FACULDADE DE TECNOLOGIA DE TERESINA - CET
GRADUADO EM REDES DE COMPUTADORES
MADSON DA SILVA SANTOS

PROJETO DE REDES
www.projetoderedes.com.br

ESTUDO DE GERENCIAMENTO DA REDE DE DISTRIBUÍÇÃO COM O PROTOCOLO SNMP E TUTORIAL PARA IMPLANTAÇÃO DE FERRAMENTAS DE GERÊNCIA

MADSON DA SILVA SANTOS

ESTUDO DE GERENCIAMENTO DA REDE DE DISTRIBUÍÇÃO COM O PROTOCOLO SNMP E TUTORIAL PARA IMPLANTAÇÃO DE FERRAMENTAS DE GERÊNCIA

Trabalho de pesquisa e implementação de um esquema de gerenciamento de redes para PoP-PI / RNP localizado na FAPEPI.

Orientador: Profº Mestre Carlos Giovanni Nunes Carvalho

Teresina - PI
2006

ÍNDICE

RESUMO

Atualmente nas empresas, o aumento do número e diversidade dos componentes das redes, vem tornando o gerenciamento de redes indispensável e parte integral da rede.

E para garantir a qualidade de serviço (*Quality of Service* – QoS) a seus usuários, redes de computadores devem ser gerenciadas.

Assim a implantação de um sistema de gerenciamento é de extrema importância para poder detectar e prever falhas, monitorar o desempenho, planejar futuras expansões, evitando dessa forma o baixo desempenho da rede; travamento de equipamentos; a queda nos serviços de rede (serviços de e-mail, dns, dhcp, etc). Além de garantir o pleno funcionamento de equipamentos gerenciáveis (roteadores, switchs) que vão ser essenciais para que a rede possa funcionar, atendendo às necessidades dos usuários em geral.

No Ponto de Presença da Rede Nacional de Ensino e Pesquisa no Piauí (PoP-PI/RNP), que disponibiliza uma estrutura de acesso à Internet para instituições de ensino e pesquisa do estado, além de órgãos públicos e privados, é onde foi implementada as ferramentas de gerência: What´s Up, MRTG, Nagios, Cacti, Ntop.

Portanto, esse tutorial, elaborado no corrente ano de 2006 para o PoP-PI, irá descrever brevemente os principais conceitos e terminologias de gerenciamento de redes, bem como as ferramentas que foram utilizadas, detalhando suas principais funcionalidades e também um guia de instalação e configuração das ferramentas citadas.

Palavras-chave: SNMP, Gerência de Redes, Softwares de Gerenciamento.

1. INTRODUÇÃO

Por volta de 1960 os americanos criaram a ARPANET, rede de computadores destinada ao tráfego de dados confidenciais militares e também para troca de informações entre pesquisadores. Desde então esta rede cresceu muito rapidamente, passando a conectar milhares de computadores. Surge então um problema: a interoperabilidade, onde diferentes *hosts* de diferentes fabricantes deveriam ser conectados, precisando de sistemas de suporte à troca de arquivos, interação entre os terminais e hosts.

De modo a resolver o problema da interoperabilidade, foi desenvolvido um conjunto de protocolos padronizados, que deram origem aos protocolos da pilha TCP/IP.

Durante o desenvolvimento do TCP/IP pouco se estava pensando em relação à gerência da rede. Nesta época não foi desenvolvida nenhuma ferramenta, nem um protocolo em especial para o gerenciamento da rede. O protocolo *Internet Control Message Protocol* (ICMP) era a única "ferramenta" simples que era efetivamente utilizada no início da Internet para a gerência da rede, pois estava disponível em qualquer equipamento com suporte IP.

O ICMP funciona com um mecanismo echo/echo-reply. Quando uma mensagem do tipo *echo* é recebida, a entidade é obrigada a retornar o conteúdo da mensagem como uma mensagem do tipo *echo-reply.* Outro par de mensagens útil é a *time-stamp/time-stamp-reply*, o qual fornece um mecanismo para verificar as características de atraso na rede.

Um exemplo disso é o famoso PING (Packet Internet Groper). Com ele é possível determinar se um equipamento de rede pode ser alcançado, verificar se uma rede pode ser alcançada e verificar as operações entre um servidor e um *host*. O PING pode ser utilizado para verificar a taxa de perda de pacotes em uma sub-rede, podendo ajudar no isolamento de áreas de congestionamento e pontos de falha.

Com o crescente aumento da utilização das redes, foi necessário que se desenvolvesse um protocolo padronizado com mais funcionalidades que o PING. Surge então o protocolo SNMP.

SNMP é um protocolo não orientado à conexão, ganho de velocidade; é um protocolo da camada de aplicação designado para facilitar a troca de informações de gerenciamento entre dispositivos de rede; além de ser o mais popular protocolo para gerenciamento de redes.

Com isso a gerência de redes foi impulsionada, surgindo ferramentas e dispositivos gerenciáveis para disponibilizar e auxiliar o administrador a verificar, isolar e corrigir possíveis falhas que venham a comprometer a operacionalidade da rede.

No Brasil, a Internet só teve início em 1991 com a RNP (Rede Nacional de Pesquisa), que é o "backbone" principal e envolve instituições e centros de pesquisa (FAPEPI, FAPESP, FAPERJ, FAPEMIG, etc.), universidades, laboratórios, etc. Contuto, nesta época, já se tinham os protocolos e algumas ferramentas eficazes para gerenciar as redes de computadores.

2. Objetivos

O objetivo principal desse trabalho é desenvolver uma estratégia de gerenciamento da rede local do POP-PI utilizando-se do funcionamento paralelo dos softwares, W*hat's Up Gold, MRTG, Nagios, Cacti e NTOP*. A criação de um mapa da rede local e de um esquema para monitoração dos links e equipamentos desta rede.

A meta é garantir a proatividade do sistema de redes, antecipando os problemas antes que aconteçam, tendo um diagnóstico mais preciso, de modo a automatizar as tarefas de administração da rede da FAPEPI/POP-PI, tornando a resolução de problemas mais rápida, conseqüentemente, com menor tempo e ocorrência de interrupções.

E que através deste tutorial, unidades de ensino superior, administradores de redes e outros que se interessem pela gerência de redes tenham um guia de implementação.

3. METODOLOGIA

O Projeto foi dividido na seguinte seqüência de etapas:

ETAPA 1 – PESQUISA DOS TEMAS A SEREM ABORDADOS

Foi realizada uma coleta de dados e ferramentas, através de pesquisa em livros, revistas e na internet.

ETAPA 2 - ESTUDO DA ESTRUTURA E DO FUNCIONAMENTO DA REDE DO POP-PI

Realizou-se uma pesquisa junto com os técnicos.

ETAPA 3 – CONFIGURAÇÃO DO SOFTWARE

Implantação e Configuração dos softwares de gerenciamento adotados.

ETAPA 5 – RELATÓRIO FINAL E TUTORIAL

Apresentar o relatório final constando todo o trabalho desenvolvido e o tutorial.

4. O Potocolo SNMP

4.1. Definição

O Simple Network Management Protocol ou Protocolo Simples de Gerenciamento de Rede é um protocolo padrão da Internet para gerenciar dispositivos de redes, desenvolvido pela IETF. Tem o objetivo de controlar, coletar e transferir informações dos equipamentos e serviços gerenciados na rede. Definido na camada de aplicação utiliza o UDP para enviar mensagens na rede. Trabalha com a arquitetura cliente-servidor e tem como premissa à flexibilidade e a facilidade de implementação.

4.2. Funcionamento

O modelo SNMP é baseado na arquitetura Cliente – Servidor. Onde o "Cliente" ou Estação Gerente é que requisita as informações de gerenciamento utilizando os serviços do protocolo de transporte UDP (User Datagram Protocol) e o "Servidor" ou Estação Agente é quem fornece os parâmetros de gerenciamento contidos na sua Base de Informações de Gerenciamento (MIB).

Em uma rede gerenciada, ou seja, quando existe um sistema de agentes e gerentes, há uma contínua troca de informações entre eles, informando sua atual situação (up ou down, por exemplo). O processo em que o gerente requisita o "status" do Agente é conhecido como um "*poll*". E quando o próprio Agente, mesmo sem requisição do Gerente, informa sua situação, ocorre um " *Trap* ". É importante lembrar que existem outras operações SNMP como: SET, GET, GET-NEXT. A "*figura 1*" representa as operações entre gerente e agente

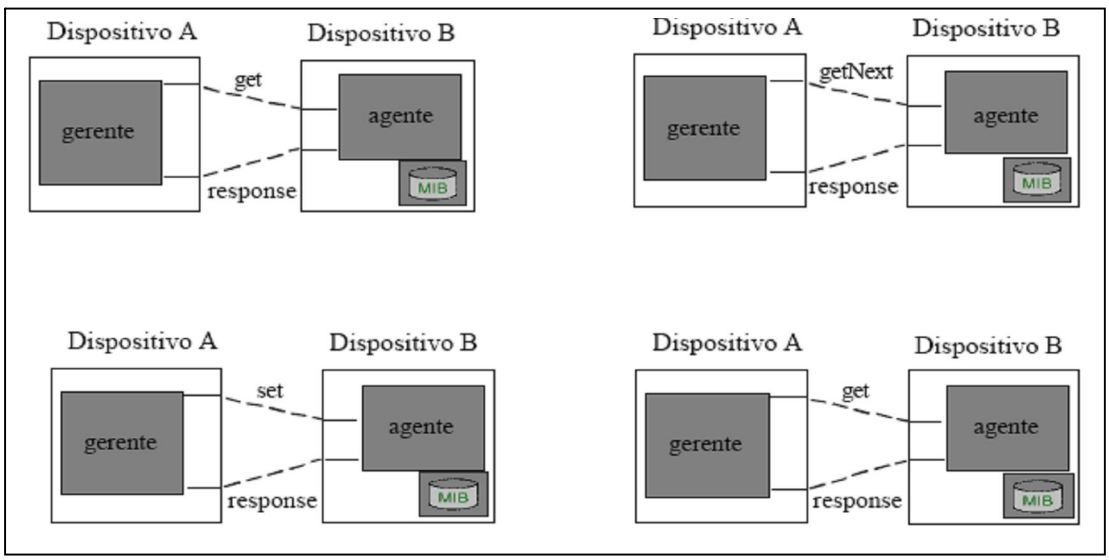

Figura 1: *operações entre gerente e agentes*

Esta troca de informações é possível porque em cada Agente reside a Base de Informações de Gerenciamento (MIB). É lá onde estão valores que informam o status e diversas características do dispositivo gerenciado. Então o Agente utiliza-se da MIB para manipular (obter/alterar) informações do dispositivo atendendo ao Gerente. No gerente, é onde vai conter as configurações do software de gerenciamento, para enviar ao Agente (MIB) as alterações adequadas para cada tipo de situação,

configuradas pelo administrador da rede. A "*figura 2*" ilustra como funciona o relacionamento de um gerente com o objeto

O SNMP utiliza ainda o conceito de comunidades (community) estabelecendo uma confiabilidade entre gerentes e agentes, para assim, dependendo da situação, o poder de ler e/ou alterar as informações da MIB no agente. Muitos equipamentos por default utilizam comunidade como sendo pública, portanto é interessante mudar essa comunidade para que pessoas não autorizadas possam obter informações sobre aquele equipamento ou até mesmo da rede.

Por tanto, o SNMP é o nome do protocolo na qual as informações são trocadas entre a MIB e a aplicação de gerência.

Figura 2: *relacionamento entre a MIB e a aplicação de gerência*

5. O Gerenciamento de Redes de Computadores

5.1. Definição

Gerenciar uma rede de computadores consiste em avaliar constantemente se os equipamentos estão em pleno funcionamento. Desta forma pode-se acompanhar o que está acontecendo nas maquinas da rede (estações de trabalho, servidores, switchs, roteadores,...) e saber quando e porque alguma delas deixa de funcionar.

O objetivo maior do gerenciamento de redes é garantir que os usuários tenham acesso aos serviços de que necessitam e com a qualidade esperada. Além de garantir sua disponibilidade, reduzir os custos operacionais, aumentar a flexibilidade de operação e integração das redes, permitir facilidades de uso e garantir características de segurança.

Portanto, o gerenciamento consiste no monitoramento de uma rede de comunicações, a fim de diagnosticar problemas e coletar dados estatísticos. As atividades básicas do gerenciamento de redes consistem na detecção e correção de falhas, em um tempo mínimo, e em estabelecer procedimentos para a previsão de problemas futuros.

A complexidade do gerenciamento de rede é diretamente proporcional ao tamanho da rede gerenciada.

5.2. Importância

Como as redes estão em constante crescimento é de fundamental importância que elas sejam gerenciadas para garantir, aos seus usuários, a disponibilidade dos serviços a um nível de desempenho aceitável e manter operante os equipamentos.

O gerenciamento pode ser justificado pelos seguintes fatores:

- As redes e recursos de computação distribuídos estão se tornando vitais para a maioria das organizações. Sem um controle efetivo, os recursos não proporcionam o retorno que a corporação requer.
- O contínuo crescimento da rede em termos de componentes, usuários, interfaces, protocolos e fornecedores ameaçam o gerenciamento com perda de controle sobre o que está conectado na rede e como os recursos estão sendo utilizados.
- Os usuários esperam uma melhoria dos serviços oferecidos (ou no mínimo, a mesma qualidade), quando novos recursos são adicionados ou quando são distribuídos.
- Os recursos computacionais e as informações da organização geram vários grupos de aplicações de usuários com diferentes necessidades de suporte nas áreas de desempenho, disponibilidade e segurança. O gerente da rede deve atribuir e controlar recursos para balancear estas várias necessidades.
- À medida que um recurso fica mais importante para a organização, maior fica a sua necessidade de disponibilidade. O sistema de gerenciamento deve garantir esta disponibilidade.
- A utilização dos recursos deve ser monitorada e controlada para garantir que as necessidades dos usuários sejam satisfeitas a um custo razoável.

Foi criada ainda uma divisão funcional para descrever as necessidades de gerenciamento: Falhas, Desempenho, Configuração, Contabilização e Segurança.

5.3. Tipos de Gerenciamento

5.3.1. Gerenciamento de Falhas

Para se entender melhor o que seja o gerenciamento de falhas é preciso distinguir falha e erro. Uma falha é uma condição anormal que requer uma ação para correção, por exemplo, se uma linha de comunicação é cortada fisicamente, nenhum sinal pode passar através dela. Enquanto que o erro é um evento simples, como um grampeamento no cabo pode causar distorções que induzem à uma alta taxa de erros

Para que a rede, em caso de falha, fique operante o mais rápido possível é interessante seguir os seguintes passos no processo de gerenciamento de falhas: depois de detectada a falha, isolar a falha, restaurar o serviço, e só então se pode identificar as causas do problema e por fim resolver o problema.

5.3.2. Gerenciamento de Desempenho

O gerenciamento do desempenho de uma rede é a monitoração das atividades da rede e o controle dos recursos através de ajustes e trocas. Algumas das questões relativas ao gerenciamento do desempenho são:

- Qual é o nível de capacidade de utilização?
- O tráfego é excessivo?
- O throughput foi reduzido para níveis aceitáveis?
- Existem gargalos?
- O tempo de resposta está aumentando?

5.3.3. Gerenciamento de Configuração

O gerenciamento de configuração está relacionado com as tarefas de manutenção, adição e atualização dos componentes e do estado dos componentes durante a operação da rede.

O gerenciamento de configuração engloba a topologia da rede, mapeamento da rede, inclui ainda o planejamento e projeto da rede.

Em nível de serviços, se devem ter disponíveis os parâmetros: tempo de resposta; taxa de rejeição e disponibilidade.

5.3.4. Gerenciamento de Contabilização

O gerenciamento de contabilização permite ao administrador determinar se um usuário ou grupo de usuários estão abusando de seus privilégios de acesso, se usuários estão usando a rede de forma ineficiente, consumindo banda da rede.

5.3.5. Gerenciamento de Segurança

O gerenciamento de segurança é permitir que políticas de segurança sejam tomadas para garantir a monitoração e o controle de acesso à rede ou parte da rede e às informações; coleta, armazenamento e análise de registros de logs de segurança.

