Desenvolvimento de Sistema para Monitoramento de Redes de Computadores e Servidor *Looking Glass*

Ednardo Ferreira de Miranda

Rio de Janeiro, RJ - Brasil 22 de Novembro de 2013

Desenvolvimento de Sistema para Monitoramento de Redes de Computadores e Servidor *Looking Glass*

Ednardo Ferreira de Miranda

Dissertação apresentada a Coordenação de Formação Científica do Centro Brasileiro de Pesquisas Físicas para a obtenção do título de Mestre no programa Mestrado Profissional em Física com ênfase em Intrumentação Científica.

Membros da banca examinadora:

Nilton Alves Júnior, D.Sc. - (Orientador)

Márcio Portes de Albuquerque, D.Sc. - (CBPF)

Artur Ziviani, D.Sc. - (LNCC)

Rio de Janeiro, RJ - Brasil 22 de Novembro de 2013

Dedicatória:
À minha família que sempre me apoiou em minhas decisões.

Resumo

Neste trabalho, são descritos dois sistemas de informação, com finalidades de apoiar a tomada de decisão na área de monitoração e gerência de dispositivos de rede.

Em ambos os sistemas foram utilizados diferentes mecanismos computacionais, voltados principalmente para ambientes de internet, sendo o principal, o conjunto LAMP: sistema operacional Linux, servidor HTTP Apache, banco de dados MySQL e linguagem de programação PHP. Com o primeiro sistema de informação foi possível armazenar, caracterizar e quantificar em gráficos, diferentes parâmetros de monitoramento nos equipamentos de rede do projeto RedeRio de Computadores.

Além disto, o sistema mantém uma base de dados com informações administrativas das fontes de informação que alimentam o sistema, resumidas em empresas públicas associadas ao projeto. Destacam-se neste sistema, o mecanismo de aquisição de dados e o conjunto de interface com o usuário, que fornece ao operador do sistema um poder de um volume de ações mais abrangente do que outros sistemas do mesmo gênero.

O segundo sistema de informação, conhecido na internet como servidor *Looking Glass*, permite uma variedade de consultas sobre roteamento na internet, testes de alcance e de tempo de resposta. Neste sistema destaca-se um repositório, organizado de forma compacta e cronológica, com informações sobre as tabelas de rotas obtidas periodicamente do roteador de borda da RedeRio de Computadores.

Palavras-chave: Sistemas de informação, monitoramento e gerência de equipamentos, *looking glass server*, repositório, roteador de borda.

Abstract

The present study describes two information systems aimed at supporting decision taking in network monitoring and management of net devices.

In both systems different computational mechanisms been used applied, mainly directed to internet environments, such as LAMP set: Linux operating system, Apache HTTP Server, MySQL database and PHP programming language. With the first information system, it was possible to store, characterize and quantify in graphics different monitoring parameters in the network equipment of the RedeRio de Computadores project.

In addition, the system stores a database with administrative information of sources that feed it, summarized in public companies associated with the project. Highlights in this system are the data acquisition mechanism and the set of user interface which provides to the operator the power of volume of actions broader than other systems of the same type.

The second information system, known on the internet as Looking Glass server, allows a variety of consultations on internet routing, reach tests and response time. This system highlights a repository, which is organized in a compact and chronological manner, with information on the routing tables periodically obtained from the RedeRio de Computadores border gateway.

Keywords : Information systems, network monitoring and management, repository, border gateway, looking glass server.

Agradecimentos

À minha esposa por sempre ter me incentivado a seguir adiante e me apoiado em cada decisão minha, mesmo não sendo, certas decisões, as melhores.

Aos meus irmãos, todos mais velhos que ajudaram meus pais em minha criação e desta maneira colaboraram na construção do meu carácter. Ao meu pai Antonio, que hoje não está mais aqui, por ter me dado o sustento e abrigo até o dia que saí de casa para fazer o mestrado; a minha mãe Teresa pela eterna preocupação com minha educação; ao meu irmão Paulo por sempre lutar por mim, como hoje luta por seus filhos; a minha irmã Juliete por me ajudar nas tarefas da escola e por se preocupar com a minha saúde; a minha irmã Rose pelos sábios conselhos; ao meu cunhado Edson que considero como irmão, obrigado pelas caronas nas madrugadas frias de Petrópolis ao Rio; a minha cunhada Diva que muito colaborou para minha educação, nos meus primeiros passos na escola.

