UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CURSO DE ESPECIALIZAÇÃO EM TECNOLOGIAS, GERÊNCIA E SEGURANÇA
DE REDES DE COMPUTADORES

MOISÉS KOCH

Uma Proposta de Solução de Gerenciamento de Contabilização utilizando Nagios e Cacti

Trabalho de Conclusão apresentado como requisito parcial para a obtenção do grau de Especialista

Prof. Dr. Lisandro Zambenedetti Granville
Orientador

Prof. Dr. Sérgio Luis Cechin
Prof. Dr. Luciano Paschoal Gaspary
Coordenadores do Curso

Porto Alegre, dezembro de 2008.

AGRADECIMENTOS

Ao Criador, Arquiteto do Universo, que inventou a vida, desenhou a Terra e deu ao homem a capacidade de aprender e de se aventurar pela maravilhosa jornada do conhecimento.

Aos meus pais, que me deram a mais valiosa das oportunidades: a de viver.

À minha esposa, sempre compreensiva e companheira, renunciando ao tempo que podíamos passar juntos.

Aos professores, pela dedicação e presteza em compartilhar informações e experiências.

Ao meu orientador, Lisandro Granville, pela sinceridade, pelo jeito acessível e pelas sugestões práticas e muito pertinentes.

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS

ASN.1	Abstract Syntax Notation One
CBC	Cipher Block Chaining
DES	Data Encryption Standard
HMAC	Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
ISO	International Organization for Standardization
MAC	Media Access Control
MIB	Management Information Base
NNTP	Network News Transfer Protocol
OID	Object Identifier
PDU	Protocol Data Unit
POP3	Post Office Protocol 3
RMON	Remote Network Monitoring
SMI	Structure Management Information
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USM	User Security Model

LISTA DE FIGURAS

LISTA DE TABELAS

RESUMO

Esta monografia apresenta uma proposta de solução de gerenciamento para uma rede local de computadores, a partir do gerenciamento de contabilização. Depois de fazer uma breve revisão dos principais tópicos de gerência de redes, o trabalho concentra-se em gerenciamento de contabilização, descrevendo os princípios desta área funcional do gerenciamento e ferramentas. Além disso, também apresenta um estudo de caso com a utilização das ferramentas Nagios e Cacti, bem como uma análise dos resultados obtidos.

Palavras-Chave: redes de computadores, gerenciamento de redes, gerenciamento de contabilização, Nagios, Cacti.

An Accounting Management Solution with Nagios and Cacti

ABSTRACT

This document aims at showing a management solution to a local area network, from the perspective of accounting management. After a short review of the main topics in the computer network management field, the work focus attention in account management, describing its capabilities and tools. Also, it shows a study with the deployment of Nagios and Cacti tools, as well as an analysis of the associated results.

Keywords: computer network, network management, accounting management, Nagios, Cacti.

1 INTRODUÇÃO

O universo das redes de computadores ocupa um lugar cada vez mais importante nesta era de crescente popularização da Internet. Hoje, parece impossível conceber um modelo de negócios que exclua o computador e, por conseqüência, uma rede de computadores com acesso à Internet. Mas além de existir, uma rede normalmente compartilha uma série de recursos, oferece serviço de correio e permite que seus usuários naveguem em páginas Web, entre outros. Como saber se o correio está funcionando? Como saber quanto de banda os usuários estão consumindo nos períodos de maior utilização do enlace com a Internet? Em que horas do dia isso ocorre? E se a conexão com a Internet cair, quanto tempo o administrador demorará para saber?

Em outras palavras, uma rede precisa, além de oferecer recursos e serviços, ser também rápida e segura e, sobretudo, estar sempre disponível. Como alcançar esses objetivos? O gerenciamento de redes vem justamente suprir esta necessidade, ou seja, fornece os instrumentos para que o administrador da rede consiga manter a rede funcionando o maior tempo possível, com o mínimo de interrupções. Com o auxílio do gerenciamento de redes, o administrador poderá, de forma mais adequada, atender as expectativas dos usuários e satisfazer as necessidades de uma corporação.

Por isso, esta monografia considera esse relevante assunto da Ciência da Computação, primeiramente por revisar brevemente os principais aspectos do gerenciamento de redes, tais como sua definição, seu modelo de funcionamento, suas áreas funcionais, sua estrutura e o seu principal protocolo: o SNMP (*Simple Network Management Protocol*). Isso será visto no capítulo 2.

Num segundo momento, por abordar com mais detalhes uma área específica do gerenciamento de redes: o gerenciamento de contabilização. Esse tópico enfocará as ferramentas de monitoração, com ênfase em duas delas: Nagios e Cacti. Isso será considerado no capítulo 3.

No capítulo 4, será apresentado um estudo de caso com a utilização das duas ferramentas já mencionadas. O estudo de caso inclui uma proposta de solução de gerenciamento, sua implantação e análise dos resultados bem como da solução proposta.

2 GERENCIAMENTO DE REDES E SNMP

As redes de computadores e seus sistemas têm se tornado cada vez mais importantes no mundo dos negócios. À medida que uma dada empresa cresce, a rede também cresce em tamanho e complexidade, suportando mais aplicações e mais usuários. Quando isso acontece, dois fatos ficam evidentes:

- A rede e seus recursos, bem como as aplicações disponíveis, passam a ser indispensáveis;
- Há uma maior probabilidade de ocorrerem falhas, deixando a rede ou parte dela inoperante, ou degradando o desempenho a um nível inaceitável (STALLINGS, 1999).

Uma rede grande não pode ser bem gerenciada apenas pelo esforço humano. É necessário o uso de ferramentas a fim de facilitar e automatizar o gerenciamento. Para suprir tal necessidade foi criado o **Simple Network Management Protocol (SNMP)**. O SNMP provê um conjunto de padrões para gerenciamento de redes, e foi adotado como padrão para gerenciar redes TCP/IP (STALLINGS, 1999) [**grifo do autor**]. As principais características do SNMP serão consideradas na seção 2.4.

2.1 Definição

A essa altura, é pertinente a pergunta: o que é gerenciamento de redes? Em (KUROSE, 2006), há uma analogia com outras situações do mundo real que ilustram bem o conceito de gerenciamento de redes. Por exemplo, a cabine de um avião tem vários instrumentos por meio dos quais o piloto pode monitorar e controlar o funcionamento da aeronave. Ele pode checar os freios, a altitude e o nível de combustível, entre outros. Assim, o piloto “administra” o avião, por analisar os dados obtidos remotamente. Caso algo não esteja de acordo, ele pode fazer ajustes ou tomar ações corretivas, como mudar a rota de vôo. De forma similar, o gerenciamento de redes consiste em monitorar os recursos da rede, analisar resultados e tomar ações para corrigir ou antecipar falhas. Em palavras simples, portanto, gerenciamento de redes significa o conjunto de ações e procedimentos necessários para manter uma rede sempre funcionando, de preferência a contento.

Pensando de forma estruturada, a ISO dividiu o gerenciamento de redes em 5 áreas funcionais: gerenciamento de falhas, gerenciamento de configuração, gerenciamento de contabilização, gerenciamento de desempenho e gerenciamento de segurança.

2.1.1 Gerenciamento de Falhas

Para manter uma rede funcionando, o administrador da rede deve cuidar para que o sistema como um todo, e também cada componente individual, esteja operando normalmente. Quando ocorre uma falha, é importante que o administrador da rede possa agir rapidamente para:

- Determinar exatamente onde está o problema;
- Isolar o resto da rede para assegurar que a mesma continue operando normalmente sem interferências;
- Fazer ajustes na configuração da rede para minimizar o impacto causado pela falha;
- Reparar ou substituir o componente com falha para restabelecer a rede ao seu estado normal.

Muito importante para a área de gerenciamento de falhas é o conceito de falha. Falha não é o mesmo que erro. Uma falha é uma condição anormal que exige uma ação de gerenciamento, enquanto que um erro é um evento único. Em geral, uma falha é ocasionada pela incapacidade de operar normalmente ou por excessiva quantidade de erros (STALLINGS, 1999).

2.1.2 Gerenciamento de Configuração

Modernas redes de comunicação são formadas de componentes individuais e subsistemas lógicos, que podem ser configurados para executar diversas aplicações. Uma máquina Linux, por exemplo, pode ser configurada para atuar como um roteador ou como um servidor, ou como ambos. Uma vez definido isso, o administrador pode escolher a configuração mais adequada para a situação, considerando parâmetros e valores.

O gerenciamento de configuração preocupa-se com a inicialização da rede e com o *shutdown* dos recursos. Também se dedica a manter, adicionar e atualizar as ligações, físicas e lógicas, entre os diversos equipamentos, bem como o estado dos mesmos durante a operação da rede.

2.1.3 Gerenciamento de Contabilização

Em muitas redes corporativas, o uso dos serviços de rede é “cobrado”, por assim dizer. Na verdade, trata-se de procedimentos contábeis internos, em vez de pagamento com dinheiro real. Por exemplo, cada centro de custo pode ter uma cota de papel para uso de uma fotocopiadora durante um mês. Mas mesmo quando procedimentos dessa natureza não são implementados, o administrador da rede deve ser capaz de monitorar o uso dos recursos de rede por um usuário ou por determinados grupos de usuários. Pelas seguintes razões, dentre outras:

- Um usuário ou um grupo de usuários pode estar abusando de seus privilégios e sobrecarregando a rede, em prejuízo dos demais usuários;
- Usuários talvez estejam fazendo uso ineficiente dos recursos de rede e o administrador pode auxiliar em procedimentos que melhorem o desempenho;

- O administrador da rede tem melhores condições de planejar o crescimento da rede por conhecer bem as atividades dos usuários.

