FERRAMENTAS PARA GERÊNCIA DE REDES TCP/IP

Antonio Benedito C. Sampaio Junior*.

RESUMO: Ferramentas para gerência de redes proporcionam a monitoração dos serviços fornecidos em uma rede de computadores.

Este trabalho discute duas ferramentas para gerência de redes: a "hopcheck" mostra a rota percorrida por um pacote; e a "netguardian" que mostra os elementos gerenciáveis na rede.

Palavras-Chaves: Gerência de redes, MIB, SNMP, centro de operações da rede (NOC), "hopcheck" e "netguardian".

1. Introdução

Gerência de redes é o processo de controlar uma rede de computadores a fim de maximizar sua eficiência e produtividade, permitindo que seus serviços e seus elementos (equipamentos, dispositivos, programas e meios de transmissão) estejam, simultaneamente, operando de maneira correta e eficiente.

O crescimento cada vez maior na utilização das redes de computadores, exige o planejamento, supervisão, monitoração e controle das atividades na rede, para manter a disponibilidade e eficiência dos serviços oferecidos. Isto deve ser feito através dos administradores da rede e de um conjunto de ferramentas de apoio para o gerenciamento da rede.

Uma das principais necessidades de gerenciamento da rede consiste em realizar tarefas relativamente simples, como saber quem está conectado à rede, ou onde o meio de transmissão está mais carregado e também tarefas mais difíceis de se monitorar, como por exemplo, a detecção de falhas.

Um gerenciamento eficaz aumenta a produtividade, pois garante a qualidade dos serviços oferecidos (sempre confiável e disponível), tendo retorno no investimento feito em equipamentos, aplicativos e treinamento dos usuários.

2. Elementos no Sistema de Gerenciamento de Rede

Uma das formas de se implementar gerenciamento em uma rede de computadores é através da instalação de um software "agente" que busque as informações de gerência nas MIBs (Management Information Bases) das máquinas da rede, conforme ilustra a figura 1.

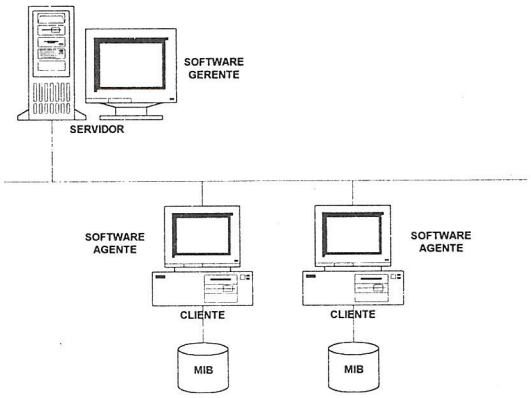


FIGURA1 - EXEMPLO DE UM SISTEMA DE GERENCIAMENTO DE REDE

- **SOFTWARE AGENTE** - É executado em cada um dos nós da rede, servindo para coletar informações da rede e terminais e executar operações sobre os objetos gereciados;
- **SOFTWARE GERENTE** - Localizado no computador servidor da rede e que tem a

* Tecnólogo em Processamento de Dados (Universidade da Amazônia, 1995); Especialista em Redes de Computadores (Universidade Federal do Pará, 1996). Atualmente exerce a função de Professor Assistente I no Departamento de Informática da Universidade da Amazônia.

tarefa principal de obter informações atualizadas sobre os objetos gerenciados e controlá-los. Para isso transmite operações aos agentes;