À profª Adriana Racco do LNCC por ter me apresentado à pesquisa física e desta maneira me aproximar do CBPF. Ao meu orientador Nilton por idealizar os projetos e acreditar que eu seria capaz de desenvolvê-los. Ao Nilton também agradeço por ser meu amigo de trabalho e conviver comigo profissionalmente; estendo este agradecimento aos tecnologistas Marcelo, Márcio, Marita, Jabur e Pablo, pela oportunidade de trabalharmos juntos, cuja convivência me proporcionou elevados valores técnicos e científicos. Ao técnico Leandro pela fundamental ajuda com as linguagens de programação, ao técnico Jaime pelas parcerias e importantes conselhos para o desenvolvimento dos projetos. E a todos os colegas da CAT pelo

companheirismo e descontração nos horários de pausa do trabalho.

Aos professores do mestrado profissional que exigem alto nível de conhecimento de seus alunos, elevando desta forma, o nível de reconhecimento do programa do mestrado profissional. Em especial, aos professores Luis Sampaio, Márcio, Marcelo, Herman, Geraldo, Nilton e Laudo. Este último, que hoje não está mais aqui, gostaria de dizer que graças a ele, hoje sei um pouco de eletrônica básica.

Aos meus amigos mestres pelo programa do mestrado profissional: Arídio, Rafael, Artur, Fernando, Antonio e Victor. Este último por ter sido meu colega de quarto. Ao Antonio por esclarecer dúvidas importantes no projeto, ao Artur e Arídio pela descontração em momentos de estresse, ao Rafael por esclarecer minhas dúvidas na disciplina de eletrônica, ao Fernando, por todos os momentos difíceis e alegres que passamos juntos no CBPF e em nossas vidas pessoais. E a todos por compartilharem comigo suas sinceras amizades.

Ao meu amigo, parceiro de publicação e colega de profissão Marcelo Giovani pelos preciosos conselhos profissionais e pessoais.

Agradeço ao CBPF por oferecer, não só para mim, mas para centenas de alunos, a oportunidade de crescimento acadêmico e profissional. A RedeRio de computadores, agradeço pela oportunidade de atuar nos laboratórios de redes e pelo apoio no desenvolvimento do trabalho e ao CNPq agradeço pelo apoio financeiro.

Nomenclatura

Siglas

B	*Bytes*
BGP	*Border Gateway Protocol*
CERN	*Conseil Européen pour la Recherche Nucléaire*
CGI	*Common Gateway Interface*
CPU	*Central Processing Unit*
FRT	*Full Routing Table*
GB	*Gigabytes*
HTML	*Hypertext Mark-up Language*
HTTP	*Hypertext Transfer Protocol*
ICMP	*Internet Control Message Protocol*
IETF	*Internet Engineering Task Force*
ISO	*International Organization for Standartization*
IP	*Internet Protocol*
LA	*Load Average*
LAMP	Linux, Apache, MySQL e PHP
LG	*Looking Glass*
MIB	*Management Information Base*
MRTG	*Multi Router Traffic Grapher*
OID	*Object Identifier*
PDU	*Protocol Data Unit*

PHP	*Hypertext Preprocessor*
RRD	*Round Robin Database*
SAD	Sistema de apoio a decisão
SCP	*Secure Copy*
SFTP	*Secure File Transfer Protocol*
SGMP	*Simple Gateway Monitoring*
SNMP	*Simple Network Management Protocol*
SQL	*Structured Query Language*
SSH	*Secure Shell*
TCP	*Transmission Control Protocol*
TTL	*Time To Live*
URL	*Uniform Resource Locator*
WWW	*World Wide Web*

Conteúdo

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

Com o avanço da tecnologia em serviços oferecidos pela internet, redes de computadores se tornaram pontos críticos nas organizações que estão cada vez mais dependentes da conexão de seus equipamentos de rede com a grande internet.

Após a comercialização da internet e a acessibilidade dos computadores nos anos 90, a internet experimentou um extraordinário crescimento de usuários, figura 1.1, na página 2, se tornando um importante canal de comunicação para todo o mundo. Em paralelo ao crescimento de usuários, os equipamentos de infraestrutura de rede sofreram evoluções para atenderem essa imensa demanda de usuários.

