técnico, solicita compras de equipamentos, aplicativos, providencia treinamentos para a sua equipe.

Dentro deste contexto, SUAVE; LOPES; NICOLLETTI, (2003, p.20) afirma:

> É importante ressaltar que esta divisão da equipe de gerência de redes é comum, mas não obrigatória. Podem existir organizações pequenas onde o mesmo profissional acumula todas as tarefas descritas. É possível também que o próprio suporte técnico realize as tarefas do operador da rede. Em organizações maiores o suporte técnico pode ser dividido em primeiro e segundo níveis. Enfim, o importante é que você saiba que, na realidade, o profissional que chamamos neste livro de gerente de redes pode assumir vários papéis distintos em momentos distintos, mas geralmente, estaremos falando com a equipe de suporte técnico.

Na figura 02, exibe os papéis dos componentes da equipe de gerência de redes.

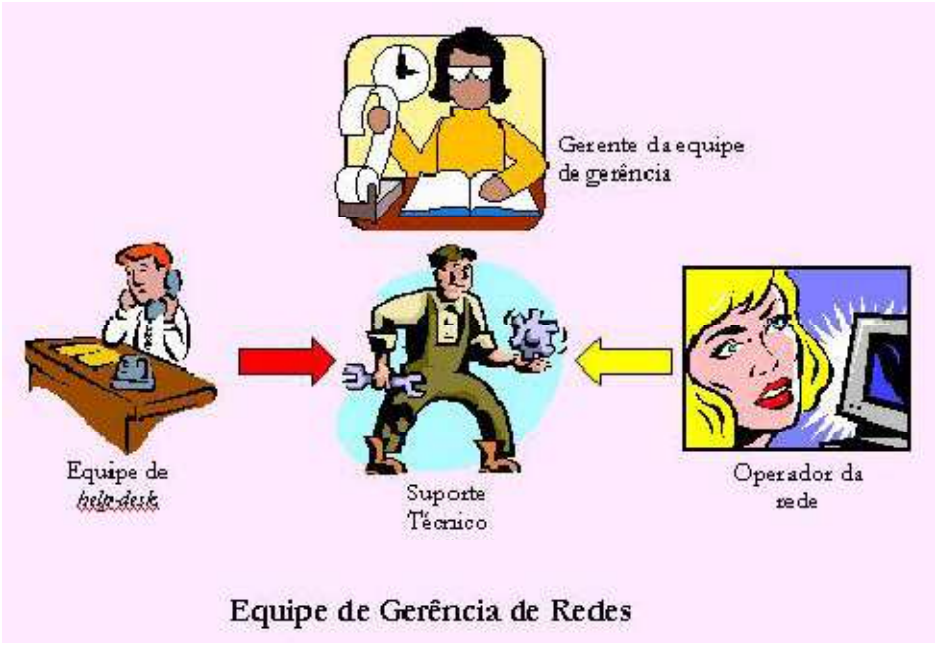


Figura.02 – Uma equipe de gerência de redes de computadores

2.3 O PROTOCOLO SNMP

Não podemos falar em gerenciamento de redes sem antes falar sobre o protocolo SNMP (*Simple Network Management Protocol* – Protocolo de Gerência Simples de Rede), este protocolo foi desenvolvido pela IETF (*Internet Engineering Task Force*), para auxiliar nas técnicas de gerenciamento de redes. Este protocolo é responsável por gerenciar redes TCP/IP *(Transmission Control Protocol/Internet Protocol)*, da camada de aplicação, o qual facilita a comunicação entre os dispositivos de rede. É através do SNMP que os administradores de rede, conseguem gerenciar o desempenho da rede, e desta forma resolver possíveis problemas na rede.

Dentro do contexto, COSTA (2008, p. 21), afirma:

> O protocolo SNMP (*Simple Network Management Protocol),* é um protocolo de gerência típica de redes TCP/IP (*Transmission Control Protocol/Internet Protocol),* da camada de aplicação que facilita o intercâmbio de informação entre os dispositivos de rede. O SNMP possibilita aos administradores de rede gerenciar o desempenho da rede, encontrar e resolver problemas de rede, e planejar o crescimento desta.

Antigamente, as redes eram simples, os números de roteadores eram pequenos, quando havia demora no acesso a um *host*, chamava-se o responsável pela rede, onde, para detectar o problema, ele simplesmente executaria o programa Ping, e certamente ele o detectaria e assim poderia tomar providências para saná-lo.

Com o passar do tempo, a rede mundial se transformou, sendo utilizados vários *backbones* e operadores, desta forma, a maneira como eram encaradas as redes, deixou de ser adequada, tornando-se necessário a criação de melhores ferramentas para gerenciamento de redes.

Dentro do contexto, COSTA (2008, p. 24), afirma:

> O Snmp é um protocolo padrão usado para gerência de redes, que define os formatos dos pedidos que o Gerente envia para o Agente e os formatos das respostas que o agente retorna, assim como o significado exato de cada pedido e resposta. Uma mensagem SNMP é codificada com um padrão designado de ASN.1 (*Abstract Syntax Notation.1)*.

> Para permitir a transferência de grandes inteiros, sem desperdiçar espaço em cada transferência, o ASN.1 usa uma combinação de tamanho e valor para cada objeto a ser transferido.

Em maio de 1990, a RFC 1157 foi publicada, definindo a **versão 1** do **SNMP** (*Simple Network Management Protocol* – chamado de **SNMPv1**). O SNMP, apresentava uma forma de monitorar e gerenciar uma rede de computadores. Essa estrutura foi implementada tornando-se o padrão para gerenciamento de redes.

Conforme as pessoas ganhavam experiências, com o passar do tempo, começaram a aparecer as deficiências do SNMP, logo, com a necessidade, veio a segunda versão do protocolo (**SNMPv2**), foi definida (nas RFCs[1] 1441 e 1452), tornando-se assim um padrão de protocolo para internet. Nesta versão foi implementado alterações como: melhoria na performance, definições de segurança e comunicação entre gerentes.

> No SNMPv2 especifica também módulos de informação, os quais organizam um conjunto de definições relacionadas. Existem 3 tipos de módulos de informação no SMI: módulos MIB, declarações de conformidade e as declarações de capacidade.
>
> - Os módulos MIB contêm definições de objetos gerenciados relacionados. As variáveis acessíveis via SNMP são organizadas hierarquicamente. Estas hierarquias e outras informações secundárias (como o tipo e a descrição das variáveis) são definidas nas *Management Information Bases* (MIBs).
>
> - Declarações de conformidade fornecem uma maneira sistemática de descrever um grupo de objetos gerenciados que devem ser implementados a fim de garantir um padrão de conformidade.
>
> - Declarações de capacidade são usadas para indicar o nível preciso de apoio que um agente reivindica no que diz respeito a um grupo de MIB. A NMS pode ajustar seu comportamento em relação aos agentes de acordo com as declarações de capacidade associada a cada agente.[2]

O padrão MIB, especifica exatamente quais os itens de dados um dispositivo gerenciado precisará manter, e qual o significado de cada operação permitida, e que podem serem acessados, e em quais dispositivos.

---

[1] Uma RFC é um documento do IETF (*Internet Engineering Task Force*) que traz as epecificações de um protocolo ou tecnologia.

[2] http://www.gta.ufrj.br/grad/10_1/snmp/versoes.htm Acesso em: 06 dez. 2011

Há muitos conjuntos de variáveis MIB, as quais correspondem a protocolos como UDP, IP, ARP , e também variáveis para *hardware* de rede como *Ethernet* , e dispositivos como *bridges, switches* ou impressoras.

> O subsistema de processamento de mensagem prepara as mensagens para que sejam enviadas e extrai dados de mensagens recebidas. Esse subsistema pode conter vários módulos de processamento de mensagens. Por exemplo, um subsistema pode ter os módulos de processamento SNMPv1, SNMPv2 e SNMPv3 pedidos. Ele também pode conter um módulo de processamento de outros modelos que ainda não foram definidos.
>
> O subsistema de segurança fornece serviços de autenticação e privacidade. A autenticação usa *strings* ou comunidade SNMP (v1 e v2) ou autenticação baseada no usuário SNMPv3.A autenticação baseada em usuários utiliza o MD5 ou o SHA, algoritmos para autenticar os usuários sem enviar uma senha em claro. O serviço de privacidade usa o algoritmo DES para criptografar e descriptografar as mensagens SNMP. Atualmente, o DES é o algoritmo utilizado, mas outros podem ser adicionados no futuro.[3]

A vantagem do **SNMPv3,** basicamente é referente à questão de segurança, como autenticação, privacidade e controle de acesso.

Dentro do contexto, COMER (2006, p. 356), afirma:

> As principais mudanças aparecem nas áreas da segurança da administração. Os objetivos são duplos. Primeiro, o SNMPv3 é projetado para ter políticas de segurança gerais e flexíveis, possibilitando para as interações entre um gerente e dispositivos gerenciados aderirem às políticas de segurança especificadas por uma organização. Segundo, o sistema é projetado para facilitar a administração de segurança.
>
> Para alcançar generalidade e flexibilidade, o SNMPv3 inclui facilidades a vários aspectos da segurança e permite que cada um deles seja configurado independentemente. Por exemplo, a v3 aceita autenticação de mensagem para garantir que intruções se originem de um gerente válido, privacidade para garantir que ninguém possa ler mensagens enquanto são transferidas da estação de um gerente para um dispositivo gerenciado, e autorização e controle de acesso baseado em visão para garantir que apenas gerentes autorizados acessem determinados itens. Para facilitar a configuração ou alteração do sistema de segurança, a v3 permite configuração remota, significando que um gerente autorizado pode mudar a configuração dos itens de segurança listados aqui sem estar fisicamente presente no dispositivo.

[3] http://www.gta.ufrj.br/grad/10_1/snmp/versoes.htm Acesso em : 06 dez. 2011

2.4 COMPONENTES BÁSICOS DO SNMP

Uma rede gerenciada pelo protocolo SNMP é composta por três elementos chaves:

1. Dispositivos Gerenciados
2. Agentes
3. Sistemas de Gerenciamento de Redes (NMS – *Network-Management Systems*)

Dentro do contexto, COMER (2006, p. 356), afirma:

> Um dispositivo gerenciado é um nó de rede que possui um agente SNMP instalado e se encontra em uma rede gerenciada. Estes dispositivos coletam e armazenam informações de gerenciamento e mantém estas informações disponíveis para sistemas NMS através do protocolo SNMP. Dispositivos gerenciados, também às vezes denominados de dispositivos de rede.

- ✓ **Dispositivo Gerenciado** – são dispositivos que coletam e armazemam informações de gerenciamento, mantendo estas informações disponíveis para o sistema NMS, através do protocolo SNMP. Estes dispositivos podem ser : roteadores, servidores de acesso, impressoras, computadores, servidores de rede, *switches*, dispositivos de armazenamento, etc.
- ✓ **Agente** – é um *software* que fica armazenado em um dispositivo gerenciado. Um agente tem informações de gerenciamento locais, os quais são traduzidos para um formato compatível com o protocolo SNMP.
- ✓ **NMS** – é responsável pelas aplicações que realizam o monitoramento e controle dos Dispositivos Gerenciados. Ele pode ser instalado em um servidor (ou mais de um) de rede, que recebe pacotes SNMP (informações) dos dispositivos gerenciados pela rede.

2.5 COMANDOS DO SNMP

O SNMP define duas operações básicas

1 Fetch, para obter um valor de um dispositivo
2 Store, para colocar um valor em um dispositivo.

O comando que define uma operação de *fetch* ou *store* deverá especificar o nome do objeto, o qual será único.

Os comandos enviados e recebidos, que trafegam na rede por meio de unidades de protocolo (PDU) classificam-se em:

- *GET*, utilizado para capturar partes de informações de gerenciamento.
- *GETNEXT*, utilizado para retirar seqüências de informações de gerenciamento.
- *SET*, utilizado para realizar mudança no agente.
- *TRAP*, utilizado para atribuir uma notificação.

Dentro do contexto, TANEMBAUM (1997, p. 733), afirma:

> O modo como o SNMP é normalmente usado é aquele em que a estação de gerenciamento envia uma solicitação a um agente solicitando informações a ele ou forçando-o a atualizar seu estado de alguma forma. Em geral, o agente simplesmente responde com as informações solicitadas ou confirma que atualizou seu estado da forma solicitada. Os dados são enviados com base na sintaxe de transferência ASN.1. No entanto, muitos erros também podem ser detectados, tais como Essa Variável Não Existe.

Para que haja comunicação entre Gerente e Agente, é necessário que falem o mesmo idioma. Este idioma é determinado como sendo um protocolo de gerência, onde este protocolo realiza operações de monitoramento (leitura) e de controle (escrita).

3 METODOLOGIA

Foi realizado pesquisa de *software* de gerenciamento de rede, onde o objetivo, era conseguir técnicas que pudessem auxiliar administradores a gerenciar suas redes com uma maior eficiência. Existem diversas ferramentas que fazem o serviço de gerenciamento, muitas destas, são comercializadas por empresas de desenvolvimento de software as quais dependendo, cobram um preço absurdo por licença para utilização. Outras opções eram os chamados *softwares* livre, desenvolvidos por comunidades ao redor do mundo, que disponibilizam distribuições de forma gratuita e que também não deixam nada a desejar, com relação às opções comerciais pagas.

Após ter procurado vários *software*, com intuito de encontrar ferramentas fáceis de instalar, e que realizassem gerenciamento com satisfação, optei por utilizar o *software* "*Neteye*" e o "*Ntop*".

O *software neteye*, é gratuito para utilizar até 05 computadores sendo gerenciados, acima, deverá adquirir licença com o fabricante. Enquanto que o ntop, é distribuição gratuita, sem limite de máquinas.

Depois de escolher quais ferramentas trabalhar para realizar os testes de gerenciamento, realizei o download dos *softwares*, e fui para o próximo passo, que era a instalação.

Optei por iniciar pelo *neteye,* pelo fato de ser em português. O tutorial de instalação se encontra no final do trabalho no Apêndice – A.

Para realização dos testes, o *neteye* foi instalado em um computador com Windows XP Professional, onde foi configurado como sendo Servidor de gerenciamento. Para as estações de trabalho, utilizei 04 computadores, sendo 02 com *Windows* 7 e 02 com *Windows* XP.

Após a instalação do servidor e das estações, foi necessário configurar o *config* do *neteye*, é aonde se define tudo o que se quer em matéria de gerenciamento. Com as tarefas previamente configuradas no console do software, de acordo com a política de segurança da empresa, iniciei os testes com as estações.

