



UNIVERSIDADE
ESTADUAL DE LONDRINA

ROGÉRIO FURLANETTI ALVES

GERÊNCIA DE REDES UTILIZANDO SOFTWARE LIVRE

LONDRINA - PARANÁ
2007



UNIVERSIDADE
ESTADUAL DE LONDRINA

ROGÉRIO FURLANETTI ALVES

GERÊNCIA DE REDES UTILIZANDO SOFTWARE LIVRE

Monografia apresentada ao Curso de Especialização em Redes de Computadores e Comunicação de Dados, Departamento de Computação da Universidade Estadual de Londrina, como requisito parcial para a obtenção do título de Especialista, sob orientação do Prof. Dr. Mario Lemes Proença Jr.

LONDRINA - PARANÁ
2007

Furlanetti Alves, Rogério

Gerência de redes utilizando software livre / Furlanetti Alves, Rogério. -- Londrina: UEL / Universidade Estadual de Londrina, 2007.

Orientador: Prof. Dr. Mario Lemes Proença Jr.
Dissertação (Especialização) – UEL / Universidade de Londrina, 2006.

1. Gerência em Redes IP. 2. Protocolos de Gerência. 3. Ferramentas de Gerência. I. Proença. II. Universidade Estadual de Londrina Especialização em Redes de Computadores e Comunicação de Dados, III. Gerência de redes utilizando software livre.

ROGERIO FURLANETTI ALVES

GERÊNCIA DE REDES UTILIZANDO SOFTWARE LIVRE

Esta monografia foi julgada adequada para obtenção do título de Especialista, e aprovada em sua forma final pela Coordenação do Curso de Especialização em Redes de Computadores e Comunicação de Dados, do Departamento de Computação da Universidade Estadual de Londrina.

Banca Examinadora:

Prof. Dr. Mario Lemes Proença Jr - Orientador
Universidade Estadual de Londrina

Prof. Msc Elieser Botelho Manhas Jr.
Universidade Estadual de Londrina

Prof. Msc Fabio Sakuray
Universidade Estadual de Londrina

Londrina, 20 de Agosto de 2007.

DEDICATÓRIA

Para Maria Alice e Ivan, com respeito e gratidão, pela vida e educação.

AGRADECIMENTOS

*A todos meus amigos, pelo incentivo e
motivação para superar os obstáculos.*

RESUMO

O presente trabalho tem como finalidade apresentar Técnicas de Gerência de Redes, utilizando Ferramentas Livres. Serão abordados os assuntos referentes ao uso dessas técnicas, como descrição de protocolos (SNMP e RMON), e ferramentas para implementação dessa Gerência (ferramentas de software livre). No protocolo SNMP, os dados são fornecidos por um ou mais Agentes SNMP aos Gerentes SNMP utilizando protocolo UDP em rede IP. O gerenciamento da rede através do SNMP permite o acompanhamento simples e fácil do estado, em tempo real, da rede, podendo ser utilizado para gerenciar diferentes tipos de sistemas. O RMON é um protocolo que tem basicamente a mesma estrutura do protocolo SNMP, porém, o mesmo foi desenvolvido como solução para gerenciamento de redes locais interconectadas à longa distância. Existem inúmeras ferramentas livres para gerência de redes, dentre as quais o MRTG e o Cacti, que são geradores de gráficos referentes a dados coletados via SNMP, o Sarg, que mesmo sem utilizar os protocolos RMON e SNMP, trabalha analisando logs e gerando relatórios de acesso web, o Nagios monitora a rede gerando eventos de falhas e o OpenNMS gerencia redes de grande porte.

ABSTRACT

This work has as purpose to show Techniques of Network Management, using Free Software. The referring subjects to the use of these will be boarded, as description of protocols (SNMP and RMON), and tools for implementation of this Management (Open Source Tools). In the SNMP protocol, the data are supplied by one or more SNMP Agents to the SNMP Manager using UDP protocol over IP based network. The network management using SNMP allows a simple and easy accompaniment of the state, in real time, of the network, being able to be used to manage different types of systems. RMON is a protocol that basically has the same structure of SNMP protocol, however, it was developed as solution for management of interconnected LANs to long distance. A lot of free tools (open source) for network management exist, amongst which the MRTG and the Cacti, that are graphs generators to the collected data using SNMP protocol, the Sarg, that without using protocols RMON and SNMP, works analyzing logs and generating web access reports, the Nagios network monitor generating events of faults and the OpenNMS manages enterprise networks.

SUMÁRIO

LISTA DE FIGURAS.....	10
LISTA DE TABELAS.....	11
1. INTRODUÇÃO.....	13
2. Gerência em Redes IP.....	14
3. Protocolos de Gerência.....	16
3.1. SNMPv1.....	17
3.2. SNMPv2.....	21
3.3. SNMPv3.....	23
3.4. RMON I.....	27
3.5. RMON II.....	29
4. Ferramentas de Gerência.....	31
4.1. MRTG.....	32
4.2. Cacti.....	35
4.3. Sarg.....	37
4.4. Nagios.....	38
4.5. OpenNMS.....	40
5. Conclusão.....	41
6. Bibliografia.....	42

LISTA DE FIGURAS

Figura 3.1 – Protocolo SNMP	18
Figura 3.2 – Object Identifier (OID) da MIB-II	20
Figura 4.1 – Gráfico de utilização organizado em horas gerado pelo MRTG	33
Figura 4.2 – Gráfico de utilização organizado em dias gerado pelo MRTG.....	33
Figura 4.3 – Gráfico de utilização organizado em semanas gerado pelo MRTG	34
Figura 4.4 – Gráfico de utilização organizado em meses gerado pelo MRTG.....	34
Figura 4.5 – Gráficos organizados em árvore pelo Cacti	35
Figura 4.6 – Gráficos de performance gerados pelo Cacti	36
Figura 4.7 – Gráfico de utilização em bytes por dia e usuário do Sarg	37
Figura 4.8 – Estatísticas por grupos de agentes através do Nagios	38
Figura 4.9 – Informações de estado de serviço através do Nagios	39
Figura 4.10 – Mapa de Rede Gerado pelo OpenNMS	40

LISTA DE TABELAS

Tabela 4.1 - Quadro comparativo entre ferramentas e áreas de Gerência de Redes	30
Tabela 4.2 - Gráfico de utilização em meses gerado pelo MRTG	34

LISTA DE ABREVIATURAS

AES	- <i>Advanced Encryption Standard</i>
ASN.1	- <i>Abstract Syntax Notation.1</i>
DES	- <i>Data Encryption Standard</i>
FCAPS	- <i>Fault, Configuration, Accounting, Performance, Security</i>
HTML	- <i>Hyper Text Markup Language</i>
HTTP	- <i>HyperText Transfer Protocol</i>
IANA	- <i>Internet Assigned Numbers Authority</i>
IETF	- <i>Internet Engineering Task Force</i>
IP	- <i>Internet Protocol</i>
IPV6	- <i>Internet Protocol Version 6</i>
IPX	- <i>Internetwork Packet Exchange</i>
LAN	- <i>Local Area Network</i>
MIB	- <i>Management Information Base</i>
MPLS	- <i>Multi Protocol Label Switching</i>
MRTG	- <i>Multi Router Traffic Grapher</i>
NETBEUI	- <i>NetBIOS Extended User Interface</i>
NETBIOS	- <i>Network Basic Input Output System</i>
MD5	- <i>Message-Digest algorithm 5</i>
OID	- <i>Object Identifier</i>
OSI	- <i>Open Systems Interconnection</i>
PDU	- <i>Protocol Data Unit</i>
PNG	- <i>Portable Network Graphics</i>
RFC	- <i>Request for Comments</i>
RMON	- <i>Remote Monitoring</i>
SARG	- <i>Squid Analysis Report Generator</i>
SHA	- <i>Secure Hash Algorithm</i>
SNMP	- <i>Simple Network Management Protocol</i>
SMI	- <i>Structure of Management Information</i>
SMON	- <i>Switched Monitoring</i>
TCP	- <i>Transmission Control Protocol</i>
UDP	- <i>User Datagram Protocol</i>
VACM	- <i>View-based Access Control Model</i>

1. INTRODUÇÃO

Com o surgimento da comunicação de dados através de redes de computadores o cenário das telecomunicações obteve um grande avanço, a possibilidade de transmissão de dados foi o início de uma estrutura que define as atuais grandes possibilidades de interconexões.