2.1.4 Gerenciamento de Desempenho

Os vários componentes de uma rede de computadores devem comunicar-se entre si e compartilhar dados e recursos. No caso de aplicações ou serviços críticos, como VoIP, a rede precisa oferecer um desempenho dentro de certos limites para que a comunicação flua sem problemas.

O gerenciamento de desempenho abrange duas grandes categorias funcionais: monitoramento e controle (STALLINGS, 1999). Monitoramento é a função de observar as atividades da rede. A função de controle possibilita que se façam ajustes para melhorar o desempenho da rede. Algumas das questões envolvendo desempenho, com as quais o administrador da rede deve se preocupar são:

- Qual é a capacidade da rede quando se fala em desempenho?
- O tráfego atual é excessivo?
- A vazão tem diminuído para níveis inaceitáveis?
- Existe algum gargalo?

Por mensurar os recursos e associar métricas apropriadas a eles, o administrador da rede pode analisar os resultados e estabelecer os níveis de desempenho aceitáveis, estando apto a detectar mudanças no comportamento da rede e tomar providências caso isso seja necessário.

2.1.5 Gerenciamento de Segurança

A área de gerenciamento de segurança tem seu foco em proteção das informações e controle de acesso. Senhas e outras informações de autorização devem ser mantidas e distribuídas. Deve-se também monitorar e controlar o acesso aos computadores da rede, assim como coletar e examinar os registros de auditoria e de *log*, bem como desabilitar ou habilitar esses registros.

2.2 Modelo Geral

O modelo de gerenciamento de rede usado em redes TCP/IP é composto pelos seguintes elementos:

- Estação de gerenciamento – Gerente
- Agente
- Base de informações de gerenciamento – MIB (*Management Information Base*)
- Protocolo de gerenciamento – SNMP (*Simple Network Management Protocol*)

2.2.1 Gerente

A estação de gerenciamento serve como uma interface para o gerente humano (administrador) se comunicar com a rede. A estação de gerenciamento é uma plataforma e deve contemplar pelo menos quatro itens:

- ✓ Um conjunto de aplicações de gerenciamento para análise de dados, recuperação de falhas, etc.;
- ✓ Uma interface por meio da qual o administrador da rede possa monitorar e controlar a rede;
- ✓ A capacidade de traduzir as solicitações do gerente humano para o sistema e controlar os elementos remotos na rede;
- ✓ Uma base de informações coletadas das MIBs de todos os elementos gerenciados na rede.

2.2.2 Agente

Qualquer dispositivo que se conecte a uma rede pode ser equipado com um agente SNMP. Por exemplo, switches, roteadores, estações de trabalho e impressoras, podem executar um agente e assim ser controlados a partir da estação gerente. Um agente responde a solicitações de informações feitas pelo gerente e executa ações que este envia, além de poder eventualmente fornecer informações importantes ao gerente de modo assíncrono, ou seja, sem ser solicitado.

2.2.3 Base de Informações de Gerenciamento

Os recursos gerenciados na rede são representados como objetos. Um objeto é um dado variável que representa uma característica do elemento gerenciado, por exemplo: ativo ou inoperante. A coleção de todos os objetos gerenciáveis é chamada de base de informações de gerenciamento – MIB (*Management Information Base*). Existem ainda categorias de objetos que são padronizadas e podem ser utilizadas para gerenciar equipamentos de diferentes fabricantes. O gerente executa o monitoramento recuperando valores dos objetos da MIB.

2.2.4 Protocolo de Gerenciamento

O gerente conversa com os agentes utilizando um protocolo de gerenciamento de redes. Como já dito anteriormente, nas redes TCP/IP este protocolo é o *Simple Network Management Protocol* – (SNMP). O SNMP será descrito em mais detalhes na seção 2.4.

2.3 MIBs

A estrutura das informações de gerenciamento (SMI – *Structure of Management Information*) define o formato geral para a construção de uma MIB. A SMI identifica os tipos de dados que podem ser usados na MIB e especifica quais os recursos que serão representados e nomeados (STALLINGS, 1999).

Todos os objetos gerenciados no ambiente SNMP são organizados de modo hierárquico, em estrutura de árvore. Cada item, ou folha, da árvore representa algum recurso, atividade ou informação relacionada a um elemento gerenciado. Além disso, cada objeto precisa ter um identificador único (OID – *Object Identifier*). Na prática, esse identificador é um número, que serve também como nome para o objeto. O modelo adotado para a representação dos objetos foi criado pela ISO e baseia-se em um subconjunto da linguagem ASN.1, conforme ilustrado na figura 2.1:

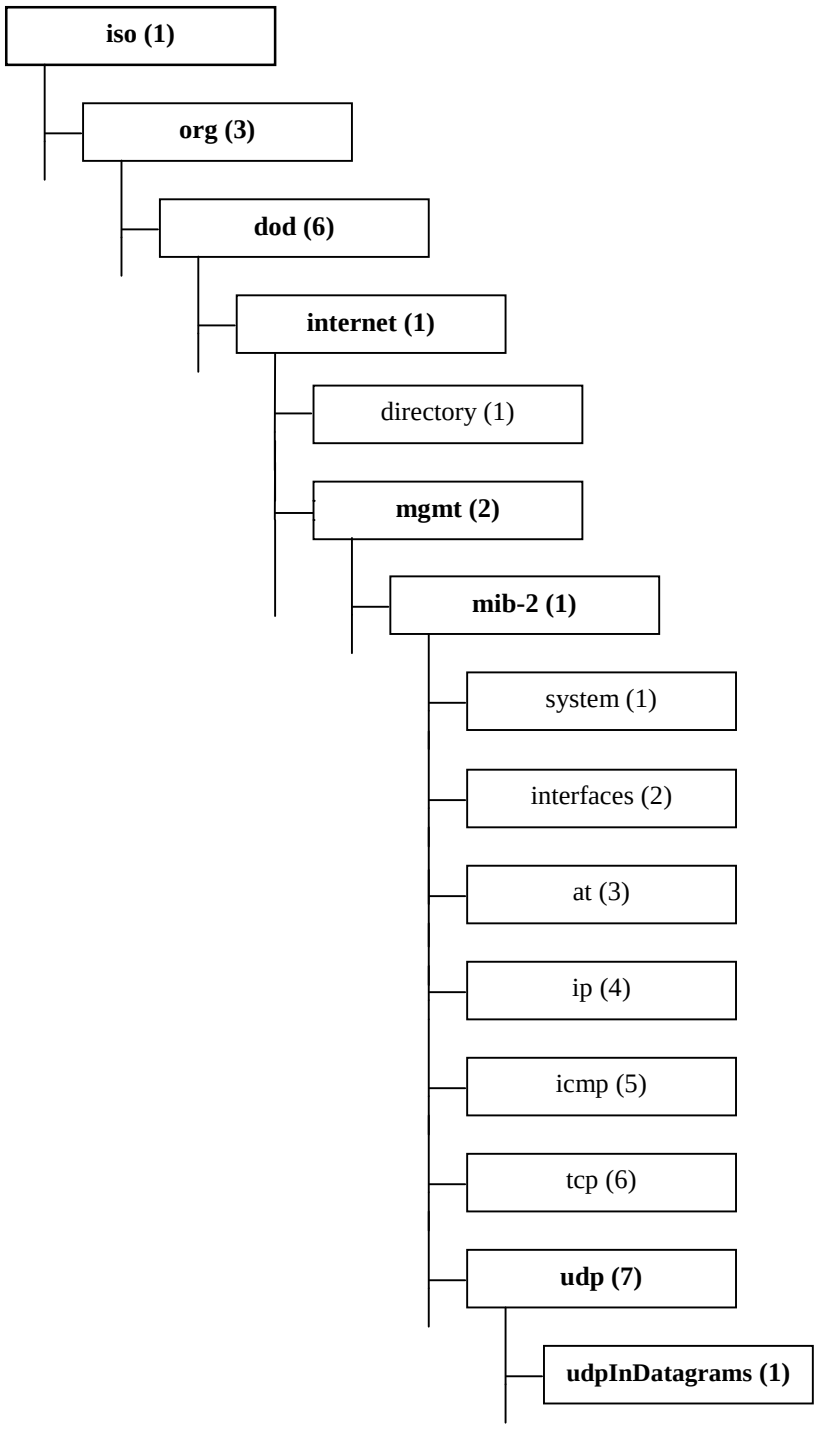

Figura 2.1: Identificador de objeto do grupo UDP

O identificador que representa o número total de datagramas entregues em um nó é derivado como mostra a figura acima. A forma correta de escrevê-lo é: 1.3.6.1.2.1.7.1, e deve ser lido da esquerda para a direita. Esse identificador é único para um objeto.

Assim como há uma série de objetos genéricos, padronizados, existem também objetos específicos, que podem ser definidos pelos fornecedores dos equipamentos. Para os objetos genéricos, existem duas versões da MIB: MIB-I e MIB-II. A segunda é uma

extensão da primeira. Já objetos específicos podem ser adicionados para MIBs proprietárias ou experimentais.

2.3.1 RMON MIB

O surgimento do RMON (*Remote Monitoring*) é um avanço importante no gerenciamento de redes. Ele define uma MIB de monitoramento remoto que complementa a MIB-II e fornece ao administrador da rede importantes informações de toda a rede, e não apenas de equipamentos ou dispositivos individuais. Dessa forma, o RMON fornece uma expansão do SNMP, possibilitando o gerenciamento distribuído.