6. O Ambiente de Gerenciamento Escolhido: PoP-PI / RNP

O PoP-PI é o ponto de presença da Rede Nacional de Ensino e Pesquisa (RNP) no Piauí, está localizada na FAPEPI (Centro Administrativo, Bloco "G", Térreo), e tem a finalidade de oferecer uma infra-estrutura para compartilhamento de um canal de conexão , além de acesso à internet às instituições de ensino e pesquisa, órgãos do governo como também entidades privadas.

Em 1996 a Fundação de Amparo à Pesquisa do Estado do Piauí (FAPEPI) criou a Rede Piauiense de Pesquisa (RPP). As informações que trafegavam da RPP atingiram âmbito nacional e internacional através do link com backbone RNP2. Nesta época o PoP-PI operava com uma tímida velocidade de 64 Kbps e estava interligado ao backbone da RNP pelo ponto de presença no Ceará (PoP-CE).

Em seguia a velocidade aumentou para 6Mbps, o link ganhou tecnologia ATM e agora estava conectado ao ponto de presença de Minas Gerais (PoP-MG) e ,via RNP, às redes acadêmicas de outros países.

Hoje o backbone do PoP-PI opera a uma velocidade de 34 Mbps e passou a estar conectado ao PoP-RJ. Atualmente este link opera com um consumo médio de 30%.

A estrutura organizacional se dispõe da existência de bolsistas que desenvolvem um projeto de pesquisa e implementação seguindo uma linha de pesquisa adotada. Nesse momento duas linhas estão em andamento: Gerência de Redes de Computadores a que se destina esse projeto e VoIP. Existem também os técnicos de operação e manutenção do PoP, que garantem a operacionalidade adequada de toda estrutura física (hardware) e lógica (software). E ainda a presença de um coordenador.

Partindo para estrutura física, tem-se uma sala de telecomunicações onde estão dispostos todos os equipamentos de rede. Esta sala é de acesso restrito, garantindo a integridade dos dispositivos presentes. E um laboratório onde estão os computadores para os usuários do PoP.

A rede do ponto de presença da RNP no Piauí, tem hoje 5 (cinco) roteadores que interligam várias instituições e ao backbone da RNP (PoP-RJ), 4 (quatro) Switchs que viabilizam a troca de informações com maior agilidade; 6 (seis) servidores sendo eles: Web, E-mail, Firewall, DHCP, DNS (primário e secundário), Proxy, servidor de gerência e servidor de testes, todos rodando em plataforma Unix e Linux. Temos também um nobreak de 10 Kva mais um módulo de baterias que garantem o funcionamento por um período maior dos equipamentos na falta de energia.

O PoP-PI recebe um link de 34 Mbps do backbone da RNP que chega ao roteador de borda, deste roteador segue para um switch Giga e posteriormente vai para os outros roteadores que fazem conexão com os setores públicos e privados do estado. Existem setores públicos que usufruem diretamente dos servidores do PoP, chegando diretamente aos Switchs.

Contudo o POP – PI interliga as seguintes instituições: Centro Federal de Educação Tecnológica do Piauí (CEFET), Sociedade Piauiense de Combate ao Câncer - Hospital São Marcos, Universidade Estadual do Piauí (UESPI), Universidade Federal do Piauí (UFPI), Secretaria de Ciência e Tecnologia (SECTEC), Secretaria de Educação (SEDUC), Tribunal de Contas do Estado (TCE), Secretaria de Fazenda (SEFAZ), Empresa Brasileira de Pesquisa Agropecuária (EMBRAPA) que são algumas instituições que usufruem do PoP-PI.

Portanto cabe ao PoP-PI garantir o pleno funcionamento do acesso à rede mundial de computadores, e para isso foram implementada as ferramentas de gerência: What´s Up Gold, Nagios, MRTG, Ntop, Cacti.

7. Os Softwares de Gerenciamento

As ferramentas de gerencia são essenciais para as atividades de gerência. São elas que vão ajudar a detectar problemas quando eles ocorrerem, ou antes, mesmo de ocorrerem (gerência de rede pro ativa). Gerenciar uma rede sem o auxílio das ferramentas de gerência é uma tarefa bastante árdua e que muito provavelmente não oferecerá uma boa qualidade de gerência.

Tendo conhecimento de toda a estrutura de gerenciamento, desde o surgimento do protocolo até o ambiente de implementação, é hora de detalhar cada ferramenta de gerência adotada para o PoP-PI.

Com uma infinidade de ferramentas de gerenciamento, foram adotados alguns softwares de gerenciamento, algum proprietário e outros livres, portanto irei detalhar com mais ênfase aqueles que são considerados essenciais para PoP neste momento.

What´s Up, MRTG, NAGIOS, CACTI e **NTOP** serão os principais focos deste trabalho e consequentemente serão bem detalhadas.

Mãos a obra!

7.1. WHAT´S UP

7.1.1. Definição:

O Whats Up é um software de gerenciamento de rede proprietário, desenvolvido pela ipswitch, que roda em plataforma Windows. Esta ferramenta permite criar um mapa de uma rede de computadores, monitorar os equipamentos e serviços desta rede, emitir notificações aos administradores quando algum equipamento ou serviço deixar de funcionar, emitir relatórios estatísticos sobre o funcionamento da rede, monitoramento via web. Através de sua interface, o acompanhamento do estado da rede fica simplificado, podendo-se verificar visualmente quando equipamentos ou serviços deixam de funcionar.

Uma abordagem interessante é que o Whats Up é compatível com o protocolo de gerenciamento SNMP.

É também interessante mencionar que um dos softwares de gerenciamento de rede utilizado no PoP-PI da RNP foi o Whats Up Gold 8.0, porque a instituição já possuía a licença do sistema no momento em que o trabalho começava a ser realizado.

7.1.2. Características:

- **Mapeamento da Rede:** Faz mapeamento da rede através de uma faixa especifica de IP ou a partir de um roteador;
- **Monitoração Rede:** usa os protocolos padrão (TCP/IP, SNMP, NetBIOS, e IPX) para monitorar sua rede. O What´s Up verifica continuamente os dispositivos e serviços;
- **Notificações:** pode enviar diversos tipos de notificações para os administradores quando o estado da rede muda. Podem ser do tipo sonora, e-mail, sms, reinicializar um serviço
- **Arquivos de log:** Com estes logs o Whats Up irá gerar os gráficos e relatórios de disponibilidade dos equipamentos da rede. Obter informações sobre o tempo em que a rede respondeu com menos ou mais tempo; e saber quando a rede e os equipamentos estão sobrecarregados ou não.
- **Relatórios e gráficos:** Mostra as mudanças de estado que ocorreram com os equipamentos e serviços da rede num determinado tempo; mostra o tempo de resposta da rede nas verificações, além de mostrar a porcentagem de pacotes de verificações que não tiveram respostas; fornece diversos gráficos informando a disponibilidade dos equipamentos; tempo de resposta da rede e de cada máquina individualmente.
- **Interface Web:** O Whats Up fornece também o monitoramento remoto da rede através de uma interface web. O próprio programa possui um web server que pode ser configurado pelo usuário. Escolha dos mapas disponíveis para a web, permissões dos usuários, porta de acesso ao web server do Whats Up, são exemplos de configurações do servidor web. Dependendo das permissões dos usuários, estes poderão ter acesso a todas as funcionalidades do software de gerenciamento que se fazem também disponíveis na interface web, acesso aos logs do sistema, verificação do estado de cada dispositivo da rede, estado dos serviços da rede

7.1.3. Funcionamento

Inicialmente, deve-se fazer o mapeamento da rede que o Whats Up deverá gerenciar. Este mapeamento pode ser feito das seguintes maneiras:

- Captura de informações SNMP a partir de um roteador: Este foi o método escolhido. Neste caso o usuário deverá fornecer ao Whats Up o Ip do roteador em que a busca será iniciada, a community utilizada no agente SNMP do roteador. Deste modo a partir do roteador o software irá coletar informações sobre os demais equipamentos que fazem parte da rede. A busca foi limitada à classe Ip do roteador inicial, evitando que informações sobre outras redes fossem mapeadas. Após algum tempo o software cria um mapa da rede com os equipamentos que fazem parte da mesma, identificando quais deles possuem serviços de rede e também agentes SNMP;
- Busca de equipamentos através de mensagens ICMP: Este método utiliza o protocolo ICMP para obter informações dos equipamentos que fazem parte da rede;
- Busca de equipamentos que fazem parte da rede do Windows: Caso a estação, onde o Whats Up está rodando, faça parte de uma rede Windows, o programa irá obter as informações para mapeamento a partir do domínio no qual a estação pertence;
- Leitura de registros do Windows para encontrar equipamentos que são referenciados por aplicações que utilizam a rede: Este método faz uma busca na própria máquina local para encontrar nos registros do Windows outros programas que utilizam a rede;
- Lê um arquivo texto contendo IP + Nome do host: Este método é mais utilizado quando se deseja mapear apenas determinados equipamentos;
- Criação manual do mapa: O Whats Up permite que o próprio usuário crie seus mapas de rede, adicionando diversos equipamentos que façam parte da rede, devendo configurar manualmente também os atributos de cada equipamento, tais como: ip, nome, serviços, etc.

Com o mapeamento feito o software já dá início ao gerenciamento. Este é feito através de mensagens ICMP enviadas a todos os equipamentos que fazem parte do mapeamento e através de mensagens SNMP aos equipamentos que possuem um agente rodando. O poll (verificação dos equipamentos que estão ativos) possui um intervalo de tempo configurável pelo usuário. Em cada poll o Whats Up confirma e qualifica as máquinas e serviços que estão ativos na rede. Os métodos de polling podem ser, além do ICMP, através dos protocolos IPX, NetBIOS para redes Windows e Novell NetWare respectivamente; ou pode ser por serviço no caso de firewalls que não aceitam mensagens ICMP, neste último método o Whats Up verifica apenas se os serviços do equipamento estão funcionando.

As alterações do estado dos equipamentos da rede são armazenadas em arquivos de logs. Esses arquivos serão a base para a geração de relatórios estatísticos.

7.1.4. Instalação e Configuração

Para instalação do What´s Up, é preciso preencher os requisitos de configuração mínima de hardware para que o software rode sem problemas. São eles:

- Intel Pentium ou eqivalente

- 30 MB de espaço em disco (100 MB recomendado)
- 64 MB de RAM (256 MB recomendado)
- Windows NT 4.0, Windows 2000 , Windows 98, Windows ME, ou Windows XP

Depois de inserido o cdrom do What´s Up no drive, inicia-se automaticamente o assistente de instalação. Se o assistente não inicializar, vá em Iniciar->Executar e digite por exemplo : d:AutoRun.exe , dependendo da sua unidade de cdrom.

Figura 3: *Assistente de instalação do Whta´s Up*

O primeiro passo na implantação do projeto de gerenciamento da rede do PoP-PI foi a criação dos mapas que compõem a rede a partir do roteador que faz a ligação das instituições de ensino e pesquisa do Piauí. A partir deste roteador foi possível identificar os demais dispositivos que fazem parte da rede, como servidores e outros roteadores.

Este foi o método escolhido. Neste caso o usuário deverá fornecer ao What´s Up o Ip do roteador em que a busca será iniciada, a community utilizada no agente SNMP do roteador. Deste modo a partir do roteador o software irá coletar informações sobre os demais equipamentos que fazem parte da rede. A busca foi limitada à classe Ip do roteador inicial, evitando que informações sobre outras redes fossem mapeadas. Após algum tempo o software cria um mapa da rede com os equipamentos que fazem parte da mesma, identificando quais deles possuem serviços de rede e também agentes SNMP;

Para montar mapa da rede utilizando o SmartScan vá no menu **File** , selecione **New Map** Wizard, depois clique em **Discover and map network devices**, em seguida em **Next.** Abrirá janelas onde se deve especificar o Ip do roteador, assim como sua comunidade e os serviços a serem monitorados em cada equipamento a ser descoberto.

Serão exibidas as seguintes janelas respectivamente:

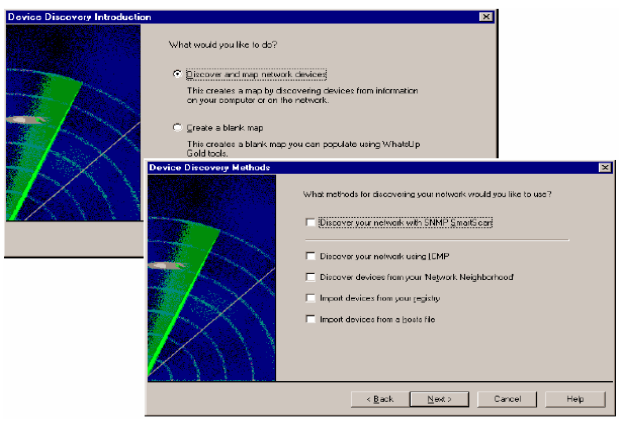

Figura 4: *Método de criação do mapa da rede*

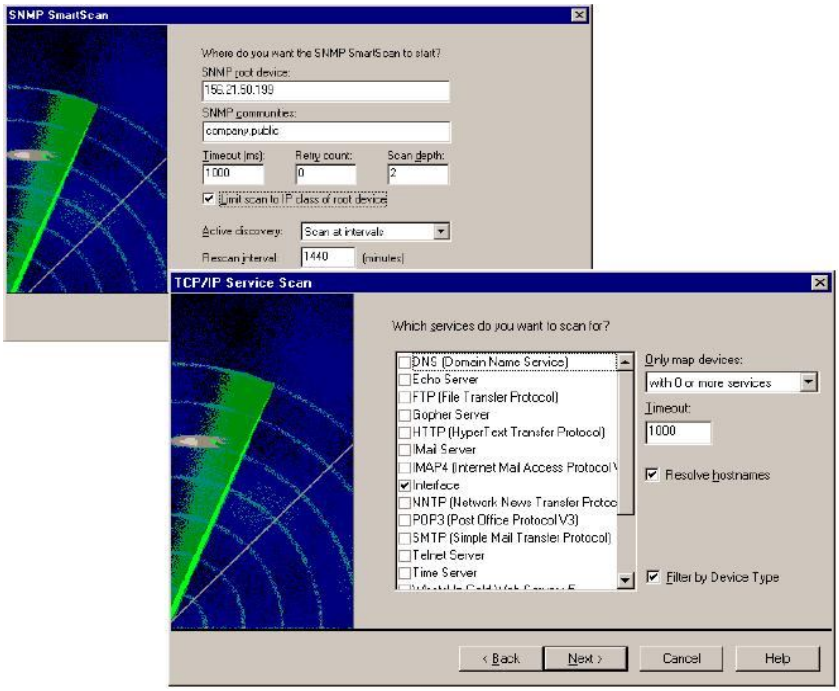

Figura 5: *Parâmetros de configuração do SmartScan para montar mapa*

Criado o mapa inicia-se neste momento a monitoração de equipamentos e seus respectivos serviços. Porém pode-se querer editar o mapa gerado, seja por que o sistema não descobriu de modo consistente todos os serviços sendo executados, exigindo uma redescoberta de serviços individuais dentro de alguns dispositivos, ou por uma adição e/ou remoção de algum dispositivo.

Depois de escolhido os dispositivos e serviços, foi feita uma classificação na interface do mapa gerado. Essa classificação separa roteadores de servidores, para facilitar a análise do estado dos equipamentos.

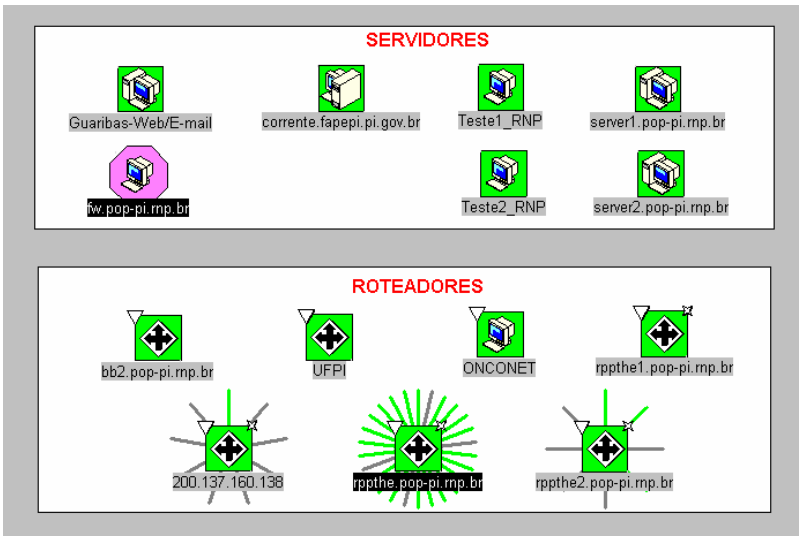

Figura 6: *Mapa da rede do PoP-PI*

O passo seguinte foi definir um projeto de monitoramento que pudesse fornecer aos administradores do PoP-PI informações sobre a alteração do estado dos equipamentos e dos serviços da rede. Pensou-se então numa maneira de deixar as informações, sobre a rede, sempre acessíveis aos técnicos que fazem o

gerenciamento e informá-los quando o estado de equipamentos ou serviços forem alterados.

