

# Uma MIB Dinâmica Baseada em Informações Alternativas de Utilização e Operação de Rede para Gerenciamento de Hosts na Internet Através de Web Services

Daniel G. Costa

Universidade Estadual de Feira de Santana

Departamento de Tecnologia

danielgcosta@ecomp.uefs.br

## Resumo

*A grande quantidade de serviços de comunicação disponibilizados nos últimos anos por redes como a Internet revolucionou a forma como os computadores são utilizados pela sociedade. A complexidade resultante vem demandando soluções robustas e eficientes capazes de minimizar interrupções e falhas em redes de computadores. As soluções atuais de gerenciamento de rede fornecem informações restritas, o que demanda a utilização de ferramentas complementares para obtenção de informações ligadas à operação e utilização das redes. Nesse contexto, foi criada uma base dinâmica de gerenciamento focada em informações de utilização e operação de rede por hosts na Internet, disponibilizando informações não presentes em soluções tradicionais da área. Essa nova base foi projetada para ser acessada através de web services, criando-se assim uma forma rápida e altamente disponível para o gerenciamento de hosts IP.*

## Abstract

*The huge amount of Internet communication services available in the past last years has changed the way IP networks have being used by society. The resulting complexity is demanding efficient solutions able to avoid harm and cease in network operations. Current management solutions provide restrict information, which requires the using of additional tools to monitor network operation details in internet hosts. It was developed a dynamic management base focused on network operation, providing information not presented in traditional solutions of this area. Such new base was designed to be accessed through web services, allowing fast and efficient management of IP hosts.*

## 1. Introdução

Os últimos 30 anos presenciaram o amadurecimento da computação como ferramenta efetiva em diversas áreas do conhecimento. Desde aplicações científicas ao entretenimento digital, os computadores alcançaram papel de destaque na vida contemporânea. Nesse contexto, as redes de computadores surgem como

catalisador das inovações tecnológicas, impulsionando novas possibilidades de comunicação. Serviços como correio eletrônico, navegação web, *chat* e compartilhamento de arquivos já fazem parte da realidade do cotidiano moderno [6].

As redes de computadores são estruturas de comunicação bastante complexas. O grande aumento no número de usuários e da utilização de serviços na Internet vem forçando cada vez mais o desenvolvimento de soluções capazes de manter o nível esperado de operação dessas redes [11].

O controle das redes passa diretamente pela obtenção de informações sobre os elementos que compõem essas estruturas. Com a obtenção das informações, o estado atual de uma determinada rede ou de um conjunto de redes pode ser conhecido dinamicamente. O conhecimento dinâmico do comportamento de uma rede permite que ações sejam tomadas rapidamente para sanar um eventual problema. Essa demanda por um controle especial é atendida, completamente ou em parte, pela grande área de Gerência de Redes.

Tipicamente, o protocolo SNMP (Simple Network Management Protocol) [4] vem sendo utilizado na Internet como solução padrão para suporte ao gerenciamento de redes. Definindo métodos com ações específicas, o SNMP permite que alguns tipos de informações sejam lidos de dispositivos previamente configurados. Além disso, é possível utilizar o SNMP para gerenciamento ativo, alterando informações em hosts e/ou ativos de rede.

Uma parte fundamental para o gerenciamento de redes de computadores e dispositivos refere-se ao conjunto de informações que podem ser acessadas. Informações de gerenciamento são armazenadas em bases de dados chamadas MIB (Management Information Base) [4], que podem ser publicamente padronizadas ou mesmo serem criadas para atender alguma demanda específica.

Verifica-se que muitas informações ligadas diretamente à administração de redes não estão disponíveis em MIB tradicionais, como, por exemplo, informações sobre conexões atualmente ativas, portas abertas e tabela ARP atual. Mesmo novas especificações de MIB não disponibilizam um conjunto abrangente de informações sobre a operação de hosts, estando mais focadas em monitoramento de fluxos e medições de utilização da rede [3][23]. Visando sanar esse problema, propõe-se aqui a utilização de programas de

monitoramento para a disponibilização de informações ligadas a operação das redes de computadores em hosts IP, formando a NMIB (Network MIB). Como os clientes e servidores da Internet estão presentes geralmente na forma de computadores com recursos de processamento disponíveis, soluções adicionais de gerência de redes podem ser facilmente implantadas, de forma diferente como ocorreria em muitos ativos de rede sendo utilizados atualmente. Adicionalmente, foram criados web services para acesso a essas informações, seguindo uma tendência na área de gerência de redes, como apresenta alguns trabalhos [15][22].