Realizei testes com a parte de inventário, produtividade, monitoramento, segurança e desempenho. Com o *neteye* foi possível receber as informações das estações de acordo com o que foi configurado no *config*, como: receber alerta de

utilização de software não autorizado com cópia da tela do que foi acessado (MSN, *youtube*, bate-papos, etc.); inventário detalhado de *hardware* e *software* das estações de trabalho, incluindo alerta de alteração de *hardware* (memória, *hard disk*, etc.); no módulo produtividade mostra o gráfico com porcentagem dos programas utilizados pelas estações de trabalho incluindo o tempo que o computador ficou ocioso; no módulo de segurança é possível saber através dos alertas, quando uma estação utilizou um dispositivo de entrada e saída de dados (*pendrive*), é gerado relatório com detalhes de que operação foi executada (o que foi copiado, alterado, excluído, data, hora), pelo usuário; também é possível no modulo segurança, verificar que documento e impressora da rede foi impresso, quantidade de folhas, data e hora; no módulo monitoramento, é possível visualizar o que as estações estão acessando na hora, conseguir interagir com as estações enviando mensagens na tela, realizar transferências de arquivos, e resolver problemas remotamente. E no módulo desempenho, pode-se gerar gráficos com relação ao uso de memória e CPU de qualquer estação.

Resolvi então simular duas situações que acontecem no dia a dia de uma empresa, para ver como poderia resolver com o auxílio do *neteye:*

- ✓ Primeiro: Em uma das estações instalei um acelerador de download, software que suga toda a banda de internet, se não tiver um controle de limite de banda para os usuários. Então deixei baixando arquivos em uma determinada estação, com certeza os outros usuários reclamariam de lentidão na rede. Fui até o servidor de gerenciamento do *neteye,* para ver como poderia localizar o problema em questão. No módulo monitoramento, tem a opção “Processos e programas” onde é possível visualizar quais *softwares* estão em execução, depois foi só localizar a máquina, e pelo próprio gerenciador fechar o programa, voltando a liberar a banda para todos. Ainda foi possível enviar uma mensagem na tela do usuário, alertando para não executar este tipo de programa novamente.
- ✓ Segundo: Instalei uma placa de rede com defeito (não funciona na rede), digamos que parou de funcionar a rede de uma estação. O usuário perceberá se estiver utilizando alguma aplicação que dependa da rede estar funcionando, senão ele trabalhará normalmente localmente sem saber que está com problema. Pelo *neteye*, se o

> encarregado pelo gerenciamento estiver verificando, perceberá que determinada estação saiu da tela, e começará a procurar qual a causa. Se por ventura não realiza consulta com freqüência, quando o usuário da estação perceber o problema, entrará em contato com o responsável, e aí sim ele perceberá que realmente não está recebendo informações desta estação e tomará as devidas providencias. Neste caso, seria, verificar, cabeamento de rede, portas no switch e placa de rede.

A instalação do *Ntop* é de fácil configuração, diferente de outros softwares de gerenciamento para Linux. Qualquer dúvida há o tutorial de instalação no final do trabalho no Apêndice–B.

Para realização dos testes com o *ntop,* foi instalado em um computador com distribuição *Linux* / *Ubuntu* 10.04, para ser o servidor de gerenciamento, portanto, trata-se de um software gratuito. Para as estações de trabalho, utilizei 03 computadores, sendo: 01 estação com sistema operacional *Windows* 7, 01 estação com *Windows XP Professional* e 01 estação com sistema *Linux / ubuntu* 10.04.

O *software* é gerenciado através de um browser, bastando colocar na barra de endereços do navegador HTTP://ip_do_servidor_Ntop:3000. É possível acessar o menu de configuração e o responsável pelo gerenciamento, terá acesso às informações como: tráfego da rede (MSN, *Kazaa*, *bittorrent*, etc.), a quantidade de dados trafegados por estação e quais foram os protocolos e portas utilizadas.

Com o *ntop* é possível: realizar análise dos pacotes que trafegam na rede; ordenar a listagem do tráfego de rede conforme os portocolos; mostrar gráficos das estatísticas de tráfego; armazena em seu banco de dados as estatísticas; identifica as informações dos *hosts* da rede; exibe a distribuição do tráfego IP sobre os protocolos da camada de aplicação; decodifica os protocolos da camada de aplicação, incluindo os *softwares* P2P; realiza coleta de fluxos gerados pelos roteadores e switches; lista dos endereços IP da rede que acessaram o servidor.

Realizado as mesmas simulações que foram aplicadas ao *neteye* para ver como se comportava o *ntop*.

- ✓ Primeira simulação com acelerador de download: com o *ntop*, foi fácil localizar a suposta “rede lenta”, pois o *ntop* gerá gráficos de acessos P2P, informando a utilização da banda. Foi só localizar o IP e derrubar o serviço da estação.
- ✓ Segunda simulação com placa de rede com defeito: mesmo caso do *neteye*, se o gerenciador do sistema visualizar que uma estação parou de enviar informações, poderá antecipar o problema, caso o usuário da estação não perceber no momento. Realizar teste de *ping* para certificar que não está obtendo resposta da placa de rede e aplicar testes padrão (cabo de rede, porta do *switch*, placa de rede, configuração), conseguirá identificar onde está o problema e solucioná-lo (neste caso a placa de rede).

3.1 SOFTWARE DE GERENCIAMENTO DE REDE ”*NETEYE*”

O *Neteye* foi desenvolvido pelo fundador e diretor Fábio Santini, o qual batizou o nome do *software* o mesmo de sua empresa. A *Neteye* está localizada na cidade de São Leopoldo – RS.

> O Software *Neteye* foi desenvolvido para facilitar o gerenciamento das informações que circulam nos computadores conectados em rede. Com ele todo o seu parque de hardware e *software* fica transparente.
>
> O fácil monitoramento das estações de trabalho, possibilita o diagnóstico das áreas que necessitam de atenção especial, seja para realizar investimentos em *upgrades*, seja para otimizar gastos.
>
> A alta tecnologia do *software* também garante a segurança das informações armazenadas através do controle do que está sendo distribuído, copiado e compartilhado.
>
> Disponível em: http://www.neteye.com.br/#produtos/index/1/descricao_produto. acesso em : 03 dez. 2011.

O *neteye* realiza o gerenciamento das estações de trabalho, onde, realiza inventario, controle de *software*, controle de *hardware*, monitoramento, gerenciamento de licença, acesso remoto, segurança. Controla as informações que circulam nas estações da rede, gerando estatísticas, com as quais, torna-se possível verificar a produtividade.

É possível controlar o acesso a sites, saber o que o usuário fez (quanto tempo levou no Excel, Word, internet, MSN, etc) durante o dia nas estações de trabalho.

O *Software Neteye é free* para até 05 computadores, após, deverá adquirir licenças para cada estação.

Foi realizado um tutorial de instalação, o qual se encontra no Apêndice – A, para sanar as dúvidas, que por ventura venha a aparecer no decorrer da instalação do *software neteye*.

O *Neteye* divide-se em cinco módulos: Inventário, Segurança, Produtividade, Monitoramento e Desempenho.

3.1.1 Inventário

Com o *Neteye* é possível obter todas as informações de *software* e *hardware* dos computadores da rede que estão sendo monitorados, onde o *software* avisa via e-mail e alertas, quando houver qualquer alteração que aconteça nas estações, desde alterações de *softwares*, entradas de dispositivos nas portas USB's, alertando também, qualquer alteração de componentes do computador, como retirada de um pente de memória, substituição de dispositivos de leitura (DVDRW). Na figura 03 podemos verificar uma tela de inventário detalhado de uma determinada estação de trabalho, mostrando também gráficos das partições do *Hard Disk*.

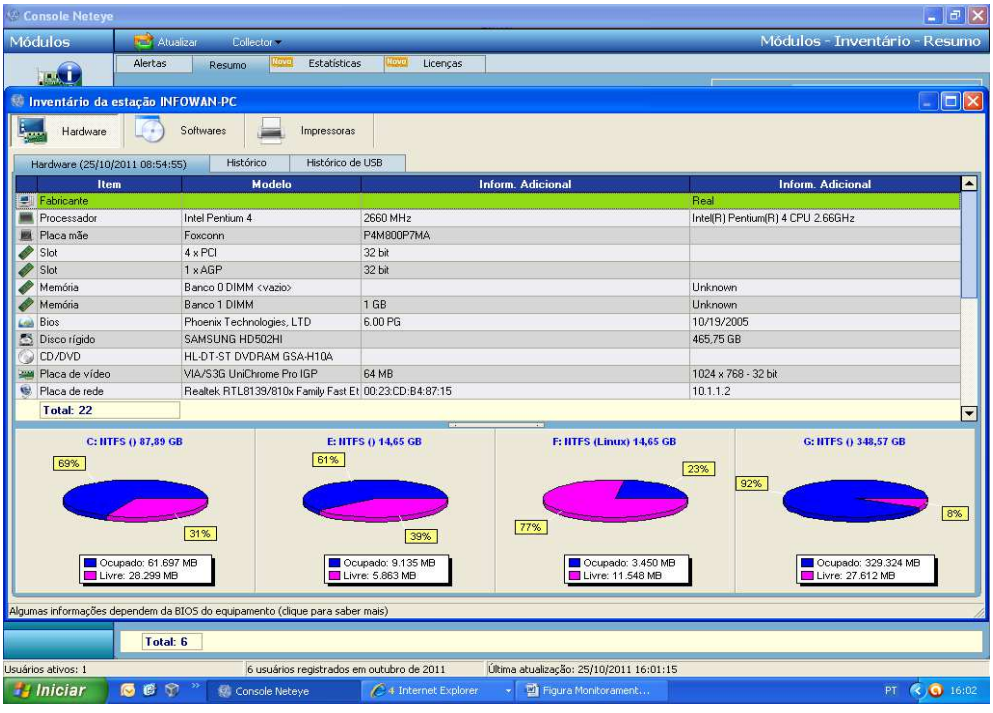


Figura. 03 - Inventario Detalhado de *Hardware* de uma estação

O *Neteye* realiza o gerenciamento das licenças dos *software* contratados, alertando quando estiver excedendo as quantidades das instalações contratadas, e também identifica as instalações de *software* não autorizados (*software* pirata).

Podemos verificar na figura 04, as listas de softwares instalados em uma estação, onde, o *software neteye* exibe com detalhes: nome do *software* instalado, a versão, empresa, data de quando foi instalado, *product key* (chave da instalação),etc.

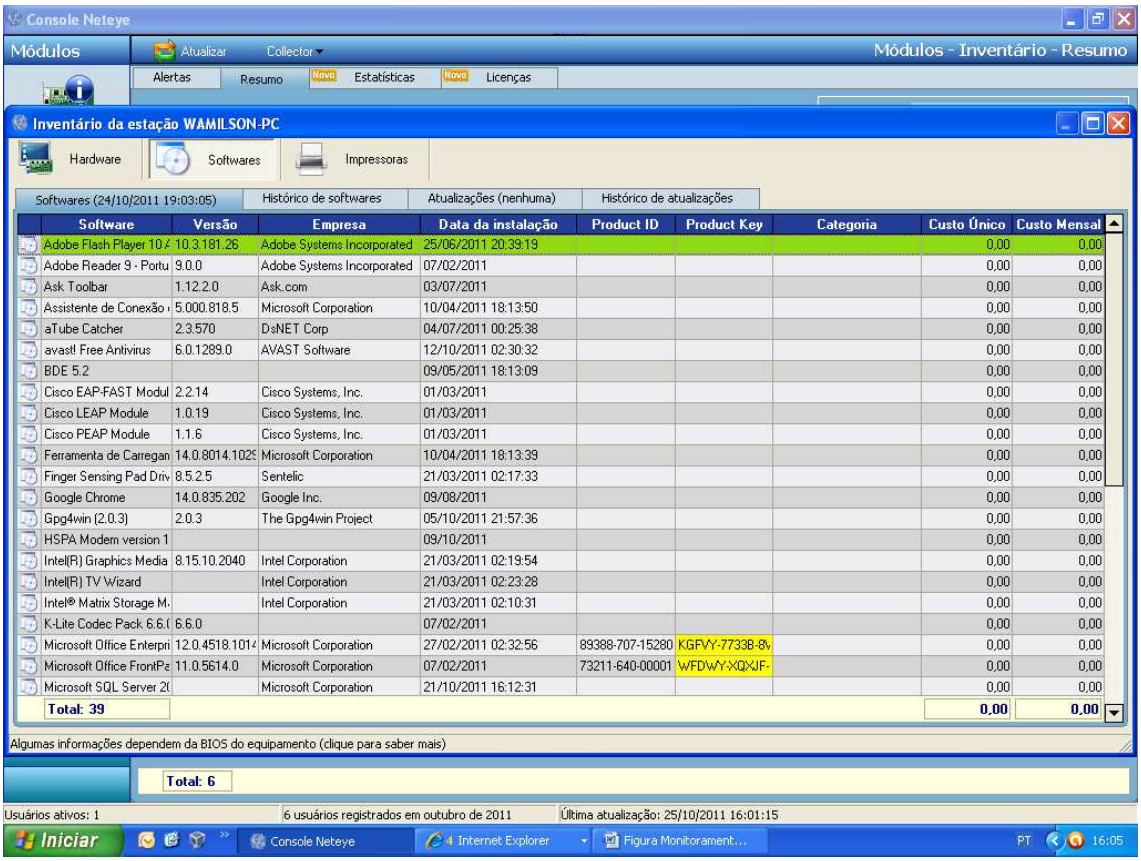


Figura.04 – Inventário detalhado de *software* em uma estação

3.1.2 Segurança

É possível com o *Neteye* criar regras de acordo com a política de segurança da empresa. Pode-se bloquear a execução de programas não permitidos nas estações, que possam interferir na produtividade da empresa, como: MSN, jogos, e outros aplicativos em desacordo com a política de segurança da empresa.

Registra todos os documentos impressos, registrando nome dos arquivos, total de páginas por usuário, por setor, etc,. Também registra os arquivos transferidos ou alterados em dispositivos USB.

Bloqueia o acesso à dispositivos USB, por usuário, por setor ou toda a empresa.

Na figura 05, o módulo de segurança, nos mostra que uma determinada estação, acessou o dispositivo USB (*pendrive*), onde, nos informa a data e hora, que o usuário acessou a *pendrive*, a estação, qual foi a ação (se o arquivo foi criado, copiado, deletado, modificado ou renomeado), e qual o arquivo foi acessado.

Garante o bloqueio de acesso às páginas e a *softwares* não autorizados, ao painel de controle, entre outros.

Registra todos os documentos impressos, registrando nome dos arquivos, total de páginas por usuário, por setor, etc.

Registra os arquivos transferidos ou alterados em dispositivos USB.

Bloqueia o acesso à dispositivos USB, por usuário, por setor ou toda a empresa.