O ambiente acadêmico, com o passar dos anos, começou a dar grande importância ao estudo de redes de computadores, em especial, ao monitoramento e gerência de redes, uma área que se preocupa, dentre outros assuntos, com as atividades, procedimentos e ferramentas que dizem respeito a operação, administração e manutenção de infraestruturas e serviços em rede [1].

Há vários exemplos de utilização da internet para diferentes finalidades, que vão deste de compras de produtos, interações com comunidades de relacionamento diversas e consultas a mapas de cidades distantes até cursos de graduações e pós-graduações a distância.

Consequentemente, as redes de computadores locais e metropolitanas pas-

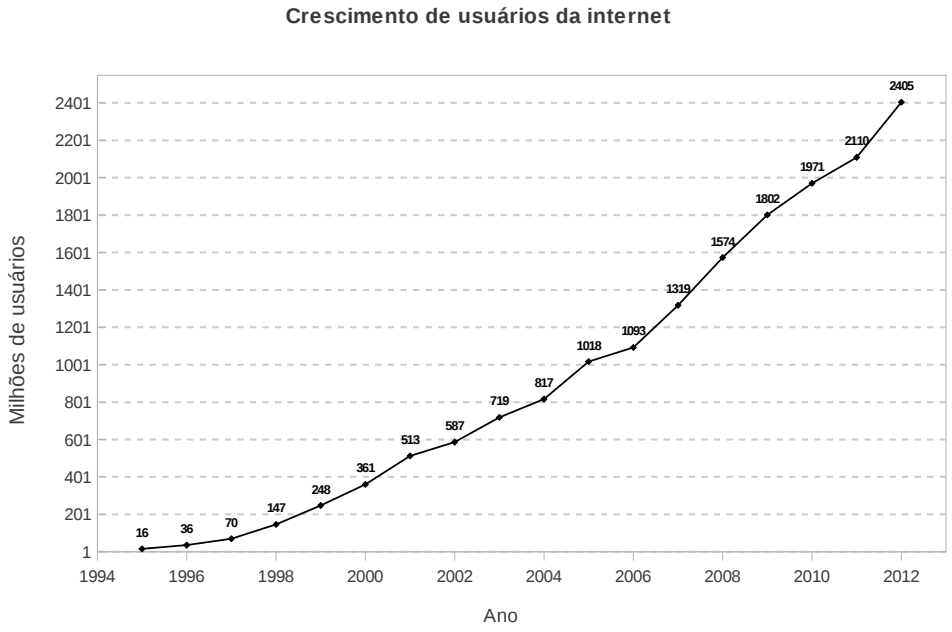

Figura 1.1: Crescimento de usuários conectados à internet desde a sua comercialização nos anos 90. O rápido crescimento afirma o que é dito na literatura e reflete a sua rápida popularização. Fonte dos dados: `http://www.internetworldstats.com`.

saram a conter uma quantidade de equipamentos que requerem a utilização de sistemas de medidas que informem visualmente o panorama atual da rede.

A motivação para o estudo destes sistemas é o problema enfrentado pelas organizações de diversos setores em manter suas redes de computadores e serviços *online* disponíveis o tempo todo.

Outra motivação deste trabalho é um tipo de sistema, conhecido na internet por servidor *Looking Glass*. Uma característica interessante deste tipo de sistema é oferecer dentre outras utilidades, a visualização da internet global sobre diferentes perspectivas, ou seja, um olhar "local" da internet no globo.

O objetivo deste trabalho é apresentar o desenvolvimento e descrever as principais características de um sistema de monitoramento de redes cujo papel é auxiliar administradores de redes nas tomadas de decisões.

Este sistema de monitoramento é composto de dois sistemas diferen-

tes, batizados de Gerenciamento da RedeRio *web* versão Linux, GRRWX, e RedeRio *Looking Glass*, RRLG. O primeiro tem a finalidade de armazenar informações corporativas de uma rede metropolitana e apresentar por meio de gráficos, as estatísticas de tráfego entre os equipamentos e as várias redes locais desta rede metropolitana. Pretende-se com a utilização deste sistema, realizar a gerência e o monitoramento de equipamentos, fornecendo dados sobre o comportamento do tráfego da rede, auxiliando desta forma, os administradores em suas decisões.