De forma diferente como ocorre em alguns trabalhos relacionados [19], focados na especificação de arquiteturas e soluções genéricas para gerenciamento de rede baseado em web services, a NMIB é uma solução pontual, focada no monitoramento do comportamento de hosts em relação às comunicações ativas em redes Internet. Pretende-se que a solução apresentada seja um modelo para a disponibilização de informações não tradicionais de monitoramento de redes, nas extremidades das comunicações.

Esse artigo está organizado da seguinte forma. Na seção 2 são apresentados conceitos e características da área de gerência de redes, incluindo acesso a informações através de web services. O capítulo 3 traz o desenvolvimento da solução, seguido por testes e resultados. Por fim encontram-se as considerações finais e as referências do trabalho.

## 2. Gerência de redes

A gerência de redes é uma área da computação relacionada a diversos aspectos, como segurança, configuração e desempenho. Além do controle dos ativos de rede, como roteadores, switches e modems [21], os hosts que pertencem a uma rede também podem sofrer algum tipo de controle. Nas soluções tradicionais de gerenciamento de redes, pretendem-se obter dos elementos gerenciados informações como o uso de CPU, o uso de memória, o número de pacotes recebidos e o número de erros encontrados em pacotes, apenas para citar alguns exemplos.

Praticamente todos os dispositivos de rede que estão atualmente à venda possuem algum suporte à gerência de rede através de mensagens SNMP. O mesmo é válido para equipamentos que se ligam à Internet, mas que não são dispositivos de comunicação. É o caso, por exemplo, de impressoras, câmeras e scanners.

A arquitetura de gerenciamento de rede baseada no protocolo SNMP utiliza diretamente os serviços do protocolo de transporte UDP (User Datagram Protocol) [17]. Nessa arquitetura, hosts com papel de gerente gerenciam informações em elementos com papel de agente, que tipicamente podem ser dispositivos de rede (roteador, switch, modem, etc.) ou hosts (servidores ou não).

Há duas formas básicas de gerenciamento. Na primeira forma, um cliente (gerente) acessa informações em elementos gerenciados (agentes). Essa forma de

gerenciamento segue estritamente o paradigma cliente/servidor. As aplicações gerentes acessam os elementos gerenciados para obter ou alterar determinada informação. Esse acesso pode ocorrer a qualquer momento, por um número indefinido de vezes, sendo que implementações comuns consideram acessos periódicos aos elementos gerenciados. A segunda forma de gerenciamento é composta pela geração de eventos assíncronos. Por exemplo, um roteador pode notificar assincronamente uma estação gerente sobre uma situação inesperada, como o recebimento de muitos pacotes com endereço de destino inválido. Essa notificação pode ocorrer imediatamente, sem precisar esperar por uma requisição explícita de uma estação gerente.

O conjunto de informações disponíveis para gerenciamento é chamado de MIB, que representa uma base de dados especial com informações disponíveis para gerência remota. Existe uma MIB padrão que todos os hosts gerenciáveis devem implementar. Grande parte dos dispositivos eletrônicos ligados em rede suporta uma versão da MIB conhecida como MIB-2 [13]. Além disso, MIB específicas são utilizadas para atender demandas específicas. Por exemplo, um roteador pode conter informações diferentes das contidas em um switch. É comum também fabricantes desenvolverem MIB específicas para seus equipamentos.

A Tabela 1 apresenta os principais grupos de informações que compõem a MIB-2.

Grupo	Descrição
at	Informações de tradução de endereços.
icmp	Informações sobre o processamento de mensagens do protocolo ICMP (Internet Control Message Protocol) [18].
interfaces	Informações sobre as interfaces de rede.
ip	Informações sobre o processamento de mensagens do protocolo IP (Internet Protocol) [7].
snmp	Informações sobre o processamento de mensagens do protocolo SNMP.
system	Informações básicas do sistema.
tcp	Informações sobre o processamento de mensagens do protocolo TCP (Transmission Control Protocol) [8].
transmission	Informações relacionadas aos meios de transmissão.
udp	Informações sobre o processamento de mensagens do protocolo UDP.