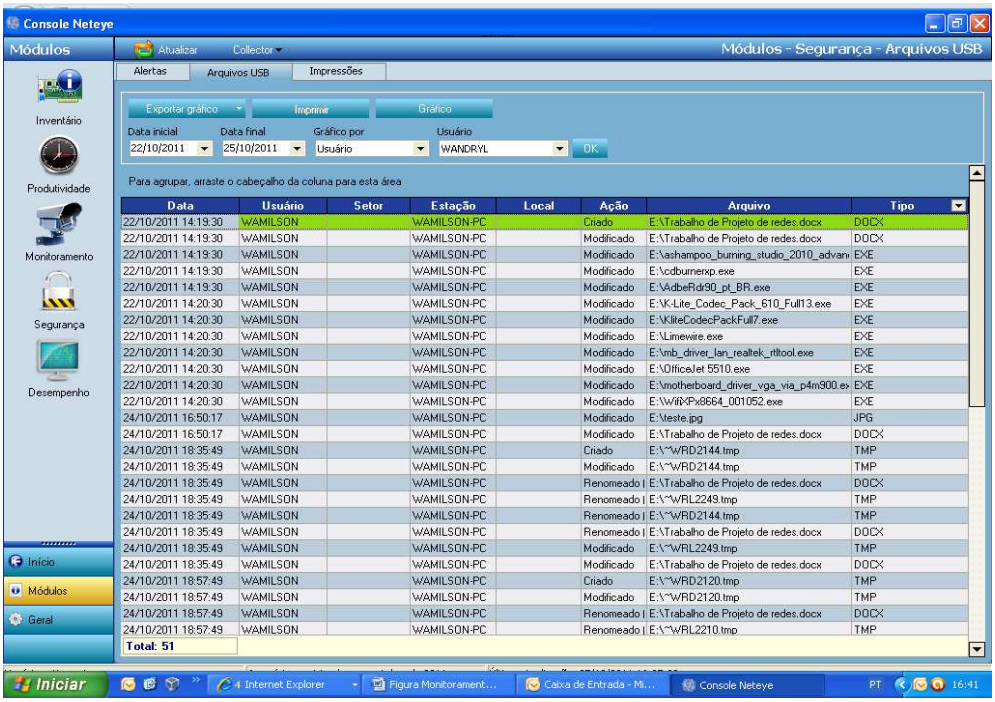


Figura.05 - Relação de arquivos acessados em *PenDrive*

3.1.3 Produtividade

Possibilita gerenciar a produtividade das estações de trabalho. Verificando o desempenho do trabalho realizado pelos seus funcionários, registrando todas as atividades realizadas nas estações, como, também o tempo de equipamento ocioso e o tempo utilizado em cada software.

O módulo de segurança, identifica palavras chaves, as quais foram previamente configuradas, caracterizando acesso indevido, sendo registrado pelo *neteye*, como mostra na figura 06, uma determinada estação que acessou a palavra chave "*youtube*" pelo Internet Explorer . O módulo de produtividade captura uma cópia da tela acessada pela estação e envia para o console de gerenciamento, informando qual foi a estação e o usuário do acesso configurado como indevido. Também verifica detalhes da utilização de cada programa, informando páginas que foram acessadas no navegador da internet, arquivos que foram editados no *Word*,

Excel, PowerPoint, etc., conforme a figura.07, mostrando em porcentagem o gráfico do tempo gasto em cada aplicativo por uma determinada estação de trabalho.

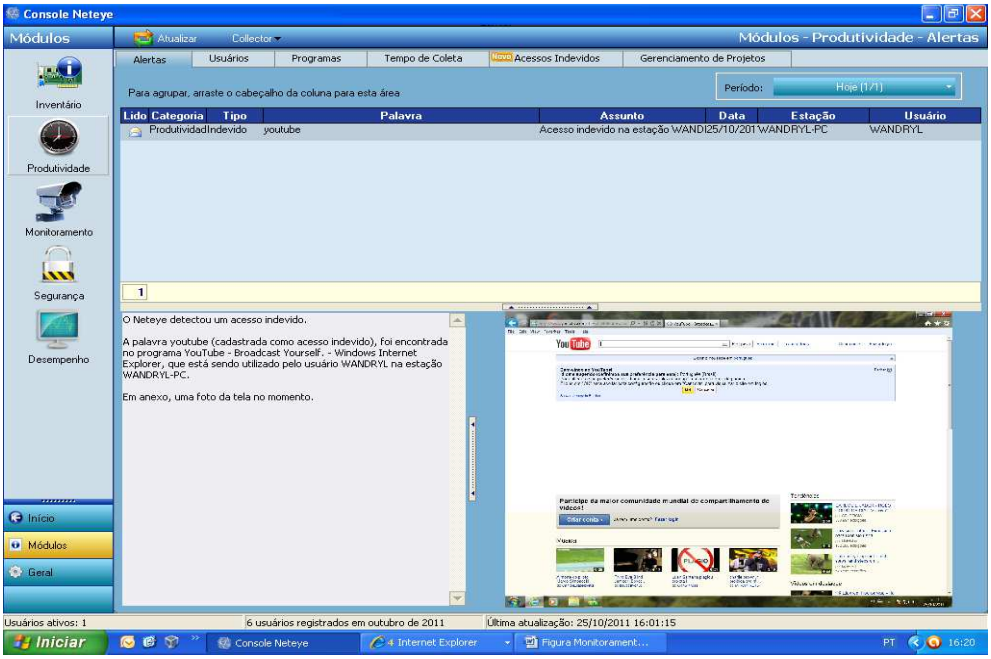


Figura.06 – Alerta de acesso indevido

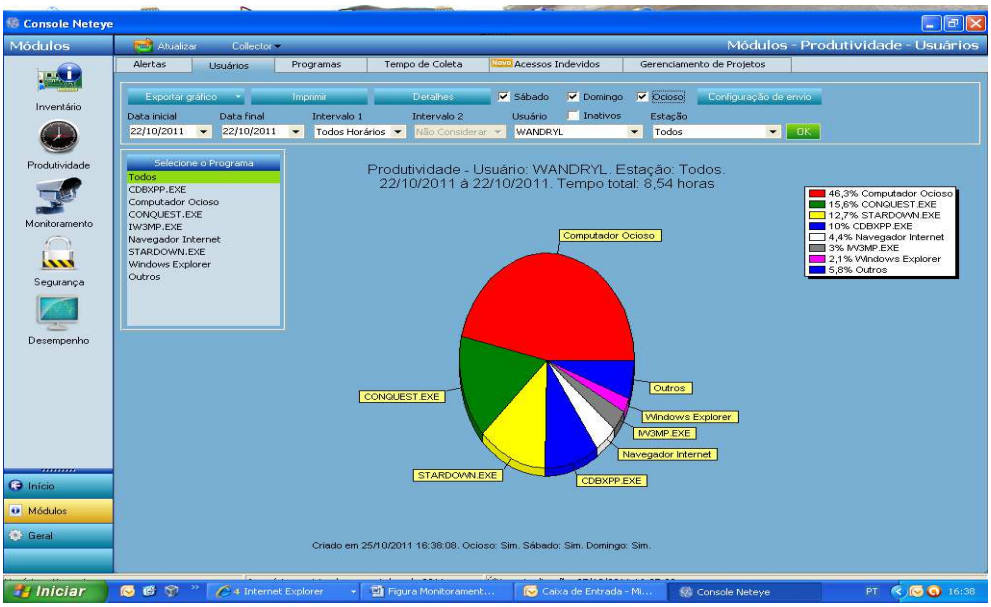


Figura.07 - Gráfico de produtividade por estação

3.1.4 Monitoramento

Com o monitoramento é possível observar o que determinada estação está realizando no momento, ou múltiplas estações, em tempo real. É possível capturar uma cópia da tela da estação. Possui a função mosaico que possibilita visualizar todas as estações de trabalho da rede.

Através do módulo de monitoramento é possível: enviar mensagens e comandos às estações, interromper processos em execução, escolher usuários e estações/setores a serem monitorados.

No monitoramento é possível realizar o acesso remoto da estação desejada, como nos mostra a figura 08, podendo realizar qualquer tipo de atividade, desde instalação de *software*, execução de *software*, transferência de arquivos, etc.

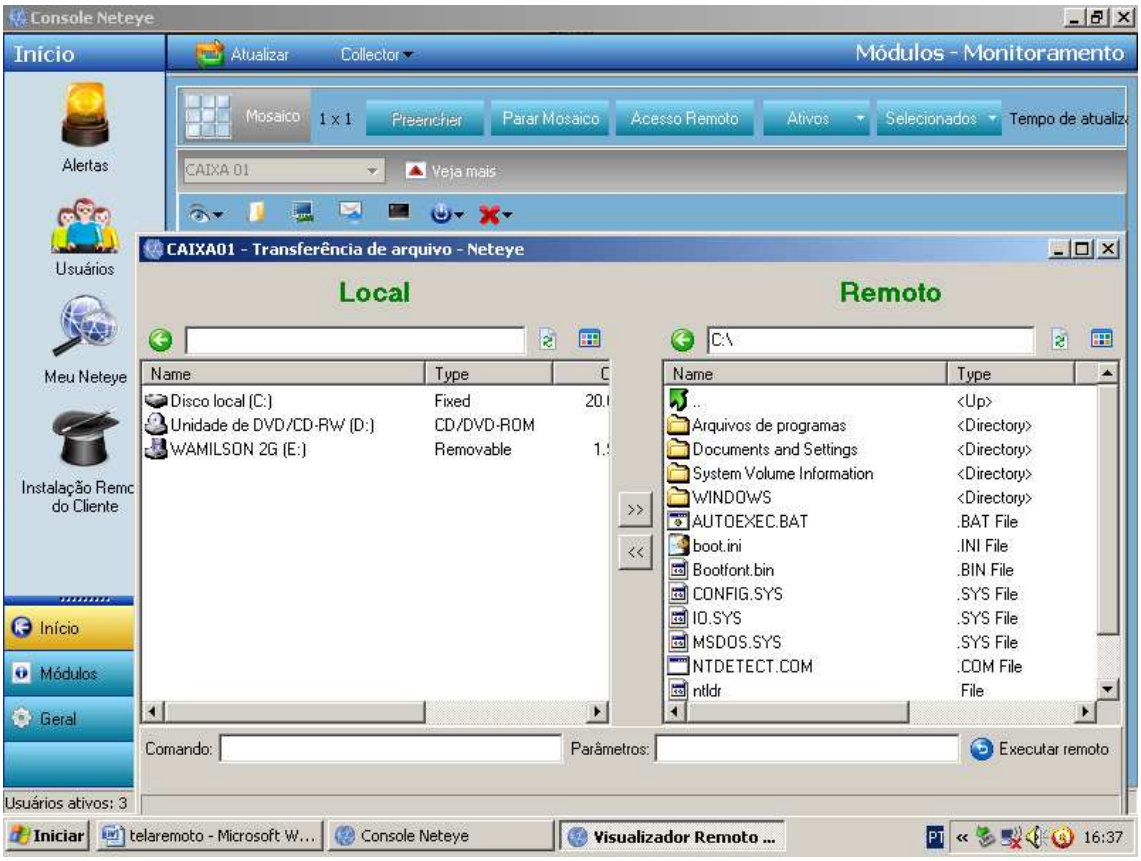


Figura.08 – Monitoramento e transferência de arquivos

3.1.5 Desempenho

No desempenho, pode-se realizar a análise do desenvolvimento de trabalhos das estações monitoradas, com registros dos históricos do uso de memória e CPU. Identificando a necessidade de atualização de equipamentos, e se for preciso, realizar o remanejamento das estações de trabalho.

No módulo desempenho também é possível: comparar o desempenho das estações de trabalho, produzir históricos de manutenção dos equipamentos, realizar o mapeamento da utilização dos recursos do computador e disponibiliza gráficos da utilização de memória e CPU das estações de trabalho, como nos mostra a figura 09.

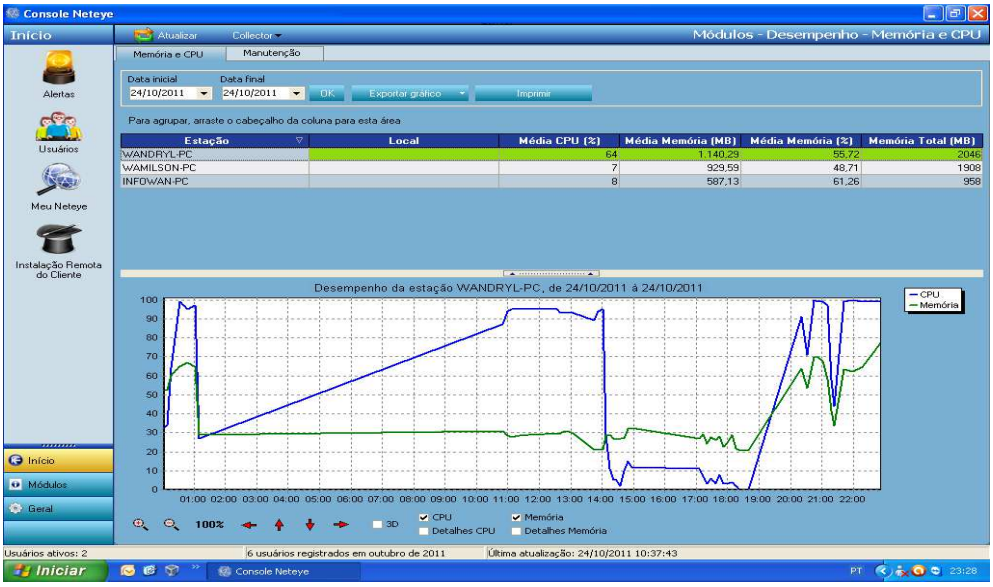


Figura.09 – Gráfico desempenho – memória e cpu

3.2 *SOFTWARE* DE GERENCIAMENTO DE REDE *“NTOP”*

O *Ntop* é uma ferramenta utilizada para monitorar e gerenciar redes. Este software tem diversos recursos que é apresentado através de gráficos e informações detalhadas permitindo a interação entre usuários. O *Ntop* roda em diversos sistemas operacionais *Unix/Linux e Win32,* onde monitora e gera relatórios com eficiência sobre o tráfego e suporte dos *hosts* pelos protocolos: TCP/UDP/ICMP, (R)ARP, IPX, DLC, *Decnet, AppleTalk, Netbios*, TCP/UDP. Foi desenvolvido por Luca Deri e Rocco Carbono na “*University of Pisa*” na Itália.

Essa ferramenta tem como característica muito boa, o acesso via Browser Web para realizar o gerenciamento e visualização das informações geradas pelo *Ntop,* para que se possa entender o status da rede, e também desta forma gerenciar a rede via acesso remoto.

