UNIVERSIDADE REGIONAL DE BLUMENAU

CENTRO DE CIÊNCIAS EXATAS E NATURAIS

CURSO DE SISTEMAS DE INFORMAÇÃO – BACHARELADO

MONITORAMENTO DE SERVIDORES E DISPOSITIVOS DE REDE UTILIZANDO SNMP

LUCIANO LINGNAU

BLUMENAU
2012

2012/2-19

LUCIANO LINGNAU

MONITORAMENTO DE SERVIDORES E DISPOSITIVOS DE REDE UTILIZANDO SNMP

Trabalho de Conclusão de Curso submetido à Universidade Regional de Blumenau para a obtenção dos créditos na disciplina Trabalho de Conclusão de Curso II do curso de Sistemas de Informação— Bacharelado.

Prof. Francisco Adell Péricas, Mestre - Orientador

BLUMENAU
2012

2012/2-19

MONITORAMENTO DE SERVIDORES E DISPOSITIVOS DE REDE UTILIZANDO SNMP

Por

LUCIANO LINGNAU

Trabalho aprovado para obtenção dos créditos na disciplina de Trabalho de Conclusão de Curso II, pela banca examinadora formada por:

Presidente:	Prof. Francisco Adell Péricas, Mestre – Orientador, FURB
Membro:	Prof. Everaldo Arthur Grahl, Mestre – FURB
Membro:	Prof. Wilson Pedro Carli, Mestre – FURB

Blumenau, 30 de novembro de 2012.

AGRADECIMENTOS

À minha namorada Caroline que mesmo distante sempre esteve presente.

À minha família que sempre esteve presente e principalmente à meu irmão Sergio que eu considero um guru do PHP e tanto me ajudou no desenvolvimento deste trabalho.

Ao meu orientador, Francisco Adell Péricas, por ter acreditado na conclusão deste trabalho.

I don't know why we are here, but I'm pretty sure that it is not in order to enjoy ourselves.

Ludwig Wittgenstein

RESUMO

À medida que as redes de computadores ficam maiores e mais complexas, fica evidente a necessidade de ferramentas padronizadas para gerência e monitoramento da sua infraestrutura. Este trabalho retrata o desenvolvimento de um sistema de monitoramento desenvolvido em PHP/MySQL que utiliza consultas SNMP para monitorar dispositivos de rede, além de gerar gráficos e alertas dos dados coletados.

Palavras-chave: Monitoramento de rede. SNMP. NMS.

ABSTRACT

As computer networks become bigger and more complex, it becomes obvious that a standard network management and monitoring tools are needed. This work presents the development of a network monitoring system developed using PHP/MySQL using SNMP queries to monitor network devices, also generating graphics and alerts with the acquired data.

Key-words: Network Monitoring. SNMP. Network Management System.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

IAB - *Internet Architecture Board*

IANA - *Internet Assigned Numbers Autorithy*

ICMP - *Internet Control Message Protocol*

IETF - *Internet Engineering Task Force*

ISO - International Organization for Standardization

LAN - *Local Area Network*

MIB - *Management Information Base*

OID - *Object Identifier*

PING - *Packet Internet Groper*

PDU - *Protocol Data Units*

RFC - *Request for Comments*

SNMP - *Simple Network Management Protocol*

TCP/IP - *Transmission Control Protocol over Internet Protocol*

UDP - *User Datagram Protocol*

WAN - *Wide Area Network*

SUMÁRIO

1 INTRODUÇÃO

A medida que as redes de computadores tornam-se maiores, mais complexas e mais heterogêneas, o custo do gerenciamento dessas redes aumenta. Para tentar controlar esses custos são necessárias ferramentas de gerenciamento que possam interoperar com qualquer tipo de dispositivo *Transmission Control Protocol over Internet Protocol* (TCP/IP) (STALLINGS, 1999, p. 1).

Existe uma série de considerações a serem levadas em conta quando se fala em monitoramento dos equipamentos de rede e dos dispositivos conectados a ela:

a) um defeito em um único dispositivo de rede pode tornar uma série de serviços providos por essa rede indisponíveis;
b) acompanhar o dimensionamento de enlaces *Wide Area Network* (WAN) ou *Local Area Network* (LAN) para ter certeza de que não existe largura de banda contratada que não está sendo utilizada ou que a largura disponível é insuficiente;
c) reduzir o tempo de resposta em caso de incidentes;
d) observar padrões de uso para identificar anomalias.

É importante também lembrar que o monitoramento deve ocorrer de forma a não comprometer o bom funcionamento e desempenho da rede, pois segundo Albuquerque (1998, p. 232), "Os sistemas usados na gerência de redes procuram prestar os serviços sem sobrecarregar as entidades gerenciadas ou os canais de comunicação."

Apesar de haver uma grande ênfase em monitorar dispositivos de interconexão de redes como roteadores e *switches*, ele pode ser utilizado também para gerenciar serviços e utilização de servidores que realizam as mais diversas tarefas, facilitando o monitoramento e como consequência o gerenciamento destes equipamentos.

1.1 OBJETIVOS DO TRABALHO

O objetivo deste trabalho é o desenvolvimento de um sistema de monitoramento de servidores e dispositivos de rede independentemente do fabricante, capaz de coletar dados de desempenho de dispositivos de rede TCP/IP interoperando com equipamentos de qualquer fabricante que siga as especificações do protocolo *Simple Network Management Protocol*

(SNMP). Além de coletar esses dados o sistema também deve ser capaz de gerar gráficos a partir dos valores coletados, confidenciar os dados coletados dentro de um *website* com acesso restrito por usuário e senha e enviar alertas por correio eletrônico aos operadores responsáveis caso algum dispositivo monitorado apresentasse uma leitura fora do comum.

Os objetivos específicos do trabalho são:

a) coletar dados de desempenho de dispositivos de rede;
b) criar representações gráficas dos dados coletados;
c) gerenciar o acesso e permissões de operadores ao sistema que disponibiliza essas informações;
d) gerar alertas de correio eletrônico quando houverem leituras que forem definidas como anormais pelo operador.

1.2 ESTRUTURA DO TRABALHO

No primeiro capítulo tem-se a introdução ao tema principal deste trabalho com a apresentação da justificativa e dos objetivos.

No segundo capítulo apresenta-se a fundamentação teórica pesquisada sobre Gerenciamento de Redes e SNMP além de trabalhos correlatos.

O terceiro capítulo apresenta o desenvolvimento do sistema iniciando-se com o levantamento de informações, tendo na seqüência a especificação, implementação e por fim resultados e discussão.

No quarto capítulo tem-se as conclusões deste trabalho com sugestões para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo aborda assuntos a serem apresentados nas seções a seguir, tais como Gerenciamento de Rede, SNMP, além de trabalhos correlatos.

2.1 GERENCIAMENTO DE REDES TCP/IP

"As redes prestam serviços fundamentais na maioria das organizações. As atividades de algumas dessas organizações se tornam inviáveis se os serviços prestados pela rede não estiverem disponíveis ou se forem prestados com tempos de resposta acima de determinados limites. À medida que as redes locais crescem e se interligam com redes de outras organizações, torna-se necessária a utilização de sistemas que facilitem a sua gerência" (ALBUQUERQUE, 1998, p. 231).

As grandes redes da atualidade são de complexidade tamanha que não podem mais ser gerenciadas unicamente pelo esforço humano, é necessária a implantação de ferramentas automatizadas de gerenciamento para lidar com a diversidade de modelos e fabricantes de equipamentos além da dispersão geográfica dos equipamentos utilizados pelas empresas (STALLINGS, 2005).

Para facilitar o gerenciamento de redes ele foi dividido pela *International Organization for Standardization* (ISO) em 5 áreas, resultando no modelo *Fault, Configuration, Accounting, Performance, Security* (FCAPS). Vale ressaltar que segundo Albuquerque (1998, p. 233) "A maioria dos sistemas de gerência não abrange todas as áreas".

2.1.1 Gerenciamento de falhas

O gerenciamento de falhas consiste em monitorar os equipamentos de uma rede e o funcionamento da rede como um todo para identificar falhas. Uma vez identificada uma falha é preciso identificar onde está o problema, tentar minimizar o impacto da falha até que ocorra uma solução definitiva e por fim reparar o substituir o equipamento falho (STALLINGS, 1999).

2.1.2 Gerenciamento de contabilidade

Consiste em monitorar o uso dos equipamentos de rede pelos usuários individuais ou grupos de usuários para permitir a divisão desse custo pelos centros de custo da empresa. Mesmo em casos onde não existe rateio da utilização dos equipamentos o gerenciamento de contabilidade ainda é uma área funcional do gerenciamento de redes pois permite identificar abuso de utilização por determinados usuários que podem estar atrapalhando outros usuários, além de poder instruir os usuários sobre como fazer seu trabalho com menor consumo de recursos da rede e até planejar o crescimento futuro da rede (STALLINGS, 1999).

2.1.3 Gerenciamento de configuração

Permite ao administrador de uma rede conhecer os dispositivos atuais da sua rede, além de consultar ou alterar suas configurações desses dispositivos gerenciados (KUROSE, 2005). A gerência de configuração é utilizada para automação de configuração de grandes quantidades de equipamento e para identificar alterações em parques de computadores, por exemplo a remoção de um disco rídigo ou de redução da quantidade de memória.

2.1.4 Gerenciamento de desempenho

O funcionamento normal e eficaz dos equipamentos ligados a uma rede está diretamente ligado ao desempenho dessa rede. Ao monitorar o desempenho é possível estabelecer métricas para então conseguir identificar se a rede está operando normalmente ou se existe algum gargalo. Se houver algum gargalo, ele precisa ser identificado e corrigido (STALLINGS, 1999).

2.1.5 Gerenciamento de segurança

O gerenciamento de segurança está ligado diretamente à geração, distribuição e armazenamento de chaves de criptografia, além do monitoramento e controle de acesso às redes de computadores e informações de gerenciamento desta rede. Está diretamente ligada a coleta, exame e registro de *logs* de segurança e registros de auditoria.

2.2 SNMP

No princípio do desenvolvimento do padrão *Transmission Control Protocol over Internet Protocol* (TCP/IP), não foi investido muito esforço na elaboração de um protocolo destinado ao gerenciamento de redes, e por isso cada fabricante desenvolvia sua solução. Até o final dos anos 70 a maior ferramenta para gerenciamento e diagnóstico era o *Internet Control Message Protocol* (ICMP), através do comando *Packet InterNet Gopher* (PING) (STALLINGS, 1999).

O ICMP atendeu as necessidades de monitoramento durante vários anos, mas em determinado momento quando a quantidade de redes e sub-redes atingiu a marca das milhares, uma solução mais elaborada foi necessária. Criou-se então o *Simple Gateway Monitoring Protocol* (SGMP) que permitia basicamente o monitoramento de roteadores.

Essa solução também atendeu as necessidades de monitoramento/gerenciamento por um determinado tempo, mas o crescimento das redes e da complexidade dessas redes era exponencial.

Foram levantadas três soluções para esse problema:

a) *High-Level Entity Management System* (HEMS);
b) *Simple Network Management Protocol* (SNMP);
c) *Common Management Information Protocol* (CMIP) sobre TCP/IP (chamado de CMOT).

Em 1988 o Conselho de Arquitetura da Internet (IAB) analisou essas soluções e aprovou o desenvolvimento do SNMP como solução de curto prazo e CMOT como solução de longo prazo (STALLINGS, 1999).

Em 1990 foi publicado pela *Internet Engineering Task Force* (IETF) um documento intitulado RFC1157 que descreve um protocolo simples pelo qual informação de

gerenciamento para um elemento da rede pode ser inspecionada ou alterada por usuários lógicos remotos (INTERNET ENGINEERING TASK FORCE, 1990).

O SNMP não é apenas um protocolo, ele define uma série de características necessárias para que ele possa ser utilizado na prática (KOZIEROK, 2005).

Existem três versões do Protocolo SNMP conforme visto no Quadro 1.

Versão	**Descrição**	**RFC**
SNMPv1	Versão inicial do SNMP.	RFC 1155, RFC 1157
SNMPv2	Versão aprimorada do SNMP, que inclui operações adicionais no protocolo.	RFC 1441, RFC 1452
SNMPv3	Terceira versão do SNMP, que implementa configuração remota e mecanismos de segurança.	RFC 2570

Fonte: Péricas (2010).

Quadro 1 - Versões do SNMP

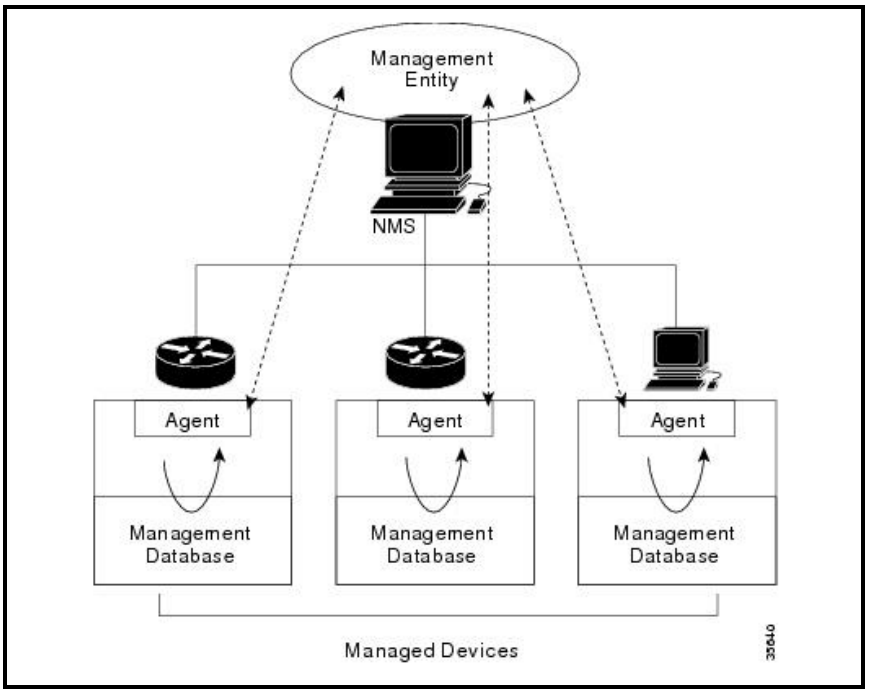
2.2.1 Arquitetura do SNMP

Os três componentes chave da arquitetura do SNMP são os seguintes:

a) dispositivos gerenciados;
b) agente;
c) *Network Management System* (*NMS*).