As redes de computadores tanto evoluíram que a demanda de cuidados adicionais surgiu. O gerenciamento de redes se fez necessário para garantir maior disponibilidade e melhor utilização dos recursos, através de metodologias e técnicas discutidas ao longo deste trabalho.

A utilização de ferramentas específicas para gerência de redes é um recurso indispensável na vida de um administrador de redes, este trabalho tem como finalidade apresentar e demonstrar a utilização de ferramentas de gerência de redes utilizando software livre.

Este trabalho está dividido da seguinte forma: no Capítulo 2 serão apresentados os conceitos de Gerência em Redes IP, no Capítulo 3, serão apresentados os Protocolos de Gerência. No Capítulo 4 as Ferramentas de Gerência, e finalmente no capítulo 5 serão apresentadas às conclusões deste trabalho e sugestões para trabalhos futuros.

2. Gerência em Redes IP

A Gerência de Redes é o conjunto de atividades voltadas para o planejamento, monitoramento e controle dos serviços prestados pela estrutura de rede e pelas aplicações que dependem dessa estrutura.

A aplicação de técnicas de Gerência de Redes disponibiliza formas de controle envolvidas em suas cinco áreas funcionais: falhas, configuração, contabilização, performance e segurança. A referência para as cinco áreas descritas é conhecida pela sigla FCAPS, esse padrão segue o modelo de referência publicado no *OSI Management Framework*. A documentação de toda a estrutura de rede, envolvendo hardware e software, também é uma virtude necessária para gerenciar os recursos de rede de forma eficiente e segura.

O controle de falhas se consiste em técnicas voltadas à detecção e solução de falhas no ambiente operacional. Através de operações executadas em rede é possível obter a capacidade de detectar, isolar e corrigir falhas nos equipamentos e serviços gerenciados.

Através do controle de configuração, é possível definir e manter padrões de configurações específicos para cada conjunto de equipamentos e serviços. A documentação das configurações é fundamental para manter o controle gerencial dos recursos, disponibilizando assim a flexibilidade de melhor distribuição e remanejamento quando necessário.

Técnicas de contabilização são aplicadas para gerenciar dados coletados na rede, as informações coletadas são processadas e organizadas a fim de prover análise de utilização dos recursos de rede ao gerente. Este tipo de técnica possui a flexibilidade de processar os dados para gerenciar e contabilizar medições de recursos, como tráfego de comunicação, nível de processamento, capacidade de armazenagem, utilização de memória, tempo de conexão, entre outros. A contabilização dos recursos é, gerencialmente, utilizada para analisar e definir parâmetros de capacidade, através da distribuição correta e definição de cotas na utilização.

O gerenciamento de performance, por sua vez, é constituído por técnicas e operações em rede que disponibilizam dados para monitoração e análise das atividades prestadas no ambiente operacional. Controlar e monitorar a performance de uma rede é fundamental para acompanhar o nível de utilização dos recursos, além de acompanhar o crescimento e prevenir sobrecargas (gargalos).

O controle de segurança é o conjunto de técnicas e operações necessárias para garantir estabilidade em definições de acessos, disponibilidade de serviços, armazenamento correto e seguro de dados, entre outros recursos que envolvem a segurança do ambiente. O gerente deve detectar e prevenir ataques externos e internos, acessos não permitidos, erros de integridade e armazenagem de dados, e os demais pontos que necessitam de segurança; utilizando técnicas como análise de históricos, controle de acessos, definições de padrões, cópias de segurança, contingência, redundância, etc.

3. Protocolos de Gerência

O formato de redes IP vem conquistando e integrando cada vez em maior escala, inúmeros tipos de serviços. A partir deste fato, a demanda de cuidados com o funcionamento desta tecnologia aumenta.

O protocolo *Simple Network Management Protocol* (SNMP) foi desenvolvido pela *Internet Engineering Task Force* (IETF) para auxiliar nas técnicas de gerência de rede, os dados trafegam sob protocolo não orientado à conexão (UDP) e a comunicação é composta de duas entidades de troca de informações denominadas Gerente e Agente.

O Agente fornece informações na rede, mantendo dados em uma estrutura denominada *Management Information Base* (MIB). Essas informações são enviadas ou coletadas pelo Gerente.

O Gerente processa essas informações gerando dados aplicáveis a técnicas de Gerência de rede, como por exemplo, contabilização e falhas de recursos de ativos.

O RMON é um protocolo de gerenciamento remoto que oferece uma arquitetura de gerenciamento distribuída, uma vez que o SNMP não é o protocolo ideal para monitoramento de redes corporativas constituídas de diversas redes locais conectadas através de outras à longa distância. Assim, o RMON nada mais é que uma capacidade de gerenciamento remoto, que dá ao gerente a capacidade de gerenciar sub-redes como um todo, e não apenas dispositivos de um mesmo agrupamento.

Ambos os protocolos, possuem uma linha evolutiva de versões que são SNMPv1, SNMPv2 e SNMPv3 para o protocolo SNMP, e RMON I e RMON II para o protocolo RMON.

3.1. SNMPv1

O *Simple Network Management Protocol* (SNMP) é um protocolo de gerência de redes TCP/IP que disponibiliza a capacidade de troca de informação entre dispositivos de rede.

O software segue um modelo convencional, de cliente-servidor. Uma máquina fica com o software “Gerente”, enviando requisições às máquinas com o software “Agente”. As denominações “Gerente” e “Agente” são usadas no lugar de “Servidor” e “Cliente”, para evitar confusões de nomenclatura com outras aplicações de rede. Com a resposta da máquina que está sendo analisada (Agente), os administradores podem monitorar completamente a rede para evitar e resolver eventuais problemas, dentre uma enorme gama de possibilidades.

Uma mensagem SNMP é codificada com um padrão designado ASN.1 (*Abstract Syntax Notation. 1*).

Os comandos transmitidos e recebidos trafegam na rede através de unidades de dados do protocolo (PDU) e são classificados por:

- **GET**, usado para “pegar” alguma informação gerencial específica.
- **GETNEXT**, usado para capturar sequências de informação de gerenciamento.
- **SET**, usado para definir alterações no agente.
- **TRAP**, usado para reportar notificações.

A figura 3.1 demonstra o funcionamento do modelo de gerencia através do protocolo SNMP.

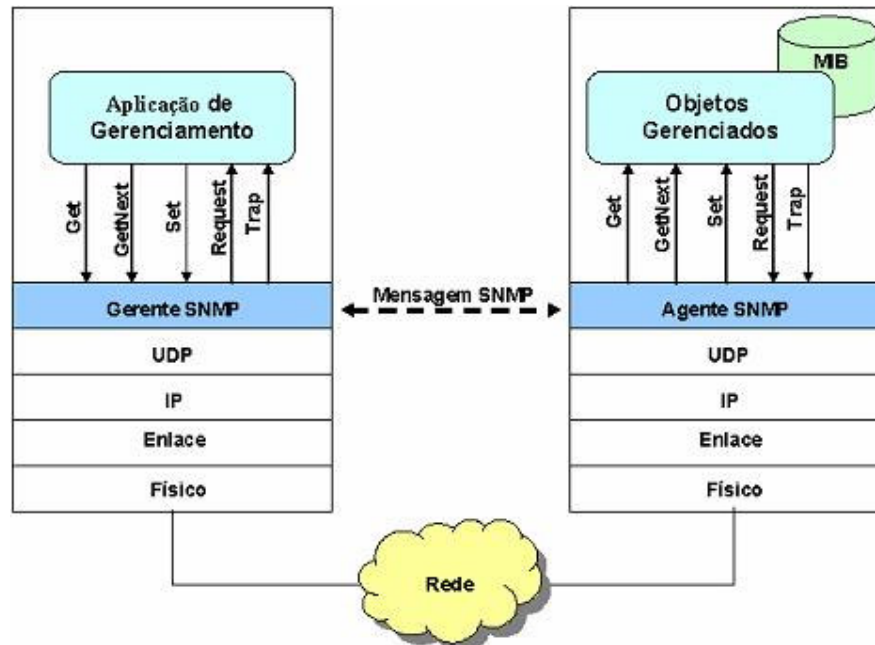


Figura 3.1 – Protocolo SNMP

A primeira versão do protocolo SNMP foi composta baseada nas seguintes descrições:

- RFC 1155 [1]. *Structure and Identification of Management Information for TCP/IP-based internets*

Descreve a identificação da estrutura de gerência de informações utilizada em redes TCP/IP. Definição dos objetos que compõe, basicamente, a *Management Information Base* (MIB).