Dentro do contexto, MORIMOTO (2009, p. 165), afirma:

> Uma forma simples de monitorar o tráfego global da sua rede interna é instalar o *ntop* no gateway da rede. Ele monitora todo o tráfego, mostrando o volume de banda consumido por cada máquina da rede e, dentro de cada relatório, informações detalhadas sobre os protocolos utilizados. Através dele, é fácil identificar máquinas da rede que estão consumindo uma grande quantidade de banda devido à utilização de programas P2P como o *Kazaa* ou o *Bittorrent*,

O *software Ntop* é *open-source* (gratuito), auxilia na administração de redes, é diferente de outras ferramentas existentes no mercado, tanto opções *free* ou pagas, pois sua instalação como veremos, é fácil e simples, mas não pensem que por não necessitar de configurações complicadas, ele não dê conta do recado, pelo contrário, ele até surpreende, a princípio não se engane com a maneira simples dos relatórios, mas ele esconde um volume grande de detalhes com relação às conexões.

Foi realizado um tutorial de instalação, o qual se encontra no Apêndice – B, para sanar as dúvidas, que por ventura venha a aparecer no decorrer da instalação do *software ntop*.

O *Ntop* realiza o monitoramento através de coletas de dados sobre os protocolos e hosts da rede.

3.2.1 Características e funcionalidade do *ntop*

- ✓ Realiza a análise dos pacotes que trafegam na rede
- ✓ Ordena a listagem do tráfego de rede conforme os protocolos
- ✓ Mostra gráficos das estatísticas de tráfego
- ✓ Armazena em seu banco de dados as estatísticas
- ✓ Identifica as informações dos *hosts* da rede, tanto do próprio sistema operacional, quanto das estações da rede
- ✓ Mostra a distribuição do tráfego IP sobre os protocolos da camada de aplicação
- ✓ Decodifica os protocolos da camada de aplicação, incluindo os *softwares* P2P encontrados
- ✓ Realiza a coleta de fluxos gerados pelos roteadores e *switches* através do *Netflow*
- ✓ Lista dos endereços IP da rede os quais acessaram o servidor, permitindo localizar estações que rodam programas P2P e outros aplicativos que consomem muito tráfego da rede, desde que todo o tráfego de dados de internet realmente tenha passado pelo servidor
- ✓ O acesso às informações, é realizado através de um *browser* integrado (*WebServer*).

3.2.2 Lista de parâmetros adicionais mais utilizados no *ntop*

Parâmetro	Descrição
-A	Define ou altera a senha do usuário do administrador
-a <arquivo>	Habilita os *logs* no servidor web: Onde por padrão o *Ntop* não gera *logs* das requisições que o servidor web recebe. Para habilitar, utilize esta opção acompanhado do nome do arquivo onde serão armazenados os *logs*.
-b	Desabilita decodificadores de protocolos: Os decodificadores realizam a coleta dos dados sobre vários tipos de protocolos das pilhas *Netbios*, *Netware* e *TCP/IP*.
-d	Inicia o *Ntop* em modo *deamon* (*background*): Parametro inserido pelo script de inicialização.
-i <nome>	Nome das interfaces que serão monitoradas
-k	Habilita o modo de depuração: para diagnosticar problemas de serviço.
-M	Não une o tráfego das interfaces de rede: O padrão do *Ntop* é unir os dados coletados das interfaces em um único conjunto de contadores.
-m	Redes que serão consideradas locais
-n	Não resolve endereços nomes.
-P <caminho>	Caminho do diretório onde contém o banco de dados do programa.
-p <arquivo>	Substitui os protocolos que o *Ntop* analisa por padrão pelos contidos no arquivo
-u	Usuário que executará o processo do *Ntop*
-W	Porta do servidor web (HTTPS): o padrão do *Ntop*, é não responder HTTPS, sendo necessário então habilitar a porta para o suporte (porta 3001).
-w	Porta do servidor web (HTTP): o padrão do *Ntop Webserver* escuta na porta 3000. O endereço pode ser também especificado no formato “endereço:porta”. Por exemplo “HTTP://192.168.0.1:3000”

Tabela 01 – Lista de Parâmetros adicionais do *Ntop*

3.2.3 Monitoramento de protocolos adicionais

Protocolos que são monitorados pelo Ntop:

Protocolo	Portas
FTP	20 21
HTTP	80 443 3128
DNS	53
Telnet	23 513
NBios-IP	137 138 139
Mail	25 109 110
DHCP/BOOTP	67 68
DNMP	161 162
NNTP	119
NFS/AFS	2049 7000 – 7009
X11	6000 – 6010
SSH	22
Kazaa	1214
WinMX	6699 7730
eDonkey	4661 – 4665
BitTorrent	6881-6999 6969
Messenger	1863 5000 5001

Tabela 02 – Protocolos que são monitorados pelo *Ntop*

Os protocolos podem ser substituídos pelo administrador por intermédio do parâmetro de execução “ –p “ , o qual recebe o nome de um arquivo que contém os protocolos a serem monitorados como sendo argumento.

Edite o arquivo /etc/sysconfig/*ntop*:

Extra_arg="-i eth0,eth1 -W 3001 -p /usr/libntop/ntop/new-protocol.list

3.2.4 Monitorando o tráfego

Realizar o monitoramento de tráfego, é a habilidade concedida a um gerente de rede, pois é ele que identificará cada tipo de ação que foi efetuada na rede, e dependendo da política da empresa, tomar as devidas providências.

O *NTop* é ainda capaz de identificar:

- ✓ O uso de um endereço IP duplicado;
- ✓ Identificar quem são os hosts da rede;
- ✓ Configurar aplicativos que podem ser ativados para a rede;
- ✓ Identificar *Proxys*;
- ✓ Identificar quais protocolos podem ou não ser utilizados;
- ✓ Utilização de banda.

3.2.5 Gerando gráficos com o *ntop*

A primeira visão do *Ntop* com relação aos gráficos gerados, parecem serem simples, mas não se engane porque ele esconde um volume surpreendente de detalhes, os quais poderão serem acessados clicando em cima de determinado item dentro do gráfico, o qual lhe retornará um outro gráfico em específico.

Através dos gráficos, poderemos por exemplo descobrir o que estará causando lentidão na rede.

3.2.5.1 Estatísticas de tráfego global

No gráfico de estatísticas de tráfego global, temos o Fluxo de Pacotes da Rede conforme a figura 10, mostra a quantidade de pacotes recebidos e processados, bem como a porcentagem de pacotes perdidos durante a transmissão. Outras informações referente aos pacotes transmitidos, é com relação ao tamanho dos pacotes, destacando características como menor pacote, maior pacote, tamanho médio de pacotes, pacotes inválidos ou corrompidos detectados através do *checksum*, e exibida uma distribuição¸ considerando os diferentes tamanhos de pacotes analisados.

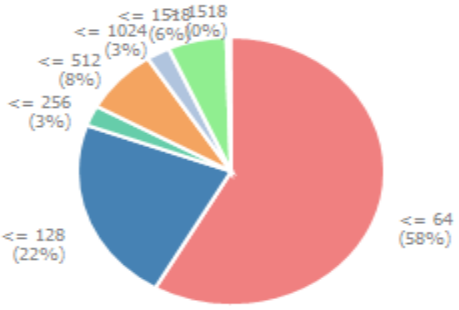
Packets	**Shortest**		42 bytes
	Average Size		155 bytes
	Longest		7,354 bytes
	Size <= 64 bytes	58.0%	66,192
	64 < Size <= 128 bytes	22.4%	25,558
	128 < Size <= 256 bytes	2.5%	2,873
	256 < Size <= 512 bytes	7.9%	9,002
	512 < Size <= 1024 bytes	2.5%	2,829
	1024 < Size <= 1518 bytes	6.3%	7,218
	Size > 1518 bytes	0.4%	492
			
	Packets too long [> 1514]	0.4%	492
	Bad Packets (Checksum)	0.0%	0

Figura.10 – Fluxo de pacotes na rede

É possível pelo *Ntop*, visualizar informações sobre a situação atual da rede, nos últimos 5 minutos, pico de acesso e acesso médio, como nos mostra na figura 11.

Network Load	Actual	39.2 Kbit/s	43.5 Pkt/s
	Last Minute	44.2 Kbit/s	52.1 Pkt/s
	Last 5 Minutes	52.0 Kbit/s	41.5 Pkt/s
	Peak	329.7 Kbit/s	75.6 Pkt/s
	Average	32.6 Kbit/s	19.4 Pkt/s

Figura.11 – Informação atual da rede

Na distribuição global de protocolos, a figura 12 nos mostra quais protocolos de internet estão sendo utilizados sobre a rede, exibe o volume e a porcentagem de dados trafegados através dele. Também são informados quais protocolos de transporte, referentes ao protocolo de internet destacado foram utilizados na sessão, exibindo seus respectivos volumes e porcentagens de dados transmitidos.

Global Protocol Distribution

Protocol	Data	Percentage			
IP	24.4 MBytes	92.3%	TCP	24.0 MBytes	98.4%
			UDP	991.6 KBytes	4.0%
			ICMP	8.7 KBytes	0%
			IGMP	1.5 KBytes	0%
			Other IP	1.9 KBytes	0%
(R)ARP	36.9 KBytes	0%			
IPv6	591.4 KBytes	2.2%			

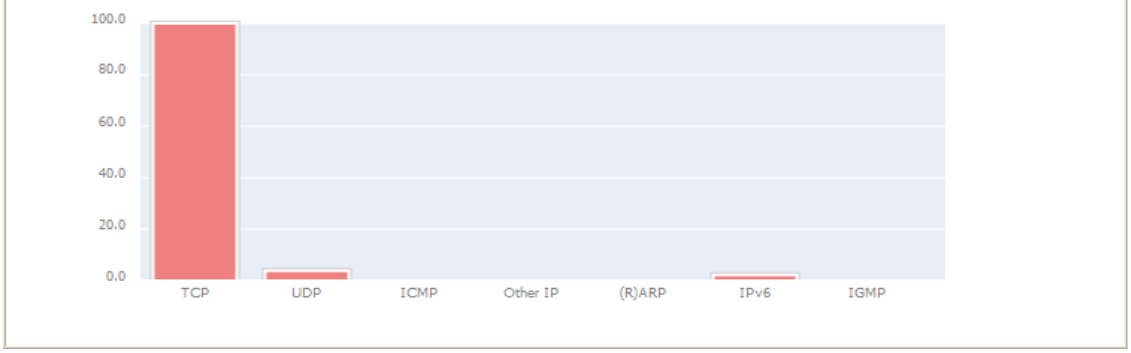


Figura.12 – distribuição global de protocolos

Nos gráficos da opção global TCP/UDP de distribuição de protocolos, é possível visualizar gráficos de uso do *Messenger* (figura 13), email (figura 14), *software* P2P como na figura 15, informando o gráfico e o volume de porcentagem de quanto foi trafegado pela rede.

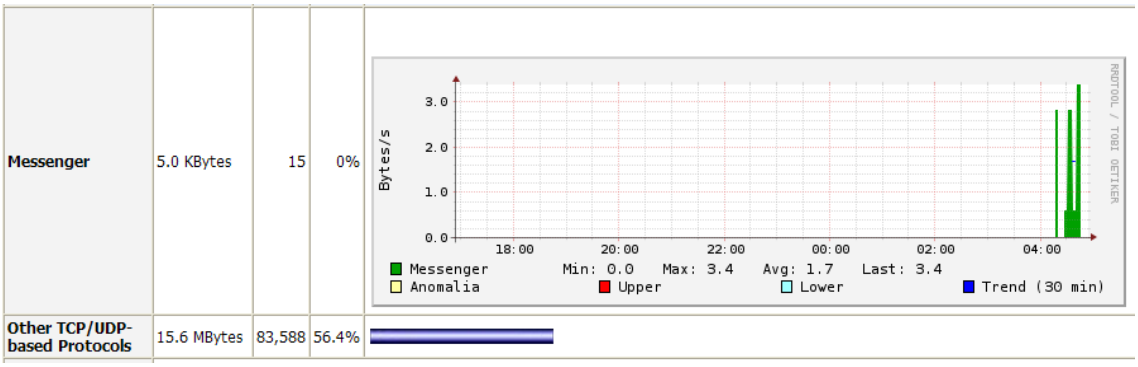


Figura.13 – gráfico de acesso *Messenger*

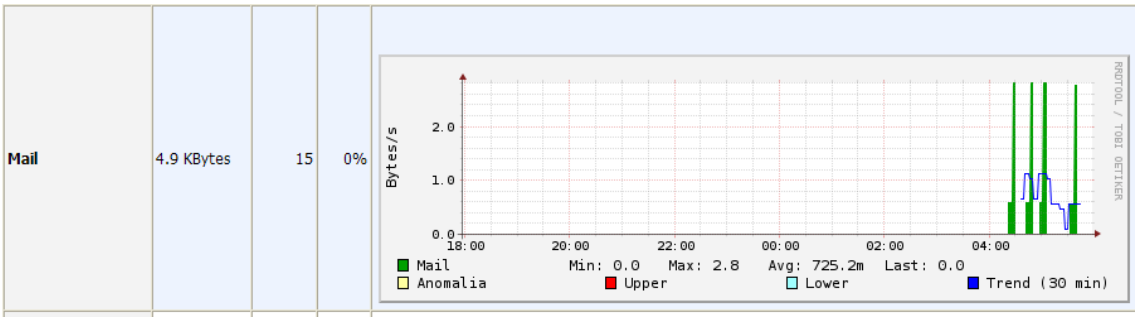


Figura.14 – gráfico de acesso *email*

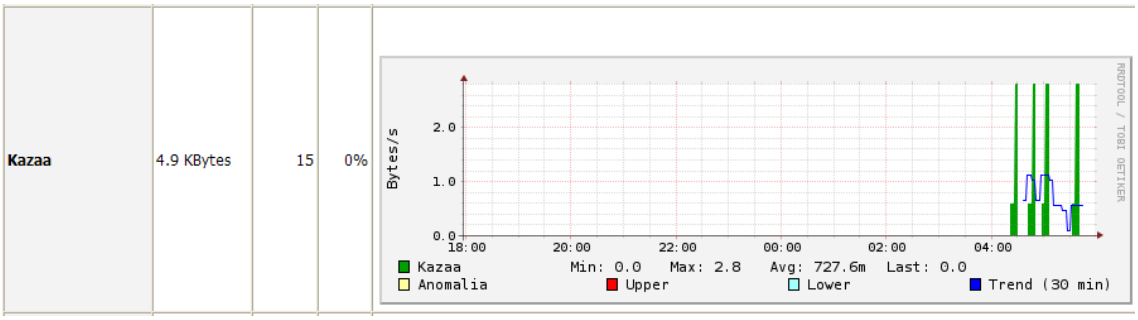


Figura.15 - gráfico de acesso ao *kazaa*

3.2.5.2 Tráfego de portas acessadas

No TCP/UDP nos mostra ainda o trafego das últimas portas utilizadas recentemente, conforme a figura 16, onde exibe a relação das portas utilizadas e quantidade de pacotes enviados e recebidos. Clicando em cima de uma porta, é possível visualizar quais servidores utilizaram a referida porta, e clicando também sobre o link do servidor, será exibida informações com relação à estação conectada na porta.

