

LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RIO GRAN-
DE DO NORTE – FARN
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

FAUSTO BATISTA DA CUNHA FILHO

A UTILIZAÇÃO DO IMC (INTELLIGENT MANAGEMENT CENTER) NO
GERENCIAMENTO DE REDES CORPORATIVAS

LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RIO GRAN-
DE DO NORTE – FARN
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

FAUSTO BATISTA DA CUNHA FILHO

A UTILIZAÇÃO DO IMC (INTELLIGENT MANAGEMENT CENTER) NO
GERENCIAMENTO DE REDES CORPORATIVAS

NATAL
2011

FAUSTO BATISTA DA CUNHA FILHO

**A UTILIZAÇÃO DO IMC (INTELLIGENT MANAGEMENT CENTER) NO
GERENCIAMENTO DE REDES CORPORATIVAS**

Monografia apresentada à Faculdade Natalense
para o Desenvolvimento do Rio Grande do
Norte – FARN, como parte dos requisitos para
obtenção do título de Bacharel em Sistemas de
Informação.

Orientador: Prof. Msc. Aluizio Ferreira da
Rocha Neto

NATAL
2011

BIBLIOTECA UNI-RN

004.4 C972u - RB: 37238 (M002069)

Título: A utilização do IMC (Intelligent

Autoria: Cunha Filho, Fausto Batista da

2011, ex. 1

Catalogação na Publicação – Biblioteca da FARN
Setor de Processos Técnicos

Cunha Filho, Fausto Batista da

A utilização do IMC (Intelligent Management Center) no
Gerenciamento de Redes Corporativas / Fausto Batista da Cunha Filho. –
Natal, 2011.

43f.

Orientador: Aluizio Ferreira da Rocha Neto. (Msc.)

Monografia (Bacharel em Sistemas de Informação) – Faculdade
Natalense para o Desenvolvimento do Rio Grande do Norte.

1. Sistemas de Informação - Monografia. 2. Redes Corporativas -
Monografia. 3. IMC – Monografia. 4. Monitoramento - Monografia.

I. Título.

RN/FARN/BC

CDU 004.4

FAUSTO BATISTA DA CUNHA FILHO

**A UTILIZAÇÃO DO IMC (INTELLIGENT MANAGEMENT CENTER) NO
GERENCIAMENTO DE REDES CORPORATIVAS**

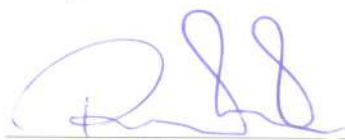
Monografia apresentada à Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte – FARN, como parte dos requisitos para obtenção do título de Bacharel em Sistemas de Informação.

Aprovado em: ____/____/____

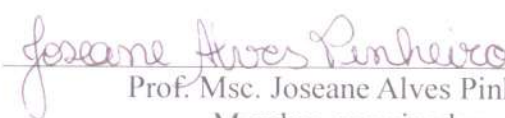
BANCA EXAMINADORA



Prof. Msc. Aluizio Ferreira da Rocha Neto
Orientador



Prof. Esp. Romulo Fagundes Catanhede
Membro examinador



Prof. Msc. Joseane Alves Pinheiro
Membro examinador

Dedico este trabalho aos meus pais por acreditarem e apoiarem os meus ideais.

AGRADECIMENTOS

Em primeiro lugar quero agradecer a Deus, por me proporcionar a capacidade de enfrentar as dificuldades e vencer mais uma etapa de minha vida.

Aos meus pais, Fausto e Rosa, pelos seus esforços para proporcionar-me uma educação digna, me passando valores e princípios, além do amor, dedicação e compreensão em todos os momentos de minha vida.

Às minhas irmãs, Mirella e Miriádine que me acompanharam nesta caminhada e até mesmo à distância me passando exemplos de perseverança e apoio nos momentos difíceis e cansativos.

Aos meus padrinhos Roberto e Katherine por quem tenho um carinho muito especial. Obrigado por seu apoio e carinho dedicados a mim como a um filho.

Aos meus amigos Guilherme, Rodrigo, Breno, João, Eduardo, Janilson, Jurandir, Luiz, Gustavo, Josias, Caty e todos mais que se fizeram presentes nas comemorações e em momentos especiais para amenizar pressões e problemas enfrentados nesta caminhada.

Aos educadores Romulo, Ricardo, Cristiane, Damasceno e aos demais professores que certamente contribuíram no meu aprendizado durante esta graduação. Em especial a minha “quase” orientadora Joseane.

À minha namorada, Adriana, pela compreensão e apoio em momentos difíceis. Por sua paciência para me suportar, sendo sempre o meu porto seguro, me passando tranquilidade e motivação para seguir em frente nos momentos mais turbulentos. E principalmente por aprender as normas da ABNT e me ajudar com este trabalho.

Ao meu orientador e Mestre, Aluizio Rocha, pelo incentivo à realização deste trabalho, por acreditar em meu potencial, assim como sua disponibilidade para orientar-me, contribuindo sempre com seu conhecimento e suas opiniões.

Por fim, agradeço a esta banca examinadora, por sua disponibilidade, opiniões e observações possibilitando o crescimento deste trabalho.

RESUMO

O presente trabalho analisa a implantação do software IMC (Intelligent Management Center) observando seus principais recursos, bem como a usabilidade proposta por esta ferramenta. Sua instalação e configuração foram realizadas em ambiente real na Secretaria de Estado do Meio Ambiente e dos Recursos Hídricos – SEMARH, do Rio Grande do Norte, permitindo, desta forma, analisar o desempenho e a eficiência da ferramenta em uma rede de médio porte, composta de diversos dispositivos como switches, servidores, impressoras e demais equipamentos. As facilidades proporcionadas por sua interface gráfica, também foram observadas durante a análise, assim como seu sistema de histórico de alertas e suas funções de gerenciamento. Outro fator que foi verificado durante o desenvolvimento deste trabalho foi a produtividade proporcionada por uma ferramenta de gerência de redes à equipe de TI, com relação à atuação do suporte técnico na antecipação aos problemas decorrentes de falhas de equipamentos e demais erros apresentados, na instituição supracitada.

Palavras-Chave: Gerenciamento de rede. Monitoramento em tempo real. IMC.

ABSTRACT

This paper analyzes the implementation of the software IMC (Intelligent Management Center) observing its key features and usability proposed by this tool. Its installation and configuration were performed in a real environment in the State Secretariat of Environment and Water Resources - SEMARH, Rio Grande do Norte, allowing, this way, to analyze the performance and efficiency of the tool in a network of medium size, composed of various devices such as switches, servers, printers and other equipment. The facilities provided by its graphic interface, were also observed during the analysis, as well as system of alert history and management functions. Another factor that was found during the development of this work was provided by a productivity tool for network management IT staff, with respect to the performance of technical support in anticipation of problems arising from equipment failures and other errors presented in the above institution.

Keywords: Network Management. Real-Time Monitoring. IMC.

LISTA DE FIGURAS

Figura 1 – Elementos de uma arquitetura geral de solução de gerência.	16
Figura 2 – Página de login do IMC.	29
Figura 3 – Tela para adição de usuários no IMC.	31
Figura 4 – Tela de visualização dos equipamentos adicionados no IMC.	33
Figura 5 – Página de “ <i>Resource</i> ” de um equipamento.	34
Figura 6 – Página de configuração do monitoramento de portas e serviços.	35
Figura 7 – Visualização de conexões switch-hosts.	36
Figura 8 – Página de alarmes do IMC.	38
Figura 9 – Página de configuração dos alarmes do IMC.	38
Figura 10 – Página de configuração do envio de notificação por e-mail.	39

LISTA DE TABELAS

Quadro 1 – Ambiente de Instalação	26
Quadro 2 – Níveis de Alarme do IMC	37

LISTA DE SIGLAS

ADSL	Asymmetric Digital Subscriber Line
CPU	Central Processing Unit
DES	Data Encryption Standard
DMA	Deployment Monitoring Agent
GB	Gigabyte
GHZ	Gigahertz
HP	Hewlett-Packard
HTTP	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
MD5	Message-Digest algorithm 5
MIB	Management Information Base
NMS	Network Management System
OSI	Open Systems Interconnection
POP3	Post Office Protocol
QoS	Quality of Service
RFC	Request for Comments
SA	System Administrator
SEMARH	Secretaria de Estado do Meio Ambiente e dos Recursos Hídricos
SHA	Secure Hash Algorithm
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOA	Service-Oriented Architecture
SQL	Structured Query Language
SSH	Secure Shell
TCP	Transmission Control Protocol
TI	Tecnologia da Informação
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network