- **OBJETOS GERENCIADOS** - São os recursos da rede, sujeito ao gerenciamento, tais como uma entidade de camada, uma conexão ou um dispositivo de comunicação;
- **MIB** - (Management Information Base) é o conjunto das informações dos objetos gerenciados da rede. A MIB é estruturada como uma árvore: no topo da árvore estão as informações mais gerais disponíveis na rede; cada galho traz mais detalhes sobre uma área específica na rede e nas folhas da árvores estão as informações.
- **OSI** - (Open System Interconection) é um conjunto de protocolos em camadas baseado em 7 camadas. O protocolo OSI é implementado tanto pelas estações de transmissão como pelas estações de recepção.
- **TCP/IP** - (Transmission Control Protocol / Internet Protocol) a arquitetura Internet TCP/IP dá uma ênfase toda especial à interligação de diferentes tecnologias de redes, baseado em dois protocolos prinipais: TCP e o IP.
- **SNMP** - (Simple Network Management Protocol) é um protocolo projetado para o gerenciamento de redes TCP/IP.
- **CMIP** - (Common Management Information Protocol) é um protocolo projetado para o gerenciamento de redes OSI.
- **ICMP** - (Internet Control Message Protocol) é um protocolo que permite que os roteadores enviem mensagens de erro ou de controle aos outros roteadores.
- **ROTEADOR** - são equipamentos que decidem sobre qual caminho o tráfego de informações (controle e dados) deve seguir em uma rede de longa distância (por exemplo, a Internet).
- **PING** - (Packet Internet Groper) é um programa utilizado em interliagação de redes TCP/IP para testar a alcançabilidade de destinos.
- **SERVIDOR DE COMUNICAÇÃO** - é um computador da rede conectado a um ou mais dispositivos de comunicação (por exemplo, modem), sendo responsável pela interface de comunicação para a rede.

3. Tipos e Modelos de Sistemas de Gerenciamento de Rede

Existem dois tipos genéricos de gerenciamento de redes: proprietários e baseados em padrões.

- **Proprietários** - São baseados em soluções proprietárias do fabricante que desenvolve ferramentas de gerência de hardware e software para gerenciar extensivamente os seus produtos, porém com limitações no gerenciamento de equipamentos de outros fabricantes.

- **Baseados em padrões** - São soluções baseadas na padronização de aplicações de gerência de rede, permitindo o gerenciamento de diversos equipamentos de rede, independente do fabricante. Existem dois tipos de padrões de gerência: CMIP, especificado para o padrão OSI; e o SNMP e SNMP2, especificado para o padrão Internet TCP/IP.

4. NOC - Network Operation Center (Centro de Operações da Rede)

"O NOC pode ser definido como uma coleção de atividades requeridas para manter dinamicamente o nível de serviço em uma rede ou um conjunto de redes. Estas atividades asseguram alta disponibilidade de recursos pelo rápido reconhecimento de problemas e degradação de performance, disparando funções de controle quando for necessário." [TER]

Assim, é possível verificar se o nível do serviço oferecido corresponde ao desejado, retirando informações da rede para verificar a funcionalidade e desempenho da mesma. Estas informações de *status* da rede são retiradas continuamente ou sob demanda e armazenadas no banco de dados da gerência da rede. Com isso é possível verificar se alguma anomalia está ocorrendo.

Deve-se preparar uma série de rotinas

para resolução de problemas, desde uma simples substituição de um dispositivo defeituoso até a execução de ferramentas mais sofisticadas para um diagnóstico mais apurado do problema.

5. Ferramentas para o Suporte do NOC

5.1. HOPCHECK (Ferramenta de Verificação de Rota)

- **CONCEITO**

O Hopcheck é uma ferramenta que mostra a rota percorrida por um pacote de um computador origem para um computador destino, especificando quais os roteadores existentes no percurso e o tempo levado para percorrer cada roteador. É executada através de uma simples linha de comando (hopcheck <identificação (IP) do computador>).

Esta ferramenta, desenvolvida em VC++ por Phil Kahn, pode determinar, por exemplo, qual a rota que um e-mail deverá percorrer. É muito útil num ambiente com muitas rotas, como a Internet, para a determinação de rotas falhas, tais como roteadores intermediários descartando pacotes. Atraso de ida e volta de pacotes entre a fonte e os roteadores intermediários são também reportados permitindo a determinação da contribuição dos roteadores individuais para o atraso da comunicação.