**Tabela 1.** Informações da MIB-2.

Outra forma de realizar operações de gerência de redes é através de web services. Web services é uma tecnologia para comunicação em rede que utiliza o suporte básico da web, o protocolo HTTP (HyperText Transfer Protocol) [10], para transferência de informações. A idéia central é a criação de serviços que podem ser acessados por hosts conectados à Internet a partir de qualquer programa que utilize os padrões de comunicação da web.

Um web service corresponde a um (tipicamente) ou mais serviço de rede da camada de aplicação, sendo independente de plataforma e linguagem de

programação. Para garantir essa característica são utilizados padrões abertos para estruturar as comunicações entre cliente e servidor, que é o modelo de comunicação usado por essa tecnologia.

O que vem fomentando a utilização de web services são as inúmeras possibilidades oferecidas por essa tecnologia, ainda mais quando consideramos a abrangência e alcance da web. Os web services podem prover informações diversas, como, por exemplo, cotações da bolsa de valores, previsão do tempo, dicas de viagens e notícias instantâneas, tudo acessível por qualquer programa, escrito em qualquer linguagem e disponibilizado em qualquer plataforma, desde que sigam corretamente os padrões abertos definidos para essa tecnologia. Nesse contexto, os benefícios da utilização dos web services em gerência de redes vêm colocando essa tecnologia como alternativa mais flexível e muitas vezes mais disponível que arquiteturas e ferramentas baseadas no protocolo SNMP.

### 3. Desenvolvendo a nova MIB

Muitas informações necessárias para o controle e administração de redes não estão presentes nas MIB tradicionais. Essa limitação faz com que, muitas vezes, ferramentas adicionais tenham que ser utilizadas para a obtenção de informações complementares, dificultando tarefas de administração das redes modernas.

Visando sanar esse problema, foi desenvolvida uma base de informações alternativas, denominada Network MIB (NMIB), disponibilizando assim informações não presentes em soluções tradicionais de gerência de redes. Adicionalmente, essa base de informações é especificada para ser acessada por web services, potencializando a disponibilidade e acessibilidade dessas informações.

As subseções seguintes descrevem, respectivamente, a especificação da NMIB e os detalhes de implementação e testes dessa solução.

#### 3.1. Especificação da NMIB

As MIB tradicionais não fornecem todas as informações diretamente relacionadas com a comunicação na Internet. Na MIB-2, por exemplo, as informações disponíveis estão restritas em sua maioria a número de pacotes, como pacotes recebidos e enviados e pacotes com erros. A NMIB surge como uma base de informações mais completa, focada no fornecimento de outras informações de comunicação em rede.

Os hosts IP modernos possuem recursos de processamento que permitem executar todo o tipo de código, salvo algumas restrições impostas por certos tipos de processamento. Nesses dispositivos, programas adicionais podem ser executados com certa facilidade, o que não ocorre em muitos ativos de rede. Dessa forma, foi decidido que a NMIB será implantada inicialmente em hosts da Internet (computadores “convencionais”), que podem ser clientes ou servidores. Versões futuras dessa solução de gerenciamento poderão ser implantadas em ativos de rede, desde que os códigos de

monitoramento esperados para a NMIB possam ser executados nesses dispositivos sem perda significativa dos resultados.

A Tabela 2 apresenta as informações contidas na versão inicial da NMIB. Cada uma dessas informações é acessada por apenas um web service, específico para o monitoramento pretendido. Como pode ser visto, essa não é uma base de informações estruturada de maneira convencional, mas uma descrição de informações que podem ser recuperadas de alguma forma por usuários remotos.

Item	Descrição
Conexões ativas	Informações sobre as conexões atualmente ativas.
Configurações DNS	Descrição sobre as configurações DNS (Domain Name System) [14], que são consideradas em consultas seguindo esse protocolo.
Informações sobre proxy	Configuração de utilização de proxy web.
Log de comunicações	Informações sobre as comunicações já realizadas. O tipo e natureza das comunicações são definidos seguindo parâmetros estabelecidos pelos usuários da NIB.
Log do sistema	Log geral do sistema. Essas informações podem ser utilizadas para descobrir/solucionar incidentes de segurança.
MIB-2	Contém todas as informações da MIB-2, caso sejam necessárias.
Portas abertas	Informações sobre todas as portas atualmente abertas, nos protocolos TCP e UDP.
Tabela ARP	Informações da tabela ARP local.
Tabela de rotas.	Informações sobre a tabela de rotas presente nos hosts.