SUMÁRIO

1 INTRODUÇÃO	12
1.1 OBJETIVO	13
1.1.1 Objetivos Específicos	13
1.2 JUSTIFICATIVA	14
2 REFERENCIAL TEÓRICO	15
2.1 GERÊNCIA DE REDES	15
2.2 APLICAÇÕES DE GERÊNCIA BASEADAS EM WEB	16
2.3 SNMP.....	17
2.3.1 Vantagens do SNMP	18
2.3.2 As Desvantagens do SNMP	19
2.3.3 Implementação.....	20
2.3.4 SNMPv2.....	21
2.3.5 SNMPv3.....	21
2.3.6 TRAP.....	22
3 IMC - INTELLIGENT MANAGEMENT CENTER (CENTRO INTELIGENTE DE GERENCIAMENTO)	23
3.1 VISÃO GERAL.....	23
3.2 IMPLANTAÇÃO FLEXÍVEL E ESCALONÁVEL.....	23
3.3 CONTROLE ADMINISTRATIVO.....	24
3.4 GERENCIAMENTO DE RECURSOS.....	24
3.5 MONITORAÇÃO E GERENCIAMENTO DETALHADOS DE DESEMPENHO.....	24
3.6 RELATÓRIOS FLEXÍVEIS CENTRALIZADOS	25
3.7 GERENCIAMENTO SIMPLIFICADO DE VLAN	25
3.8 INSTALAÇÃO DO SOFTWARE IMC	25
3.8.1 Preparação para a instalação e implantação	25
3.8.2 Instalação do IMC	27
3.8.3 Implementando o IMC	28
3.8.4 Iniciando o Uso do IMC	28
3.8.5 Protocolo de Acesso aos Equipamentos	29
3.8.6 Criação de Grupo de Dispositivos.....	30
3.8.7 Criar Operadores.....	30
4 ANÁLISE DAS FERRAMENTAS DO IMC	32
4.1 CARACTERÍSTICAS DE SOFTWARES DE GERENCIAMENTO	32
4.2 MONITORAMENTO DE COMPONENTES.....	32
4.2.1 Serviços.....	34
4.2.2 Exibição da Topologia da Rede	35
4.3 SISTEMÁTICAS DE NOTIFICAÇÃO DOS EVENTOS E ALTERAÇÕES NA REDE	37
4.3.1 Classificação dos Alarmes do IMC	37
4.3.2 Configuração das Notificações.....	38
4.4 ANÁLISE DA INTERFACE GRÁFICA	39
5 CONCLUSÕES.....	41
REFERÊNCIAS	43

1 INTRODUÇÃO

Nos dias atuais, as redes de computadores são importantes ferramentas na vida das empresas, permitindo a comunicação entre equipamentos, quer estes estejam num mesmo prédio ou em qualquer parte do planeta, superando barreiras físicas e geográficas, por meio da internet. Esse conceito permite que informações sejam permutadas continuamente entre uma empresa matriz, com suas filiais, com fornecedores, ou ainda com seus clientes, oferecendo serviços sem que haja a necessidade da presença física de qualquer um deles. No entanto para que haja esse tipo de serviço é preciso uma infraestrutura adequada, pois a falha de comunicação pode culminar na interrupção dos serviços, o que pode vir a gerar prejuízos.

Levando em consideração a importância destes serviços para as empresas, as redes de computadores têm sido usualmente controladas por técnicos especialistas que possuem a responsabilidade de instalar, manter e resolver seus problemas, é o que afirma Melchior (1999). Estes profissionais lidam com problemas que variam do suporte aos usuários, esclarecendo dúvidas até o procedimento de identificação e substituição de equipamentos com mau funcionamento.

Estes profissionais vêm sendo exigidos cada vez mais, uma vez que a crescente heterogeneidade de equipamentos e serviços produz uma grande quantidade de informações, que devem ser analisadas e interpretadas pelo administrador da rede, a fim de evitar, ou ao menos minimizar os problemas que venham a ocorrer, visando garantir uma maior eficiente e transparência dos serviços da rede para os usuários.

Com toda esta responsabilidade é preciso realizar o controle de equipamentos em uma rede de computadores da forma mais simples e prática possível. Para auxiliar o administrador de redes existem ferramentas que ajudam a detectar os problemas quando eles ocorrem, ou, antes mesmo que eles ocorram.

Realizar esta tarefa sem auxílio de instrumentos adequados, não é uma tarefa fácil e provavelmente não trará um resultado de muita qualidade. Existem ferramentas de gerência com as mais diversas finalidades, atendendo a diferentes gostos. Com a difusão da internet e a expansão dos serviços Web, as aplicações de gerência de redes baseadas nesta tecnologia estão sendo cada vez mais bem aceitas.

A proposta deste trabalho é analisar a importância das ferramentas de Gerência de Redes para auxiliar a sua administração, apresentando as principais funcionalidades e vantagens.

Um importante fator no gerenciamento é a habilidade de adquirir informações sobre os equipamentos envolvidos e as mudanças ocorridas nestes [LEI 96 apud MELCHIOR, p. 40].

A Secretaria de Estado do Meio Ambiente e dos Recursos Hídricos – SEMARH é uma pasta de Governo responsável pelo controle ambiental e pelos recursos hidrogeológicos do estado do Rio Grande do Norte. Criada em 1995, ainda como Subsecretaria de Recursos Hídricos, a SERHID (hoje SEMARH), é responsável por gerenciar os recursos hídricos naturais do estado, por meio de estudos, planejamentos, desenvolvendo e gerenciando, de forma integrada, descentralizada e participativa. Também é responsável pela organização dos usuários em torno dos módulos de oferta d'água: açudes, canais de integração, adutoras de água bruta, leitos naturais de rios perenizados e aquíferos, pelo controle do uso dos recursos hídricos, de modo a garantir a sustentabilidade do sistema no plano ambiental, social, econômico e financeiro. Presta serviços públicos pelo Estado sobre a infraestrutura hídrica referente à construção, manutenção, operação e gestão, esta incluindo o controle técnico e administrativo.

A Secretaria de Estado do Meio Ambiente e dos Recursos Hídricos possui cento e vinte e dois dispositivos de rede entre servidores, estações de trabalho, switches gerenciáveis, impressoras e access points, que não possuíam nenhum monitoramento.

1.1 OBJETIVO

Fazer uma análise da implantação do software de gerenciamento de redes IMC (Intelligent Management Center), observando recursos, vantagens e desvantagens com relação a sua instalação, usabilidade e eficiência.

1.1.1 Objetivos Específicos

- Descrever a instalação e configuração da ferramenta IMC;
- Analisar as principais dificuldades encontradas em sua instalação;
- Verificar se o software em análise alcança os principais objetivos deste tipo de ferramenta;
- Identificar os seus principais recursos e as principais limitações.

1.2 JUSTIFICATIVA

As ferramentas de gerência de rede são fundamentais para qualquer administrador. São elas que ajudam a detectar problemas no momento em que eles ocorrem, ou até mesmo antes de ocorrerem. Realizar esta gestão sem o auxílio de instrumentação adequada é uma tarefa bastante trabalhosa e que, provavelmente, não proporcionará um resultado satisfatório.

O administrador de redes tem por objetivo principal manter o bom funcionamento da rede lógica e dos serviços oferecidos por ela. Para isso é preciso prever falhas maiores e evitar a interrupção de serviços e comunicação.

Este trabalho tem como importância proporcionar uma análise da ferramenta IMC (Intelligent Management Center) da HP/3COM desde a sua instalação até sua configuração e usabilidade. Tendo como enfoque principal a verificação de seus componentes, constatando se estes satisfazem as necessidades deste tipo de software, mostrando ainda a importância e eficácia, que esse tipo de programa pode proporcionar ao administrador de redes.

2 REFERENCIAL TEÓRICO

2.1 GERÊNCIA DE REDES

De acordo com Lopes, Sauv , Nicolletti (2003), a Ger ncia de Redes tem como principal objetivo monitorar e controlar os elementos da rede (f sicos ou l gicos), o que possibilita a garantia de certo n vel de qualidade de servi o (QoS). Para isso, os respons veis pela ger ncia de redes tem em seu aux lio softwares que gerenciam redes, sistemas que s o compostos por uma cole  o de ferramentas integradas para monitorar e controlar equipamentos e servi os da rede. Tais sistemas oferecem uma interface  nica, geralmente amig vel, de comandos que permite trazer informa  es e enviar ordens aos objetos monitorados.

O principal objetivo de um software de gerenciamento de redes   informar ao administrador qualquer problema em sua rede, antes mesmo que terceiros lhe informem.

A necessidade de monitorar e controlar os elementos de redes, tanto f sicos, quanto l gicos, visa garantir um determinado n vel de qualidade do servi o.

Nos dias atuais a informatiza  o nas empresas vem sendo diferencial estrat gico e operacional. Uma paraliza  o de servi o afeta n o s o a disponibilidade, como tamb m a confiabilidade. Isto pode gerar preju zo, o que n o   interessante para ningu m, independente de ramo de atua  o.

Um bom administrador de redes deve perseguir o que se tem por ideal, com rela  o   funcionalidade, que   manter o sistema funcionando 100% do tempo, evitando a todo custo a paraliza  o de servi os e comunica  o entre os envolvidos, sejam clientes ou colaboradores.