Para que o hopcheck funcione adequadamente, é necessário que um computador IBM Compatível com uma placa de rede Ethernet esteja ligado na Internet, tendo como sistema operacional o windows NT ou windows 95.

Esta ferramenta está disponível gratuitamente no endereço http://www.net-serv.com/cooltool/win95.htm

- **MECANISMO**

A ferramenta Hopcheck utiliza um mecanismo de reportagem de erro através do protocolo ICMP. Para poder determinar quais são os roteadores que receberão o pacote IP transmitido e em quanto tempo, é necessário a utilização de uma variável. Esta variável é conhecida como *time-to-live* (TTL).

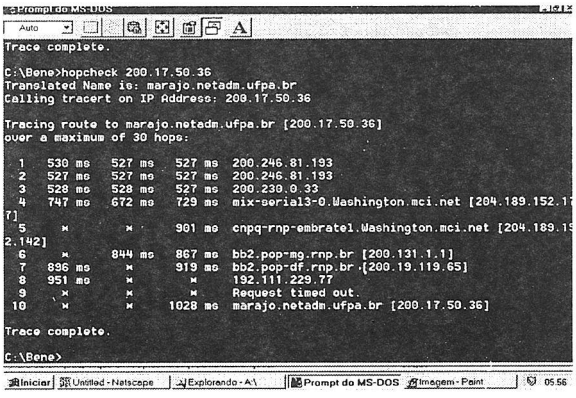
Pelos pacotes transmitidos para um destino com TTL de 0, poder-se-á determinar qual o próximo "salto". Pelo aumento do campo TTL, os "saltos" subsequentes podem ser identificados. Cada pacote transmitido com erro é *time stamped.* O *time stamp* é retornado como parte do pacote ICMP, assim o atraso de ida e volta do pacote pode ser calculado.

- **PROCEDIMENTO**

Foram obtidos as rotas percorridas por um pacote IP durante o intervalo de 17:50h às 18:25h, tendo como computador origem a UNAMA (o servidor de comunicação com IP 200.241.252.226) e computador destino a UFPA (o servidor de comunicação com IP 200.17.50.36). Obtiveram-se quatro tabelas descritas abaixo:

Foi executado o comando hopcheck 200.17.50.36 para verificar a rota do pacote e o tempo desta rota.

Situação1-14/10/97-17:50h



Observa-se que foram executados 10 saltos (hops) entre os roteadores intermediários, obtendo-se o tempo de cada salto. Por exemplo do roteador da UNAMA (200.241.252.225) até o roteador da EMBRATEL (200.246.81.193) são decorridos 527 ms - tempo médio. Da EMBRATEL para o IP 200.230.0.33 são decorridos 528 ms.

Situação2-14/10/97-18:00h

1	527 ms	200.246.81.193
2	528 ms	200.246.81.193
3	530 ms	200.230.0.65
4	877 ms	mix-serial3-0.Washington.mci.net (204.189.152.177)
5	1166 ms	cnpq-rnp-embratel.Washington.mci.net (204.189.152.142)
6	1446 ms	bb2.pop-mg.rnp.br (200.131.1.1)
7	x	Request timed out
8	886 ms	192.111.229.77
9	985 ms	rt1.pop-pa.rnp.br (200.129.132.131)
10	948 ms	marajo.netadm.ufpa.br (200.17.50.36)
11	x	Request timed out
12	906	marajo.netadm.ufpa.br (200.17.50.36)

Nesta segunda situação foram executados 12 saltos entre os roteadores intermediários (nem todos os mesmos da tabela anterior), com tempo superior a situação1.