**Tabela 2.** Informações da NMIB.

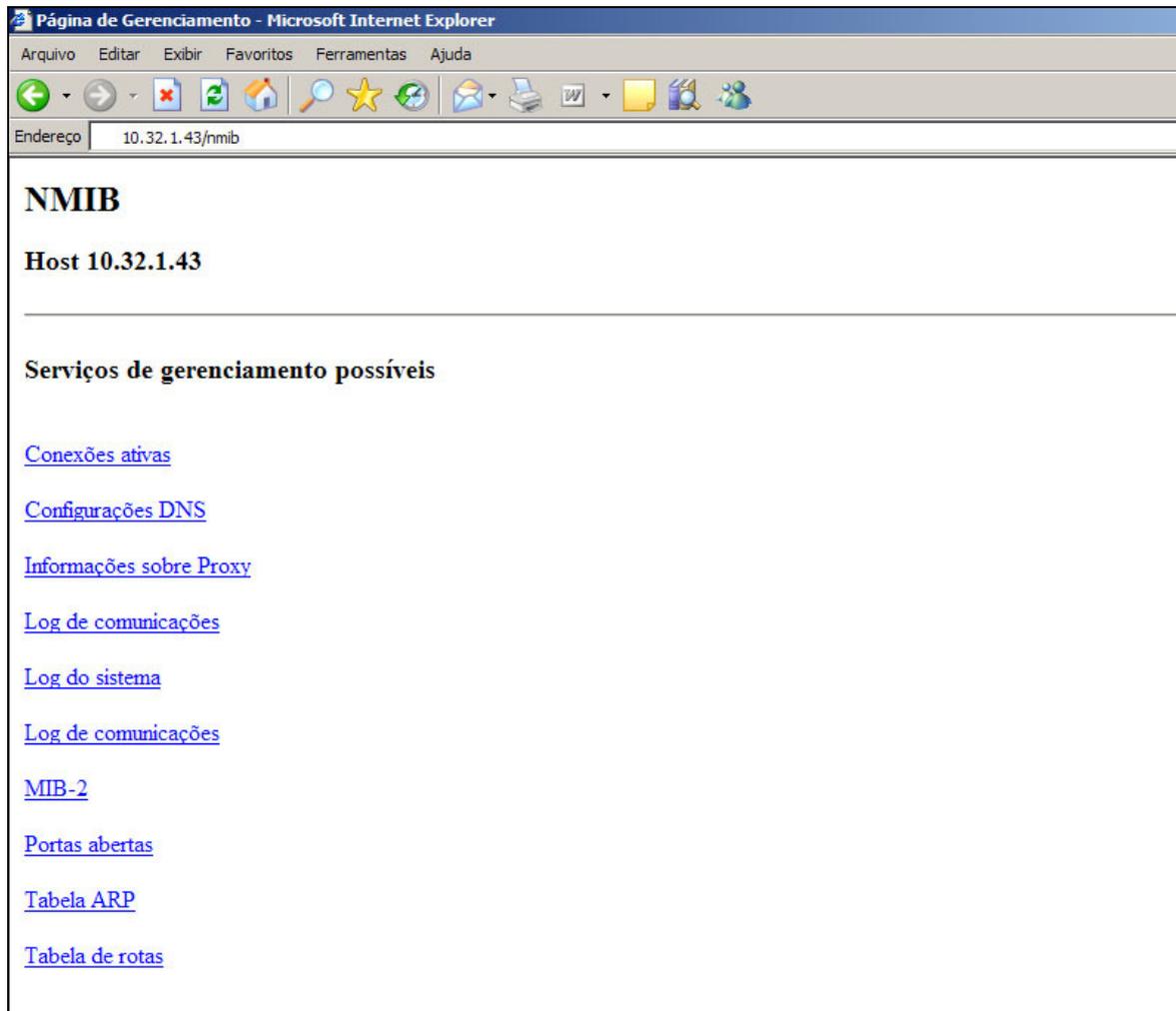
Informações da MIB-2 também estão presentes na NMIB, caso informações dessa MIB sejam necessárias. A idéia é apenas disponibilizar informações da MIB-2 já presentes no elemento gerenciado, caso esteja presente.