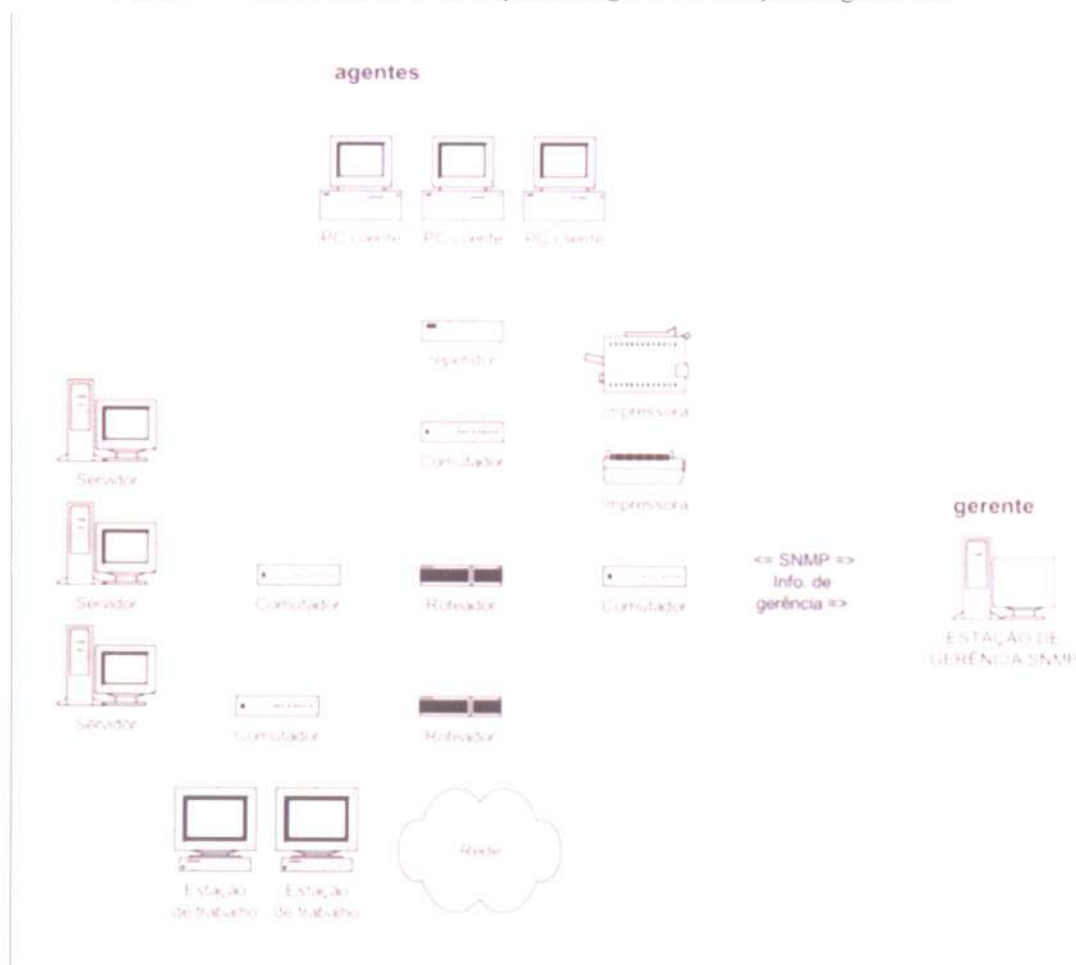
  preciso conhecer seus equipamentos e o funcionamento destes, para que seja poss vel ganhar em antecipa  o   ocorr ncia de problemas. Para isso,   necess rio que o administrador utilize ferramentas de monitoramento de redes, que poder o lhe proporcionar essa vantagem na pr via detec  o de falhas, possibilitando a interven  o no equipamento ou servi o que venha a funcionar de maneira indesejada.

Desta forma tamb m   poss vel reduzir o per odo de interrup  o de servi os, quando h  a queima de algum equipamento, pois   poss vel detectar, exatamente, em que n o est  o equipamento e substituí-lo de maneira mais r pida, minimizando poss veis preju zos.

No entanto, como o sistema de gerência informa também o mau funcionamento, ou intermitência dos equipamentos, é possível se antecipar à falha destes e efetuar a correção ou substituição dos mesmos.

Na figura 1 é possível entender o funcionamento de uma rede gerenciada, utilizando o protocolo SNMP (Simple Network Management Protocol), realizado por uma estação de gerência.

Figura 1 – Elementos de uma arquitetura geral de solução de gerência.



Fonte: LOPES, SAUVÉ, NICOLLETTI (2003).

2.2 APLICAÇÕES DE GERÊNCIA BASEADAS EM WEB

Lopes, Sauvé, Nicolletti (2003) afirmam que as aplicações de gerência que permitem o monitoramento, assim como o controle a partir de um navegador, são bem atrativas para os administradores da rede.

Dentre as vantagens das ferramentas de gerência baseadas em Web podemos citar a possibilidade de efetuar o monitoramento e o controle dos elementos da rede usando qualquer navegador, em qualquer nó da rede. Ao falar em aplicações de gerência stand-alone, apenas era possível usar a ferramenta em máquinas onde ela estivesse instalada e devidamente configurada.

Uma vantagem mais plausível é a economia com treinamentos de pessoal, já que a interface gráfica da Web já é bem conhecida e as operações realizadas em um navegador também. Um outro fator é a riqueza da interface gráfica sendo bastante superior a interfaces de linha de comando obtidas através de telnet, conclui Lopes, Sauvé, Nicolletti (2003).

2.3 SNMP

Segundo Costa (2008, p. 22), uma rede gerenciada pelo protocolo SNMP é formada por três componentes:

1. Dispositivos Gerenciados
2. Agentes
3. Sistemas de Gerenciamento de Redes (NMS – Network-Management Systems)

Um nó de rede que possua um agente SNMP instalado e encontre-se em um ambiente gerenciado, é considerado um Dispositivo Gerenciado. Tais dispositivos passam a ter a capacidade de coletar e armazenar informações de gerenciamento, mantendo estas informações disponíveis, através do protocolo SNMP, para sistemas NMS. Dentre os dispositivos que podem se enquadrar nesta categoria, estão: computadores, dispositivos de armazenamento, impressoras, roteadores, servidores de acesso, switches, dentre outros (COSTA, 2008, p. 22).

Para o autor supracitado, qualquer equipamento que o software do agente SNMP esteja sendo executado é um Agente. Em outras palavras, o Agente é um Dispositivo Gerenciado que possui um agente SNMP instalado e se encontra em uma rede gerenciada. Geralmente as mensagens geradas pelos Agentes são respostas às solicitações realizadas pelo Sistema de Gerenciamento, sendo exceção às mensagens de interceptação, esta é iniciada pelo Agente e tem a função de informar uma reinicialização do sistema, ou um acesso não autorizado. Algo como um alarme.

É necessário definir uma comunidade, algo como um domínio onde os equipamentos monitorados e o sistema de gerenciamento devem estar configurados para que seja possível a

comunicação entre eles. Esta configuração fornece segurança permitindo que apenas os agentes e sistemas de gerenciamento contidos na mesma comunidade se comuniquem.

Ao longo dos anos, o SNMP vem sendo usado como o principal protocolo no gerenciamento de rede. E o sucesso deste protocolo é tão grande, que ele não é somente usado para gerenciamento de equipamentos tradicionais de rede como computadores, roteadores, etc. Atualmente, qualquer equipamento que tenha a necessidade de estar 100% em funcionamento e condizente com as perspectivas de mercado, deve ter incorporado à capacidade de permitir ser gerenciado via SNMP. E essa tendência, faz com que os mais variados equipamentos já saiam com suporte ao SNMP de fábrica para estar na realidade de mercado, como por exemplo: Modem ADSL, Impressoras e etc.

Como o próprio nome do protocolo diz “simples”, ele ganhou fama pela facilidade em implementação de soluções com o seu uso. Quando o modelo RM-OSI (Reference Model – Open System Interconnection) ficou pronto em 1993, após um cuidadoso e demorado desenvolvimento, o SNMP já estava difundido em diversos produtos.

O sistema de gerenciamento de rede da arquitetura TCP/IP opera na camada da aplicação e baseia-se no protocolo SNMP.

Os padrões que definem a estrutura de gerenciamento de redes Internet são descritos nos documentos RFC-1155, RFC-1156 (MIB – Management Information Base) e RFC-1157 (SNMP). Como no esquema de gerenciamento OSI, os processos que implementam as funções de gerenciamento Internet atuam como agentes e gerentes (CAMATTA; GOBIRA; MELOTTI, 2007).

O SNMP (Protocolo de Gerência Simples de Rede) é um protocolo de gerenciamento típico de redes TCP/IP.

2.3.1 Vantagens do SNMP

De acordo com Freitas (2000), a popularidade é, sem dúvida, a sua maior vantagem, pois estão disponíveis para dispositivos de rede que variam de computadores, pontes, modems, até impressoras. Este fator é que permite a interoperabilidade, fator bastante considerável dado à diversidade de equipamentos e marcas em parques tecnológicos.

Esta interoperabilidade só é possível devido a simplicidade deste protocolo, que concentra a maior parte do processamento na máquina do manager, permitindo que os nós da rede

utilizem o protocolo mesmo não tendo grande poder de processamento e sem interferir no desempenho destes.

Tendo em vista a simplicidade de seu projeto, a implementação em uma rede de grande porte torna-se simples para um usuário programar variáveis que ele gostaria de estar monitorando, pois cada variável contém apenas as seguintes informações:

- O nome da variável;
- Os tipos de dados da variável (inteiro, string, etc.);
- Se a variável é somente de leitura ou de leitura e escrita;
- O valor da variável.

Outro benefício observado é a facilidade de expansão, devido essa simplicidade apresentada pelo SNMP, permitindo ser atualizado de forma que ele possa ser adequado às necessidades de usuários no futuro. E como os agentes de SNMP podem ser estendidos para cobrir dados de dispositivos específicos, SNMP pode assumir numerosos trabalhos específicos para classes de dispositivos como impressoras, roteadores, e pontes, provendo um mecanismo padrão de controle e monitoramento de rede.

2.3.2 As Desvantagens do SNMP

Ainda segundo Freitas (2000) toda essa flexibilidade proporciona ao projeto SNMP algumas falhas. No entanto a maioria delas pode ser contornada.

A segurança pode ser considerada a deficiência mais crítica do protocolo SNMP. As falhas podem dar acesso a intrusos da rede à informações que transitam pela mesma. Também é possível que estes desligar terminais ou alterar a configuração de algum equipamento gerenciável. Contudo, a solução para este problema é simples devido a expansibilidade do SNMP, a versão de SNMPv2, somou alguns mecanismos de segurança que ajudam a combater os 3 principais problemas de segurança: privacidade de dados (prevenir os intrusos de ganhar acesso a informação levadas pela rede), autenticação (impedir os intrusos de enviar falsos dados pela rede), e controle de acesso (que restringe acesso de variáveis particulares a certos usuários, removendo assim a possibilidade de um usuário derrubar a rede acidentalmente).

Na verdade, SNMP provê pouco suporte para esquemas de autenticação. Ele suporta apenas um esquema de duas palavras-chave. Uma pública permite ao manager pedir o valor de variáveis (get), e outra privada permite ao manager fixar valores de variáveis (set). Essas

palavras-chave são chamadas communities, e todo dispositivo conectado numa rede gerenciada por SNMP deve ter essas duas communities configuradas.