Situação3-14/10/97-18:15h

1	527 ms	200.246.81.193
2	528 ms	200.246.81.193
3	530 ms	200.230.0.65
4	698 ms	mix-serial3-0.Washington.mci.net (204.189.152.177)
5	755 ms	cnpq-rnp-embratel.Washington.mci.net (204.189.152.142)
6	849 ms	bb2.pop-mg.rnp.br (200.131.1.1)
7	x	Request timed out
8	1003 ms	192.111.229.77
9	x	Request timed out
10	x	Request timed out

11	1020 ms	marajo.netadm.ufpa.br (200.17.50.36)
12	x	Request timed out
13	1023 ms	marajo.netadm.ufpa.br (200.17.50.36)
14	x	Request timed out
15	970 ms	marajo.netadm.ufpa.br (200.17.50.36)
16	901 ms	marajo.netadm.ufpa.br (200.17.50.36)

Nesta terceira situação foram executados 16 saltos entre os roteadores intermediários, sendo que em vários pontos não houve resposta dos mesmos (*Request timed out*), observando um excesso de tráfego neste horário.

Situação4-14/10/97-18:25h

1	527 ms	200.246.81.193
2	528 ms	200.246.81.193
3	530 ms	200.230.0.33
4	771 ms	mix-serial3-0.Washington.mci.net (204.189.152.177)
5	x	Request timed out
6	840 ms	bb2.pop-mg.rnp.br (200.131.1.1)
7	x	Request timed out
8	933 ms	192.111.229.77
9	868 ms	rt1.pop-pa.rnp.br (200.129.132.131)
10	933 ms	marajo.netadm.ufpa.br (200.17.50.36)

Nesta quarta situação foram executados 10 hop saltos entre os roteadores intermediários.

Percebe-se então que um pacote para fluir de um computador origem até outro destino, pela Internet, irá percorrer diferentes rotas definidos pelos respectivos roteadores existentes no caminho. Com o hopcheck é possível o administrador da rede definir um gráfico estatístico, baseado em diversas coletas de testes (como feito acima) em diferentes períodos do dia e da semana, objetivando verificar qual o melhor período para o usuário acessar qualquer informação na Internet, reduzindo assim, a probabilidade de retransmissão das informações.

É interessante observar que o pacote sempre percorre alguns roteadores fixos, no caso o roteador da Embratel que está ligado a UNAMA e a UFPA, e os roteadores intermediários bb2.pop-mg.rnp.br e o bb2.pop-df.rnp.br. Isto pode ser explicado através do mapa de backbone da RNP (Rede Nacional de Pesquisa) que interliga as universidades brasileiras.