Uma informação muito importante presente na NMIB é o log de comunicações. A finalidade dessa informação é apresentar o número de pacotes recebidos e/ou enviados de acordo com algum critério estabelecido pelo usuário. Por exemplo, o usuário pode querer saber quantos pacotes tendo a porta 5060 como origem ou destino foram recebidos até o momento da consulta à NMIB. Mais de uma configuração desse tipo pode estar presente simultaneamente. Seguindo um princípio semelhante, é possível verificar o log do sistema sendo gerenciado, facilitando diversos tipos de análises sobre a situação real dos hosts.

Além da NMIB em si, o serviço de gerenciamento sendo proposto também é formado por uma interface de acesso. Essa interface de acesso às informações de gerenciamento é composta por web services, apontados por uma página html, de forma que cada funcionalidade da NMIB é acessada por um web service

correspondente. Na versão inicial da solução proposta, uma página html simples foi criada, visando apenas apresentar os serviços de gerenciamento possíveis

(através dos web services) e os resultados das consultas. A Figura 1 apresenta essa página de gerenciamento.



**Figura 1.** Página de gerenciamento.

É importante lembrar que essa página de gerenciamento possui apenas links para os web services, não sendo obrigatória para a utilização da solução. De fato, os web services podem ser usados diretamente, individualmente ou não e por uma quantidade indefinida de vezes. Inclusive, podem ser chamados diretamente por códigos remotos, provendo informações de gerenciamento de acordo com a necessidade de cada usuário da solução proposta.

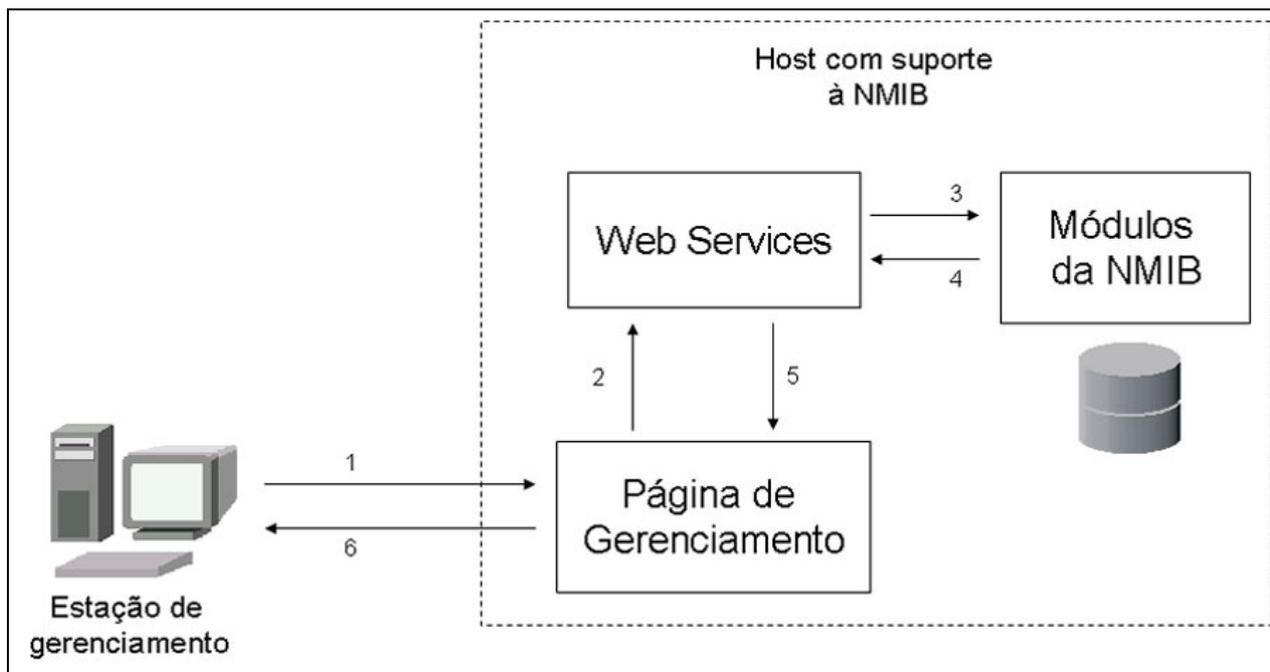
A Figura 2 apresenta o esquema geral de gerenciamento para a solução proposta (considerando a utilização da página apresenta na Figura 1). Nessa figura, o fluxo normal de operação é indicado pelos números de 1 a 6. O número 1 representa um acesso à página de gerenciamento, com a escolha do serviço de monitoramento desejado. O fluxo 2 corresponde à chamada do web service referente ao serviço escolhido. O número 3 indica a chamada do código que está relacionado ao web service, e que será executado diretamente no host gerenciado. O resultado dessa

execução é indicado pelo fluxo 4. Por fim, esse resultado é retornado ao host remoto que solicitou o serviço, como representam os fluxos 5 e 6.