Ao menos uma das communities está sempre presente em cada mensagem do manager para o agente, mas é descrita sem nenhuma proteção, como texto simples, propiciando falhas de segurança. O que torna fácil para o intruso descobrir as palavras-chave e influir no funcionamento da rede.

Além da questão da segurança, SNMP é tão simples que a informação com a qual ele lida não é detalhada ou bem-organizada o bastante para suportar redes de grande porte. Isto é principalmente devido à rápida criação do SNMP sendo o protocolo mais utilizado atualmente.

Outros problemas podem ser citados: a eficiência do protocolo é questionável, pois o mesmo transmite muitos dados desnecessários; também é questionada a eficiência da organização das variáveis na árvore MIB. Freitas (2000) também afirma que, por usar endereçamento IP, se há um problema de roteamento na rede e um dispositivo não pode ser alcançado, é impossível monitorá-lo ou reconfigurá-lo remotamente.

2.3.3 Implementação

A implementação do protocolo SNMP vem sendo cada vez mais difundida por muitos administradores de rede atualmente é o que afirma Freitas (2000). Tendo como primeiro passo a implementação da comunicação por TCP/IP, onde cada nó da rede recebe um endereço IP diferente, diferenciando um nó do outro. Em seguida deve se adquirir (ou programar) softwares para o agente e o gerente, geralmente os dispositivos mais recentes já fornecem por padrão uma interface gráfica para facilitar a configuração e a visualização dos dados.

A configuração dos agentes deve ser realizada em cada nó da rede, enquanto o gerente deve ser instalado em máquinas das quais se deseja monitorar a rede. Geralmente após essas configurações é só seguir as instruções dos programas para configurar a rede SNMP, especificando as MIBs.

2.3.4 SNMPv2

Definida na RFC 1448, nesta versão é possível uma especificação de variáveis com mais detalhes, incluindo o uso de uma tabela de estrutura de dados que facilita a recuperação de dados.

As características adicionadas geraram uma expansão nas especificações para SNMP, que estas se expandiram de 36 páginas (com v1) para 416 páginas com SNMPv2.

Com relação a segurança, os avanços foram muitos. Como exemplo pode-se citar o emprego de técnicas criptográficas na transmissão das palavras-chave (passwords) de autenticação do manager, dificultando o acesso de intrusos.

A MIB foi melhorada para MIB-II incluindo muito mais objetos padrão, passando ao total de 175. Também foram adicionadas novas categorias para os objetos.

Apesar do esforço, o SNMPv2 não vingou, pois tornou-se bastante complexo em relação a versão 1 do projeto original do SNMP. É difícil encontrar agentes que suportem totalmente o padrão v2.

Em 1997 foi lançado o SNMPv3, com mais avanços na questão de segurança. Mas ainda não está tão difundido com relação a sua utilização.

2.3.5 SNMPv3

SNMP versão 3 (SNMPv3), é uma expansão do SNMP, que tem a função de complementar o SNMPv2 trazendo como principais vantagens aspectos ligados à segurança. Esta segurança busca evitar a alteração das mensagens enviadas. Além disto, limita-se o acesso a elementos estranhos à execução de operações de controle, que são realizadas através da primitiva "SetRequest". Evita-se também o acesso à leitura das mensagens por parte de estranhos, além de se garantir ao gerente o direito de alteração da senha dos agentes.

A segurança é conseguida através da introdução de mecanismos de criptografia com o DES (Data Encryption Standard) e de algoritmos de autenticação que podem ser tanto o MD5 quanto o SHA (Secure Hash Algorithm) de acordo com o RFC 2571.

2.3.6 TRAP

Segundo RFC 1215 o gerente, normalmente, é quem tem a função de iniciar a comunicação com os agentes. Isso é o padrão no mundo SNMP. Essa operação tem o nome de sondagem (polling). Essa sondagem são consultas realizadas pelo gerente, com determinado nível de periodicidade aos agentes de todos os elementos gerenciados. Desta forma é solicitado que seja informado o valor de algumas variáveis de gerência mais críticas. Desta maneira a estação de gerência descobre a existência de eventos anormais nos elementos gerenciados.

Embora não tão frequente, é possível que o agente inicie a comunicação. Isto ocorre quando o agente necessita enviar um trap à estação de gerência para notificar algum comportamento ou evento anormal, sem esperar pela próxima operação de sondagem. (LOPES, SAUVÉ, NICOLLETTI 2003).

3 IMC - INTELLIGENT MANAGEMENT CENTER (CENTRO INTELIGENTE DE GERENCIAMENTO)

3.1 VISÃO GERAL

O Centro Inteligente de Gerenciamento é uma ferramenta de gerência desenvolvida pela 3Com, uma plataforma independente e abrangente extremamente flexível com escalabilidade criada para atender às necessidades de redes corporativas avançadas.

O IMC foi projetado em uma arquitetura orientada para serviços (SOA), tendo por núcleo um modelo de fluxo para aplicativos corporativos e apresentando uma estrutura modular escalonável. A combinação permite a implementação eficiente de um gerenciamento corporativo ponta a ponta enquanto o design modular do IMC possibilita a integração efetiva de ferramentas de gerenciamento tradicionalmente isoladas, oferecendo um total gerenciamento de recursos, serviços e usuários.

Esta estrutura é compatível com o Windows Server 2003 e permite o gerenciamento de dispositivos 3Com, H3C e demais fabricantes.

O IMC é licenciado com base no número de dispositivos que exigem o gerenciamento. Ele oferece suporte para até 200 dispositivos gerenciados.

Para que se nós adicionais possam ser monitorados é preciso adquirir licença adicional para estender o limite de nós do IMC.

3.2 IMPLANTAÇÃO FLEXÍVEL E ESCALONÁVEL

O IMC disponibiliza um amplo conjunto de recursos para o gerenciamento de redes de grande porte. Proporciona uma enorme flexibilidade, que suporte heterogeneidades de fabricantes em seus equipamentos e serviços.

A implantação é dada de maneira distribuída e flexível, o que permite escalabilidade e alta disponibilidade. O IMC pode ser implantado em vários servidores, oferecendo maior escalabilidade, o que evitará que a queda de um servidor, ou uma interrupção de comunicação isolada, interrompa o monitoramento.

3.3 CONTROLE ADMINISTRATIVO

O controle administrativo é multiusuário e baseado em funções, permitindo ao administrador prover administração e monitoramento flexíveis da infraestrutura de rede da organização. Desta forma o Administrador do Sistema possui um controle sobre quais usuários do IMC têm permissão para gerenciar dispositivos e grupos de dispositivos, assim como também é possível restringir as operações realizadas pelos usuários. Também é possível ter acesso a trilhas de auditoria completas que detalham todas as modificações na rede e identifica quem as executou. Isso ajuda a garantir que os processos e controles necessários estejam em vigor para atender à conformidade e desempenho do ambiente de TI.

3.4 GERENCIAMENTO DE RECURSOS

O recurso de descoberta e topologia de rede, possui inclusive um inventário detalhado da rede e descrições bastante precisas de como a rede está configurada. As visualizações compatíveis incluem Camada 2 e Camada 3, além de topologia VLAN e visualização personalizada. A visualização personalizada permite ao usuário a organização e o controle da infraestrutura de rede com base em qualquer modelo organizacional. O painel de gerenciamento de dispositivos integrado ao IMC oferece um amplo gerenciamento de elementos tanto para dispositivos 3Com quanto H3C.

3.5 MONITORAÇÃO E GERENCIAMENTO DETALHADOS DE DESEMPENHO

Um processo completo de gerenciamento de falhas é oferecido pelo software, assim como a correlação e análise detalhadas, alarmes em tempo real, solução de problemas e captura de experiência. A monitoração de desempenho é dada de forma simples, tornando mais fácil detectar gargalos e outros problemas de rede, inclusive os relacionados a CPU, memória e utilização de largura de banda, tempo de resposta de dispositivos e disponibilidade.

As estatísticas TopN permitem uma rápida identificação das áreas e dos dispositivos mais carregados na rede. Um limiar pode ser definido para gerar alarmes em qualquer monitor, alertando rapidamente os operadores sobre eventuais problemas. Para que o operador não

receba um excesso de alarmes, o IMC oferece a opção de definir eventos personalizáveis, além de regras de filtragem de alarmes e eventos.

3.6 RELATÓRIOS FLEXÍVEIS CENTRALIZADOS

O gerenciamento centralizado de relatórios simplifica a administração de relatórios da organização. Os relatórios históricos flexíveis do IMC fornecem as informações necessárias à análise de tendências da rede e planejamento de capacidade, oferecendo relatórios predefinidos ou permitindo que os usuários definam os parâmetros de seus próprios relatórios por meio de um gerador de relatórios.

Os relatórios podem ser visualizados em diversos formatos, inclusive “pdf” e “xls”, e podem ser enviados automaticamente por e-mail ou programados para execução regular.

3.7 GERENCIAMENTO SIMPLIFICADO DE VLAN

Com a utilização, cada dia mais frequente de VLANs, o software simplifica a implantação e o gerenciamento destas na infraestrutura de rede da organização. Isso inclui a capacidade de visualizar as topologias de VLAN atuais e implantar VLANs em massa pela rede.

3.8 INSTALAÇÃO DO SOFTWARE IMC

3.8.1 Preparação para a instalação e implantação

Antes da instalação, é preciso certificar-se de que todos os requisitos listados no quadro 1 são atendidos.

