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

TOMAS LOVIS BLACK

Comparação de Ferramentas de Gerenciamento de Redes

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

Prof. ME. Henrique Brodbeck
Orientador

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

Porto Alegre, dezembro de 2008.

AGRADECIMENTOS

Agradeço eternamente aos meus pais por entenderem (e me ensinarem) que ser pai e mãe é dar-se pelos filhos; agradeço à minha esposa pelo amor incondicional à mim dirigido durante este não-tão breve período de estudos; aos meus filhos que, ainda tão pequenos, já entendem a importância do desenvolvimento intelectual e da produção científica, ainda que essas palavras estranhas para eles sejam apenas “o colégio de gente grande”.

Bem-aventurado o homem que acha sabedoria, e o homem que adquire conhecimento. Porque melhor é a sua mercadoria do que a mercadoria de prata, e a sua renda do que o ouro mais fino. Mais preciosa é do que os rubis; e tudo o que podes desejar não se pode comparar a ela. Aumento de dias há na sua mão direita; na sua esquerda, riquezas e honra. Os seus caminhos são caminhos de delícias, e todas as suas veredas, paz. É árvore da vida para os que a seguram, e bem-aventurados são todos os que a retêm.

(Livro de Provérbios capítulo 3, versículos 13-18)

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS **7**

LISTA DE FIGURAS **9**

LISTA DE TABELAS **10**

RESUMO **11**

ABSTRACT **12**

1 INTRODUÇÃO **13**

2 GERENCIAMENTO DE REDE **14**

2.1 Introdução e importância do Gerenciamento de Redes **14**
2.1.1 Necessidade de Gerenciamento de Redes 16
2.1.2 Histórico do Gerenciamento de Redes 17
2.2 Paradigmas de Gerenciamento **24**
2.2.1 Classificação de Leinwand 24
2.2.2 Classificação de Martin-Flatin 27
2.2.3 Classificação de Schönwälder 28
2.2.4 Gerenciamento usando *Web Services* 29

3 FERRAMENTAS PARA GERENCIAMENTO DE REDES **30**

3.1 CACTI **30**
3.2 Nagios **34**
3.3 ZenOSS **37**
3.4 ManageEngine OpManager **43**
3.5 BigBrother4 ..... **45**
3.6 Spiceworks **48**
3.7 Zabbix **50**
3.8 Look@LAN **54**

4 COMPARAÇÃO DAS FERRAMENTAS **55**

4.1 CACTI **55**
4.2 Nagios **56**
4.3 ZenOSS **56**
4.4 OpManager **57**
4.5 BigBrother4 ..... **57**
4.6 Spiceworks **58**

4.7 Look@LAN 58
4.8 Zabbix 58
5 CONCLUSÃO 60
REFERÊNCIAS 61

LISTA DE ABREVIATURAS E SIGLAS

ACL	Access Control List
API	Application Programming Interface
ATM	Asynchronous Transfer Mode
BZN	Acrônimo para “Brasa Zona Norte”, Igreja onde efetuei os testes
BSD	Berkeley Software Distribution
CPU	Central Processing Unit
DNS	Domain Name System
FTP	File Transfer Protocol
GNU	Acronismo recursivo para “GNU is not Unix”
GPL	General Public License
GUI	Graphic User Interface
HTTP	Hyper Text Transfer Protocol
IFIP	International Federation for Information Processing
ISO	International Standards Organization
ICMP	Internet Control Message Protocol
IP	Internet Protocol
MAC	Medium Access Control
MIB	Management Information Base
MS	Microsoft
NAT	Network Address Translation
OID	Object ID
OSI	Open Systems Interconnect
QoS	Quality of Service
RFC	Request for Comments
RMON	Remote Network Monitoring
RNP	Rede Nacional de Pesquisa
RPC	Remote Procedure Call

SMTP	Simple Mail Transfer Protocol
SNTP	Simple Network Management Protocol
SOAP	Service Oriented Architecture Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Protocol
TMN	Telecommunication Management Network
TTL	Time to Live
UDP	User Datagram Protocol
URL	Uniform Resource Locators
VPN	Virtual Private Network
ZOPE	Z Object Publishing Environment
WAN	Wide Area Network
XML	Extensible Markup Language

LISTA DE FIGURAS

Figura 2.1: Formas de Implantação do Módulo Tradutor. 17
Figura 2.2: Exemplo de arquitetura centralizada 25
Figura 2.3: Exemplo de arquitetura hierárquica 26
Figura 2.4: Exemplo de arquitetura distribuída 27
Figura 3.1: Arquitetura do sistema ZenOSS 38
Figura 3.2: Ilustração dos serviços do BB4 47

LISTA DE TABELAS

Tabela 3.1: Meios de se obter dados com SNMP no Cacti 31
Tabela 3.2: Requisitos de software do Cacti (Linux/Unix) 32
Tabela 3.3: Tipos de objetos contidos no sistema Nagios 35
Tabela 3.4: Principais plugins e addons para o Nagios 36
Tabela 3.5: Serviços da camada Collection & Control Services 39
Tabela 3.6: Exemplo de configuração de entidades no banco de dados 40
Tabela 3.7: Características de cada versão do ZenOSS 41
Tabela 3.8: Requisitos de hardware para o OpManager 45
Tabela 3.9: Sistemas Operacionais suportados pelo BB4 48
Tabela 3.10: Requisitos de hardware aproximados para o Zabbix 51
Tabela 3.11: Requisitos de software para utilização do Zabbix 52
Tabela 3.12: Características do suporte comercial Zabbix 53
Tabela 4.1: Comparação das ferramentas utilizada 59

RESUMO

A proliferação de redes de computadores de todos os portes, e a massiva integração com um vasto número de outros componentes eletrônicos, tais como telefones celulares, televisões digitais, eletrodomésticos, relógios de pulsos, entre outros, eleva o gerenciamento destas redes complexas a uma importância como nunca vista antes, tornando-o parte vital de uma organização que deseja atingir um determinado padrão de comportamento global.

Neste ínterim, observamos um também crescente número de ferramentas para auxiliar senão totalmente, pelo menos em parte essa tarefa, cada um com suas características próprias, suas vantagens e desvantagens, seu custo e seu benefício.

O presente trabalho consiste na apresentação e comparação de nove dessas ferramentas de gerenciamento e monitoramento de rede: o CACTI, um *front-end* para ferramentas de gerenciamento baseado em *RRD*, ZENOSS¸ ManageOP Engine, BigBrother4, SpiceWorks, Look@LAN, Zabbix e o Nagios.

São muitos os parâmetros de comparação destas ferramentas e não é objetivo dessa dissertação apontar o melhor software dentre os analisados e sim auxiliar o pesquisador a tomar a melhor escolha de acordo com suas necessidades. Em particular, são observados os parâmetros mais relevantes dentre os procurados pelos administradores de rede: performance, facilidade de utilização e necessidade de recursos tanto de hardware quanto humanos.

Palavras-chave: Gerenciamento de Redes, Ferramentas de Gerenciamento de Redes, SNMP, MIB, Comparação de Ferramentas de Gerenciamento de Redes, Desempenho.

Comparison of Network Management Tools

ABSTRACT

The proliferation of computer networks of all sizes, as well as a massive integration with a wide range of other electronic devices such as cell phones, digital television, home appliances, wrist-watches, among others, raises the management of these complex networks to a role ever seen before, making it a vital part of an organization that wants to reach standards for network management.

In the mean time, we can see a growing number of tools intended to help this tasks, if not fully, at least partially, each one with its own features, its advantages and disadvantages, as well as its costs and benefits.

This study aims to present and compare nine of these tools for managing and monitoring network: Cacti, a RRD-based front-end for management tool, ZENOSS, ManageOP Engine, BigBrother4, SpiceWorks, Look @ LAN, Zabbix, and Nagios.

There are many parameters for comparison of these tools and the purpose of this dissertation is not to point out the best software among the studied ones, but to help researchers make the best choice in accordance to their needs. In short, only the most relevant and demanded features by network administrators are studied and compared: performance, ease of use and needs of both hardware/software and human resources.

Keywords: Computer Network Management, SNMP, MIB, Tools for Computer Network Management, Comparison of Tools for Computer Network Management.

1 INTRODUÇÃO

A cada ano, novas aplicações e novos usuários impulsionam o crescimento da redes de computadores internas (*intranets*) e externas (*extranets/internet*) tanto em escala como em complexibilidade. A necessidade de monitorar essas redes diante desse crescimento impulsiona também o desenvolvimento de software cada vez mais aprimorado tecnicamente e abrangendo uma gama maior de características, adaptando-se ao *boom* de novas tecnologias jogadas no mercado anualmente. Neste ínterim, o gerenciamento de tais redes tornou-se uma tarefa indispensável para manter o seu funcionamento correto (STALLINGS, 1998).

O contínuo crescimento em número e diversidades dos componentes das redes de computadores tem tornado a necessidade de gerenciamento de redes cada vez mais complexa. Por menor e mais simples que seja uma rede de computadores, precisa ser gerenciada, a fim de garantir, aos seus usuários, a disponibilidade de serviços a um nível de desempenho aceitável. Novos produtos surgem dia a dia, cujo gerenciamento é indispensável.

O gerenciamento permite controle sobre os recursos da rede assim como a identificação e prevenção de problemas, sendo tal investimento justificado quando queremos controle dos recursos, de sua complexibilidade, serviços melhores e controle de custo. O gerenciamento envolve, basicamente cinco pontos: desempenho, segurança, falhas, configuração e contabilização. Analisaremos estes pontos sob a ótica de algumas ferramentas disponíveis sob licença GPL/BSD (gratuitas na sua concepção) ou proprietárias – sendo que tal particularidade está fora do escopo desse trabalho.

Este trabalho individual visa ilustrar nove ferramentas populares de gerenciamento de redes, compará-las e destacar suas características, pontos fortes e fracos e, por fim, propor uma base para escolha para gerentes de redes que procuram ferramentas com características únicas.

O presente estudo divide-se da seguinte forma:

O capítulo 2 descreve uma revisão geral sobre o gerenciamento de redes, os protocolos mais comuns utilizados, arquitetura dos dispositivos e modernos paradigmas gerenciais. No capítulo 3 serão apresentadas as nove ferramentas, descrevendo suas características principais de forma sucinta. No capítulo 4 as ferramentas estudadas serão comparadas sob diversos aspectos e, por fim, no capítulo 5 serão apresentadas as conclusões da presente obra.

2 GERENCIAMENTO DE REDE

O gerenciamento de redes é uma atividade importante para manter as mesmas operando corretamente. Para se realizar tais tarefas gerenciais, o uso de software específico (aqui chamados de ferramentas) tornou-se uma constante, dado o notório aumento do número de dispositivos a serem gerenciados, o que impede um tratamento individualizado de cada um, bem como dado à necessidade de procedimentos automatizados de configuração, monitoração, reportes, entre outros.

Neste capítulo são apresentados o histórico e importância desde tópico, bem como conceitos básicos sobre gerenciamento de redes, arquiteturas comumente usadas, comparação entre os protocolos mais usados (SNMP e OSI) e os paradigmas de gerenciamento. Estes conceitos são importantes para um melhor entendimento de como as ferramentas atuam sobre os dispositivos da rede e de como a distribuição lógica influencia na distribuição e aplicação física.

2.1 Introdução e importância do Gerenciamento de Redes

Os avanços tecnológicos exercem hoje um grande impacto na sociedade. A informação tem-se tornado cada vez mais uma vantagem competitiva para as empresas e organizações em investimentos futuros. O fato é que, cada vez mais, as empresas, para se tornarem competitivas e sobreviverem no mercado, têm investido em tecnologia de informação, como a única forma de tornar seguro o processo decisório. E é nesse quadro que as redes de computadores se proliferam, encurtando as distâncias e diminuindo o tempo de resposta entre as transações entre as organizações de todo o mundo.

De acordo com Stallings (1998), o gerenciamento e monitoração de redes são tarefas extremamente importantes para a saúde de uma rede de computadores, sendo que, sem operações de gerenciamento, uma rede local não tem como manter-se operacional por muito tempo. Em especial, grandes redes corporativas estão fadadas ao caos sem estas funções. Além de agirem reativamente, as tarefas gerenciais de rede também são proativas no sentido de prevenir e detectar possíveis problemas.

Segundo Martin-Flatin; Znaty; Hubaux (1999), uma aplicação de gerenciamento é composta por *gerentes* executando nas estações de gerenciamento e *agentes* executando nos elementos gerenciados. O termo *gerente* pode ser utilizado, também, para designar a pessoa responsável pelo gerenciamento da rede e, sendo assim, para evitar problemas de interpretação, serão utilizados os termos *operador* e *administrador* nestes casos, ficando o termo *gerente* exclusivo para denominar as entidades de software.

Gerenciar uma rede é uma atividade complexa. Nos últimos anos o tráfego de informações dentro das redes corporativas aumentou exponencialmente devido ao surgimento de novas aplicações. Concorrentemente, novas tecnologias e padrões proporcionaram uma grande proliferação de dispositivos heterogêneos conectados à rede.

A área de gerência de redes foi inicialmente impulsionada pela necessidade de monitoração e controle do universo de dispositivos que compõem as redes de comunicação. Com esta crescente necessidade de gerenciamento, fez-se necessário que padrões para ferramentas fossem estabelecidos.

Em resposta a esta necessidade surgiram dois padrões:

- Família de Protocolos SNMP: o protocolo Simple Network Management Protocol (SNMP) refere-se a um conjunto de padrões para gerenciamento que inclui um protocolo, uma especificação de estrutura de dados, e um conjunto de objetos de dados. Este protocolo hoje já está na sua segunda versão oficial, chamada de SNMPv2 e já se encontra em desenvolvimento o SNMPv3. Este é o protocolo de gerência adotado como padrão para redes TCP/IP.
- Sistemas de gerenciamento OSI: este termo refere-se a um grande conjunto de padrões de grande complexidade, que definem aplicações de propósito gerais para gerência de redes, um serviço de gerenciamento e protocolo, uma especificação de estrutura de dados, e um conjunto de objetos de dados. Este conjunto de protocolos é conhecido como Common Management Information Protocol (CMIP) [ISO 1991] mas, segundo STALLINGS, 1993, pela sua complexidade e lentidão do processo de padronização, este sistema de gerenciamento não é muito popular.

O gerenciamento da rede realizado pelo protocolo SNMP, permite que uma ou mais máquinas na rede sejam designadas gerentes da rede. Estas máquinas recebem informações de todas as outras máquinas da rede, chamadas agentes, e através do processamento destas informações pode gerenciar toda a rede e detectar facilmente problemas ocorridos. As informações coletadas pela máquina gerente estão armazenadas nas próprias máquinas da rede, em uma base de dados conhecida como Management Information Base (MIB). Nesta base de dados estão gravadas todas as informações necessárias para o gerenciamento deste dispositivo, através de variáveis que são requeridas pela estação gerente. Entretanto, em uma interligação de diversas redes locais, pode ser que uma rede local esteja funcionando perfeitamente, mas sem conexão com as outras redes, e, conseqüentemente, sem conexão com a máquina gerente. O ideal é implementar em alguma máquina, dentro desta rede local, um protocolo para gerenciamento que permita um trabalho off-line, isto é, que a rede local possa ser gerenciada, ou pelo menos tenha suas informações de gerenciamento coletadas, mesmo que estas informações não sejam enviadas instantaneamente a estação gerente.

A título de curiosidade, temos o protocolo Remote Monitoring (RMON), que permite uma implementação neste sentido ilustrado acima, devendo ser implementado em diversas máquinas ao longo da rede. É possível, ainda, que uma estação com implementação RMON, envie dados à estação gerente apenas em uma situação de falha na rede. Isto contribuiria para redução do tráfego de informações de controle na rede (*overhead*), facilitando seu gerenciamento, propiciando-se a instalação de um servidor

proxy, que, além de servir como cache dos documentos acessados por uma rede local, pode também restringir o acesso a alguns documentos ou a utilização de algum protocolo, garantindo segurança à rede.

2.1.1 Necessidade de Gerenciamento de Redes

Por menor e mais simples que seja uma rede de computadores, precisa ser gerenciada, a fim de garantir, aos seus usuários, a disponibilidade de serviços a um nível de desempenho aceitável. À medida que a rede cresce, aumenta a complexidade de seu gerenciamento, forçando a adoção de ferramentas automatizadas para a sua monitoração e controle. A adoção de um software de gerenciamento não resolve todos os problemas da pessoa responsável pela administração da rede. Geralmente o usuário de um software de gerenciamento espera muito dele e, conseqüentemente, fica frustrado quanto aos resultados que obtém. Por outro lado, esse mesmo software quase sempre é subutilizado, isto é, possui inúmeras características inexploradas ou utilizadas de modo pouco eficiente. Para gerenciar um recurso, é necessário conhecê-lo muito bem e visualizar claramente o que este recurso representa no contexto da rede.