TCP/UDP Port		Total	Sent	Rcvd
www	80	13.5 KBytes	8.7 KBytes	4.7 KBytes
52229	52229	5.2 KBytes	1.4 KBytes	3.7 KBytes
48688	48688	3.5 KBytes	1.4 KBytes	2.0 KBytes
57315	57315	2.9 KBytes	937	2.0 KBytes
57316	57316	1.9 KBytes	947	1015
3000	3000	865	187	678
2646	2646	865	678	187
63226	63226	624	624	0
1900	1900	624	0	624

Notes:

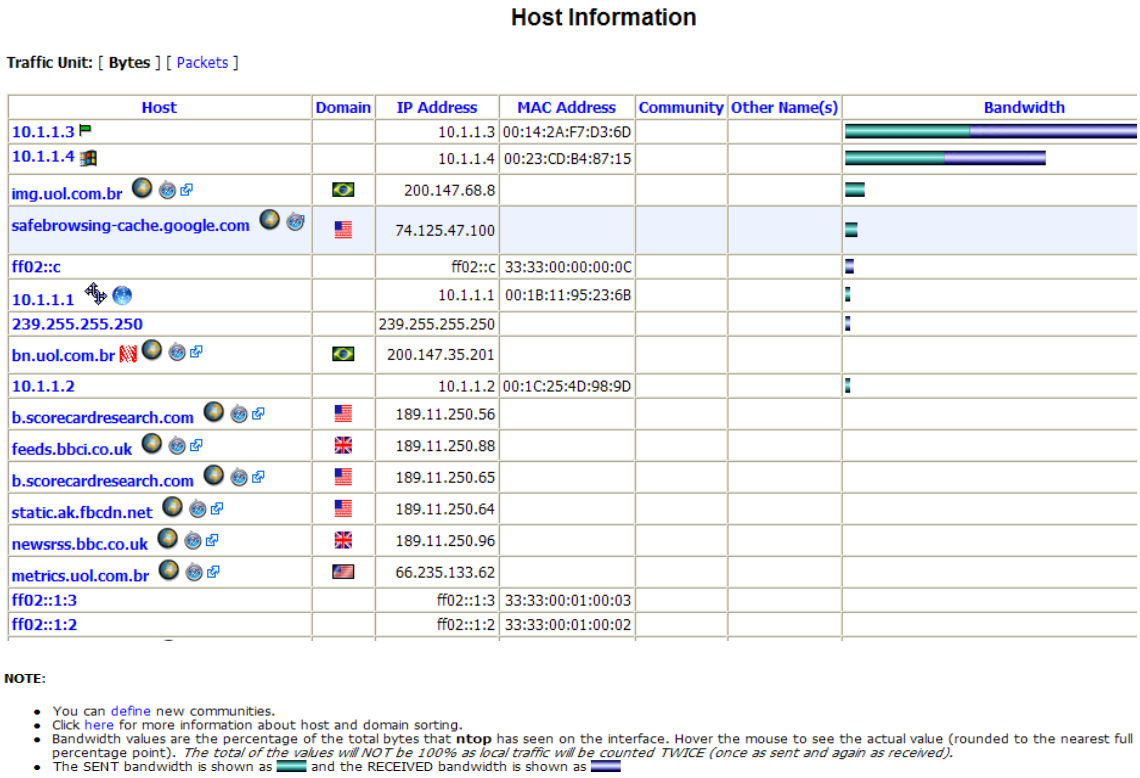
- sum(total traffic per port) = 2*(total IP traffic) because the traffic per port is counted twice (sent and received)
- This report includes broadcast packets

Figura.16 – Tráfego de portas acessadas

3.2.5.3 Gráfico *summary hosts*

O gráfico de informações dos *hosts*, captura os acessos, através da rede monitorada. É visualizado em forma de tabela, conforme figura 17, onde exibe os dados gerais dos *hosts*, como endereço IP, MAC, largura da banda que está sendo utilizado.

Se clicarmos sobre o identificador do *host*, na primeira coluna da tabela, será possível visualizar mais a fundo informações detalhadas do *host*, conforme figura 18.



Host Information

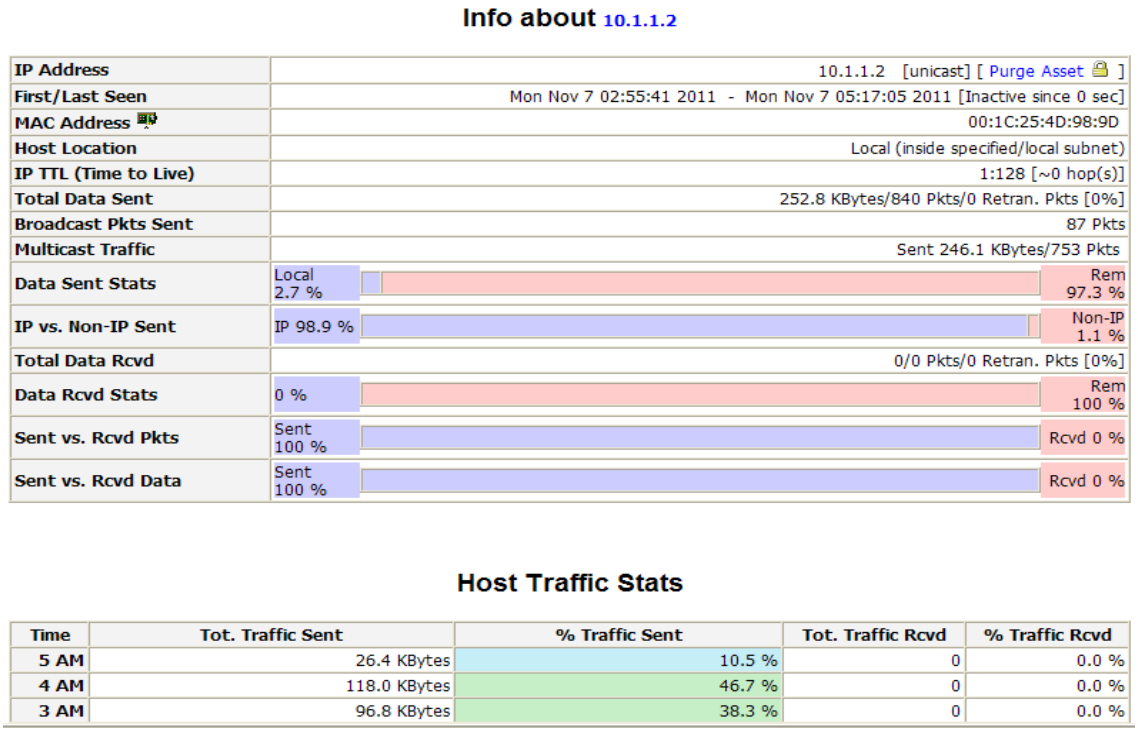
Traffic Unit: [**Bytes**] [Packets]

Host	Domain	IP Address	MAC Address	Community	Other Name(s)	Bandwidth
10.1.1.3		10.1.1.3	00:14:2A:F7:D3:6D			
10.1.1.4		10.1.1.4	00:23:CD:B4:87:15			
img.uol.com.br		200.147.68.8				
safebrowsing-cache.google.com		74.125.47.100				
ff02::c		ff02::c	33:33:00:00:00:0C			
10.1.1.1		10.1.1.1	00:1B:11:95:23:6B			
239.255.255.250		239.255.255.250				
bn.uol.com.br		200.147.35.201				
10.1.1.2		10.1.1.2	00:1C:25:4D:98:9D			
b.scorecardresearch.com		189.11.250.56				
feeds.bbci.co.uk		189.11.250.88				
b.scorecardresearch.com		189.11.250.65				
static.ak.fbcdn.net		189.11.250.64				
newsrss.bbc.co.uk		189.11.250.96				
metrics.uol.com.br		66.235.133.62				
ff02::1:3		ff02::1:3	33:33:00:01:00:03			
ff02::1:2		ff02::1:2	33:33:00:01:00:02			

NOTE:

- You can define new communities.
- Click here for more information about host and domain sorting.
- Bandwidth values are the percentage of the total bytes that **ntop** has seen on the interface. Hover the mouse to see the actual value (rounded to the nearest full percentage point). *The total of the values will NOT be 100% as local traffic will be counted TWICE (once as sent and again as received).*
- The SENT bandwidth is shown as and the RECEIVED bandwidth is shown as

Figura.17 – gráfico Informação de *Hosts***.**



Info about 10.1.1.2

IP Address	10.1.1.2 [unicast] [Purge Asset]
First/Last Seen	Mon Nov 7 02:55:41 2011 - Mon Nov 7 05:17:05 2011 [Inactive since 0 sec]
MAC Address	00:1C:25:4D:98:9D
Host Location	Local (inside specified/local subnet)
IP TTL (Time to Live)	1:128 [~0 hop(s)]
Total Data Sent	252.8 KBytes/840 Pkts/0 Retran. Pkts [0%]
Broadcast Pkts Sent	87 Pkts
Multicast Traffic	Sent 246.1 KBytes/753 Pkts
Data Sent Stats	Local 2.7 % / Rem 97.3 %
IP vs. Non-IP Sent	IP 98.9 % / Non-IP 1.1 %
Total Data Rcvd	0/0 Pkts/0 Retran. Pkts [0%]
Data Rcvd Stats	0 % / Rem 100 %
Sent vs. Rcvd Pkts	Sent 100 % / Rcvd 0 %
Sent vs. Rcvd Data	Sent 100 % / Rcvd 0 %

Host Traffic Stats

Time	Tot. Traffic Sent	% Traffic Sent	Tot. Traffic Rcvd	% Traffic Rcvd
5 AM	26.4 KBytes	10.5 %	0	0.0 %
4 AM	118.0 KBytes	46.7 %	0	0.0 %
3 AM	96.8 KBytes	38.3 %	0	0.0 %

Figura.18 – Informações detalhada sobre o IP 10.1.1.2

4 RESULTADOS / VALIDAÇÃO

Com o trabalho de conclusão de curso sobre gerenciamento de rede, foi possível adquirir conhecimentos de gerência de rede, os quais serão aplicados à prática no mercado de trabalho. Os *softwares* analisados obtiveram excelentes resultados, de acordo com os testes realizados. O *neteye* e o *ntop* podem ser instalados facilmente por um administrador sem ter conhecimentos específicos, e realizar o gerenciamento de uma empresa de acordo com as suas necessidades.

O *software neteye* realiza o gerenciamento através dos módulos: inventário, produtividade, monitoramento, segurança e desempenho. Com um ótimo desempenho, e facilidade no processo de configuração e manipulação do *software*. Quando a empresa optar por adquirir licença do produto, terá a vantagem de suporte técnico para sanar qualquer dúvida.

O *ntop* é um *software* de gerência de rede livre (gratuito), sendo uma opção para as empresas que não querem investir em um *software* pago, não deixando a desejar para os *softwares* proprietários.

5 CONCLUSÃO

O gerenciamento de rede via *software*, independentemente do tamanho da rede a ser gerenciada, as empresas não podem ficar sem um sistema de controle gerenciável, pois a evolução da informática é muito rápida, e as empresas necessitam ter em mãos um controle confiável para tomada de decisões, seja no âmbito da questão de segurança das informações, controle de equipamentos ou mesmo para verificar a produtividade de seus colaboradores.

Com a implantação de *softwares* de gerenciamento de redes, é possível controlar os equipamentos da rede, além de aumentar a qualidade no serviço da empresa. Ao utilizar os *softwares* de gerência, diminuirá o tempo gasto por técnicos para resolução de problemas, aumentado a eficiência da equipe de gerência.

As ferramentas de gerenciamento estudadas corresponderam de forma positiva nos testes realizados, demonstraram que são de extrema importância, para que se possa garantir qualidade no gerenciamento de redes nas empresas.

Como sugestão para estudos futuros, pesquisar outras ferramentas, porque além destas estudadas, existem “ n “ *softwares* que realizam gerenciamento, desta maneira ou quem sabe até melhor. Fica o desafio lançado.

APÊNDICE

A – Instalação do *Neteye*

O primeiro passo antes de começar a instalação do *Neteye*, será necessário criar uma pasta (pode ser com o próprio nome *neteye*), nesta pasta, ficará os instaladores do *Neteye* Cliente. Portanto, deverá ser compartilhada na rede com acesso de leitura para todas as estações da rede.

Para iniciar a instalação do Programa *Neteye* v.5, é necessário executar o "*Instalador_neteye.exe*", que foi realizado o download do próprio site da *Neteye*, figura 19.

Figura.19 – Tela de apresentação do *Neteye*

Na figura 20 é solicitado o diretório para instalação do *Neteye*, pode-se deixar no padrão mesmo.

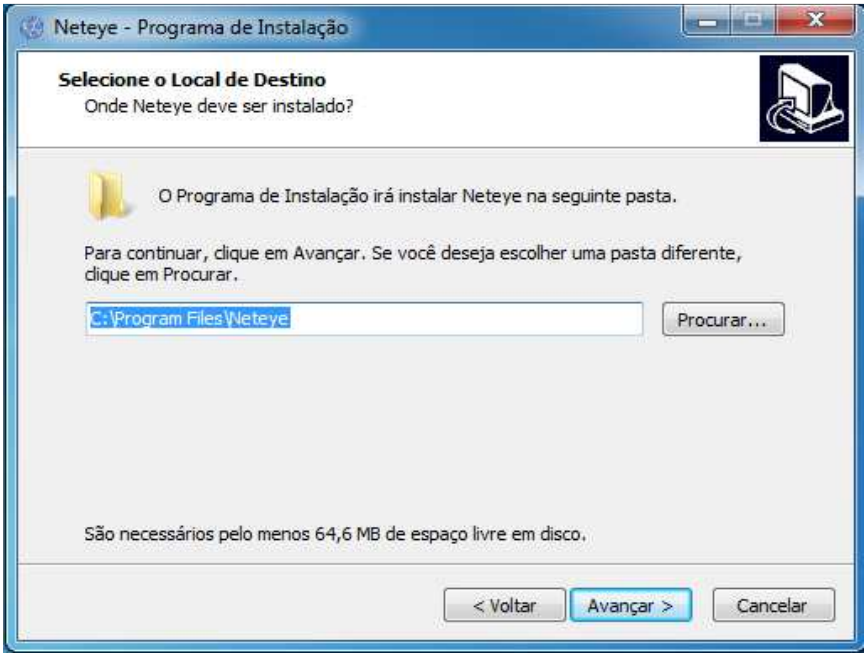


Figura.20 – Tela definir caminho da instalação

Na figura 21 apresenta 06 opções de instalação do *Neteye* para utilizar com banco de dados.