Um agente RMON é chamado de *probe* (sonda) e possui as seguintes características:

- ✓ Operação offline: deve poder coletar informações mesmo quando não está sendo acessado por um gerente. Estatísticas são armazenadas para acesso futuro pelo gerente;
- ✓ Ter a capacidade de detectar erros e reportá-los. Como uma *trap* SNMP (mensagem de notificação) pode ser perdida, precisa haver um *log* para que o gerente possa examinar eventos passados;
- ✓ Ser capaz de fazer certos tipos de análise dos dados coletados. Exemplo: ordenar os *hosts* de um determinado segmento por ordem de tráfego;
- ✓ Ser controlável por mais de um gerente.

Assim sendo, por monitorar redes locais e interfaces de longa distância, a monitoração remota RMON auxilia na compreensão da rede, permitindo também ao administrador saber de que forma dispositivos locais podem afetar a rede como um todo. O RMON1 tem nove grupos. Como exemplo, o grupo *Statistics* fornece estatísticas Ethernet monitoradas pelo *probe*, e o grupo *Host* apresenta estatísticas dos *hosts* da subrede monitorada. No RMON2, foram adicionados objetos que permitem gerar estatísticas de protocolos de vários níveis (como transporte e aplicação) e serviços de rede. É possível, por exemplo, selecionar pacotes tanto pelo endereço MAC como pelo endereço IP.

2.4 SNMP

O SNMP é o protocolo de gerenciamento de redes utilizado na Internet. É um protocolo do nível de aplicação, que utiliza UDP como protocolo de transporte. Basicamente, o SNMP pode apenas ler ou alterar o conteúdo de variáveis, que são instâncias de objetos gerenciados. Isso é possível por meio de três operações genéricas:

- Get – permite ao gerente consultar informações dos agentes; essa consulta pode ser de dois tipos: *GetRequest*, recupera a primeira informação da lista de informações de um objeto ou *GetNextRequest*, recupera a próxima informação disponível na lista, a partir da última informação solicitada. Para cada *GetRequest* ou *GetNextRequest* enviado pelo gerente haverá uma resposta do agente, um *GetResponse*.

- Set – operação de escrita, permite ao gerente alterar valores dos objetos dos agentes; para cada *SetRequest* executado pelo gerente, o agente também responde com um *GetResponse*.

▪ Trap – possibilita que um agente notifique um gerente sobre eventos significativos, sem que o gerente tenha solicitado.

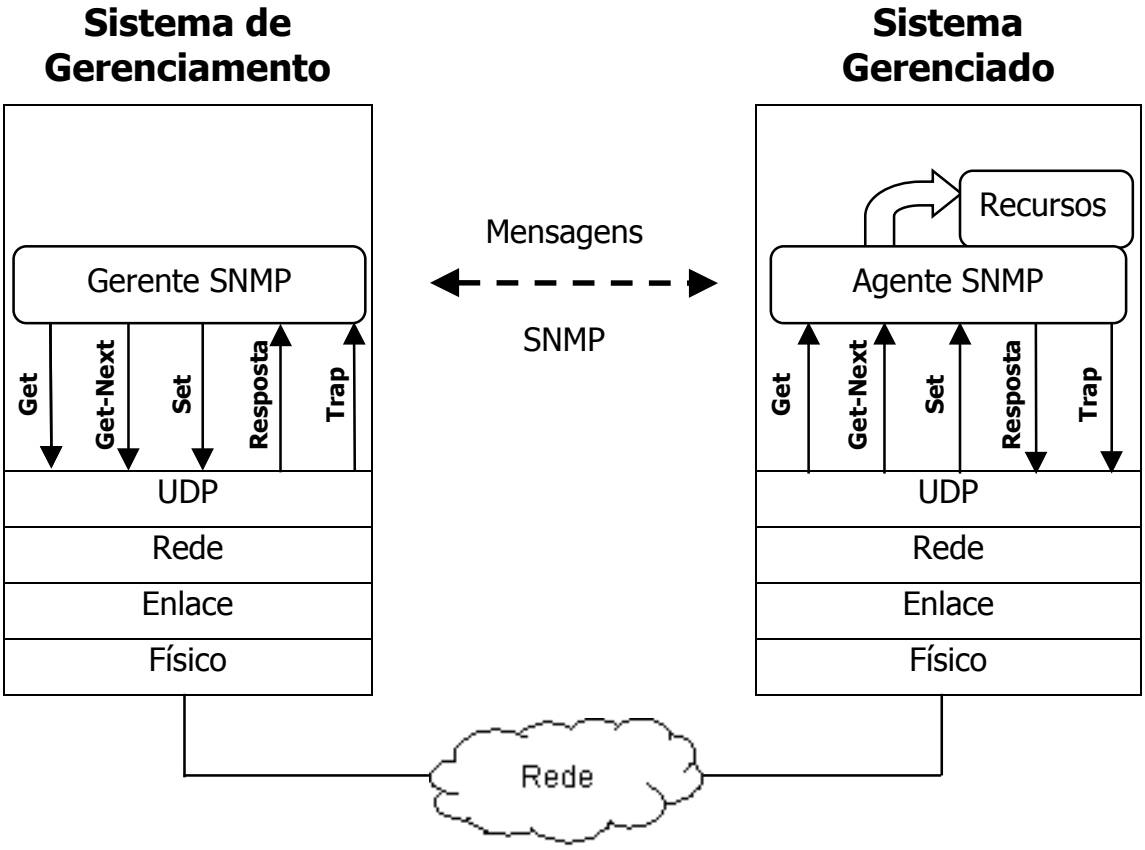

Figura 2.2: Modelo de comunicação entre gerente e agente usando o SNMP

Os agentes SNMP escutam na porta 161 e os gerentes recebem as notificações na porta 162 (STALLINGS, 1999). A mensagem SNMP é formada por 3 partes:

Versão	Comunidade	PDU

Figura 2.3: Formato da mensagem SNMP

Esta primeira versão do protocolo SNMP é caracterizada por operações simples de leitura e escrita. De acordo com a figura 2.2, as informações são trocadas entre um gerente e um agente na forma de mensagens SNMP. Cada uma dessas mensagens, por sua vez, como mostra a figura 2.3, inclui um número que indica a versão do protocolo SNMP; um nome de comunidade, o qual atua como uma senha para a autenticação da mensagem SNMP; e um dos 5 tipos de PDU (*Protocol Data Unit*) possíveis.

Tabela 2.1: Operações do SNMP

PDU	Interação	Descrição
0 – GetRequest 1 – GetNextRequest	Gerente-agente	Solicitação de leitura sobre o conteúdo dos objetos: ▪ Apenas uma instância de objeto ▪ Próximo na lista
2 – SetRequest	Gerente-agente	Altera o valor de um objeto
3 – GetResponse	Agente-gerente	Retorna o valor de um objeto em resposta ao pedido do gerente
4 – Trap	Agente-gerente	Notifica o gerente da ocorrência de um evento excepcional

Se o agente e o gerente estiverem executando a mesma versão do SNMP e se o gerente enviar o nome de comunidade correto, a PDU da mensagem é processada. O campo PDU contém, entre outras coisas, o código que identifica o tipo da PDU, o nome de um ou mais objetos envolvidos na operação e um código de erro. A PDU do tipo *GetRequest* é enviada por um gerente e inclui o nome de um ou mais objetos cujos valores devem ser consultados. Essa operação é atômica: ou os valores de todos os objetos consultados são devolvidos ou nenhum é. A PDU do tipo *GetNextRequest* também é enviada por um gerente e inclui a lista de um ou mais objetos que são predecessores dos objetos a serem consultados. Já a PDU do tipo *SetRequest* é enviada por um gerente para solicitar que um ou mais objetos tenham seus valores alterados. Para esses três tipos de PDU, o agente responde com uma PDU do tipo *GetResponse*, a qual contém os valores dos objetos em questão. Um código de erro associado indica o sucesso ou a falha da operação. Em caso de falha, os valores solicitados não serão enviados.

Tabela 2.2: Erros que podem ocorrer nas mensagens SNMP

Status de Erro	Descrição
0 – noError	Operação bem sucedida
1 – tooBig	PDU GetResponse extrapola limite local
2 – noSuchName	Não existe objeto com o nome solicitado
3 – badValue	Uma PDU SetRequest contém uma variável de tipo, tamanho ou valor inconsistente
4 – readOnly	Compatibilidade SNMP
5 – genErr	Erro genérico

Finalmente, a PDU do tipo *Trap* é diferente de todas as outras. Ela é enviada por um agente para notificar um gerente a respeito de um evento significativo. O campo PDU

contém, entre outras coisas, o nome da empresa, o endereço IP da origem da *trap*, bem como o tipo da *trap* que está sendo gerada (STALLINGS, 1999).

Tabela 2.3: Algumas *traps* do SNMP

Código da Trap	Descrição
0 – coldStart	Equipamento foi ligado
1 – warmStart	Equipamento foi reinicializado
2 – linkDown	Enlace com a Internet caiu
3 – linkUp	Enlace com a Internet foi restabelecido
4 – authenticationFailure	Falha na autenticação

2.4.1 SNMPv2

O SNMPv2 apresenta uma série de melhorias em relação à versão inicial, tais como recuperação de dados mais refinada, maior segurança, suporte a vários protocolos de transporte, tratamento de erros mais preciso e novos tipos de PDU.