O investimento em um software de 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.

Além desta visão qualitativa, uma separação funcional de necessidades no processo de gerenciamento foi apresentada pela International Organization for Standardization (ISO), como parte de sua especificação de Gerenciamento de Sistemas OSI. Esta divisão funcional foi adotada pela maioria dos fornecedores de sistemas de gerenciamento de

redes para descrever as necessidades de gerenciamento: Falhas, Desempenho, Configuração, Contabilização e Segurança.

2.1.2 Histórico do Gerenciamento de Redes

Quando em 1986 reuniu-se, pela primeira vez, o Grupo de Trabalho sobre gerenciamento de Redes do Comitê Técnico em Comunicação de dados International Federation for Information Procesing (IFIP) havia apenas o consenso sobre a necessidade de gerenciamento. Cerca de 20 pessoas reunidas em Dallas, provenientes de diversos países, sequer concordavam sobre o escopo do gerenciamento de rede. Enquanto representantes incorporasse apenas as três camadas inferiores da arquitetura Open System Interconnection (OSI) (pois era com estava-se acostumado a trabalhar), para os outros o gerenciamento de redes devia englobar as sete camadas. Percebia-se claramente que cada fornecedor tinha construído uma arquitetura proprietária de gerenciamento para seus produtos e tinha dificuldade de impingi-la aos clientes, ao lado de outros fornecedores. Já se falava na oportunidade sobre o gerenciamento OSI, embora muitos tenham encarado com certo ar de dúvida aquela alternativa.

A abordagem clássica para integrar o gerenciamento de redes era, pois, baseada em arquitetura proprietária. Para que pudessem funcionar como elemento de integração, os arquitetos de tais soluções incorporaram nelas uma abertura para agregar a informação e gerenciamento de sistema de outros fornecedores. A IBM, por exemplo, com o conceito de ponto focal abriu esta porta para integrar outros sistemas de gerenciamento ao Netview, principalmente por interesse próprio, uma vez que a aquisição da RDLM (fabricante PABX) levou a esta necessidade. Módulos para traduzir o fluxo de informação de gerenciamento de um esquema para outros tinham de ser constituídos e podiam ser implantados em vários pontos, como mostra a figura abaixo:

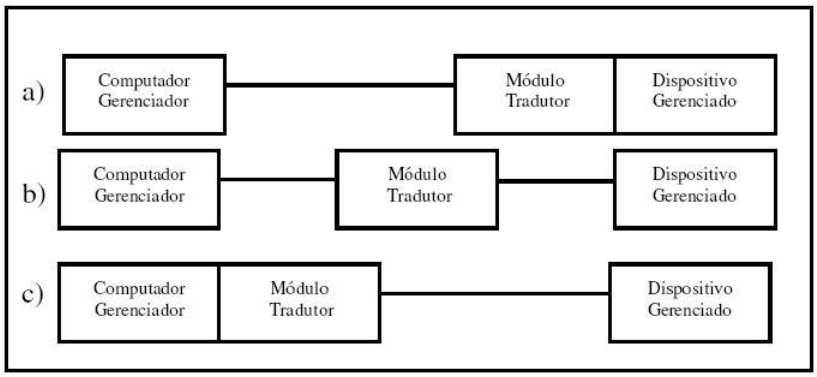

Figura 2.1: Formas de Implantação do Módulo Tradutor.

Na figura 1, a) poderia ser um servidor de rede Novell, com um módulo interno capaz de gerar os “vetores de alerta” esperados pelo Netview e b) poderia ser a solução para integrar o gerenciamento de um PABX digital em que a tradução seria feita em um PC que receberia as mensagens de gerenciamento de um lado e as traduziria, quando possível, para o outro. A terceira abordagem seria para o caso em que um roteador fosse

o dispositivo gerenciado e que usasse um protocolo padrão de fato na indústria, tal como o SNMP (Simple Network Management Protocol da arquitetura Internet), com a conversão feita internamente no computador gerenciador.

Dentro dos problemas decorrentes desta solução, pode-se destacar principalmente a limitação imposta pelo fato de somente usar opções gerenciamento (dados recebidos e comandos veiculáveis) que tinham similar na arquitetura proprietária do fornecedor do computador gerenciador. Opções de interação propiciadas pelos dispositivos gerenciados podiam não ser aproveitadas simplesmente pela falta de condições de mapeá-las para uma forma passível de reconhecimento pelo computador gerenciador. Em decorrência, os dispositivos gerenciados providos pelo mesmo fornecedor do computador gerenciador apareciam mais facilmente.

Para não parecerem diminuídos sob este prisma, muitos fornecedores não se mostravam entusiasmados em cooperar para tornar seus produtos gerenciáveis por um computador gerenciador de outro fabricante. Esta abordagem foi adotada por alguns fornecedores no mercado, como a IBM e a DEC, mas cada vez mais acrescida do desejo de que um sistema de gerenciamento independente de fornecedor pudesse rodar numa máquina dedicada, de modo a não sobrecarregar nem prejudicar o atendimento dos serviços normais a serem executados no mainframe. A AT&T também entrou no cenário, definindo uma arquitetura de gerenciamento e se propondo a gerenciar as redes de seus clientes de telecomunicações. Criando o impasse, uma solução alternativa teria de ser buscada, implicando a agregação de esforços que levassem a uma solução mais universal e padronizada. Obviamente, tal solução deveria englobar os serviços de gerenciamento mais importantes e relevantes, além de formalizar a interação entre os dispositivos gerenciados e os gerenciadores. A ISO tomou a bandeira e o esquema básico da arquitetura de gerenciamento de rede foi adicionado ao modelo de referência ISO/OSI em 1989.

A colaboração entre a ISO/ International Eletrotechnical Committee (IEC) resultou na série de documentos X.700, cujo objetivo maior é criar condições para o desenvolvimento de produtos de gerenciamento de redes de computadores e sistema de comunicações heterogêneos.

Todavia, o embate das forças dominantes no cenário internacional dificultou a estabilização dos detalhes operacionais do modelo de gerenciamento. Anos se passaram sem que os documentos atingissem o estágio do padrão ISO internacional. As implantações, baseadas em interpretações da documentação disponível, começaram a aparecer e, em 1989, percebendo a necessidade de acordos que assegurassem a interoperabilidade das implementações, os fornecedores começaram a reunir-se em associações como a ISO/NM Fórum, para buscar um acordo que viabilizasse a definição de um conjunto de opções de implantação capaz de assegurar a interoperabilidade dos sistemas de gerenciamento. Outro grupo foi criado sob a tutela do National Institute of Standards and Technology (NIST) dos Estados Unidos para atender às necessidades do governo americano, que já havia determinado, através de seu documento Government OSI Profile (GOSIP), que as soluções de redes a serem adquiridas deveriam atender às recomendações ISO/IEC. Este trabalho resultou no Government Network Management Profile (GNMP), cuja versão 1, de 30 de julho de 1992, constitui a referência que todas as agências do governo federal dos Estados Unidos devem usar ao adquirir funções e serviços de gerenciamento de rede.

O primeiro dos protocolos de gerência de rede foi o Simple Gateway Monitoring Protocol (SGMP) que surgiu em novembro 1987. Entretanto, o SGMP era restrito à monitoração de gateways. A necessidade crescente de uma ferramenta de gerenciamento de rede mais genérica fez emergirem mais algumas abordagens:

- High-Level Entity Management System (HEMS) – generalização do Host Management Protocol (HMP);
- Simple Network Management Protocol (SNMP) – um melhoramento do SGMP;
- CMIP over TCP/IP (CMOT) uma tentativa de incorporar o máximo possível o protocolo (CMIP), serviços e estrutura de base de dados que estava sendo padronizada pela ISO para gerenciamento de redes.

No início de 1988 a Internet Architecture Board (IAB) revisou os protocolos e escolheu o SNMP como uma solução de curto prazo e o CMOT como solução de longo prazo para o gerenciamento de redes. O sentimento era que, em um período de tempo razoável, as instalações migrariam do TCP/IP para protocolos baseados em OSI. Entretanto, como a padronização do gerenciamento baseado no modelo OSI apresentava muita complexidade de implementação e o SNMP, devido à sua simplicidade, foi amplamente implementado nos produtos comerciais, o SNMP tornou-se um padrão de fato. Posteriormente, pela existência de lacunas funcionais (devido exatamente à simplicidade do SNMP), foram definidas novas versões do protocolo SNMP chamadas de SNMPv2 e SNMPv3, e o SNMP original ficou conhecido como SNMPv1.

A primeira versão da arquitetura de gerenciamento SNMP foi definida no RFC 1157 de maio de 1990. O RFC 1157 define ainda três objetivos a serem alcançados pelo SNMP: minimizar o número e complexidade das funções de gerenciamento, ser flexível o suficiente para permitir expansões futuras e ser independente da arquitetura e mecanismo dos dispositivos gerenciados. A definição das informações de gerenciamento requer não apenas profundo conhecimento da área específica em foco, mas também do modelo de gerenciamento.

2.1.2.1 Sobre o SNMP:

Até o início da década de 1980, redes de computadores eram baseadas em arquiteturas e protocolos patenteados, a exemplo de System Network Architecture (SNA) da IBM e DECNET da Digital Equipment Corporation. Já no final da década de 1980, redes interconectadas baseadas na arquitetura e protocolos TCP/IP estavam em franca ascensão. Porém, do ponto de vista da gerência de tais redes, a situação ainda favorecia arquiteturas proprietárias, devido à inexistência de soluções de gerência de redes TCP/IP. Com o crescimento das redes TCP/IP, aumentaram consideravelmente as dificuldades de gerência. A demora no aparecimento de soluções abertas baseadas no modelo OSI fez com que um grupo de engenheiros decidisse elaborar uma solução temporária baseada num novo protocolo: Simple Network Management Protocol (SNMP). A simplicidade do SNMP facilitou sua inclusão em equipamentos de interconexão.

No final da década de 1990, a solução SNMP já era tão difundida que se estabelecera como padrão de gerência de redes de computadores. Hoje, praticamente todos os equipamentos de interconexão dão suporte a SNMP, bem como muitos outros dispositivos (nobreaks, modems etc.), e sistemas de software (servidores Web, sistemas de bancos de dados etc.).

Os principais objetivos do protocolo SNMP são:

- Reduzir o custo da construção de um agente que suporte o protocolo;
- Reduzir o tráfego de mensagens de gerenciamento pela rede necessárias para gerenciar os recursos da rede;
- Reduzir o número de restrições impostas as ferramentas de gerenciamento da rede, devido ao uso de operações complexas e pouco flexíveis;
- Apresentar operações simples de serem entendidas, sendo facilmente usadas pelos desenvolvedores de ferramentas de gerenciamento;
- Permitir facilmente a introdução de novas características e novos objetos não previstos ao se definir o protocolo;
- Construir uma arquitetura que seja independente de detalhes relevantes a somente a algumas implementações particulares.

2.1.2.1.1 Agentes de Gerenciamento:

O agente de gerenciamento é o componente contido nos dispositivos que devem ser gerenciados. Bridges, roteadores, hubs e switches podem conter agentes SNMP que permitem que eles sejam controlados pela estação de gerenciamento. O agente de gerenciamento responde à estação de gerenciamento de duas maneiras:

- Polling: a estação de gerenciamento solicita dados ao agente e o agente responde com os dados solicitados;
- Interceptação: é um método de reunião de dados projetado para reduzir o tráfego na rede e para o processamento nos dispositivos que estão sendo monitorados. Em vez de a estação de gerenciamento fazer polling nos agentes em intervalos determinados e contínuos, são definidos limites (superiores e inferiores) no dispositivo de gerenciamento. Se esses limites forem ultrapassados no dispositivo, o dispositivo de gerenciamento enviará uma mensagem de alerta à estação de gerenciamento. Isso elimina a necessidade de fazer polling em todos os dispositivos gerenciados na rede. A interceptação é muito útil em redes com muitos dispositivos que precisem ser gerenciados. Ela reduz a quantidade de tráfego SNMP na rede para fornecer mais largura de banda para a transferência de dados.

O mundo SNMP está baseado em três documentos:

- Structure of Management Information (SMI). Definido pela RFC 1155, a SMI traz essencialmente, a forma pela qual a informação gerenciada é definida;
- Management Information Base (MIB) principal. Definida na RFC 1156, a MIB principal do mundo SNMP (chamada MIB-2) define as variáveis de

gerência que todo elemento gerenciado deve ter, independentemente de sua função particular. Outras MIBs foram posteriormente definidas para fins particulares, tais como MIB de interfaces Ethernet, MIB de nobreaks, MIB de repetidores etc;

- Simple Network Management Protocol (SNMP). Definido pela RFC 1157, é o protocolo usado entre gerente e agente para a gerência, principalmente trocando valores de variáveis de gerência.

2.1.2.1.2 Mensagens no Protocolo SNMP:

Ao contrário de muitos outros protocolos TCP/IP, as mensagens no protocolo SNMP além de não apresentarem campos fixos, são codificadas usando a sintaxe ASN.1 (tanto a mensagem de pedido, como a de resposta) o que dificulta o entendimento e a decodificação das mensagens.
Os cinco tipos de mensagens SNMP são:

- get-request-PDU: mensagem enviada pelo gerente ao agente solicitando o valor de uma variável;
- get-next-request-PDU: mensagem utilizada pelo gerente para solicitar o valor da próxima variável depois de uma ou mais variáveis que foram especificadas;
- set-request-PDU: mensagem enviada pelo gerente ao agente para solicitar que seja alterado o valor de uma variável;
- get-response-PDU: mensagem enviada pelo agente ao gerente, informando o valor de uma variável que lhe foi solicitado;
- trap-PDU: mensagem enviada pelo agente ao gerente, informando um evento ocorrido.

As partes mais importantes de uma mensagem são: as operações (GET, SET e GET-NEXT) e a identificação, no formato ASN.1, dos objetos em que as operações devem ser aplicadas. Deve existir um cabeçalho que informe o tamanho da mensagem, que só será conhecido após a representação de cada campo ter sido computada. Na verdade, o tamanho da mensagem depende do tamanho de sua parte remanescente (que contém os dados), portanto o tamanho só poderá ser computado após a construção da mensagem. Uma maneira de evitar este problema é construir a mensagem de trás para frente.

Uma mensagem SNMP deve definir o servidor do qual obtemos ou alteramos os atributos dos objetos, e que será responsável por converter as operações requisitadas em operações sobre as estruturas de dados locais. Após verificar os campos de uma mensagem, o servidor deve usar as estruturas internas disponíveis para interpretar a mensagem e enviar a resposta da operação ao cliente que requisitou o pedido. Uma mensagem é constituída por três partes principais:

1) A versão do protocolo;
2) A identificação da comunidade, usada para permitir que um cliente acesse os objetos gerenciados através de um servidor SNMP;
3) A área de dados, que é dividida em unidades de dados de protocolo (Protocol Data Units - PDUs). Cada PDU é constituída ou por um pedido do cliente, ou por uma resposta de um pedido (enviada pelo servidor).

O primeiro campo de uma mensagem SNMP é um operador seqüencial, seguido por um campo com o tamanho total da mensagem (se este tamanho não for igual ao do datagrama, será retornado um código de erro). O próximo campo é um número inteiro que identifica a versão do protocolo SNMP, seguido por um campo usado para a autentificação, indicando a comunidade à qual o cliente pertence (a comunidade public permite a qualquer cliente acessar os objetos, não precisando o servidor verificar se o cliente pode ou não acessar o objeto). O quarto campo contém a operação que será executada, devendo ser um GET, SET ou GETNEXT pois a operação de TRAP só é gerada pelo servidor. O quinto campo é usado para o servidor ter certeza de que o valor deste campo é igual ao tamanho da parte da mensagem que contém os dados. O sexto campo é uma identificação para o pedido, e o sétimo e o oitavo campos são flags que indicam erros quando estão setadas (campos de status e de índice de erro).

Na definição de uma mensagem, cada uma das PDUs são constituídas ou por um os cinco tipos de PDUs para as operações ou por uma PDU para a resposta. Na definição da mensagem SNMP, deve-se ter uma sintaxe individual para cada um das cinco operações da PDU. Alguns termos encontrados nas sintaxes das PDUs das operações são:

a) O campo RequestID é um inteiro de 4 bytes (usado para identificar as respostas);
b) Os campos ErrorStatus e ErrorLevel são inteiros de um byte (sendo nulos em um pedido de um cliente);
c) O campo VarBindList é uma lista de identificadores de objetos na qual o servidor procura os nomes dos objetos, sendo definida como uma sequência de pares contendo os nomes dos objetos (em ASN.1 este par é representado como uma sequência de dois itens). Na sua forma mais simples (com um objeto) apresenta dois itens: o nome do objeto e um ponteiro nulo.