O segundo sistema, RRLG, tem a finalidade de adquirir e organizar periodicamente, tabelas de rotas ou *Route Information Base*, RIB, geradas pelo *Border Gateway Protocol* ou simplesmente BGP. Espera-se com este sistema, disponibilizar um repositório nos moldes de repositórios disponíveis na comunidade. Por meio deste sistema, podem ser feitas consultas às cópias das tabelas de rotas BGP e o interessado terá acesso à informações como: o tamanho da tabela de roteamento, o caminho entre os diversas sistemas autônomos presentes em uma rota anunciada, testes de conectividade e alcance do roteador BGP até uma rede qualquer, entre outras.

Destaca-se como metas deste trabalho:

- O aprendizado em Redes de Computadores.
- Caracterização do tráfego de pacotes TCP/IP em redes metropolitanas.
- A aquisição periódica e a organização das tabelas de rotas do roteador de um importante roteador de borda.

Espera-se que este trabalho seja de grande valor e contribuição para a área de gerência e monitoramento de redes porque envolve assuntos fundamentais como:

- Aplicação de metodologia para aferir a taxa média de bits por segundo que trafegam pelas interfaces dos equipamentos de redes monitorados.
- Criação de um banco de dados para armazenar um histórico de medidas, para que no futuro sejam recuperadas informações sobre variações no fluxo de dados ou quedas de serviço.

- Criação de um mecanismo aberto na internet para consultas sobre o roteamento na internet, testes de alcance e de tempo e resposta.
- Criação de um repositório de dados adquiridos dos equipamentos que executam o roteamento na internet. Tal repositório é de grande valia tanto para os operadores de rede quanto para a comunidade acadêmica/ científica da área.

1.1 Instrumentação Científica

O desenvolvimento de novos instrumentos científicos permite o avanço e a renovação de ideias com mudanças visíveis em todas as classes da sociedade [2]. É possível citar, como exemplos, a invenção do gerador de raios-X, o laser, os reatores nucleares, os aceleradores de partículas, o *world wide web*, etc.

No ambiente da instrumentação científica, o Centro Brasileiro de Pesquisas Físicas, CBPF, se posiciona como um instituto de pesquisa que busca o desenvolvimento, transferência de tecnologia e inovação em diversas áreas. Alguns projetos de instrumentação científica realizados pelo CBPF são:

- Desenvolvimento de eletrônica para detecção de partículas [3, 4],
- Pesquisa e desenvolvimento de materiais nanoscópicos [5],
- Processamento de sinais e imagens aplicados à detecção de eventos em reatores de fusão nuclear [6],
- Desenvolvimento de protótipo para monitoramento ambiental [7],
- Sistema para aquisição de dados em alta velocidade com lógica programável [8],
- Desenvolvimento de sistema de monitoramento de redes por meio do protocolo *spanning tree* [9].

A conduta para o desenvolvimento de muitos dos sistemas desenvolvidos nestes projetos, certamente demanda ambientes de infraestrutura muitas vezes complexos e dispendiosos, como visto no CBPF e em outras instituições [10, 11, 12]. Em muitos casos é possível associar a esta demanda

uma instrumentação que está no nível dos sistemas de aquisição de dados. As informações fornecidas por estes sistemas, a respeito das operações dos equipamentos de redes, podem auxiliar os administradores na tomada de decisão a respeito de ações, ativas e proativas, contra possíveis falhas de segurança e na própria infraestrutura de rede sobre sua responsabilidade.

Um dos principais objetivos das redes metropolitanas que interligam diversas universidades e centros de pesquisas é prover a conexão e o suporte a diversos tipos de serviços que demandam transmissão de dados via rede. Dentre os diversos benefícios que redes deste tipo oferecem estão a criação de produtos e serviços. Como por exemplo:

- *Grids* computacionais. Necessários por exemplo, para a colaboração entre institutos de pesquisa que demandam velocidade transmissão e capacidade de processamento de informações de diferentes experimentos científicos.
- A telemedicina e a videoconferência. Em geral, os equipamentos que permitem este tipo de comunicação realizam transmissões audiovisuais e permitem a troca de informações e atenção médica a pacientes distantes.

Para que estas redes evoluam para um alto nível de disponibilidade e desempenho, uma instrumentação baseada em medidas, quantitativas e qualitativas de rede se faz necessário. Com a implantação desta instrumentação, perguntas importantes podem ser respondidas, como por exemplo:

- Como está neste momento a disponibilidade desta rede?
- Qual o tempo mínimo de resposta entre dois pontos extremos da rede?
- Qual o valor da vasão da rede neste momento?
- Qual é a capacidade real de transmissão desta rede?