Da mesma forma como no SNMPv1, as mensagens no SNMPv2 também apresentam a versão do protocolo, a comunidade e uma PDU. Uma novidade nesta versão, porém, é a possibilidade de interação entre dois gerentes. Isso é possível por meio da nova PDU *InformRequest*. Quando um gerente envia uma PDU do tipo *InformRequest* a outro gerente, recebe como retorno uma PDU do tipo *Response*. As outras interações, gerente-agente e agente-gerente, continuam valendo.

Com relação às PDUs *GetRequest* e *GetNextRequest*, são idênticas em ambas as versões do SNMP, exceto pelo fato de que no SNMPv2 elas não são mais atômicas. Ou seja, em caso de erro na leitura de uma determinada variável, a PDU de resposta enviará um código de erro associado com aquela variável em particular, os demais objetos terão seus valores recuperados normalmente.

2.4.1.1 PDU GetBulkRequest

Uma das melhorias mais significativas no SNMPv2 é a nova PDU *GetBulkRequest*. Seu objetivo é minimizar o número de troca de mensagens do protocolo na recuperação de uma grande quantidade de informações de gerenciamento. Seu princípio de funcionamento é o mesmo da PDU *GetNextRequest*, recuperar as próximas instâncias dos objetos da MIB. A diferença é que com o comando *GetBulkRequest* pode-se especificar o número de sucessores que serão lidos (STALLINGS, 1999).

Essa PDU tem dois campos que não são encontrados em nenhuma outra: *non-repeaters* (que não deve ser repetido) e *max-repetitions* (número máximo de repetições). O primeiro especifica o número de objetos para os quais a consulta deverá retornar apenas um único sucessor, o próximo, exatamente como na PDU *GetNext*. O segundo especifica o número de sucessores a serem recuperados para os demais objetos. A figura 2.4 ilustra como eles podem ser configurados:

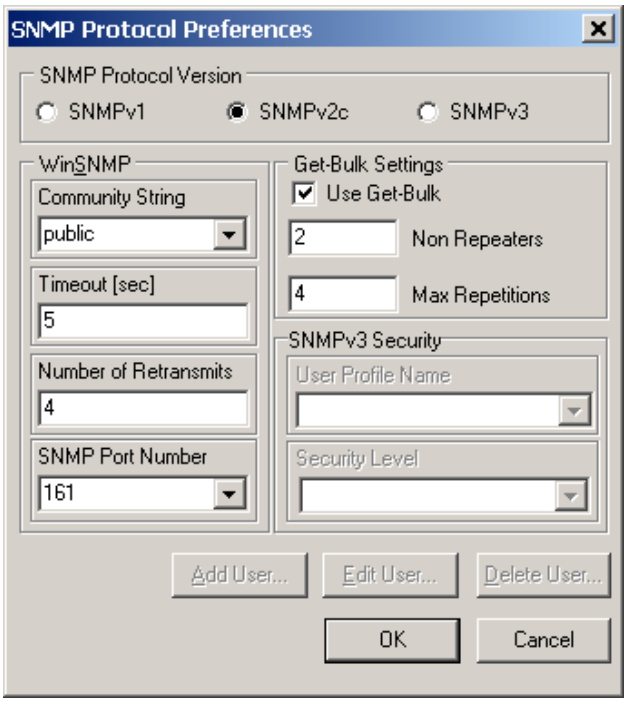

Figura 2.4: Campos parametrizáveis da PDU *GetBulkRequest*

Na prática, o resultado é que, no caso de variáveis com tabelas, estas serão recuperadas linha por linha, em vez de todos os sucessores da primeira variável, depois todos os sucessores da segunda variável e assim por diante. Considerando o exemplo da figura 2.4, o resultado seria:

GetBulkRequest (non-repeaters = 2, max-repetitions = 4, A, B, TX, TY)

Response [A, B, TX(1), TY(1),
TX(2), TY(2),
TX(3), TY(3),
TX(4), TY(4)]

Figura 2.5: Comando *GetBulkRequest*

2.4.2 SNMPv3

O SNMPv3 não é exatamente uma nova versão do protocolo, mas um complemento para as versões atualmente em uso, SNMPv1 e SNMPv2, esta última preferencialmente. Tanto é assim que não há novos tipos de PDU definidos; portanto, uma aplicação desenvolvida para o SNMPv3 deve considerar as PDUs do SNMPv2 mais a infra-estrutura de segurança e administração da arquitetura de gerenciamento do SNMPv3 (STALLINGS, 1998).

A arquitetura do SNMPv3 é modular, sendo que os módulos interagem provendo serviços uns aos outros através de primitivas. Essa arquitetura trabalha com o conceito de entidade. Uma entidade é formada por um *engine*, uma espécie de núcleo que

implementa as funcionalidades básicas do módulo, denominadas funções no SNMPv3, e por aplicações que executam funcionalidades específicas. O processamento da mensagem SNMP é executado pelas funções do despachante e do subsistema de processamento de mensagens, ambos parte do engine SNMP, como mostra a figura 2.6.

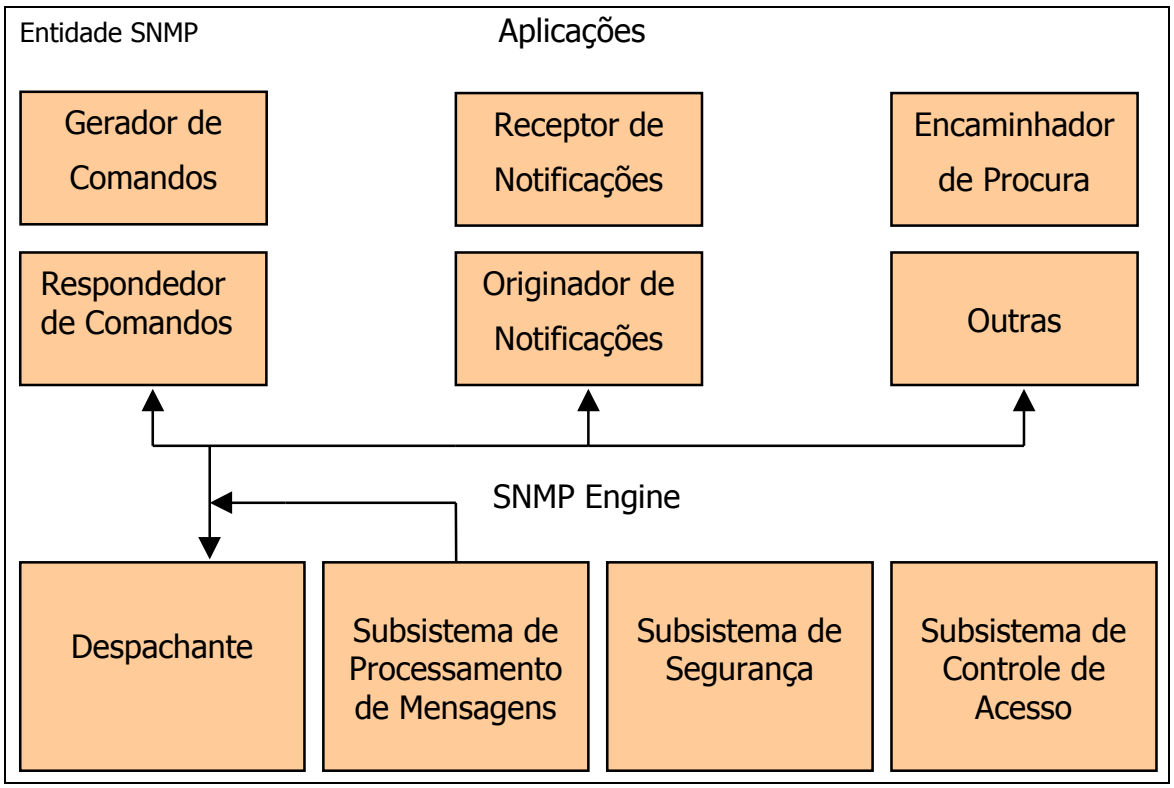

Figura 2.6: A arquitetura modular do SNMPv3

A arquitetura modular do SNMPv3 oferece algumas vantagens. Uma delas é que o papel de uma entidade SNMP é determinado pelos módulos que essa entidade implementa. Por exemplo, alguns módulos são requeridos por um agente SNMP, enquanto que outros são exigidos por um gerente SNMP. Outra vantagem é que essa estrutura modular propicia a definição de diferentes versões de cada módulo. Assim, pode-se melhorar alguns aspectos do SNMP, sem a necessidade de criar uma nova versão do protocolo, como um SNMPv4.

2.4.2.1 Segurança no SNMPv3

O SNMPv3 propõe um modelo de segurança baseado em usuário (USM – *User Based Security Model*), o qual oferece autenticação e serviços de privacidade para o SNMP. O modelo USM provê segurança contra as seguintes ameaças:

- Alteração de informações: em essência, essa ameaça é caracterizada pelo fato de uma entidade não autorizada poder alterar qualquer parâmetro de gerenciamento, inclusive aqueles relacionados com configuração e contabilização;
- Mascaramento: operações de gerenciamento não autorizadas podem ser originadas por uma entidade falsa, que se faz passar por uma entidade válida;

- Alteração do fluxo de mensagens: essa ameaça pode ocasionar o reenvio, a duplicação ou o atraso de mensagens SNMP, com o objetivo de efetuar operações de gerenciamento não autorizadas. Por exemplo, uma mensagem para reinicializar um equipamento poderia ser copiada e reenviada posteriormente;
- Revelação de informações: uma entidade poderia observar trocas de mensagens entre um gerente e um agente e, a partir daí, capturar valores de objetos gerenciados, bem como mensagens de notificação. Por exemplo, a observação de um comando *set* que altera senhas poderia habilitar um atacante a aprender novas senhas (STALLINGS, 1998).