Limitações do SNMP:

- Falta de segurança;
- Esquema de autenticação trivial;
- Limitações no uso do método SET;
- Ineficiência;
- Esquema de eventos limitado e fixo;
- Operação baseada em pooling;
- Comandos transportam poucos dados;
- Falta de Funções Específicas;
- MIB com estrutura fixa;
- Falta de comandos de controle;
- Falta de comunicação entre gerenciadores;
- Não Confiável;
- Baseado em UDP/IP;
- Trap sem reconhecimento

2.1.2.1.3 SNMPv2 e SNMPv3:

Visando obter melhorias com relação aos aspectos de segurança foram desenvolvidas novas versões do SNMP. A segunda versão, o SNMPv2 contém mecanismos adicionais para resolver os problemas relativos à segurança como a privacidade de dados, autenticação e controle de acesso. A terceira versão, o SNMPv3 tem como objetivo principal alcançar a segurança, sem esquecer-se da simplicidade do protocolo, através de novas funcionalidades como:

- Autenticação de privacidade;
- Autorização e controle de acesso;
- Nomes de entidades;
- Pessoas e políticas;
- Usernames e gerência de chaves;
- Destinos de notificações;
- Relacionamentos proxy;
- Configuração remota.

2.1.2.1.4 Palavras finais sobre SNMP:

Como o protocolo SNMP é amplamente utilizado, seria impossível imaginar uma gerência de rede sem o uso da ferramenta que o implementa. Os mecanismos oferecidos pelo protocolo SNMP permitem efetuar tarefas de monitoração; além da possibilidade de efetuar configuração nos equipamentos gerenciados. Com o surgimento das novas versões o SNMPv2 e SNMPv3, foram realizadas alterações na especificação do protocolo, tais como a forma de representação das variáveis, e inclusão de novos tipos de PDUs e o retorno dos tipos de erros, que acabaram por tirar a simplicidade do protocolo. Entretanto, o SNMP é amplamente usado, sendo que, a maioria dos fabricantes de hardware para internet (como bridges e roteadores) projetam seus produtos para suportar o SNMP.

2.2 Paradigmas de Gerenciamento

O modelo inicial de gerenciamento de rede (com SNMP) era baseado no modelo gerente-agente, onde o gerente concentrava as funções de controle e monitoração e era o responsável pelo acesso aos diversos agentes (dispositivos) da rede. Os agentes cumpriam e ainda cumprem o papel de fornecimento das variáveis (MIB) ao passo que o gerente, através de mecanismos tipo *polling*, controlam a rede efetuando operações de controle. O objetivo deste modo de gerenciamento era facilitar as tarefas do agente, permitindo um desenvolvimento rápido e exigindo poucos recursos dos equipamentos, considerando-se ainda que não era definido nenhum mecanismo para a comunicação entre vários gerentes. Esta abordagem sobrecarregava o gerente com todas as funções, gerando grande processamento dos mesmos, alto volume de tráfego na rede e degradando o tempo de resposta na detecção dos problemas – basicamente, uma abordagem pouco eficaz.

Com o passar do tempo, novas abordagem foram surgindo tendo, como base, novos estudos e necessidades para a questão do gerenciamento de redes crescentes e complexas. O modelo inicial havia tornado-se obsoleto por motivos óbvios ao passo que a demanda de processamento e tráfego de rede crescia a níveis exponenciais ano a ano, gerando uma nova corrente de software que distribuía estas tarefas gerenciais. Nascia uma nova abordagem de gerenciamento de dispositivos ligados através de uma rede de dados, com novas idéias surgidas, produzindo um novo conjunto de paradigmas, onde podemos destacar três em especial: Leinwand (1996), Martin-Flatin (1999) e Schönwälder (2000).

2.2.1 Classificação de Leinwand

Segundo Leiwand (1996), as arquiteturas de gerenciamento podem ser dividas em: Centralizada, Hierárquica e Distribuída.

Na **arquitetura centralizada**, apenas um gerente é o responsável pelos procedimentos de gerenciamento em todos os equipamentos. Esse modelo usa um banco de dados de gerenciamento centralizado concentrando todos dados disponíveis para serem analisados.

As vantagens desse modelo são:

- possuir um único local para visualização das informações da rede, facilitando tarefas administrativas de banco de dados;
- facilidade de monitoramento de segurança, visto que somente um ponto de concentração de dados é mais simples de ser vigiado contra possíveis falhas de segurança;

- melhores condições de expansibilidade e portabilidade já que um banco único não depende de outros sistemas remotos para ser manipulado e/ou transformado.

As desvantagens desse modelo são:

- é necessário ser replicado para outro sistema se deseja-se almejar tolerância à falhas;
- dependência de um ponto único: em caso de falha, o sistema pode ficar inoperante (dependendo da opção anterior);
- não-escalabilidade: todo tráfego gerado para o gerenciamento no enlace de acesso ao banco central é concentrado nele, sem alternativas que o possibilitassem de ser escalado.

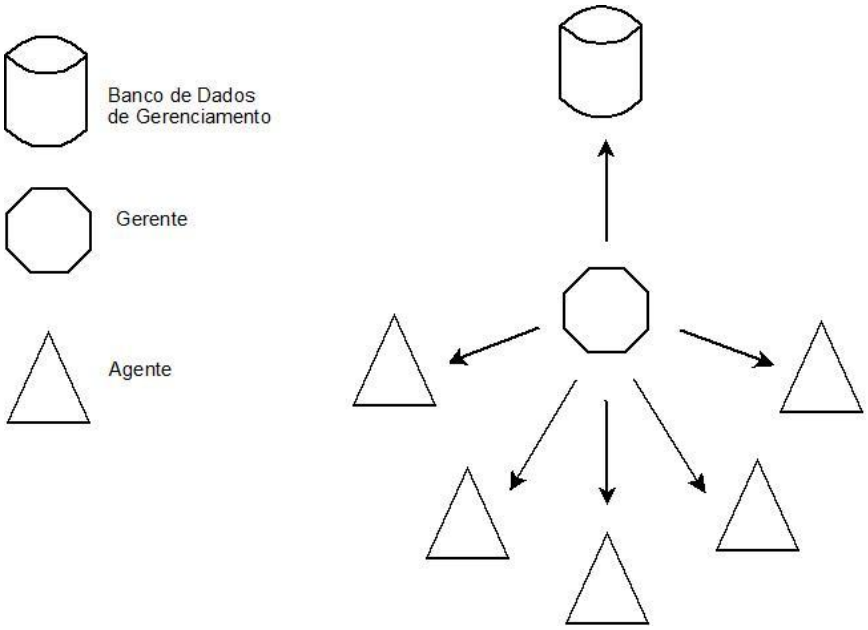

Figura 2.2: Exemplo de arquitetura centralizada

Por outro lado, um **arquitetura hierárquica** usa diversos gerentes, onde um atua como servidor central e outros como clientes, possibilitando a divisão das tarefas administrativas entre esses agentes.

Vantagens:

- não depende de um ponto central de consultas, agilizando o processo, aliviando os "gargalos" na rede e no processamento dos dados;
- monitoração distribuída pela rede através de diversos gerentes locais;
- informação de gerenciamento armazenadas de forma centralizada e diminuição do *overhead* entre o banco de dados e o gerente central.

Desvantagens:

- banco de dados centralizado, dependente de replicação para evitar indisponibilidade de sistema;
- maior riscos de segurança devido ao maior número de dispositivos envolvidos e consequente aumento de tarefas administrativas;

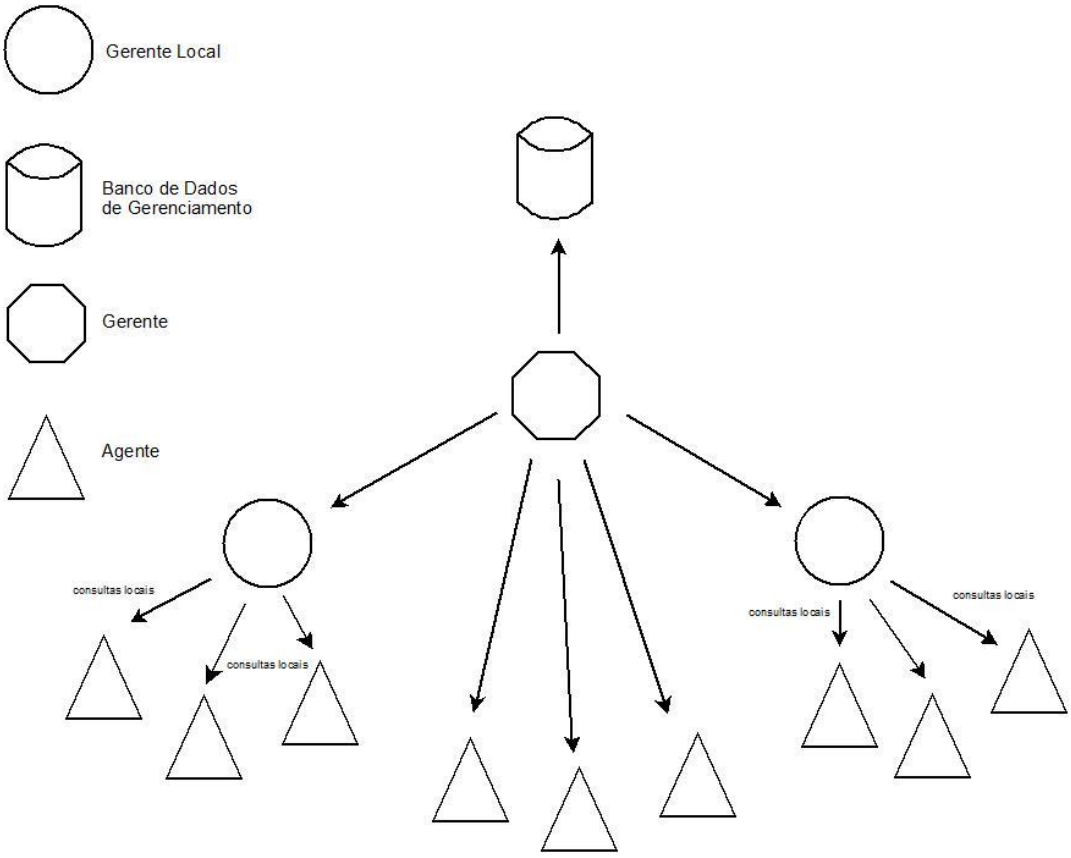

Figura 2.3: Exemplo de arquitetura hierárquica

Por fim, a **arquitetura distribuída** basicamente é uma combinação das duas anteriores onde há diversos pontos de gerenciamentos distribuídos, cada um com seu banco de dados, seus gerentes e seus clientes. Estes bancos de dados são replicados entre si, eliminando o problema de redundância, aumentando a disponibilidade e otimizando o desempenho do processamento como um todo, entretanto isso agrega um tráfego extra de dados pela rede.

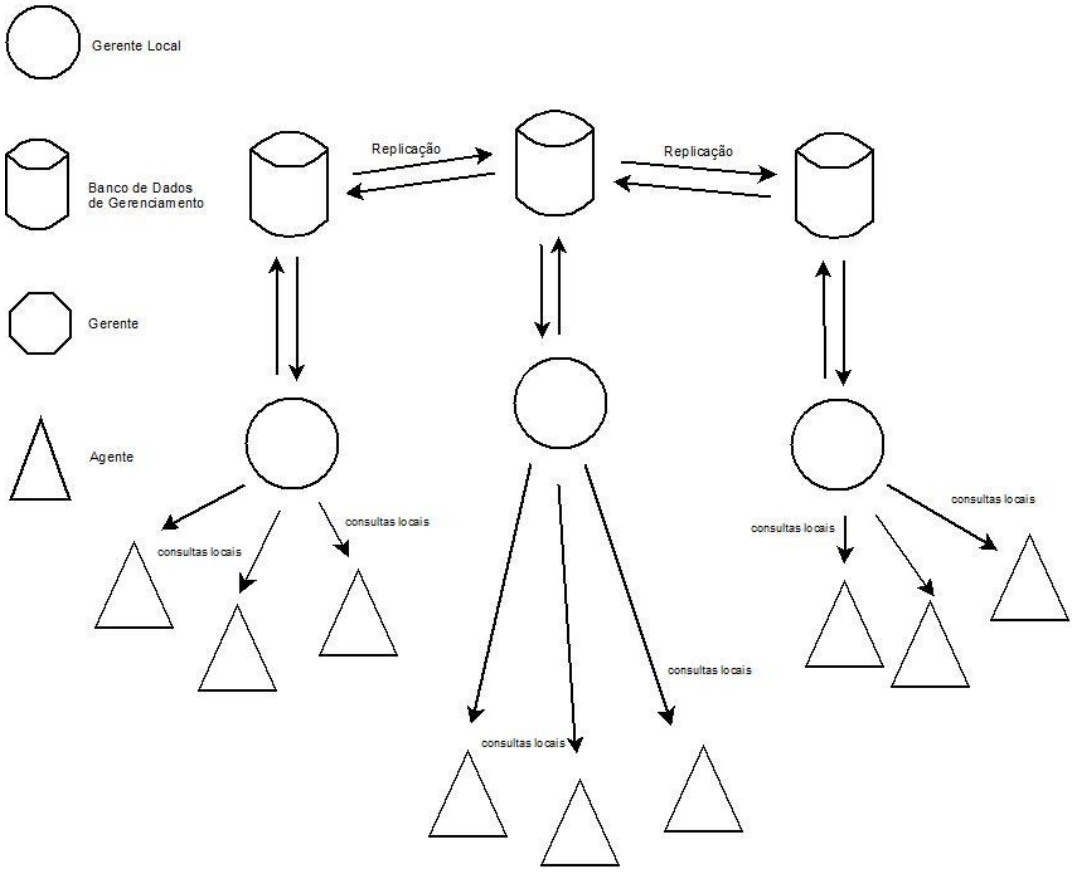

Figura 2.4: Exemplo de arquitetura distribuída

2.2.2 Classificação de Martin-Flatin

A classificação apresentada por Martin-Flatin (1999) baseia-se em três princípios:

- separa os paradigmas entre dois tipos: centralizados e distribuídos;
- isola as diferenças entre os paradigmas novos e tradicionais;
- distingue os paradigmas baseados em delegação vertical e horizontal.

Os paradigmas tradicionais são constituídos pelos paradigmas centralizados, pelos paradigmas hierárquicos fracamente distribuídos e paradigmas hierárquicos fortemente distribuídos. Nestes paradigmas estão incluídas as arquiteturas SNMP, OSI e TMN, que caracterizam-se pelo fato do processamento realizado para gerenciar a rede ficar concentrado em um grupo pequeno de estações de gerenciamento e os agentes serem meros coletores de informação.

A arquitetura OSI não é utilizada para gerenciamento internet e a arquitetura TMN é destinada à telecomunicações.

Nos paradigmas hierárquicos fortemente distribuídos encontram-se aqueles baseados em Código Móvel e Objetos Distribuídos. Os paradigmas baseados em código móvel visam prover flexibilidade transferindo dinamicamente programas para os agentes onde será executados. Duas abordagens utilizam estes conceitos: redes ativas e gerenciamento por delegação, sendo que estas redes ativas permitem que os usuários injetem programas nos nodos da rede que podem manipular o fluxo de dados do usuário que trafega pelo nodo. A proposta do gerenciamento por delegação é transferir funcionalidades para agentes remotos ou gerentes delegando a execução dinâmica de tarefas. O gerenciamento por delegação será apresentado com mais detalhes nas próximas seções.

Nos paradigmas de gerenciamento baseado em objetos distribuídos estão as tecnologias CORBA (*Common Object Request Broker Architecture*) e ODMA (*Open Distributed Management Architecture*). Essas tecnologias foram uma iniciativa da indústria para os problemas de interoperabilidade da orientação a objetos que acabou sendo utilizada para o gerenciamento de rede.

Os paradigmas cooperativos fortemente distribuídos são baseados em agentes inteligentes. Oriundos da Inteligência Artificial distribuída (multi-agentes), os agentes deixam de ser meros coletores de dados e passam a efetuar processamento sobre os dados coletados. Essa abordagem permite dividir as tarefas de gerenciamento entre um grupo de entidades autônomas, posicionadas o mais próximo possível do equipamento gerenciado, reduzindo o volume de informações de gerenciamento que precisam trafegas pela rede.

2.2.3 Classificação de Schönwälder

Para classificar os paradigmas de gerenciamento, Schönwälder (2000) estabelece uma relação entre o número de agentes e gerentes. Os autores definem quatro classes de sistemas ou formas de gerenciamento de rede: gerenciamento centralizado, quando o sistema possuem apenas um agente, gerenciamento fracamente distribuído, quando o sistema possuir dois ou mais gerentes, porém com um número bem inferior ao número total de componentes (soma de agentes e gerentes), gerenciamento fortemente distribuído, quando existe no sistema muito mais do que dois gerentes, mas em número inferior ao total de componente e gerenciamento cooperativo quando o número de gerentes é aproximado ao número total de componentes.