Sendo assim, este trabalho contribui de duas formas para a instrumentação científica. A primeira contribuição é o desenvolvimento de uma nova ferramenta para monitoramento de redes, de caráter específico, capaz de oferecer

um volume de ações mais abrangente do que outros sistemas do mesmo gênero. Por exemplo, a maioria dos sistemas relacionados não permitem a associação de dados corporativos referentes as interfaces dos equipamentos.

A segunda contribuição deste trabalho é a disponibilidade de tabelas por meio de um repositório de tabelas de rotas BGP desenvolvido. Tal repositório é de grande valia tanto para os operadores de rede quanto para a comunidade acadêmica/científica da área, o que torna o trabalho de grande contribuição prática.

1.2 Sistemas relacionados

Desenvolvidos principalmente por comunidades científicas, os serviços disponíveis na internet e até mesmo o sistema *world wide web*, www, desenvolvido por pesquisadores do *Conseil Européen pour la Recherche Nucléaire* CERN, tiveram suas primeiras aplicações nas universidades e institutos de pesquisa.

O avanço da tecnologia tem levado ao surgimento de novos grupos de estudo, que utilizam como base, a internet e seus serviços. Esses grupos se preocupam, dentre outros assuntos, com a disponibilidade destes serviços.

Ainda na década de 80, a organização *Internet Engineering Task Force* conhecida pela sigla IETF , começou a desenvolver o protocolo *Simple Network Management Protocol*, SNMP, com o objetivo de facilitar o monitoramento e controle de equipamentos em uma rede de computadores.

Após a firmação do protocolo SNMP [13], pesquisadores e empresas divulgam, frequentemente, novos *softwares* de monitoramento baseados neste protocolo, visando difundir e compartilhar seus produtos e resultados. É o caso de alguns *softwares* de fins comerciais ou não, como os sistemas MRTG (*Multi Router Traffic Grapher*)[14], Cacti [15] e Nagios [15].

Contudo, o sucesso destas ferramentas dependeu do êxito de outras ferramentas e sistemas. A impulsão do *software* livre, no começo dos anos 90, surpreendeu os desenvolvedores e usuários que passaram a contar com a adoção de uma política livre para o desenvolvimento de *softwares*. Assim, uma comunidade de desenvolvedores, habitando principalmente instituições

acadêmicas, começou a disponibilizar seus produtos para que outros membros, em outros lugares, usassem livremente.

Foi assim que surgiram muitos dos sistemas conhecidos hoje, como: o sistema operacional Linux , o servidor *web* Apache , o banco de dados MySQL e a linguagem de programação PHP. Juntos, esse conjunto, conhecido por servidor LAMP, oferece suporte para a maioria dos *softwares* de monitoramento e gerência disponíveis.

O sistema MRTG, no final dos anos 90, se tornou referência para sistemas de monitoramento. Foi assinado por Tobias Oetiker[1] que também foi coautor da importante ferramenta RRDtool, responsável pelo armazenamento das consultas de monitoramento , explicada mais adiante. O MRTG foi o precursor deste modelo de sistemas de monitoramento e gerência sobre plataforma *web* e sua metodologia para a aquisição de medidas de monitoramento é a mesma utilizada, por muitos sistemas, até hoje.

O sistema Cacti , também assinado por Tobias Oetiker, é uma evolução do MRTG. Tem uma interface amigável com o usuário e exibe bons gráficos sobre o tráfego de dados que circula pelos equipamentos. A vantagem sobre outros sistemas, é que o Cacti permite a adaptação de *plugins*. *Plugins* são programas auxiliares que atuam em paralelo com o programa principal. Um exemplo de *plugin* é a inserção de um mapa sensitivo da rede [2] sobre a base de dados do Cacti.

O Nagios foi desenvolvido logo após o Cacti e faz parte de uma categoria de sistemas que monitoram, principalmente serviços. A grande vantagem de sua utilização é a possível integração com o Cacti. Está cada vez mais comum nos dias atuais, utilizar o Nagios e o Cacti em conjunto. Fazendo uso desta configuração, o administrador tem um sistema que monitora o tráfego de dados e os serviços disponíveis em seus servidores simultâneamente.