Quadro 1– Ambiente de Instalação

Item	Requisitos
Hardware	Atende as especificações do CPU, memória e disco rígido no contrato.
Software	Certifique-se que o tipo e a versão do sistema operacional, versão do banco de dados, e a versão IMC atende os requisitos de instalação. O servidor é reiniciado após a instalação do banco de dados.
Verificar a instalação do banco de dados	Antes de instalar o IMC, instalar o primeiro banco de dados. Durante o procedimento de instalação do IMC, as conexões de banco de dados correspondentes são verificadas.
Verificação de patches do SQL Server	Service Pack 3 é necessário para o SQL Server 2005. Service Pack 1 é necessário para o SQL Server 2008.
Auto inicialização do serviço do SQL Server	Selecione Painel de Controle > Ferramentas Administrativas > Serviços e certifique-se o item Tipo de Inicialização do MSSQLSERVER está definido como Automático.
Auto inicialização do agente do SQL Server	Selecione Painel de Controle > Ferramentas Administrativas > Serviços e certifique-se o item Tipo de Inicialização do ServerAgent SQL é definido como Automático.
Desinstalação do software IMC	A desinstalação completa é necessária se o IMC software já tenha sido instalado anteriormente no sistema.
Verificar as configurações de firewall	Para implantar o IMC em modo distribuído, você deve abrir a porta de escuta no servidor instalado com o banco de dados. O número padrão da porta de escuta do banco de dados SQL server é 1433, o número padrão da porta de escuta do banco de dados Oracle é 1521, e o número padrão da porta de escuta do banco de dados MySQL é 3306.

Fonte: <http://www1.hp.com/us/en/products/imc>

Para a instalação do IMC foi utilizada uma microcomputador com processador Intel® Core 2 Quad (Q8200) clock de 2,33GHz, duas memórias de 2 GB DDR2, HD Seagate 320

GB, Fonte alimentadora de 500 Watts (potência real), Sistema Operacional Microsoft Windows Server 2003 R2 e banco de dados Microsoft SQL Server 2005 Enterprise.

A instalação do IMC foi realizada no mesmo servidor onde o SQL está rodando, todas as etapas da descrição de procedimentos foram focada sobre esta situação.

3.8.2 Instalação do IMC

Executou-se o arquivo de instalação. No diretório de instalação escolheu-se a raiz do sistema "C:\", executou-se o arquivo "install.bat".

Depois disso, uma janela foi exibida solicitando a senha para o SA (System Administrator) do sql. Após a escolha da senha clicou-se em ok.

Na tela seguinte foi escolhida a opção "Next" no "IMC Welcome Installation Wizard". Logo depois, na tela de contrato, aceitou-se o mesmo selecionando a opção "Accept" e clicando em "Next".

Por padrão, o IMC é instalado em "C:\Program Files\IMC". Porém optou-se por instalá-lo em "C:\IMC". Depois de selecionar um caminho de instalação, pressiona-se novamente "Next", onde foi apresentada a janela de "Installation Summary", iniciou-se a instalação propriamente dita clicando em "Install".

Observou-se que a janela "Installation Summary" fornece as seguintes informações:

- O nome, descrição, versão e espaço necessário de cada componente;
- A localização da instalação de cada componente;
- O espaço total;
- O espaço livre da partição onde está instalado IMC.

Se não houver espaço suficiente em disco disponível, a quantidade de espaço em disco irá aparecer em vermelho.

É preciso disponibilizar espaço suficiente para que a aplicação possa armazenar dados referentes aos equipamentos existentes.

Na janela de "Installation Completed", você pode selecionar "Proceed with Deployment" ou "Install other IMC Components". Se você deseja instalar apenas a plataforma IMC sem qualquer componente, selecione "Proceed with Deployment" e clique em "Finish" para iniciar a implantação.

3.8.3 Implementando o IMC

No caso de nova instalação, é preciso implantar os componentes instalados para torná-los prontos para uso. Após a instalação, o IMC inicia automaticamente a instalação do agente de monitoramento inteligente, que guiará a implantação.

Na tela de "Batch Deploy", é possível escolher todos os componentes disponíveis, colocando uma marca na caixa correspondente e clicando em ok.

O IMC utilizara o sistema de banco de dados Microsoft SQL Server. Deve-se passar a autenticação do banco antes de criar um banco de dados. Portanto, na caixa de texto SA (System Administrator) senha, digite a senha SA especificado na instalação do SQL Server.

Por padrão, arquivos de banco de dados são armazenados em C:\Program Files\Imcddata, mas é possível escolher o caminho aonde o IMC armazenará seus dados, caso não se queira utilizar o local padrão, digite um novo caminho na caixa de texto "Data File Location", ou clique em "Browse" e escolha o caminho, clique em "Next".

A porta padrão para acesso HTTP é a 8080 e para acesso via HTTPS é 8443. Você pode escolher outras portas. Depois clique em "Deploy".

Depois de iniciado a implementação do IMC, você verá os componentes do IMC sendo instalado um de cada vez. Uma vez que a implantação foi concluída, IMC será carregado.

Quando carregado clicar em "View Readme File" vai abrir uma janela com documentação IMC, clicou-se em "Start IMC Server Now" esta ação trouxe a primeira página do Agente de Monitoramento de Implantação (DMA – Deployment Monitoring Agent).

Depois que a implantação foi concluída, a janela de implantação inteligente Agente de Monitoramento aparece. Selecionando a guia "Deploy", é possível visualizar informações sobre a implantação do componente.

3.8.4 Iniciando o Uso do IMC

Para acessar o IMC via navegador é preciso digitar o endereço IP da máquina onde o software está instalado seguido da porta 8080 (ex.: <http://xxx.xxx.xxx.xxx:8080>).

A primeira vez que entrar, não haverá dados na página inicial do software.

No primeiro acesso ao IMC, haverá uma solicitação da instalação do ActiveX e do cliente Java, já na janela de Bem-vindo.

Figura 2 – Página de login do IMC.

3Com Intelligent Management Center

3COM **IMC**

The new generation of network management systems, named 3Com Intelligent Management Center (IMC), is a platform to address issues in network operations and management. Designed with the concept of a Service-Oriented Architecture (SOA), with the business application flow model as the core, and the on-demand modularized structure, IMC helps clients to implement end-to-end business management by providing a complete solution that integrates applications, resources and users. With flexible functional components, IMC can offer customized business-specific solutions, simplifying the business operation and management.

IMC utilizes a design concept, which integrates users, resources and services on an open technology platform. This design concept enables the IMC to provide business-specific solutions, relieving clients from laborious and chaotic task of managing today's complex infrastructures and services.

Your license is a trial version and it will expire on November 11, 2011. Please activate it before the expiry date.

<http://www.3com.com>

3COM Copyright © 2008-2009 3Com Corporation and its licensors. All Rights Reserved.

Product: IMC 5.0 SP1 Platform: Linux 32-bit Operating System: MS24 x86_64

Login

Operator: admin

Password:

Login [Forgot your password?](#)

Fonte: O autor.

Após essa instalação, é preciso efetuar o login para acessar o sistema. Feito isso o IMC irá exibir a página básica Auto Discovery. É possível realizar a descoberta de dispositivos de maneira automática, que é feita por uma varredura em uma determinada faixa de IP, que deve ser definida, ou de maneira individual informando IP por IP.

3.8.5 Protocolo de Acesso aos Equipamentos

O IMC permite que se use os protocolos SNMP, TELNET e SSH utilizando a ideia de modelos predefinidos. A utilização de modelos predefinidos (templates) visa reduzir operações repetidas ao definir os parâmetros.

Na criação destes modelos, é possível definir configurações que se repetirão para o um mesmo tipo de equipamento, como por exemplo switches. Para isso, após a criação do modelo, basta selecionar um modelo SNMP, TELNET ou SSH dentre os pré-definidos.

3.8.6 Criação de Grupo de Dispositivos

O grupo de dispositivos serve para definir funções ou parâmetros para um mesmo tipo de equipamento.

É possível criar um grupo de dispositivos que contenham um mesmo tipo de função, configuração e/ou determinado tipo de monitoramento. Desta forma é possível criar um grupo de dispositivos de switches, que fazem parte da espinha dorsal da rede, onde pode se definir um grupo de portas que serão monitoradas, como exemplo, as portas 25 e 26 que podem ser usadas para interligar os switches entre si.

A criação de grupos de dispositivos torna-se interessante, pois com grupos de equipamentos é possível definir uma equipe, ou um profissional responsável por determinado(s) grupo(s), ou por poder se criar um grupo onde contenham dispositivos críticos à infraestrutura da rede, como switches, roteadores, servidores, entre outros.

3.8.7 Criar Operadores

O administrador pode criar contas de manutenção, isso permitirá que diferentes papéis específicos sejam definidos para administradores de nível mais baixo.

Os “logins” de nível mais baixo só irão visualizar os grupos de dispositivos que se aplicam a esse usuário “logado”.

Uma vez que seu “Grupo de Dispositivos” foi adicionado, há opções para criar mais grupos, adicionar dispositivos ou voltar à lista de grupo de dispositivos. A tela de cadastro de usuário pode ser vista na figura 3.

Figura 3 – Tela para adição de usuários no IMC.

The screenshot displays the 3COM Intelligent Management Center (IMC) interface. At the top, the title bar reads '3COM Intelligent Management Center'. Below it, a navigation bar includes 'My Shortcut', 'Home', 'Resource', 'User', 'Service', 'Alarm', 'Report', and 'System'. The 'User' tab is selected. On the left, a sidebar menu shows 'User Management' with options like 'Add User', 'All Users', 'Supplemental User Information', 'Batch User Operations', and 'Import Users'. Below this is the 'Guest Access Manager' section with options like 'Guest Access Operator', 'Guest Access User Group', 'Guest Access Log', and 'Guest Access System Parameters'. The main area is titled 'Users >> Add User' and contains the 'Add User' form. The form has a 'Basic Information' section with fields for 'User Name', 'Contact Address', 'Email', 'Identity Number', 'Telephone', and 'User Group'. The 'User Group' dropdown is currently set to 'Ungrouped'. At the bottom right of the form are 'OK' and 'Cancel' buttons.