Em uma análise da composição de cada gerenciamento, percebe-se que o centralizado é um modelo mais simples ao passo que o cooperativo é mais escalável e flexível, sendo estas as principais características desse último modelo de gerenciamento, o qual focamos nossa atenção.

A escalabilidade do sistema baseia-se em três pilares: a carga computacional do gerente é reduzida pela delegação das funções administrativas; os gerentes intermediários monitoram um subconjunto de agentes e repassam informações agregadas aos gerentes. A redução de carga computacional na rede é o segundo pilar pois a localização dos gerentes intermediários, mais próximos dos gerentes, permite enviar dados processados e compactados para os gerentes. Por fim, com a delegação

dinâmica das funções de gerenciamento ou mobilidade de processos, apenas os procedimentos ativos precisam ser armazenados, reduzindo o volume de armazenamento nos nodos.

Já a flexibilidade consegue-se devido às tarefas de gerenciamento poderem ser atribuídas dinamicamente, podendo ser alteradas livremente, com novas tarefas podendo ser definidas rapidamente.

2.2.4 Gerenciamento usando *Web Services*

Os serviços da *web* são baseados em uma arquitetura XML com mecanismos de processamento distribuído para pesquisa e publicação dos serviços de gerenciamento, sendo essa arquitetura distribuída, aliada à definição de interfaces complexas e falíveis, viabilizadora de sua aplicação na comunicação entre gerentes de diversos domínios.

Podemos citar as seguintes vantagens dos serviços da *web* no gerenciamento de rede, de acordo com MANNAERT, 2005:

- Os serviços *web* oferecem os mecanismos para implementar a arquitetura desejada. Entretanto, ele por si só não define a arquitetura a ser usada para gerenciar a rede;
- Pode-se definir mensagens pré-definidas e configurada nos serviços *web* para gerenciar os recursos da rede localmente ou em sites remotos, sendo esse um grande facilitador das tarefas administrativas destes serviços;
- O servidor *web* pode adaptar-se para receber tanto informações do modelo convencional de gerenciamento (gerente-gerente) como dos modelos distribuídos (gerente-agente e suas ramificações);
- A segurança de dados é privilegiada por poder-se implementar HTTS e SSL no transporte de dados;
- Pode-se migrar com facilidade os serviços *web* para outros *spots* tendo em vista da facilidade de reutilização de código.

3 FERRAMENTAS PARA GERENCIAMENTO DE REDES

A maioria das ferramentas disponíveis para monitoramento de rede são baseadas e/ou descendentes do Multi Router Traffic Grapher (MRTG). 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 belos gráficos representando o tráfego da conexão de rede monitorada. Estes gráficos são incluídos em páginas web que podem ser visualizadas de qualquer navegador moderno. Somadas à 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 obteve do roteador. Este log é automaticamente consolidado, e com isso ele não cresce com o tempo, mas ainda contém todos os dados relevantes de todo o tráfego dos últimos 2 anos. Isto tudo é realizado de uma maneira muito eficiente. Com ele você pode monitorar mais de 200 links de rede de qualquer estação UNIX decente.

As ferramentas expostas a seguir tem suas raízes baseadas nos conceitos do MRTG, mas evoluíram em muitos aspectos, acompanhando as novas tendências voltadas para a *web* e as novas e poderosas ferramentas de desenvolvimento com foco na usabilidade e visibilidade do produto.

3.1 CACTI

Cacti é uma ferramenta *freeware* que recolhe e exibe informações sobre o estado de uma rede de computadores através de gráficos, sendo um *frontend* para a ferramenta *RRDTool*, que armazena todos os dados necessários para criar gráficos e inserí-los em um banco de dados *MySQL*. Foi desenvolvido para ser flexível de modo a se adaptar facilmente a diversas necessidades, bem como ser robusto e fácil de usar. Monitora o estado de elementos de rede e programas bem como largura de banda utilizada e uso de CPU. O frontend foi escrito na linguagem PHP e contém suporte ao protocolo SNMP.

RRDTool é um sistema de base de dados Round-Robin criado por Tobias Oetiker sob licença GNU GPL. Foi desenvolvido para armazenar séries de dados numéricos sobre o estado de redes de computadores, porém pode ser empregado no armazenamento de qualquer outra série de dados como temperatura, uso de CPU, etc. RRD é um modo abreviado de se referir a Round Robin Database (base de dados *round-robin)*.

Com o Cacti é possível gerar gráficos referentes a uso de memória física, memória virtual, quantidade de processos, processamento, tráfego de rede, quantidade de espaço em disco etc. Através do SNMP, permite ter acesso a gráfico não só de sistemas operacionais Linux, mas também de Windows e de dispositivos de rede como roteadores e switches, bem como qualquer dispositivo que suporte SNMP. O modo como o Cacti busca informações via SNMP de um dispositivo tem efeito direto nas opções de SNMP disponíveis nele, que atualmente divide-se em três tipos, ilustrados abaixo:

Tabela 3.1: Meios de se obter dados com SNMP no Cacti

Tipo	Descrição	Opções Suportadas	Onde é utilizado
SNMP Externo	Chama os binários net-snmp snmpwalk e snmpget que estão instalados no sistema	Todas opções de SNMP	Interface Web e *poller* PHP
SNMP Interno (php-snmp)	Usa as funções de SNMP do PHP que estão ligadas à net-snmp ou ucd-snmp durante o tempo de compilação	Versão 1 apenas	Interface Web e *poller* PHP (poller.php)
Spine SNMP	Liga-se diretamente com net-snmp ou ucd-snmp e chama a API diretamente	Todas opções de SNMP	*Poller* baseado em linguagem C (spine)

Fonte: CACTI web site: <http://www.cacti.net/>, acessado em 28.11.2008

Todas as três versões do SNMP são suportadas atualmente pelo Cacti.

Sua arquitetura prevê a possibilidade de expansão através de inúmeros plugins desenvolvidos por sua comunidade que adicionam novas funcionalidades. Um bom exemplo destes plugins é o PHP Network Weathermap que mostra um mapa da rede e o estado de cada elemento. O produto permite aos usuários agendar serviços em intervalos pré-determinados a gerar gráficos a partir destes resultados e ele permite lidar com diversos usuários simultâneos, cada um com seus gráficos gerados e com suas *queries* na rede, além de ser flexível, permitindo outros tipos de coletas de dados desde que obedeçam os limites do RDDTool.

O Cacti pode usar dois tipos de agentes remotos: o primeiro, um script PHP previsto para pequenas redes - via o arquivo cmd.php, ou então através do *poller* “spine” (antigamente chamado de agente ou *daemon* cactid), um pequeno agente escrito em C que pode ser amplamente escalado para grandes redes de computadores.

A base de dados gerada possui um tamanho máximo o qual uma vez atingido não é ultrapassado. Os dados numéricos armazenados são consolidados conforme a configuração fornecida, de modo que a resolução deles seja reduzida de acordo com o tempo que eles estão armazenados. Neste processo, apenas as médias dos valores antigos são armazenados.

O produto foi desenvolvido para Linux/Unix e somente este ano que desenvolveu-se uma versão para Windows, mas ainda em fase de testes *beta*. Seus requerimentos estão listados na tabela 2:

Tabela 3.2: Requisitos de software do Cacti (Linux/Unix)

Software	**Versão**	**Comentários**
RRDTool	1.0.49 ou 1.2.x/superior	
MySQL	4.1.x ou 5.x/superior	
PHP	4.3.6/superior ou 5.x/superior	A versão 5.x é recomendada por suas funcionalidades avançadas
Apache	2 ou superior	
IIS	6.0 ou superior	

Fonte: CACTI web site: <http://www.cacti.net/>, acessado em 28.11.2008

Devido à suas características, o Cacti pode ser utilizado tanto por administradores inexperientes assim como pelos mais experientes. Conforme sua própria documentação, o Cacti é:

> "uma solução completa de geração de gráficos sobre redes computacionais, desenhado à maximar a utilização dos dados armazenados via RRDTool, gerando gráficos funcionais. Cacti provêm um agente rápido, com modelos de gráficos avançados, múltiplos métodos de aquisição de dados e opções de gerenciamento de prontas para serem usadas. Tudo isso é provido em uma interface intuitiva, de fácil utilização e fácil adaptação tanto à pequenas LANs com grandes redes com centenas de dispositivos"

Uma vez instalado no sistema e logado, o administrador tem que informar o Cacti sobre os dispositivos que deseja controlar. Ele vem com uma lista de dispositivos comuns, tais como servidores Linux, roteadores Cisco, servidores NetWare, e até mesmo workstations Windows 2000/XP. Se o dispositivo não está na lista, você pode criar um dispositivo genérico e especificar os parâmetros que você precisa para monitorá-lo. Você também pode salvar isto como um modelo para uso futuro, sendo essa interface web *user-friendly*, junto com a documentação disponível, o destaque da ferramenta.

Depois de criar os dispositivos, você tem que selecionar os parâmetros que pretende acompanhar de cada dispositivo, e criar os gráficos. O Cacti fornece modelos para os parâmetros comuns, tais como o uso da CPU, o tráfego de rede, os usuários conectados

e coisas do gênero, mas você pode rapidamente fazer seus próprios modelos também, bastando alguns minutos para criar os gráficos para servidores Linux/Windows. Os parâmetros para monitorar cargas médias de dispositivos são, por padrão, a largura de banda utilizada e os processos em execução, já oferecidos pela ferramenta. Para controlar os switchers/roteadores é mais complexo, mas a documentação é ampla e satisfatória.

As informações recolhidas são muitas e só serão úteis se apresentadas corretamente, sendo que, se há uma gama muito grande de dispositivos a serem monitorados, pode-se visualizar um pequeno número de gráficos, facilitando a administração do sistema, ao passo que dezenas ou centenas de parâmetros estão sendo monitorados, essa tarefa torna-se muito difícil. O Cacti permite que os gráficos gerados sejam organizados de diversos modos: configurando-os em forma de árvores ou agrupando todos os gráficos de um mesmo tipo sob um gráfico maior, podendo-se ter um gráfico em duas ou mais árvores também. Estas árvores de gráficos possuem diversas maneiras de serem organizadas, de acordo com a necessidade do administrador, podendo-se gerar gráficos de praticamente qualquer dispositivo que se deseje. A variedade de modelos que vêm com a instalação padrão é suficiente para cuidar de redes simples, e você pode criar seus próprios tipos de dados e modelos mais complexos para redes, apesar do Cacti não conseguir exibir e tabular dados numéricos.

Importante salientar que o Cacti não está limitado ao protocolo SNMP somente, pode-se alimentá-lo de outros modos – podendo apontá-lo para um caminho de um script ou comando externo – padrão *nix bash scripts, scripts Perl, ou qualquer script que é executado a partir do prompt de comando do servidores *nix. O Cacti reúne os dados em uma tarefa *cron* e preenche uma base de dados MySQL própria os resultados. Nos *sites* de usuários de Cacti, há muitos scripts desenvolvidos para esses fins, que vão da coleta de dados em servidores Apache até filas de e-mail em servidores Sendmail para recolher estatísticas.

O Cacti não exige demasiados recursos do *host* em que ele está rodando, pois foi escrito em PHP sobre plataforma *web*, sendo por natureza uma ferramenta ágil e rápida. Pode-se autorizar vários administradores como usuários do Cacti ou então dando-lhes direitos restritos a apenas algumas áreas da ferramenta, permitindo criar usuários que podem altera apenas alguns parâmetros de gráficos e outros que podem apenas visualizá-los, mas preservando as configurações individuais de cada um

Como pontos negativos, destaca-se o fato do produto não possuir um agente de descoberta automático, ou seja, toda rede tem que ser adicionada manualmente, apesar de já haver plugins de terceiros que fazer esse trabalho – ainda assim, não é uma *feature* padrão da ferramenta, podendo tornar o trabalho do administrador muito penoso se a rede for grande. Mesmo assim, o software é extremamente escalável, e pode ser usado para controlar praticamente qualquer parâmetro mensurável em hardware, tais como temperatura e umidade (quando suportado). O desenvolvimento da ferramenta é constante e ela possui uma rede grande de usuários que compartilham suas experiências em diversos fóruns espalhados pela Internet.

3.2 Nagios

O Nagios é um aplicativo de monitoramento de sistemas e de redes, podendo ser estendido amplamente a um gerenciador de redes graças aos diversos plug-ins disponíveis em cua comunidade. Ele verifica clientes e serviços especificados, gerando alertas quando algo está fora dos padrões pré-definidos. Originalmente desenvolvido para rodar em Linux, há pacotes personalizados para distribuições comuns como Fedora, Ubuntu, SUSE e Debian.

Algumas das várias ferramentas do Nagios TM incluem:

- Monitoramento de rede e serviços (SMTP, POP3, HTTP, NNTP, PING, etc.);
- Monitoramento dos recursos de clientes (carga de processador, uso de disco, etc.);
- Organização simples de plugins que permite aos usuários facilmente desenvolverem seus próprios serviços de checagem;
- Checagem paralela de serviços;
- Habilidade para definir hierarquia de redes de clientes usando clientes pais (*parent hosts*), permitindo a detecção e distinção entre clientes que estão desativados e aqueles que estão inalcançáveis;
- Notificação de contatos quando problemas em serviços e clientes ocorrerem ou forem resolvidos (via email, pager, ou métodos definidos pelo usuário);
- Habilidade para definir tratadores de eventos (event handlers) que serão executados durante eventos de serviços ou clientes na tentativa de resolução de problemas;
- Rotação automática de arquivos de logs;
- Suporte para implementação de clientes de monitoramento redundantes;
- Interface *web* opcional para visualização do status atual da rede, histórico de notificações e problemas, arquivos de log, etc;

A única exigência para rodar o Nagios é ter um computador rodando Linux (ou variantes do UNIX) e um compilador C, além de ter, evidentemente, a pilha TCP/IP instalada, já que a maioria das checagens de serviços serão feitas através da rede. Não é obrigatório usar os CGIs incluídos com o Nagios por padrão, mas se optar por usá-los,os seguintes programas serão necessários:

1. Um servidor *web* (preferencialmente Apache);
2. gd library de Thomas Boutell versão 1.6.3 ou superior (exigido pelos CGIs statusmap e trends).

O Nagios é distribuído sob os termos da GNU General Public License Versão 2, publicado pela Free Software Foundation, popularmente conhecido apenas por GPL, garante permissão de copiar, distribuir e modificar o produto sob certas condições. Condições estas especificadas no arquivo ‘LICENSE’ que vem na distribuição do software ou acessível online no site www.nagios.org. O Nagios é fornecido sem

qualquer garantia de qualquer tipo, incluindo a garantia de desenho, mercantibilidade e adequação para um propósito particular.

Uma vez instalado, existem muitos arquivos de configurações que será necessário criar ou editar antes de iniciar o monitoramento da rede. Eis um sumário de cada um:

3.2.1 Arquivo de configuração principal:

O arquivo de configuração principal (comumente */usr/local/nagios/etc/nagios.cfg*) contém várias diretivas que afetam a operação do Nagios. Este arquivo de configuração é lido pelo processo do Nagios e pelos CGIs e deve ser o primeiro arquivo de configuração a ser criado/editado. Um exemplo deste arquivo é gerado automaticamente quando o script de inicialização do sistema é executado, antes de compilar os binários, localizado no diretório da distribuição ou no subdiretório *etc/* do sistema operacional. Quando instalam-se os exemplos de arquivos de configuração usando o comando *make install-config*, um exemplo de arquivo de configuração principal será colocado no seu diretório de configuração (geralmente */usr/local/nagios/etc*). O nome padrão para o arquivo de configuração principal é *nagios.cfg*. A tabela abaixo ilustra alguns dos tipos de objetos que podem ser manipulados neste e em outros arquivos de configuração do Nagios:

Tabela 3.3: Tipos de objetos contidos no sistema Nagios

Object	Description
host	Hosts are physical devices like servers, routers, and firewalls.
hostgroup	Host groups are collections of hosts that generally have something in common, like their type or location.
service	Services run on hosts and can include actual services like SMTP or HTTP, or metrics such as disk space.
servicegroup	Service groups are collections of services that generally have something in common.
contact	Contacts are escalation or notification points that can potentially be contacted when an event occurs.
contactgroup	Contact groups are collections of contacts. All contacts need to be in a contact group.
timeperiod	Time periods are defined windows of time—for example, during business hours.
command	Commands are called by the check process to perform an action—for example, a command to check the status of a host using the ping command.
servicedependency	Allows a service or services to be dependent on other services.
serviceescalation	Provides a notification escalation process for services.
hostdependency	Allows a host or hosts to be dependent on other hosts.
hostescalation	Provides a notification escalation process for hosts.
hostextinfo	Host Extended Information changes and customizes the way hosts are displayed on the Nagios web console.
serviceextinfo	Service Extended Information changes and customizes the way services are displayed on the Nagios web console.