7.1.4.1. Configuração de Servidor web

O Whats Up fornece o monitoramento remoto da rede através de uma interface web. O próprio programa possui um web server que pode ser configurado pelo usuário. Escolha dos mapas disponíveis para a web, permissões dos usuários, porta de acesso ao web server do Whats Up, são exemplos de configurações do servidor web integrado ao software.

Dependendo das permissões dos usuários, estes poderão ter acesso a todas as funcionalidades do software de gerenciamento que se fazem também disponíveis na interface web, acesso aos logs do sistema, verificação do estado de cada dispositivo da rede, estado dos serviços da rede,...

Configurou-se o servidor web para que os dados referentes ao monitoramento da rede pudessem ser acessíveis pelos administradores a qualquer momento independente de localização. O próprio Whats Up possui um módulo de configuração para disponibilizar este serviço. Neste módulo pode-se habilitar o serviço bem como configurações gerais, de segurança e de usuários.

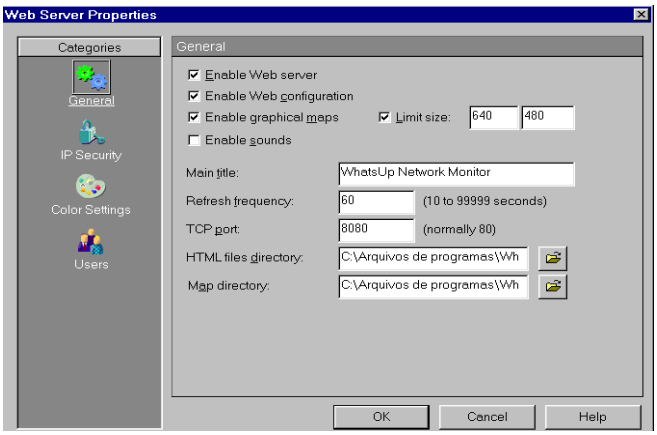

Figura 7: *Configuração geral Web Server What´s Up*

Na opção de segurança pode-se definir os Ips ou conjunto de Ips que não devem ter acesso ao servidor web e assim restringir o acesso às informações da rede.

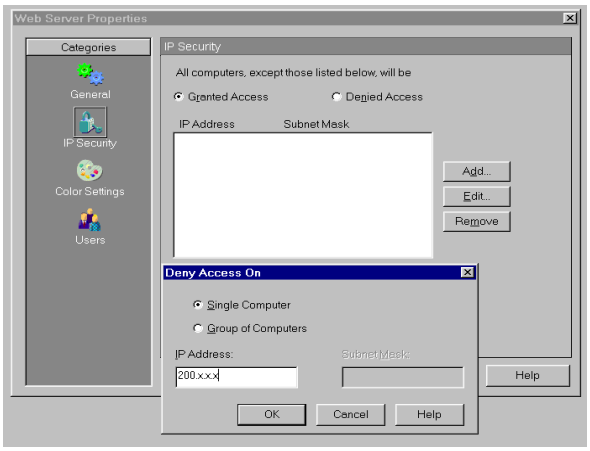

Figura 8: *Definição de restrição de Ips para acessar os dados da rede via web*

Nas configurações de usuário pode-se adicionar e remover usuários bem como alterar as permissões que cada usuário possui no momento que estiver acessando as

informações da rede pelo servidor web. Para cada usuário é possível adicionar os mapas que poderão ser analisados.

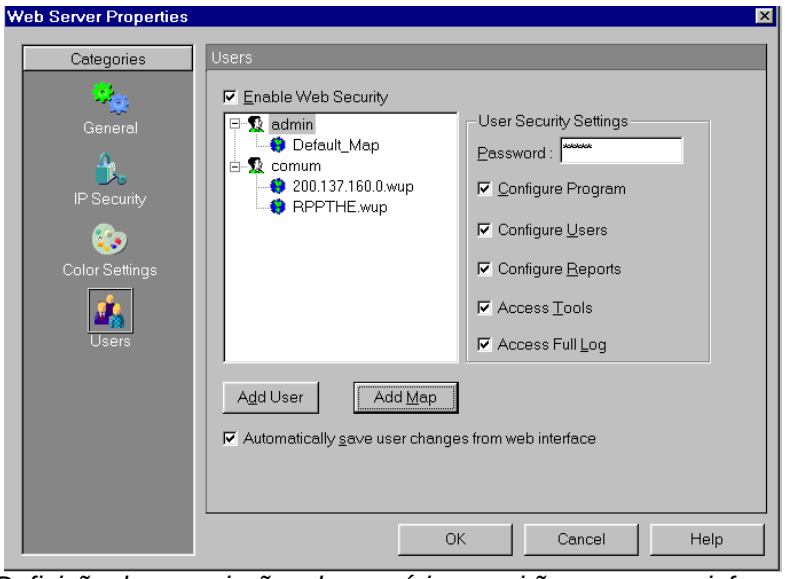

Figura 9: *Definição das permissões dos usuários que irão acessar as informações via web*

7.1.4.2. Configuração de Notificações

Ficamos limitados a configurar apenas algumas notificações no Whats Up, tais como envio de SMS, Pager, Beeper e outros, pois esses serviços requerem requisitos que são a restrições de regiões e limitações de hardwares.

Então configuramos alguns serviços que consideramos importantes e que satisfazem nossas exigências. São eles:

- Notificação de envio de mensagens de e-mail;
- Notificação de envio de mensagem sonora e;
- Notificações de WinPopup.

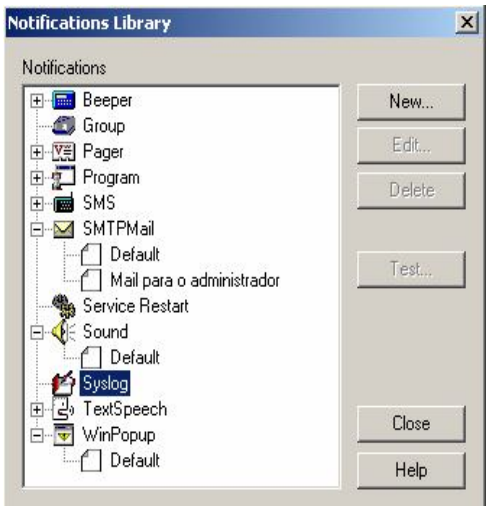

Figura 10: *Menu principal de configuração de notificações*

Para definir notificações de E-mail você deve dá entrada com o “Display Name” para identificar a notificação do e-mail. Vai incorpore o endereço ip do servidor de E-mail. Incorpore também um ou mais endereço do E-mail de usuários do smtp. Separe cada endereço com uma vírgula. Na caixa de mensagem, vai ser preenchido com

uma mensagem do texto mais algumas das variáveis de notificação do próprio Whtas Up.

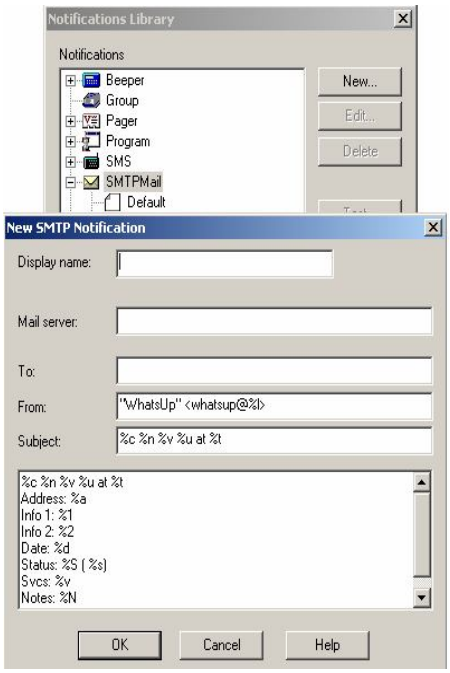

Figura 11: *Caixa de adição de notificação por mensagem de e-mail*

Para definir uma notificação sonora vá ao menu da configuração, selecione a notificação Sound, então clique em adicionar novo ou use o Default. você deve dá entrada com o “Display Name” para identificar a notificação sonora. Escolha o tipo sonoro para cada tipo de serviço, ou seja, pode-se ter diferentes tipos de emissão de som quando um serviço cai ou não(Service Up/Service Down).

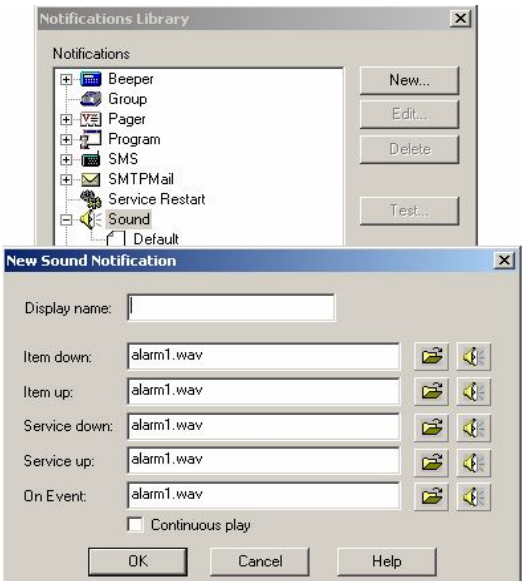

Figura 12: *Caixa de adição de notificação sonora*

Definindo uma notificação de WinPopup significar dizer que uma mensagem na janela de WinPopup aparecerá no Windows. Você define uma notificação para cada anfitrião de Windows em que você quer indicar a mensagem.

Para definir uma notificação de WinPopup: no menu da configuração de notificações selecione o WinPopup. Clique em novo e dá entrada com um nome

original da exposição para a notificação ou use o Default. Na caixa de lista do destino, especifique o anfitrião de Windows ou o domínio que você quer receber esta notificação. Na caixa de texto da mensagem, incorpore uma mensagem do texto mais algumas das variáveis da notificação existente no próprio Whats Up.

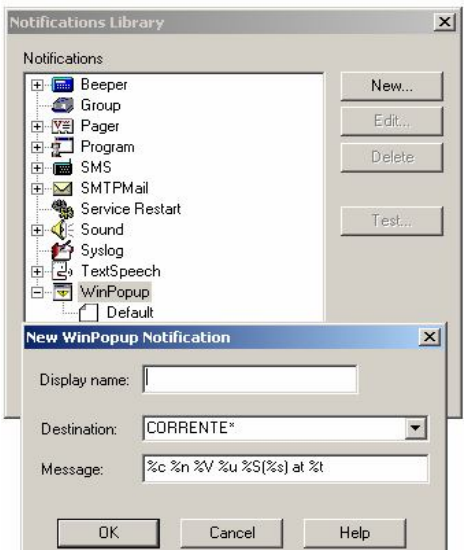

Figura 13: *Caixa de adição de notificação WinPopup*

7.1.4.3. Configuração Gerais

Nas propriedades gerais do Whtas Up foram feitas as seguintes configurações: foi permita a votação de status para todos os mapas; permita a descoberta ativa para todos os mapas; permita entrega de eventos para todos os mapas; permita notificações alertas para todos os mapas; carregar automaticamente sub-redes ao abrir mapas(whats up).

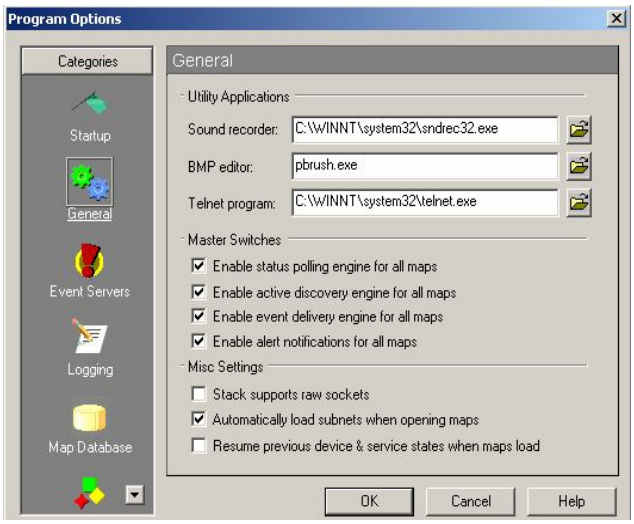

Figura 14: *Tela de configuração das propriedades gerais do Whats up*

Nas configurações de Registro: configurou-se os arquivos de registro para registrarem arquivos de log a cada 30 dias (quatro semanas), que corresponde a um mês, e esses mesmos arquivos de log serão apagados a cada 90 dias. Podemos assim fazer um levantamento de como a rede tem se comportado a cada trimestre.

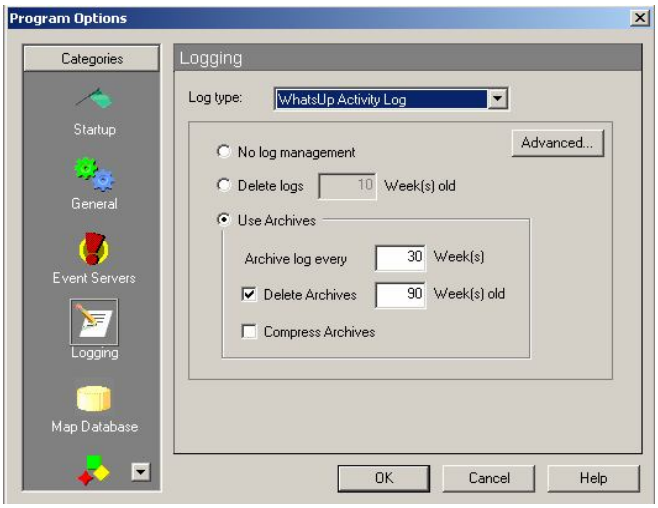

Figura 15: *Tela de configuração das propriedades de registro do Whats up*

7.1.4.4. Configuração dos Dispositivos

Na configuração de dispositivo pode-se identificar o tipo (servidor, roteador, etc), pode-se escolher o método de votação (ip ou do nome), identificar o nome do host; o endereço ip.

Propriedades de monitoração: iremos especificar a freqüência de como as votações irão ocorrer para verificar o dispositivo; o tempo de votação em segundos para esperar uma resposta de um dispositivo monitorado, ou seja, a cada 5 segundos verifica-se o status do dispositivo; os dispositivos irão está sendo monitorados 7 dias por semana, sendo 24h por dia; e dependências;

A monitorização de serviços dos dispositivos foi utilizada a auto descoberta, assim todos os serviços descobertos estão sendo monitorados (http, dns, ftp).