Escolha a opção padrão "*Collector Primário* + *Sql Express* (Recomendado).

Se o seu computador não tiver instalado o *Netframework*, será solicitado a instalação, caso já possua, seguirá para o próximo passo.

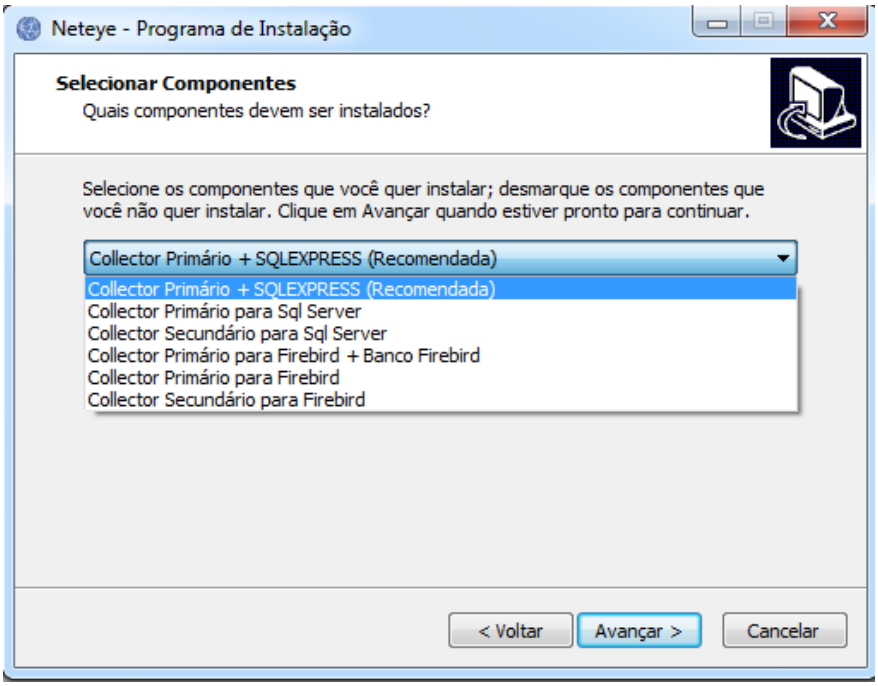


Figura.21 – Opções de banco de dados

Na figura 22, será solicitada o Código do *Collector*, o número da porta que será utilizada para conexão e o nome ou o IP da máquina que será o servidor do *Neteye*.

Pode-se deixar na sugestão que o próprio sistema já preenche, ou se preferir, poderá alterá-la.

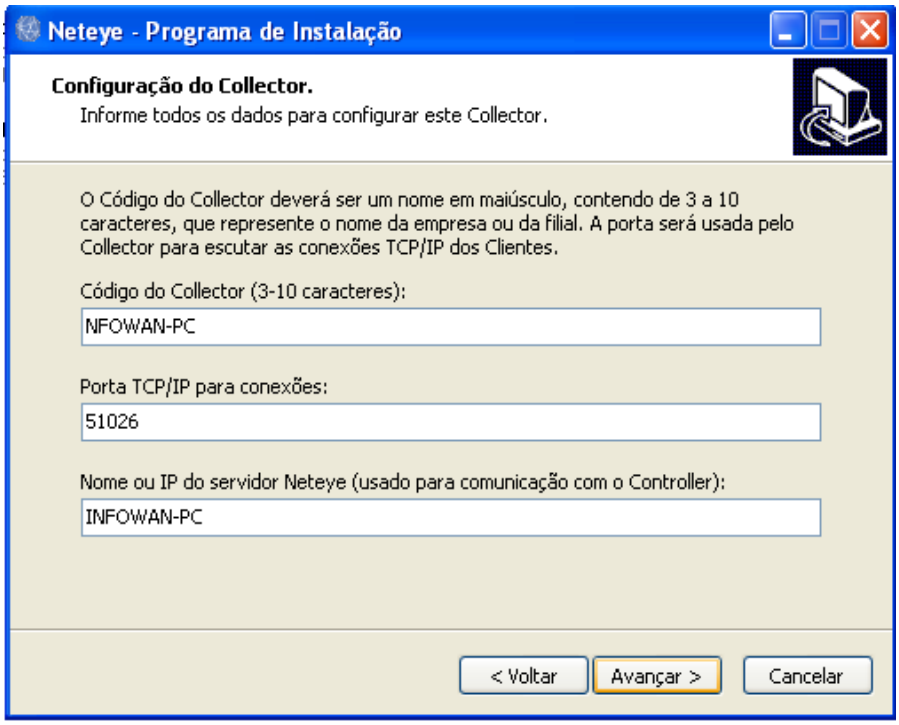


Figura.22 – Configuração do *collector*

Nesta tela conforme figura 23, terá que informar o caminho onde ficarão os instaladores do *Neteye* Cliente (programa necessário para instalar em todas as estações, que serão monitoradas). É neste ponto, que utilizaremos aquela pasta que foi criada e compartilhada antes do início da instalação.

É recomendado, que seja informado o caminho do diretório da rede no formato UNC, ou seja, “ \\ “).

No exemplo acima, havia criado uma pasta no diretório Raiz, com o nome de *Neteye*. A sintaxe é a seguinte:

\\nome_do_computador_servidor\nome _da_pasta_criada

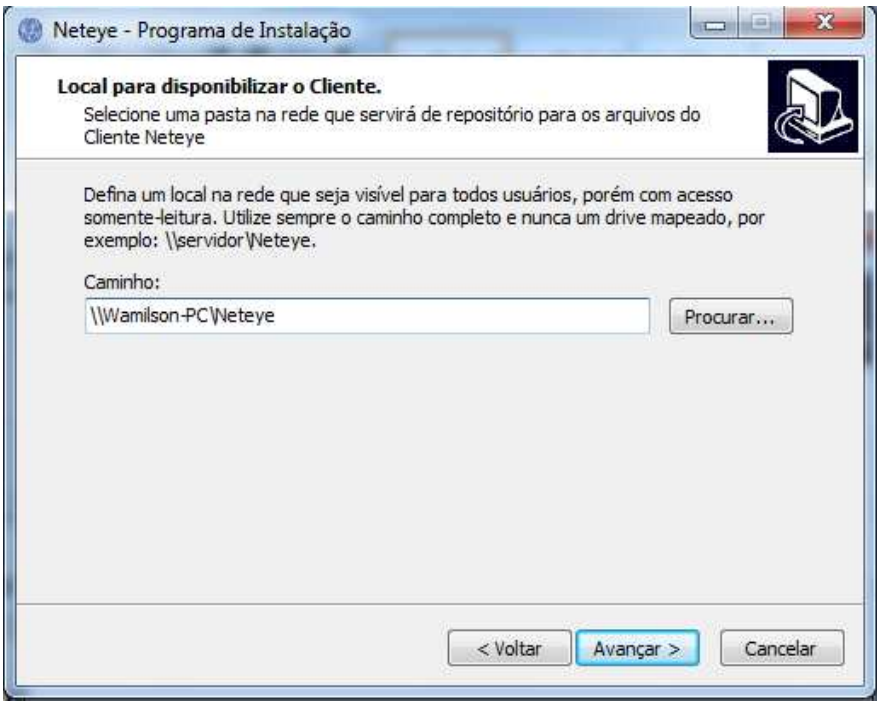


Figura.23 – Caminho para disponibilizar o cliente

Na figura 24, terá que informar o nome da pasta na rede, onde os usuários terão acesso à console.

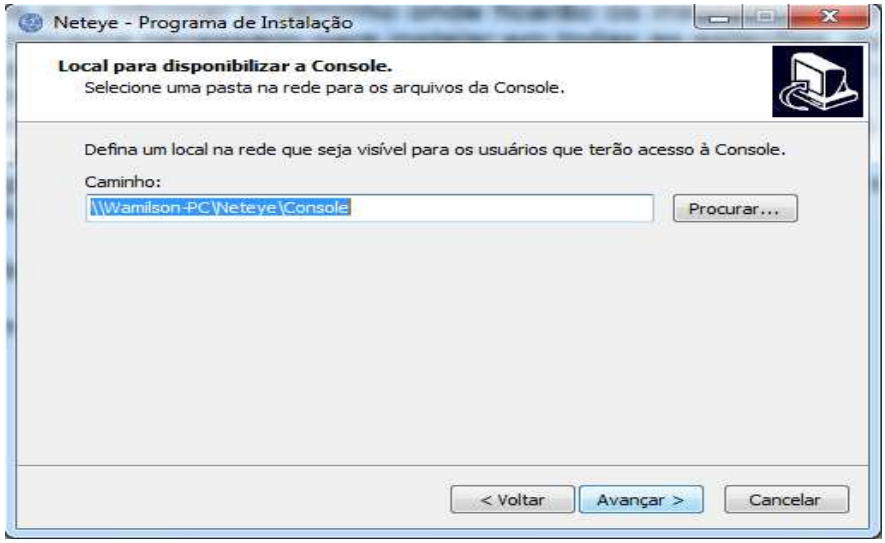


Figura.24 – Tela local para disponibilizar a console

Será necessário informar o endereço do computador *Collector* (o que está sendo instalado o *Neteye*), conforme figura 25, onde através deste endereço, as estações irão ter acesso. Pode ser o endereço do computador (nome na rede), ou o IP (endereço na rede).

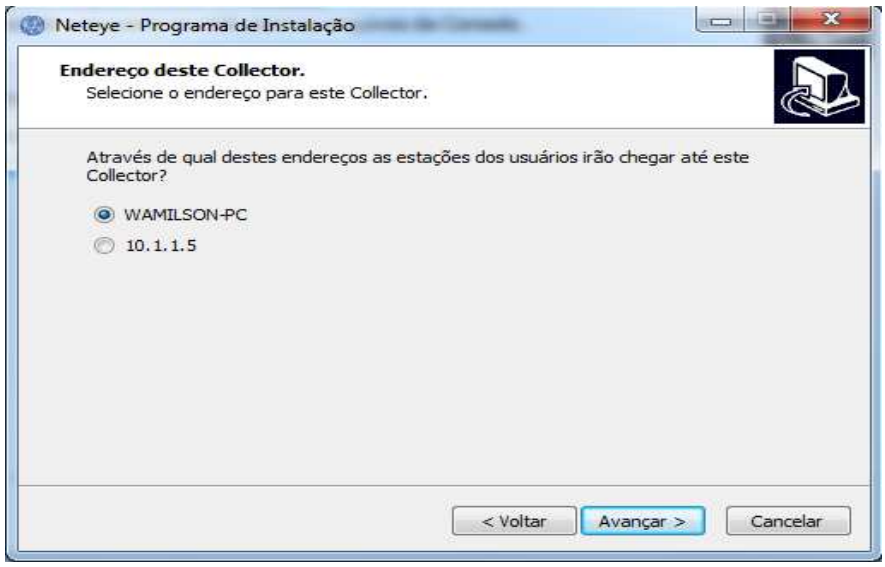


Figura.25 – Tela endereço do *collector*

Na figura 26, será solicitado para escolher a conta que irá iniciar o serviço do *collector*. Utilize a opção padrão recomendado.

Figura.26 – Tela conta para executar o *collector*

Na figura 27, é solicitado o nome da pasta onde o programa instalará os atalhos para acesso.

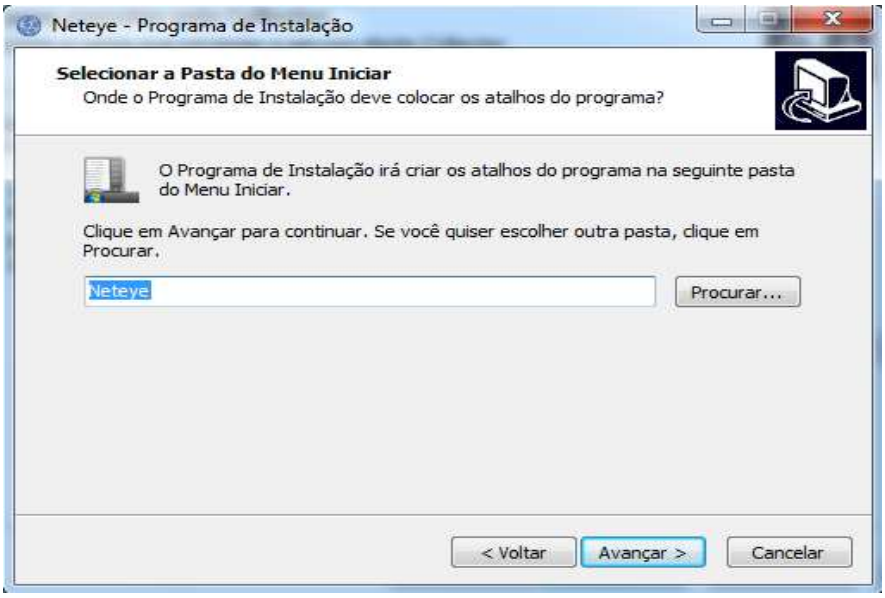


Figura.27 – Selecionar a pasta do menu iniciar

Na figura 28, deverá escolher quais as tarefas adicionais que você deseja que seja executado enquanto instala o *neteye*.

Figura.28 – Selecionar tarefas adicionais

Neste ponto da instalação (figura 29), iniciará a instalação do *neteye*. Se não foi informado o endereço da rede corretamente ou se o usuário que esteja utilizando, não tiver privilégio de administrador, dará erro e não prosseguirá com a instalação. Desta forma, reinicie a instalação e certifique-se de estar como usuário administrador e informe o caminho correto da rede.

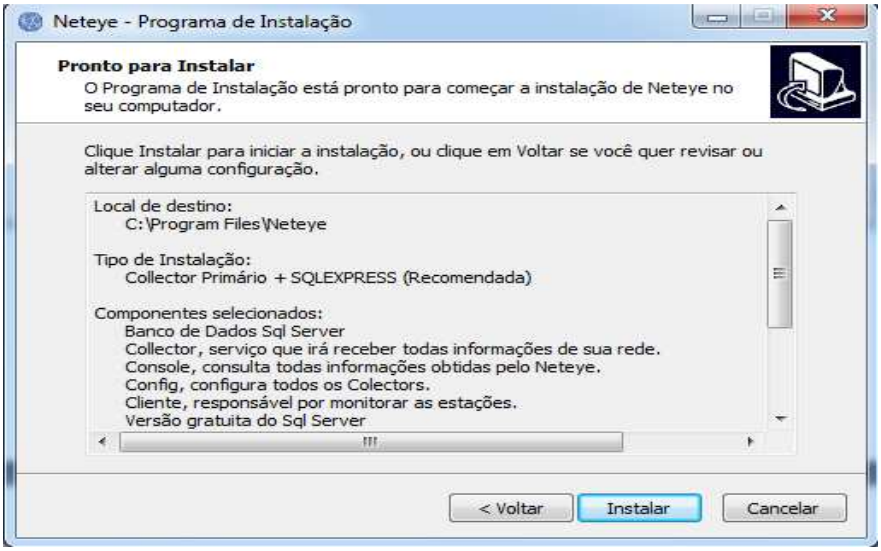


Figura.29 – Tela pronto para instalar

No final da instalação (figura 30), aparecerá a tela, onde exibe o caminho que deverá ser anotado para instalar o instalador do Cliente (“Instala.bat”). Este caminho será utilizado para que se possa realizar a instalação do Cliente nas estações de trabalho. Em cada estação, terá que executar o “instala.bat”.