- RFC 1157 [2]. *A Simple Network Management Protocol (SNMP)*

Neste documento são descritas as funcionalidades do protocolo em si, o *Simple Network Management Protocol* (SNMP) é utilizado para gerenciar nós de rede IP. O protocolo foi desenvolvido seguindo como modelo de referência descrições da RFC 1065,

o qual descreve uma estrutura de gerência de informações denominada *Structure of Management Information* (SMI) e também da RFC 1066, onde é descrito a MIB.

- RFC 1212 [3]. *Concise MIB Definitions*

Onde é definida a forma correta de desenvolvimento de módulos para a MIB, obedecendo as especificações descritas no documento para integrar opções dos objetos da base.

- RFC 1213 [4]. *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*

Definições da estrutura de objetos presentes na MIB-II, uma versão de objetos atualizados em relação aos descritos na RFC 1156 (objetos MIB-I). A estrutura da MIB-II é bastante difundida e está presente na maioria dos ativos que utilizam agentes SNMP.

Para o armazenamento de informações na MIB-II é definida uma estrutura em árvore, compostas por nós, onde cada nó tem um *Object Identifier* (OID) e um nome associado. O OID é uma série de inteiros separados por pontos. Cada nó da árvore pode ter uma nova sub-árvore associada. Partindo da raiz da árvore a MIB-II tem o OID 1.3.6.1.2.1 conforme demonstrado na figura 3.2.

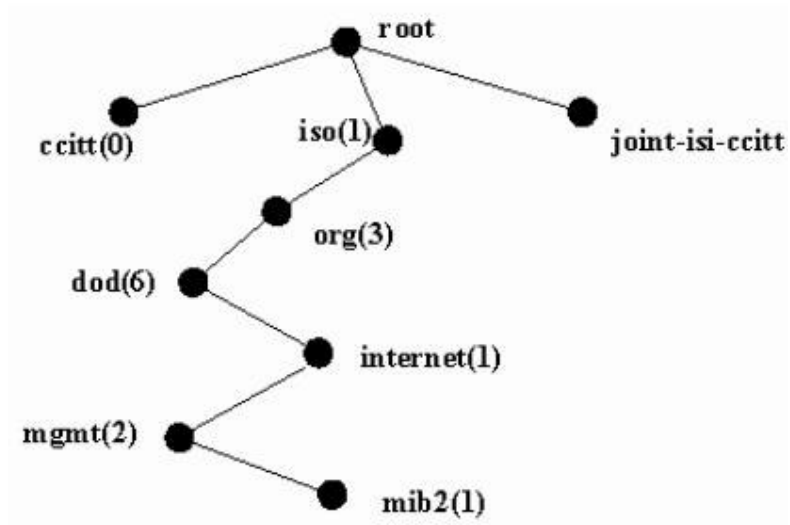


Figura 3.2 – Object Identifier (OID) da MIB-II

3.2. SNMPv2

O SNMPv2 é a segunda versão do protocolo SNMP. Esta versão possui melhoras em relação à primeira versão SNMPv1 incluindo operações adicionais, melhoria de performance, definições de segurança e comunicação entre Gerentes.

A segunda versão do protocolo SNMP foi composta baseada nas seguintes descrições:

- RFC 1901 [5]. *Introduction to Community-based SNMPv2*

Documentação da segunda versão do protocolo SNMP aprimorada a partir do SNMPv1. As operações dessa versão do protocolo envolvem complementos como autenticação, autorização, controle de acesso e política de privacidade.

- RFC 2578 [6]. *Structure of Management Information Version 2 (SMIv2)*

Definições de gerência de informações estruturadas, em segunda versão criada a partir da SMI descrita na RFC 1065. A SMIv2 é dividida em três partes: Definição de módulos, definição de objetos e definição de notificações.

- RFC 2579 [7]. *Textual Conventions for SMIv2*

Descreve a textualidade utilizada para integrar os módulos e objetos na MIB seguindo os parâmetros definidos na SMIv2.

- RFC 2580 [8]. *Conformance Statements for SMIV2*

Documento que define as notações utilizadas para documentação de desenvolvimento baseado na SMIV2.

3.3. SNMPv3

O SNMPv3 se diferencia das outras versões de SNMP no que diz respeito a 3 importantes serviços: autenticação, privacidade e controle de acesso. Para que esses serviços possam ser utilizados pelo SNMPv3 de forma organizada e eficiente, foi criado um novo conceito, o Gerente (Principal). O Gerente fica numa estação com software de gerente, enviando requisições SNMP para as estações com software agente. Essa convergência do Gerente com o software agente permite a criação de políticas de segurança que serão utilizadas, com aspectos como autenticação, privacidade e controle de acesso.

O SNMPv3 é composto por módulos, e cada entidade tem um mecanismo SNMP. Este mecanismo implementa diversas funções, como por exemplo: envio e recebimento de mensagens, controle de acesso a objetos, autenticação e criptografia de mensagens.

Dentre as vantagens incorporadas na terceira versão do SNMP (SNMPv3) pode-se citar melhorias nos aspectos de segurança, o que define diretivas para garantir a integridade e a confiabilidade das mensagens. A encriptação é obtida através do mecanismo de criptografia *Data Encryption Standard* (DES) e a autenticação processada através de algoritmos como o *Message-Digest algorithm 5* (MD5) e o *Secure Hash Algorithm* (SHA).

A terceira versão do protocolo SNMP foi composta baseada nas seguintes descrições:

- RFC 3410 [9]. *Introduction and Applicability Statements for Internet Standard Management Framework*

Introdução à terceira versão do protocolo SNMP. Descreve as diferenças entre as versões (mantendo a idéia de compatibilidade), além de descrição de implementações sob a mesma arquitetura.

- RFC 3411 [10]. *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*

Descrição da arquitetura SNMP, a qual deve ser modular para permitir a evolução dos padrões do protocolo. O documento define também o vocabulário empregado para descrever os componentes da arquitetura. A arquitetura do protocolo é dividida em quatro módulos, que são especificados como: sub-sistema de processamento de mensagens, sub-sistema de segurança e sub-sistema de controle de acesso e despachador de versões.

- RFC 3412 [11]. *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*

O processamento e envio de mensagens SNMP são descritas através de um sistema despachador, que envia e recebe mensagens SNMP com transmissão e recepção através de controle de versão, modelo de segurança e controle de acesso.

- RFC 3413 [12]. *Simple Network Management Protocol (SNMP) Applications*

Descreve 5 tipos de aplicações utilizando o protocolo SNMP, os tipos de aplicações descritas são definidos por: Gerador de Comandos, Responder de Comandos, Originador de Notificações, Receptor de Notificações e Direcionador de *Proxy*.

- RFC 3414 [13]. *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*

Modelo de segurança baseado em usuário, trabalha na arquitetura SNMP através dos módulos de arquitetura descritos na RFC 3411, utiliza os protocolos HMAC-

MD5-96 e HMAC-SHA-96 para autenticação e o protocolo CBC-DES para controle de privacidade. O modelo de segurança baseado em usuário, além de verificar se cada mensagem SNMP não foi modificada ao longo da transmissão, verifica a identidade do gerador da mensagem.

- RFC 3415 [14]. *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*

Modelo de segurança baseado em usuário, trabalha na arquitetura SNMP através dos módulos de arquitetura descritos na RFC 3411.

- RFC 3416 [15]. *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*

Documentação da segunda versão do protocolo, onde define os padrões de transporte das operações e informações gerenciais via SNMP. Os objetos gerenciais são acessados na MIB e definidos através de mecanismos do SMI, utilizando o modelo de comunicação agente/gerente do SNMP.

- RFC 3417 [16]. *Transport Mappings for the Simple Network Management Protocol (SNMP)*

Definição de mapeamento de transporte para o SNMP encapsulado através de vários tipos de protocolos, dentre eles o principal que é o SNMP através de UDP por IPv4, e os opcionais através de OSI ou através de DDP.

- RFC 3418 [17]. *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*

Implementação de um padrão de entidade SNMP para gerenciamento de objetos presentes na MIB, com capacidade de tratamento dos objetos da base gerencial de informações.

- RFC 3584 [18]. *Coexistence between SNMP Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*

Descreve a coexistência entre SNMPv1, SNMPv2 e SNMPv3. Existem quatro aspectos gerais de coexistência entre as versões, divididos em: conversão de documentação MIB entre os formatos SMIV1 e SMIV2, mapeamento de notificação de parâmetros, processamento de operações do protocolo em formato multi-idioma e modelo de segurança baseado em comunidades.