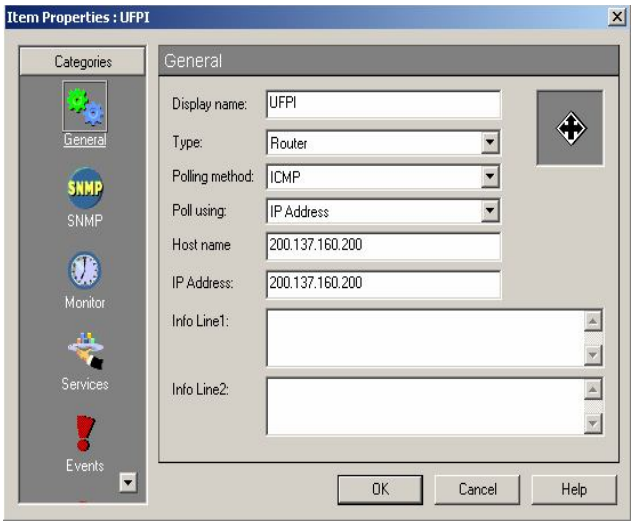

Figura 16: *Propriedades Gerais do dispositivo*

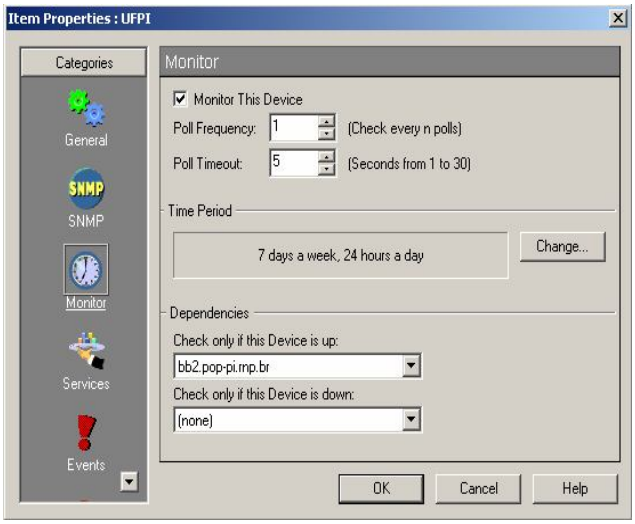

Figura 17: *Propriedades de monitoração dispositivo*

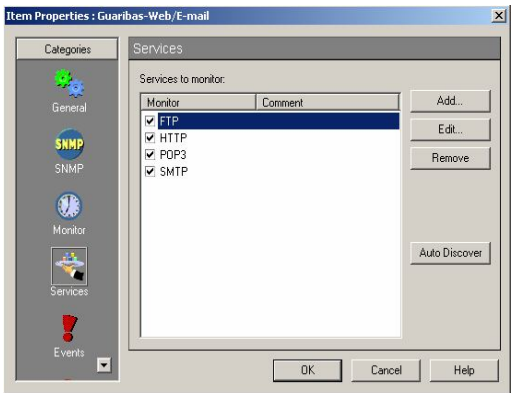

Figura 18: *Serviços monitorados*

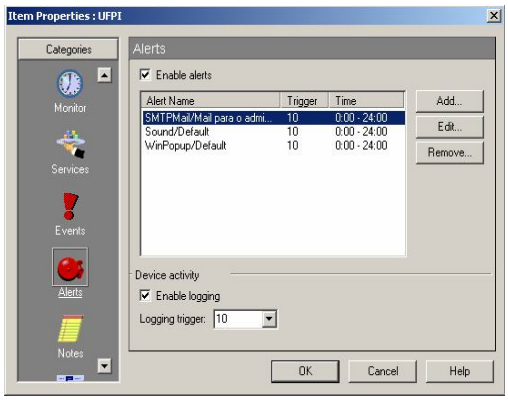

Figura 19: *Alertas de notificação*

Com o Status rápido (Quick Status) tem-se acesso para indicar informações de status do dispositivo associado.

Na aba **Status**: indica o Status atual do dispositivo, se o dispositivo está acima ou pra baixo;

Contagem (count): indica Número total de votações deste dispositivo;

RTT: indica o tempo em milisegundos do tempo que o último pacote emitido levou para chegar no dispositivo e para retornar;

ICMP Status: indica a contagem de quantas votações respondeu;

Total. total de quantas votações ocorreram em que o dispositivo ou o serviço não responderam desde que o contador foi cancelado pela última vez.

Última Vez De Resposta**:** hora da última resposta;

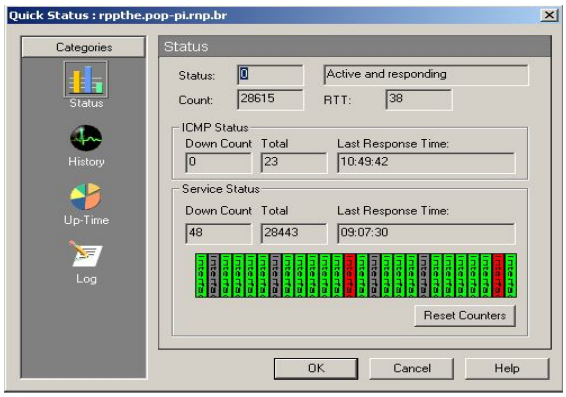

Figura 20: *Quick Status: Status atual do dispositivo*

Na aba **Histórico** indica um gráfico com o tempo de atividade do dispositivo sobre as últimas 30 votações.

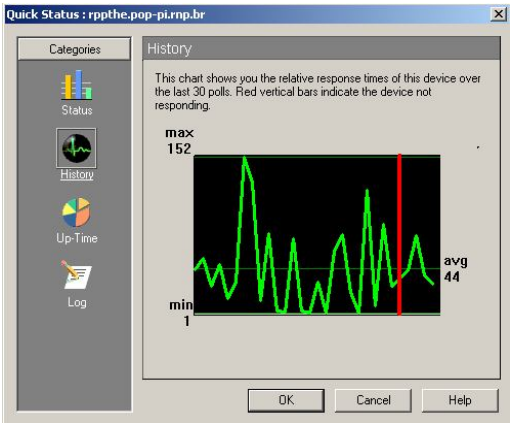

Figura 21: *Quick Status: Histórico*

A aba **Up-Time:** indicar um gráfico que mostra a porcentagem de votações bem sucedidas para a contagem total da votação para o dispositivo.

Log: indica todo os serviços do dispositivo estão para "cima" ou "para baixo", indicando mudanças para este dispositivo.

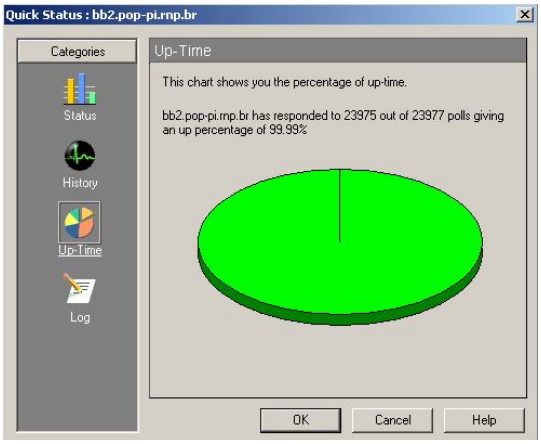

Figura 22: *Quick Status: Up Time*

E a aba **Log:** indica todo os serviços do dispositivo estão para "cima" ou "para baixo", indicando mudanças para este dispositivo.

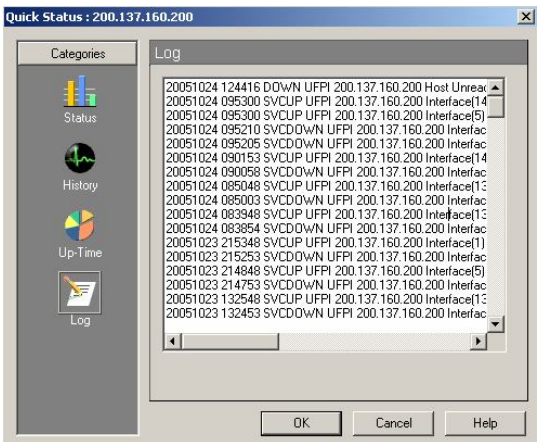

Figura 23: *Quick Status: Log (Registro)*

7.1.4.5. Geração de gráficos

O Whats Up oferece diversos tipos de relatórios que informam o estado da rede em intervalos de tempo diversos, escolhidos pelo próprio usuário da ferramenta. Os tipos de relatórios são descritos a seguir:

- Outage Reports: Mostra as mudanças de estado que ocorreram com os equipamentos e serviços da rede num determinado tempo;
- Statistics Reports: Mostra o tempo de resposta da rede nas verificações, além de mostrar a porcentagem de pacotes de verificações que não tiveram respostas;
- Performance Graphics: Fornece diversos gráficos informando a disponibilidade dos equipamentos; tempo de resposta da rede e de cada máquina individualmente. Os gráficos podem ser exportados para arquivos de diversos formatos (pdf, html, doc, xls, rpt, wks,...).

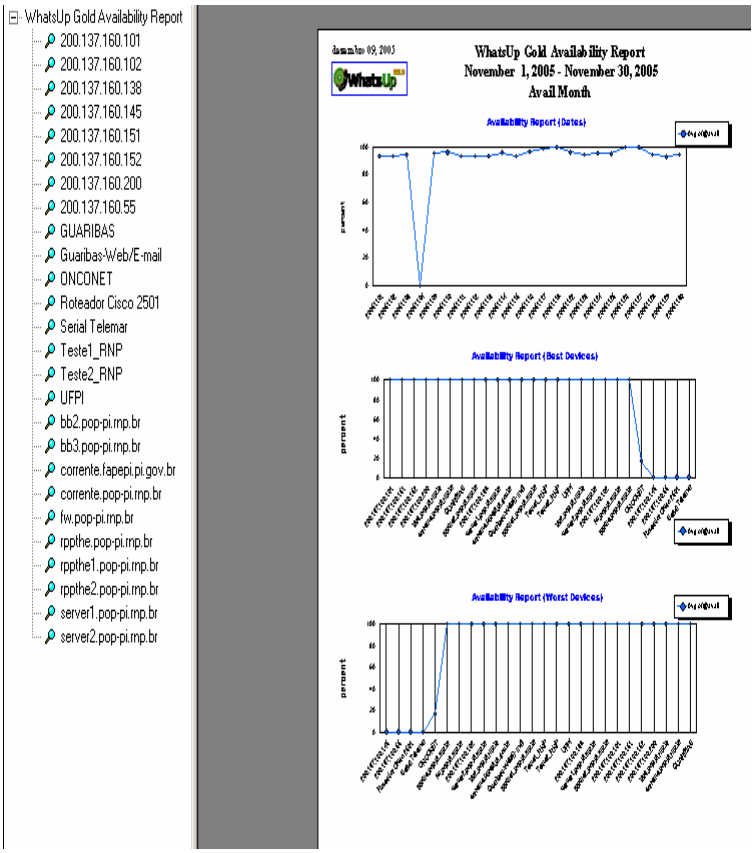

Figura 24: *Gráfico informando parametros de atividade/inatividade e tempo de resposta*

7.1.4.6. Arquivos de log:

O Whats Up possui quatro tipos de logs:

- SysLogs: Mensagens UDP enviada pelos equipamentos. O formato do arquivo é SL – yyyy-mm-dd.tab;
- Activities: Atividades que alteram o status da rede como equipamento/serviço cai ou é recuperado. O formato do arquivo é EV – yyyy-mm-dd.tab;
- Polling Statistics: Acumula os valores de tempo de resposta dos equipamentos quando ocorrem as verificações de estado. Arquivo ST – yyyy-mm-dd.tab;
- SNMP Traps: Mostra todas as traps SNMP que foram recebidas;

A formatação dos arquivos de log do Whats Up varia conforme é o tipo de log. Para logs do tipo Activites a formatação é a seguinte:

Data	Hora	Ocorrência	Equipamento	Ip	Serviço
20030805	091943	UP	Lab10	200.200.200.200	-
20030805	091955	DOWN	Lab10	200.200.200.200	-
20030805	092001	SVCDOWN	Router01	200.200.200.201	Interface(1)
20030805	092015	SVCUP	Router01	200.200.200.201	Interface(1)

Com este log o Whats Up irá gerar os gráficos e relatórios de disponibilidade dos equipamentos da rede.
Logs do tipo Polling Statistics fornecem os tempos de resposta dos equioamentos monitorados. Estes logs têm a seguinte formatação:

				Tempo de resposta			Pacotes Perdidos
Data	Hora	Mapa	Equipamento	Média	Máximo	Mínimo	
20030804	094552	C:\Arq...	Router01	2	4	1	0

Com base neste log, pode-se obter informações sobre o tempo em que a rede respondeu com menos ou mais tempo; e saber-se quando ela e os equipamentos estavam mais ou menos sobrecarregados.

7.2. MRTG

7.2.1. Definição

O MRTG é um programa que gera páginas HTML, onde apresenta dados de monitoração provenientes de variáveis de gestão nos equipamentos.

Basicamente o Multi Router Grapher – MRTG é uma ferramenta para monitorar o tráfego na rede, a utilização de interfaces, links de redes, utilização de CPU e qualquer outra variável numérica de equipamentos que suportem estas características de gerenciamento.

As páginas HTML geradas utilizam imagens GIF atualizadas em um determinado período de tempo. Estas páginas representam os dados obtidos dos dispositivos gerenciados.

Para poder visualizar os dados deste aplicativo, é precisa ter um servidor HTTP instalado na estação onde se pretende instalá-lo. E depois disso, instalar o pacote via apt-get no caso do debian.

Após ter instalado devidamente o mrtg deve-se proceder à sua configuração. Ele pode funcionar através de uma plataforma Unix/Linux e Windows NT Como requisitos de máquina, temos como configuração mínima: Pc 486 DX 100/66 MHz, 16 MB de memória.

Primeiramente, antes de instalar o MRTG, é necessário ter um HD de boa capacidade, devido aos logs que o MRTG gera, e aos gráficos que são montados utilizando arquivos no formato GIF.

Baseado na linguagem Perl e C, é aconselhável ser usado juntamente com um servidor WEB (exemplo: Apache) para facilitar as consultas aos gráficos de monitoramento. Utiliza o SNMP para ler as informações dos dispositivos gerenciados e programas escritos em linguagem C para montar os gráficos. Estas páginas geradas pelo MRTG podem ser consultadas de qualquer computador que possua um browser instalado.

É interessante utilizar o MRTG em conjunto com um outro software de gerenciamento de redes, com suporte a SNMP, como o WhatsUP.

A coleta é pontual, possibilidade de visualização diária, semanal, mensal e anual das estatísticas geradas nos gráficos. Isto é possível, pois o MRTG armazena os logs das informações dos equipamentos contendo as datas.

O MRTG possui um programa (cfgmaker) para geração de arquivos de configuração onde é especificado <comunidade>@<host ou IP> e o identificador das variáveis a serem coletadas.

Para gerar um gráfico é necessário conhecer o *OID* da variável que o agente responde. O MRTG não possui um limite de equipamentos para se gerenciar, e pode monitorar qualquer variável SNMP. As variáveis mais usadas são: taxas de utilização do canal, utilização do modem e carga de CPU.

Para que o MRTG tenha um bom funcionamento é necessário que todos os dispositivos que serão gerenciados tenham o agente SNMP habilitado. O servidor MRTG precisa ter permissão de leitura das informações de gerenciamento nestes agentes.

Como o MRTG é uma coleção de scripts escritos em Perl é necessário que se tenha uma versão do interpretador de comandos Perl para a plataforma na qual se deseja instalar o MRTG.

7.2.2. História

Em 1994 foi escrito um programa que constantemente atualizava um gráfico na web, mostrando a utilização do link de Internet. Isso finalmente tornou-se um script configurável em Perl chamado MRTG-1.0 que foi lançado na primavera de 1995. Em Janeiro de 1996, Dave Rand decidiu melhorar a velocidade do MRTG, reescrevendo as sessões que demoravam mais tempo do MRTG em C. A ferramenta que ele desenvolveu melhorou a velocidade do MRTG em 40 vezes!

Logo depois do desenvolvimento MRTG-2 ter começado passou-se a distribuir cópias beta para pessoas interessadas. E muitas contribuições e correção de bugs foram recebidas.

7.2.3. Características

- **Portabilidade:** MRTG trabalha na maior parte das plataformas UNIX e Windows NT.
- **Perl:** MRTG é escrito em Perl e vem com todo o código fonte.
- **Portabilidade SNMP:** MRTG usa uma implementação SNMP de alta portabilidade escrita toda em Perl graças a Simon Leinen. Não é necessário instalar qualquer pacote SNMP externo.
- **Suporte a SNMPv2c:** MRTG pode ler os novos contadores de 64 bits do SNMPv2c. Os contadores não serão mais problema.
- **Interface de Identificação Confiável:** As interfaces dos roteadores podem ser identificadas pelo Endereço IP, Descrição e Endereço Ethernet em adição ao número da interface normal.
- **Tamanho dos arquivos de Log Fixos:** Os arquivos de log do MRTG NÃO crescem. Graças ao uso de um algoritmo de consolidação de dados único.
- **Configuração Automática:** MRTG vem com um conjunto de ferramentas de configuraçao que fazem a configuração muito simples.
- **Desempenho:** As rotinas mais críticas foram escritas em C graças a iniciativa de Dave Rand meu Co-Autor.
- **Livre de Gráficos GIF:** Os gráficos são gerados diretamente no formato PNG, usando a biblioteca GD de Thomas Boutell.
- **Customizável:** A aparência das páginas produzidas pelo MRTG são altamente configuráveis.
- **RRDtool:** MRTG foi construído para ser compátivel com RRDtool. Se você precisa de performance isso pode ajudar.