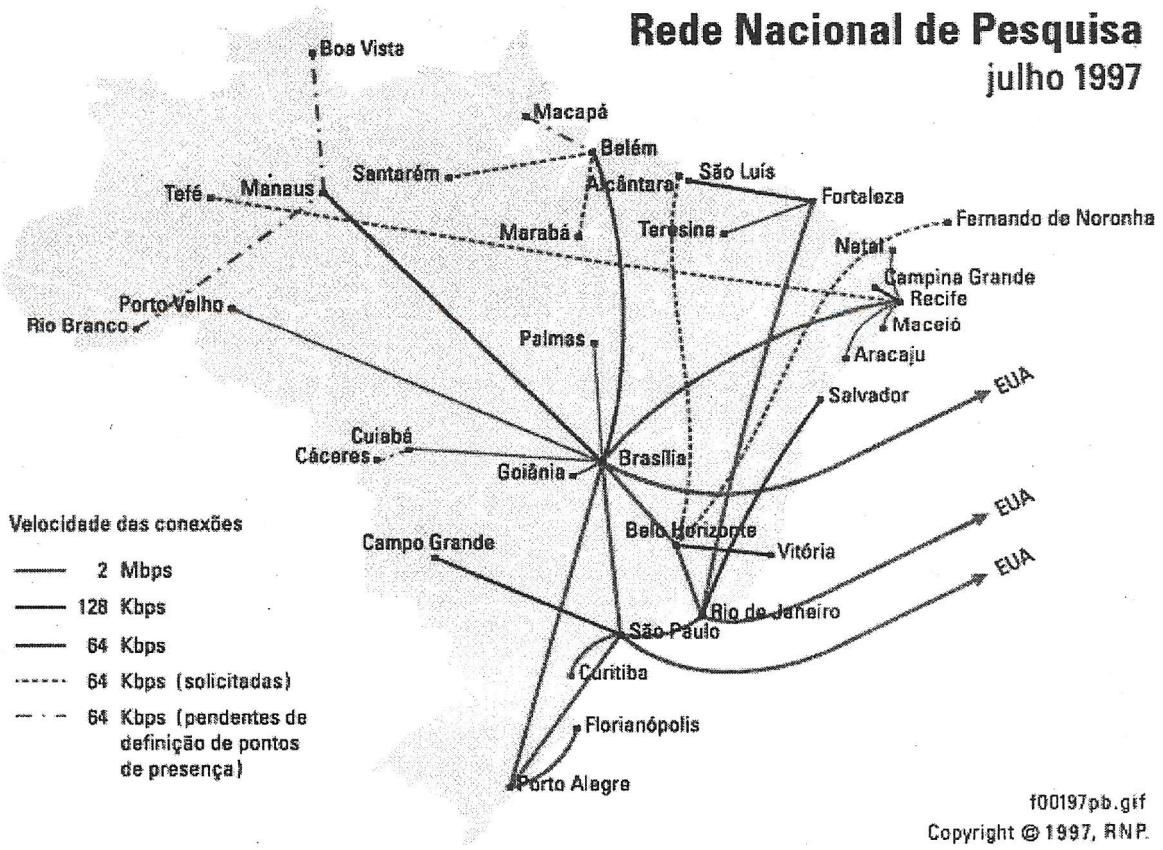


FIGURA2 - BACKCONE RNP (WWW.RNP.COM.BR)

Pela Figura2 percebe-se que existe uma rota fixa entre Belém / Brasília (link 128 Kbps - linha azul), Brasília / Belo Horizonte (2 Mbps - linha vermelha), Belo Horizonte / Rio de Janeiro (2 Mbps - linha vermelha) e Rio / EUA (Washington) a 2Mbps. Então compreende-se o por que destes dois rotadores fixos entre a rota.

Interessante observar que neste exemplo, para mandar um pacote da UNAMA para UFPA, o mesmo sobe até Washington e desce, provavelmente pelo diferente tipo de ligação entre a UNAMA - EMBRATEL e a UFPA - EMBRATEL, ou seja, apesar destas duas instituições estarem separadas por alguns Kilômetros, é necessário percorrer um rota mais demorada e dispendiosa, por não haver uma comunicação direta. Entretanto, esta comunicação direta só existirá no dia em que o tráfego de dados entre as duas instituições for suficiente para viabilizar este investimento de interligação.

5.2. NETGUARDIAN (Ferramenta de Gerência de Grupo de Objetos)

- **CONCEITO**

A ferramenta NetGuardian, é utilizada para auxiliar os gerentes de rede em suas tarefas básicas de monitoramento e análise de tráfego em elementos gerenciáveis da rede. Estes elementos podem ser o servidor de comunicação e o roteador, por exemplo. Para que se tenha acesso as configurações e ao funcionamento dos elementos que estão sendo observados, é necessário que se tenha permissão.

Essa ferramenta foi produzida por alunos do curso de Ciências da Computação, da Faculdade de Ciências, da Universidade de Lisboa. Foi feita em BC ++ 3.1 para windows.

Possui um módulo gerenciador e um módulo agente SNMP para instalar na estação que faz a monitoração. Já vem com a MIB I (RFC

1066), MIB II (RFC 1213), MIB RMON, embutido no programa e permite que se inclua outras MIB's.

Para que o Netguardiam funcione adequadamente, é necessário que um computador IBM Compatível com uma placa de rede Ethernet esteja ligado na Internet, tendo como sistema operacional o windows NT ou windows 95.

O NetGuardian pode ser conseguido via FTP anonymous no endereço ftp.fc.ul.pt/pub/networkinng/snmp/netg2b3.zip, gratuito, ou via WWW no endereço www.di.fc.ul.pt/software/netguard.html.