- RFC 3826 [19]. *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*

Descreve um protocolo simétrico de criptografia que complementa o protocolo USM definido na RFC 3414. O protocolo é baseado no algoritmo AES (*Advanced Encryption Standard*) de cifragem, usado no modo CFB (*Cipher Feedback Mode*) com um chave de 128 bits.

3.4. RMON I

O padrão *Remote Monitoring* (RMON) oferece a capacidade de monitoramento remoto através de uma arquitetura de gerenciamento distribuída. Assim torna-se mais fácil o monitoramento de múltiplos segmentos remotos de rede. O RMON não se trata especificamente de um protocolo, mas sim de uma MIB.

Para fazer o monitoramento de operações básicas de redes, a primeira versão do RMON MIB é baseada em SNMP. No primeiro padrão de RMON, são definidos dois grupos de redes Ethernet. Atualmente, esses padrões já são treze, contribuindo para que o monitoramento de redes com agentes RMON possa ser feito independente de marca ou vendedor.

A primeira versão do protocolo RMON foi composta baseada nas seguintes descrições:

- RFC 2613 [20]. *Remote Network Monitoring MIB Extensions for Switched Networks Version 1.0*

Arquitetura de objetos da RMON MIB definidos para monitoramento remoto de *Switched Networks* (SMON), caracteriza a interface entre os Agentes RMON e Gerentes RMON.

- RFC 2819 [21]. *Remote Network Monitoring Management Information Base*

Definições de uso da MIB para protocolos de gerenciamento em redes TCP/IP remotas.

- RFC 2895 [22]. *Remote Network Monitoring MIB Protocol Identifier Reference*

Descreve as notações de identificação das camadas em um protocolo encapsulado, utilizadas em objetos da RMON MIB.

- RFC 2896 [23]. *Remote Network Monitoring MIB Protocol Identifier Macros*

Exemplos de identificadores de diversos protocolos que interagem com a RMON MIB. As Macros são distribuídas com portabilidade para TCP/IP, Novell IPX, XEROX, AppleTalk, Banyon Vines, DECNet, IBM SNA, NetBEUI e NetBIOS.

- RFC 3577 [24]. *Introduction to the Remote Monitoring (RMON) Family of MIB Modules*

O protocolo RMON é constituído por um número de documentos que definem suas características. Esta referência descreve esses documentos e como eles se relacionam uns aos outros.

- RFC 3737 [25]. *IANA Guidelines for the Registry of Remote Monitoring (RMON) MIB modules*

Documento que define os procedimentos de padronização utilizados pela IANA (*Internet Assigned Numbers Authority*) para administrar a árvore de identificação de objetos (OID) no modelo RMON.

- RFC 3919 [26]. *Remote Network Monitoring (RMON) Protocol Identifiers for IPv6 and Multi Protocol Label Switching (MPLS)*

Descrição de integração dos protocolos IPv6 e MPLS no modelo de gerenciamento utilizando RMON.

3.5. RMON II

Através do RMON II é possível gerenciar até a camada de Aplicação, diferente de sua primeira versão RMON I que transmite somente até a camada de Enlace do modelo OSI. Com isso torna-se possível gerenciar diretamente dados de aplicativos.

A figura 3.3 descreve a atuação das versões do protocolo RMON.

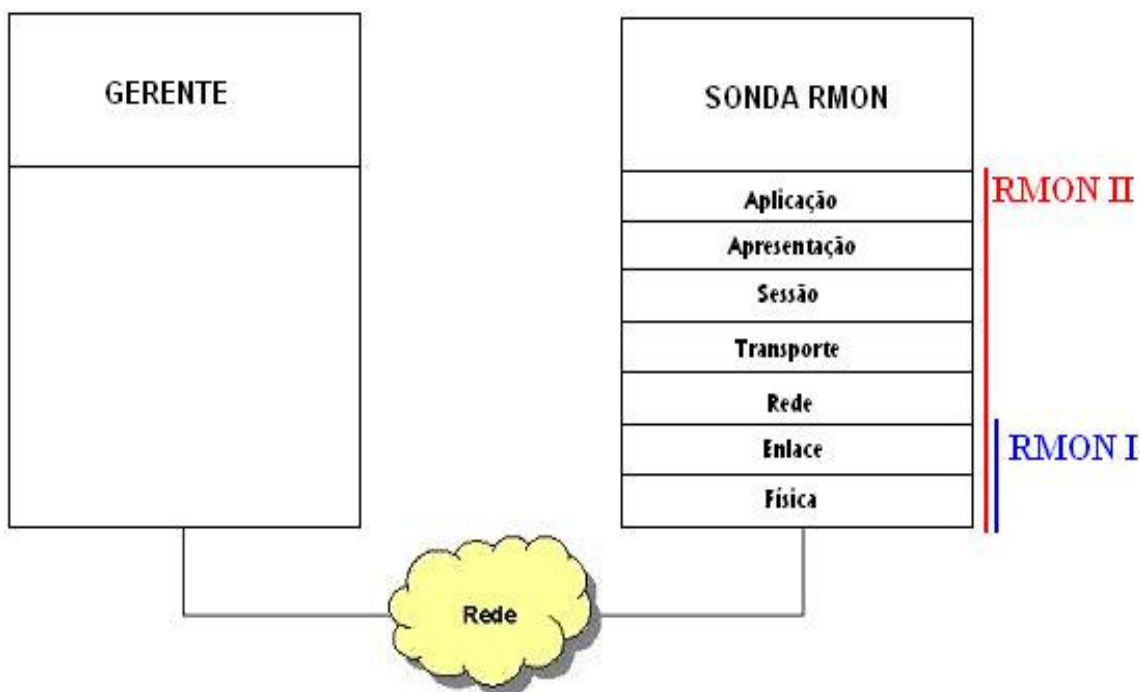


Figura 3.3 – Atuação das versões do protocolo RMON

As informações são gerenciadas através de grupos de controle que formam a RMON II MIB.

A segunda versão do protocolo RMON foi composta baseada nas seguintes descrições:

- RFC 4502 [27]. *Remote Network Monitoring Management Information Base Version 2*

Define o uso do protocolo RMON na camada de Aplicação e os objetos da RMON II MIB, organizados nos seguintes grupos:

- Protocolo de diretório
- Protocolo de distribuição
- Mapeamento de endereço
- Camada de rede host
- Camada de rede matriz
- Camada de aplicação host
- Camada de aplicação matriz
- Histórico
- Teste de configuração

4. Ferramentas de Gerência

As ferramentas de gerência são aplicações desenvolvidas com o intuito de auxiliar na gerência de redes. Existem dois tipos básicos de Ferramentas de Gerência: as de código fechado, que são softwares proprietários, e as de código aberto, que são softwares livres. Não desmerecendo as ferramentas de código fechado, que são ótimas, neste trabalho o foco são as ferramentas de código aberto, uma vez que os softwares proprietários geralmente têm um custo financeiro muito elevado.

Uma outra grande vantagem da utilização do software livre é sua grande flexibilidade em relação a customizações de código, para atender as necessidades do gerente. Além disso, essas ferramentas têm uma grande portabilidade, ou seja, são multiplataforma, facilitando assim as adaptações necessárias ao ambiente operacional.

A Tabela 4.1 apresenta um quadro comparativo entre os principais focos das ferramentas em software livre descritas neste trabalho e as áreas funcionais de Gerência de Redes.

	Falha	Configuração	Contabilização	Performance	Segurança
MRTG	X		X	X	
Cacti	X	X	X	X	
Sarg			X		X
Nagios	X	X			X
OpenNMS	X	X			X

Tabela 4.1 – Quadro comparativo entre ferramentas e áreas de Gerência de Redes

4.1. MRTG

O MRTG (*Multi Router Traffic Grapher* [28]), é uma ferramenta para monitorar o tráfego de equipamentos em rede, que gera páginas HTML (*HyperText Markup Language*) contendo imagens no formato PNG (*Portable Network Graphics*) que mostram, estatisticamente, representação deste tráfego.

O MRTG trabalha na maioria das plataformas UNIX e também Windows NT. Foi desenvolvido em Perl e apresenta código livre. Ele usa uma implementação de SNMP com grande portabilidade, escrita toda em Perl, não sendo necessária a instalação de nenhum pacote SNMP adicional. As rotinas de tempo crítico são escritas em C para aumentar a performance da ferramenta.