7.2.4. Detalhes

MRTG consiste em um script em Perl que usa SNMP para ler os contadores de tráfego de seus roteadores e um rápido programa em C que loga os dados do tráfego e cria gráficos representando o tráfego da conexão de rede monitorada. Estes gráficos são incluídos em páginas web que podem ser visualizadas de qualquer Browser.

Somadas a detalhada visão diária o MRTG também cria representações visuais do tráfego durante os últimos 7 dias, das últimas 4 semanas e dos últimos 12 meses. Isto é possível porque o MRTG mantém um log de todos os dados que ele conseguiu do roteador.

O MRTG não se limita a monitorar somente tráfego, é possível monitorar qualquer variável SNMP que você escolher. Você pode até usar um programa externo para pegar os dados que você deve monitorar via MRTG. As pessoas usam o MRTG,

para monitorar Carga do Sistema, Sessões Logadas, Disponibilidade de Modens e muito mais. O MRTG ainda permite a você acumular 2 ou mais fontes de dados em um único gráfico.

7.2.5. Funcionamento

O mrtg tem um funcionamento muito simples. O programa é baseado em um script (mrtg) que toma as decisões e um programa (rateup) que faz o trabalho pesado de inserir dados no banco de dados e gerar as imagens. Tudo que o vovê precisa saber é que existe o script mrtg e um arquivo de configuração que indica qual o roteador e qual a informação será obtida deste. O processo de criação do banco de dados é o mesmo processo de alimentar o banco de dados. A alimentação do banco de dados é feita pelo programa em perl "mrtg" que recebe como parâmetro um arquivo de configuração "cfg".

7.2.6. Instalação e Configuração

O MRTG roda tanto em plataforma Windows como Linux. Este trabalho descreve os procedimentos para instalação e configuração do Servidor de Gerência e Monitoramento - MRTG, utilizando a distribuição *Debian GNU/Linux*

.

A instalação requer três programas:

- Interpretador Perl (active Perl);
- Apache 2 (recomendado)
- O próprio MRTG

Para instalar o interpretador Perl e o sistema **MRTG**, execute os seguintes comandos:

apt-get install perl
apt-get install mrtg

A partir daí, o processo de instalação do MRTG está finalizado.

A instalação do MRTG não requer a criação de uma pasta, pois a pasta será criada por ele mesmo. Apenas será necessária a criação de uma pasta para a publicação das páginas com os gráficos criados pelo MRTG. Esta pasta é criada dentro de ***"/var/www"*** com nome de mrtg e subpastas com nomes de cada dispositivo por questões de organização:

mkdir /var/www/mrtg/router100, por exemplo

Para compor um arquivo de configuração do MRTG existe uma ferramenta chamada cfgmaker que constrói um arquivo cfg e os arquivos html dos itens monitorados. Um exemplo de linha de comando do cfgmaker é:

cfgmaker --output etc/mrtg/router100.cfg community@ip_dispositivo --global 'WorkDir: /var/www/mrtg/router102'

Onde "/var/www/mrtg/router100.cfg" é a pasta criada pelo próprio mrtg e vai ter um arquivo de configuração para o dispositivo apelidado de router100.

Commuinity é a comunidade do equipamento a ser monitorado. Seguido do ip ou nome (host name) e em seguida o parâmetro que vai conter as páginas com os gráficos criados pelo MRTG.

Criado os arquivos de configuração, iremos configurá-lo de acordo com as necessidades de gerenciamento escolhida pelo administrador da rede.

Os gráficos foram configurados, para que de forma clara e simples o administrador possa detectar qualquer anomalia rapidamente. Como por exemplo, linguagem em português - Brasil, cores nítidas, legendas, título nos gráficos, informações sobre velocidade link, instituição para onde link vai, "ip" de saída e destino, especificações do equipamento monitorado além de informações a quem se deve contactar em caso de falha.

É importante lembrar que: **Caso a linha inicie com um espaço em branco, esta será anexada à linha anterior**. O símbolo # na primeira coluna indica que a linha está comentada e não possui valor algum para o MRTG.

Utilize um visualizador de texto, seja ele o "nano", "gedit" ou qualquer outro de sua preferência.

nano /etc/mrtg/router100.cfg, diretório onde foi criado o arquivo de configuração para o dispositivo router100.

Abaixo será mostrado um exemplo do arquivo de configuração listado com o comando acima e posteriormente irei listar os principais e alguns parâmetros adicionais do script de configuração para um dispositivo.

WorkDir: /var/www/mrtg/router101
Options[_]: growright, bits
Refresh: 300
Interval: 5
Language: brazilian
RunAsDaemon: Yes

##
#
 # System: [not configured]
 # Description: Portable M68360 C Gateway [not configured] S/N 303 V1 R3.0 NP00712_13D []
 # Contact:
 # Location:
##
#

Interface 1 >> Descr: 'lan_enet_1' | Name: '' | Ip: 'ip_dipositovo' | Eth: '00-20-35-93-10-88'

Target[ip_dipositovo]: 1:public@ip_dipositovo:
SetEnv[ip_dipositovo]: MRTG_INT_IP="ip_dipositovo"
MRTG_INT_DESCR="lan_enet_1"
MaxBytes[ip_dipositovo]: 1250000
Title[ip_dipositovo]: Trafego Ethernet Router RPPTHE2 do PoP-PI
*PageTop[ip_dipositovo]: <H1>Analise de Trafego Ethernet RPPTHE2</H1> *
*PageFoot[ip_dipositovo]: <H3>Ponto de Presenca da RNP no Piaui - PoP-PI/RNP</H3> *
<TABLE>

<TR><TD>System:</TD> <TD>rppthe2.pop-pi.rnp.br</TD></TR>
<TR><TD>Maintainer:</TD> <TD>Nivaldo[ncardoso@fapepi.pi.gov.br](86)3216-6090</TD></TR>
<TR><TD>Description:</TD><TD>lan_enet_1 </TD></TR>
<TR><TD>ifType:</TD> <TD>ethernetCsmacd (6)</TD></TR>
<TR><TD>ifName:</TD> <TD></TD></TR>
<TR><TD>Max Speed:</TD> <TD>1250.0 kBytes/s</TD></TR>
<TR><TD>Ip:</TD> <TD>ip_dipositovo</TD></TR>
</TABLE>

PNGTitle[ip_dipositovo]:PoP-PI - SDR | LINK | Trafego
WithPeak[ip_dipositovo]:wm
XSize[ip_dipositovo]:410
YSize[ip_dipositovo]:100
XZoom[ip_dipositovo]:1.0
YZoom[ip_dipositovo]:1.0
YTics[ip_dipositovo]:6
YTicsFactor[ip_dipositovo]:1
Background[ip_dipositovo]:#BBBBBB
YLegend[ip_dipositovo]:bits por segundo
Legend1[ip_dipositovo]:Entrada bits por segundo
Legend2[ip_dipositovo]:Saida bits por segundo
Legend3[ip_dipositovo]:Entrada Maximo
Legend4[ip_dipositovo]:Saida Maximo

7.2.6.1. Detalhamento dos parâmetros de Configuração do exemplo:

WorkDir: Especifica o diretório em que serão armazenados os registros de acesso e as páginas web geradas.

Options (grownrigth): Essa opção inverte o sentido de crescimento dos gráficos.

Options (bits): os valores em bytes são convertidos para bits e apresentados.

Refresh: Especifica o intervalo de tempo, em segundos, que o browser deve recarregar a página. Se não for especificado, será assumido 300 segundos (5 minutos).

Interval: Especifica o intervalo de “pooling”, ou amostragem dos dados. O valor padrão é 10 (minutos).

Languague: Define o idioma do formato da saída.

RunAsDaemon:

Target[ip_dispositivo]: 24:public@10.8.3.1
| | | | |__ Host Name ou IP
| | | |__ comunidade
| | |__ index da interface, endereço físico ou endereço IP
| |__ nome atribuído ao *target*
|__ keyword (palavra reservada)

MaxBytes - Indica o valor máximo que pode ser assumido pelas variáveis SNMP.

Title – É o título do gráfico na página html gerada.

PageTop - Dados adicionais que serão exibidos no topo da página html.

PageFoot: Dados adicionais que serão exibidos no final da página.

Terão parâmetros com características do equipamento gerenciado, consultado na sua MIB, como por exemplo o *Max Speed* que é a velocidade máxima daquela porta gerenciada, o *Maintainer* que é um contato por exemplo do administrador.

***PNGTitle* :** título na borda superior do mapa

WithPeak - Por padrão, o MRTG gera os gráficos com os valores médios dentro do período de "amostragem" do gráfico em questão, ou seja, 5 minutos para gráfico diário, 30 para semanal, 2 horas para mensal e 1 dia para gráfico anual. Com essa opção, pode-se estipular que os gráficos semanais, mensais ou anuais devem apresentar o valor de pico obtido das amostras colhidas a cada 5 minutos.

Xsize e Ysize - Definem, em pixels, a largura e a altura dos gráficos gerados. O padrão é *XSize=400* e *YSize=100*. Os valores para XSize podem variar entre 20 e 600; e os valores para YSize devem ser maiores que 20.

XZoom e YZoom - Definem pixels maiores, permitindo o efeito de *zoom* nos gráficos.

YTics e YTicsFactor - Os valores padrão para YTics e YTicsFactor são, respectivamente, 4 e 1, e definem quantas linhas de referência serão exibidas nos gráficos e qual será o fator de divisão utilizado. Por exemplo, para obter uma visualização mais apropriada dos valores grafados, pode-se exibir mais linhas para referência através desta opção. Se os valores variarem em saltos grandes, como por exemplo, de 100 em 100, pode-se definir que a legenda do eixo Y tenha seus valores multiplicados pelo valor 0.01, de forma a apresentar valores variando de 1 em 1.

Background - Define a cor de fundo das páginas html geradas. O formato é o mesmo usado para a definição de cores do item anterior.

YLegend - Define a legenda do eixo Y nos gráficos gerados, a despeito dos valores padrão. Se o texto for grande demais a ponto de não poder ser escrito na figura, este será descartado.

Legend[1234] - Define as strings para a legenda de cores.

Assim o MRTG foi configurado de acordo com as características de gerenciamento escolhido pelo administrador do PoP-PI visando uma rápida e detalhada visão do comportamento da rede.

Para acessar a pagina html com gráficos gerados para dispositivo escolhido basta ir ao navegador e digitar: http://localhost/mrtg/, onde localhost pode ser o ip do servidor MRTG seguido do caminho para onde as páginas foram geradas**.**

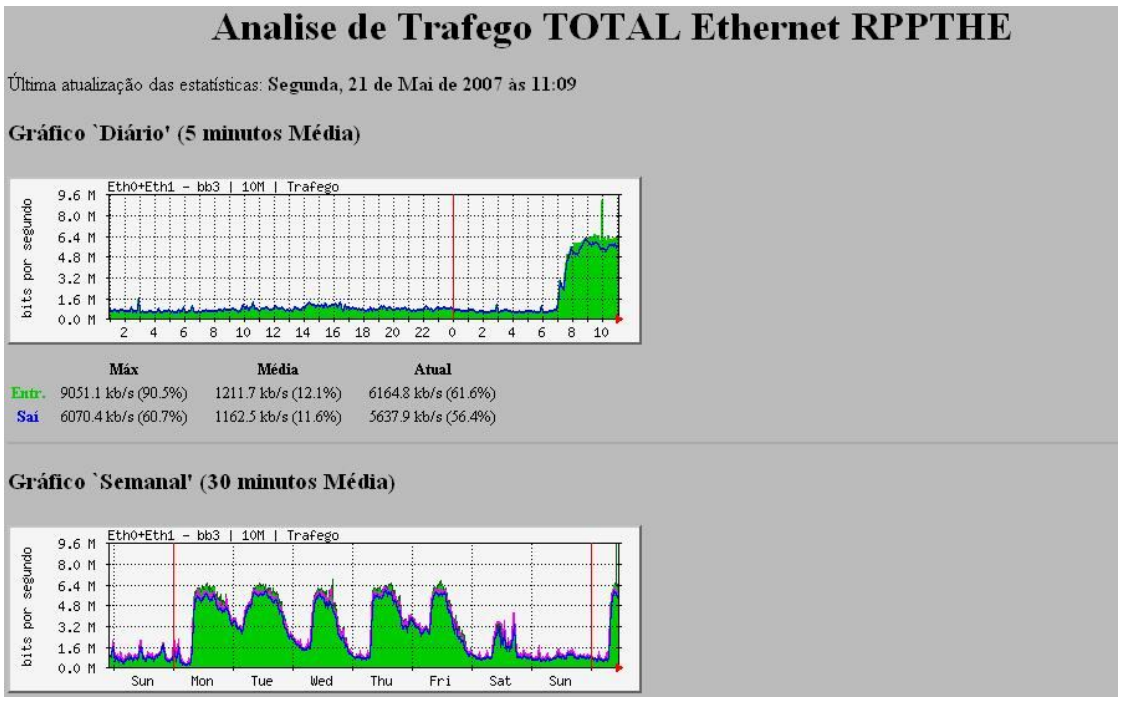

Figura 26: *Características e Informações de um equipamento monitorado*

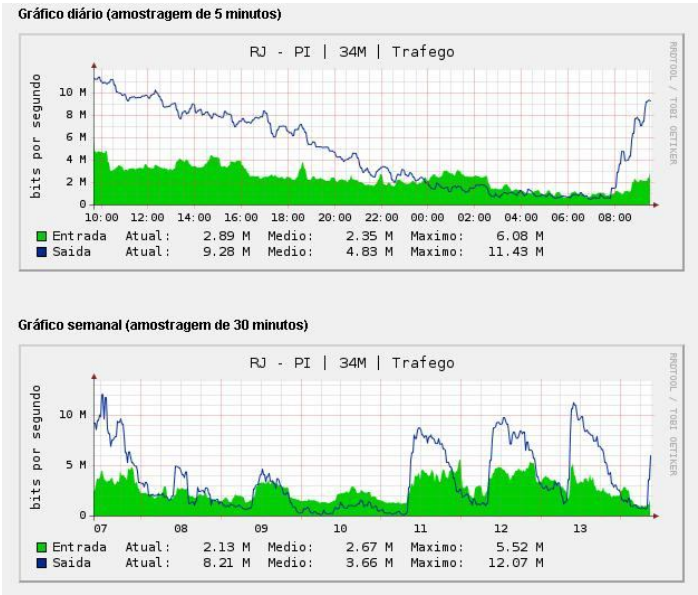

Figura 27: *Gráfico de consumo de banda*

7.3. Nagios

7.3.1. Introdução

O Nagios é um programa open source de monitoração de hosts, de serviços e de rede. Ele é desenvolvido para informar sobre problemas de rede antes que seus clientes, end-users ou gerentes o façam. Ele tem sido projetado para rodar em GNU/Linux, mas trabalha muito bem com outras variantes *NIX.

O daemon de monitoração roda checagens intermitentes nos hosts e serviços que são especificados usando plugins externos que retornam informações de estado para o Nagios. Quando são encontrados problemas, o daemon pode enviar notificações para contatos administrativos de várias formas diferentes (email, instant message, SMS, etc.). Informações sobre o estado atual, histórico de logs e reports podem ser todos acessados através de um navegador web.

Portanto o Nagios constitui-se em um software para monitoramento de redes, que podem possuir infra-estrutura de WAN, LAN e MAN. Possui uma GUI – Interface Gráfica. Além do mais, é totalmente livre e distribuído sobre a lei de copyleft GPL. Sua aplicação é designada a redes de grande porte, porém seu desempenho é excelente em redes de pequeno porte. Vigia hosts e serviços que o administrador de redes determinar nos arquivos de configuração, alertando quando o serviço ou host caírem e também quando eles retornarem, também permite o monitoramento de equipamentos com suporte a protocolos SNMP, o principal agente que permite a troca de informações entre o Nagios e os hosts monitorados.