Outro tipo de sistema que se destaca principalmente no campo de visualização e disponibilidade de tabelas de rotas BGP é o servidor *Route View*, que em alguns casos se confunde com servidor Looking Glass ou servidor LG.

[1] Na época, trabalhando no Instituto Federal de Tecnologia em Zurique, Suíça.

[2] Mapas sensitivos são vistos com muita frequência em redes metropolitanas, o administrador o utiliza para obter uma visão mais abrangente da rede.

A universidade de Oregon é pioneira no projeto Route View [16]. Este projeto envolve diversas operadoras de internet localizadas em diferentes locais no mundo. O projeto foi originalmente concebido como uma ferramenta para operadores de internet para obter informações em tempo real sobre o sistema de roteamento global a partir das perspectivas de vários sistemas autônomos ao redor da internet. Atualmente, o projeto conta com aproximadamente 17 colaboradores e com um repositório de dados com informações de rotas BGP atualizadas periodicamente, deste o ano de 1997.

Com o passar do tempo, o projeto passou a receber atenção da comunidade científica que passou a utilizar os dados obtidos no repositório para estudar diferentes assuntos como:

- A utilização do espaço de endereços IPv4 [17, 18].
- A evolução da tabela BGP [19].
- Desenvolvimento de modelos matemáticos que simulam problemas científicos em diversas áreas do conhecimento [20].
- Desenvolvimento de ferramentas para detecção de falhas de segurança e fontes maliciosas [21, 22].

Neste breve histórico, foram destacados, ordenadamente, alguns dos sistemas de monitoramento de redes de computadores e servidores *Looking Glass* estudados e algumas referências bibliográficas que serviram de base para este trabalho.

Os motivos que levaram a realização deste trabalho foram:

- Desenvolver e implantar um sistema de gerência e monitoramento de redes específico que atenda à necessidades operacionais e administrativas de uma rede de computadores de dimensão metropolitana.
- Desenvolver um servidor LG com dois propósitos distintos: o primeiro, de observar o comportamento da internet mundial sobre a perspectiva de um AS brasileiro por meio das tabelas rotas BGP armazenadas em um repositório BGP. E o segundo é permitir consultas sobre o roteamento na internet, testes de alcance e de tempo de resposta por meio de comandos BGP pré estabelecidos.

Este trabalho está organizado da seguinte forma: no capítulo 2, **Sistemas de Apoio à Decisão**, é apresentada a arquitetura relativa ao desenvolvimento dos sistemas, a justificativa científica do trabalho e a sua contribuição para a instrumentação científica;

No capítulo 3, **Principais Protocolos e Ferramentas utilizadas no Projeto**, são descritos os principais protocolos e ferramentas utilizadas no trabalho. Neste capítulo são discutidas a aplicabilidade e funcionalidades relevantes dos protocolos necessárias para compreender o desenvolvimento do trabalho.;

Nos capítulo 4 **RRLG - Principais características** e 5 **GRRWX - Principais características**, são descritos os principais mecanismos que compõem os sistemas. São apresentados fluxograma da estrutura de ambos os sistema e imagens capturadas da interface com usuário, bem como gráficos com taxas de utilização dos recursos computacionais de cada um separadamente.

No capítulo 6, **Conclusões**, as conclusões sobre cada sistema desenvolvido separadamente e os trabalhos futuros.

Todos os módulos que compõem os sistemas desenvolvidos para este trabalho, foram desenvolvidos sobre a plataforma LAMP, com a distribuição Linux Fedora v9, Apache v2 , MySQL v5.0 e PHP v5; Net-SNMP v5.4.2.1 ; RRDtool v1.3.8; utilizados os editores Netbeans v6.9.1 para escrever os códigos PHP; Kompozer v0.8b3, para o desenvolvimento HTML e phpMyAdmin para gerenciar o banco de dados. Para compilar este documento foi utilizado o editor Kile v2.0.3 em conjunto com pdfTEX.

Capítulo 2

Sistemas de Apoio à Decisão

Sistemas de Apoio à Decisão ou SADs começaram a ser desenvolvidos na década de 70 e com o passar dos anos, migraram das grandes estações *mainframes* para computadores comuns e atualmente grande parte dos SDAs pode ser acessados por qualquer dispositivo de rede ou *host* conectado a internet.