Espera-se que os elementos gerenciados possuam recursos de rede e de processamento suficientes para a execução e disponibilização dos web services e da página de gerenciamento. Além disso, servidores especializados devem ser empregados para disponibilização da página de gerenciamento e dos web services, a exemplo dos servidores Apache [1] e Axis [2].

### 3.2. Implementação, testes e resultados

A implementação da versão inicial da NMIB e dos web services foi feita utilizando a linguagem de programação Java [9], devido, entre outros fatores, a sua portabilidade e a existência de bibliotecas capazes de fornecer um robusto ferramental para o desenvolvimento do trabalho proposto.



**Figura 2.** Esquema geral de gerenciamento da NMIB.

O sistema de gerenciamento é formado por dois módulos: o código gerador das informações dinâmicas, formando a NMIB propriamente dita, e os web services, que acessam as informações desejadas.

Para cada tipo de informação esperada para a NMIB, uma abordagem de implementação diferente foi adotada. Para todos os tipos de verificação, com exceção dos logs de comunicações, as informações são obtidas em tempo real, tão logo o web service faça a solicitação. Assim, o usuário solicita o serviço através do web service que então executa o código que irá recuperar as informações apropriadas diretamente do sistema operacional. Dessa forma, a NMIB não representa uma base de dados pré-montada, mas sim a composição de diversos módulos que, quando solicitados, retornam a informação desejada.

A linguagem Java permite a execução de programas externos e a recuperação das informações geradas por esses programas. Assim, a verificação de todas as informações foi feita acessando programas pré-instalados ou arquivos presentes no sistema operacional do host gerenciado. A exceção do programa nmap [16], utilizado para verificação de portas abertas, todos os outros programas executados já estão disponíveis nos sistemas operacionais modernos: netstat, arp e route [11]. Como há diferenças nos parâmetros desses programas em relação ao sistema operacional, os códigos de monitoramento fazem uma verificação de qual é o sistema operacional corrente, escolhendo assim a forma correta de execução dos programas nativos.

A descoberta das configurações de DNS e proxy ocorre de forma indireta, através da execução de programas nativos ou leitura de arquivos de

configuração, dependendo do sistema operacional considerado. Já o acesso ao log do sistema ocorre verificando informações do log principal, a exemplo do arquivo syslog em sistemas Linux [11].

A verificação das informações referentes aos logs de comunicações representa uma tarefa mais complexa que os outros testes. Na versão inicial da NMIB, apenas módulos para Linux foram disponibilizados. Isso se deve ao fato de que versões para Linux do programa iptables [12] foram utilizadas para geração das informações de logs. Quando o usuário configura, através dos web services, um parâmetro para o armazenamento de logs, uma funcionalidade do programa iptables é executada. Essa funcionalidade especifica um parâmetro para log, a exemplo de “iptables -A INPUT -p tcp --destination-port 80 -j LOG --log-prefix ‘Parametro 1’”, que armazena na forma de logs pacotes destinados à porta TCP 80.

Para disponibilizar as informações da MIB-2, a biblioteca SNMP4J [20] foi utilizada. Para esse módulo de verificação, opções pré-definidas de monitoramento auxiliam a verificação rápida de informações importantes e comumente consultadas da MIB-2. As informações pré-definidas foram estabelecidas como: Descrição do sistema, Tempo em que o sistema está ligado, Número de interfaces de rede, Número de pacotes recebidos, Número de datagramas UDP recebidos e Número de datagramas TCP recebidos. Adicionalmente, o usuário pode especificar uma OID (Object Identifier) [4] referente a qualquer informação presente na MIB tradicional.

Os web services foram implementados também utilizando os recursos da linguagem Java. Para execução, foi utilizado nessa versão inicial o servidor

Axis [2]. As interfaces foram feitas de forma simples, de modo apenas a permitir a coleta das informações desejadas. Para a consulta às informações da MIB-2 e a verificação dos logs de comunicações, entretanto, a interface permitia também que os usuários passassem parâmetros de configuração ou consulta.