O USM (*User Security Model*) não provê segurança contra ataques de negação de serviço e análise de tráfego. Para tratar as demais ameaças, já mencionadas, o SNMPv3 utiliza funções de criptografia e mecanismos de temporização. A tabela 2.4 resume as principais características de segurança do SNMPv3:

Tabela 2.4: Segurança no SNMPv3

Ameaça	**Aspecto de Segurança Envolvido**	**SNMPv3 Contempla?**	**Mecanismo**
Alteração não Autorizada de Informações	Autenticação	SIM	HMAC (*Hash Message Authentication Code*)Protocolo de autenticação – utiliza algoritmos de *hash* MD5 ou SHA
Mascaramento	Autenticação	SIM	HMAC (*Hash Message Authentication Code*). Protocolo de autenticação – utiliza algoritmos de *hash* MD5 ou SHA
Alteração do Fluxo de Mensagens	Integridade	SIM	Algoritmo de criptografia de chave privada DES (*Data Encryption Standard*) em modo CBC (*Cipher Block Chaining*)
Revelação de Informações	Confidencialidade	SIM	Algoritmo de criptografia de chave privada DES (*Data Encryption Standard*) em modo CBC (*Cipher Block Chaining*)
Negação de Serviço	Disponibilidade	NÃO	
Análise de Tráfego	Confidencialidade	NÃO	

3 GERENCIAMENTO DE CONTABILIZAÇÃO

3.1 Monitoramento de Contabilização

O gerenciamento de contabilização está diretamente ligado ao monitoramento da rede. Especificamente, envolve o registro da utilização dos recursos de rede pelos usuários. As necessidades para essa função variam muito. Por exemplo, um sistema de contabilização interno pode ser usado apenas para avaliar o uso global dos recursos e determinar qual a proporção de utilização de um ou mais desses recursos por cada departamento. Em outros casos, como em sistemas que oferecem um serviço público, é necessário que se faça uma divisão por conta, por projeto, ou mesmo por usuários individuais para efeitos de rateio do custo. Neste caso, a informação colhida precisa ser mais detalhada e mais precisa. (STALLINGS, 1999).

Exemplos de recursos que podem estar sujeitos à contabilização:

- Instalações de comunicações: LANs, WANs e sistemas telefônicos;
- Hardware: estações e servidores;
- Software: aplicações e utilitários de software em servidores, um *data center* e *sites* de usuários finais;
- Serviços: inclui toda comunicação comercial, bem como serviços disponíveis para usuários de rede.

Para cada tipo de recurso, dados de contabilização são colhidos com base nas necessidades da organização. Por exemplo, os seguintes dados de contabilização ligados à comunicação podem ser reunidos e mantidos sobre cada usuário:

- Identificação do usuário: fornecida pelo originador de uma transação ou pedido de serviço;
- Receptor: identifica o componente da rede com o qual a tentativa de conexão será feita;
- Número de pacotes: contagem dos dados transmitidos;
- Códigos de estado da rede: indica a natureza de quaisquer erros que possam ser detectados;
- Recursos utilizados: indica quais recursos são requisitados por uma determinada transação ou evento de serviço.

Assim sendo, o monitoramento de rede para a área de gerenciamento de contabilização preocupa-se em registrar o uso dos recursos no nível de detalhe exigido para a correta contabilização.

3.2 Ferramentas

As ferramentas de gerenciamento são o braço direito do administrador de rede. Sem elas, o administrador seria como um cego andando pelas ruas. Seja um simples comando ou um sistema especializado, elas auxiliam no diagnóstico de erros, resolução de problemas, detecção de gargalos, ou seja, permitem que o administrador "enxergue" a rede e seus componentes, controlando-os ou interagindo com eles quando necessário.

Algumas ferramentas mais simples já vêm embutidas no sistema operacional na forma de comandos como *ping*, *netstat* e *traceroute*. Outras estão disponíveis na forma de aplicações que analisam protocolos, monitoram dispositivos, sistemas e serviços e oferecem recursos que facilitam procedimentos de configuração. Existem ainda plataformas de gerenciamento, que muitas vezes são sistemas distribuídos, compostos de hardware e software específico para realizar as atividades de gerenciamento. Esses sistemas manipulam e organizam dados e os apresentam na forma de gráficos, tabelas ou relatórios.

Não importa qual a ferramenta, ela sempre vai focar em uma ou mais das cinco áreas de gerenciamento descritas nas seções 2.1.1 a 2.1.5; relembrando: gerenciamento de falhas, gerenciamento de configuração, gerenciamento de contabilização, gerenciamento de desempenho e gerenciamento de segurança. No caso do gerenciamento de contabilização, existem ferramentas que registram dados dos recursos monitorados e geram gráficos de apresentação, além de oferecerem outros recursos valiosos.

3.2.1 Ferramenta 1 (e.g., Nagios)

O Nagios é uma aplicação desenvolvida para monitoramento de rede. Ele pode monitorar *hosts* e serviços, enviando notificações de eventos. Ele foi originalmente desenvolvido para Linux, embora funcione também com Unix e com Windows. Algumas de suas principais características são:

- Monitoramento de serviços de rede: SMTP, SAMBA, HTTP, DNS, etc.;
- Monitoramento de recursos de *hosts*: carga do processador, utilização de espaço em disco, utilização de cpu, etc.;
- Notificações quando problemas com serviços ou *hosts* ocorrem e são resolvidos;
- Funcionalidade de definição de eventos que serão disparados durante a ocorrência de eventos de *host* ou serviço, para a resolução pró-ativa de problemas;
- Geração automática de arquivo de log;
- Interface Web para visualização do estado atual da rede, histórico de problemas e notificações, arquivos de log, etc.

É importante salientar que além da área de contabilização, o Nagios atua no gerenciamento de falhas, verificando periodicamente o estado dos recursos monitorados

e enviando alertas caso ocorra alguma falha. E o Nagios é também capaz de notificar o administrador caso os valores de utilização de um determinado dispositivo extrapolem os limites máximos previamente definidos na sua configuração. Por exemplo, caso seja definido que o espaço em disco livre em um servidor não deve ser menor que 10%, um e-mail de alerta poderá ser enviado pelo Nagios caso isso aconteça.

Na página Web do Nagios é possível verificar todas as informações sobre os *hosts* e serviços monitorados, além da configuração geral do sistema. Quando um serviço ou *host* fica indisponível, o Nagios altera o estado e a cor do mesmo, refletindo a atualização na página Web e emitindo um sinal sonoro. Caso haja alguma manutenção programada para um equipamento, é possível desabilitar o serviço de notificação para o *host* correspondente e todos os seus serviços. A figura abaixo apresenta uma visão geral da página Web do Nagios.