Fonte: Nagios web site: <http://www.nagios.org/>, acessado em 12.10.2008

3.2.2 Arquivo(s) de recurso(s):

Arquivos de recurso são usados para armazenar macros definidas por usuários. Arquivos de recursos podem também conter outras informações (como configurações de conexão a banco de dados), ainda que isso dependa de como o Nagios foi compilado. O ponto principal de ter arquivos de recurso é usá-los para armazenar informações de configuração sensitivas e não para torná-las disponíveis aos CGIs. Um ou mais arquivos podem ser especificados opcionalmente usando a diretiva *resource_file* no arquivo de configuração principal.

3.2.3 Arquivos de configuração de objetos:

Arquivos de configuração de objetos (historicamente chamados de arquivos de configuração de "clientes") são usados para definir clientes, serviços, grupos de clientes, contatos grupos de contatos, comandos, etc. É neste arquivo que são definidos parâmetros que se deseja monitorar.

3.2.4 Arquivo de configuração de CGI:

O arquivo de configuração de CGI (geralmente */usr/local/nagios/etc/cgi.cfg*) contém numerosas diretivas que afetam a operação dos CGIs. Um exemplo de arquivo de configuração de CGI é gerado automaticamente quando o script *configure* é executado antes de compilar os binários. Quando os exemplos de arquivos de configuração são instalados usando o comando *make install-config*, um arquivo de configuração de CGI será colocado no mesmo diretório que o arquivo de configuração de clientes e o arquivo de configuração principal (geralmente */usr/local/nagios/etc*). O nome padrão para o arquivo de configuração de CGI é *cgi.cfg*.

3.2.5 Arquivos de configuração de informações estendidas:

Arquivos de configuração de informações estendidas são usados para definir informações adicionais para serviços e clientes que devem ser usados pelo CGI. São nestes arquivos que se definem elementos como coordenadas dos gráficos, formato do ícones, entre outros.

Sendo o foco do produto em monitoramento, diversas opções existem de como aperfeiçoar essa tarefa, apoiados em muitos plugins externos. Abaixo uma lista dos mais comuns:

Tabela 3.4: Principais plugins e addons para o Nagios

Nome	Site	Comentário
Centreon	www.centreon.com	Um frontend em PHP/MySQL com novas funcionalidades e configuração simplificada
NagVis	www.nagvis.org	Addon para visualizar resultados de monitoramento de dispositivos
NagCon	vanheusden.com/nagcon	Monitor de console para Unix

Check_Nagios_Summary	vanheusden.com/check_nagios_summary	Addon que permite monitoramento distribuido com o Nagios
NagiosQL	www.nagiosql.org	Extensão de configuração web para o Nagios 2.x-3.x usando MySQL como armazenamento
Monarch	Sourceforge.net/projects/monarch	*Engine* web para configuração e gerenciamento do Nagiox 1.x e 2.x
PerfParse	Perfparse.sf.net	Analisador de dados focado em performance
PNP	www.pnp4nagios.org	Ferramenta para otimizar os dados de performance em gráficos
phpNagios	www.phpnagios.com	Ferramenta via Web para configurar o Nagios
NagMin	Nagmin.sf.net	Módulo adicional ao Webmin que administra centralmente o Nagios versão 1.x
Opsview	Opsview.sourceoforge.net	Configurador Web para alertas de monitoramento SNMP distribuído.

Fonte: Web sites de cada produto. Acessados em 29.11.2008

3.3 ZenOSS

O ZenOSS foi desenvolvido em meados de 2002, quando o mercado já estava aquecido pelos produtos proprietários da IBM, HP e Computer Associates e por soluções open-source como Nagios, Net-SNMP e RRDTool. Entretanto essas soluções cobriam lacunas específicas nas tarefas administrativas de rede, mas nenhuma delas tinha um pacote completo. Esse foi o motivo que levou a Erik Dahl iniciar o desenvolvimento dessa ferramenta de gerenciamento de redes.

3.3.1 Arquitetura base

A arquitetura base do produto possui uma característica interessante: ela é desenvolvida seguindo uma representatividade única de um ambiente de TI. Os objetos armazenados chamados “ZenModel” armazenam classes e estrutura de dados que refletem um ambiente de TI, incluindo configuração detalhada de recursos, relacionamentos entre componente, perfis de recursos, coleções de configurações e até mesmo regras de processamento.

Essa visão consolidada e detalhada permite ao ZenOSS prover visibilidade ampla e profunda do problema de rede, assim que ele ocorre. Adicionalmente, a classificação hierárquica do sistema ZenOSS torna simples a configuração e o gerenciamento de grandes redes computacionais, bem como compartilhar essas regras com outros sistemas. A figura abaixo ilustra a arquitetura do sistema:

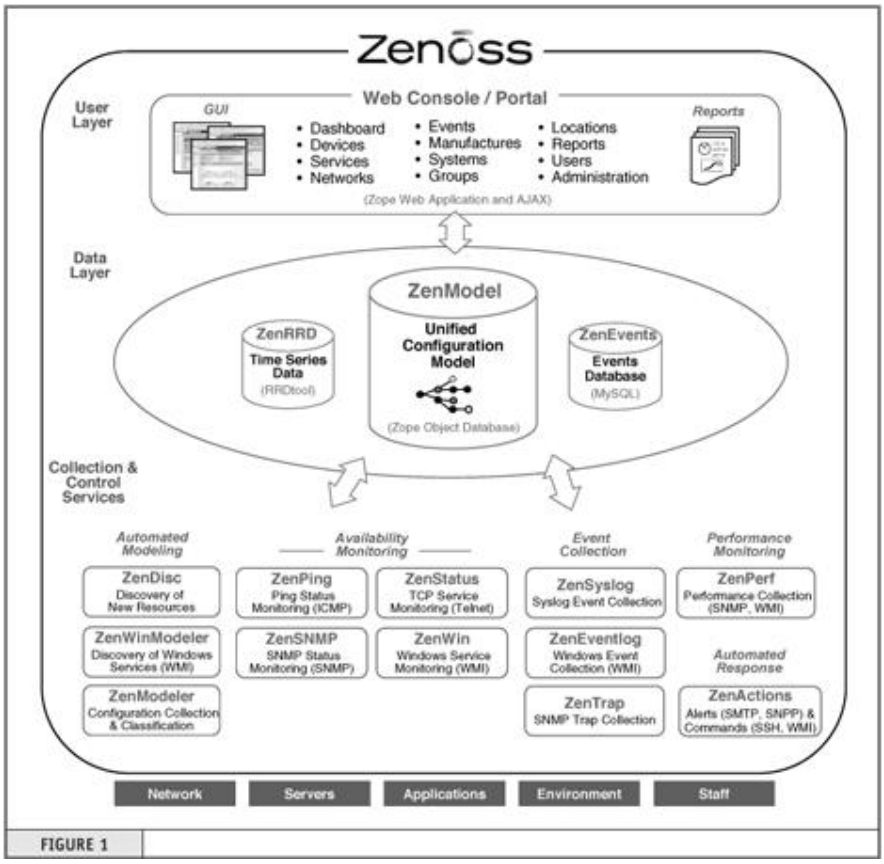

Figura 3.1: Arquitetura do sistema ZenOSS

A camada de dados do usuário consiste de um GUI apresentado por relatórios em HTML. Escrito usando o Zope Web, o GUI é seguro e fácil de ser customizado e/ou estendido. Componentes feitos em Ajax são usados para melhorar a experiência do usuário através das diferentes telas.

As principais características do console web são:

- acesso seguro;
- facilidade de customizar e estender as *features*;
- portal integrado via navegador;
- principais telas: Dashboards, Devices, Services, Networks, Events, Manufactures, Systems, Groups, Locations, Reports, Users, and Management;

As principais características da interface de relatórios (*reporting interface*) incluem:

- biblioteca de relatórios padrão;
- relatórios gerados em gráficos;
- relatórios customizáveis de fácil criação;

- relatórios padrões gerados pela biblioteca padrão: Device Inventory, Software Inventory, Service Inventory, EventClasses Inventory. Event Mapping Inventory, Heartbeats, Device Detail, Device History, Load Average, Configuration Collection Age, New Devices, Ping Status Issues, and SNMP Status Issues;

A camada de dados do ZenOSS engloba três tipos diferentes de informações, cada um armazenado usando um mecanismo próprio:

- ZenModel: modelo unificado do ambiente padrão de TI e gerenciamento de configurações. Esses dados são armazenados no *Zope Object Database (ZODB)*;
- ZenRRD: modelo usado para armazenar históricos de informações e gerar gráficos a partir desses dados. Baseado na ferramenta RRDtool;
- ZenEvents: banco de dados para eventos ativos e guardar histórico de eventos, construído e baseado em MySQL.

A camada de ***Collection & Control Services*** é uma série de processos de longa duração que provêm uma gama de tarefas de controle que incluem a configuração de modelagem, monitoramento de disponibilidade, monitoramento de performance, catalogar eventos e resposta automatizadas. Cada um desses serviços perfaz uma diferente função ao passo que mantém um modo similar de operação. Cada serviço:

- interage com o banco de dados ZenModel para consultar e configurar informações;
- pode rodar como uma instância local ou distribuída para melhorar a escalabilidade e disponibilidade do mesmo;
- tem seu próprio script de linha de comando ou pode ser manipulado por um script global chamado de “ZenOSS global script”.
- pode ser executado como um serviço em modo *daemon* ou a partir da linha de comando para *debugging*. A figura abaixo ilustra esses diferentes modos de serviço:

Tabela 3.5: Serviços da camada Collection & Control Services

Service	Group	Description	Runs As
ZenDisc	Modeling	Discovers new devices on the network	Linux daemon
ZenModeler	Modeling	Retrieves configuration detail and map resources to the classification model	Linux daemon
ZenWinModeler	Modeling	Discovers Windows-based services	Windows service
ZenStatus	Availability	TCP service monitoring (Telnet, SSH)	Linux daemon
ZenPing	Availability	Ping Availablity Monitoring (ICMP)	Linux daemon
ZenSNMP	Availablity	SNMP Availability Monitoring (SNMP)	Linux daemon
ZenWin	Availability	Windows service monitoring	Windows Service
ZenPerf	Performance	Performance collection (SNMP, Telnet, SSH)	Linux daemon
ZenSyslog	Event Collection	Syslog Event Collection	Linux daemon
ZenEventlog	Event Collection	Collectioon of windows events (WMI)	Windows Service
ZenTrap	Event Collection	SNMP trap collection (SNMP)	Linux daemon
ZenActions	Automated Response	Alerting (SMTP, SNPP) and command execution (SSH)	Linux daemon

A configuração de banco de dados do ZenOSS é apresentada em uma estrutura tipo árvore, muito parecida com um gerenciador de arquivos onde pode-se navegar entre pastas diferentes facilmente, facilitando a referência à classes (como se fossem diretórios), instâncias (como se fossem arquivos) e grupos lógicos (como se fossem *links*). A tabela abaixo ilutra essa um exemplo dessa representatividade:

Tabela 3.6: Exemplo de configuração de entidades no banco de dados

/Device/Servers/Linux	*Path* referência para todos dispositivos, servidores de outras classes (sub-classes) e sub-classes Linux
/Device/Servers/Linux/Http	*Path* referência para todos servidores web Linux
/Devices/Servers/Linux/Http/hrweb01	*Path* referência para servidore web Linux chamado de hrweb01 (exemplo)
/Network/10.0.0.0	*Path* referência para rede iniciando em 10.0.0.0
/Systems/Hrweb01 /Systems/HR/hrdb01	Dois servidores associados ao nome lógico de sistema HR
/Locations/East/Datacenter	*Path* para todos dispositivos no Datacenter da região leste

Fonte: ZenOSS web site: <http://www.zenoss.com/>, acessado em 30.08.2008

Em cada nodo de *path*, podem-se visualizar relatórios (que se aplicam ao nodo corrente e nodos filhos) e aplicar novas regras (que serão herdadas por todos os nodos filhos, a não ser se explicitamente bloqueadas para tal delegação no próprio nodo). A

hierarquia estrutural completa dos objetos é divida em cinco partes primárias que provêm nomes físicos para entidades de *core* (básicas) de sistema (/Device, /Networks, /Services, /Manufacturers e /Events) e três partes organizacionais que provêm a possiblidade e agrupar logicamente os dispositivos (/Locations, /Systems e /Groups).

- *Automated Discovery* (Procura automática): assim que o sistema é iniciado, ele faz um rastreamento pela(s) rede(s) cadastrada(s) através do seu sistema de serviço de procura e modelagem. Esses serviços automaticamente mantém o ZenModel atualizado e a configurações e relacionamentos catalogadas em uma base de dados, que também matém o histórico dos dispositivos de rede;

- *Layered Customization* (Camadas customizáveis): como descrito anteriormente, o ZenOSS mantém uma estrutura customizada, semelhante à um ambiente real de TI, permitindo configurar e classificar independentemente os dados, regras de processamento, plug-ins, serviços de integração de aplicações e o código base do sistema.

Na página do produto (www.zenoss.com), pode-se baixar três versões: a gratuita (CORE) e duas versões pagas, a PRO e a ENTERPRISE, cada uma com suas características, conforme tabela abaixo:

Tabela 3.7: Características de cada versão do ZenOSS

	CORE	PRO	ENTERPRISE
Capabilities			
Configuration Management Database (CMDB)	✓	✓	✓
Auto-Discovery	✓	✓	✓
Inventory & Change Tracking	✓	✓	✓
Availability Monitoring	✓	✓	✓
Performance Monitoring	✓	✓	✓
Event/Log Management	✓	✓	✓
Alerting & Reporting	✓	✓	✓
Automatic Remediation	✓	✓	✓
Web Portal & Dashboards	✓	✓	✓
Integration APIs	✓	✓	✓
Network Visualization (Geography & Topology)	✓	✓	✓
Community Report Library	✓	✓	✓
Community Monitor Library	✓	✓	✓
Role-Based Access Control		✓	✓
Commercial Report Library		✓	✓
Commercial Monitor Library		✓	✓
Commercial Integration Library		✓	✓
Commercial Model Library		✓	✓
WMI based modeling of disk, CPU, h/w & s/w inventory		✓	✓
Windows Perfmon Support		✓	✓
RANCID Integration		✓	✓
Tomcat Monitoring		✓	✓
Complete VMware Virtual Infrastructure (VI3) Management			✓
Enhanced Oracle Monitoring			✓

	CORE	PRO	ENTERPRISE
Advanced WebLogic and JBoss Monitoring			✓
Synthetic Transactions (Web, Email, Database)			✓
Predictive Thresholds			✓
Remedy Integration			✓
Global Dashboard			✓
Distributed Configuration Manager			✓
High Availability Package Available			✓
Builds/Deployment Options			
Software Appliance (Evaluation)	✓	✓	✓
Source Installation	✓		
Native Binary Installers	✓		✓
Point & Click Stack Installers	✓		✓
Certified Commercial Builds		✓	✓
Software Appliance (Production)		✓	✓
Hardware Appliance		✓	✓
Distributed Collector Package			✓
Service Features			
Community Forum Access	✓	✓	✓
Deployment Planning Professional Services		2 hours	3 hours
Web-based Portal		Unlimited	Unlimited
E-mail Incident Support		✓	✓
Phone Support		4 / year	Unlimited
Priority 1/High Severity Response Time SLA		8 hours	4 hours
Automatic Patch Management		✓	✓
Software Update Service		✓	✓
Unlimited Phone Support			✓
Remote Troubleshooting			✓
Platinum Upgrade Option			✓
IP Assurance			
Repair and Replace		✓	✓

Fonte: ZenOSS web site: <http://www.zenoss.com/>, acessado em 30.11.2008

O produto é customizável em todos os aspectos possíveis, desde sua "cara" (skin) até os componentes que deseja-se integrar para monitorar a rede, tais como regras, serviços, plug-ins, entre outros, que divide-se da seguinte forma:

- *Processing rules* (regras de processamento): eventos, configurações de regras que são gerenciados via web GUI do produto;
- *Skins*: layout customizável, modificável através de *templates* e *stylesheets* (ZPT, CSS);
- *Plug-Ins*: adicionando ou removendo funcionalidades através de código-base (Python, Perl);
- *Interfaces*: integração de aplicações através de APIs de web services (XML, RPC);

- *Core Coding* (código base): modificar o código base do produto (Python, Zope, MySQL);

A integração com a plataforma Windows da Microsoft está garantida através do serviço *WMI Collector*, um serviço nativo do Windows que levanta dados usados para fins de monitoramento de rede. Esse serviço roda nas máquinas Windows e envia dados e métricas remotamente, eventos e estatísticas para a o ZenOSS. Em desenvolvimento encontram-se agentes próprios do ZenOSS para coletar dados pela rede bem como suporte direto aos plug-ins do Nagios.