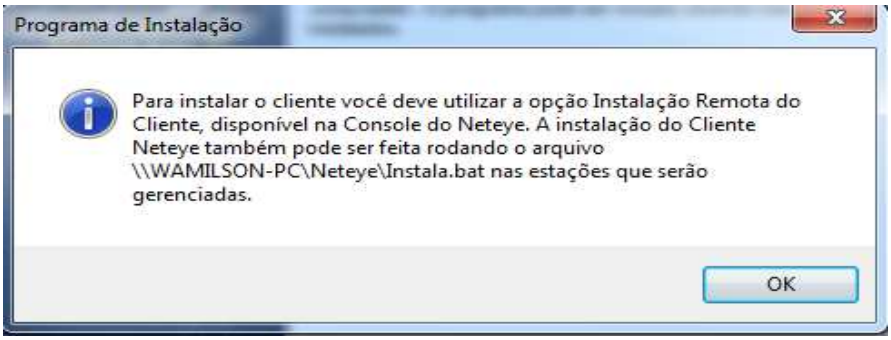


Figura.30 – Orientação do caminho para as estações

Na figura 31, mostra que você terminou a instalação no servidor, que irá realizar o gerenciamento da rede.

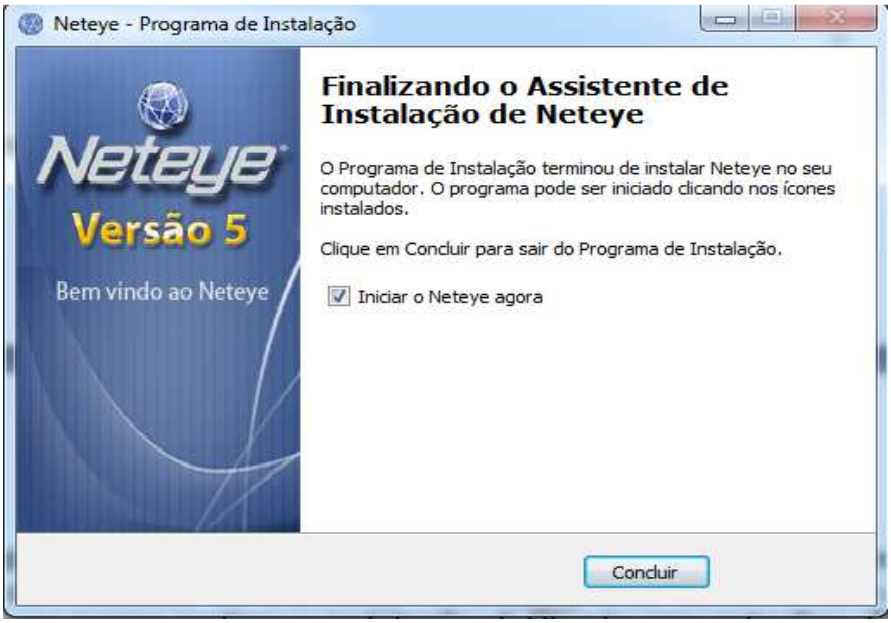


Figura.31 – Tela finalização da instalação do *neteye*

Após a instalação do *neteye* no servidor, será necessário antes de prosseguir com as configurações no sistema, configurar as estações para que o *neteye* consiga realizar o monitoramento.

Lembrando que, deve-se então, ir a todas as estações que serão monitoradas, e acessar a pasta do *neteye* que foi criada antes do início da instalação, para que as estações pudessem acessar o arquivo “instala.bat”.

Na figura 32, mostra que o software foi instalado na estação de trabalho, esta tela fechará automaticamente. Depois reinicie a estação de trabalho e verifique se apareceu no servidor de gerenciamento de rede. Se por acaso a estação não aparecer no servidor, volte na estação e refaça a instalação e aperta as CTRL + Break para você poder visualizar se houve algum erro na instalação.

Quando for executado o arquivo “instala.bat”, a instalação criará automaticamente na estação a pasta \windows\ne , aonde ficarão os arquivos do programa.

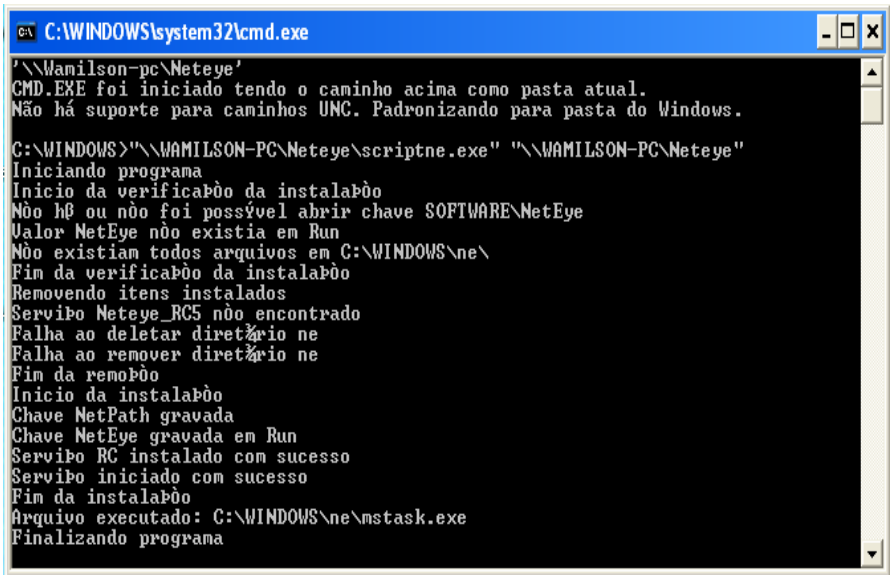


Figura.32 – Tela após executar o arquivo Instala.bat na estação

Se for utilizar a versão free para 05 estações, clique em “Quero usar o *Neteye Free* (máximo 05 estações), conforme figura 33.

Deverá preencher os campos: empresa, nome e email (*email* válido, pois será enviado para este email o número de série e chave de ativação).

Após receber o número de série e código de ativação, copie para os devidos campos e clique em ativar.

Ao clicar em ativar, será enviado para a empresa *neteye* e será verificado se os dados conferem com os informados e liberados para utilização.

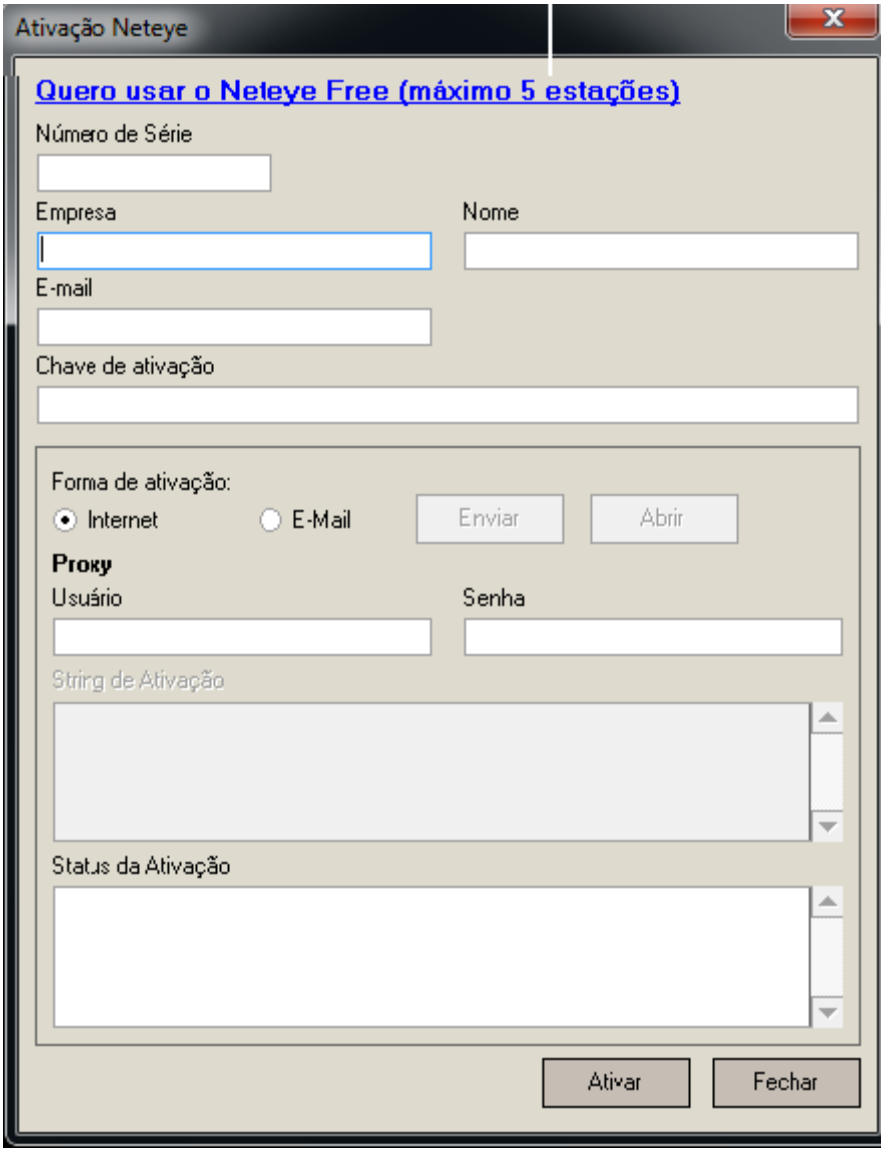


Figura.33 – Tela de ativação do *Neteye*

CONFIGURAÇÕES DO *NETEYE*

Após a instalação do *Neteye*, é necessário iniciar o *config* do *neteye*, conforme figura 34. O primeiro passo após abrir a tela de configurações, será dar permissão aos usuários que terão acesso às informações captadas pelo gerenciador *neteye*.

Figura.34 - *Config Neteye*

Na tela Permissões de Acesso (figura 35), deverão ser cadastrados os usuários que poderão ter acesso às informações captadas pelo *neteye* das estações. Poderá ser definido também o que o usuário cadastrado poderá acessar.

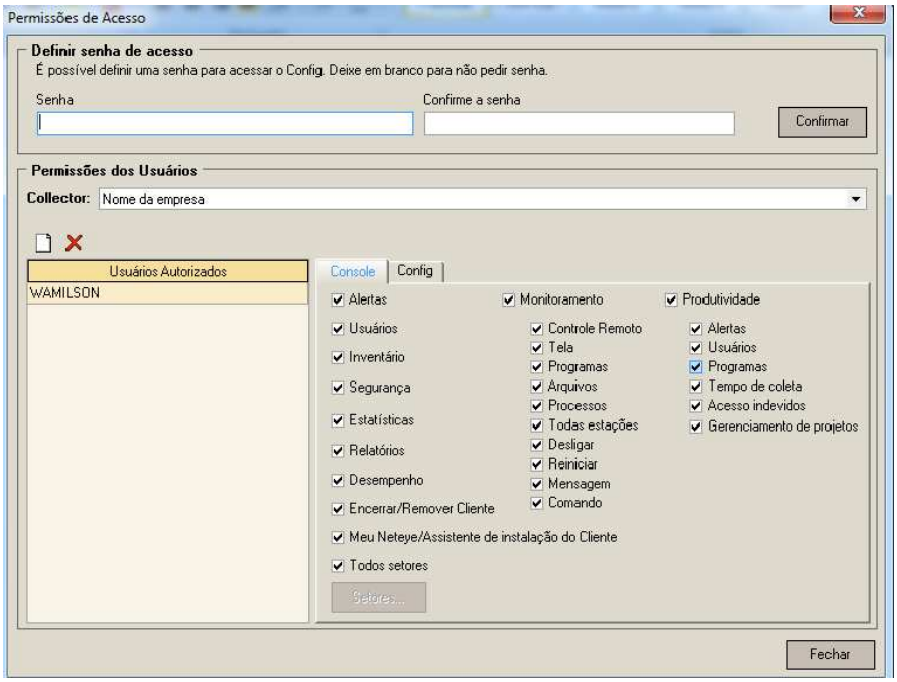


Figura.35 – Tela permissão de acesso

Na opção de “Acessos Indevidos” (figura 36), ainda no *config neteye*, poderá selecionar palavras chaves, as quais a empresa irá monitorar, onde, quando a estação “X” realizar algum acesso com palavra chave pré-definida, irá automaticamente, capturar a tela e enviar para o servidor, onde ficará registrado o acesso, e o administrador do sistema, tomará as devidas providências.

Há as seguintes opções: Adicionar, remover, selecionar tudo e ordenar.

Função :

- Adicionar: acrescentar uma nova palavra chave para ser monitorada pelo *Neteye*.
- Remover: para remover uma palavra chave a qual não se quer realizar o monitoramento pelo *Neteye*.
- Selecionar tudo: opção para selecionar tudo, e depois por exemplo, apagar tudo de uma só vez.
- Ordenar: colocar em ordem alfabética as palavras chaves que são monitoradas.

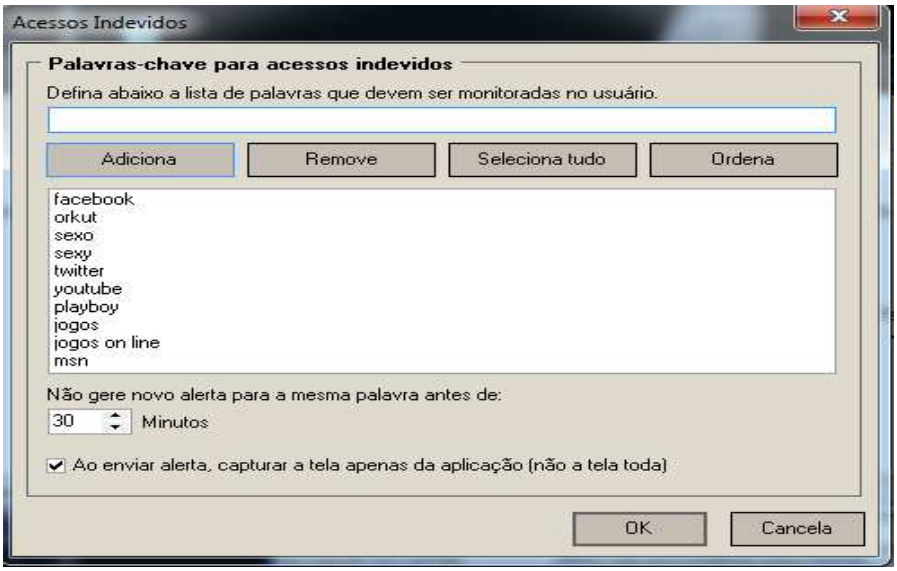


Figura.36 – Tela de configuração de acessos indevidos

Na opção “Alerta” (figura 37), configurar as opções de alertas que se queira realizar o monitoramento. Receberá os alertas no servidor de gerenciamento do *neteye*, ou através de email, se optar também por receber desta maneira, e é claro, terá que configurar na opção “Notificações”, uma conta de email para receber os alertas.