A ferramenta consiste em um script programado em Perl que usa o protocolo SNMP para ler contadores de tráfego nas interfaces dos equipamentos de rede interconectados e um programa em C que analisa os dados gerando figuras de gráficos que exibem a utilização e performance de forma gerencial via WEB em HTML.

Estes gráficos demonstram estatísticas detalhadas e armazenadas em históricos que contém informações alimentadas cada vez que o Gerente SNMP solicita as informações para os Agentes SNMP configurados.

A Figura 4.1 demonstra um gráfico gerado pelo MRTG onde é contabilizada a utilização de uma interface de rede, o gráfico é dividido em intervalos de horas alimentados com dados coletados a cada cinco minutos. A escala, neste caso, é medida em Mb/s onde o preenchimento em verde demonstra o tráfego de entrada e as linhas em azul o tráfego de saída.

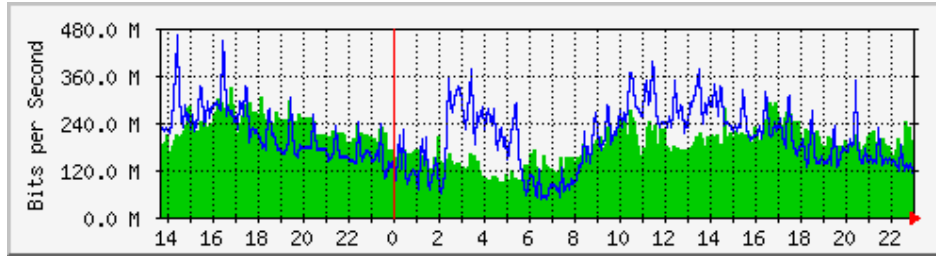


Figura 4.1 – Gráfico de utilização organizado em horas gerado pelo MRTG

A Figura 4.2 demonstra um gráfico gerado pelo MRTG onde é demonstrada a utilização de uma interface de rede, o gráfico é dividido em intervalos de dias alimentados com dados coletados a cada trinta minutos. A escala, neste caso, também é medida em Mb/s onde o preenchimento em verde demonstra o tráfego de entrada e as linhas em azul o tráfego de saída.

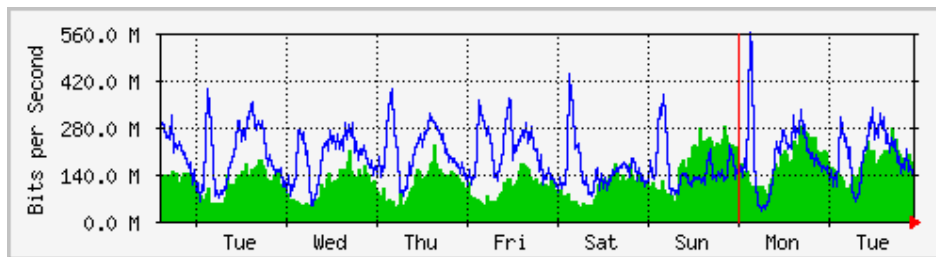


Figura 4.2 – Gráfico de utilização organizado em dias gerado pelo MRTG

A Figura 4.3 demonstra um gráfico gerado pelo MRTG onde é demonstrada a utilização de uma interface de rede, o gráfico é dividido em intervalos de semanas alimentados com dados coletados a cada duas horas. A escala, neste caso, também é medida em Mb/s onde o preenchimento em verde demonstra o tráfego de entrada e as linhas em azul o tráfego de saída.

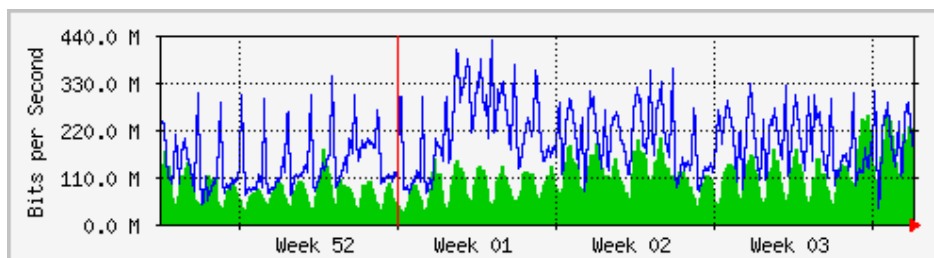


Figura 4.3 – Gráfico de utilização organizado em semanas gerado pelo MRTG

A Figura 4.4 demonstra um gráfico gerado pelo MRTG onde é demonstrada a utilização de uma interface de rede, o gráfico é dividido em intervalos de meses alimentados com dados coletados a uma vez por dia. A escala, neste caso, também é medida em Mb/s onde o preenchimento em verde demonstra o tráfego de entrada e as linhas em azul o tráfego de saída.

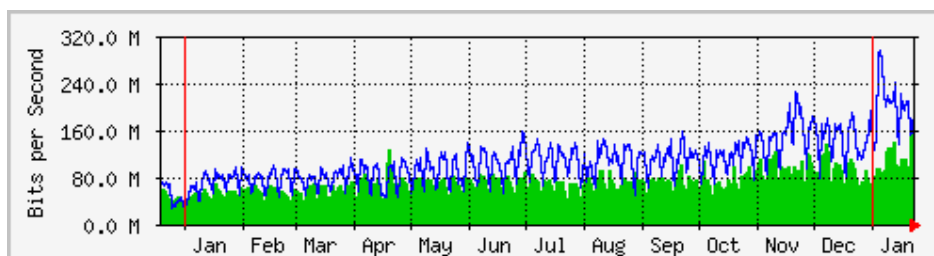


Figura 4.4 – Gráfico de utilização organizado em meses gerado pelo MRTG

As informações descritas na Tabela 4.1, também foram geradas pelo MRTG e definem o tráfego, tanto de entrada como de saída de dados em uma interface de rede. As informações encontram-se organizadas em entrada de dados (*IN*) e saída de dados (*OUT*), divididas em tráfego máximo (*Max*), média de tráfego (*Average*) e tráfego atual (*Current*).

	<i>Max</i>	<i>Average</i>	<i>Current</i>
IN	329.2 Mb/s (7.7%)	192.0 Mb/s (4.5%)	177.4 Mb/s (4.1%)
OUT	460.4 Mb/s (10.7%)	200.1 Mb/s (4.7%)	102.9 Mb/s (2.4%)

Tabela 4.2 – Gráfico de utilização em meses gerado pelo MRTG

4.2. Cacti

O Cacti [29] é uma ferramenta que pode ser perfeitamente utilizada substituindo o MRTG, pois este não possui tantas facilidades como organização gerenciada de gráficos em árvores, customização de relatórios e outras funcionalidades apresentadas pelo Cacti, apesar de ambos terem semelhanças na base do sistema. Utilizando o Cacti, em pouco tempo e de forma muito simplificada, o gerente pode configurar para coleta e armazenamento de dados, vários ativos de rede. As medições contabilizam e medem a performance de vários objetos, que disponibilizam dados para geração de gráficos de processamento, temperatura, tráfego de rede, uso de memória, tempo de uso (*uptime*), capacidade de armazenagem, etc.

A figura 4.5 demonstra como os dados gerenciáveis são organizados e documentados de forma flexível, onde o gerente define seus grupos de equipamentos bem como quais gráficos serão exibidos e em que ordem.