7.3.2. Características

- Monitoração de serviços de rede (POP3, SMTP, HTTP, Ping, NNTP, etc.)
- Monitoração de recursos de hosts (uso de disco, memória, carga do processador, etc.)
- Definição de hierarquia de hosts de rede usando “parent” hosts
- Notificação de contatos quando ocorrem problemas em hosts ou serviços por e-mail, pager, etc, em tempo real
- Uso de *event handlers* para serem rodados em eventos de hosts ou serviços
- Automoção de rotação de logs
- Interface Web informativa, que podemos identificar de maneira fácil os problemas.
- Pode ainda fazer monitoramento da temperatura ambiental através de um um aparelho chamado “Esensor”,

7.3.3. Instalação

Neste artigo iremos abordar a instalação, configuração dos plugins e sua integração com o MySQL, o processo foi realizado em um servidor rodando Debian GNU/Linux.

7.3.3.1. Pré-requisitos para instalação do nagios:

Para compilar Nagios requer o GCC, make, autoconf e automake. As bibliotecas requeridas são libgd e openssl. Os pacotes do desenvolvimento para estes

devem ser instalados (dependendo da distribuição, com ou o - dev ou - devel): libssl-dev, libgd-dev, libc6-dev.

Recomenda-se que você instale também os seguintes pacotes ao mesmo tempo: ntpdate, SNMP, smbclient, libldap2, e libldap2-dev, assim como o cliente e os pacotes do colaborador para que a base de dados seja usada (por exemplo, e.g., postgresqlclient e postgresql-dev).

7.3.3.2. Compilando o código de fonte

O código de fonte próprio de Nagios está disponível para o download na página do projeto http://www.nagios.org.

linux: # **mkdir /usr/local/src**
linux:~ # **cd /usr/local/src**
linux:local/src # **tar xvzf *Path/to/*nagios-versão.tar.gz**

Os três comandos extraem o código de fonte no diretório criado para esta finalidade, /usr/local/src. Quando isto é feito, um subdiretório com o "nagios-versão" também é criado. Antes da compilação e da instalação reais, os grupos requeridos para a operação, nagios e nagcmd, são ajustados para groupadd e useradd:

linux:~ # **groupadd -g 9000 nagios**
linux:~ # **groupadd -g 9001 nagcmd**
linux:~ # **useradd -u 9000 -g nagios -G nagcmd -d /usr/local/nagios** \ **-c "Nagios Admin" nagios**

Em vez do usuário (9000) e do grupo IDs (9000 ou 9001) usado aqui, qualquer outro ID (disponível) pode ser usado.

A fim de que este usuário possa alcançar certas áreas protegidas do Nagios, um grupo adicional é requerido: somente o usuário web Server e o usuário do Nagios devem pertencer a este grupo. O usuário do Web Server pode ser determinado na linha de configuração do Apache:

linux:~ # **grep "^User" /etc/apache2/httpd.conf**
User www-data
linux:~ # **usermod -G nagcmd www-data**

No exemplo, o usuário do Web Server é chamado WWW-dados. O comando usermod (muda os dados para um usuário que existe) inclui também o usuário do Web Server no grupo do nagcmd, à opção -G manipula a entrada correspondente no diretório /etc/group.

Além do diretório especificado como o diretório home do usuário nagios, o /usr/local/nagios, o diretório /etc/nagios da configuração e o diretório /var/nagios, que grava dados variáveis quando Nagios funcionar, são ajustados e atribuídos o usuário e ao grupo:

linux:~ # **mkdir /usr/local/nagios /etc/nagios /var/nagios**
linux:~ # **chown nagios.nagios /usr/local/nagios /etc/nagios /var/nagios**

Entre no diretório com as fontes do Nagios para preparar para a compilação:

linux:~ # **cd /usr/local/src/nagios-2.0b3**
linux:src/nagios-2.0b3 # **./configure --sysconfdir=/etc/nagios --localstatedir=/var/nagios --with-command-group=nagcmd**

*** Configuration summary for nagios 2.6 11-27-2006 ***:
General Options:

Nagios executable: nagios
Nagios user/group: nagios,nagios
Command user/group: nagios,nagcmd
Embedded Perl: no
Event Broker: yes
Install $prefix: /usr/local/nagios
Lock file: /var/nagios/nagios.lock
Init directory: /etc/init.d
Host OS: linux-gnu

Web Interface Options:

HTML URL: http://localhost/nagios/
CGI URL: http://localhost/nagios/cgi-bin/
Traceroute (used by WAP): /usr/sbin/traceroute

Vamos começar a compilação e instalação do software:

linux:src/nagios-2.0b3 # **make all**
linux:src/nagios-2.0b3 # **make install**
linux:src/nagios-2.0b3 # **make install-init**
linux:src/nagios-2.0b3 # **make install-commandmode**
linux:src/nagios-2.0b3 # **make install-config**

Depois de tudo compilado, todos os programas são copiados para os diretórios apropriados, junto com o cgi e documentação, que também fazem parte da instalação.

Diretórios do Nagios dentro "/usr/local/nagios"

./bin	Programa executável do Nagios
./libexec	Plugins
./sbin	CGI scripts
./share	Documentação, arquivos HTML para interface Web

Para que o Nagios comece automaticamente, as seguintes ligações simbólicas devem ser criadas:

linux:~ # **ln -s /etc/init.d/nagios /etc/init.d/rc2.d/S99nagios**
linux:~ # **ln -s /etc/init.d/nagios /etc/init.d/rc2.d/K99nagios**

7.3.3.3. Instalando e testando plugins

O download e a instalação dos plugins devem ser separados. Como são programas independentes, são sujeitos a uma versão diferente do Nagios. A versão atual na altura de ir pressionar era a versão 1.4.5.

A instalação das fontes do plugin ocorre no diretório /usr/local:

linux:~ # **cd /usr/local/src**
linux:local/src # **tar xvzf /nagios-plugins-versão.tar.gz**
linux:src/nagios-plugins-versão # **./configure --sysconfdir=/etc/nagios --localstatedir=/var/nagios**

Teste se o Plugin está rodando corretamente com o seguinte comando:

linux:nagios-plugins-versão/contrib # **make check_cluster2**
cc check_cluster2.c -o check_cluster2

Para que o plugin esteja funcionando corretamente ele deve rodar com usuário root:

linux:~ # **chown root.nagios /usr/local/nagios/libexec/check_icmp**
linux:~ # **chmod 4711 /usr/local/nagios/libexec/check_icmp**
linux:~ # **ls -l /usr/local/nagios/libexec/check_icmp**
-rwsr-x--x 1 root nagios 61326 2005-02-08 19:49 check_icmp

As instruções breves para o plugin são dadas com a opção de -h:

nagios@linux:~$ **/usr/local/nagios/libexec/check_icmp -h**
Usage: check_icmp [options] [-H] host1 host2 hostn
Where options are any combination of:
* -H | --host specify a target
* -w | --warn warning threshold (currently 200.000ms,40%)
* -c | --crit critical threshold (currently 500.000ms,80%)
* -n | --packets number of packets to send (currently 5)
* -i | --interval max packet interval (currently 80.000ms)
* -I | --hostint max target interval (currently 0.000ms)
* -l | --ttl TTL on outgoing packets (currently 0)
* -t | --timeout timeout value (seconds, currently 10)
* -b | --bytes icmp packet size (currenly ignored)
-v | --verbose verbosity++
-h | --help this cruft
The -H switch is optional. Naming a host (or several) to check is not.

Para um teste simples basta especificar um endereço IP:

user@linux:~$ **cd /usr/local/nagios/libexec**
user@linux:nagios/libexec$ **./check_icmp -H 192.168.1.13**
OK - 192.168.1.13: rta 0.261ms, lost 0%|rta=0.261ms;200.000;500.000;0;
pl=0%;40;80;;

7.3.3.4. Configuração da Interface WEB

O Web Server deve saber o diretório do cgi e o diretório da base do próprio Web Server.

ScriptAlias /nagios/cgi-bin /usr/local/nagios/sbin
<Directory "/usr/local/nagios/sbin">
AllowOverride AuthConfig
Options ExecCGI
Order allow,deny
Allow from 192.168.0.0/24
</Directory>

O ScriptAlias diretivo assegura-se de que Apache alcance o diretório do cgi de Nagios ao chamar um URL tal como http://nagios-server/nagios/cgi-bin, e os respectivos diretórios do cgi do Apache podem ser encontrados. As opções ExcecCGI asseguram-se de que o web server aceite todos os certificados situados lá como o

cgi.. As diretrizes orientadoras requisitam e asseguram que somente os clientes da rede 192.168.0.0 /24 (/24 estão para o subnet mask 255.255.255.0) possam obter o acesso ao diretório especificado.

Dirigem-se ao diretório de original /usr/local/nagios/share do Nagios sob http://nagios-server/nagios (independentemente de onde o Apache DocumentRoot é encontrado), o seguinte é adicionado:

Alias /nagios /usr/local/nagios/share
<Directory "/usr/local/nagios/share">
Options None
AllowOverride AuthConfig
Order allow,deny
Allow from 192.168.0.0/24
</Directory>

Estas linhas devem ser incluidas no diretório /etc/apache2/httpd/conf.d.
Recarregue as configurações do Apache2 com o comando:

linux:˜ # **/etc/init.d/apache reload**

Para exibir página principal de Nagios abra seu browser e digite o endereço:

http://nagios-server/nagios

7.3.3.5. User Authentication

O Nagios permite somente o acesso de usuários autenticados. Isto significa que os usuários “não cadastrados” não têm nenhuma maneira ver qualquer coisa na Home Page e da documentação. São obstruídos fora do acesso a outras funções.

A maneira a mais fácil executar um authentication correspondente é através de uma linha dentro do .htaccess no diretório /usr/local/nagios/sbin. O parâmetro use_authentication em cgi.cfg da configuração do cgi do Nagios deve ser ajustado para 1:

use_authentication=1

Este é o defeito durante a instalação. No diretório /usr/local/nagios/sbin do cgi uma lima de .htaccess é criada com os seguintes índices:

AuthName "Nagios-Monitoring"
AuthType Basic
AuthUserFile /etc/nagios/htpasswd
require valid-user

AuthName indique para o web server pedir autenticação.

7.3.4. Configuração

Descrição dos arquivos de configuração:

nagios.cfg - arquivo de configuração principal do Nagios, responsável por iniciar os serviços de monitoramento.
cgi.cfg - arquivo de configuração dos programas CGIs localizados na pasta sbin.
hosts.cfg - arquivo contendo informações dos hosts.
hostgroups.cfg - arquivo contendo informações dos hosts por grupos.

contacts.cfg - contatos que deverão ser notificados caso ocorra algum problema.
contactgroups.cfg - contatos divididos em grupos.
service.cfg - serviços que deverão ser monitorados
hostextinfo.cfg - onde serão definidos as imagens que serão apresentadas no statusmap.
dependencies.cgf - informações de serviços que dependem de outros serviços.
timeperiods.cfg - Informações sobre o período de monitoramento, podem ser definidos vários períodos de monitoramento diferentes.
checkcommands.cfg - definição dos comandos que podem ser executados pelo Nagios.
resource.cfg - macros definidas pelos usuários.

7.3.4.1. Exemplo dos arquivos de configuração:

7.3.4.1.1. Nagios.cfg

−−−−−−−−−−−−−−−−−−−− nagios.cfg −−−−−−−−−−−−−−−−−−−

```
.....
log_file=/var/log/nagios/nagios.log
cfg_file=/etc/nagios/checkcommands.cfg
cfg_file=/etc/nagios/misccommands.cfg
cfg_file=/etc/nagios/contactgroups.cfg
cfg_file=/etc/nagios/contacts.cfg
cfg_file=/etc/nagios/dependencies.cfg
cfg_file=/etc/nagios/escalations.cfg
cfg_file=/etc/nagios/hostsgroups.cfg
cfg_file=/etc/nagios/hosts.cfg
cfg_file=/etc/nagios/services.cfg
cfg_file=/etc/nagios/timeperiods.cfg
.....
```

7.3.4.1.2. Cgi.cfg

Nós configuramos para que só o usuário "nagiosadmin" tenha acesso. Não queremos que mais ninguém tenha acesso.

−−−−−−−−−−−−−−−−−−−− cgi.cfg −−−−−−−−−−−−−−−−−−−

```
.....
authorized_for_system_information=nagiosadmin
authorized_for_configuration_information=nagiosadmin
authorized_for_system_commands=nagiosadmin
authorized_for_all_services=nagiosadmin
authorized_for_all_hosts=nagiosadmin
authorized_for_all_service_commands=nagiosadmin
authorized_for_all_host_commands=nagiosadmin
.....
```

7.3.4.1.3. Hosts.cfg

No arquivo hosts.cfg você incluirá TODAS as máquinas que quer que seja monitorada. Cada máquina deverá ter pelo mínimo um serviço, seja um check_ping, check_http, check_ftp.....

−−−−−−−−−−−−−−−−−−−− hosts.cfg −−−−−−−−−−−−−−−−−−−

```
# Default gateway host definition
define host{
```

```
use generic−host ; Name of host template to use
host_name router
alias Router Zyxel 650−HW ADSL
address 192.168.1.1
check_command check−host−alive
max_check_attempts 20
notification_interval 60
notification_period 24x7
notification_options d,u,r
}
# \'casandra\' host definition
define host{
use generic−host ; Name of host template to use
host_name casandra
alias AMD XP 1.7+ Debian SID
address 192.168.1.2
parents router
check_command check−host−alive
max_check_attempts 10
notification_interval 120
notification_period 24x7
notification_options d,u,r
}
}
# \'servidor\' host definition
define host{
use generic−host ; Name of host template to use
host_name servidor
alias AMD 266Celeron Wi−Fi
address 192.168.1.4
parents router
check_command check−host−alive
max_check_attempts 10
notification_interval 120
notification_period 24x7
notification_options d,u,r
}
```

Explicação dos parametros:

host_name: Nome do micro na rede.
alias: Um apelido para o computador (ou uma descrição, como no nosso caso).
address: O endereço IP da máquina.
check_command: Aqui definimos o comando de checagem do host a ser executado, que será definido em checkcommand.cfg.
max_ckeck_attempts: Quantidade de tentativas de checagem antes de reportar erro/indisponibilidade.
notification_interval: Espaço de tempo (em minutos) em que deve ser enviada a notificação de erro/indisponibilidade dos serviços ao usuário responsável por ele
notification_period: Intervalo de tempo em que o serviço está ativo (intervalos de tempo podem ser definidos no arquivo timeperiods.cfg)
notification_options: Tipos de erros que deve notificar para este host, onde:

d - O serviço está inativo (down)
u - O serviço não pode ser encontrado (unrecheable)

r - O serviço voltou a funcionar (recovery)

Obs.: A opção parents é utilizada normalmente caso a máquina seja ligada a outra, no nosso exemplo temos uma máquina firewall e as outras máquinas acessam a internet através dela, então os outros hosts serão parents do nosso host firewall, desta forma, a administração fica mais eficiente)

7.3.4.1.4. Hostgroups.cfg

Cada host, deve pertencer a um hostgroups e cada " hostgroups " deve ter um contacts_groups pelo menos.

−−−−−−−−−−−−−−−−−−−− hostgroups.cfg −−−−−−−−−−−−−−−−−−−

```
# Default gateway host group definition
define hostgroup{
hostgroup_name AdmPoP
alias AdmPoP
contact_groups admins
members servidor, casandra, router
}
```

7.3.4.1.5. Contacts.cfg

As pessoas de contatos, serão notificadas das possíveis falhas ou erros das máquinas da Rede.

−−−−−−−−−−−−−−−−−−−− contacts.cfg −−−−−−−−−−−−−−−−−−−

```
# \'nagios\' contact definition
define contact{
contact_name nagios
alias Nagios Admin
service_notification_period 24x7
host_notification_period 24x7
service_notification_options w,u,c,r
host_notification_options d,u,r
service_notification_commands notify−by−email
host_notification_commands host−notify−by−email
email admin−nagios@servidor.net
# pager pagenagios−admin@localhost.localdomain
}
```

7.3.4.1.6. Contactgroups.cfg

Cada contato, deve pertencer a um contato de grupo:

−−−−−−−−−−−−−−−−−−−− contactgroups.cfg −−−−−−−−−−−−−−−−−−−

```
# \'admins\' contact group definition
define contactgroup{
contactgroup_name admins
alias Administrators
members nagios
}
```

7.3.4.1.7. Services.cfg

Este é possivelmente o arquivo de configuração mais importante, nele incluiremos TODOS os serviços que queremos monitorar.