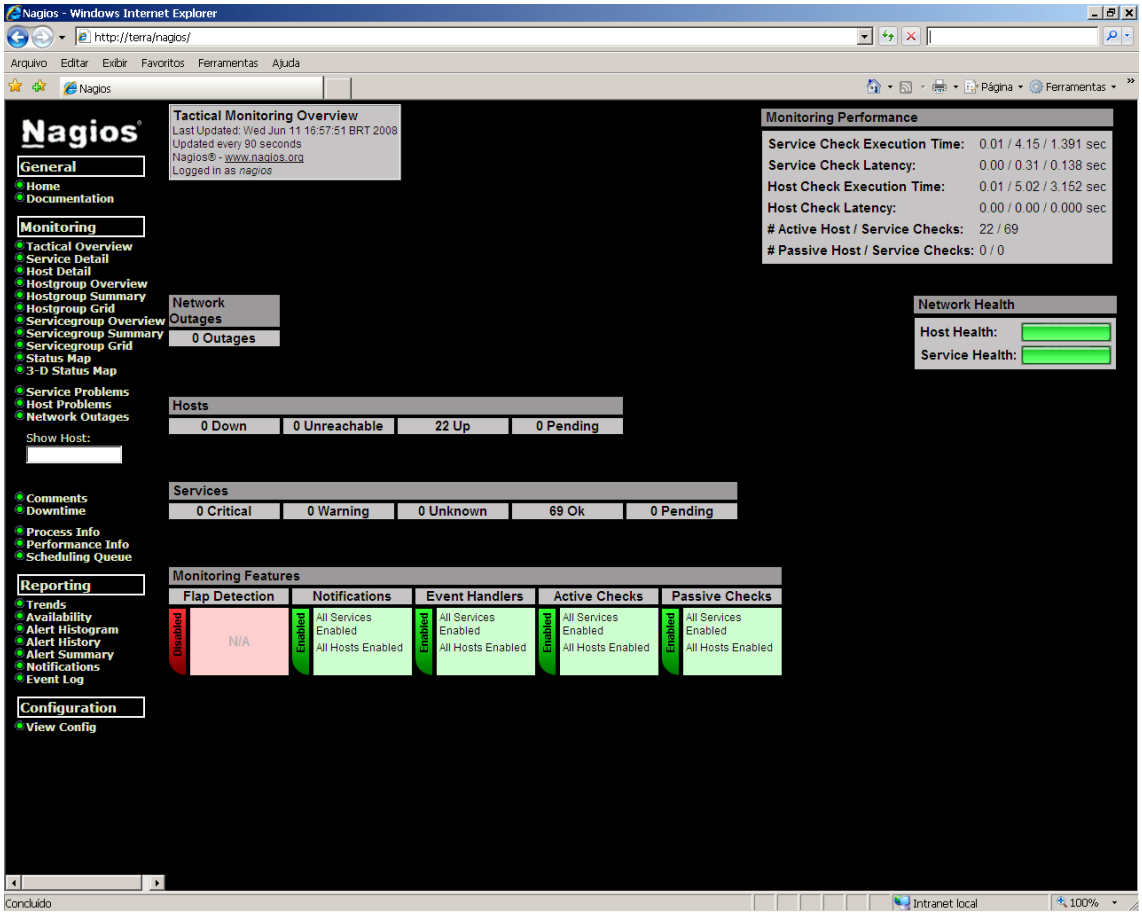

Figura 3.1: A interface Web do Nagios

3.2.2 Ferramenta 2 (e.g., Cacti)

A segunda ferramenta utilizada nesta proposta de solução é o Cacti. Assim como o Nagios, o Cacti é uma ferramenta de monitoramento de rede, porém com enfoque principal em gerenciamento de contabilização. Escrito em PHP, o Cacti atua em conjunto com o RRDtool, um sistema capaz de reproduzir em gráficos as informações dos elementos monitorados. Exemplos de tipos de informação que podem ser monitorados são: largura de banda, e-mails enviados e recebidos, requisições HTTP, média de processos, utilização de memória, entre muitas outras. Os gráficos são gerados em função de intervalos de tempo, produzindo assim um histórico de monitoramento. Vários modelos de *hosts*, de gráficos e de tipos de dados estão disponíveis. As informações coletadas são armazenadas numa base de dados MySQL e podem ser consultadas através da amigável interface Web do Cacti. Os gráficos criados podem ainda ser organizados em árvores. Isso é útil caso haja muitos equipamentos sendo monitorados, que assim ficarão separados, por exemplo, por tipo.

Para que o Cacti possa operar, é necessário que o SNMP esteja instalado no servidor de monitoramento e também nos equipamentos que serão monitorados. E, uma vez que o Cacti trabalha diretamente com SNMP, qualquer informação que este possa recuperar, pode também ser reproduzida no *front end* do Cacti. Além disso, é possível criar scripts e configurar o intervalo de tempo de obtenção dos dados, além dos tradicionais dia, semana, mês e ano.

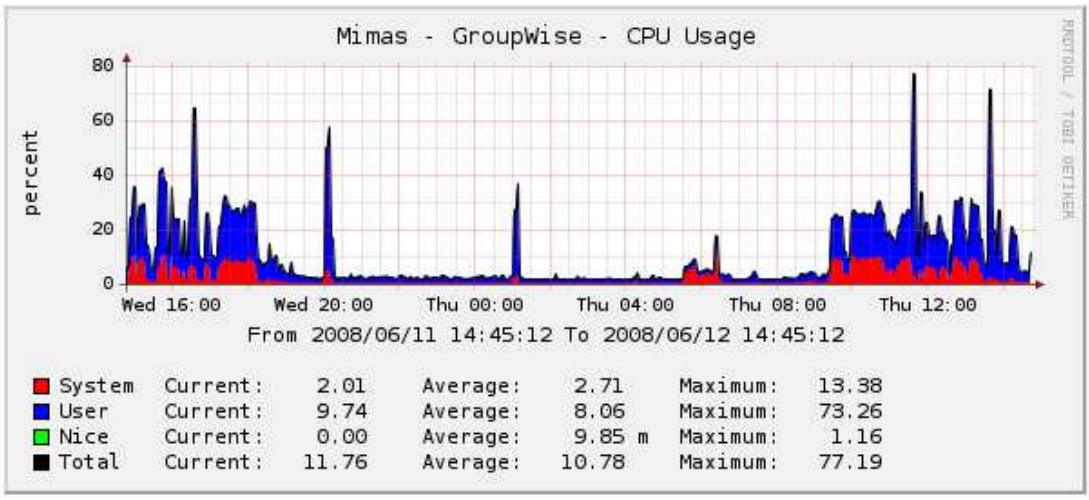

Figura 3.2: Exemplo de gráfico gerado no Cacti

Diferentemente do Nagios, o Cacti não envia alertas em caso de paradas de serviço ou algum outro evento anormal. Contudo, ele possui um log de mensagens que permite ao administrador saber caso as consultas SNMP para um determinado equipamento não estejam sendo efetuadas com sucesso. Outro aspecto interessante é que o Cacti possui um controle de acesso personalizado, que permite criar usuários com diferentes perfis. Assim, um usuário pode ter controle administrativo sobre a ferramenta, o que significa que terá plenos poderes sobre ela. Já um segundo usuário pode receber apenas permissão para visualizar os gráficos existentes, ou parte deles, ficando restrito.

4 ESTUDO DE CASO

4.1 Descrição do Ambiente a ser Gerenciado

O estudo de caso de que trata esse documento tem como escopo uma LAN Fast Ethernet, com o núcleo em Gigabit Ethernet. É uma rede composta de doze servidores e aproximadamente trezentas estações. Há também um enlace em fibra óptica de 100 Mbps conectando estações que estão em outro prédio. Um roteador faz a conexão com a Internet, cuja velocidade do enlace é de 4 Mbps. A rede provê serviços de correio, Proxy, HTTP e *firewall*, entre outros. Todos rodam sobre a pilha de protocolos do TCP/IP. Duas redes classe C estão disponíveis para endereçar servidores e estações.

O ambiente dos usuários é criado no SAMBA. Existem pastas compartilhadas para grupos, que representam os diversos departamentos, pastas pessoais para cada usuário e pastas comuns, onde pode-se acessar determinados sistemas e realizar troca de arquivos entre diferentes setores. Todos esses mapeamentos são criados por meio de um *script* que é executado no momento do *login*. Todos os compartilhamentos têm restrições de acesso, permitindo apenas que os respectivos grupos ou usuários possam trabalhar neles. Dessa forma, os usuários acessam um ambiente Linux de forma transparente, como se estivessem no Windows.

4.1.1 Sistemas Operacionais

Servidores:

- Suse Open Enterprise Server 6.5
- Suse Linux Enterprise Server 10
- Windows 2003 Server Standard Edition

Estações:

- Windows XP Professional SP2

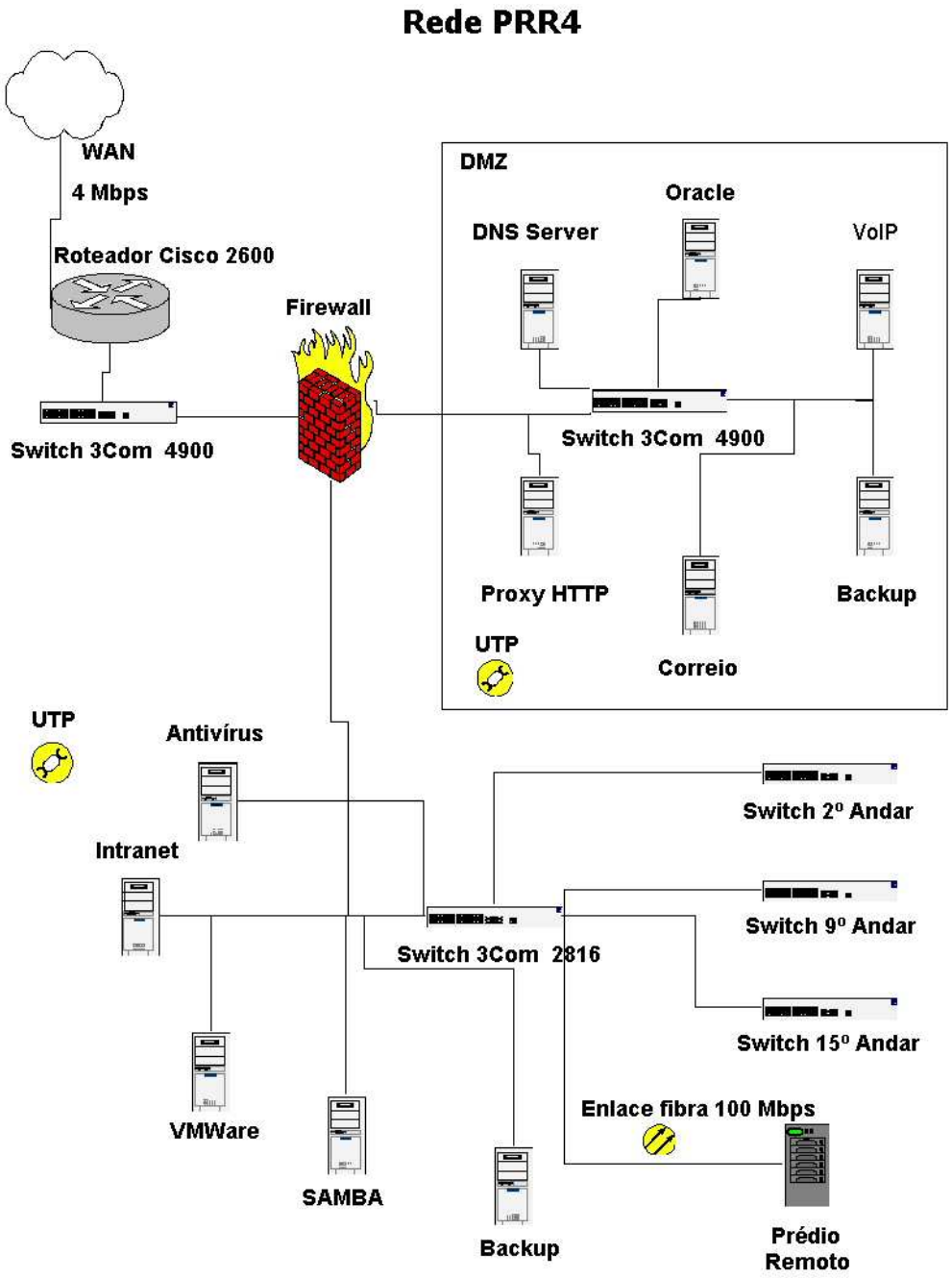

Figura 4.1: Visão do ambiente a ser gerenciado

4.2 Estado Atual da Operação dos Serviços

Há diversos serviços em execução para que a rede esteja disponível, seja segura e possa atender às demandas dos usuários. Por exemplo, o serviço de Proxy tem que estar sempre ativo para que o acesso à Internet esteja disponível. O serviço de correio também é essencial para o bom andamento da rotina dos usuários, que hoje não podem ficar muito tempo sem ele. Entretanto, atualmente não há um monitoramento efetivo desses e de outros serviços, tampouco dos servidores sobre os quais eles rodam. Quando um serviço fica indisponível, seja porque simplesmente parou ou porque o servidor que o fornece está apresentando algum problema, uma de duas coisas acontece: ou os

usuários ligam para a equipe de suporte avisando que há algo de errado com a rede, ou os administradores se antecipam e enviam uma mensagem coletiva reportando o problema, via serviço interno de mensagens instantâneas, e tomam medidas para restaurar a rede ao seu estado normal o mais rapidamente possível. Se o diagnóstico for falha de hardware, um chamado é aberto para a empresa de manutenção.