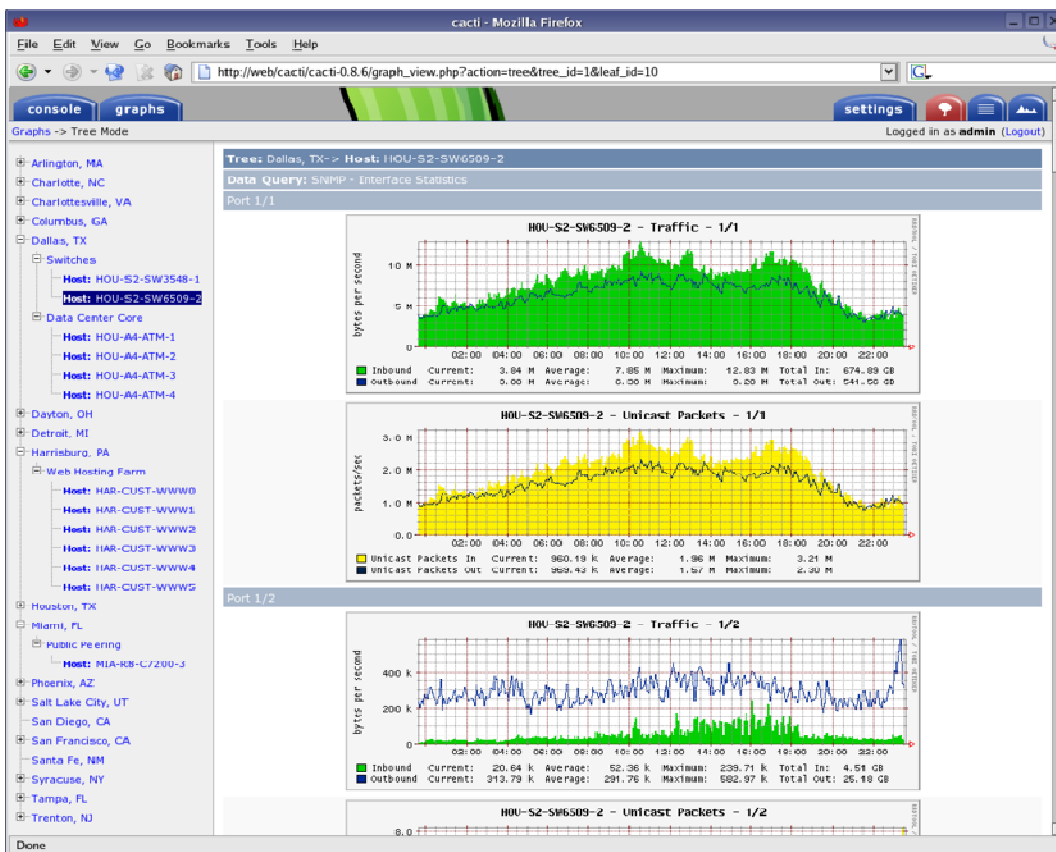


Figura 4.5 – Gráficos organizados em árvore pelo Cacti

Utiliza como base o RRDTools, um sistema de armazenagem e mostragem de dados coletados via SNMP entre um determinado período de tempo, que além de armazenar os dados de maneira bastante compacta que não aumenta com o tempo (forma circular), também disponibiliza a geração de gráficos. É o mesmo sistema utilizado pelo MRTG. O Cacti é uma ferramenta com interface via WEB, desenvolvida em PHP e armazena seus dados em banco de dados MySQL.

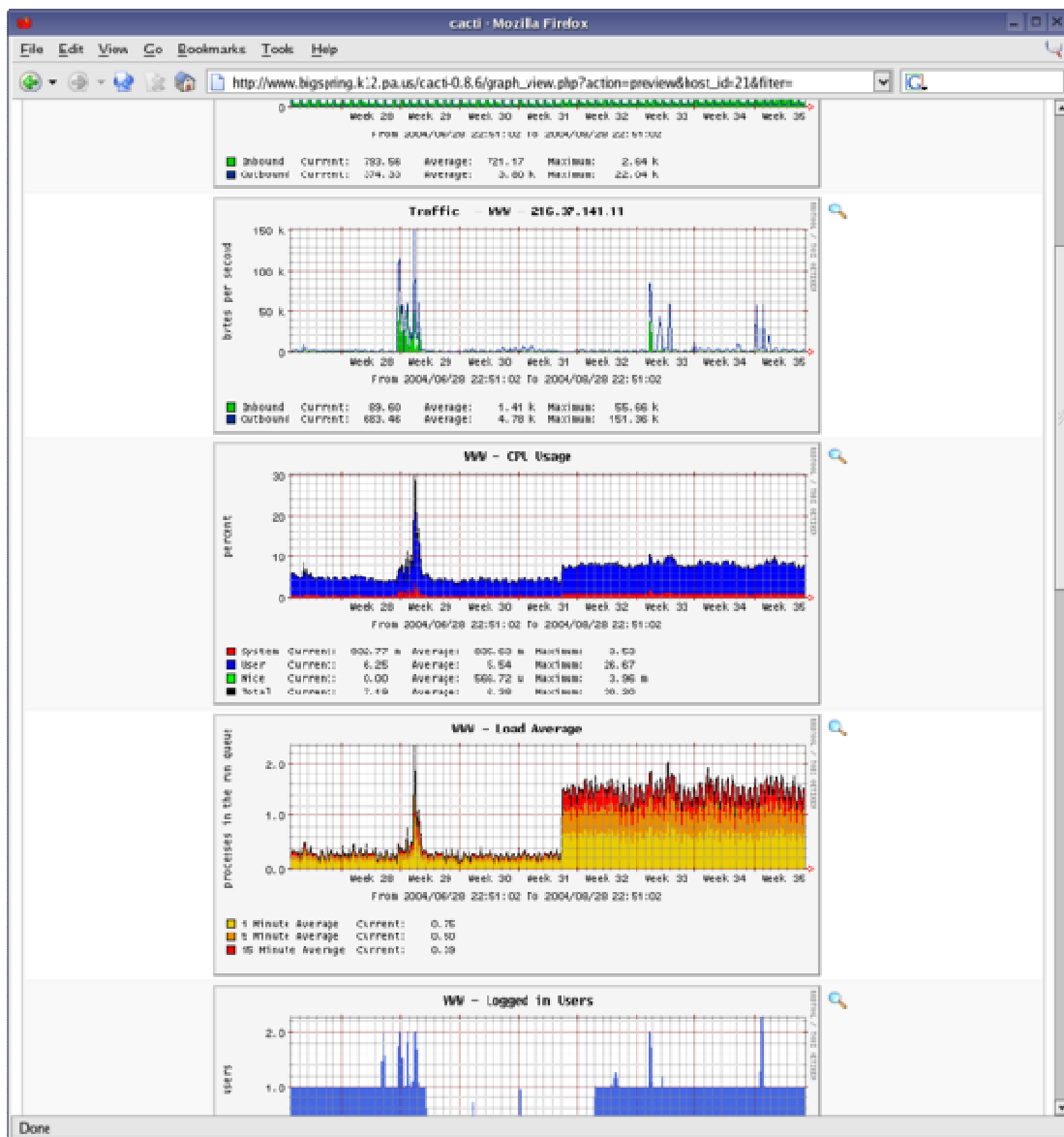


Figura 4.6 – Gráficos de performance gerados pelo Cacti

4.3. Sarg

O SARG (*Squid Analysis Report Generator*) [30] é uma ferramenta que permite ao gerente gerar relatórios de acesso WEB através da análise do arquivo de log "access.log" do famoso proxy Squid, com informações de para "onde" seus usuários estão indo na Internet. Apesar de não utilizar um protocolo de gerência de redes, o poder da ferramenta é incrível, através dela é possível gerenciar quais usuários acessaram quais sites, em que horas, quantos bytes foram baixados, quantas conexões foram feitas, relatórios de sites mais acessados, usuários que mais acessam, relatório de sites negados, falha de autenticação, entre outros.

A ferramenta trabalha lendo o arquivo "access.log" do servidor proxy e processa todas as informações armazenadas das requisições de usuários ao proxy, a partir de então é gerado um relatório em HTML com informações gerenciais de acessos WEB. Pode ser automatizada através do agendador de tarefas do sistema operacional, e disponibiliza as informações processadas ao gerente de forma organizada e precisa.

A figura 4.7 exibe um, dos vários recursos do Sarg, que é o gráfico de utilização por usuário, organizado em dias do mês e quantidade de bytes.