3.4 ManageEngine OpManager

O OpManager é um software completo de gerenciamento de rede. Ele é desenhado para oferecer a integração entre help-desk, WAN, servidores, aplicações, gerenciamento de ativos e análise de tráfego da WAN, bem como monitoramento real-time de firewalls, servidores Windows/Linux/Unix, servidores de e-mail Exchange, servidores Active Directories, roteadores, impressoras, switches, no-breaks, serviços Web, entre outros. Escrito em Perl e Python, o OpManager automatiza várias tarefas de monitoramento e remove a complexidade associada ao gerenciamento da rede, com um complexo mas eficiente sistema de alertas e gatilhos, notificando instantaneamente os administradores quando e como ocorrem erros.

Historicamente o OpManager não se utilizava de *probes* (ou agentes) remotos para suas tarefas, entretanto essa característica se faz presente nas mais novas versões do sistema (incorporado no início de 2007). Este agente (chamado pela AdventNet de *probe*) fica residente nos clientes e executa diversas tarefas de rede tais como *discovering*, *polling* e *data collection*, enviando periodicamente (o intervalo de tempo é customizável) esses dados para gerentes locais ou gerente central, que recebem dados de vários dispositivos remotos.

O *design* simples e funcional do sistema permite instalações e configurações sem problemas e todos aspectos do software podem ser administrados através de uma central de operações de rede (gerente geral), que coordena todos os relatórios e provê suas soluções. O *setup* inicial consiste em fazer o download do instalador e seguir os passos do instalador, ao melhor estilo Windows. A seguir é feita a configuração do servidor central (gerente geral) com suas inúmeras opções de gerar e receber relatórios da rede e, a seguir, é feita a instalação dos *probes* remotos, que pode ser configurada em conjunto com o Active Directory, via Group Policies ou remotamente através do próprio instalador, desde que se possuam acessos à todos dispositivos com direitos de administrador. O servidor central (gerente geral) usa, por padrão, a porta 443 para rodar o serviço Web sobre SSL, entretanto pode-se alterar essa porta à gosto do administrador. Todo tráfego gerado pelos agentes e gerente geral é independente de configurações de firewall, o que é uma qualidade muito apreciada para este tipo de software.

O programa vem com um sistema de auto-discovery embutido, muito útil e facilmente configurável, pois dispõe de dispositivos pré-configurados, bem como 160

tipos de gráficos pré-configurados que abrangem a maioria dos produtos das grandes empresas do ramo, tais como dispositivos Cisco, MS-Exchange, Active Directory, Lotus Notes, Oracle, MSSQL, e servidores Dell e Compaq.

Outras ótimas opções do software são a integração/monitoramento com servidores Microsoft Exchange 2000/2003, podendo-se indentificar problemas de configuração, performance, segurança, entre outros, antes que isso afete severamente o ambiente produtivo.

As suas características principais são:

- Monitoramento de infra-estrutura de rede - Servidores, switches, roteadores, impressoras, eventos, URL, serviços, aplicações e outros;
- Suporte a SNMP, WMI, CLI e NMAP;
- Monitoramento de Aplicações - MS SQL Server, Active Directory e MS Exchange;
- Gráficos de utilização de CPU, Memória e Disco;
- Ferramentas de diagnóstico de rede;
- Monitoramento remoto;
- Alertas configuráveis e escalonáveis;
- Integrável com o ServiceDesKPlus e outras ferramentas de Help Desk.

Todavia, apesar dessas qualidades, o produto tem alguns ponto importantes que devem ser melhorados e levados em conta na hora de compará-lo com outras ferramentas: as opções de varredura e identificação do tráfego de rede gerado pelos dispositivos são limitados, sem opções detalhadas e/ou avançadas; não há integração ou suporte à políticas de segurança de redes e não há padrões para se medir performance da rede monitorada, os dados são simplementes gerados e fica a critério do administrador identificar tais gargalos.

O produto está disponível sob licença comercial e divide-se em 4 tipos: a versão gratuita, a versão Professional que custa US$995 e suporta até 50 nodos, a versão Premium que custa US$2.495,00 e suporta até 250 nodos e a versão Enterprise, que custa US$ 9.995,00 e não tem limite de nodos suportados. As versões pagas englobam todas opções de suporte e diferem apenas em algumas características do produto. Para uma comparação entre os 4 tipos, acesse http://manageengine.adventnet.com/products/opmanager/comparison.html.

A documentação é vasta e atual e o suporte oferecido é completo, desde a avaliação inicial do ambiente, instalação e configuração propriamente dita e pós-instalação. A tabela abaixo ilutra os requerimentos de hardware para instalá-lo:

Tabela 3.8: Requisitos de hardware para o OpManager

# of devices	Processor	RAM	Hard Disk	Supported Operating Systems
Up to 50	1.7 GHz	1GB	20 GB	Windows: 2003 Server, 2000 professional +SP4, XP Professional
50-150	2.4 GHz	2GB		
150-300	3.4 GHz	2GB		
300-500	2*3.4GHz	4GB		
501 and above	4*3.4GHz	4GB		Linux: RedHat 7.x and above, Debian 3.0

3.5 BigBrother4

O BigBrother 4 da Quest Software é um produto comercial de monitoramento e gerenciamento de redes baseado em um GUI Web que utiliza-se de uma arquitetura cliente-servidor para receber e enviar dados na rede monitorada, sem agentes remotos para testes de rede (performance, segurança, capacidade, gargalos, etc) e monitoramento simples de clientes ou com agentes remotos para detalhamento completos dos dispositivos monitorados, possuindo ampla flexibilidade de funcionamento, podendo, inclusive, utilizar os dois tipos de configuração ao mesmo tempo.

O produto possui as seguintes características:

- Redundância: suporte à redundância que permite diversas instâncias do produto rodando em paralelo, para evitar falhas que possam afetar o ambiente produtivo, podendo os clientes monitorados reportar para diversos servidores ou diversos monitores Web que estejam rodando;
- Interface: interface gráfica que mostra, em tempo real, o status do sistema via Web ou via WML (Unix/Linux somente) para dispositivos *wireless* que rodam sob WAP. Uma disposição de cores intuitiva representa os diversos dispositivos e servidores monitorados, ilustrando quais estão gerando alertas, quais estão OK, etc.;
- Testes de Rede: o DVD de instalação possuem, ainda durante o boot, opções para testar conexões FTP, HTTP, SMTP, POP3, DNS, Telnet, IMAP, NNTP, SSH, entre outros (similar às distribuições Linux que possuem opções de teste de memória). Essas opções de teste também estão presentes durante o setup de instalação da ferramenta, quando feito via download do site;
- Testes Locais: quando instalado em um única máquina, o BigBrother 4 monitora o espaço em disco, utilização da CPU, memória, processos rodando, entre outros;
- Notificações e Alertas: um sistema sofisticado baseado em horários pré-definidos, dispositivos monitorados, erros, gargalos ou alertas, entre outras

definições, gera notificações em tempo real para o administrador nas mais diversas formas: e-mail, SMS, ligações para celular, pager; opções avançadas como grupamento de dispositivos, pré-classificação e análise lógica de erros (para evitar envio de alerta incorreto quando o erro é corrigido automaticamente) e escalonamento de problema são suportados. Há, ainda, um sistema de criação de notificações completo, incluindo suporte à scripts externos, permitindo ampla flexibilidade de criação;

- Reports de disponibilidade: permite criação e manutenção de reports com históricos sobre as mudanças de estado dos cliente monitorados, bem como gerar e armazenar reportes de SLA e disponibilidade em geral;
- Plug-Ins e Extensões: Big Brother 4 foi criado e desenvolvido focando extensibilidade e disponibilidade desde seu início, resultando em suporte à plug-ins escrito em qualquer linguagem disponível para esse fim. Mais de 1000 plug-ins estão disponíveis para incrementar o produto e podem ser encontradas em www.bb4.com/community.
- Arquitetura: do tipo cliente-servidor, utilizada em conjunto com mecanismos internos do sistema para enviar e receber dados na rede, provêm um baixo *overhead* e alta flexibilidade

O produto é composto pelos componentes abaixo:

- BBDISPLAY: é o serviço que mostra as informações em janelas *web* rodando sobre um serviço HTTP. Suporta os servidores mais comuns como Apache e IIS;
- BBPAGER: é o serviço que processa os alertas e envia-os para os destinatários corretos para tomar as ações seguintes. Esses alertas são enviados por esse serviço via e-mail, SMS, *SNMP-traps* ou mensagens de formato genérico do tipo alfa-numérico;
- BBNET: é o serviço que faz todos os testes de rede do produto, testando os protocolos citados anteriormente;
- LSM: sigla para *Local System Monitors* (também chamados de *bbclients*), que coletam as informações locais e remotas e enviam para o BBDISPLAY e/ou BBPAGER.

O BigBrother 4 utiliza-se do protocolo TCP para todas suas comunicações. O servidor aceita novas conexões, aceita-as se válidas, rejeita se inválidas, não se identifica na conexão ou então envia um ACK aleatório para desencorajar possíveis hackers. Uma vez estabelecida a conexão, os clientes enviam suas informações locais para o(s) servidor(es) BBDISPLAY e BBPAGER a cada 5 minutos (configurável) – é neste ponto que a redundância entra em cena ao permitir aos clientes BB enviar mensagens com seu status atual para vários BBDISPLAYs e BBPAGERs configuradas para *failover*. O BBDISPLAY, então, formata todas mensagens recebidas e as compacta de tal forma que pode-se visualizar um país inteiro na janela Web sem perder nenhum detalhe dos dispositivos monitorados.

O serviço BBNET testa todos serviços definidos e configurados a cada 5 minutos também (configurável) e envia os resultados para os servidores BB. Por padrão, o serviço BBNET vem configurado para rodar na mesma máquina que o BBDISPLAY.

A Quest Software recomenda um máximo de 500 clientes reportando para cada servidor BB, entretanto não há limite de dispositivos a serem monitorados, desde que haja servidores o suficiente para lidar com o tráfego gerado. O BB utiliza-se de um arquivo próprio de hosts chamado *bb-hosts* para armazenar as configurações dos dispositivos da rede e pode-se monitorar redes segmentadas, sub-redes e redes atrás de firewalls remotos utilizando-se do serviço BBRELAY, que também permite enviar mensagens do entre BBDISPLAYs pertencente à estas redes externas. Adicionalmente, o BB suporta criptografia ponto-a-ponto através de chaves compartilhadas, se necessário.

A figura abaixo ilustra o funcionamento destes serviços:

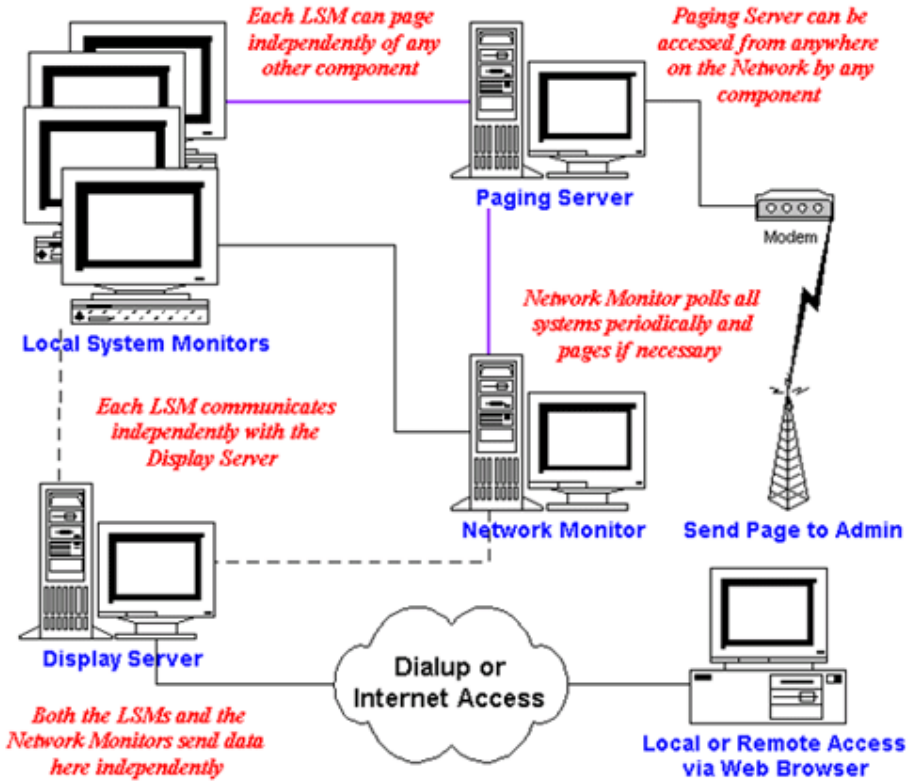

Figura 3.2: Ilustração dos serviços do BB4

É possível fazer download do produto e testá-lo gratuitamente por 30 dias, com todas as funcionalidades disponíveis. Após esse período, deve ser adquirida a licença. O BigBrother 4 é suportado por uma grande gama de sistemas operacionais, ilustrado na tabela abaixo:

Tabela 3.9: Sistemas Operacionais suportados pelo BB4

Big Brother for Windows 2000/2003/XP
Windows 2008/2000/2003/XP

Big Brother for UNIX/Linux
HP-UX 11.0
HP-UX 11i
HP-UX 11i Itanium 64-Bit (Client Only)
IBM AIX 5.2 (Client Only)
IBM AIX 5.3 (Client Only)
IBM AIX 6.1 (Client Only)
Red Hat Enterprise Server 3.0
Red Hat Enterprise Server 4.0
Red Hat Enterprise Server 5.0
Sun Solaris 5.8
Sun Solaris 5.9
Sun Solaris 10
Sun Solaris 5.8 i386 (x86)
Sun Solaris 5.9 i386 (x86)
Sun Solaris 10 i386 (x86)
SUSE Linux 9
SUSE Linux 10

Big Brother for MAC OSX 10
Darwin 9.5 (Client Only)

3.6 Spiceworks

O Spiceworks é um software de gerenciamento de redes totalmente gratuito e com muitos recursos e pode ser melhor definido como sendo uma ferramenta 3 em 1: um sistema de inventário online, um portal de help desk e uma solução de monitoramento de redes computacionais.

Originalmente lançado em Julho de 2006, o Spiceworks vem crescendo a passos largos em termos de funcionalidades bem como foco no cliente. Utilizando um sistema baseado em propagandas embutidas na interface *web* (similar ao Google Ads) para gerar receita e rodando sobre o banco de dados SQLite, a companhia – e consequentemente o produto - já nasceram adaptados às novas tendências de renda via *web*. Todavia, se o cliente não deseja visualizar o tempo todo esses *Ads* (propagandas), pode-se pagar mensalmente a quantia de US$10 para eliminá-los e deixar o GUI mais “limpo”.

O produto possuem as seguintes características:

- Sistema de Help-Desk embutido;
- Possibilidade de rodar e editar os próprios reports em uma imensa gama de dados catalogados;
- Monitoramento remoto de dispositivos através de ferramentas comuns como *ping*, *traceroute* e *remote control*;

- Comparação de configurações (hardware e software) de 2 ou mais estações de trabalho;
- Indexação e um monitor “Event Log” próprio para rastrear dados e estatísticas;
- Fóruns de ajuda (Help Forums) e da comunidade totalmente integrados ao produto;
- Serviço de *automatic discover* de sistemas Windows, Linux, Mac e dispositivos baseados em SNMP;
- Inventário de software incluindo catálogo de *license keys* de diversas aplicações populares;
- Possibilidade de se anexar documentação extra, bem como notas e anotações customizadas em qualquer dispositivo catalogado;
- Foco em usabilidade: possibilidade de determinar / identificar a rede toda, contendo todo hardware e seu software relacionado;
- Monitoramento de servidores Microsoft Exchange e serviços baseado em LDAP;
- Organização de dispositivos por grupos para fins de facilidade de administração;
- Navegação eficiente e voltada à usabilidade;
- Compartilhar praticamente toda configuração e reports do sistema com outros usuários na comunidade Spiceworks;

O software possui um GUI extremamente amigável e ágil, com um menu interativo à esquerda onde é possível navegar entre as mais diversas opções do software rapidamente. Com ilustrações limpas e bem acabadas, o software prima pela beleza visual, mas não sem antes corresponder, também, ao que se espera dele. A opção de inventário é extremamente bem elaborada e os produtos testados foram classificados corretamente. Há opções, inclusive, para se adicionar outros bens que não são nem relacionados à TI, como móveis, estantes e afins. O sistema de monitoramento de dispositivos é ligado ao inventário e, ao clicar sobre algum dispositivo catalogado, imediatamente teremos uma leitura do seu status e situação atual.