- **MECANISMO**

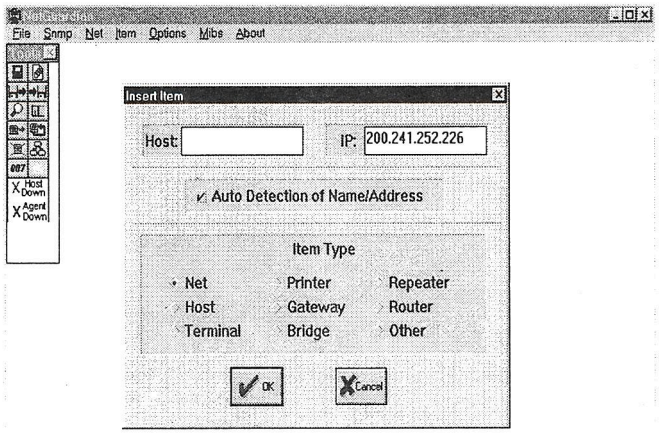
É necessário especificar o endereço IP do elemento que se quer gerenciar. Feito isto o Netguardian envia um ping para o elemento e produz um mapa da rede.

- **PROCEDIMENTO**

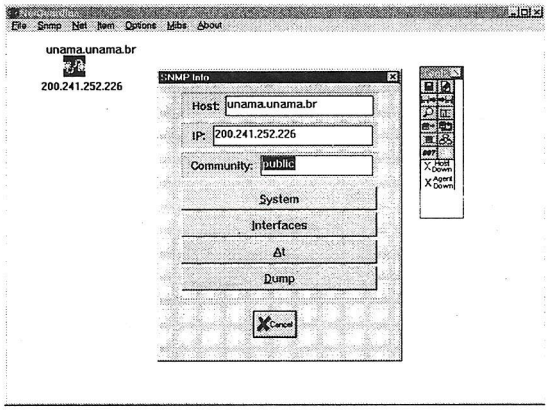
Foi feita a observação dos elementos que compõem a rede da UNAMA (o servidor de comunicação com IP 200.241.252.226 e S.O WINNT4.0) gerenciável SNMP.

Percebe-se que o Netguardian procura o elemento da rede que possui o IP 200.241.252.226. Isto é feito através de um ping. Se o objeto responder, então é mostrado um ícone com o objeto (provavelmente o nome referente ao IP especificado), conforme as situações 1 e 2.

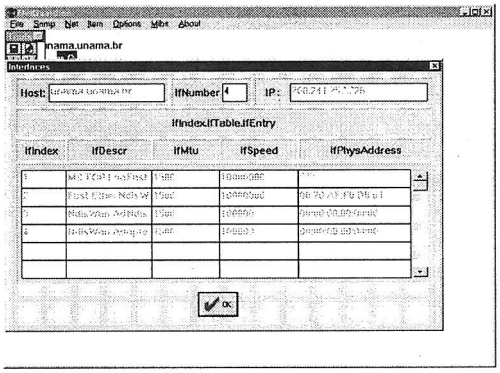
Situação 1 - Procurando o objeto que possui o IP 200.241.252.226



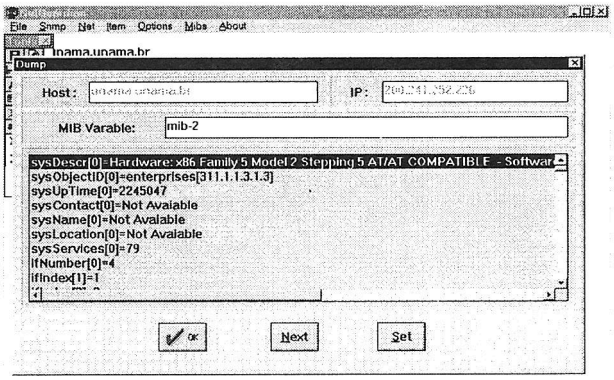
Situação 2 - Encontrou o objeto (Servidor unama.unama.br). Mostra o ícone do objeto.