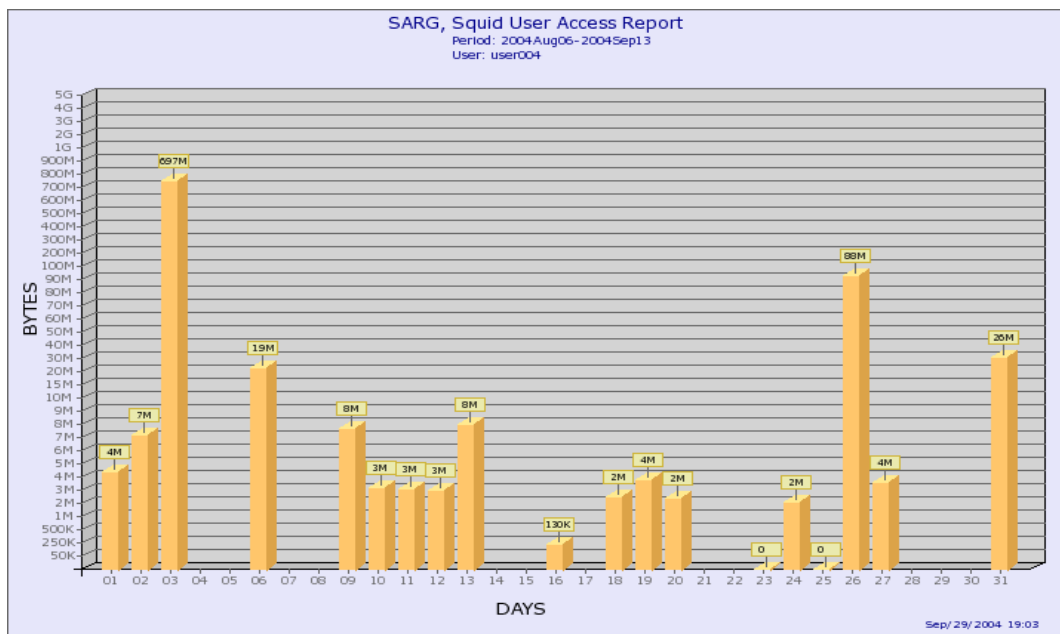


Figura 4.7 – Gráfico de utilização em bytes por dia e usuário do Sarg

4.4. Nagios

O Nagios [31] é um monitor de ativos e serviços de rede, desenvolvido para detectar e informar falhas. Apesar de ser homologado para rodar em sistemas operacionais Linux, possui uma portabilidade capaz de operar em sistemas operacionais UNIX em geral. O servidor de monitoramento faz checagens periódicas nos agentes (equipamentos e serviços), que retornam informações de estado ao gerente (Nagios).

Quando problemas são encontrados, o servidor pode mandar notificações aos contatos administrativos em várias formas diferentes como e-mail, SMS, Mensagem Instantânea, e outros. As informações processadas em tempo real, históricos e chamados podem ser acessados via WEB.

A figura 4.8 demonstra um relatório de serviços agrupados por servidores, que por sua vez, são agrupados em tipos de equipamentos. Todos os dados são contabilizados e exibidos através da interface WEB.

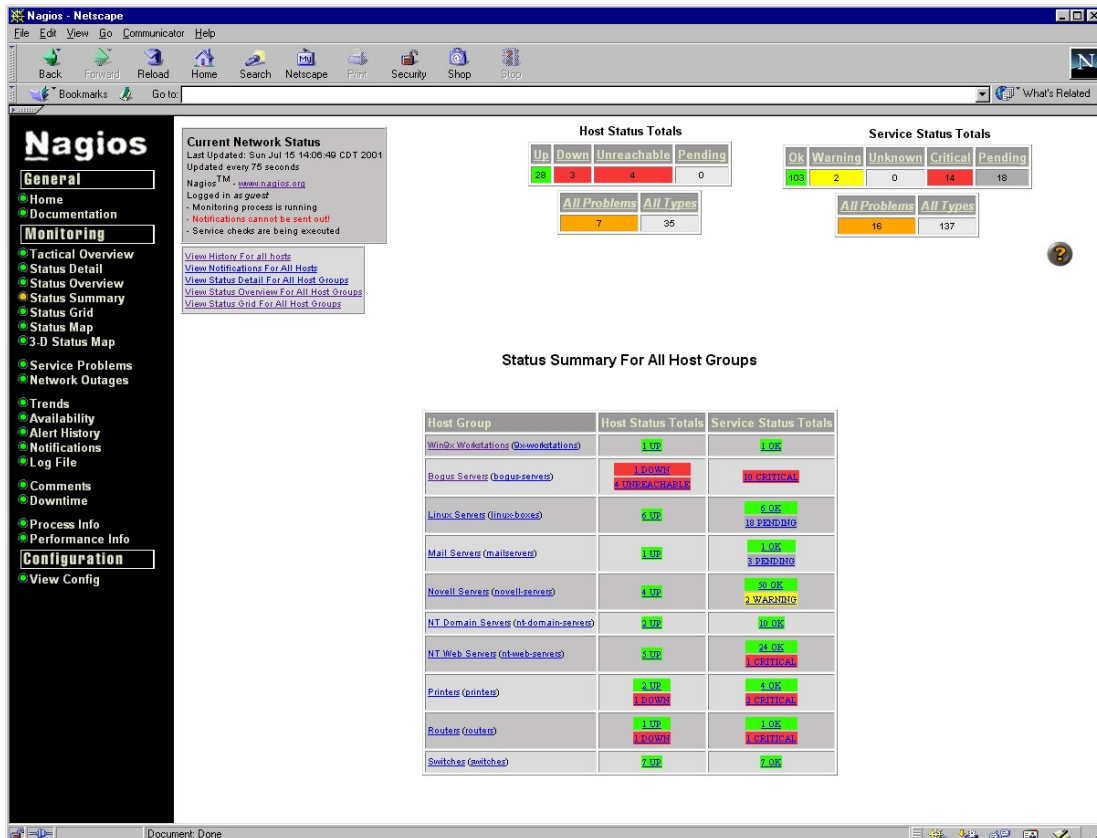


Figura 4.8 – Estatísticas por grupos de agentes através do Nagios.

A figura 4.9 exibe informações de serviços, gerado pelo Nagios, de um determinado servidor com dados informativos de estado e operações administrativas interagindo diretamente com o gerente.

Information For Service Total Cache Buffers On Host netware3
 Last Updated: Sun Jul 15 14:18:03 CDT 2001
 Updated every 75 seconds
 Nagios™ - www.nagios.org
 Logged in as guest
 - Monitoring process is running
 - Notifications can be sent out
 - Service checks are being executed

Total Cache Buffers
 on
Netware Server #3
192.168.14

Service State Information

Variable	Value
Current Status	WARNING
Status Information	Total cache buffers = 21223
Current Attempt	3/3
State Type	HARD
Last Check Type	ACTIVE
Last Check Time	07-15-2001 14:14:48
Next Scheduled Active Check	07-15-2001 14:19:48
Latency	< 1 second
Check Duration	< 1 second
Service Checks Enabled?	YES
Passive Checks Being Accepted?	YES
Last State Change	07-11-2001 10:34:48
Current State Duration	4d 3h 43m 15s
Last Service Notification	N/A
Current Notification Number	0
Service Notifications Enabled?	YES
Event Handler Enabled?	YES
Flap Detection Enabled?	YES
Is This Service Flapping?	NO
Percent State Change	0.00%
In Scheduled Downtime?	NO
Last Update	07-15-2001 14:17:52

Service State Statistics

State	Time	% Time
OK	0d 0h 9m 25s	0.2%
WARNING	4d 3h 43m 15s	99.8%
UNKNOWN	0d 0h 0m 0s	0.0%
CRITICAL	0d 0h 0m 0s	0.0%
All States	4d 3h 52m 40s	100.0%

Service Commands

- [Disable notifications for this service](#)
- [Delay next service notification](#)
- [Schedule downtime for this service](#)
- [Disable checks of this service](#)
- [Delay next service check](#)
- [Schedule an immediate check of this service](#)
- [Submit passive check result for this service](#)
- [Stop accepting passive checks for this service](#)
- [Disable event handler for this service](#)
- [Disable flap detection for this service](#)

Service Comments

Figura 4.9 – Informações de estado de serviço através do Nagios.

4.5. OpenNMS

Assim como o Nagios, o OpenNMS [32] também é uma ferramenta de gerência em plataforma livre utilizando o protocolo SNMP, focada no monitoramento de equipamentos e serviços, prevendo e notificando falhas. A diferença entre as ferramentas é que de um modo geral o OpenNMS é melhor recomendado para o caso de redes grandes, inclusive de longa distância, enquanto o Nagios é mais utilizado, na maior parte dos casos, em redes locais e sem exagero de hosts. Entretanto, isso não significa que o OpenNMS também possa ser utilizado em redes pequenas e locais.

A figura 4.10 demonstra um mapa de rede configurada, gerado pelo OpenNMS, onde é possível visualizar as entidades envolvidas documentadas por endereço e interconexões, além de acompanhar o monitoramento de disponibilidade.