Após a implementação da NMIB, diversos testes foram executados. O objetivo dos testes foi tanto verificar a ausência de erros de programação quanto a adequação da solução em relação a seus requisitos iniciais. A análise inicial da execução desses testes em diferentes plataformas mostrou que a solução desenvolvida está corretamente implementada e atende

a seus requisitos. Ainda é esperada a execução experimental da solução em hosts IP para a verificação de eficiência da solução em relação às outras ferramentas de gerência e administração de redes, mesmo que essa comparação ocorra entre a NMIB e a execução conjunta de ferramentas distintas.

Um resultado típico de verificação de portas TCP abertas é apresentado na Figura 3. Esse resultado é obtido diretamente de um web service. Nesse exemplo, está sendo apresentado apenas o resultado do acesso ao web service, que pode ou não ser exibido em uma página web. Já a Figura 4 apresenta um resultado típico de monitoramento de conexões ativas.

PORT	STATE	SERVICE
22/tcp	open	ssh
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
389/tcp	open	ldap
953/tcp	open	rndc
3306/tcp	open	mysql
5001/tcp	open	complex-link
8009/tcp	open	ajp13
8080/tcp	open	http-proxy

**Figura 3.** Exemplo de verificação de portas TCP abertas.

Proto	Endereço local	Endereço externo	Estado
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	10.32.1.43:139	0.0.0.0:0	LISTENING
TCP	10.32.1.43:1858	10.65.16.2:3128	TIME_WAIT
TCP	10.32.1.43:1862	10.65.16.2:3128	TIME_WAIT
TCP	10.32.1.43:1866	10.65.16.2:3128	TIME_WAIT
TCP	10.32.1.43:1872	10.65.16.2:3128	ESTABLISHED
TCP	10.32.1.43:1877	10.65.16.2:3128	ESTABLISHED
TCP	10.32.1.43:1878	10.65.16.2:3128	ESTABLISHED
TCP	10.32.1.43:1882	10.65.16.2:3128	ESTABLISHED
TCP	10.32.1.43:1884	10.65.16.2:3128	ESTABLISHED
TCP	10.32.1.43:1886	10.65.16.2:3128	ESTABLISHED
UDP	0.0.0.0:445	*:*	
UDP	0.0.0.0:500	*:*	
UDP	0.0.0.0:1057	*:*	
UDP	0.0.0.0:4500	*:*	
UDP	10.32.1.43:123	*:*	
UDP	10.32.1.43:137	*:*	
UDP	10.32.1.43:138	*:*	
UDP	10.32.1.43:1900	*:*	
UDP	127.0.0.1:123	*:*	
UDP	127.0.0.1:1900	*:*	

**Figura 4.** Exemplo de verificação de conexões ativas.

#### 4. Considerações finais

A complexidade das redes de computadores é um fator constante nos ambientes computacionais modernos. A proliferação de serviços de rede e o aumento do número de usuários estão ligados diretamente a esse fator. Essa complexidade pode gerar

uma maior possibilidade de falhas ou erros, necessitando atenção especial para que os serviços continuem funcionando normalmente. A instabilidade na comunicação, gerada pelos potenciais problemas existentes em redes de computadores, revela um cenário propício para a prática de soluções inovadoras de gerência de redes.

A NMIB é uma forma alternativa de disponibilização dinâmica de informações não tradicionais de gerenciamento de redes através de web services. Soluções convencionais da área não possuem a flexibilidade e disponibilidade dos web services, nem disponibilizam todas as informações presentes na NMIB.

Os testes iniciais da solução de gerenciamento revelaram a adequação da NMIB em relação aos seus requisitos iniciais. Contudo, novos testes estarão relacionados com verificações de eficiência, tanto no processo de gerenciamento quanto na execução da solução em hosts. Os resultados desses testes serão comparados com a execução de ferramentas que, separadamente, fornecem apenas parte das informações de monitoramento disponibilizadas pela solução proposta. Pretende-se assim tornar a solução completamente apta a ser utilizada em cenários reais de gerência e administração de redes, embora esteja totalmente funcional para cenários experimentais.