Pelos mesmos motivos, é difícil atualmente saber como os recursos da rede estão sendo consumidos. E, se em alguns casos não é difícil, é pelo menos trabalhoso. Por exemplo, o espaço livre em disco é um fator importante no caso dos servidores. Como o recurso não é monitorado, quase que diariamente um administrador precisa acessar os servidores e verificar manualmente a quantidade de espaço livre em disco. Outro exemplo, há momentos do dia em que os usuários reclamam de lentidão na Internet. Pode-se estimar, mas não saber exatamente, os níveis de utilização da banda.

4.3 Proposta de Solução de Gerenciamento

Esta proposta tem o objetivo de fornecer uma solução de gerenciamento capaz de monitorar a disponibilidade da rede, contabilizar a utilização de seus recursos e notificar aos administradores quando um evento indesejado ocorrer. Mais especificamente, a proposta contempla:

- Monitorar o estado de todos os servidores de rede;
- Monitorar o estado dos principais serviços de rede nos servidores;
- Monitorar e contabilizar erros nas interfaces de rede dos servidores e dos ativos de rede
- Contabilizar o tráfego nas interfaces dos servidores e dos ativos de rede
- Contabilizar a utilização de espaço em disco nos servidores;
- Contabilizar a utilização de CPU nos servidores;
- Contabilizar o consumo de banda no enlace da Internet;
- Enviar alertas aos administradores de rede sempre que um servidor ou um serviço monitorado estiver indisponível;
- Enviar alertas aos administradores de rede sempre que os valores máximos definidos para o consumo de recursos forem excedidos;
- Gerar histórico da utilização dos recursos e da ocorrência de falhas;
- Propiciar aos administradores de rede maneiras de visualizar, a qualquer tempo, os resultados gerais ou parciais de tudo o que está sendo monitorado.

Esses objetivos devem ser alcançados com a implantação das ferramentas Nagios e Cacti.

4.4 Análise dos Resultados e da Proposta de Gerenciamento

A implantação das ferramentas Nagios e Cacti foi bem sucedida. A proposta de gerenciamento foi contemplada a contento. Atualmente, todos os servidores e ativos de rede estão sendo monitorados, bem como uma série de serviços tais como:

- ♦ Serviço DNS
- ♦ Serviço SMTP
- ♦ Serviço HTTP
- ♦ Serviço SAMBA
- ♦ Serviço de PROXY

A equipe de redes tem agora à disposição um panorama completo da saúde da rede. É possível visualizar, a qualquer instante de tempo, o estado atual da disponibilidade de todos os servidores e seus respectivos serviços. O mesmo acontece com os ativos de rede. O Nagios, por exemplo, foi configurado para enviar uma mensagem de alerta aos administradores de rede sempre que um *host* perder a conectividade ou um serviço não estiver respondendo. E ele faz o mesmo no caso de outros recursos, tais como utilização de CPU e ocupação de espaço em disco, quando os valores de limiar estabelecidos na configuração desses recursos são extrapolados. Além de enviar um *e-mail*, o Nagios também emite um sinal sonoro associado a cada evento de alerta e altera a cor do estado, o que facilita muito a ação dos administradores na identificação dos problemas.

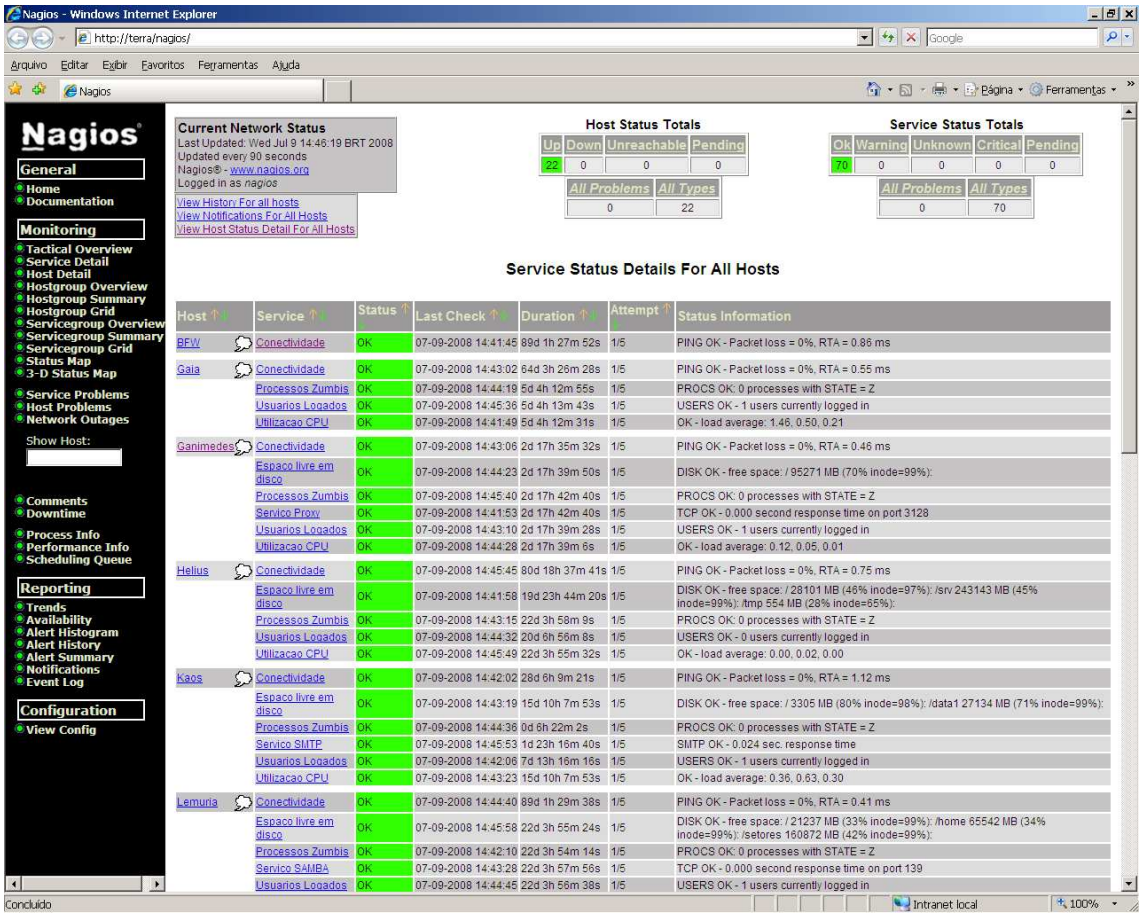

Figura 4.2: Nagios – relação de servidores e serviços e seus estados

Como outra parte da solução, o Cacti apresenta gráficos que geram um histórico preciso do consumo de recursos tais como memória, tráfego de interfaces de rede, erros nas interfaces de rede e outros. O interessante é que a ferramenta está configurada para registrar eventos a cada 5 minutos, resultando em gráficos diários com histórico da média de utilização calculada de 5 em 5 minutos; gráficos semanais, com histórico da média de utilização calculada de 30 em 30 minutos; gráficos mensais, com histórico da média de utilização calculada de 2 em 2 horas e gráficos anuais com histórico da média de utilização calculada a cada 24 horas. Isso possibilita que os administradores de rede vislumbrem os momentos de maior utilização de um determinado recurso, identificando assim possíveis gargalos e planejando com maior segurança a expansão da rede.