A utilização mais comum do SNMP é em um modo comando-resposta, no qual a entidade gerenciadora ou *NMS* envia uma requisição a um agente em execução num dispositivo gerenciado, que a recebe, realiza alguma ação e envia uma resposta à requisição. (KUROSE, 2005)

A interação dos componentes descritos acima pode ser observada na Figura 1 (CISCO, 2000).



Fonte: Cisco (2000).

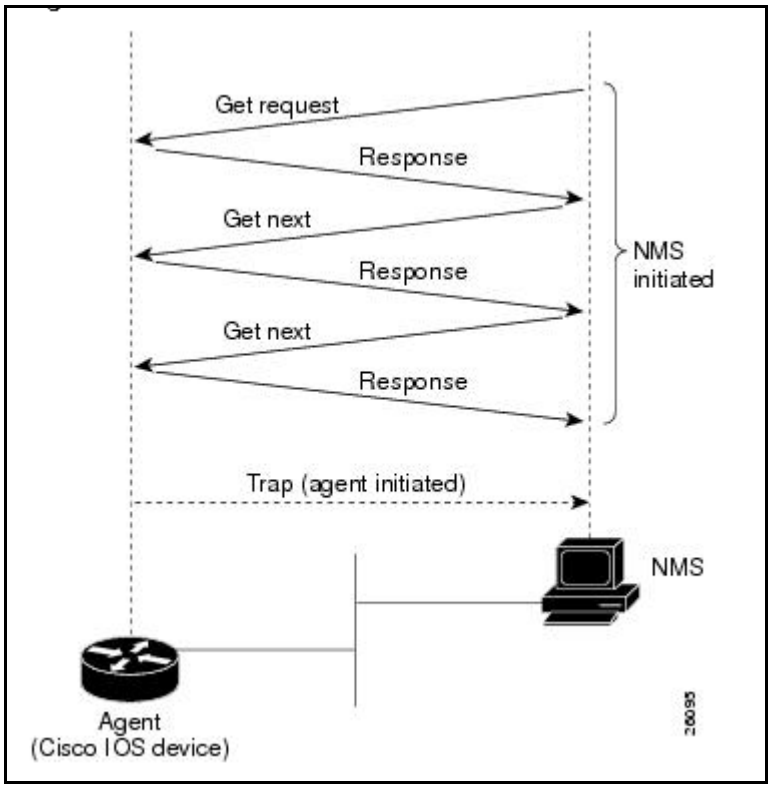
Figura 1 - Interação NMS/Agente SNMP

O NMS ou estação de gerenciamento como também pode ser chamado pode ser tanto um dispositivo exclusivo para este fim ou ser executado em um sistema compartilhado, ele pode ser descrito como (STALLINGS, 2005, p.414) "A interface entre o gerente de rede humano e o sistema de gerenciamento de rede". Os componentes mínimos exigidos pela arquitetura do SNMP para a estação de Gerenciamento são:

a) atender a necessidade de monitoramento de dispositivos remotos do administrador de redes;
b) manter um banco de dados das informações coletadas dos dispositivos gerenciados por esta estação (STALLINGS, 2005).

O dispositivo gerenciado por sua vez é um equipamento de rede e seu software, ele pode ser um computador, um roteador, uma ponte, um hub, uma impressora ou um modem (KUROSE, 2005).

O dispositivo gerenciado executa um software chamado Agente ou Agente de Gerenciamento (STALLINGS, 2005, p. 414). "O agente responde as requisições de informações a partir de uma estação de gerenciamento e pode de vez em quando, fornecer à estação de gerenciamento informações importantes mas não solicitadas". Estas informações importantes não solicitadas são chamadas de *traps*. Na Figura 2 é ilustrada a comunicação entre o gerente e o agente.



Fonte: Cisco (2000).

Figura 2 - Comunicação entre Gerente (NMS) e agente

2.2.2 Comunicação/Protocolo SNMP

A comunicação entre o gerente e agente do SNMP utiliza sete tipos de mensagens, conhecidas também como *Protocol Data Unit* (*PDU*). A lista de PDU's pode se conferida no Quadro 2.

Tipo de PDU	Remetente-Receptor	Descrição
GetRequest	gerente a agente	pega o valor de uma ou mais instâncias de objetos MIB
GetNextRequest	gerente a agente	pega o valor da próxima instância de objeto MIB na lista ou tabela
GetBulkRequest	gerente a agente	pega valores em grandes blocos de dados, por exemplo, valores em uma grande tabela
InformRequest	gerente a gerente	informa à entidade gerenciadora remota da MIB que são remotos para seu acesso
SetRequest	gerente a agente	define valores de uma ou mais instâncias de objetos MIB
Response	agente a gerente ou gerente a gerente	gerada em resposta aos itens acima
Trap	agente a gerente	informa ao gerente um evento excepcional

Fonte: Kurose (2005).

Quadro 2 - Tipos de PDUs (SNMPv2)

Quando um agente em execução num dispositivo gerenciado recebe um comando (Ex.: GetRequest ou SetRequest) isso requer uma interação com os parâmetros do dispositivo gerenciado, seja ela uma leitura de dados atuais ou a gravação de novos valores para uma variável. Essas alterações e consultas são feitas por intermédio da *Management Information Base* (MIB).

> [...] a Base de Informações de Gerenciamento pode ser imaginada como um banco virtual de informações que guarda objetos gerenciados cujos valores, coletivamente, refletem o 'estado' atual da rede. Esses valores podem ser consultados e/ou definidos por uma entidade gerenciadora por meio do envio de mensagens SNMP ao agente que está rodando em um dispositivo gerenciado em nome da entidade gerenciadora. (KUROSE 2005, p. 582).

Embora as PDU's possam ser transportadas por uma diversidade de protocolos de transporte eles normalmente são transportados utilizando datagramas do tipo *User Datagram Protocol* (UDP), isto porque segundo a RFC 1906 o UDP é descrito como "mapeamento de transporte preferencial". Como o UDP não é um protocolo de transporte confiável, não existe garantia de que um comando ou a resposta a esse comando seja entregue no destino, uma das soluções adotadas pelos software NMS é utilizar o campo *Request id* do PDU para enumerar as mensagens enviadas, podendo assim identificar mensagens que foram perdidas. A entidade gerenciadora pode então decidir re-transmitir uma mensagem ou enviar uma nova mensagem se não for recebida uma resposta em tempo hábil. O padrão SNMP não define nenhum

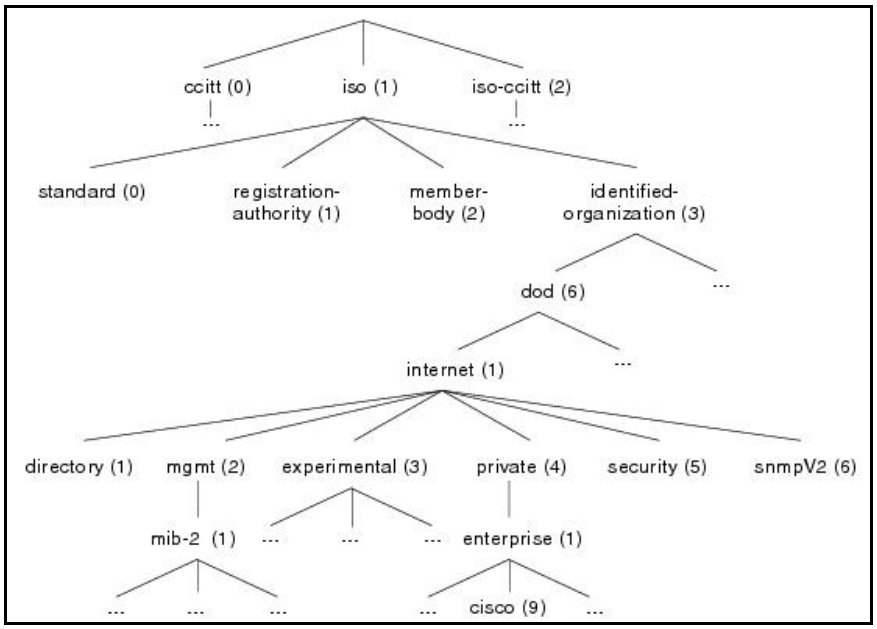
procedimento em relação a retransmissão, o protocolo define apenas que se deve agir responsavelmente em relação a freqüência e duração das retransmissões (KUROSE, 2005).

A comunicação do gerente com o agente é feita na porta 161, as traps geradas pelo agente são enviadas ao gerente na porta 162 (ALBUQUERQUE, 1998).

2.2.3 Base de Informações de Gerenciamento

A MIB é uma estrutura de dados organizada como uma árvore, ela deriva de uma estrutura padronizada de identificação de objetos publicada anteriormente pela ISO. A estrutura que foi adotada é parte da linguagem de definição de objetos ANS.1 (KUROSE, 2005)

A MIB é composta basicamente de Objetos Gerenciados e Identificadores de objetos. Os objetos gerenciados são as características de um dispositivo que podem ser lidas ou alteradas e os Identificadores (conhecidos como OID) identificam a posição desse objeto gerenciado dentro da hierarquia da MIB. A estrutura dessa árvore de dados é padronizada conforme pode ser conferido na Figura 3.



Fonte: Cisco (2000).

Figura 3 – Estrutura da árvore MIB

Observando a árvore da Figura 3, vê-se que no caminho 1.3.6.1 estão os padrões para internet. Mais abaixo em 1.3.6.1.2.1 está a definição dos módulos MIB padronizados pela

definição da MIB-II (RFC 1158), os objetos desse nó são divididos em 11 grupos básicos conforme Quadro 3 (PÉRICAS, 2010).

Grupo	Nº Objetos	Informação
system(1)	7	Sistema de operações dos dispositivos da rede: nome, local e descrição dos equipamentos
interfaces(2)	23	Interface da rede com o meio físico e seu tráfego
translation(3)	3	Mapeamento de endereços IP em endereços físicos
ip(4)	42	Estatísticas dos pacotes IP
icmp(5)	26	Estatísticas sobre mensagens ICMP recebidas
tcp(6)	19	Algoritmos TCP, parâmetros e estatísticas de pacotes
udp(7)	6	Estatísticas de tráfego UDP
egp(8)	20	Estatísticas de tráfego de protocolo de gateway externo
transmission(10)	0	Meios físicos de transmissão específicos
snmp(11)	29	Estatísticas de SNMP

Fonte: Péricas (2010).

Quadro 3 - Informações MIB-II

Existem também as MIB que são específicas de cada fabricante no endereço 1.3.6.1.4.1. Neste nó estão todas as empresas privadas que fizeram seu registro na *Internet Assigned Numbers Autorithy* (IANA) (KUROSE, 2005). Atualmente a lista conta com 40486 empresas cadastradas sob o prefixo 1.3.6.1.4.1 ou iso.org.dod.internet.private.enterprise (IANA, 2012).

2.3 TRABALHOS CORRELATOS

Pode citar-se entre outros trabalhos, o trabalho desenvolvido por Stange (2008) como TCC do curso de Engenharia de Telecomunicações da Universidade Regional de Blumenau (FURB) que consistia de um aplicativo para computadores *desktop* desenvolvido em linguagem “AutoIT” que podia fazer consultas SNMP de dispositivos de rede e exibir mensagens referentes a condição do dispositivo, além de fazer testes utilizando a ferramenta PING para confirmar o funcionamento do dispositivo. O protótipo permitia também receber

notificações dos equipamentos utilizando SYSLOG, recurso útil para recebimento de logs remotos de equipamentos de rede pela estação de gerenciamento.

Vale comentar também o trabalho de conclusão de curso desenvolvido por Guillermo (2008) da Universidade Federal do Rio Grande do Sul onde é descrito um caso prático de implantação de Monitoramento SNMP utilizando uma série de ferramentas comerciais para monitorar a infraestrutura de pontos de Acesso sem Fios da Universidade Federal do Rio Grande do Sul (UFRGS). No trabalho o acadêmico detalha a interface e configuração de dois softwares de monitoramento muito populares, o PRTG e CACTI. Além disso ele demonstra o funcionamento de softwares de apoio como um MIB Browser e MIB Compiler.

Por fim pode citar-se outro trabalho do Curso de Engenharia de Telecomunicações que foi desenvolvido por Schulz (2004) e este também utilizou-se de SNMP para coletar dados de pontos de acesso sem fio da Agere Systems utilizando uma MIB privada do fabricante e armazenar esses dados em memória, focou-se em obter o tráfego gerado por cliente e o nível do sinal de cada cliente. O software foi desenvolvido utilizando a linguagem Delphy 7 da Borland, utilizando a biblioteca Synapse.

3 DESENVOLVIMENTO

Neste capítulo é detalhado o levantamento de informações, especificação e implementação além dos resultados do trabalho e discussão a respeito dos mesmos.

3.1 LEVANTAMENTO DE INFORMAÇÕES

O sistema desenvolvido surgiu como uma solução para simplificar o monitoramento de servidores e dispositivos de rede diversos que já incorporam o suporte ao protocolo SNMP sobre TCP/IP.

Primordialmente o sistema permite coletar dados de dispositivos de rede que foram pré-configurados dentro do sistema. Esses dados são armazenados em uma base de dados que por sua vez serão representados de forma gráfica a fim de permitir que os operadores acompanhem a utilização dos recursos de rede cadastrados. Além disso o sistema alerta os usuários por correio eletrônico quando algum limiar pré-definido de utilização de algum recurso for atingido (por exemplo, uso de processador superior a 70%).