−−−−−−−−−−−−−−−−−−−− services.cfg −−−−−−−−−−−−−−−−−−−−

```
# Service definition
define service{
# use generic−service ; Name of service template to use
host_name router
service_description PING
is_volatile 0
check_period 24x7
max_check_attempts 3
normal_check_interval 5
retry_check_interval 1
contact_groups admins
notification_interval 240
notification_period 24x7
notification_options c,r
check_command check_ping!100.0,20%!500.0,60%
}
# Service definition
define service{
# use generic−service ; Name of service template to us
host_name router
service_description FTP
is_volatile 0
check_period 24x7
max_check_attempts 3
normal_check_interval 5
retry_check_interval 1
contact_groups admins
notification_interval 120
notification_period 24x7
notification_options w,u,c,r
check_command check_ftp
}
# Service definition
define service{
# use generic−service ; Name of service template to us
host_name router
service_description HTTP
is_volatile 0
check_period 24x7
max_check_attempts 3
normal_check_interval 5
retry_check_interval 1
contact_groups admins
notification_interval 120
notification_period 24x7
notification_options w,u,c,r
check_command check_http
}
```

7.3.4.2. Verificando a configuração:

Para verificar se tudo está configurado corretamente usamos o comando:

/usr/sbin/nagios -v /etc/nagios/nagios.cfg

Com esse comando é possível verificar os erros e warnings que porventura existam, e ver também em qual arquivo está ocorrendo o erro de configuração.

IMPORTANTE: O Nagios não inicia se houver qualquer erro, já com warnings ele inicia, mas é bom verificar a causa dos mesmos.

7.3.4.3. Iniciando o Nagios:

Se tudo foi certo no passo anterior, o Nagios pode ser iniciado:

/etc/init.d/nagios start

Obs: O Debian já coloca um atalho no /etc/rc2.d para o nagios, para que ele seja iniciado a cada reboot do sistema.

Dica: Verifique com atenção se seu apache está funcionando corretamente, se todos os arquivos de configuração e todas as permissões para o usuário e grupo nagios estão definidas e tudo mais, as vezes um erro muito pequeno como uma linha sem descomentar pode nos dar uma dor de cabeça)

7.3.4.4. Acessando o Nagios:

Para acessar o nagios é simples, abra o browser e digite:
http://ipdoseuservidor/nagios
Para se autenticar, use o login nagiosadmin e a senha definida na instalação.

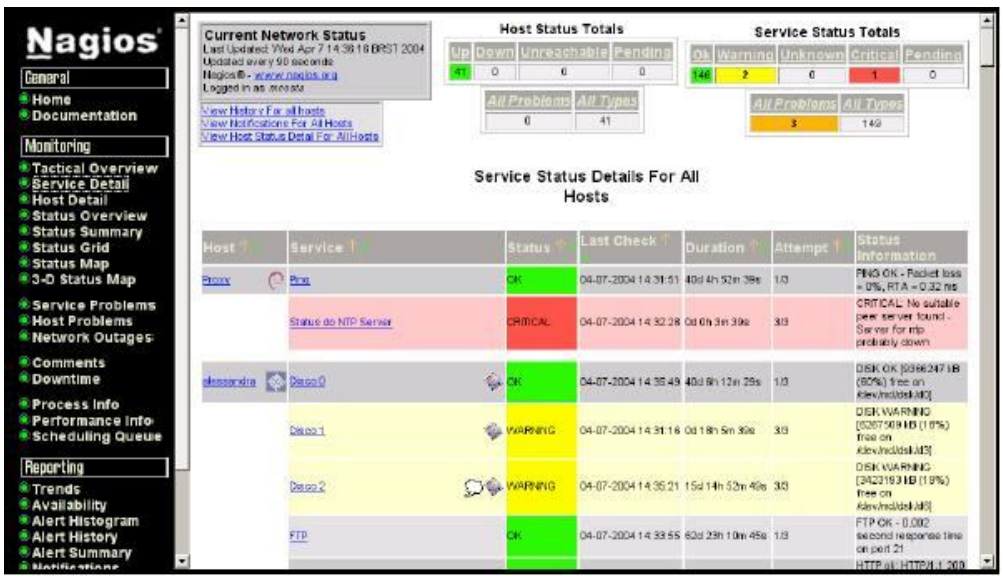

Figura 28: *Detalhes dos serviços monitorados*

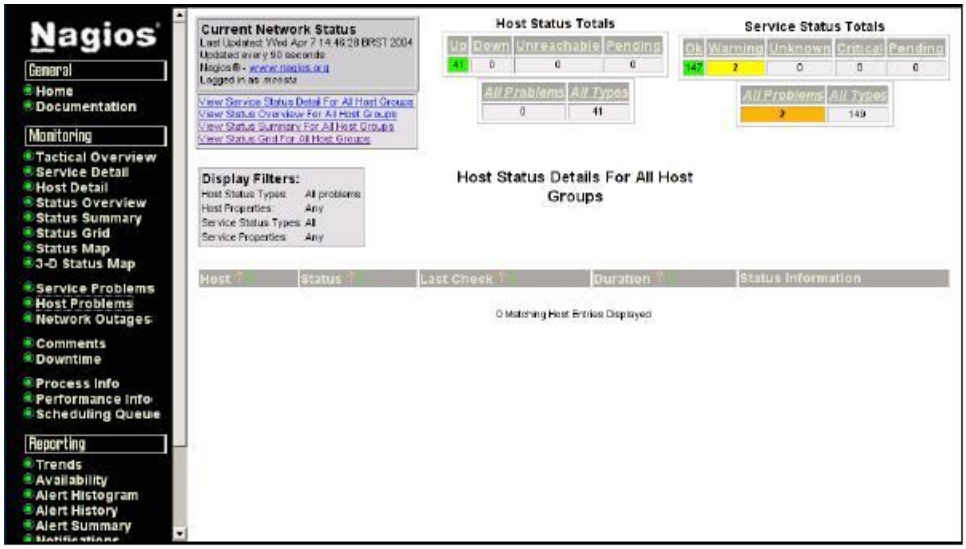

Figura 29: *Status dos Hosts com problemas*

Figura 30: Contatos de Notificação

7.4. CACTI

7.4.1. Definição

O Cacti é uma ferramenta gráfica de gerenciamento de dados de rede desenvolvido para ser utilizado por administradores de rede com uma não muito rica experiência na área, enquanto por outro lado, disponibiliza recursos bem poderosos para serem utilizados em redes bastante complexas. O Cacti é um front-end para o RRDTOOL desenvolvido na linguagem PHP, possui uma interface web e armazena todos os seus dados em um banco de dados MySql. Utilizando essa ferramenta, é possível fazer o polling de hosts SNMP, criar gráficos e gerenciar o acesso de usuários a toda a informação já coletada.

RRD é a abreviação de Round Robin Database, sistema cujo objetivo é armazenar e monitorar dados em série obtidos durante um período de tempo pré-determinado. Esses dados não aumentam com o decorrer do tempo e nem com a quantidade de dados já armazenados. Entretanto, o RRDTOOL não é capaz de gerar páginas html ou produzir gráficos, fato que torna necessário a sua comum utilização associada a um front-end.

7.4.2. Caracterísitcas

Esta ferramenta disponibiliza a seus usuários uma interface bem agradável de usar. Com o Cacti, é possível fazer o controle de acesso por nível de usuário, ou seja, podemos configurar o acesso a certas informações apenas por determinados usuários. Além disso, o fato do usuário desejar adicionar algum novo equipamento para ser monitorado não é uma tarefa complicada como em outras ferramentas (por exemplo o MRTG), bastando para isso alguns poucos minutos.

O CACTI é um programa LIVRE, ou seja, disponibilizado para qualquer um baixá-lo e instalá-lo em seu computador.

A versão atual do Cacti é a cacti-0.8.6i

7.4.3. Instalação

Iremos abordar o tipo de instalação do cacti, baseada no Debian.

O Cacti exige que se tenha instalado em seu computador os seguintes pacotes:

- Apache (ou outro servidor web)
- PHP (versão > 4) + extensões php-snmp e php-gd2
- Banco de dados MySQL
- net-snmp
- RRDtool

Faça download da ultima versão estável do cacti 0.8.6i, em http://www.cacti.net/download_cacti.php

Primeiramente é necessário instalar todos os compiladores requeridos. Execute os seguintes comandos:

apt-get install apache2

apt-get install php5

apt-get install mysql-server

apt-get install rrdtool

Depois de feito download da versão mais nova do Cacti, descompate-o dentro de “/var/www”:

tar xzvf cacti-version.tar.gz

mv cacti-version.tar.gz cacti

Agora iremos criar mapa base de dados do Cacti no MySQL:

mysqladmin --user=root create cacti

Importar a base de dados default do cacti:

mysql cacti < cacti.sql

Criar no MySQL um usuário e uma senha para Cacti:

mysql --user=root mysql

mysql> **GRANT ALL ON cacti.* TO cactiuser@localhost IDENTIFIED BY 'suasenha';**

mysql> **flush privileges;**

Edite as linhas abaixo no “/include/config.php” dentro da pasta Cacti descompactada e especifique o usuário MySQL, senha e a base de dados de configuração do Cacti:

nano /www/var/cacti/include/config.php

$database_default = "cacti";
$database_hostname = "localhost";
$database_username = "cactiuser";
$database_password = "cacti";

Vamos ajustar as permissões apropriadas em diretórios dos Cacti para a geração do gráfico/registro. Você deve executar estes comandos do diretório do Cacti internos para mudar as permissões.

chown -R cactiuser rra/ log/

Adicione a linha abaixo dentro de “/etc/crontab” :

nano /etc/crontab

***/5 * * * * cactiuser php /var/www/cacti/poller.php > /dev/null 2>&1**

Pronto, agora abra seu web browser e digite:

http://your-server/cacti/

OBS.: Se tiver utilizando php4, descomente a seginte linha:

nano /etc/php4/cgi/php.ini

extensions=mysql.so;

7.4.4. Configuração

Depis de aberto o borwser aparece a seguinte tela:

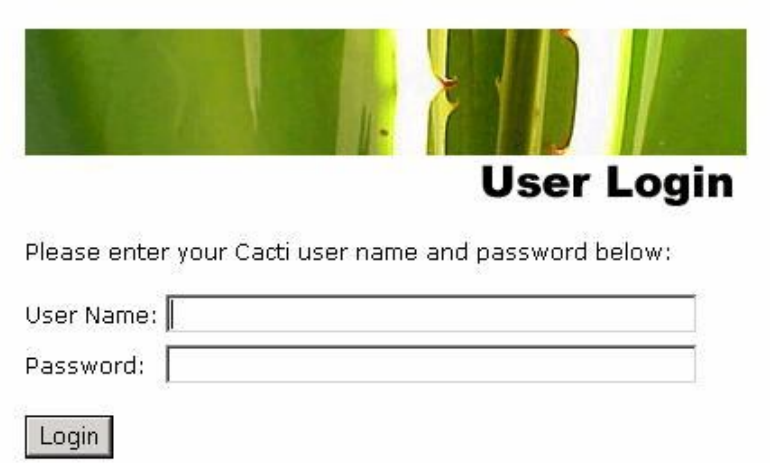

Figura 31: *Autenticação Cacti*

User name : **admin**
Password : **admin**

Irá aparecer outra tela para você informar nova senha de acesso e aparecerão outras telas de configuração, responda elas de acordo com seus parâmetros escolhidos e clique em NEXT.

Pronto agora com o software aberto é só cadastrar dispositivos a serem monitorados.

O Cacti nos fornece a possibilidade de poder personalizar cada gráfico: como mudar as cores dos gráficos, cores de áreas específicas, largura e altura dos gráficos, escala, dentre outros requisitos.

Para isso, no menu da esquerda da página, clique em Graph Templates.

O Cacti nos permite setar configurações personalizadas para cada usuário, permitindo que este apenas visualize o que realmente o interessa. É possível criar novos usuários e também alterar permissões de usuários já existentes. Para isso, no menu esquerdo da tela clique em User Management.

Agora você pode alterar os dados, atribuir uma senha e dar ou retirar permissões para esse usuário. É possível alterar também as permissões de cada gráfico por vez clicando na aba Graph Permissions e as configurações dos gráficos clicando em Graph settings.

Para adicionar um novo usuário, basta clicar em ADD, e setar as configurações as quais desejar.

Para verificar ou alterar algumas configurações do cacti, clique no menu Settings presente no canto esquerdo da tela na guia Configuration.

General

Nessa aba você pode visualizar e alterar as configurações do SNMP, algumas especificações dos arquivos de Log, dentre outros.

Paths

Aqui você pode visualizar os caminhos dos diretórios onde o Cacti guarda seus arquivos, quais os diretórios onde SNMP e o RRDTOOL trabalham, e o path para o arquivo de log.

Poller

Nesse local você encontra as configurações do Poller, pode ativar ou desativá-lo, alterar quais scrips PHP são utilizados, alterar as configurações do Poller Host, dentre outras.

Graph Export

Aqui se encontra as configurações para a exportação de gráficos, como o Tiiming e as configurações dos servidores FTP os quais disponibilizarão as exportações dos gráficos.

Visual

É o local onde você pode alterar o visual do seu gráfico, isto é, alterar a quantidade de linhas a serem mostradas por página para a gerência dos seus gráficos, a quantidade de caracteres máximas por campo, além da possibilidade de se poder alterar as fontes das letras que o RRDtool, incorporado ao Cacti, utiliza nos gráficos.

Authentication

Local onde você pode alterar as configurações da autenticação no cacti, incluindo a possibilidade de se usar o LDAP para fazer a autenticação.

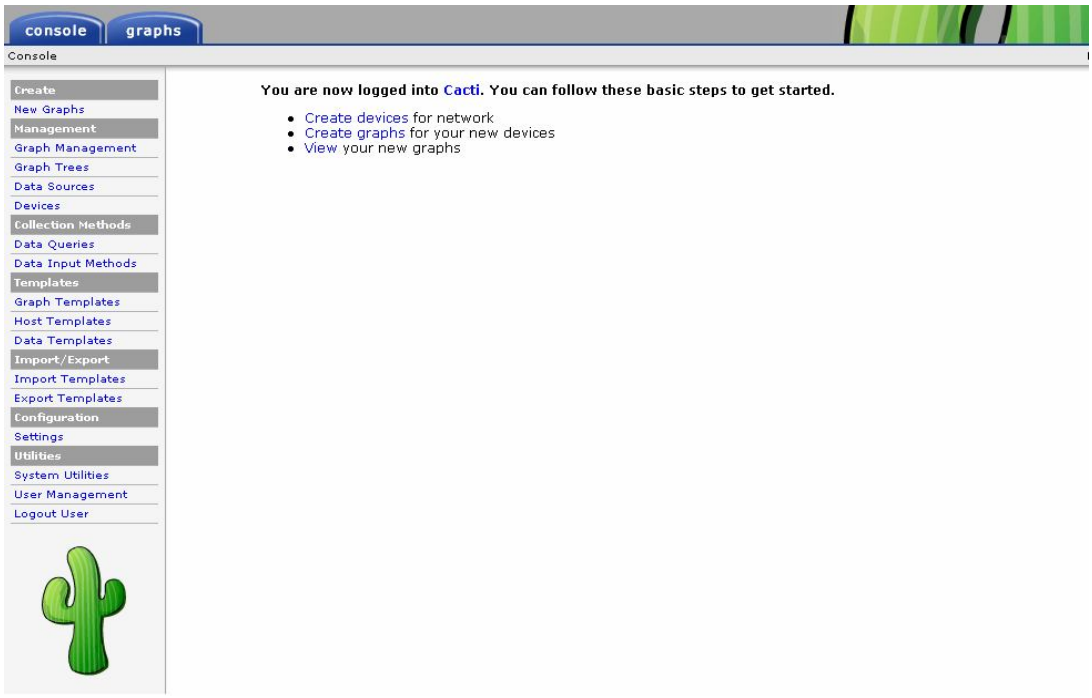

Figura 32: Tela inicial de configuração Cacti

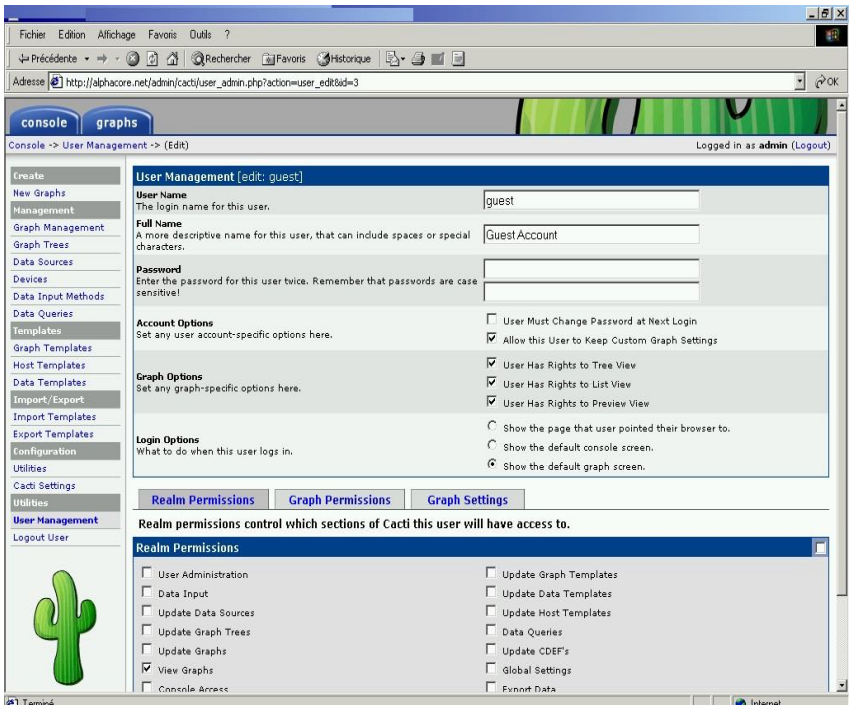

Figura 33: *Cadastro de novo equipamento a ser monitorado*

Figura 34: *Mapa de monitoração*

7.5. NTOP

7.5.1. Definição

Ntop é uma ferramenta software livre, simples de usar e portável com a finalidade de monitoramento e análise de tráfego de rede. Atividades de gerência como: otimização da rede, planejamento e detecção de violações de segurança são algumas características oferecidas por este aplicativo. Este também tem se mostrado uma ferramenta com grande simplicidade por possuir um rápido acesso para monitoramento de redes (baseado em interface web). A grande vantagem de utilizar o ntop é devido a pouca necessidade de esforço e custo (para instalação e aprendizado) comparado a outras complexas e caras (apesar de sofisticados e flexíveis) plataformas de gerência.