Os requerimentos para instalar o software são os seguintes:

- **Sistemas Operacionais**: Windows XP SP2 ou superior; Windows Vista (todas versões); Windows 2003 Server SP1, SP2 e R2 e Windows 2008;
- **Hardware:** Pentium III 1Ghz ou superior; 1Gb RAM ou superior;
- **Sistemas que serão detectados através de scan de rede**: Windows 2000 Professional e/ou superior; Macintosh OS X (SSH tem que estar habilitado) e Linux/Unix (kernel 2.4 e/ou superior – SSH tem que estar habilitado);
- **Antivirus que serão detectados através de scan de rede**: Panda (todas versões), Trend Micro PC-Cillin (todas versões); Norton Internet Security 2006 e/ou superior; Avast (todas versões); Kaspersky (todas versões); eTrust

EZ Antivirus; CA Internet Security Suite; F-Secure Anti-Virus 2006 e/ou superior;

- **Sistemas de e-mail**: Microsoft Exchange 2003 ou 2007; suporte à alertas para qualquer sistema de e-mail POP ou IMAP e SMTP;
- **Controle remoto**: suporte à VNC e RDP;
- **Requisitos de browser**: Firefox 1.5 e/ou superior; Internet Explorer 6 e/ou superior.

O Spiceworks utiliza-se do protocolo SNMP para fazer o rastreamento remoto dos dispositivos de rede, de respostas na porta Jet Direct para impressoras, respostas em SIP para dispositivos VoIP, WMI ou SSH para notebooks e estações de trabalho e WMI, SSH ou HTTP para servidores Windows/Linux/Unix. Há, também, uma seção de dispositivos desconhecidos encontrados, que pode ser manualmente editada, além de vasta documentação online para auxiliar a identificar tais dispositivos.

Para fazer rastreamento de software, o Spiceworks usa o Windows Management Instrumentation (WMI), provendo a localização do software (onde está instalado), sua versão e quando foi instalado no dispositivo. Destaca-se a identificação de *serial keys* em produtos Microsoft, que são coletadas e visualizadas com o **Produkey** ou **MSKeyViewer Plus,** ambos podem ser encontrados na internet.

O produto utiliza a chave de registro *HKLM/Software/MicrosoftCurrentVersion/Uninstall* e, também, a chave de registro MS *HKLM/Software/Wow6432Node/MicrosoftCurrentVersion/Uninstall* para ter acesso à estes dados.

O produto tem uma comunidade ativa que produz diversos plugins para incrementar suas funcionalidades, bem como uma área especifica para criá-los e gerenciá-los, em *Settings→ Plugins*. Ainda dentro de *Settings*, há um grande número de opções que podem ser configuradas, indo desde a linguagem do produto até configurações do UUID do produto.

No que diz respeito à parte de Help-Desk, ele possui uma aba exclusiva para essa funcionalidade, permitindo completa configuração de chamados, customização das telas às quais os usuários terão acesso, listagem dos produtos cadastrados no inventário, tipos de alertas, templates para serem usados nos e-mails, tipo de relatórios, classificação dos *tickets*, entre outras muitas opções.

3.7 Zabbix

Zabbix é um produto de gerenciamento de redes de todos os portes, novo no mercado e distribuído sob a licença GPL. Possui uma grande variedade de opções e tem sido comumente considerado superior aos demais produtos GPL disponíveis justamente

por cobrir lacunas deixadas em branco por seus concorrentes, o que forçava muitos administradores a usarem 2 (ou até mais) produtos ao mesmo tempo.

Zabbix é um software que utiliza o tipo servidor-agente de funcionamento, permitindo mais de um servidor rodando ao mesmo tempo – redundante, por tanto – recolhendo os dados gerados por seus agentes rodando nos mais diversos clientes. A arquitetura do Zabbix é distribuída e isso implica que não é possível ter um gerente central para gerenciar todas informações e dados dos demais gerentes e clientes. Estes dados são armazenados em bancos de dados relacionais – MySQL, PostgreSQL ou Oracle – e o software pode rodar em todas distribuições Linux/Unix. Seus agentes estão disponíveis para sistemas operacionais Linux, Unix (AIX, HP-UX), MacOS X, Solaris, FreeBSD, Netware, Windows e dispositivos rodando SNMP v1, v2 e v3.

O produto é relativamente fácil de se instalar e configurar, necessitando fazer o download do código fonte ou de um pacote pronto para algumas distribuições de Linux (Debian, Ubuntu, Fedora ou Gentoo) e FreeBSD. As tabelas abaixo ilutram os pré-requisitos para instalar o produto.

Tabela 3.10: Requisitos de hardware aproximados para o Zabbix

Tipo de rede	**Plataforma**	**CPU/Memória**	**Banco de Dados**	**Hosts monitorados**
Pequeno	Ubuntu Linux 32-bit	Intel PentiumII 350Mhz / 256Mb	MySQL MyISAM	20
Médio	Ubuntu Linux 64-bit	AMD Athlon64 3200+ / 2Gb	MySQL InnoDB	500
Grande	Ubuntu Linux 64-bit	Intel Dual Core 6400 / 4Gb	MySQL InnoDB, Oracle ou PostgreSQL	>1000
Muito Grande	RedHat Enterprise	2x Intel Xeon 2Ghz / 8Gb	MySQL InnoDB, Oracle ou PostgreSQL	>10000

Fonte: Zabbix web site: <http://www.zabbix.com/>, acessado em 09.11.2008

A tabela acima serve apenas como referencial, uma vez que não há uma combinação definitiva, cada instalação deve levar em conta os seguintes fatores:

- Capacidade do hardware utilizado;
- Se o banco de dados é gratuito ou comercial;
- Qual a carga de utilização do servidor ou proxy Zabbix.

O MySQL InnoDB é recomendado para grandes cargas de nodos monitorados, para um servidor único de banco de dados com performance alta/média e para um proxy de grande volume de dados; o MySQL MyISAM é recomendado para pequenas/médias cargas de nodos monitorados, para um servidor único de banco de dados com performance média/baixa e para um proxy de volume médio/baixo de dados; o Oracle é

recomendado para grandes cargas de nodos monitorados e cluster de servidores de banco de dados; o PostgreSQL é recomendado para grandes carga de nodos monitorados, para um servidor único de banco de dados com performance alta/média e para um proxy de grande volume de dados e o SQLite é recomendado para proxy de baixa/média carga de dados.

Tabela 3.11: Requisitos de software para utilização do Zabbix

Software	Versão	Comentários
Apache	1.3.12 ou superior	
PHP	4.3 ou superior	
Módulos PHP: php-gd e pgp-bcmatch	4.3 ou superior	Os módulos PHP GD devem suportar imagens do tipo PNG
MySQL: php-mysql	3.22 ou superior	Necessário se MySQL é utilizado como banco de dados do Zabbix
Oracle: php-sqlora8	9.2.0.4 ou superior	Necessários se Oracle é utilizado como banco de dados do Zabbix
PostgreSQL: php-pgsql	7.0.2 ou superior	Necessários se PostgreSQL é utilizado como banco de dados do Zabbix
SQLite: php-sqlite3	3.3.5 ou superior	Necessários se SQLite é utilizado como banco de dados do Zabbix

Fonte: Zabbix web site: <http://www.zabbix.com/>, acessado em 09.11.2008

Da mesma forma que o servidor, os agentes vem pré-compilados em pacotes amigáveis, executáveis (família Windows) ou em código-fonte, pronto para ser compilado à gosto do administrador. A distribuição remota dos agentes é elementar e bem documentada no manual do produto.

O Zabbix permite monitoramento em tempo real através de uma interface *web* contralizada onde é possível visualizar todos dispositivos e seus status. Os monitores de performance, segurança, utilização de CPU/HD são de fácil acesso e respondem rapidamente aos comandos. Estes dados geram gráficos atraentes visualmente e atualizados em tempo real, bem como armazenados em um inventário confiável. Outra característica atraente do Zabbix é sua capacidade de gerar mapas da rede a partir de um ponto único central, definido pelo administrador. Utilizando elementos visuais de fácil identificação, em poucos minutos consegue-se ter uma idéia de toda rede gerenciada, e com todos dados acessíveis, bastando mover o mouse sobre um dispositivo ilustrado no mapa. (abre-se uma pequena janela tipo *pop-up* com as informações, que podem ser customizadas à vontade)

As opções de alertas são muitas e pode-se definir limites (*threshold*s) para cada um destes alertas, que são ativados e enviados por diversos meios aos responsáveis pelo sistema (e-mail, SMS, ligação telefônica). Todas estas atividades são logadas pelo sistema, recurso importante caso algum envio de alerta não seja notado pelo administrador.

Quanto aos relatórios, o Zabbix vem com várias opções comuns por padrão, mas facilmente pode-se agregar relatórios diversos através de sua comunidade ativa, bem como customizar conforme a necessidade. Os relatórios são de fácil leitura e podem ser gerados em diversos formatos comumente encontrados, tais como .html, .rtf, .msg, entre outros.

O suporte ao Zabbix divide-se em dois tipos: o gratuito, que está disponível através da página do produto, fórums, canal IRC de suporte e lista de e-mails (*mailing lists*); e o comercial, que, por sua vez, subdivide-se em Bronze, Prata, Ouro e Platina, sendo que eles diferem entre si pelo número de incidentes, tipos de suporte (Web, por telefone ou e-mail) e tempos de respostas oferecidos, além de suporte local em diversas partes do mundo. A tabela abaixo ilustra os tipos de suporte comercial.

Tabela 3.12: Características do suporte comercial Zabbix

	Bronze	**Silver**	**Gold**	**Platinum**
Software				
Software pré-compilado?	Não	Sim	Sim	Sim
Compilações customizadas Zabbix?	Não	Não	Opcional	Opcional
Monitoramento Distribuído				
Servidor Zabbix (nodo)	Não disponível	Não disponível	Sim, com descontos	Sim, gratuito
Suporte				
Número de incidentes reportados	4	8	Sem limites	Sem limites
Suporte Web?	Sim	Sim	Sim	Sim
Suporte por telefone?	Não	8x5	8x5	24x7
Tempo inicial de resposta	2 dias úteis	8 horas	4 horas	4 horas (resposta de emergência: 90 minutos)
Consultoria Remota				
Resolução de problemas remotos?	Não	Não	Sim	Sim
Otimização de performance?	Não	Não	Opcional	Sim
Gerente de Conta				
Gerente técnico de conta?	Não	Não	Opcional	Opcional
Visitas onsites?	Não	Não	Opcional	Opcional
Revisão do	Não	Não	Opcional	Opcional

ambiente?				

Fonte: Zabbix web site: <http://www.zabbix.com/>, acessado em 09.11.2008

3.8 Look@LAN

O software Look@LAN é um *freeware* disponível em www.lookatlan.com, desenvolvido por um único desenvolvedor (Carlo Medas – www.treemenu.net) que tem por características rodar apenas em plataformas Windows, facilidade de instalação e utilização, customização de ferramentas de monitoramento (*ping*, *trace route*, *scan* de portas, geração de gráficos, entre outros) e um *front-end* amigável. É importante realçar que ele não se enquadra em nenhuma dos paradigmas modernos recomendados de gerenciamento de redes, uma vez que não possui clientes remotos, gerentes locais ou bancos de dados distribuído. Antes, classifica-se como tendo uma arquitetura centralizada (segundo Leiwand, 1996), sendo um gerente centralizado que executa todas tarefas de gerenciamento, não tendo a opção de armazenar os resultados em um banco de dados locais (ou seja, exibe os resultados em *real-time* e que guarda-os em arquivos salvos localmente através da opção 'Export' dentro de 'Reports').

Como pontos negativos, podemos citar que ele não tem opções de escolha de protocolos de gerenciamento, sendo limitado ao SNMPv2. Também não possui redundância de informações – no caso de *crash* do programa, todas informações são perdidas. Não possui interface ou protocolo de comunicação com outros sistemas operacionais, em especial a família *NIX, sendo limitado à administração de plataformas Microsoft somente.

É recomendado em casos onde necessita-se de um monitoramento de poucos hosts Windows onde o mais importante é monitorar se o host está *up* (usando-se a ferramenta de *ping* primariamente) em uma rede pequena a média (500 hosts máximo).

O programa utiliza primariamente o protocolo UDP para fazer tais varreduras, o que explica sua ótima performance em *scans* na rede (portas 12035 e 12066). Entretanto, pode ser configurado para usar o protocolo TCP/IP (portas 49592 e 49608). Utiliza NetBIOS em conjunto com SNMP para buscar mais informações dos hosts sendo varridos, mas possuem detecção de sistemas operacionais fraca, não indentificando a versão do Windows e tratando todos "outros" dispositivos como sendo Não-Windows.

4 COMPARAÇÃO DAS FERRAMENTAS

As ferramentas estudadas apresentam muitas semelhanças entre si e, em geral, fornecem soluções para a maioria das necessidades que o gerenciamento de redes exige. Ainda assim, observa-se características únicas entre elas que sobressaem-se na hora da escolha.

Para fins de comparação, as mesmas foram testadas em uma rede real com a seguinte configuração:

- um servidor Windows 2000 Server: servidor de domínio, impressoras e arquivos;
- um firewall Linux entre a internet e a LAN interna;
- um servidor Linux: DHCP, DNS, proxy transparente;
- um servidor Windows com múltiplas máquinas virtuais Linux/Windows rodando; nesta máquina que foram instaladas as ferramentas avaliadas;
- um Access Point (AP) provendo acesso sem-fio para os clientes da rede;
- um AP repetidor sem-fio para estender o sinal para outros prédios;
- 8 workstations Windows XP/Windows 98;
- 6 notebooks Windows Vista/Windows XP;
- 6 impressoras jato de tinta, sendo 2 ligadas em rede e as demais, localmente;
- 1 switch não-gerenciável;
- 2 hubs.

4.1 CACTI

O Cacti se mostrou uma ferramenta muito abrangente, com gráficos esplêndidos e ótima usabilidade, não deixando de funcionar mesmo em condições adversas tais como desligar e religar diversas máquinas da rede, efetuar flood, *broadcasts* e “pings da morte”, executar testes de exaustão no servidor onde ele estava instalado, entre outros. Muitas funcionalidades podem ser adicionais via plugins de terceiros, suprimindo algumas lacunas encontradas na instalação padrão.

Como ponto fraco, observamos um desempenho aquém dos seus concorrentes para levantar, armazenar e exibir os dados e seus respectivos gráficos, ainda que não seja nada de alarmante, mas considerando-se o tamanho da LAN testada (pequena), pode-se levantar suspeitas em ambientes mais complexos.

4.2 Nagios

O Nagios confirmou aquilo que se encontra documentado vastamente na internet: um software abrangente e experiente com algumas particularidades, notadamente no que diz respeito à segurança, com suporte à todas tecnologias padrão de mercado, tais como SSL, kerberos, HTTPS no WebGUI e diversas configurações específicas para seu código, facilmente encontradas na sua documentação. Destaca-se a capacidade de monitoramento de dispositivos, com muitas opções disponíveis não somente na instalação padrão, mas também entre plugins desenvolvidos por sua comunidade.

Os gráficos não são tão exuberantes quanto os do Cacti, todavia toda informação relevante é corretamente reportada e atualizada, dando-se ênfase maior ser em cima do quesito disponibilidade, tendo este produto diversas ferramentas para monitorar os mais variados serviços e plataformas Windows/Linux/Unix. Como ponto fraco, também observou-se uma lentidão um pouco maior do que seus concorrentes para finalizar a varredura e agregar os dados, bem como um excessivo número de *features* disponíveis apenas através de plug-ins externos, aumentando a tarefa do administrador de configurar o ambiente como se desejar.

4.3 ZenOSS

O ZenOSS foi o software que agregou o maior número de virtudes que vem disponíveis na instalação padrão. Trata-se de um produto robusto, moderno e muito bem acabado, que surpreende o usuário nos seus detalhes – facilidade de configuração e usabilidade, bem como gráficos bem-tratados, software atualizado, grande e ativa comunidade *open-source*, além de propaganda bem divulgada – há uma versão (*appliance)* pronta para ser usada com o software VMWare, basta baixar do site e abrí-la com o VMWare Player. O sistema subirá em instantes e o ZenOSS já estará pronto para ser utilizado via navegador. Todo o monitoramento e geração de relatórios é refinado e customizável, com a maior parte das funções disponíveis diretamente via navegador.

Como ponto negativo, pode-se citar o fator segurança, visto que não há uma documentação específica sobre este quesito, além do acesso ser feito via navegador e do ZenOSS não ofereçer a mesma gama de configurações de segurança encontrada nos seus concorrentes. Sua instalação também não é das mais simples, requerendo um

conhecimento mais profundo de sistemas *nix. Todavia, após configurado, o nível de manutenção de sua configuração é mínima.