Além das funções anteriormente descritas o sistema permite o acesso ao sistema somente à usuários autorizados e permite ao administrador do sistema definir usuários operadores e quais serão os sensores dentro do sistema aos quais esses operadores têm acesso. Os usuários não autorizados não devem ter acesso aos dados contidos no sistema e o acesso deverá ocorrer através de um navegador *web*.

3.2 ESPECIFICAÇÃO

Para o desenvolvimento da especificação dos casos de uso, além do diagrama de casos de uso do sistema foi utilizada a ferramenta Enterprise Architect da Sparx Systems. O fluxograma do monitoramento foi criado utilizando a ferramenta “Gliffy” que pode ser acessada em http://www.gliffy.com. A representação e modelagem do Banco de Dados foi criada utilizando o MySQL Workbench desenvolvido pela Oracle Corporation (ORACLE, 2012). Para fins de especificação, a seguinte legenda esclarece alguns termos utilizados na especificação/modelagem:

a) O administrador é a figura responsável pelo NMS, que cria novos sensores, cria novos usuários e delega acesso aos sensores/sistema para os operadores;
b) o operador é o usuário do sistema que tem interesse nos dados coletados e apresentados pelo sistema;
c) um sensor é alguma propriedade de algum dispositivo que pode ser monitorada (uso de memória, uso de rede, uso de disco).

3.2.1 REQUISITOS FUNCIONAIS

A partir dos objetivos especificos definidos no capitulo 1 foram elaborados os requisitos funcionais do software que estão descritos no Quadro 4.

Requisito Funcional	**Caso de Uso**
RF01: O sistema deverá permitir que o administrador gerencie usuários.	UC02
RF02: O sistema deverá permitir que o administrador gerencie sensores.	UC03, UC08
RF03: O sistema deverá permitir aos usuários visualizar os gráficos (diário e última hora) e o valor da última leitura de casa sensor.	UC04
RF04: O sistema deverá permitir definir limiares de notificação para cada sensor/usuário.	UC06
RF05: O sistema deverá permitir que o administrador gerencie as configurações globais do sistema (dados para envio de email, servidor, conta, etc.).	UC05
RF06: O sistema deverá controlar o acesso.	UC01
RF07: O sistema deverá permitir que o administrador gerencie o acesso aos sensores	UC07

Quadro 4 - Requisitos Funcionais

3.2.2 REQUISITOS NÃO FUNCIONAIS

O Quadro 5 enumera os requisitos não funcionais do sistema.

Requisitos não funcionais
RNF01: O sistema deverá ser compatível com o protocolo SNMP v2
RNF02: O sistema deverá ser compatível com o navegador Google Chrome

RNF03: O sistema deverá funcionar em um Servidor Web Apache
RNF04: O sistema deverá ser compatível com o SGBD MySQL

Quadro 5 - Requisitos não funcionais

3.2.3 DIAGRAMA DE CASOS DE USO

Esta subseção apresenta o diagrama de casos de uso conforme Figura 4. A descrição dos principais casos de uso sistema são apresentados no Apêndice A.

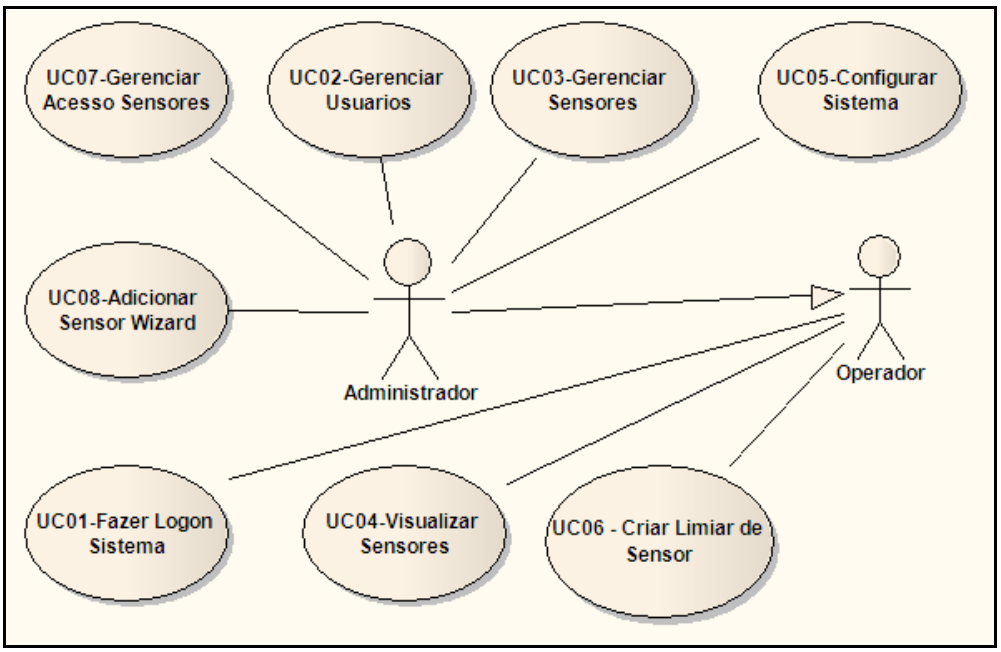


Figura 4 - Diagrama de Casos de Uso

3.2.4 MODELO CONCEITUAL DA BASE DE DADOS

A Figura 5 é uma representação gráfica das tabelas utilizadas para armazenar os dados do sistema.

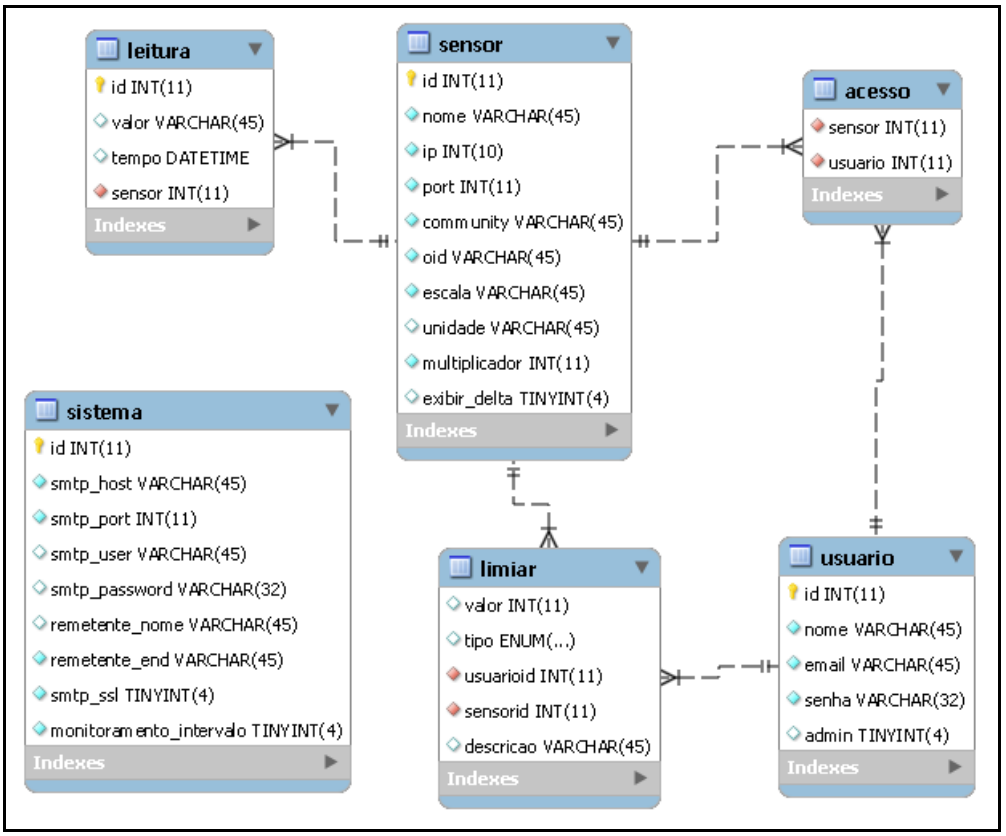


Figura 5 - Representação da Base de Dados

O sistema utiliza o banco de dados MySQL para armazenar todos os seus dados dinâmicos.

A tabela `sistema` é utilizada para armazenar configurações gerais do sistema como os dados utilizados para envio de email e a configuração do intervalo de monitoramento. Somente o administrador pode alterar esta configuração e ela afeta todo o sistema.

A tabela `usuario` armazena as propriedades dos usuários utilizadas para diferenciar os usuários no sistema, permitir a entrada no sistema e controlar o acesso. Somente administradores podem cadastrar ou excluir usuários.

A tabela `acesso` é uma matriz que define quais usuários podem visualizar quais sensores. Para um usuário (administrador ou operador) poder visualizar o monitoramento de um sensor, ele precisa ter seu acesso permitido nesta tabela.

A tabela `sensor` armazena as propriedades de cada sensor que o sistema monitora. Somente administradores podem cadastrar, alterar ou excluir sensores.

A tabela `limiar` armazena a configuração do limiar definido para cada usuário e é uma configuração por sensor. Qualquer usuário pode configurar um limiar.

A tabela `leitura` armazena todos os dados coletados identificando a qual sensor pertence aquela leitura. Estes dados são utilizados para trazer a última leitura ou os gráficos dentro do sistema.

3.2.5 FLUXOGRAMA DE MONITORAMENTO DO SISTEMA

O monitoramento é parte vital do sistema, ele é executado paralelamente a interface *web* e realiza consultas SNMP, armazena e recupera valores do SGBD e envia mensagens de correio eletrônico, seu funcionamento pode ser conferido abaixo na Figura 6.

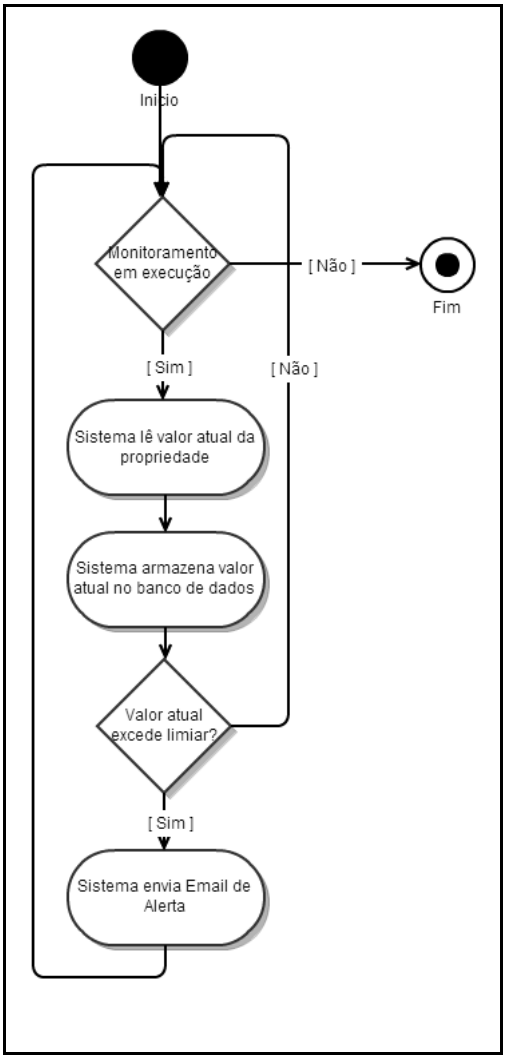


Figura 6 - Fluxograma Monitoramento

Este fluxo é executado para cada sensor cadastrado no sistema, se o monitoramento estiver em execução, o sistema consulta uma propriedade de um sensor, em seguida o sistema armazena o resultado dessa consulta no banco de dados, posteriormente o sistema verifica se

esse valor que foi retornado da consulta excede um limiar cadastrado, se um limiar for ultrapassado o sistema envia uma mensagem eletrônica de alerta para o usuário que criou o monitoramento, se nenhum limiar for atingido o sistema simplesmente volta ao inicio do *loop* de monitoramento.

3.3 IMPLEMENTAÇÃO

A seguir são mostradas as técnicas e ferramentas utilizadas e a operacionalidade da implementação.

3.3.1 Técnicas e ferramentas utilizadas

O sistema foi desenvolvido utilizando a linguagem *Hypertext Preprocessor* (PHP) que é uma linguagem de código aberto criada originalmente para gerar páginas *web* dinâmicas. O código fonte é interpretado pelo servidor *web* no momento que as páginas são requisitadas (PHP, 2012).

Foram utilizadas também bibliotecas PHP para facilitar o desenvolvimento. Bibliotecas são conjuntos de código criadas para facilitar a implementação de tarefas comuns como envio de email ou geração de gráficos.

Além do PHP, foi utilizado javascript para permitir uma funcionalidade do sistema. O javascript foi criado em 1994 e permite adicionar funcionalidades sofisticadas a páginas web, o javascript é executado pelo cliente em páginas web mesmo após a página já ter sido carregada (MOZILLA, 2012).

O servidor web utilizado é o Apache *Hypertext Transfer Protocol* (HTTP) Server, lançado em 1995 como uma alternativa ao *Public Domain HTTP Daemon* que era o servidor web mais popular da época, mas que teve seu desenvolvimento interrompido em meados de 1994 (APACHE, 2012).

Os dados do sistema são armazenados em um Sistema Gerenciador de Banco de Dados (SGBD) chamado MySQL, escolhido pela facilidade e simplicidade do uso e integração fluente com o PHP.

Para auxiliar o desenvolvimento foram utilizados softwares como o PRTG Network Monitor desenvolvido pela Paessler para observar o comportamento e funcionamento de um

sistema NMS, além do software NetCrunch da AdRem na sua terceira versão. O NetCrunch permite navegar e consultar facilmente os valores da MIB SNMP, auxiliando muito no desenvolvimento do sofware.