Fonte: O autor.

A criação de grupos é bastante útil quando não se quer dar acesso além das atribuições de um determinado cargo e pode ser usado onde empresas com filiais e diferentes equipes existentes não devem ter acesso à todos os dispositivos, mas necessitem de monitorar um grupo específico que lhe é de responsabilidade.

É possível gerenciar os operadores através da plataforma e especificar direitos de sua gestão. Além da senha, também é possível limitar o acesso do operador através da lista de controle de Login. Ou seja, pode-se limitar o acesso ao sistema apenas com os endereços IP contidos na lista de controle de login.

4 ANÁLISE DAS FERRAMENTAS DO IMC

4.1 CARACTERÍSTICAS DE SOFTWARES DE GERENCIAMENTO

De acordo com Costa (2008) e Lopes, Sauvé, Nicolletti (2003), são características de um bom software monitor de rede:

- O monitoramento de serviços de rede SMTP, POP3, HTTP, entre outros;
- O monitoramento de recursos de servidores como CPU, memória, disco, e processos;
- A capacidade de definir hierarquia da rede;
- As notificações imediatas sobre problemas na rede, via e-mail e pager;
- A capacidade de tomar contramedidas de acordo com o problema na rede;
- Possuir interface web com mapa da rede, relatórios, gráficos e históricos.

Tendo isso como principais características de um software de gerenciamento de rede, será analisada a ferramenta IMC, verificando se seus elementos satisfazem os seguintes requisitos:

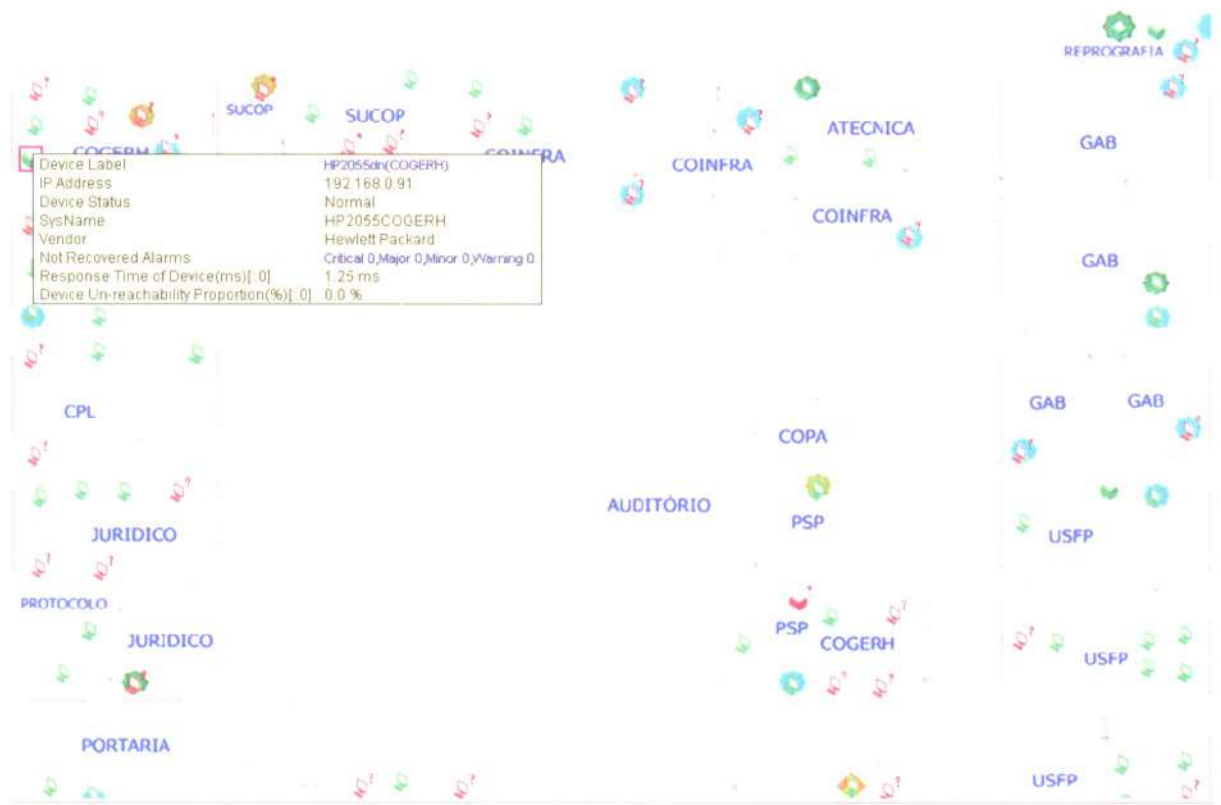
- Monitoramento de todos os componentes de software e hardware da rede através de uma estrutura hierárquica mostrando a topologia da rede;
- Sistemática de notificação dos eventos de alteração do estado da rede;
- Interface amigável que permita visualizar eventos, relatórios, gráficos estatísticos e outras informações de gerência da rede.

4.2 MONITORAMENTO DE COMPONENTES

O monitoramento de componentes se dá logo após a adição do equipamento ou serviço, bastando apenas que o componente possua um endereço lógico (IP) e esteja acessível logicamente ao IMC.

A adição do equipamento ou serviço pode ser realizada de maneira individual, ou de forma automática, passando um faixa de IP, sendo o próprio IMC o encarregado de fazer a adição dos equipamentos que estejam ligados e acessíveis consultando dentro da faixa de endereços informados.

Figura 4 – Tela de visualização dos equipamentos adicionados no IMC.



Fonte: O autor.

O software permite que seja adicionado um plano de fundo na tela da “View”, que pode ser uma planta baixa, tornando possível dispor as máquinas em sua real posição física, o que permite uma localização rápida destas, facilitando a identificação para o administrador.

Ao selecionar algum dispositivo, já possível observar informações pontuais, tais como: nome netbios, IP, status atual, o nome no sistema do equipamento, fabricante, histórico de alertas, tempo de resposta e porcentagem de falhas do dispositivo.

A cor do equipamento é dada de acordo com a última sondagem deste. Se a sondagem apontar um equipamento em normalidade seu status estará ok e ícone que representa o dispositivo assumirá a cor verde. Se após a sondagem o equipamento não responder este receberá um alarme do tipo crítico e assumirá a cor vermelha. Outros tipos de status também são apresentados, é o caso do “Major Alarm” que é o alarme principal, apontado quando o funcionamento do dispositivo não está de acordo com a normalidade.

Em um ambiente experimental simulou uma possível falha de uma impressora de rede, que estava sendo monitorando pelo IMC. Removeu-se o toner do equipamento, o que fez com que o próprio dispositivo enviasse ao IMC uma “TRAP”, informando que seu funcionamento não estava de acordo com o ideal.

Também foi simulada a queda de portas em um “switch” gerenciável. Ao desconectar um cabo, a porta assume o status de “down” e envia ao servidor de monitoramento um alerta crítico.

Para obter esse nível de resposta, é preciso ativar e configurar no equipamento, o protocolo SNMP, onde é preciso substituir, por questões de segurança, as palavras chaves que vem por padrão “public” e “private”. Assim como é necessário configurar no IMC este protocolo.

Sem configurar o SNMP em ambas as pontas só é possível monitorar o estado de resposta, que verifica se a host está respondendo ao “ping” ou não, tendo isso como definição de disponível ou indisponível.

Após configurar o SNMP, o monitoramento passa a ser mais detalhado, o que torna possível o envio das “TRAPs” e checagem de serviços e portas dos equipamentos.

4.2.1 Serviços

A adição de serviços ao monitoramento necessita que o dispositivo onde cada serviço está rodando seja adicionado primeiro. Após sua adição basta acessá-lo na aba “Resource” e adicionar o monitoramento de algum serviço. Para isso basta acessar, na área “Service Monitoring” a opção “Customize”, segundo a Figura 5.

Figura 5 – Página de “Resource” de um equipamento.

The screenshot displays the 'Resource' page for a device named 'SERVIDOR01'. The left sidebar contains navigation options like 'Network Topology View', 'Custom View', 'IP View', 'Device View', 'Resource Management', 'IP Address Management', and 'Network Assets'. The main content area shows a success message at the top: 'Modifying monitor service of device "SERVIDOR01(192.168.0.200)" succeeded.' Below this, the 'Device Details' section lists attributes such as Device Label, Device Status (Normal), sysOID, Mask, Location, Device Model, Hardware Version, Serial Number, and System Description. The 'Service Monitoring' section includes a 'Monitoring Information' table with columns for Service Name, Service Port, Service Type, and Service Status. The table lists UDP services on ports 53, 80, and 87, all with a status of 'Running'. At the bottom, there is a 'Performance Monitor' section with a 'Monitor Index' and 'Monitored Value'.

Service Name	Service Port	Service Type	Service Status
UDP	53		Running
TCP	80		Running
UDP	87		Running

Fonte: O autor.

Nesta customização é possível utilizar um nome de serviço já existente, ou criar um novo nome para o serviço a ser monitorado. O próximo passo é informar qual a porta que o serviço que se deseja monitorar vai utilizar, assim como que tipo de porta UDP ou TCP. Na figura 6 é possível ver como é simples a adição ou alteração do monitoramento dos serviços.

Figura 6 – Página de configuração do monitoramento de portas e serviços.