Existem diferentes tipos de SADs, sendo ums dos mais importantes o SAD baseado em *web*. Conceitualmente, este tipo de sistema se refere a programas de computador desenvolvidos exclusivamente para serem operados via navegadores de internet [23]. Por meio destes sistemas é possível consultar, analisar e apresentar estruturas de dados recuperadas de pequenos ou grandes bancos de dados *on line*. Em geral, todas estas facilidades visam a comunicação e a tomada de decisão de um grupo de administradores ou empresários.

Um SAD baseado em *web* é hospedado em um dispositivo de rede ou *host* que dispõe de um servidor *web*. Os recursos contidos neste *host* podem ser acessadas pela internet por meio de seu endereço *Uniform Resource Locator*, URL. Grande parte dos SDAs baseados em *web* são desenvolvidos visando oferecer suporte a requisições *HyperText Markup Language* (HTML) via HTTP. Uma arquitetura típica desde tipo de sistema é apresentada pelo diagrama em bloco, representado pela Fig 2.1.

O funcionamento destes sistemas, se resumem nas interpretações e execuções

de scripts baseados em em linguagens de programação. As respostas são validadas e apresentadas pelo servidor *web* em um novo HTML ou outro mecanismo de saída padrão.

Entretanto, SADs que se propõem a fornecer informações em escala sobre monitoramento de redes de computadores, estão sujeitos a modelagem e requisitos que forneçam subsídios à informação e a performance operacional.

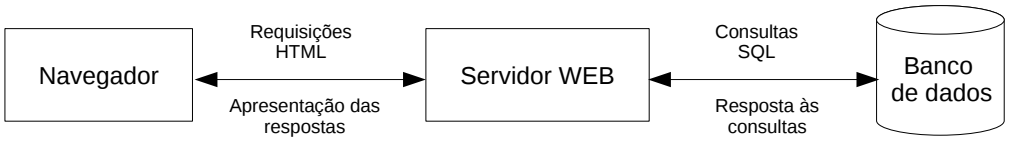

Figura 2.1: Arquitetura típica de sistemas de apoio a decisão *web*.

2.1 Alta Disponibilidade

Alta disponibilidade é um requisito para o desenvolvimento de projetos que garante a performance operacional de um conjunto de soluções durante um alto período de tempo. Projetos de infraestrutura de redes de computadores com esta característica são desenvolvidos visando a redução dos pontos de falhas a fim de conservar o sistema disponível o máximo de tempo possível.

Um importante trabalho sobre o tema [24], aponta que sistemas que oferecem disponibilidade de 99% ao ano sofreram em média interrupção de 100 minutos por semana. Do ponto de vista do referido autor, sistemas que requerem alta disponibilidade devem oferecer 99.999% de disponibilidade. Esta porcentagem permite um limite de 5 minutos de interrupção por ano.

A disponibilidade em sistemas pode ser classificada e mensurada de acordo com medidas de tempo de operação que se resumem em dois parâmetros:

- Tempo médio de recuperação. Esta medida revela a média de tempo que decorre entre a ocorrência da falha e a total recuperação do sistema ao seu estado operacional.

Tabela 2.1: Classificação dos níveis de disponibilidade de sistemas

Tipo de Sistema	Indisponibilidade (min por ano)	Disponibilidade
Não Gerenciado	50.000	90%
Gerenciado	5.000	99%
Bem gerenciado	500	99.9%
Tolerante à falhas	50	99.99%
Alta Disponibilidade	5	99.999%

- Tempo médio entre falhas. Esta medida é dada pelo tempo médio entre uma falha e outra do sistema.

Conhecendo estes dois parâmetros é possível realizar o cálculo da disponibilidade que é a relação de tempo entre a vida útil do sistema e o seu tempo total de vida.

A disponibilidade é normalmente expressa em porcentagem. Esta medida é distinta da medida de tempo que o sistema esteve ligado, pois o sistema poderia estar ligado porém não disponível.

A Tabela 2.1, na página 13, apresenta um comparativo entre níveis de disponibilidades, expressos em porcentagem e tempos de indisponibilidade. Segundo a literatura, [24, 25], esta tabela deve ser considerada como uma proposta, na qual sistemas podem ser classificados por níveis de disponibilidade que estão relacionados à sua magnitude de interoperabilidade anual.

- Sistemas considerados do tipo não gerenciados, saem do ar constantemente e em média demoram 10 horas para serem restabelecidos. Se todos os períodos de tempo em que estes sistemas estiveram fora do ar forem somados, em um ano, daria um total de aproximadamente 833 horas, ou quase 35 dias. Estes sistemas oferecem 90% de disponibilidade.