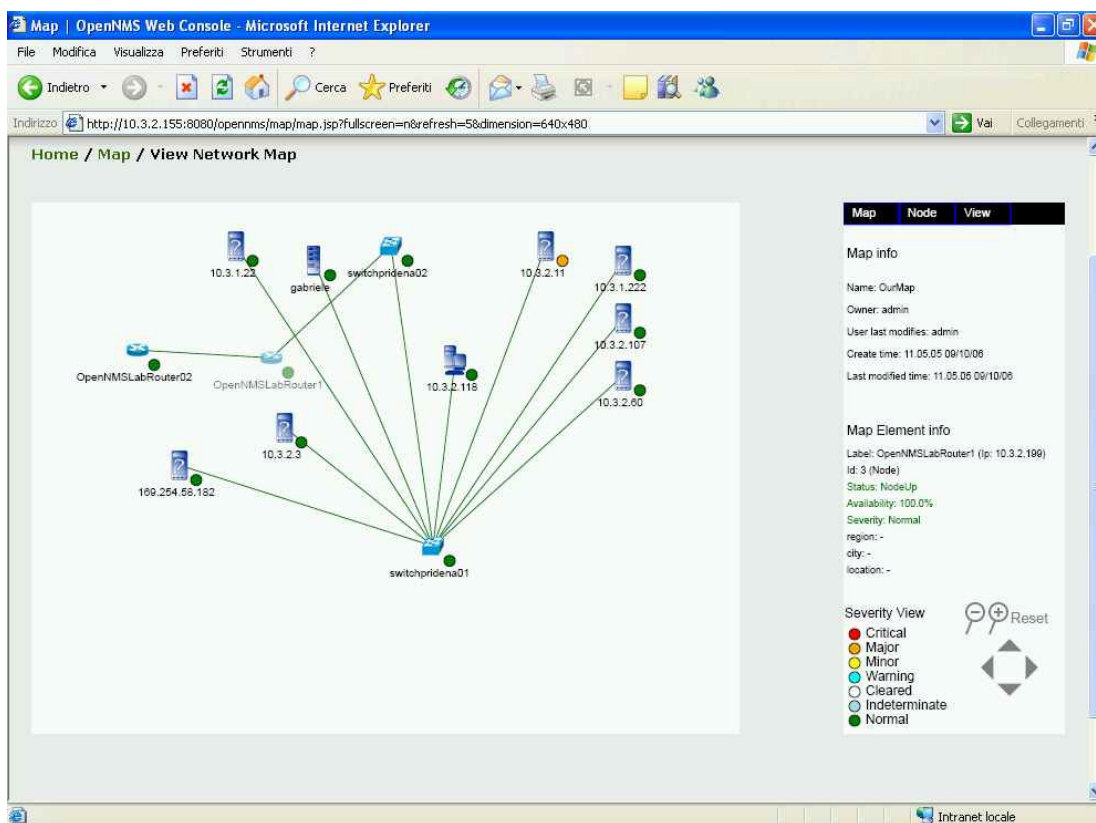


Figura 4.10 – Mapa de Rede Gerado pelo OpenNMS

5. Conclusão

Observando as ferramentas citadas ao longo deste trabalho, conclui-se que independente de seu tamanho e distância, uma rede deve ser gerenciada para garantir o controle de disponibilidade, agilidade e confiabilidade; através de coleta de dados, processamento e documentação.

Pode-se observar também que a utilização de Técnicas de Gerência de Redes baseadas em software livre são tão vantajosas quanto soluções utilizando software proprietário, tendo ainda, a flexibilidade de serem altamente customizáveis. Apesar da ausência de suporte técnico para implantação e utilização, os softwares citados disponibilizam todas as documentações necessárias.

Contando com os protocolos SNMP e RMON, as ferramentas disponibilizam relatórios, que ajudam no monitoramento e gerenciamento de redes locais, mesmo que estas estejam interconectadas à distância.

6. Bibliografia

- [1] INTERNET ENGINEERING TASK FORCE (IETF). **Structure and Identification of Management Information for TCP/IP-based Internets**, RFC 1155, mai. 1990.
- [2] INTERNET ENGINEERING TASK FORCE (IETF). **A Simple Network Management Protocol (SNMP)**, RFC 1157, mai. 1990.
- [3] INTERNET ENGINEERING TASK FORCE (IETF). **Concise MIB Definitions**, RFC 1212, mar. 1991.
- [4] INTERNET ENGINEERING TASK FORCE (IETF). **Management Information Base for Network Management of TCP/IP-based internets: MIB-II**, RFC 1213, mar. 1991.
- [5] INTERNET ENGINEERING TASK FORCE (IETF). **Introduction to Community-based SNMPv2**, RFC 1901, jan. 1996.
- [6] INTERNET ENGINEERING TASK FORCE (IETF). **Introduction Structure of Management Information Version 2 (SMIv2)**, RFC 2578, abr. 1999.
- [7] INTERNET ENGINEERING TASK FORCE (IETF). **Textual Conventions for SMIv2 (SMIv2)**, RFC 2579, abr. 1999.
- [8] INTERNET ENGINEERING TASK FORCE (IETF). **Conformance Statements for SMIv2**, RFC 2580, abr. 1999.
- [9] INTERNET ENGINEERING TASK FORCE (IETF). **Introduction and Applicability Statements for Internet Standard Management Framework**, RFC 3410, dez. 2002.
- [10] INTERNET ENGINEERING TASK FORCE (IETF). **An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks**, RFC 3411, dez. 2002.
- [11] INTERNET ENGINEERING TASK FORCE (IETF). **Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)**, RFC 3412, dez. 2002.

- [12] INTERNET ENGINEERING TASK FORCE (IETF). **Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)**, RFC 3413, dez. 2002.
- [13] INTERNET ENGINEERING TASK FORCE (IETF). **User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)**, RFC 3414, dez. 2002.
- [14] INTERNET ENGINEERING TASK FORCE (IETF). **View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)**, RFC 3415, dez. 2002.
- [15] INTERNET ENGINEERING TASK FORCE (IETF). **Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)**, RFC 3416, dez. 2002.
- [16] INTERNET ENGINEERING TASK FORCE (IETF). **Transport Mappings for the Simple Network Management Protocol (SNMP)**, RFC 3417, dez. 2002.
- [17] INTERNET ENGINEERING TASK FORCE (IETF). **Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)**, RFC 3418, dez. 2002.
- [18] INTERNET ENGINEERING TASK FORCE (IETF). **Coexistence between SNMP Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework**, RFC 3584, ago. 2003.
- [19] INTERNET ENGINEERING TASK FORCE (IETF). **The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model**, RFC 3826, jun. 2004.
- [20] INTERNET ENGINEERING TASK FORCE (IETF). **Remote Network Monitoring MIB Extensions for Switched Networks Version 1.0**, RFC 2613, jun. 1999.
- [21] INTERNET ENGINEERING TASK FORCE (IETF). **Remote Network Monitoring Management Information Base**, RFC 2819, mai. 2000.
- [22] INTERNET ENGINEERING TASK FORCE (IETF). **Remote Network Monitoring MIB Protocol Identifier Reference**, RFC 2895, ago. 2000.

- [23] INTERNET ENGINEERING TASK FORCE (IETF). **Remote Network Monitoring MIB Protocol Identifier Macros**, RFC 2896, ago. 2000.
- [24] INTERNET ENGINEERING TASK FORCE (IETF). **Introduction to the Remote Monitoring (RMON) Family of MIB Modules**, RFC 3577, ago. 2003.
- [25] INTERNET ENGINEERING TASK FORCE (IETF). **IANA Guidelines for the Registry of Remote Monitoring (RMON) MIB modules**, RFC 3737, abr. 2004.
- [26] INTERNET ENGINEERING TASK FORCE (IETF). **Remote Network Monitoring (RMON) Protocol Identifiers for IPv6 and Multi Protocol Label Switching (MPLS)**, RFC 3919, out. 2004.
- [27] INTERNET ENGINEERING TASK FORCE (IETF). **Remote Network Monitoring Management Information Base Version 2**, RFC 4502, mai. 2006.
- [28] OETIKER, Tobi. **MRTG: The Multi Router Traffic Grapher**. Disponível em: <http://oss.oetiker.ch/mrtg/>. Acesso em 12 mar. 2007.
- [29] The Cacti Group. **Cacti: The Complete RRDTOol-based Graphing Solution**. Disponível em: <http://cacti.net/>. Acesso em 16 mar. 2007.
- [30] ORSO, Pedro. **SARG: Squid Analysis Report Generator**, Disponível em <http://sarg.sourceforge.net/>. Acesso em 22 mar. 2007.
- [31] GALSTAD, Ethan. **Nagios**. Disponível em <http://www.nagios.org/>. Acesso em 02 Abr. 2007.
- [32] **OpenNMS: Enterprise-grade Open-source Network Management**, Disponível por WWW em 10/04/2007 no endereço: <http://www.opennms.org/>