Select	Service Name	Service Port	Service Type
☐	Telnet	23	TCP
☐	FTP	21	TCP
☐	SMTP	25	TCP
☒	DNS	53	UDP
☒	HTTP	80	TCP
☐	TFTP	69	UDP
☒	DHCP	67	UDP
☐	CustomService_2	65532	TCP
☐	CustomService_3	65533	TCP
☐	CustomService_4	65534	TCP
☐	CustomService_5	65535	TCP

OK Cancel

Fonte: O autor.

O monitoramento é iniciado automaticamente ao clicar no botão salvar. Para desabilitá-lo basta acessar novamente a customização e desmarcar a caixa de texto do serviço que se deseja remover do monitoramento.

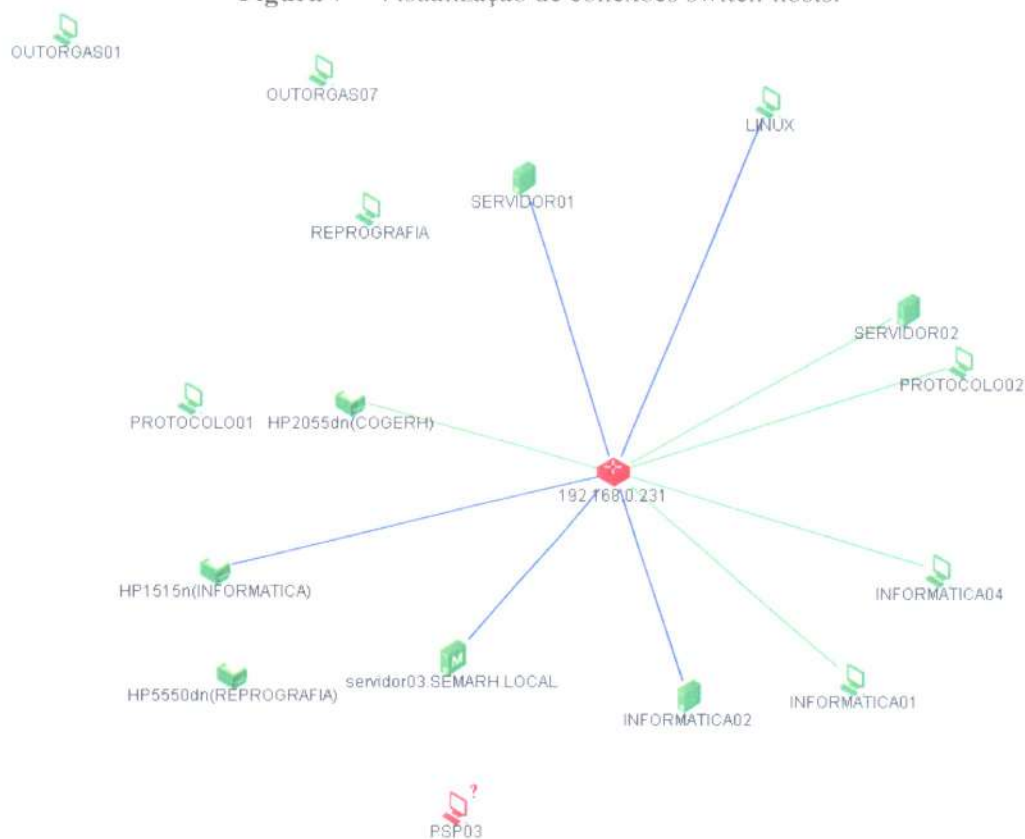
4.2.2 Exibição da Topologia da Rede

A topologia da rede é realizada em “views” que podem ser configuradas de forma flexível, permitindo ao administrador criar quantas visualizações achar necessário e configurar cada uma destas da maneira que for de seu entendimento, podendo exibir todos os serviços, ou os hosts ligados a determinado ativo de rede, ou ainda criar uma “view” com apenas a espinha dorsal da rede. Esta flexibilidade é muito interessante, pois permite que as visualizações sejam feitas por seguimento, serviços, dispositivos, entre outros.

Também é possível criar as conexões entre os dispositivos, mesmo que a conexão não seja detectada pelo IMC, ele apenas alterará a coloração da conexão o que indicará que a conexão foi “forçada” pelo criador da “view”.

Na figura 7 pode-se observar uma “view” criada com o intuito de exemplificar essas conexões reconhecidas e as forçadas, onde as conexões de cor verde são conexões de hosts reconhecidas a partir do switch. A cor de uma conexão forçada é azul, indicando que é uma conexão desconhecida.

Figura 7 – Visualização de conexões switch-hosts.



Fonte: O autor.

Mesmo não reconhecendo a conexão do host pelo caminho indicado, o sistema permite que seja criada, para organizar da maneira desejada a visualização.

Esta flexibilidade torna possível uma abstração maior do funcionamento da rede, tornando o seu entendimento facilitado para quem precisa gerenciar, ou apenas monitorar os dispositivos.

A flexibilidade do software é tanta, que permite, que uma máquina que já foi detectada, mas encontra-se inacessível, possa ser ligada a um equipamento, por uma ligação forçada.

4.3 SISTEMÁTICAS DE NOTIFICAÇÃO DOS EVENTOS E ALTERAÇÕES NA REDE

De todos os recursos oferecidos por este software o que mais chama a atenção é a de notificação, devido à riqueza da estrutura de alarmes que o software dispõe.

As notificações podem ocorrer com a sondagem do IMC ao dispositivo monitorado, ou pode ser enviado pelo próprio dispositivo, quando este apresenta alguma modificação de ser estado. Este envio pelo próprio equipamento ou serviço é realizado através das “TRAP’s” e são classificadas na página de alarmes, de acordo com sua classificação.

Além deste recurso que é padrão aos sistemas de monitoramento ele ainda dispõe de um alarme sonoro, que por padrão vem ativado e informa a quem está realizando o monitoramento o nível do alerta recebido no momento em que ele é detectado.

4.3.1 Classificação dos Alarmes do IMC

A classificação dos alarmes possui um nível de detalhes satisfatório, apresentando o nível, que além de um rótulo que o identifica é representado por uma cor específica, como é mostrado no quadro 2.

Quadro 2 – Níveis de Alarme do IMC

Rótulo	Cor
Info	
Warning	
Minor	
Major	
Critical	

Fonte: O autor.

As cores apresentadas são de acordo com a necessidade de atenção ao alarme, partindo do cinza que é apenas uma informação simples sobre o dispositivo monitorado, até o vermelho que é nível mais crítico do equipamento ou serviço e indica que ele está parado ou que não se tem acesso sobre ele.

Pode-se observar na figura 8, a listagem das mensagens de alarme apresentadas pelo IMC. É possível observar o nível do alerta, a origem, o tipo (por sondagem ou por TRAP), uma breve descrição e a data e hora que o alerta foi gerado.

Figura 8 – Página de alarmes do IMC.

Recover

Delete

Recent 50 not recovered alarms. New 0 not recovered alarms

Refresh It

☐	Level	Alarm Source	Type	Description	Alarm at
☐	Critical	COOHIDR008(192.168.0.3)	IMC	Device COOHIDR008 is not accessible	2011-10-27 12:06:03
☐	Critical	USFP10(192.168.0.111)	IMC	Device USFP10 is not accessible	2011-10-27 12:03:44
☐	Critical	USFP03(192.168.0.75)	IMC	Device USFP03 is not accessible	2011-10-27 12:03:03
☐	Critical	CPL02(192.168.0.28)	IMC	Device CPL02 is not accessible	2011-10-27 12:02:52
☐	Critical	IIIFORMATIC404(192.168.0.45)	IMC	Device IIIFORMATIC404 is not accessible	2011-10-27 12:01:18
☐	Critical	US4003(192.168.0.94)	IMC	Device US4003 is not accessible	2011-10-27 12:00:45
☐	Critical	USFP11(192.168.0.11)	IMC	Device USFP11 is not accessible	2011-10-27 12:00:45
☐	Critical	US4005(192.168.0.4)	IMC	Device US4005 is not accessible	2011-10-27 12:00:38
☐	Major	192.168.0.231(192.168.0.231)	Trap	The interface Ethernet0/4 connecting 192.168.0.231:192.168.0.231 is Cc-Down	2011-10-27 12:00:36
☐	Critical	COGERH03(192.168.0.5)	IMC	Device COGERH03 is not accessible	2011-10-27 11:47:04
☐	Warning	IMC alarm system has received 100 alarms about the event (authentication failure) of device 6(192.168.0.211) from 2011-10-27 08:46:15 to 2011-10-27 11:44:55			2011-10-27 11:44:55
☐	Critical	ATECHN403(192.168.0.72)	IMC	Device ATECHN403 is not accessible	2011-10-27 11:43:08
☐	Critical	CPL03(192.168.0.28)	IMC	Device CPL03 is not accessible	2011-10-27 11:38:30

10

324

1/2

Copyright © 2008 H3C Technologies Co., Ltd. All rights reserved. All Rights Reserved

Fonte: O autor.

4.3.2 Configuração das Notificações

As notificações são contínuas e o volume dificulta a monitoramento de um grupo de dispositivos por exemplo. Isto se dá por que qualquer alteração, da mais simples a mais crítica é notificada sem demora pelo sistema e listado na página de alarmes.

No entanto esta dificuldade pode ser contornada de maneira simples. Para isto basta acessar a página de configuração das notificações e optar entre os três tipos de notificações que o sistema oferece que são por E-mail, por SMS, ou ainda por encaminhamento para outro host. Podemos observar na figura 9 a simplicidade deste processo, onde só é necessário clicar em “add”, na tipo de notificação escolhido e atribuir as informações necessárias.

Figura 9 – Página de configuração dos alarmes do IMC.