4.4 OpManager

O OpManager da AdventNet mostrou-se um sistema muito amigável de ser utilizado, principalmente na plataforma Windows, com acesso à menus via botão direito do mouse e configurações simples de serem efetuadas. A instalação é simples e já traz bando de dados embutido (MySQL) ou seleciona-se um existente (MSSQL, MySQL). Os gráficos gerados são de boa qualidade e tem um layout (assim como todo sistema) “Windows-like”, entretanto o OpManager não gera mapas de rede, o que faz falta para se ter uma visualização geral do ambiente. O software disponibiliza 30 dias com todas funcionalidades habilitadas para avaliação, o que se mostra muito útil para esse fim.

O site do produto é bem completo e apresenta, entre outras coisas, estudos de casos completos que podem ser baixados em formato PDF ou visualizados no navegador em HTML.

Como ponto negativo, o produto não possui uma qualidade que se destaque em relação aos demais; antes, todas opções que ele oferece são superadas em um ou outro produto testado e o fato de ser um produto comercial não o ajuda na sua apreciação final.

4.5 BigBrother4

O BigBrother4 é, sem dúvida, a ferramenta mais sofisticada dentre as avaliadas, destacando-se, principalmente, pelo visual atual e deslumbrante e pela sua infra-estrutura de suporte. A documentação é bem elaborada e a comunidade, ativa, colaborando com mais de 1000 plugins que podem ser adicionados ao produto, ainda que o site do mesmo possui um layout bem simples. O controle é completamente feito via navegador e a resposta do servidor foi uma agradável surpresa, superando os demais produtos. Também destacou-se na varredura da rede e dos dispositivos, identificando a maioria deles corretamente, graças ao seu amplo banco de dados, além de produzir gráficos e mapas claros e de fácil leitura.

O fato de ser uma ferramenta apenas para Windows tira um pouco do seu brilho, assim como ser o produto mais caro dentre os testados, além de ter uma aceitação de mercado inferior às demais ferramentas testadas.

4.6 Spiceworks

O Spiceworks é uma ferramenta que, além de prover monitoramento de rede, provê, também, um sistema de gerenciamento de Help-Desk, onde chamados podem ser abertos por usuários cadastrados em cima de produtos catalogados pelo sistema, bem como um inventário que não exige agentes remotos rodando. Com um front-end muito limpo e informativo a ferramenta se destaca mais por essas características gerenciais do que pelas características de monitoramento de rede, onde possui menos recursos que os outros produtos testados. Todavia, mostrou excelente usabilidade para uma rede pequena e, quando utilizado com outros produtos mais voltados ao monitoramento de dispositivos em rede, obtêm-se o máximo que pode-se obter atualmente em termos de gerenciamento de redes.

4.7 Look@LAN

O freeware Look@LAN situa-se em um capítulo a parte pois trata-se de um software mais simples, sem interface com banco de dados para armazenar seus dados e sem opções avançadas de monitoramento. Entretanto, destaca-se pela facilidade e rapidez em ser instalado, utilizado e explorado, podendo facilmente escanear redes e mapear dispositivos e serviços rodando. Todavia, falta muitas propriedades para definí-lo como uma ferramenta de gerenciamento, ficando mais para uma de monitoramento de alguns serviços na rede.

4.8 Zabbix

O Zabbix promete ser a ferramenta mais completa dentre as GPL, pois une todas as opções que as demais debaixo de uma interface robusta e amigável. Gráficos e mapas são facilmente gerados e acessados e os agentes remotos propiciam um levantamento detalhado do ambiente, ainda que não tenham a mesma qualidade visual de outros produtos (tendência essa seguida por todos produtos GPL). A documentação excelente facilita a vida do administrador e o software é constantemente atualizado, com comunidade ativa e participante. Como ponto forte, destaca-se a gama de bancos de dados compatíveis com o mesmo, além de não apresentar um ponto fraco marcante. O termo “promete” foi utilizado porque é um produto recente no mercado, em constante atualização mas que já produz diversos *feedbacks* positivo de sites especializados no assunto.

Por fim, a tabela abaixo traz uma comparação das ferramentas ilustradas:

Tabela 4.1: Comparação das ferramentas utilizada

	Cacti	Nagios	ZenOSS	OpManager	BigBrother4	Spiceworks	Look@LAN	Zabbix
SLA Reports	Não	Através de plugin	Não	Em desenvolvimento	Sim	Sim	Não	Sim
Auto Discovery	Através de plugin	Através de plugin	Sim	Sim	Sim	Sim	Sim	Sim
Agente	Não	Sim	Não	Não	Sim	Sim	Não	Sim
SNMP	Sim	Através de plugin	Sim	Sim	Sim	Sim	Sim	Sim
Syslog	Não	Através de plugin	Sim	Sim	Sim	Sim	Não	Sim
Permite Scripts Externos	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim
Plugins	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Linguagem que foi escrito	PHP	Perl	Python e Zope	Perl e Python	C	Ruby	C	C e PHP
Gatilhos / Alertas	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Front-end Web	Controle Completo	Controle Parcial	Controle Completo	Controle Completo	Controle Completo	Controle Completo	Não	Controle Completo
Monitoramento Distribuído	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Inventário	Através de plugin	Através de plugin	Sim	Sim	Sim	Sim	Não	Sim
Método de Armazenamento de Dados	RRDTool, MySQL. PostgreSQL em desenvolvimento	MySQL, MSSQL.	RRDTool para dados de performance. MySQL para eventos.	MySQL e MSSQL	Oracle, MSSQL, MySQL	MySQL e SQLite	Não	Oracle, MySQL, PostgreSQL e SQLite
Licenciamento	GPL	GPL	Core: GPLPro: ComercialEnterprise: comercial	Comercial. 30 dias para testar o produto.	Comercial	GPL	Freeware	GPL
Geração Gráficos / Mapas	Sim / Através de plugin	Sim / Sim	Sim / Sim	Sim / Não	Sim / Sim	Sim / Parcial	Sim / Sim	Sim / Sim
Eventos	Através de plugin	Sim	Sim	Não	Sim	Sim	Não	Sim

5 CONCLUSÃO

Este trabalho teve como principal objetivo comparar soluções de mercado para gerenciamento de redes. Com esse objetivo, o trabalho iniciou-se com um levantamento sobre o gerenciamento de redes moderno e suas características, bem como um breve histórico do mesmo, passando então para a análise das nove ferramentas propostas. Com o advento do protocolo SNMP e suas versões posteriores, assim como linguages web e facilidade em geral de se obter e configurar essas ferramentas, o rastreamento dos diversos dispositivos conectados em LANs e WANs é hoje possível e fácil de ser alcançado.

Dentro dessa realidade, diversas ferramentas destacam-se no mercado, cada uma com suas características únicas, porém todas buscando maximizar o uso da tecnologia atual. Após esta análise, verifica-se que não há um produto apenas que disponibiliza, de forma satisfatória, todos os recursos existentes no âmbito do gerenciamento de redes; para pesquisadores, a melhor combinação é unir duas ou mais ferramentas para, então, atingir a totalidade do conceito de gerenciamento de redes.

Ainda, deve-se levar em conta a questão do licenciamento do software, se ele é comercial ou não. Os produtos comerciais possuem um apelo maior no que diz respeito ao suporte e ao conceito em geral de que há uma empresa que se responsabiliza pelo produto, suas possíveis falhas e futuras melhorias; os software GPL, por sua vez, possuem uma comunidade maior e mais ativa e destacam, principalmente, sua flexibilidade e expansibilidade através de plugins.

Finalizando, a tabela 10, exibida no capítulo anterior, comparativa entre os produtos, tenta auxiliar na questão sobre qual é o melhor produto para necessidades especiais de empresas, pesquisadores e entusiastas desta área.

REFERÊNCIAS

ADVENTNET Inc. **OpManager Website**. Disponível em: <http://manageengine.adventnet.com/products/opmanager/>. Acesso em: ago. 2008.

AVALLE, R. P. **Gerenciamento de Redes**. Disponível em: <http://www.gta.ufrj.br/grad/99_1/rodrigo/ger_redes.htm>. Acesso em: set. 2008.

BATTISTI, G. **Modelo de Gerenciamento para Infra-Estruturas de Medições de Desempenho em Redes de Computadores.** 2007. 120 f. Dissertação (Doutorado em Ciência da Computação) – Instituto de Informática, UFRGS, Porto Alegre.

BEETHOVEM, Z. D.; ALVEZ JUNIOR, N. **Protocolo de Gerenciamento SNMP.** Disponível em: <http://mesonpi.cat.cbpf.br/naj/snmp_color.pdf>. Acesso em: out. 2008.

CACTIUSERS.ORG. **CACTI Users**. Disponível em: <http://www.cactiusers.org/>. Acesso em: nov. 2008.

CARVALHO, T. C. M. **Gerenciamento de redes**: uma abordagem de sistemas. São Paulo: Makron Books,1993. p. 364.

CASTRO, A. A. **Internet:** Conceito: Histórico: Funcionamento. Disponível em: <http://www.aldemario.adv.br/infojur/conteudo4texto.htm>. Acesso em: ago. 2008.

CENTRO BRASILEIRO DE PESQUISAS FÍSICAS. **SNMP (Simple Network Management Protocol)**. Disponível em: <http://www.cbpf.br/~sun/pdf/snmp.pdf>. Acesso em: out. 2008.

COELHO, G.F. de; ALMEIDA, M.B.; TAROUCO, L.R.; GRANVILLE, L.Z. Network Executive: Implementação de uma Arquitetura para Substituição Automática de Políticas em Sistemas PBNM. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES, 22., 2004. **Anais...** Gramado: TI/UFRGS, 2004. p.263-276.

COELHO, J. **Gerenciamento Distribuído**. Disponível em: <http://penta3.ufrgs.br/twiki/bin/view/Main/GerenciamentoDistribuido>. Acesso em: nov. 2008.

DE MELLO, J. L. **Protótipo de um Agente SNMP para uma Rede Local utilizando a plataforma JDMK.** Disponível em: <http://www.inf.furb.br/~pericas/orientacoes/JDMK2000.pdf>. Acesso em: nov. 2008.

FIOREZE, T.; GRANVILLE, L.Z.; ALMEIDA, M.J.; TAROUCO, L.R. Comparing *web* services with SNMP in a management by delegating environment. In: IFIP/IEEE INTERNATIONAL SYMPOSIUM, 2005, France. **Integrated Network Management IX.** Piscataway: IEEE, 2005. p.600-614.

FITZPATRICK, J. **Look@Lan Monitors Your Network**. Disponível em: <http://lifehacker.com/400291/looklan-monitors-your-network>. Acesso em: ago. 2008.

GEOTEK DATENTECHNIK. **Popular Network Managements Software in Comparision**. Disponível em: <http://ipinfo.info/html/network_management_software.php>. Acesso em: nov. 2008.

KWECKO, M. **Gerência de Rede Distribuída**. Disponível em: <http://www.pead.faced.ufrgs.br/twiki/bin/view/Main/Distribu%EDdas>. Acesso em: nov. 2008.

LEITE, S. L. **Integrando Ferramentas de Software Livre para Gerenciamento e Monitoração de Redes Locais.** 2004. 109f. Dissertação (Mestrado em Ciência da Computação) – Instituto de Informática, UFRGS, Porto Alegre.

LEIWAND, A.; CONROY, K.F. **Network Management:** a pratical perspective. 2nd ed. Massachusetts: Addison-Wesley, 1996.

LINUX HOME NETWORKING. **Quick HOWTO:** chapter 23: Advanced MRTG for Linux. Disponível em: <http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch23_:_Advanced_MRTG_for_Linux#Table_23-1_Important_Objects_In_The_UCD-SNMP-MIB_MIB>. Acesso em: out. 2008.

MALIMA CONSULTORIA. **SNMP – Protocolo de Gerenciamento Simples de Rede**. Disponível em: <http://www.malima.com.br/article_read.asp?id=50>. Acesso em: out. 2008.

MARTIN-FLATIN, J.P.; ZNATY, S.; HUBAUX, J.P. A Survey of Distributed Enterprise Network and System Management Paradigms. **Journal of Network and Systems Management,** New York, v.7, n.1, p.9-26, Mar. 1999.

MEDAS, C. **Look@LAN Website**. Disponível em: <http://www.lookatlan.com/>. Acesso em: ago. 2008.

MULTIREDE Ltda. **Arquitetura de Gerenciamento de Dispositivos de Rede**. Disponível em: <http://www.multirede.com.br/pagina.php?codigo=10>. Acesso em: set. 2008.

MURATI, J. **Nagios vs CACTI vs ZenOSS The most difficult comparision**. Disponível em: <http://www.linkedin.com/answers/technology/information-technology/computers-software/TCH_ITS_CMP/238671-17575109?browseCategory=TCH_ITS_CMP&goback=.nrp_1_1210986746585>. Acesso em: ago. 2008.

NASCIMENTO, J. Q. **Uma História das Comunicações**. Disponível em: <http://www.teleco.com.br/emdebate/quadros02.asp>. Acesso em: out. 2008.

PEREIRA, J. T. **Modelo de Gerenciamento baseado em Ferramentas de Baixo Custo para Redes de Pequeno Porte**. 2002. Dissertação (Ciência da Computação) – PPGCC, Universidade Federal de Santa Catarina, Florianópolis.

PERES, A. **Análise de Tolerância a Falhas no Protocolo SNMP.** Disponível em: <http://www.inf.ufrgs.br/gpesquisa/tf/estudantes/trabalhos/peres.html>. Acesso em: nov. 2008.

PINHEIRO, J. M. S. **Conceitos Básicos de Gerenciamento de Redes**. Disponível em <http://www.projetoderedes.com.br/tutoriais/tutorial_conceitos_gerenciamento_01.php >. Acesso em: out. 2008.

PINHEIRO, J. M. S. **Criação de Subredes**. Disponível em: <http://www.projetoderedes.com.br/tutoriais/tutorial_subredes_01.php>. Acesso em: out. 2008.

PINHEIRO, J. M. S. **Equipamentos para Redes**. Disponível em: <http://www.projetoderedes.com.br/tutoriais/tutorial_equipamentos_de_redes_01.php>. Acesso em: out. 2008.

QUEST SOFTWARE Inc. **BigBrother4 Website**. Disponível em: <http://www.bb4.com/>. Acesso em: set. 2008.

REDE NACIONAL DE ENSINO E PESQUISA (RNP). **Introdução a Gerenciamento de Redes TCP/IP.** Disponível em: <http://www.rnp.br/newsgen/9708/n3-2.html>. Acesso em: out. 2008.

ROSA, D. M da. **Suporte a Cooperação em Sistemas de Gerenciamento de Rede Utilizando Tecnologias Peer-to-Peer.** 2007. 73 f. Dissertação (Mestrado em Ciência da Computação) – Instituto de Informática, UFRGS, Porto Alegre.

SCHÖNWÄLDER, J.; QUITTEK, J.; KAPPLER, C. Building Distributed Management Applications with the IET Script MIB. **IEEE Journal on Selected Areas in Communications,** New York, v.18, n.5, p.702-714, May 2000.

SPICEWORKS Inc. **Spiceworks Website** Disponível em: <http://www.spiceworks.com/>. Acesso em: set. 2008.

STALLINGS, W. **Data and Computer Communications**. New York: Pearson Education, 2004.

STALLINGS, W. **SNMP, SNMPv2, SNMPv3 and RMON 1 and 2:** the practical guide to network management standards. 3rd ed. Reding: Addison-Wesley, 1999.

SZTAJNBERG, A. **Conceitos Básicos sobre os Protocolos SNMP e CMIP.** Disponível em: <http://www.gta.ufrj.br/~alexszt/ger/snmpcmip.html>. Acesso em: set. 2008.

TEIXEIRA JÚNIOR, J.H. et al. **Redes de Computadores.** São Paulo: Makron, 1999.

TELECO CONHECIMENTO EM TELECOMUNICAÇÕES. **Tutorial Banda larga**. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialsnmp/pagina_2.asp>. Acesso em: out. 2008.

THE CACTI GROUP. **CACTI, the complete rrdtool-based graphing solution.** Disponível em: <www.cacti.net>. Acesso em: ago. 2008.

THE INTERNET ENGINEERING TASK FORCE. **A Simple Network Management Protocol (SNMP)**. Disponível em: <http://www.ietf.org/rfc/rfc1157.txt>. Acesso em: nov. 2008.

VIEIRA, A. T. **Gerência de Rede Distribuída**. Disponível em: <http://penta3.ufrgs.br/twiki/bin/view/Main/GerenciaRedeGroup>. Acesso em: nov. 2008.

ZABBIX SIA. **Zabbix Website**. Disponível em: <http://www.zabbix.com>. Acesso em: set. 2008.

ZENOSS Inc. **ZenOSS Website**. Disponível em: <http://www.zenoss.com>. Acesso em: set. 2008.