Os alertas serão monitorados na parte de: inventário, segurança, produtividade e administrativo.

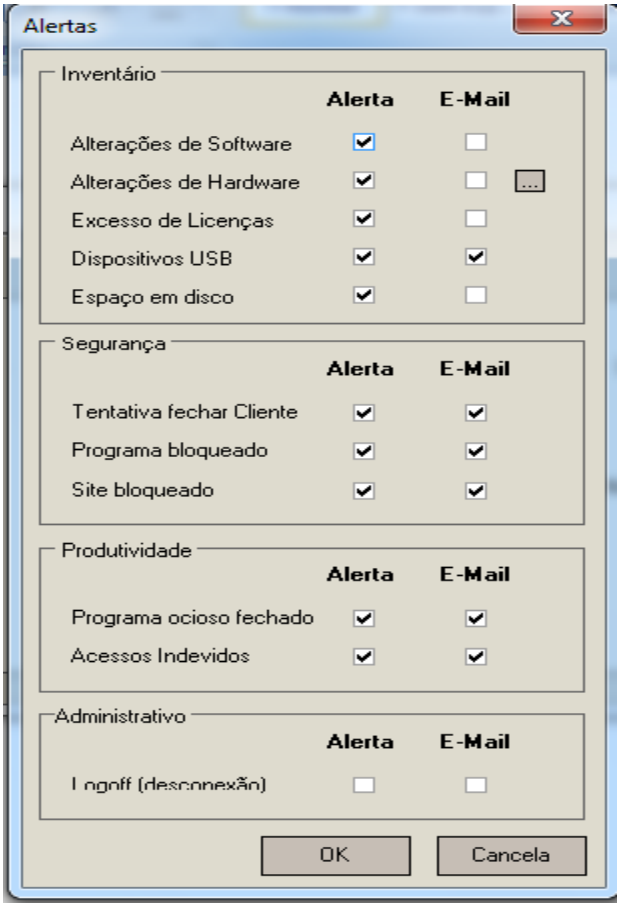


Figura.37 – Tela de configuração de alertas

Na tela de configuração de alertas, existe a opção “Alterações de *Hardware*”, e ao lado existe o ícone [...] onde dará acesso para que seja selecionado o que será monitorado na parte de *hardware*, conforme figura 38, caso haja alguma alteração na estação, automaticamente será enviado um alerta de alteração de *hardware*, especificando de qual estação ocorreu a alteração.

Configure de acordo com as suas necessidades.

Figura.38 – Opções do ítem alterações de *hardware*

Nesta tela (figura 39), você define qual a máquina *collector*. Deve-se configurar se o programa ficará oculto, *systray* ou aparecer nas estações. Definir também de quantos minutos as informações serão gravadas no banco de dados e de quantos minutos será a comunicação da estação com o *collector*.

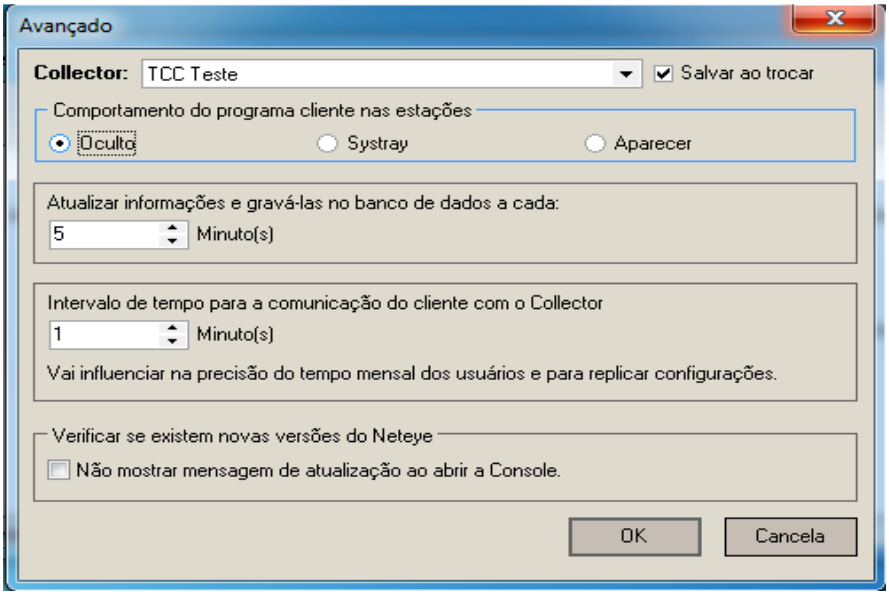


Figura.39 – Tela de configuração do item Avançado

Na opção “Desempenho” (figura 40), você vai escolher se quer realizar a monitoração do desempenho de *hardware* das estações e em quantos minutos será enviado a média de utilização de CPU e memória. . Definir também quanto tempo deverá ficar gravado as estatísticas.

Figura.40 – Configuração de desempenho

Nas configurações de “Produtividade” (figura 41), já vem pré-configurado uma lista de programas, quando o usuário acessar, ele estará sendo monitorado pelo gerenciador de rede *neteye* e ficará registrado quanto tempo o usuário ficou no programa.

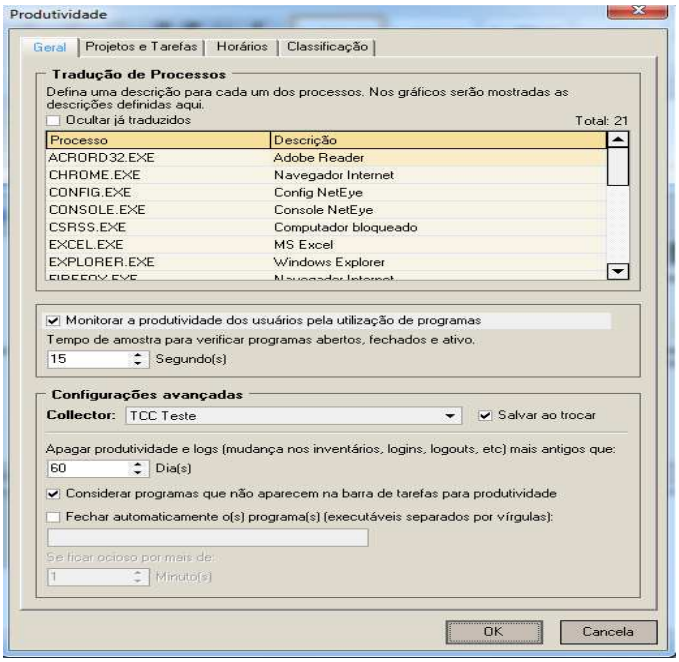


Figura.41 – Tela de configuração Produtividade

B – Instalação do *Ntop* no *Ubuntu* 10.04

Primeiramente, será necessário atualizar o arquivo " *sources.list*", onde poderá acessar através do *shell*, seguindo os seguintes passos:

$ sudo su

Digite a senha de usuário administrativo.

Com o comando abaixo, você estará editando o arquivo de configuração e atualizar o arquivo *sources.list.*

 # joe /etc/apt/*sources.list*

Após abrir o arquivo "*souces.list*", incluir as seguintes linhas abaixo para atualizar o arquivo de *sheel.*

deb http://ftp.br.debian.org/debian/ stable main
deb-src http://ftp.br.debian.org/debian/ stable main

deb http://ufpr.dll.sourceforge.net/ stable main

deb-src http://ufpr.dll.sourceforge.net/ stable main

deb http://ftp.br.debian.org/debian/ testing main
deb-src http://ftp.br.debian.org/debian/ testing main
deb http://download.unesp.br/linux/debian/ testing main
deb-src http://download.unesp.br/linux/debian/ testing main

Depois de realizar as alterações, salve o arquivo. No caso do editor "Joe", aperte a tecla CTRL + K + W para salvar as informações, e para sair do editor de texto aperte CTRL + K + Q, estará novamente no prompt de comando.

Após isto, execute o seguinte comando:

 # apt-get update

Neste passo, irá realizar atualização do ubuntu.

Após o termino do update execute a instalação do ntop:

 # apt-get install ntop

Após o termino da instalação execute o ntop:

 # ntop

Ele irá pedir a senha que você deseja para o admin da conta:

Please enter the password for the admin user:
Please enter the password again:

Após inserir uma senha para a conta *admin* acesse um navegador web e digite o seguinte endereço:

http://localhost:3000/

Se foram seguidos os passos acima, você estará visualizando a tela inicial do NTOP.

TELA INICIAL DO *NTOP*

O *Ntop* será iniciado através de qualquer browser, bastando colocar na barra de endereços do navegador HTTP://ip_do_servidor_Ntop:3000, conforme figura 42, e também poderá acessar via remoto desde que esteja configurado.

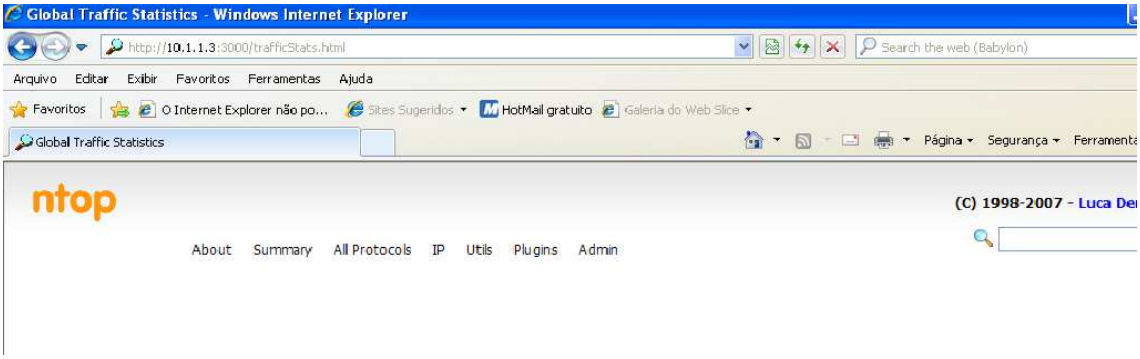


Figura.42 – Tela inicial do *Ntop*

Na tela inicial, podemos observar o menu do *Ntop*, com as seguintes opções:

About

- *What is ntop?*
- *Credits*
- *Make a Donation*
- *Ntop world*
- *Online documentation*
- *Show configuration*
- *Report a problem*

Summary

- *Traffic*
- *Hosts*
- *Network load*
- *Network flows*

All Protocols

- *Traffic*
- *Throughput*
- *Activity*

IP

- *Summary*
    - ✓ *Traffic*
    - ✓ *Multicast*
    - ✓ *Internet domain*
    - ✓ *Networks*
    - ✓ *ASs*
    - ✓ *Hosts clusters*
    - ✓ *Distribution*
- *Traffic directions*
    - ✓ *Local to local*
    - ✓ *Local to remote*
    - ✓ *Remote to local*
    - ✓ *Remote to remote*
- *Local*
    - ✓ *Ports used*
    - ✓ *Active TCP/UDP Sessions*
    - ✓ *Host fingerprint*
    - ✓ *Host characterization*
    - ✓ *Network traffic map*
    - ✓ *Local matrix*

Utils

- *Data dump*
- *View log*

Plugins

- *Host last seen*
    - ✓ *Activate*
    - ✓ *Describe*
- *ICMP watch*
    - ✓ *Activate*
    - ✓ *Describe*
- *Netflow*
    - ✓ *Activate*
    - ✓ *View/configure*
    - ✓ *Describe*
    - ✓ *statistics*
- *Pda*
    - ✓ *Activate*
    - ✓ *Describe*
- *Remote*
    - ✓ *Activate*
    - ✓ *View*
    - ✓ *Describe*
- *Round-Robin databases*
    - ✓ *Activate*
    - ✓ *Configure*
    - ✓ *Describe*
    - ✓ *Statistics*
    - ✓ *Arbitrary graphs*
- *sFlow*
    - ✓ *Activate*
    - ✓ *View/configure*
    - ✓ *Describe*
- *All*

Admin

- *Switch NIC*
- *Configure*
    - ✓ *Startup Options*
    - ✓ *Preferences*
    - ✓ *Packet filter*
    - ✓ *Reset stats*
    - ✓ *Web users*
    - ✓ *Protect URLs*
- *shutdown*

Através do menu acima, poderemos verificar “N” gráficos, de várias formas, ficando a critério do administrador da rede escolher qual gráfico e opção lhe atenderá de acordo com a necessidade.

6 REFERÊNCIAS

TANENBAUM, A. S. **Redes de computadores.** 10. ed. Rio de Janeiro: Elsevier, 2003.

TANENBAUM, A. S. **Redes de computadores.** 9. ed. Rio de Janeiro: Campus, 1997.

COSTA, F.. **Ambiente de redes monitorados com nagios e cacti.** Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

MORIMOTO, C. E. **Redes:** guia prático. 2. ed. Porto Alegre: Sul Editores, 2010.

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

SAUVÉ, J. P; LOPES, R.V; NICOLLETTI, P.S. **Melhores práticas para a gerência de redes de computadores.** 1. ed. Rio de Janeiro: Campus.

COMER, D. E. **Interligação de redes com TCP/IP.** Rio de Janeiro: 2006.

http://www.cedet.com.br/index.php?/O-que-e/Internet-e-Convergencia/rfc-request-for-comments.html - Autor: Dr. César Kyn d´Ávila. Acesso em 10 out. 2011.

http://imasters.com.br/artigo/6498/redes/monitorando_redes_utilizando_ntop/ - Autor: Guilherme Zanoni acesso em: 15 out. 2011.

http://info.abril.com.br/reviews/software/redes/na-rede-nada-escapa-do-ntop.shtml?2 – Autor: André Cardozo acesso em: 05 nov. 2011.

http://www.neteye.com.br/#produtos/index/1/descricao_produto. acesso em : 03 dez. 2011.

http://www.gta.ufrj.br/grad/10_1/snmp/mibs.htm acesso em 07 dez 2011.