3.3.1.1 PHP

O PHP foi utilizado para desenvolvimento de maior parte do código final do sistema. Na Figura 7 pode ser observado um trecho de código SNMP. Neste segmento de código pode ser observada a sintaxe e peculiaridades da linguagem.

```php
if ($_SERVER['REQUEST_METHOD'] == "POST") {
    $s['sensor_instancia']       = @$_POST['oid_instancia'];

    if ($s['sensor_instancia'] != "")
    {
        switch ($s['sensor_tipo']) {
            case "storage":
                $s['sensor_multiplicador'] = snmp2_get($s['sensor_ip'].":"
                .$s['sensor_porta'], $s['sensor_comunidade'], '.1.3.6.1.2.1.25.2.3.1.4.'.$s['sensor_instancia'],'3000000', '0');
                break;
            default:
                $s['sensor_multiplicador'] = 1;
        }
        $s['step']++;
        reload();
    }else{
        $error = true;
        echo "Selecione uma opção";
    }
}
```

Figura 7 - Trecho de Código PHP

O código acima é utilizando no passo a passo de adição de novo sensor. Quando o sensor for do tipo *storage* (armazenamento) ele faz uma consulta SNMP para determinar o multiplicador a ser utilizado para converter o valor fornecido pelas leituras para bytes. A função *snmp2_get* é utilizada para retornar valores de objetos SNMP.

A coleta dos dados do sistema depende da execução interativa de um script chamado “get.php”, que verifica todos os sensores cadastrados no sistema e faz as consultas respectivas, armazenando esses valores. Para a execução desse script precisa ser utilizado a seguinte linha de comando: “php.exe get.php”, isto inicia o monitoramento e ele só é interrompido quando o script é finalizado.

3.3.1.2 Bibliotecas PHP

Foram utilizadas duas bibliotecas de terceiros no desenvolvimento do sistema.

A primeira é a PHPGraphLib desenvolvida por Elliot Brueggman e é uma biblioteca para geração de gráficos desenvolvida em PHP que pode ser integrada com websites e outros sistemas PHP. Ela é gratuita para uso pessoal e a versão comercial pode ser licenciada por servidor ou para servidores ilimitados. O site do desenvolvedor é "http://www.ebrueggeman.com" (BRUEGGMAN, 2011).

Para utilizar a biblioteca é armazenado o resultado de uma consulta em uma variável, em seguida é criado um novo gráfico, são definidas as propriedades e é fornecido o intervalo de dados.

A geração do gráfico no sistema começa armazenando o resultado de uma consulta do banco em uma variável conforme a Figura 8.

```
$_SESSION['graphdata'][$id] = array("query"=>"select ROUND(AVG(valor*".$sensor['escala']."),2) as valor, from_UNIXTIME(AVG(UNIX_TIMESTAMP(tempo)))
as tempo from leitura  where sensor = ".$_REQUEST['id']." and valor IS NOT NULL and tempo > DATE_SUB(now(),
INTERVAL 1 HOUR) GROUP BY UNIX_TIMESTAMP(tempo) div 300 order by tempo","title"=>$sensor['nome']." / ".$sensor['unidade']." - Ultima Hora");
```

Figura 8 - Consulta de Geração do Gráfico

Em seguida os valores retornados desta consulta são transferidos para um *array*, uma vez os dados no *array* são definidos o titulo e outras propriedades do gráfico e é utilizada a função *createGraph()* para gerar o gráfico na tela conforme a Figura 9.

```
<?php
include "include/phpgraphlib.php";
include "include/auxiliar.php";

$g = $_SESSION['graphdata'][($_GET['id'])];

$graph=new PHPGraphLib(800,450);
$dataArray=array();

//get data from database
$sql=$g['query'];
$result = mysql_query($sql) or die('Query failed: ' . mysql_error());
if ($result) {
  while ($row = mysql_fetch_assoc($result)) {
      $eixox=$row["tempo"];
      $eixoy=$row["valor"];
      //add to data array
      $dataArray[$eixox]=$eixoy;
  }
}

//configure graph
if (count($dataArray) > 0) $graph->addData($dataArray);
$graph->setTitle($g['title']);
$graph->setGradient("lime", "green");
$graph->setBarOutlineColor("black");
$graph->setBars(false);
$graph->setLine(true);
$graph->createGraph();

?>
```

Figura 9 - Geração do Gráfico

O gráfico gerado fica com a aparência do gráfico apresentado na Figura 10.

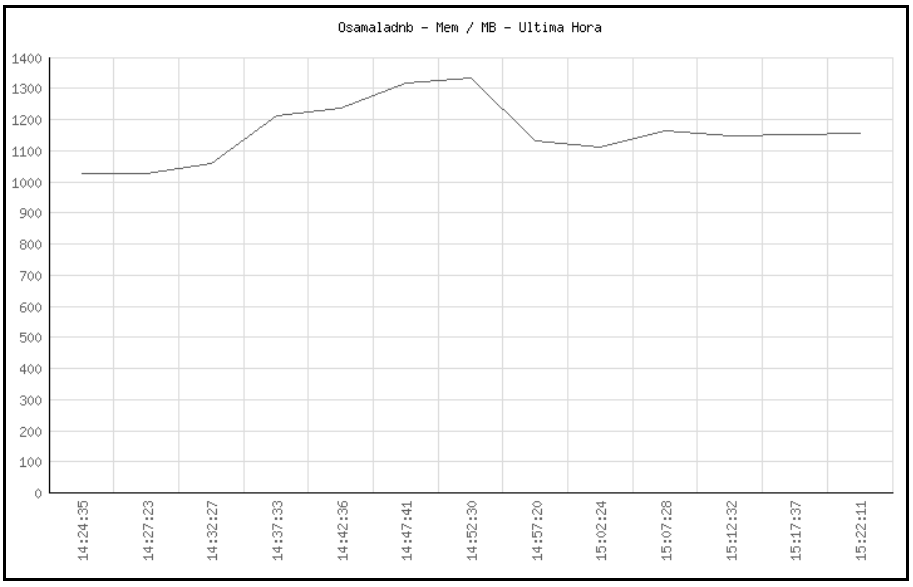


Figura 10 - Gráfico Gerado

Além da Biblioteca de Geração de Gráficos é utilizada uma biblioteca adicional para o envio da correspondência eletrônica de alertas. A biblioteca chama-se PHPMailer e foi desenvolvida pela Worxware. É distribuída gratuitamente para uso comercial ou pessoal sob a licença *Lesser General Public License* (LGPL) (WORXWARE, 2009). A utilização é bastante simples e pode ser conferida na Figura 11.

```php
$mail             = new PHPMailer();

$body             = "Olá.<br> Foi atingido/ultrapassado o limiar de um sensor:<br>Sensor: ".$sensor['nome']."<br>"."IP: ".$se
$body             = eregi_replace("[\]",'',$body);

$mail->IsSMTP();                              // telling the class to use SMTP

$mail->SMTPAuth   = $sistema[smtp_ssl];       // enable SMTP authentication
$mail->SMTPSecure = "ssl";                    // sets the prefix to the servier
$mail->Host       = $sistema[smtp_host];      // sets GMAIL as the SMTP server
$mail->Port       = $sistema[smtp_port];      // set the SMTP port for the GMAIL server
$mail->Username   = $sistema[smtp_user];      // GMAIL username
$mail->Password   = $sistema[smtp_password];  // GMAIL password

$mail->SetFrom($sistema[remetente_end], $sistema[remetente_nome]);

$mail->Subject    = "SNMP Monitor";

$mail->MsgHTML($body);

$address = $limiar['email'];
$mail->AddAddress($address, $limiar['usuario_nome']);

if(!$mail->Send()) {
  echo "Mailer Error: " . $mail->ErrorInfo;
} else {
  echo "Message sent!";
}
```

Figura 11 - Utilização da Biblioteca PHPMailer

Para enviar uma mensagem basta informar os campos servidor de email, porta, destinatário, e depois de definir todos os valores utilizar a função *$mail->Send()*. O trecho de código da Figura 11 envia o alerta de que um limiar de sensor foi ultrapassado.

3.3.1.3 JavaScript

O javascript foi utilizado no sistema para permitir a atualização automática da página que exibe os dados e valores coletados dos sensores. Na Figura 12 é possível observar o código do script.

```
<title>SNMP Monitor - ".$menu[(substr(strrchr( $_SERVER['SCRIPT_NAME'], '/'), 1))][1]."</title>
<link rel=\"stylesheet\" href=\"web.css\" title=\"Basic\" type=\"text/css\" />

<script type=\"text/JavaScript\">
var c=30;

function timedCount(){
    c=c-1;
    if (c == 0) {location.reload();}
    setTimeout(function(){timedCount()},1000);
}

function increaseTimer(){
    c=c+20;
}
</script>

</head>
<body>
";
```

Figura 12 - Script javascript

A função *timedCount()* é executada a cada 1000 milissegundos e decrementa um contador *c*. Quando este contador chega a 0 é executado o comando *location.reload* que recarrega a página no navegador. A função *increaseTimer()* é utilizada quando o usuário clica sobre um dos campos do limiar, aumentando o contador e evitando que a página seja atualizada enquanto o usuário estiver criando ou alterando um limiar. O script javascript precisa ficar dentro da tag <head> do documento *HyperText Markup Language* HTML (REFSNES, 2012).

3.3.1.4 MySQL

O MySQL é um SGBD desenvolvido pela Oracle Corporation. Ele é utilizado para armazenar todos os dados do sistema proposto. São utilizados comandos *Data Manipulation Language* (DML) para que o sistema possa comunicar-se com o banco. Através destes

comandos DML, o SGBD pode recuperar, gravar ou alterar registros do banco (ORACLE, 2012).

A utilização pode ser conferida na Figura 13 que apresenta a interação com o SGBD no sistema(Código PHP).

```
else { //Se o metodo for POST, insere os dados do POST no Banco de Dados
  mysql_query("INSERT INTO usuario (nome, email, senha, admin)
  VALUES ('".$_POST['nome']."', '".$_POST['email']."', md5('".$_POST['senha']."'), ".$_POST['admin'].")")
   or die("Não foi possível cadastrar. Verifique os campos.");
  echo "Usuário cadastrado.";

  //Exibe a lista de usuários cadastrados.
$userlistq = mysql_query("SELECT id, nome, email, IF(admin, 'Sim','Não') admin FROM usuario");
if (mysql_num_rows($userlistq) > 0) {
  echo "<h3>Lista de usuários atualmente cadastrados:</h3>";
  echo "<table>\r\n<tr><th>Nome<th>email<th>Admin<th> ";
  while ($user = mysql_fetch_array($userlistq))
   echo "<tr><td>".$user['nome']."<td>".$user['email']."<td>".$user['admin']."<td><a href=?action=del&id=".$user['id'].">X</a>\r\n";
  echo "</table>";
}
```

Figura 13 - Linguagem DML do SGBD

No primeiro trecho de código é utilizado o comando *INSERT* para inserir um grupo de dados no banco de dados. No segundo trecho de código é utilizado o comando *SELECT* para recuperar dados do banco de dados.

3.3.1.5 Ferramentas de Monitoramento

O NetCrunch é uma ferramenta completa de monitoramento compatível com SNMP, foi utilizado principalmente um recurso chamado “IP and SNMP Tools”, especificamente o MIB Browser SNMP (ADREM, 2012). Através do MIB Browser é possível visualizar e navegar a árvore da MIB SNMP e observar todos os campos que podem ser consultados ou gravados. Além de exibir os campos, o sistema traz uma descrição do campo o que em alguns casos facilita o desenvolvimento, conforme Figura 14.

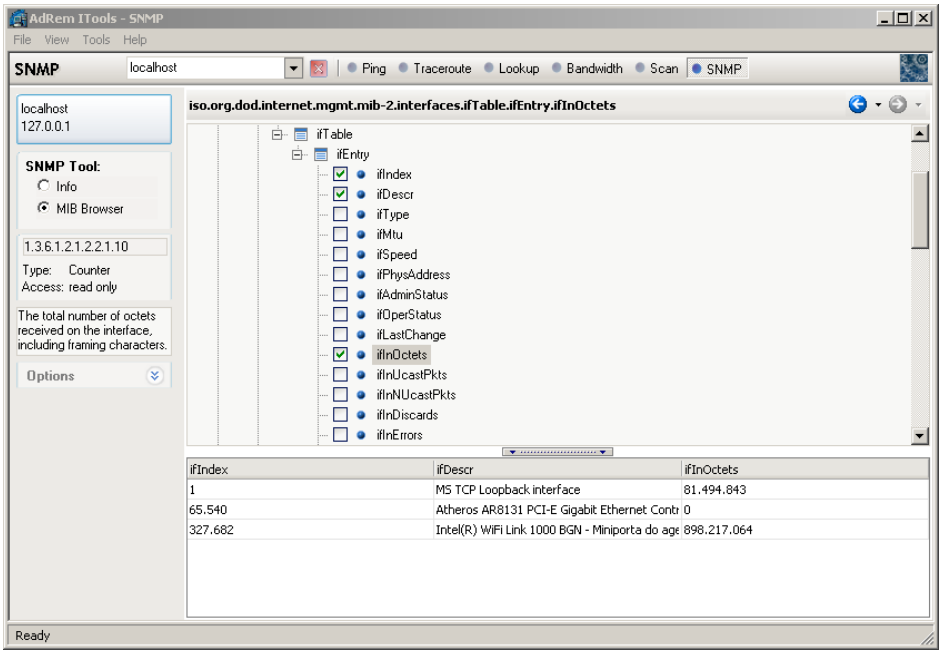


Figura 14 - AdRem iTools SNMP

Também foi utilizado durante o desenvolvimento o software PRTG Network Monitor na versão 6 como referência de como deve funcionar um NMS. Ele é gratuito até 10 sensores.

3.3.2 Operacionalidade da implementação

Para demonstrar a operacionalidade da implementação foi desenvolvido um estudo de caso onde será considerado um caso hipotético de monitoramento de uso de rede e processamento de um servidor que será chamado de caso de “overlord” com IP 192.168.100.4. Será criado um monitoramento do tráfego de saída da placa de rede “Realtek RTL8168C” e o uso de disco da unidade C:\ .