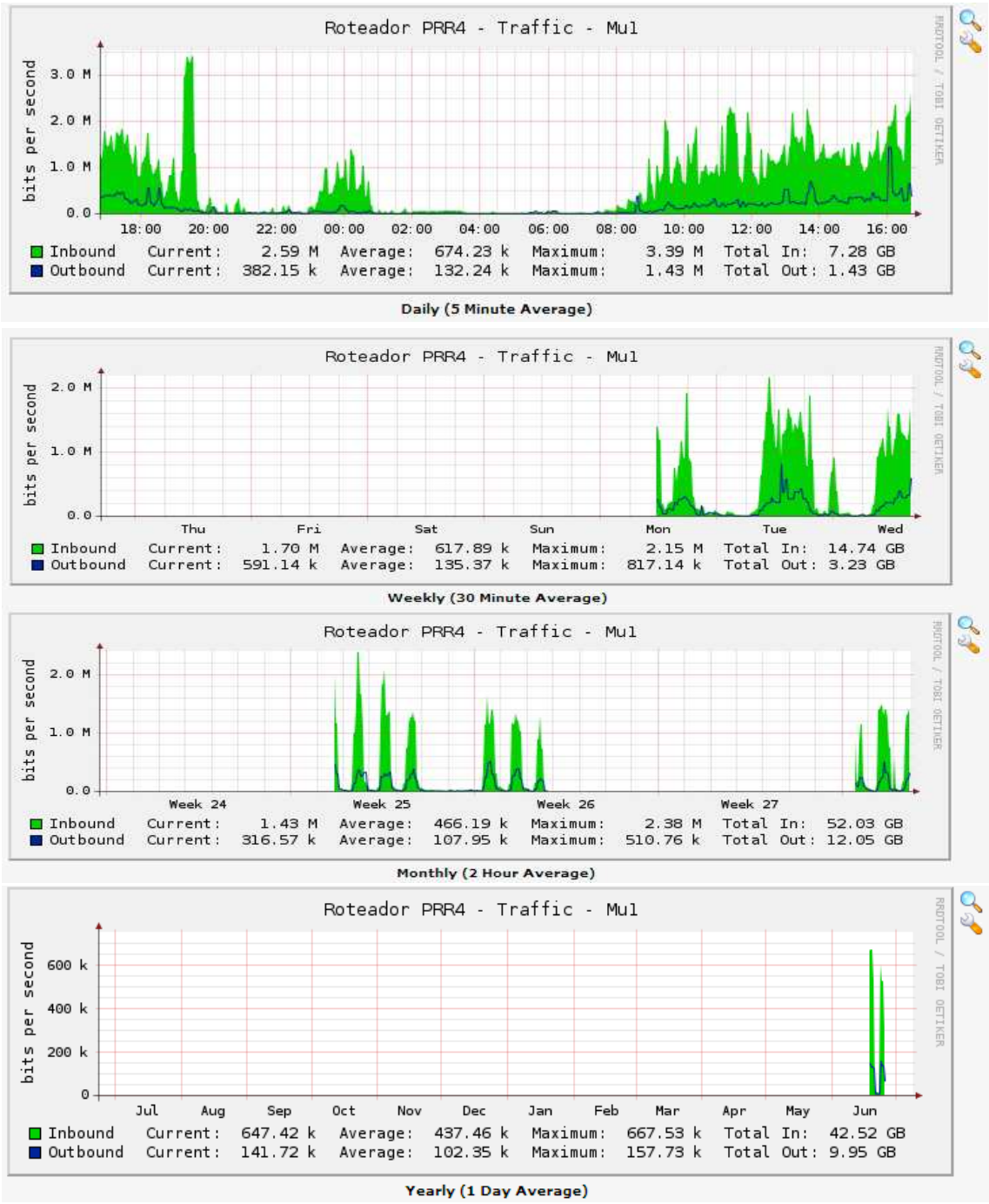

Figura 4.3: Cacti - histórico da contabilização de recursos

De posse dessa “radiografia” da saúde rede, os administradores conseguem antecipar-se aos usuários, o que significa perceber um problema e tomar uma ação corretiva antes que os usuários liguem para o setor de informática avisando que alguma coisa deixou de funcionar. Ou então, se não for possível solucionar o problema antes que os usuários percebam, às vezes pode-se enviar uma mensagem coletiva, via serviço interno de mensagens instantâneas, informando a todos que um serviço parou antes que as ligações comecem. Isso passa uma imagem de agilidade e competência da equipe de redes, tornando seus serviços mais confiáveis. E a própria equipe de redes sente-se mais segura no exercício de suas funções.

Um aspecto interessante, que ressalta a confiabilidade da solução, é o esforço que foi feito para evitar falsos-positivos. Neste caso tirou-se proveito de uma característica do Nagios, que permite estabelecer níveis de dependência entre serviços e *hosts* e entre serviços e serviços. Assim, no caso de um serviço como o SAMBA, por exemplo, se o servidor no qual esse serviço roda estiver indisponível, o alerta enviado deve informar que o servidor perdeu a conectividade, em vez de notificar a parada do serviço. Para que isso funcione é necessário estabelecer uma relação de dependência do serviço SAMBA com a conectividade do *host* que o executa. O exemplo abaixo ilustra como isso foi configurado:

```
##############################################################################
##############################################################################
#
# SERVICES - SAMBA
#
##############################################################################
##############################################################################

define service{
        name                    SAMBA
        host_name               Lemuria

        use                     padrao
        service_description     Servico SAMBA
        check_command           check_nrpe!check_tcp
        }
```

```
#----------------------------Service Dependencies---------------------------#

define servicedependency{
        host_name                       Lemuria
        service_description             Servico SAMBA
        dependent_host_name             Lemuria
        dependent_service_description   Conectividade
        execution_failure_criteria      c
        notification_failure_criteria   w,c
        }
```

Figura 4.4: Dependência entre serviço e *host* para evitar falso-positivo

Como mostra a figura, o *host* Lemuria executa o serviço SAMBA. Se a conectividade desse servidor estiver comprometida, a mensagem de alerta notificará a falha na conectividade do servidor e não a parada do serviço. Caso contrário, se o teste de conectividade do *host* Lemuria não apresentar problemas e o teste da disponibilidade do serviço SAMBA retornar erro, aí sim o alerta notificará problema no serviço.

Obviamente, nem tudo é perfeito. A solução de gerenciamento está praticamente centralizada em uma única máquina, o que torna sua disponibilidade dependente dela. Talvez a solução pudesse ter sido distribuída entre duas máquinas, ficando assim menos vulnerável, mas um único servidor foi eleito para a tarefa. Porém, no caso de ambas as ferramentas, há uma interdependência de elementos da solução com todos os servidores. Explicando: no caso do Nagios, há um agente instalado em cada servidor que precisa estar “ouvindo” as chamadas da máquina de monitoramento para coletar os dados solicitados e repassá-los à origem. O mesmo acontece no caso do Cacti, que faz consultas SNMP diretamente ao agente na máquina cliente. Ou seja, há serviços que precisam estar executando nos clientes para que a solução funcione redonda e perfeitamente.

5 CONCLUSÃO

Com a crescente complexidade das redes de computadores, um sistema de gerenciamento de redes torna-se cada vez mais indispensável. E um sistema de gerenciamento eficaz não pode prescindir de boas ferramentas. Elas são para os administradores de rede o que os telescópios são para os astrônomos: seus olhos. Somente com o auxílio de ferramentas é possível enxergar mais precisamente o que acontece no interior de uma rede de computadores. Sem elas, seria como observar os céus estrelados a olho nu; há uma enorme cortina que pode ser aberta para revelar um mundo de novas informações.

E assim como os telescópios podem captar imagens em regiões obscuras do Universo, lançando luz sobre a compreensão dos cientistas, assim também as ferramentas de gerenciamento são capazes de fotografar áreas e elementos internos de uma rede, revelando ao administrador de rede focos que requerem sua intervenção ou simplesmente tranqüilizando-o com o fato de que tudo vai muito bem naquele momento.

Tudo isso é possível graças ao SNMP, sem o qual provavelmente o mundo do monitoramento das redes de computadores não seria o mesmo. Uma solução de gerenciamento baseada em SNMP, ainda que não contemple todas as áreas nas quais o protocolo se desdobra, se implantada numa rede antes desprovida de um sistema de gerenciamento, eleva significativamente o padrão de qualidade do trabalho do administrador de rede. Faz isso por diminuir o tempo de detecção de falhas, auxiliar proativamente na detecção de gargalos e na expansão da rede, manter histórico de contabilização de recursos, de disponibilidade e de tendências, e por permitir ao administrador ter uma visão acurada e centralizada de todos os elementos importantes da rede.

Naturalmente, uma solução de gerenciamento de rede não substitui o administrador de rede, apenas o instrumentaliza para suas atividades, facilitando sua vida. Por outro lado, o fato de ferramentas de software poderem fazer a leitura do estado do próprio software e também do hardware, é fascinante. Talvez num futuro seja possível desenvolver ferramentas mais inteligentes, capazes de reparar falhas de software ou até mesmo de hardware, o que certamente tornará ainda mais interessante a fantástica área de monitoramento de redes de computadores!

REFERÊNCIAS

FERRAMENTA de gerenciamento de redes Cacti. Disponível em: <http://www.cacti.net/>. Acesso em: maio 2008.

FERRAMENTA de gerenciamento de redes Nagios. Disponível em: < http://www.nagios.org/ >. Acesso em: abr. 2008.

KUROSE, J.F.; ROSS, K.W. **Redes de computadores e a Internet:** uma abordagem top-down. 3. ed. São Paulo: Person/Addison Wesley, 2006.

MONITORAMENTO de redes com RRDtool. Disponível em: <http://oss.oetiker.ch/rrdtool/ >. Acesso em: jun. 2008.

STALLINGS, W. **SNMP, SNMPv2, SNMPv3, and RMON 1 and 2**. 3rd ed. Massachusetts: Addison-Wesley, 1999.

STALLINGS, W. SNMPv3: A security enhancement for SNMP. **IEEE Communications Surveys & Tutorials**, [S.l.], v.1, n.1, p.2-17, Fourth Quarter 1998. Disponível em: <http://dl.comsoc.org/cocoon/comsoc/servlets/Search?type=4&query=stallings&node=&render=false&Search.x=26&Search.y=13>. Acesso em: mar. 2008.