O desenvolvimento da NMIB foi efetuado com a implementação de módulos independentes, que podem ser adicionados ou retirados da solução final com certa facilidade. Isso permite que novas funcionalidades sejam inseridas, atendendo outros requisitos de monitoramento. Nesse contexto, trabalhos futuros estarão relacionados com a ampliação das funcionalidades da NMIB, como a adição de novos recursos de monitoramento e o armazenamento local de arquivos de log na forma de arquivos. Além disso, pretende-se ampliar as possibilidades de utilização das funcionalidades já presentes, adicionando novos tipos de informações. Características ligadas à segurança de redes [5], como certificados de segurança, também estarão disponíveis em novas versões da NMIB.

## 5. Referências

- [1] Apache. “The Apache HTTP Server Project”. Disponível em: <<http://httpd.apache.org/>>. 2009.
- [2] Axis. “Apache Web Services Project”. Disponível em: <<http://ws.apache.org/axis/>>. 2009.
- [3] Brownlee, N. “RFC 2720: Traffic Flow Measurement: Meter MIB”. Disponível em: <<http://www.ietf.org/rfc/rfc2720.html>>. 1999.
- [4] Case, J. et al. “RFC 1157: A Simple Network Management Protocol”. Disponível em: <<http://www.ietf.org/rfc/rfc1157.txt>>. 1990.
- [5] Cheswick, W. R. et al. *Firewalls e Segurança na Internet*. 2ª ed. Porto Alegre: Ed Bookman. 2005.
- [6] Comer, D. E. *Interligação em Redes com TCP/IP*, vol. 1. 2ª ed. Rio de Janeiro. Campus. 1998.
- [7] DARPA. “RFC 791: Internet Protocol”. Disponível em: <<http://www.ietf.org/rfc/rfc791.txt>>. 1981.
- [8] DARPA. “RFC 793: Transmission Control Protocol”. Disponível em: <<http://www.ietf.org/rfc/rfc793.txt>>. 1981.
- [9] Deitel, P. J.; Deitel, H. M. “Java: Como Programar”. 6ª ed. Prentice-Hall. 2005.
- [10] Fielding, R. et al. “RFC 2616: Hypertext Transfer Protocol – HTTP/1.1”. Disponível em: <<http://www.ietf.org/rfc/rfc2616.txt>>. 1999.
- [11] Hunt, C. *TCP/IP Network Administration*. 3ª ed. O’reilly. 2002.
- [12] Iptables. “Netfilter/iptables project homepage”. Disponível em: <<http://www.netfilter.org/>>. 2009.
- [13] McCloghrie, K., Rose, M. “RFC 1213: Management Information Base for Network Management of TCP/IP-based internets: MIB-II”. Disponível em: <<http://www.ietf.org/rfc/rfc1213.txt>>. 1991.
- [14] Mockapetris, P. “RFC 1034: Domain Names – Concepts and Facilities”. Disponível em: <<http://www.ietf.org/rfc/rfc1034.txt>>. 1987.
- [15] Moreira, G. M. et al. On the Performance of Web Services Management Standards for Network Management - An Evaluation of MUWS and WS-Management. *Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management (IM 2007)*. Munich, Germany. 2007.
- [16] NMAP. “Free Security Scanner for Network Exploration and Security Audits”. Disponível em: <<http://nmap.org/>>. 2009.
- [17] Postel, J. “RFC 768: User Datagram Protocol”. Disponível em: <<http://www.ietf.org/rfc/rfc768.txt>>. 1980.
- [18] Postel, J. “RFC 792: Internet Control Message Protocol”. Disponível em: <<http://www.ietf.org/rfc/rfc792.txt>>. 1981.
- [19] Soldatos, J. et al. Web Services-based Network Management: Approaches and the WSNET System. *International Journal of Network Management*, V. 17, N. 1. 2007.
- [20] SNMP4J. “The Object Oriented SNMP API for Java Managers and Agents”. Disponível em: <<http://www.snmp4j.org/>>. 2009.
- [21] Tanenbaum, A. S. *Redes de Computadores*. 4ª ed. Campus. 2003.
- [22] Vianna, R. L. et al. Evaluating the Performance of Web Services Composition for Network Management. *Proceedings of the 2007 IEEE International Conference on Communications (ICC 2007)*. Glasgow, Scotland. 2007.
- [23] Waldbusser, S. “RFC 3729: Application Performance Measurement MIB”. Disponível em: <<http://www.ietf.org/rfc/rfc3729.html>>. 2004.