Assume-se que o sistema já esteja corretamente instalado e configurado no servidor Localhost e que já existe um usuário administrador criado.

Por fim presume-se que o SNMP já esteja habilitado no servidor “Overlord” com a comunidade “public”.

Para acessar o sistema NMS é necessário acessar a url do servidor: http://localhost/snmp/ . O usuário será então confrontado com a tela de *Login* conforme Figura 15. O usuário luciano@lingnau.com.br (Luciano) será utilizado para demonstrar o uso.

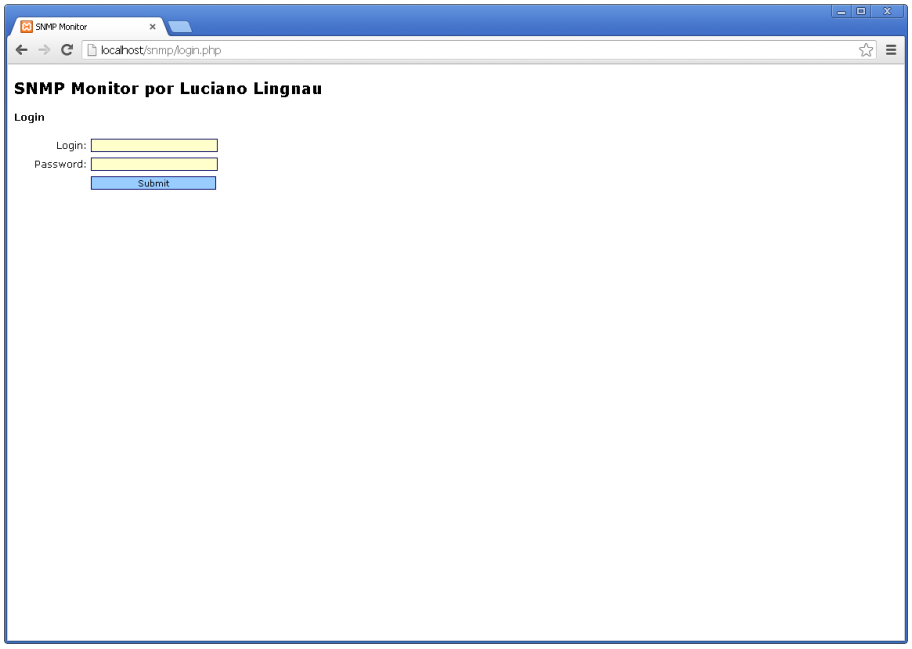


Figura 15 - Tela de *Login*

Após informar as credencias válidas o usuário é redirecionado a tela inicial onde são exibidos os gráficos dos sensores atuais e o menu do sistema como pode ser visto na Figura 16.

Figura 16 - Tela inicial Sistema

Uma vez dentro do sistema, o usuário clica sobre a opção “Adicionar Sensor”. O usuário é então confrontado com a tela inicial do *wizard* criado para adicionar sensores (Figura 17).

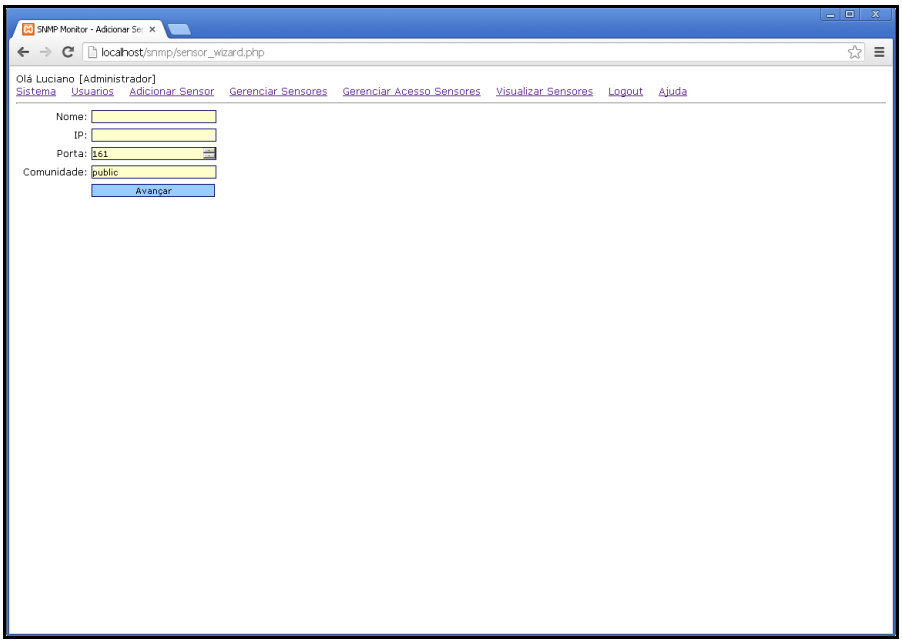


Figura 17 - *Wizard* de Adição de Sensor

O usuário informa então o nome do Sensor a ser criado “Disco C: Overlord”, IP 192.168.100.4 e clica sobre “Avançar”. Os dados porta e comunidade já tem valores default que são os valores padrão. Neste ponto quando o usuário clica em “Avançar” o sistema faz uma consulta SNMP do OID 1.3.6.1.2.1.1.1.0 (*System Description*). Se a consulta falhar é gerado um erro pedindo ao usuário verificar se o SNMP está habilitado. Todos dispositivos que suportam SNMP e estejam funcionando retornam um valor para essa consulta. O código-fonte deste teste pode ser observado na Figura 18.

```
if (@snmp2_get($s['sensor_ip'].":".$s['sensor_porta'], $s['sensor_comunidade'], '.1.3.6.1.2.1.1.1.0', '3000000', '0'))
{
    $s['step']++;
    reload();
}else{
    $error = true;
    echo "Host não respondeu, verifique se ele está ligado e se o SNMP está habilitado";
}
```

Figura 18 - Testando o Host para SNMP habilitado

Se o *host* informado tiver SNMP habilitado, será trazida a lista de opções a serem monitoradas, sendo elas: CPU, Memória/Armazenamento, Rede (Ingresso) e Rede (Egresso).

Os sensores precisam ser adicionados individualmente, então primeiramente será descrita a criação do sensor de monitoramento do disco C:, onde o usuário seleciona Memória/Armazenamento e clica em “Avançar” conforme a Figura 19.

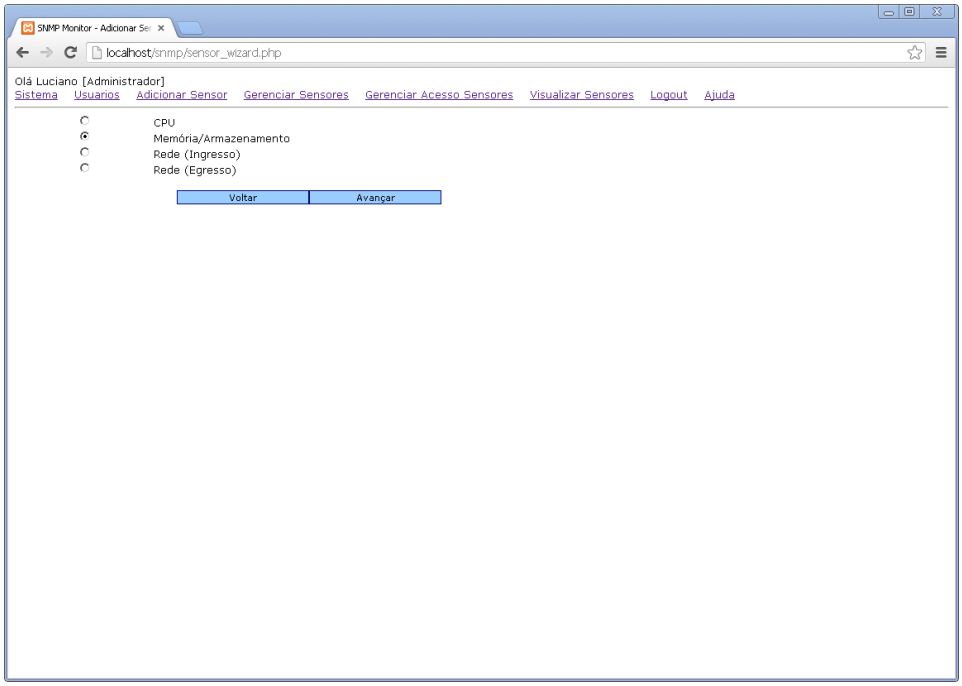


Figura 19 - Selecionar tipo do monitoramento

No passo seguinte o sistema consulta todos os armazenamentos do computador (o que inclui discos, memória física e memória virtual). É apresentada então a lista de todos esses armazenamentos e o usuário deve selecionar uma das opções. Como o objetivo é monitorar o uso de disco da unidade C:\ o usuário seleciona "C:\ Label: Serial Number 8293c158" conforme a Figura 20.

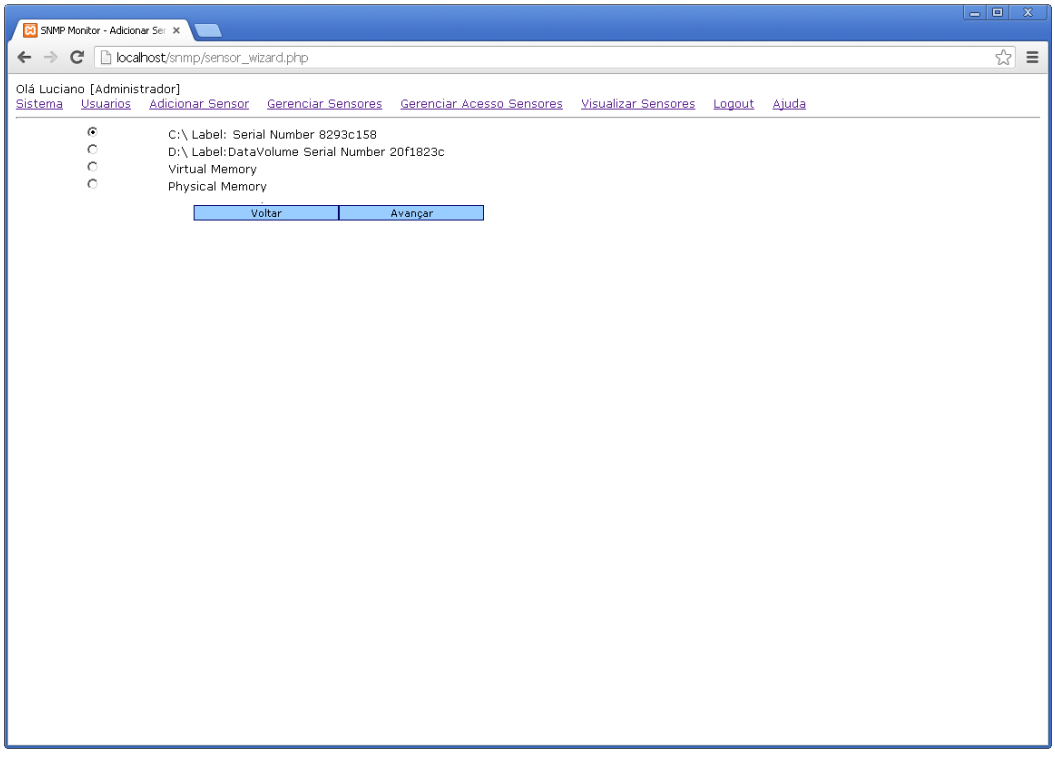


Figura 20 - Seleção do armazenamento/memória

Após informar o armazenamento selecionado e clicar sobre o botão “Avançar” é apresentada uma lista dos parâmetros a serem definidos para um novo sensor. Se o usuário localizar algum erro ele pode voltar e fazer a devida alteração. Este passo pode ser observado na Figura 21.

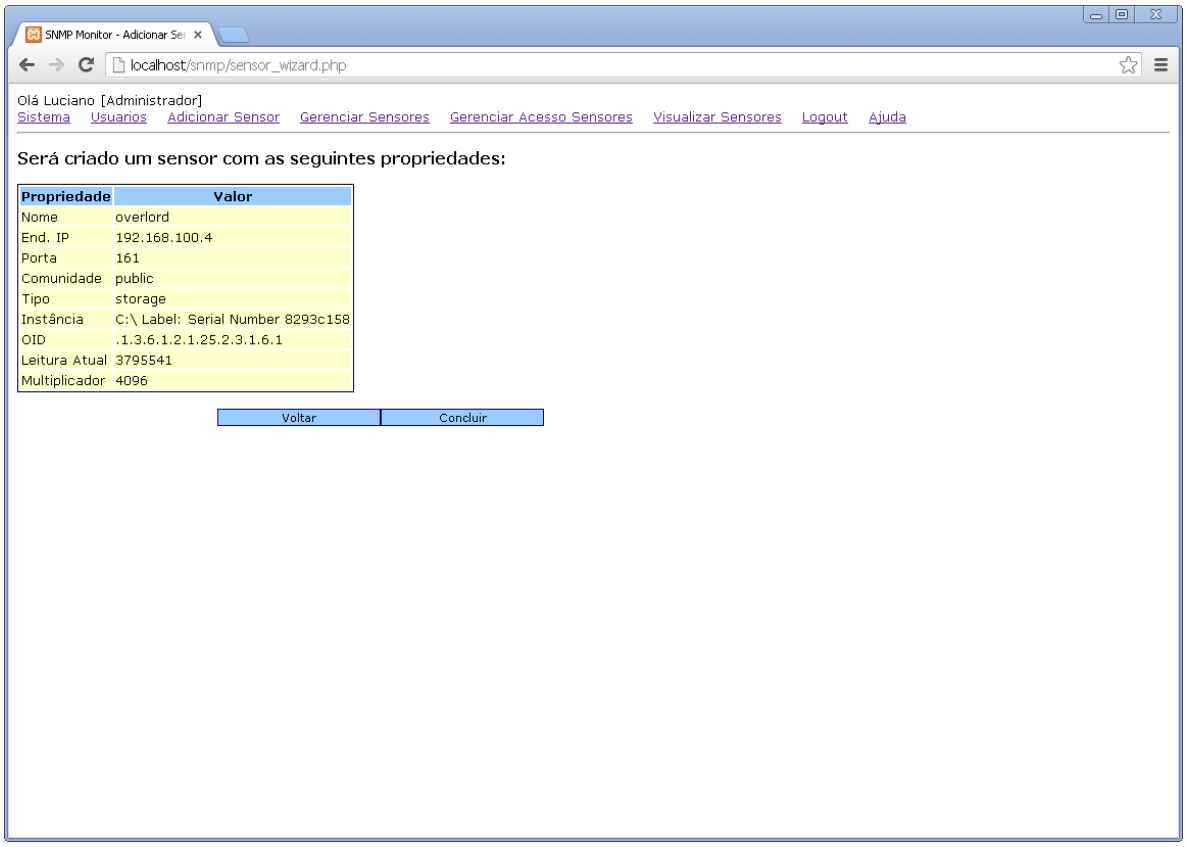


Figura 21 - Resumo do Sensor

Após clicar no botão Concluir que pode ser visto na Figura 21 é apresentada a mensagem “Sensor Criado com Sucesso” e o sensor é criado.