Home	Resource	User	Service	Alarm	Report	System	admin	Help	About	Logout
Go Advanced										
Add to My Favorites Help										
Alarm Notification										
Mail Notification										
Add Refresh Configure Mail Server Total Items: 0										
Rule Name	Destination Mail Address	Status	Modify	Copy	Delete					
Message Notification										
Add Refresh Configure SMS Total Items: 0										
Rule Name	Mobile Phone Number	Status	Modify	Copy	Delete					
Alarm Forwarding										
Add Refresh Total Items: 0										
Rule Name	Destination Address/Port	Status	Modify	Copy	Delete					

Fonte: O autor.

Para os alarmes serem enviados por e-mail ou por SMS é necessário possuir um servidor que provenha este(s) serviço(s), já a opção de encaminhamento basta informar o host que deverá receber as notificações informando seu IP e a porta.

A configuração de notificação dos alarmes tem uma flexibilidade total, permitindo que se configure qual o grupo de dispositivos se deseja receber, qual o nível das mensagens, assim como o dia da semana e o horário de cada dia.

Na figura 10 temos o exemplo dos campos a serem configurados para o envio das notificações por e-mail.

Figura 10 – Página de configuração do envio de notificação por e-mail.

The screenshot shows a configuration window for email notifications. It contains the following elements:

- Rule Name:** A text input field.
- Destination Mail Address:** A text input field with 'Add' and 'Delete' buttons to its right.
- Concerned Alarm Levels:** Checkboxes for 'Critical', 'Major', 'Minor', 'Warning', and 'Info'. 'Critical', 'Major', and 'Minor' are checked.
- Concerned Devices:** A dropdown menu currently showing 'All Devices'.
- Concerned Alarms:** A dropdown menu currently showing 'Selected Alarms'.
- Time Range Configuration:** A table with columns for the day of the week, a time range, and a format '(hh:mm to hh:mm)'. All time ranges are set to '00:00-24:00'.
- Buttons:** 'Select' and 'Delete' buttons next to the 'Concerned Alarms' dropdown, and 'OK' and 'Cancel' buttons at the bottom right.

Day	Time Range	Format
Monday	00:00-24:00	(hh:mm to hh:mm)
Tuesday	00:00-24:00	(hh:mm to hh:mm)
Wednesday	00:00-24:00	(hh:mm to hh:mm)
Thursday	00:00-24:00	(hh:mm to hh:mm)
Friday	00:00-24:00	(hh:mm to hh:mm)
Saturday	00:00-24:00	(hh:mm to hh:mm)
Sunday	00:00-24:00	(hh:mm to hh:mm)

Fonte: O autor.

4.4 ANÁLISE DA INTERFACE GRÁFICA

Embora a documentação e material sobre o IMC ainda estejam muito escassos na internet e os disponibilizados por seu fabricante ainda deixem muito a desejar, não se encontrou muitas dificuldades para a instalação e configuração desta ferramenta.

Desde o primeiro acesso ao sistema IMC, ainda na sua instalação, é possível seguir de forma intuitiva a cada passo e instalá-lo sem maiores obstáculos.

A sua facilidade de uso chega a impressionar, pois com alguns cliques e em um único dia foi possível instalar, configurar e já iniciar o monitoramento de toda a rede, ainda que de forma limitada, pois houve a necessidade de se configurar os equipamentos monitorados.

A usabilidade é um atributo de qualidade relacionado à facilidade do uso de algo. Mais especificamente, refere-se à rapidez com que os usuários podem aprender a usar alguma coisa, ou a eficiência deles ao usá-la.

Neste quesito o IMC tem sua interface amigável, dividida em módulos que facilitam sua utilização e acesso a informações sem burocracia. Permitindo que apenas com conhecimentos de gerenciamento e de redes seja possível iniciar o monitoramentos dos dispositivos com a opção de *"auto-discovery"*

Quase 100% do programa é editável ou customizável, o que o torna uma ferramenta muito flexível, capaz de se adaptar a diversas necessidades e situações.

5 CONCLUSÕES

Com a implantação do sistema de Gerenciamento Inteligente de Redes, o IMC, permitiu-se cadastrar todos os equipamentos e serviços que possuem um número de IP (Internet Protocol) e que compõe o Parque de Tecnologia da Informação. Foi possível cadastrar informações dos equipamentos como: tipo, nome, IP e Sistema Operacional de cada equipamento, além de permitir monitorar de forma contínua estes dispositivos, exibindo em tempo real o status de cada um. Este gerenciamento proporcionou uma maior eficiência na solução de problemas e falhas nos componentes da rede. Esta eficiência gerou maior velocidade na atuação dos profissionais responsáveis pela gerência e manutenção da estrutura de informática da SEMARH. Com o sistema de monitoramento, é possível criar e manter um histórico de cada equipamento, sabendo quando apresentou problemas, ou quando foi ligado e desligado por exemplo.

Apesar de não possuir, em quantidade satisfatória, material de referência sobre o software IMC, sua interface intuitiva, permite que sua configuração seja realizada de forma descomplicada. A única dificuldade encontrada durante sua instalação foi a configuração do grupo de Traps, que não foi encontrado na interface do sistema.

Com a configuração realizada, sua operação proporcionou agilidade à gerência dos equipamentos e serviços da rede. Com a exibição do status, em tempo real, de cada equipamento, permitiu à equipe de informática se antecipar aos problemas decorrentes das falhas e erros apresentados pelos dispositivos e serviços que compõe a rede, seja com a manutenção, correção do erro, ou pela substituição do dispositivo, possibilitando uma maior transparência para seus usuários e clientes.

Algumas desvantagens foram encontradas durante a avaliação do IMC, o alto custo é um empecilho na utilização da ferramenta por empresas de pequeno porte; a falta de opções em idiomas é outro fator que não favorece sua instalação, embora o idioma inglês seja uma língua obrigatória, para quem trabalha no ramo da informática; no entanto, a principal desvantagem observada neste software é que o seu funcionamento seja totalmente vinculado à MicroSoft, só funcionando em sistema operacional Windows.

Já as vantagens são inúmeras dentre elas podemos citar como principais a usabilidade de suas telas e ícones, que proporcionam uma operação descomplicada para o usuário; a interoperabilidade que permite a interação do sistema IMC com vários dispositivos de diversos fabricantes, inclusive já trazendo em seu banco os principais produtos existentes no mercado, como impressoras, switches e sistemas operacionais; a simplicidade no

monitoramento, em particular aos alertas sonoros emitidos em tempo real, informando o tipo alerta do sistema; a disponibilização da ferramenta em sua versão completa para testes e análise é outra grande vantagem, pois permite ao administrador usar e testar todo o recurso que este sistema de monitoramento é capaz de realizar, da mais simples função de detectar dispositivos na rede, até o inventário completo deste, incluindo o histórico de ocorrência dos alertas.

Com a utilização da ferramenta IMC no ambiente de produção, durante um curto período de 2 (dois) meses, foi possível despertar em toda a equipe de TI da SEMARH o interesse em se adquirir esta ferramenta de gerência, dado o impacto positivo que esta promoveu, tanto na gerência, como nos serviços de suporte, evitando, em alguns casos, que o usuário chegasse a abrir o chamado, uma vez que a própria ferramenta detectava alterações nos dispositivos, por ela gerenciados.

REFERÊNCIAS

COSTA, Felipe. **Ambiente de Redes Monitorado com Nagios e Cacti**. Rio de Janeiro: Editora Ciência Moderna, 2008.

LOPES, Raquel Vigolvino; SAUVÉ, Jacques Philippe; NICOLLETTI, Pedro Sérgio. **Melhores Práticas para Gerência de Redes de Computadores**. Rio de Janeiro: Editora Campus, 2003.

MELCHIORS, Cristina. **Raciocínio Baseado em Casos Aplicado ao Gerenciamento de Falhas em Redes de Computadores**. 1999. 151 f. Dissertação (mestrado) - Curso de Ciências da Computação, Departamento de Ppgc, Ufrgs, Porto Alegre, 1999.

FREITAS, João Carlos da Silva. **SNMP - SIMPLE NETWORK MANAGEMENT PROTOCOL**. Disponível em: <http://www.gta.ufrj.br/grad/00_1/joao/index.html>. Acesso em: 14 set. 2011.

3COM. **HP Intelligent Management Center Enterprise Software Platform**. Disponível em: <http://h17007.www1.hp.com/us/en/products/network-management/IMC_ES_Platform/?jumpid=reg_R1002_USEN>. Acesso em: 17 set. 2011.

THE INTERNET ENGINEERING TASK FORCE. **Structure and Identification of Management Information for TCP/IP-based Internets**. Disponível em: <<http://www.ietf.org/rfc/rfc1155.txt>>. Acesso em: 18 set. 2011

THE INTERNET ENGINEERING TASK FORCE. **Management Information Base for Network Management of TCP/IP-based internets**. Disponível em: <<http://www.ietf.org/rfc/rfc1156.txt>>. Acesso em: 18 set. 2011

THE INTERNET ENGINEERING TASK FORCE. **A Simple Network Management Protocol (SNMP)**. Disponível em: <<http://www.ietf.org/rfc/rfc1157.txt>>. Acesso em: 19 set. 2011

THE INTERNET ENGINEERING TASK FORCE. **Simple Network Management Protocol (SNMPv2)**. Disponível em: <<http://www.ietf.org/rfc/rfc1157.txt>>. Acesso em: 20 set. 2011

THE INTERNET ENGINEERING TASK FORCE. **An Architecture for Describing SNMP Management Frameworks**. Disponível em: <<http://www.ietf.org/rfc/rfc2571.txt>>. Acesso em: 23 set. 2011

THE INTERNET ENGINEERING TASK FORCE. **A Convention for Defining Traps for use with the SNMP**. Disponível em: <<http://www.ietf.org/rfc/rfc1157.txt>>. Acesso em: 02 out. 2011