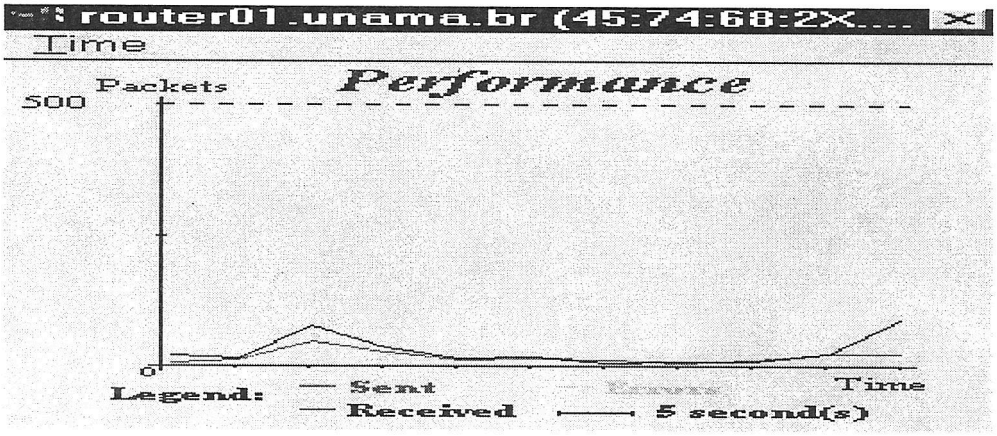
Situação 3 - O número de interfaces do servidor WWW da UNAMA. (São 4 interfaces, sendo duas a 10Mbps).



Situação 4 - Objetos da MIBII do Servidor unama.unama.br



Pode-se também determinar a performance em tempo real do objeto (neste caso o roteador unama.br) gerenciado.



6. CONCLUSÃO

Com o desenvolvimento e crescimento da tecnologia de interconectividade, onde diversos computadores distribuídos fisicamente trocam informações e compartilham recursos, forma-se uma malha viária de informações digitais de abrangência global, como é o caso da Internet.

Para que todos possam acessar esses recursos de forma eficiente, é necessário o estabelecimento de padrões para cada serviço fornecido e ferramentas de gerência destes serviços. Este trabalho teve como objetivo mostrar e classificar gerência de redes, verificando como são classificados os diversos elementos que compõem um sistema de gerência de redes e utilizando duas situações de pesquisa com ferramentas do centro de operações da rede (NOC). Entretanto, percebe-se que atualmente existem os mais diversos tipos de ferramentas, desde o "freeware" (utilizados neste trabalho) de uso limitado a um determinado serviço e os proprietários utilizados em ambientes mais complexos, onde o perfeito gerenciamento representa economia nos custos e melhora nos serviços, como por exemplo ferramentas proprietárias: HP OpenView, IBM NetView/6000, Novell Network Manegement System (NMS), entre outros. Dependendo da ambiente computacional existente e do tipo aplicação requerida, a correta aplicação destas ferramentas será fundamental no desenvolvimento de sistemas mais confiáveis no tratamento de informações.

7. BIBLIOGRAFIA CONSULTADA

CARVALHO, Teresa Cristina. **Gerenciamento de Redes**. Ed. Brisa, 1997.

LEINWAND, Allan; KAREN, Conroy. **Network Management: a pratical perspective** - Addison Wesley - 1996.

TAROUCO, Liane Margarida Rockenbach. **Curso de Gerência de Redes de Computadodores**. Disponível por http://ww.penta.ufrgs.br/gere97/gereunama.htm

PROENÇA JR, Mario Lemes. **Ferramentas para o Noc: NetGuardian**. Disponível por http://penta.ufrgs.br/uel/mario/marioro.htm

CAMPOS, Vitor Valério de Souza. **Ferramentas para o Noc: Hopcheck**. Disponível por http://penta.ufrgs.br/uel/valerio/homenw3.htm