O passo seguinte é atribuir acesso ao novo sensor criado. Isto é feito no menu “Gerenciar Acesso Sensores”. Em “Gerenciar Acesso Sensores” é apresentada a matriz de permissões, sendo que um *checkbox* marcado significa que o usuário tem acesso. Neste caso é necessário localizar a interseção do sensor “Disco C: Overlord” com o usuário “Luciano”. Este *checkbox* precisa ser marcado para que o usuário tenha acesso a visualização do Sensor conforme a Figura 22 onde foi realçado o usuário e o sensor em questão.

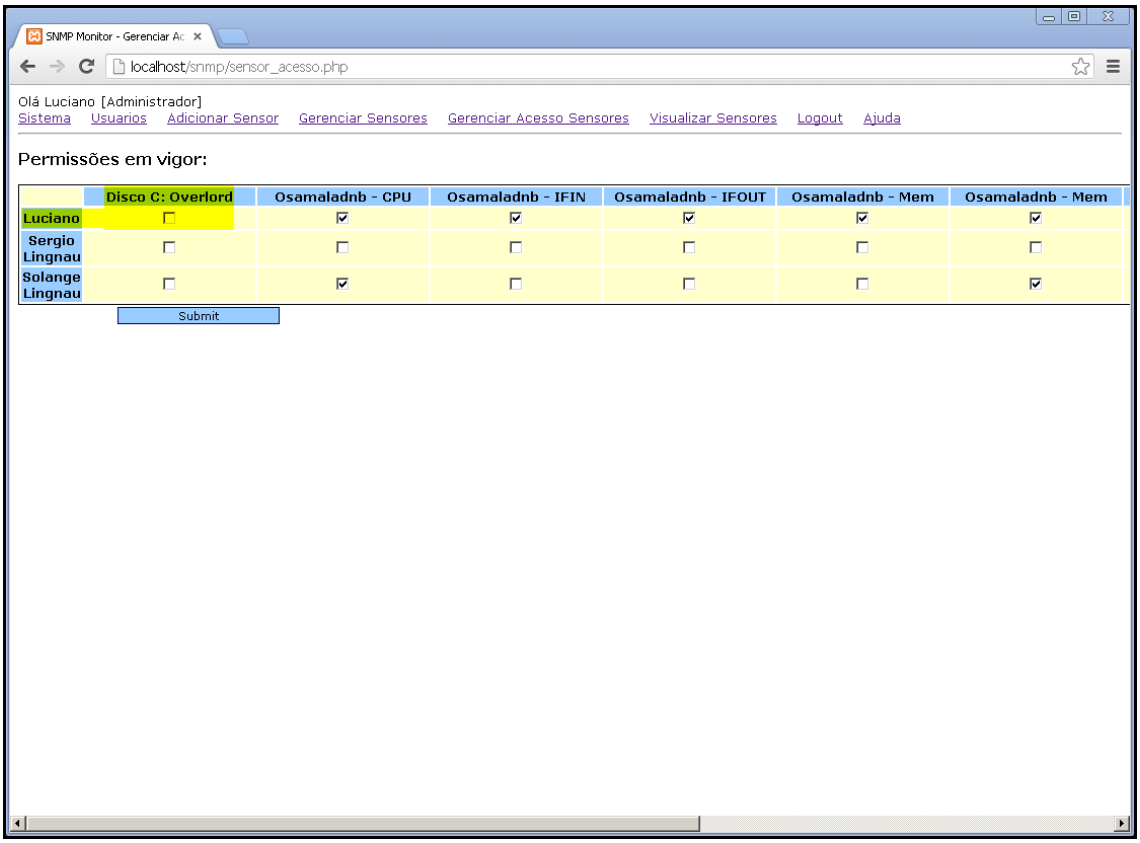


Figura 22 - Configuração do Acesso ao Sensor

Após marcar o *checkbox* e clicar sobre o botão “Submit” é gravada a alteração do acesso e gerada e mensagem “Permissões Atualizadas”.

Agora é possível visualizar o sensor em “Visualizar Sensores” mas a leitura apresentada será em Bytes. Para cadastrar uma unidade de Medida e Escala de conversão é necessário acessar “Gerenciar Sensores”. Ao acessar a tela “Gerenciar Sensores” e clicar sobre o link “E” do respectivo sensor na lista é possível alterar as propriedades do sensor conforme a Figura 23.

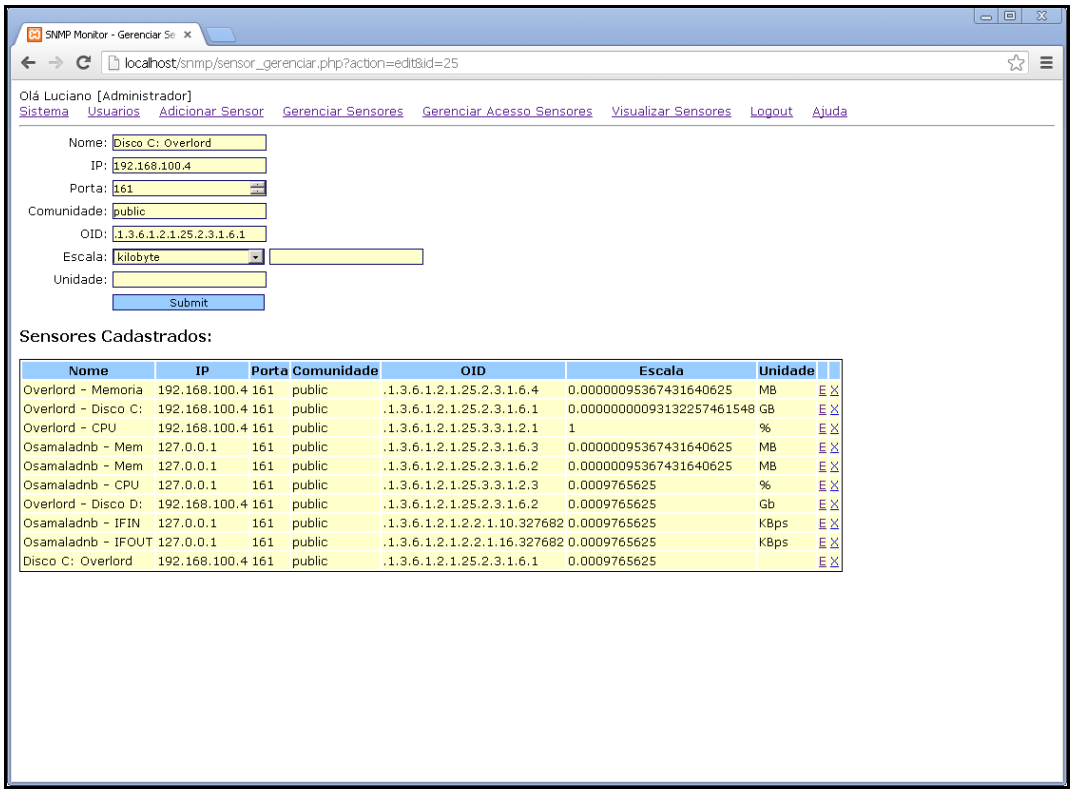


Figura 23 - Edição do Sensor

Após clicar no “E” na Figura 23 são completados os formulários da parte superior da página, lá podem ser feitas as alterações no sensor já cadastrado. Nesse caso é feita a alteração da escala de *Kilobyte* para *Gigabyte* pois o sensor em questão é uma unidade de disco. É possível informar também que a Unidade é “GB” e clicar em submit. É recebida a mensagem “Sensor Alterado”.

Agora é possível acessar “Visualizar Sensores” e localizar o sensor criado anteriormente. “Disco C: Overlord” conforme Figura 24.

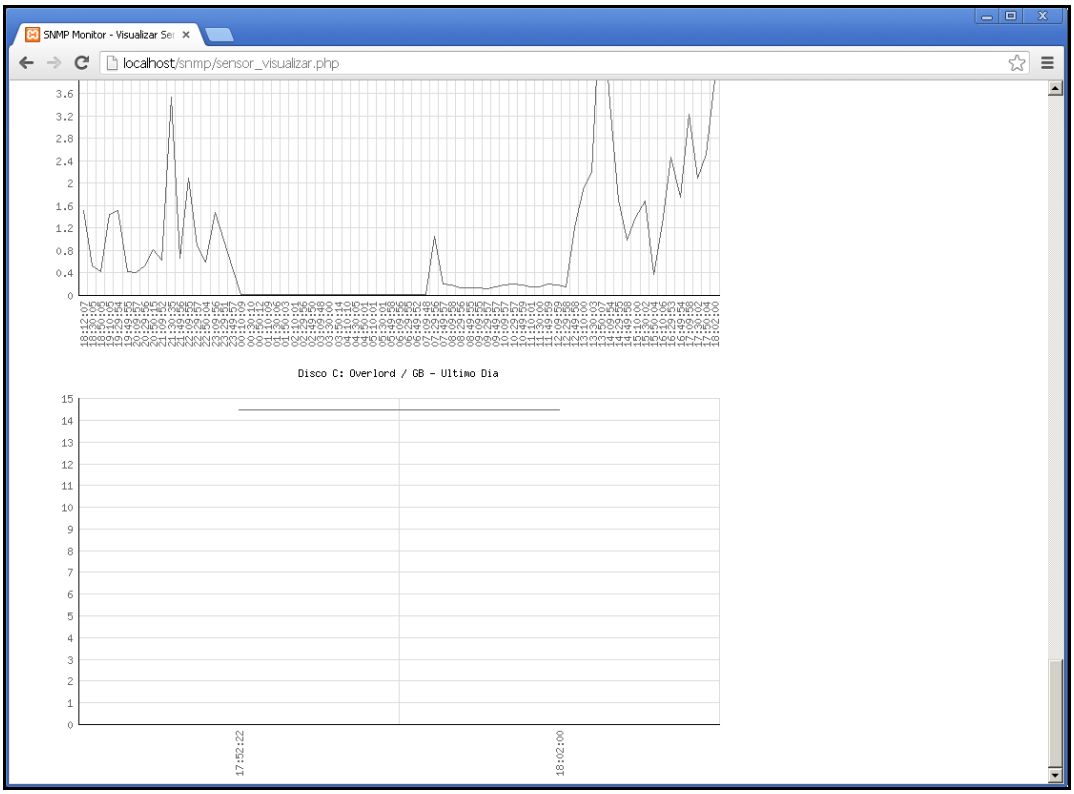


Figura 24 - Visualizar Sensores Geral

Na Figura 24 após clicar sobre o gráfico do sensor são trazidos os detalhes do sensor. Infelizmente como a quantidade de amostras ainda é pequena o gráfico não é muito nítido, a medida que o espaço amostral aumenta o gráfico fica mais completo. A Figura 25 apresenta os detalhes do sensor. Dentro dos detalhes do sensor é apresentado o gráfico diário e da última hora, além da última leitura e do tempo da última leitura.

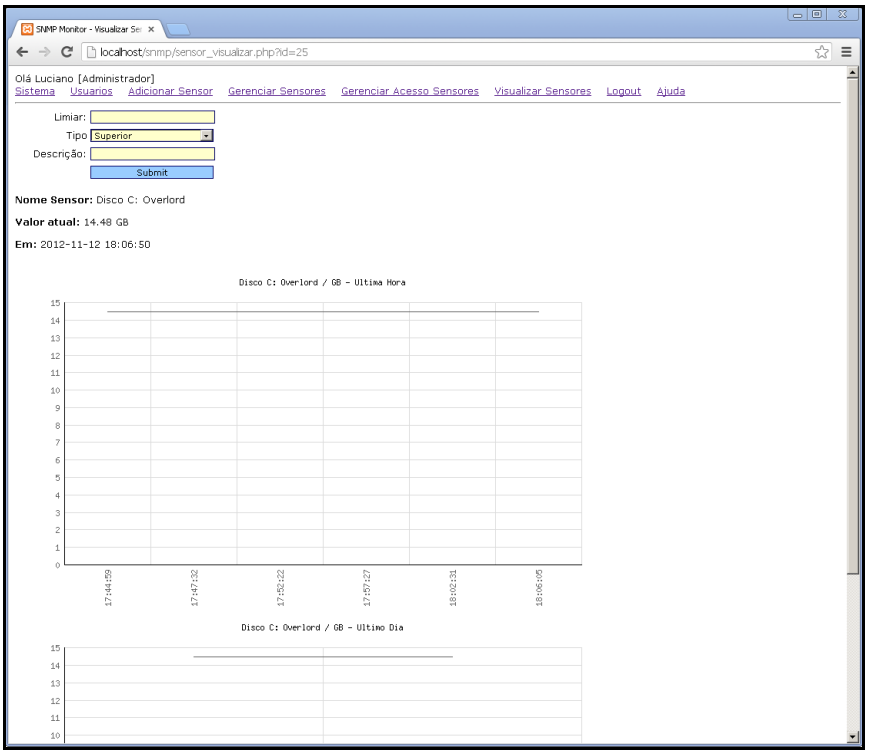


Figura 25 - Visualizar Sensor (Detalhes)

Na Figura 25 pode ser observado que o valor atual é 14.48Gb. Acima dos detalhes do sensor existe o botão para criar um “Limiar”. Um limiar é um valor que quando ultrapassado (Acima ou Abaixo) gera uma mensagem de alerta para o usuário que criou o limiar. Será definido um Limiar com valor 15 para teste. É informado o valor 15, o tipo “Superior”(Para que seja gerado um evento quando a leitura ficar acima desse valor) e a descrição será “Espaço Livre Crítico”. Após clicar em “Submit” a página é atualizada e o valor do limiar fica gravado e é exibido dentro dos campos utilizados para fazer o cadastro. Para efeito do caso de uso foi copiado um arquivo de 1.59Gb para o Disco C: do servidor “Overlord”. Após alguns insantes quando o gráfico foi atualizado com os valores de novas consultas o valor passou para 16.08Gb, ultrapassando o Limiar definido de 15Gb, o resultado pode ser visto nas Figuras 26 e 27.