7.5.2. Características

No mundo Unix, existe uma ferramenta chamada "top" que é utilizada para mostrar a utilização da CPU pelos processos ativos na máquina. Os autores basearam nessa idéia para a criação do Ntop, pois sentiram necessidade na identificação rápida dos "hosts"(usuários) que estivessem ocupando valiosos recursos de rede.

Ntop oferece interfaces baseados em linha de comando e web com disponibilidade para plataformas Unix-like e Windows.

As principais funções do Ntop são:

- Medição do Tráfego da Rede.
- Monitoramento do Tráfego da Rede.
- Otimização e Planejamento da Rede.
- Detecção de Violações de Segurança da Rede.

A Medição do tráfego consiste em ilustrar a utilização da rede por atividades relevantes. O Ntop acompanha a utilização da rede gerando uma série de estatísticas para cada "host"(cliente) em sua subrede e também por toda as outras subredes. Sendo assim, as informações que se desejam ser adquiridas, são coletadas pelo "host" (cliente com o ntop ativo) simplesmente observando o tráfego da rede. O modelo centrado no cliente favorece uma diminuição das necessidades para processar e adquirir dados de outros nós (computadores) ativos. Todos os pacotes da subrede são capturados e associados a uma tupla "remetente/destinatário", deste modo, é possível acompanhar todas as atividades de um host conectado à uma rede.

A tabela a seguir mostra as informações guardadas pelo ntop para cada host ligado na rede:

Dados Enviados/Recebidos	O tráfego total (por volume e pacotes) gerados ou recebedos pelo host. Classificação de acordo com o protocolos da camada de rede (IP, IPX, AppleTalk, etc...) e protocolos da camada de aplicação (FTP, HTTP, NFS, etc...)
Largura de Banda Utilizada	Valor Atual, a Média ou os picos de utilização da Banda.
IP MultiCast	Quantidade do tráfego multicast gerados ou recebidos pelo host.
Sessões TCP / Histórico	Sessões TCP atualmente ativas, estabelecidas ou aceitas pelo host e estatísticas de tráfego associadas a estas sessões.
Tráfego UDP	Quantidade Total de Tráfego UDP ordenado por portas.
TCP/UDP - Serviços Utilizados	Lista de serviços baseados em IP (ex.: portas abertas ou ativas) fornecidadas pelo host juntamente com uma lista dos últimos hosts externos que utilizaram esses serviços.
Tráfego - Distribuição	Lista do Tráfego Local, Tráfego Local para Remoto, Tráfego Remoto para Local
Tráfego IP - Distribuição	Tráfego UDP x TCP, distribuição relativa do protocolo IP de acordo com o nome do host.

O Ntop além de capturar dados locais do host (cliente com o ntop instalado), ele também gera relatório estatístico do tráfego global da rede. A tabela a seguir mostra os dados que o Ntop consegue capturar:

Tráfego - Distribuição	Tráfego local da subRede, local vs remoto, remoto vs local.
Pacotes - Distribuição	Número total de Pacotes ordenado por tamanho do pacote, unicast vs broadcast vs multicast e tráfego IP vs não-IP.
Largura de Banda	Atual, média e o pico de uso da Largura de Banda da Rede.
Protocolos - Utilização e Distribuição	Distribuição do tráfego observado de acordo com protocolo e origem/destino(local vs remoto).
SubRede Local - Matriz do Tráfego	Tráfego monitorado entre cada par de hosts da Subrede
Fluxo da Rede	Estatísticas de tráfego para fluxos definidos pelo usuário (Tráfegos específicos de interesse do usuário)

Além dos dados fornecidos acima, a versão testada do ntop (versão 3.2 SourceForge .tgz) permite a adição de plugins para estatísticas detalhadas de protocolos em particular, não presentes na versão básica. Além de tudo isso, Ntop também gera dados sobre o host (rodando Ntop), listando sockets abertos (portas), dados recebidos/enviados e máquinas contactadas em cada processo.

Uma configuração não muito organizada dos hosts pode influenciar negativamente toda a performace de uma rede. Ntop permite que administradores identifiquem potenciais focos de uso improdutivo da largura de banda da rede. Os principais fatores para o desperdício de serviço disponível podem ser relacionados ao uso de protocolos desnecessários e má eficiência por problemas de roteamento. De forma indireta; podemos, pela caracterização e distribuição do tráfego da rede, fazer uma revisão das políticas para que obtenha um uso mais inteligente da largura de banda disponível.

Em redes de computadores, as maiorias dos ataques ocorrem de dentro da própria rede. Por esta razão Ntop fornece aos usuários serviços para acompanhamento de ataques e identificação de potenciais furos na segurança da rede (Ex.: ip Spoofing, ataques de negação de serviço, trojan horses , ataques de varredura de portas e redes em modo promíscuo fazendo sniffing).

Quando uma violação de segurança ou má configuração da rede é detectada, Ntop oferece facilidades para gerar alarmes para o gerente de rede (via email, SNMP traps ou pequenos sistemas de envio de mensagem) e também de executar determinadas ações (se possível) com o objetivo de bloquear o ataque. Isso também possibilita manter a informação do tráfego armazenada em um banco de dados, esses registros podem ser usados para entender o ataque e previnir de futuros acontecimentos semelhantes.

É bem importante notar que Ntop, assim como outras ferramentas de monitoramento, pode permitir que furos na segurança não sejam identificados caso o aplicativo não esteja instalado corretamente. Ntop oferece uma interface web na qual permite qualquer usuário com acesso web ler as informações fornecidas/geradas pelo ntop, adquirindo conhecimento sobre a rede, revelando situações antes não identificadas.

7.5.3. Instalação

Ntop está atualmente na versão 3.2, distribuido sob a GPL (GNU General Public LIcense) e pode ser copiado do site oficial do Ntop pelo endereço: http://www.ntop.org/download.html

Existem duas formas de instalação do Ntop:

- Código fonte (na qual será compilada para plataformas Unix-like)

- Pacotes binários de acordo com as diferentes distribuições Linux e Sistemas Operacionais existentes. (Linux, IRIX, Solaris, i386/SPARC, Freebsd, etc...)

Como o trabalho é baseado na distribuição Debian, irei abordar a instalação irei e configuração do Ntop 3.2, a partir do código fonte do software.

Pacotes necessários:

- Libgdbm-dev - download via Apt-Get (Mirrors listados abaixo)
- Libpng3-dev - download via Apt-Get (Mirrors listados abaixo)
- Libpcap2 - http://www.firewalls.com.br/tcpdump/release/libpcap-0.7.2.tar.gz
- GD 2.0.33 - http://www.boutell.com/gd/
- Ntop 3.2 - www.ntop.org

Vamos compilar as bibliotecas e aplicativos necessários.

Para instalar a biblioteca libgdbm-dev você deve usar o comando abaixo:

apt-get install libgdbm-dev

E para instalar o Libpng use o comando abaixo:

apt-get install libpng3-dev

Vamos instalar os outros pacotes através do código fonte com as seguintes linhas de comando.

tar -zxvf libpcap-0.7.1.tar.gz
cd libpcap-0.7.1
./configure
make
make install

Para instalar o GD a partir da fonte use os comandos:

tar -zxvf gd-2.0.33.tar.gz
cd gd-2.0.33
./configure
make
make install

Primeiramente, crie um grupo chamado ntop, Crie/Adicione o usuário Ntop ao grupo Ntop e depois descompacte e compile o arquivo digitando:

groupadd ntop
useradd -s /bin/false -d /dev/null -g ntop ntop
tar -zxvf ntop-3.2.tgz
./configure
make
make install

Quando ativado o modo web (ativado por padrão), Ntop inicia seu próprio servidor (setado geralmente na porta 3000). Para acessar o aplicativo pela web, abra seu browser favorito (ex.: firefox) e digite na barra de endereço: http://localhost:3000

Com gráficos gerados se pode observar o tráfego, por exemplo, de saída e entrada do protocolo TCP e verificar e constatar alguma anomalia tal como: tráfego para saída maior do que o gráfico de entrada de tráfego TCP, pode significar que requisições remotas estão acontecendo, ou seja, alguém está capturando informações da sua rede.

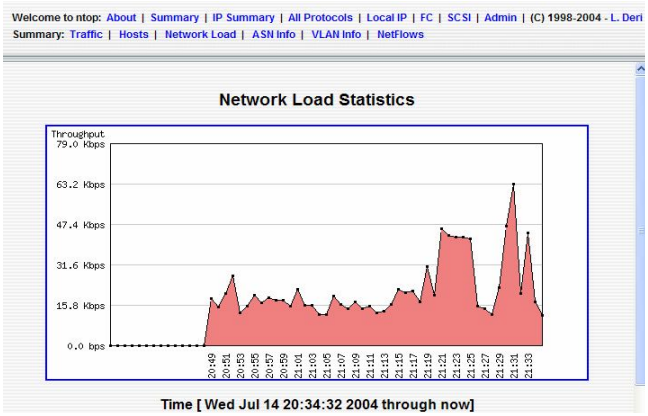

Figura 35: *Gráfico da placa de rede de um dispositivo*

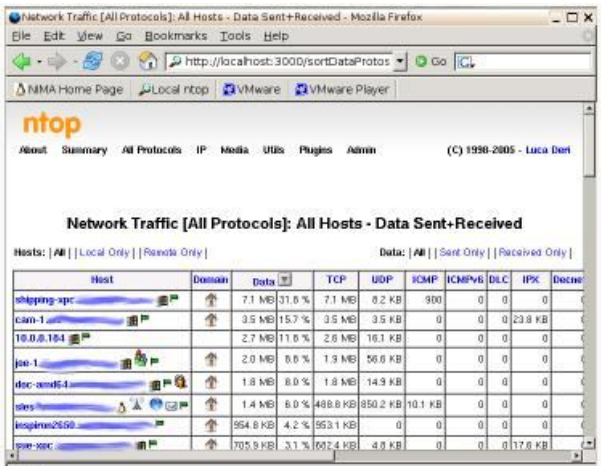

Figura 35: *Protocolos de cada dispositivo encontrado*

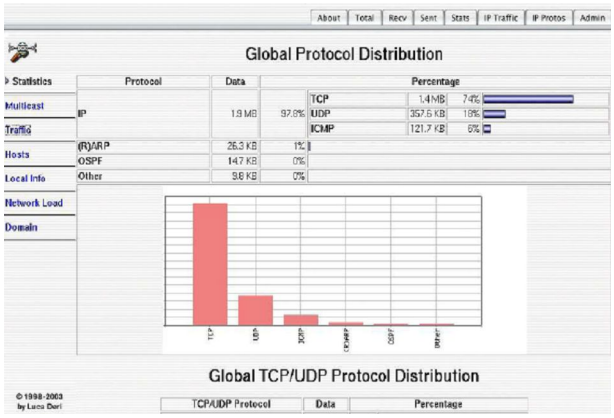

Figura 36: *Estatística consumo de protocolos*

8. CONCLUSÃO

Este trabalho apresentou os conceitos básicos relativos a sistemas de gerenciamento de redes de computadores, destacando a implementação destes sistemas onde a rede já está em pleno funcionamento e algumas ferramentas de monitoração e controle já tinham sido adquiridas. O foco principal foi nas áreas funcionais de gerenciamento de desempenho e de falhas.

A partir do estudo de trabalhos existentes e, considerando o ambiente do PoP-PI, foi proposta uma estratégia para implantação de sistemas de gerenciamento. A questão da seleção das informações que deveriam ser coletadas facilitou a tarefa de monitoração, evitando desperdício de tempo, tornando o sistema ágil e útil.

A utilização de ferramentas automatizadas para a coleta de informações relativas aos componentes principais da rede facilitou a tomada de decisão quanto aos aspectos de configuração da rede e identificação de causas para problemas relativos ao desempenho da rede. A implantação do sistema de gerenciamento de acordo com a estratégia proposta neste trabalho mostrou ser eficiente e o resultado pode ser considerado plenamente satisfatório para os objetivos pretendidos inicialmente.

A solução implementada baseou-se ou em ferramentas de gerência que o PoP-PI já possuía ou em ferramentas de domínio público, demonstrando a viabilidade de implementação de gerenciamento e de disponibilização de informações a custo extremamente baixo. Se por um lado o custo é bastante baixo, por outro lado a precariedade da documentação de algumas destas ferramentas e a falta de suporte técnico pode dificultar o processo de implementação.

Como trabalho futuro, sugere-se o aprimoramento das ferramentas de coleta de informações e a expansão do monitoramento. Tal aprimoramento pode envolver os seguintes aspectos:

- Expansão do monitoramento aos demais equipamentos de rede;
- Implementação de monitoramento sobre servidores e aplicações críticas;
- Modificações da ferramenta visando melhoria de performance;

9. BIBLIOGRAFIA

[1] "Gerência de Redes", Esmilda Saez Artola, http://penta.ufrgs.br/gr952/e_capa.html

[2] "Grupo de Gerência de Redes do METROPOA – PUCRS", http://pucmgmt.metropoa.tche.br/

[3] SNMP Research International, http://www.snmp.org/

[4] SNMP Link, http://www.snmplink.org/

[5] Introdução a Gerenciamento de Redes TCP/IP. "**NewsGeneration**". Rede Nacional de ensino e pesquisa. RNP. http://www.rnp.br/newsgen/9708/n3-2.html, 1997

[6] Ipswitch. **User's Guide**, WhatsUp Gold, versão 8.0, http://www.ipswitch.com/

[7] **MULTI ROUTER TRAFFIC GRAPHER** On-line: URL http://www.mrtg.org

[8] SNMP for the public Community. http://www.wtcs.org/snmp4tpc/

[9] OTSUKA Joice Lee. MIB – management Information base. http://penta.ufrgs.br/gr952/trab1/2capa.html

[10] TANENBAUM, Andrew. **Redes de Computadores**. Primeira Edição. Editora Campus, 1994.

[11] RRDTOOL: http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/

[12] Cacti: http://www.raxnet.net/products/cacti/

[13] Ntop: http://www.ntop.org e http://sourceforge.net/projects/ntop

[14] Nagios http:www.nagios.org

[15] BARTH Wolfgang**, System and Network Monitoring**. **NAGIOS.** Copyright 2006 Open Source Press GmbH

[16] Yahoo, lista de discussão (português) http://groups.yahoo.com/group/nagios-br