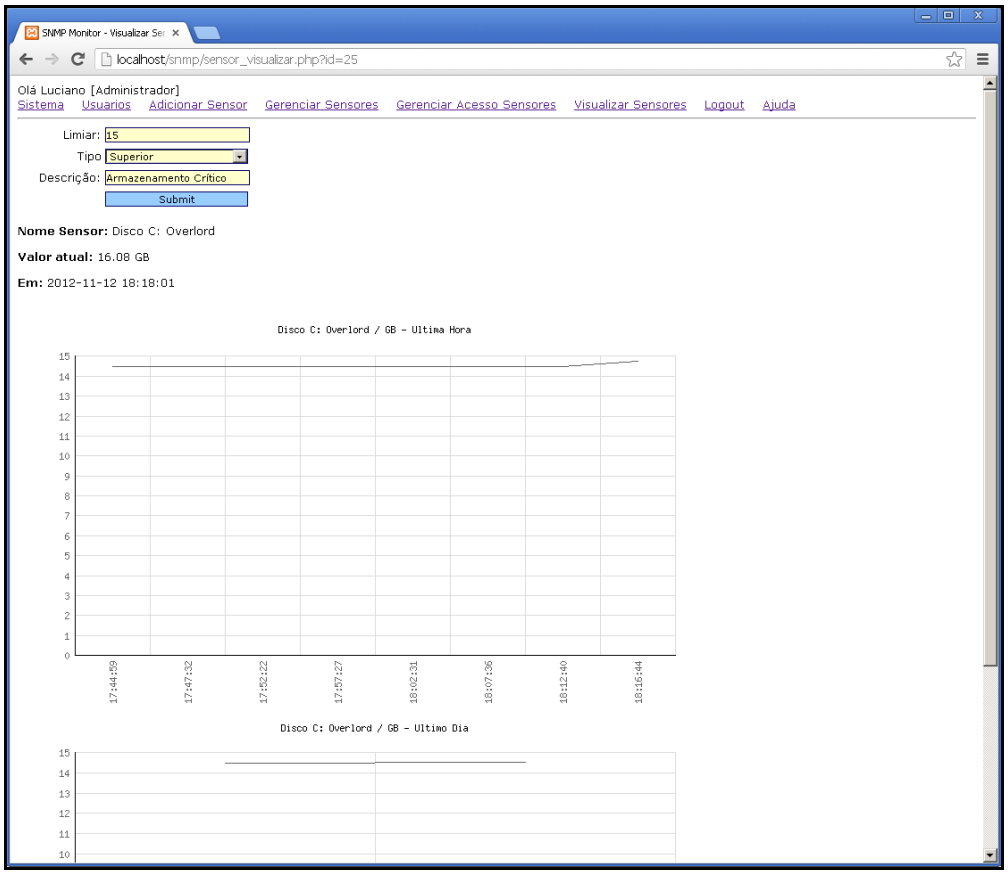


Figura 26 - Alteração no Gráfico e Valor

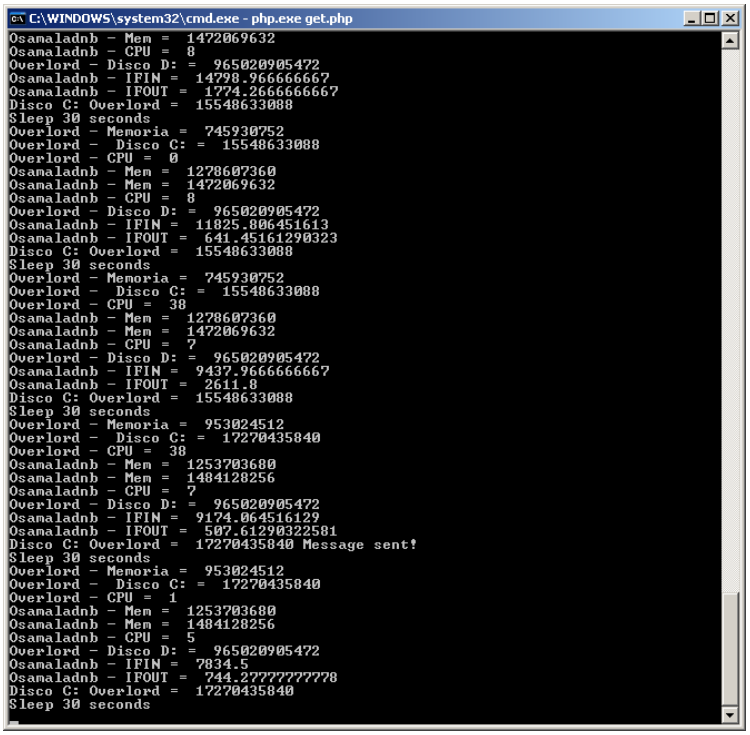


Figura 27 – Monitoramento

Na Figura 27 pode ser visto o momento em que o serviço de monitoramento faz a consulta que ultrapassa o limiar definido e envia uma mensagem. A mensagem recebida tem o seguinte formato conforme Figura 28.

Figura 28 - Mensagem de Alerta

A mensagem de alerta é enviada uma única vez cada vez que o limiar é rompido. Isso impede que o sistema inunde a caixa postal do usuário com mensagens repetidas. A criação do sensor de monitoramento da interface de rede do servidor “Overlord” segue exatamente o mesmo procedimento da criação do sensor de disco, exceto pelo fato de que no da Criação onde anteriormente foi selecionado o sensor tipo “memória/armazenamento” deve ser selecionado o sensor do tipo “Rede (Egresso)” e posteriormente a placa de rede física do servidor.

Para encerrar sua sessão o usuário pode clicar sobre a opção “logoff”, que encerra seu acesso ao sistema e impede o uso indevido da sua sessão. Os alertas são recebidos mesmo quando o usuário não está logado no sistema, dependendo apenas da execução do serviço de monitoramento do sistema.

3.4 RESULTADOS E DISCUSSÃO

O sistema final que é o produto deste trabalho não só atendeu os objetivos definidos no item 1.1 deste documento como também foram desenvolvidos mecanismos para facilitar a utilização por usuários que não estejam habituados ou que não conheçam o SNMP, tornando o sistema mais prático e fácil de utilizar.

Ao ser apresentado a um atual usuário do NMS CACTI em uma entrevista informal a reação foi muito positiva, principalmente em relação à facilidade de uso do sistema, houve porém uma crítica em relação aos gráficos que segundo o usuário entrevistado “poderiam ser

melhores". CACTI é um sistema de monitoramento e geração de gráficos baseado no RRDTool, que utiliza PHP e MySQL para prover uma interface e armazenar os dados coletados (CACTI, 2012).

Em relação aos trabalhos correlatos, o sistema desenvolvido aqui faz o que é sugerido como extensão do trabalho de conclusão de curso desenvolvido por Schulz (2004), no qual ele conseguia ler contadores de tráfego de pontos de acesso sem fios mas não chegou a armazenar esses dados coletados em um SGBD. Ele sugeriu como extensão do seu trabalho esses dados poderiam ser armazenados em um banco de dados e então recuperados através de métodos estatísticos para gerar gráficos de determinados períodos de tempo.

Já Stange (2008) sugeria que um sistema de monitoramento como o desenvolvido por ele na linguagem AutoIT fosse desenvolvido em uma linguagem de programação avançada, acredito que nesse sentido o PHP tenha sido uma linguagem mais do que mais do que apta para essa tarefa.

Se comparado aos sistemas de monitoramento apresentados por Guillermo (2008) o sistema desenvolvido neste trabalho tem vários aspectos em comum com os sistemas profissionais apresentados, como a geração de gráficos e adição de sensores por um passo-a-passo.

4 CONCLUSÕES

O objetivo proposto no inicio do desenvolvimento deste trabalho foi atendidos, assim como os objetivos específicos.

Foi possível coletar os dados de desempenho da MIB-II de dispositivos inter-conectados em uma rede TCP/IP, além de ser possível ainda criar uma interface simples com um passo a passo para adicionar novos monitoramentos ao sistema.

A partir dos dados coletados e armazenados no banco de dados foi possível gerar gráficos de diferentes intervalos de tempo e apresentar esses gráficos ao usuário, apresentando o tempo e valor de cada média do espaço amostral.

O sistema tem um controle de usuários para permitir que somente usuários autorizados acessem o sistema, uma vez dentro do sistema o administrador pode definir a quais dispositivos monitorados aquele usuário tem acesso através de uma matriz de acesso.

O sistema também gera alertas por correio eletrônico quando ocorrem leituras superiores ou inferiores a um valor determinado pelo operador a fim de notificá-los quando por exemplo o armazenamento de um volume estiver chegando perto do fim ou o uso de uma interface de rede estiver acima de um patamar normal.

As ferramentas utilizadas para o desenvolvimento do trabalho foram mais do que adequadas. A extensão SNMP do PHP funciona muito bem apesar de a documentação ser relativamente escassa. O SGBD MySQL mais do que atendeu as necessidades de recuperação e armazenamento de dados e o servidor web Apache é mais do que capaz de servir às páginas e processar os scripts PHP que geram as páginas. O maior desafio do trabalho foi em relação a compreender o funcionamento do SNMP e entender a lógica das estruturas de dados, pois a documentação a respeito não é muito amigável, por isso uma ferramenta como o AdRem NetCrunch foi de grande ajuda no desenvolvimento pois permitia navegar diretamente na MIB e observar quais valores precisavam ser lidos, além de exibir o OID referente à aquele valor.

O sistema infelizmente tem algumas limitações que são claras e precisam ser documentadas. Atualmente o sistema só coleta dados utilizando o protocolo SNMP V2, não sendo compatível com o protocolo SNMP v1 que foi depreciado pelo SNMP v2 ou com o SNMP v3 que ainda tornar-se-á um padrão de mercado. O sistema também não permite criar mais de um limiar por sensor, para casos onde o operador gostaria de ter dois limiares, um de “aviso” e outro de “nível crítico”. Outra grande limitação do sistema que não foi resolvida

durante o desenvolvimento é o endereçamento dinâmico das interfaces de rede. Em alguns sistemas quando o sistema é reiniciado ou a interface de rede é desligada e re-ligada perde-se o endereço da instância daquela interface pois o número do índice é dinâmico. Atualmente nesse caso é necessário alterar manualmente a instância na configuração do sensor. Alguns sistemas como roteadores da Cisco que executam o iOS podem ser configurados para utilizar um valor de índice permanente para que o NMS não precise resolver esse tipo de situação (CISCO, 2003).

4.1 EXTENSÕES

Apesar do sistema atender todos os objetivos que foram especificados, podem ser sugeridos uma série de extensões deste projeto:

a) inicialmente, desenvolver uma forma de resolver o problema descrito como limitação na seção 4, em relação ao endereçamento dinâmico do índice das interfaces de rede em alguns sistemas operacionais/dispositivos;
b) permitir a criação de mais de um limiar por sensor, conforme limitação descrita na seção 4;
c) alterar o sistema para permitir a consulta de vários sensores em paralelo, pois atualmente o sistema faz a consulta na forma de uma fila, e se houverem muitos sensores cadastrados essa pode não ser a forma ideal;
d) localizar e utilizar uma biblioteca de gráficos mais adequada para o sistema, por exemplo uma que permita criar sensores agregados e gerar um gráfico com vários intervalos de valores, como por exemplo tráfego de ingresso e egresso no mesmo gráfico de uma interface de rede;
e) implementar a recepção de *traps* SNMP no NMS, para receber alertas de comunicação iniciada pelos dispositivos de rede;
f) fazer alterações no script get.php que é responsável pelo envio de email e pela coleta de dados para que este script seja executado como um serviço do Windows, eliminando a necessidade de logon interativo para executar o serviço de monitoramento do NMS.

REFERÊNCIAS

ADREM. **Monitoring Network Infrastructure.** [S.l], 2012. Disponível em: <http://www.adremsoft.com/netcrunch/page/infrastructure-monitoring>. Acessado em: 02 dez. 2012

ALBUQUERQUE, Fernando. **TCP/IP internet:** protocolos e tecnologias**.** Rio de Janeiro: Axcel Books, 1998.

APACHE. **About the Apache HTTP server project.** [S.l], 2012. Disponível em: <http://httpd.apache.org/ABOUT_APACHE.html>. Acessado em: 04 nov. 2012

BRUEGGMAN, Elliot. **PHPGraphLib Graphing Library.** [S.l], 2011. Disponível em: <http://www.ebrueggeman.com/phpgraphlib>. Acessado em: 17 nov. 2012

CACTI. **What is Cacti**? [S.l.], 2012. Disponível em: <http://www.cacti.net/what_is_cacti.php>. Acessado em: 13 nov. 2012

CISCO. **Overview of basic SNMP building blocks**. [S.l.], [2000?]. Disponível em: <http://www.cisco.com/en/US/docs/ios/internetwrk_solutions_guides/splob/guides/dial/dial_nms/snmpover.pdf>. Acessado em: 15 abr. 2012

CISCO. **Interface Index Persistence**. [S.l.], [2003?]. Disponível em: <http://www.cisco.com/en/US/docs/ios/12_1t/12_1t5/feature/guide/dt5ifidx.pdf>. Acessado em: 13 nov. 2012

GUILLERMO, Oscar. **Uso de agentes SNMP para monitoramento de servidores e equipamentos de rede com mobilidade.** 2008. 72f. Trabalho de Conclusão (Curso de Especialização em Tecnologias, Gerência e Segurança de Redes de Computadores) – Universidade Federal do Rio Grande do Sul, Porto Alegre.

IANA. **Private Enterprise Numbers.** [S.l], 2012. Disponível em: <http://www.iana.org/assignments/enterprise-numbers>. Acessado em: 02 set. 2012

INTERNET ENGINEERING TASK FORCE. **A simple network management protocol (SNMP)**. [S.l.], 1990. Disponível em: <http://www.ietf.org/rfc/rfc1157.txt?number=1157>. Acessado em: 14 abr. 2012

KOZIEROK, Charles. **The TCP/IP guide - overview and history of the TCP/IP internet standard management framework and simple network management protocol (SNMP).** [S.l.], 2005. Disponível em: <http://www.tcpipguide.com/>. Acessado em: 14 abr. 2012

KUROSE, James F. **Redes de Computadores e a Internet.** São Paulo: Pearson Addison Wesley, 2005.

MOZILLA. **JavaScript**. [S.l.], 2012. Disponível em: <https://developer.mozilla.org/en-US/docs/JavaScript>. Acessado em: 13 nov. 2012

ORACLE. **MySQL Data Sheet.** [S.l], 2012. Disponível em: <http://www.oracle.com/us/products/mysql/mysql-enterprise-ds-067312.pdf>. Acessado em: 02 dez. 2012

PHP. **PHP Manual.** [S.l], 2012. Disponível em: <http://www.php.net/manual/en/preface.php>. Acessado em: 04 nov. 2012

PÉRICAS, Francisco Adell. **Redes de Computadores:** Conceitos e a Arquitetura Internet. 2.ed. Blumenau: Edição do Autor, 2010

REFSNES. **Javascript and HTML DOM Reference.** [S.l], 2012. Disponível em: <http://www.w3schools.com/jsref/>. Acessado em: 02 dez. 2012

SCHULZ, Murilo. **Protótipo de software de gerência de desempenho de um Access Point de rede sem fio utilizando o protocolo SNMP** . 2004. Trabalho de Conclusão de Curso (Engenharia de Telecomunicações) – Centro de Ciências Tecnológicas, Universidade Regional de Blumenau, Blumenau.

STALLINGS, William. **Redes e Sistemas de Comunicação de Dados**. Rio de Janeiro : Campus, 2005.

STALLINGS, William. **SNMP, SNMPv2, SNMPv3, and RMON 1 and 2.** 3.ed. Boston : Addison-Wesley, 1999.

STANGE, Rodrigo. **Ferramenta para gerenciamento de falhas em rede ethernet baseada em protocolo SNMP** . 2008. 66 f. Trabalho de Conclusão de Curso (Engenharia de Telecomunicações) – Centro de Ciências Tecnológicas, Universidade Regional de Blumenau, Blumenau.

WORXWARE. **PHP Mailer.** [S.l], 2009. Disponível em: <http://phpmailer.worxware.com/>. Acessado em: 17 nov. 2012

APÊNDICE A – Descrição dos Casos de Uso

Este Apêndice apresenta a descrição dos principais casos de uso descritos na seção 3.2.3 deste trabalho. O Quadro 06 apresenta o caso de uso Controlar Acesso ao Sistema.

UC01 – Fazer Logon Sistema
Ator: Administrador/Operador(Usuário)
Objetivo: Fazer *logon* no sistema
Pré-condições: Usuário Cadastrado
Pós-condições: Usuário tem uma sessão ativa no sistema

Cenário Principal:
1. Usuário acessa a página de *logon* do sistema em um navegador web
2. Sistema solicita as credenciais (email e senha) do usuário através de um formulário
3. Usuário informa seu email e senha no formulário e clica sobre o botão "Submit"
4. Sistema valida as credenciais fornecidas e redireciona o usuário a página de ínicio, se o usuário for um usuário do tipo "administrador" existe opções adicionais no menu

Cenário Alternativo 01:
No passo 3 o usuário informa credenciais inválidas:
1. Sistema apresenta mensagem "Usuário ou senha incorreta."
2. Sistema solicita novamente as credenciais através de um formulário.
3. Usuário informa credenciais validas e clica sobre o botão "Submit"
4. Volta ao passo 4 do cenário principal

Quadro 6 - Caso de Uso Controlar Acesso ao Sistema

No Quadro 07 pode ser visto o detalhamento do caso de uso Gerenciar Usuários.

UC02 – Gerenciar Usuários
Ator: Administrador
Objetivo: Cadastrar ou Excluir um Usuário do Sistema
Pré-condições: Usuário membro de Administradores com sessão ativa no sistema
Pós-condições: Usuário novo cadastrado ou excluido

Cenário Principal:
1. Usuário pretende cadastrar um novo usuário.
2. Usuário acessa a opção "Usuários"
3. Sistema apresenta um formulário de criação de novo usuário e os usuários atualmente cadastrados
4. Usuário informa o Nome, Email, Senha e informa se o novo usuário é administrador, em seguida clica em "Submit"
5. Sistema cadastra um novo usuário com as propriedades informadas

Cenário Alternativo 01:
No passo 1 do cenário principal o usuário pretende excluir um usuário:
1. Usuário acessa a opção "Usuários"
2. Sistema apresenta um formulário de criação de novo usuário e os usuários atualmente cadastrados
3. Usuário clica sobre o "X" da linha correspondente ao usuário que ele pretende excluir
4. Sistema exclui aquele usuário

Quadro 7 - Caso de Uso Gerenciar Usuários

No Quadro 08 pode ser visto o detalhamento do caso de uso Gerenciar Sensores.

UC03 – Gerenciar Sensores
Ator: Administrador
Objetivo: Cadastrar, Alterar ou Excluir Sensores

Pré-condições: Usuário membro de Administradores com sessão ativa no sistema
Pós-condições: Sensor é Criado, Alterado ou Excluido

Cenário Principal:
1. Usuário pretende cadastrar um novo sensor
2. Usuário acessa no menu a opção "Gerenciar Sensores"
3. Usuário informa todos os campos solicitados (Nome, IP, Porta, Comunidade, OID, Escala e Unidade) e clica em "Submit"
4. Sistema cadastra o novo sensor e ele é exibido no fim da lista de sensores cadastrados

Cenário Alternativo 01:
No passo 3 do cenário principal o usuário deixa de informar algum campo obrigatório:
1. Sistema apresenta mensagem "Não foi possível cadastrar. Verifique os campos."
2. Usuário clica novamente sobre a opção "Gerenciar Sensores" e desta vez informa todos os campos no formulário
3. Volta ao passo 4 do cenário principal

Cenário Alternativo 02:
No Passo 1 do cenário principal o objetivo do usuário é editar um sensor
1. Usuário acessa a opção de menu "Gerenciar Sensores"
2. Usuário visualiza a lista de sensores cadastrados
3. Usuário clica sobre a letra "E" da linha correspondente ao sensor que ele pretende editar
4. Sistema preenche os campos de formulário com os valores do sensor atual
5. Usuário faz a alteração desejada e clica em Submit
6. Sistema grava as alterações feitas pelo usuário

Cenário Alternativo 03:
No Passo 1 do cenário principal o objetivo do usuário é excluir um sensor
1. Usuário acessa a opção de menu "Gerenciar Sensores"
2. Usuário visualiza a lista de sensores cadastrados
3. Usuário clica sobre o "X" da linha correspondente ao sensor que ele pretende excluir
4. Sistema exclui aquele sensor

Quadro 8 - Caso de Uso Gerenciar Sensores

No Quadro 9 é apresentado o detalhamento do caso de uso Visualizar Sensores.

UC04 – Visualizar Sensores
Ator: Administrador/Operador (Usuário)
Objetivo: Visualizar os dados de monitoramento de um sensor
Pré-condições: Usuário tem sessão ativa no sistema
Pós-condições: Usuário visualizou as estatísticas do monitoramento de um sensor específico

Cenário Principal:
1. Usuário acessa a opção "Visualizar Sensores".
2. Usuário acessa a opção "Usuários"
3. Sistema apresenta o gráfico do último dia de todos sensores cadastrados
4. Usuário localiza através do nome o Sensor que ele gostaria de visualizar em detalhes
5. Usuário clica sobre o sensor que ele gostaria de visualizar em detalhes
6. Sistema apresenta o Nome, Valor Atual e data dessa leitura, além dos gráficos do último dia e da última hora para aquele sensor
7. Usuário pode clicar sobre um dos gráficos para retornar ao "índice" de sensores
8. Usuário pode clicar sobre um outro sensor para visualizar algum outro sensor

Cenário Alternativo 01:
No Passo 3 do cenário principal se o usuário não tiver acesso a nenhum sensor ou se não houver nenhum sensor cadastrado
1. Usuário não visualiza gráfico algum pois não tem acesso

Quadro 9 - Caso de Uso Visualizar Sensores

No Quadro 10 abaixo é detalhado o caso de uso Configurar Sistema.

UC05 – Configurar Sistema
Ator: Administrador
Objetivo: Alterar/Configurar os parâmetros globais do Sistema
Pré-condições: Usuário membro de Administradores com sessão ativa no sistema
Pós-condições: Parâmetros globais configurados

Cenário Principal:
1. Usuário acessa a opção "Sistema"
2. Sistema apresenta a configuração atual de email e de intervalo de monitoramento
3. Usuário pode alterar ou cadastrar as configurações do sistema, em seguida pressionar "Submit"
4. Sistema grava as alterações, que são usadas no monitoramento

Quadro 10 – Caso de Uso Configurar Sistema

No Quadro 11 está descrito o caso de uso Criar Limiar de Sensor.

UC06 – Criar Limiar de Sensor
Ator: Administrador/Operador (Usuário)
Objetivo: Visualizar os dados de monitoramento de um sensor
Pré-condições: Usuário tem acesso a um sensor específico e sessão ativa no sistema
Pós-condições: Limiar de notificação de Sensor Cadastrado para aquele usuário

Cenário Principal:
1. Usuário acessa a opção "Visualizar Sensores"
2. Usuário clica sobre o gráfico de um dos sensores no índice
3. Sistema apresenta os detalhes do Sensor e três campos relativos ao Limiar (Limiar, Tipo, Descrição)
4. Usuário informar um valor para o limiar, informa se a notificação ocorrer quando o valor da leitura for maior ou menor do que o valor do limiar e a descrição do evento.
5. Usuário clica em Submit
6. Sistema grava aquela configuração de Limiar
7. Sistema apresenta os gráficos do sensor e as informações de Limiar já gravadas

Quadro 11 - Caso de Uso Criar Limiar de Sensor

No Quadro 12 está descrito o funcionamento do caso de uso Gerenciar Acesso Sensores.

UC07 – Gerenciar Acesso Sensores
Ator: Administrador
Objetivo: Definir as permissões de acesso de cada usuário aos sensores
Pré-condições: Usuário membro de Administradores com sessão ativa no sistema
Pós-condições: Definidas as permissões de acessos dos sensores x usuários.

Cenário Principal:
1. Usuário acessa a opção "Gerenciar Acesso Sensores"
2. Sistema apresenta a matriz de acesso de todos usuários e sensores
3. Usuário informa (Marca o checkbox) dos sensores ao qual um determinado usuário deve ter acesso. Para remover algum acesso, usuário desmarca o checkbox
4. Após fazer todas as alterações, usuário clica na opção "Submit"

Quadro 12 - Caso de Uso Gerenciar Acesso Sensores

No Quadro 13 pode ser visto o detalhamento do caso de uso Adicionar Sensor Wizard.

UC08 – Adicionar Sensor Wizard
Ator: Administrador
Objetivo: Cadastrar Sensores
Pré-condições: Usuário membro de Administradores com sessão ativa no sistema
Pós-condições: Sensor é cadastrado

Cenário Principal:

1. Sistema solicita Nome, IP, Porta e Comunidade (Sendo que Porta e Comunidade tem valor default definido)
2. Usuário informa Nome e IP
3. Usuário clica sobre o botão "Avançar"
4. Sistema solicita o tipo do Sensor (CPU / Memória/Armazenamento / Rede Ingresso / Rede Egresso)
5. Usuário seleciona o tipo e clica em "Avançar"
6. Sistema apresenta todas as instanciais disponíveis daquele tipo de monitoramento. (Interfaces de Rede, Discos, etc)
7. Usuário seleciona uma instancia em clica em "Avançar"
8. Sistema apresenta um resumo das configurações informadas e do sensor a ser criado
9. Usuário clica em "Concluir" para gravar o novo sensor ou "Voltar" para fazer alguma alteração

Cenário Alternativo 01:

No Passo 2 do cenário principal o usuário informa um IP onde o serviço SNMP não está em execução ou o IP de um host que não está ativo na rede.

1. Usuário clica sobre o botão Avançar
2. Sistema apresenta mensagem: "Host não respondeu, verifique se ele está ligado e se o SNMP está habilitado"
3. Usuário informa um IP de host valido ou habilita o SNMP naquele dispositivo e clica novamente em "Avançar".
4. Retorna ao passo 4 do caso principal.

Quadro 13 – Caso de Uso Adicionar Sensor Wizard