- Sistemas gerenciados saem do ar várias vezes por ano. Somados, todos estes períodos dariam cerca de 3 dias em meio de indisponibilidade.

- Sistemas tolerante à falhas saem do ar em média 8 horas por ano. Esta característica indica uma disponibilidade de 99.99%.

- Sistemas de alta disponibilidade admitem poucas falhas e rápido reparo. Os requerimentos de interoperabilidade não permitem falhas que somadas, ultrapassem 5 minutos por ano.

2.2 Gerência de Redes

Uma rede de computadores é um conjunto de muitos elementos de *hardware* e *software* que interagem uns com os outros [26]. Esta interação atinge desde as conexões físicas, *switches*, roteadores e demais dispositivos que compõem a estrutura física da rede, até os muitos protocolos que permitem controlar e coordenar este conjunto.

Quando uma rede de computadores, composta por dezenas ou centenas de elementos é implementada por alguma organização, acaba sendo factível que ocasionalmente, um ou outro elemento apresente problemas. Estes problemas podem ser consequentes da má configuração de algum elemento da rede, da alta taxa de utilização de algum componente ou até mesmo por defeitos de fabricação.

O administrador da rede que tem a tarefa de mantê-la funcionando, necessita de ferramentas que o auxiliem a monitorar, e manter a rede sobre controle.

Com o intuito de estruturar e padronizar os assuntos relativos a gerência de redes, a *International Organization for Standartization*, ISO, criou um modelo [27] que define cinco importantes tópicos dentro de gerenciamento de rede:

- Gerenciamento de desempenho. O objetivo deste tópico é quantificar, medir, informar, analisar e controlar o desempenho de diferentes elementos da rede. Entre esses elementos estão dispositivos de qualquer tipo com endereços de rede válidos e autorização de acesso.

- Gerenciamento de falhas. A meta do gerenciamento de falhas é registrar, detectar e reagir às condições de falha da rede. O limite entre gerenciamento de falhas e de desempenho é indefinido. Autores

importantes, [26, 28], consideram o gerenciamento de falhas como o tratamento imediato de uma interrupção de serviço ou algum dispositivo enquanto que o gerenciamento de desempenho adota uma abordagem de médio/longo prazo sobre as ocasionais falhas em relação a rede. O gerenciamento de falhas aponta os seguintes passos para a rápida solução de uma falha:

1. Isolar o problema através de ferramentas que determinem seus sintomas.
2. Resolver o problema.
3. Gravar em um histórico de falhas o processo pelo qual foi isolado e resolvido o problema.

- Gerenciamento de configuração. Este tópico permite que um administrador de rede visualize quais dispositivos fazem parte da rede administrada e quais são as suas configurações de *hardware* e *software*

- Gerenciamento de contabilização. Este tópico permite que o administrador de rede especifique, registre e controle o acesso de usuários e dispositivos aos recursos da rede. Quotas de utilização e alocação de acesso privilegiado a dispositivos e recursos fazem parte do gerenciamento de contabilização.

- Gerenciamento de segurança. O objetivo do gerenciamento de segurança é controlar o acesso aos recursos da rede de acordo com alguma política definida. A aplicação de filtros e o modelo de criação e distribuição de senhas fazem parte do gerenciamento de segurança.

Em Gerência de Redes de Computadores, existem mecanismos que propõem reduzir os pontos de falhas realizando observações periódicas em cada elemento importante da rede. Estas observações levam em conta medidas quantitativas de diferentes parâmetros de monitoramento de toda a infra estrutura. Com base nestas medidas é possível desenvolver uma metodologia de gerência pró-ativa.

A gerência pró-ativa de redes significa a capacidade de antecipar problemas que possam provocar determinado impacto na rede, principalmente em seu desempenho e falhas. Além disso, a gerência pró-ativa deve ter a capacidade de evitar a ocorrência desses problemas para que o seu impacto seja o menos prejudicial possível.

2.2.1 Arquitetura do gerenciamento de redes

Dentre as arquiteturas de sistemas de gerenciamento de redes conhecidas na literatura [29, 30, 31], uma das mais utilizadas é apresentada na Figura 2.2. Nesta figura há três componentes principais em uma arquitetura de gerenciamento de rede:

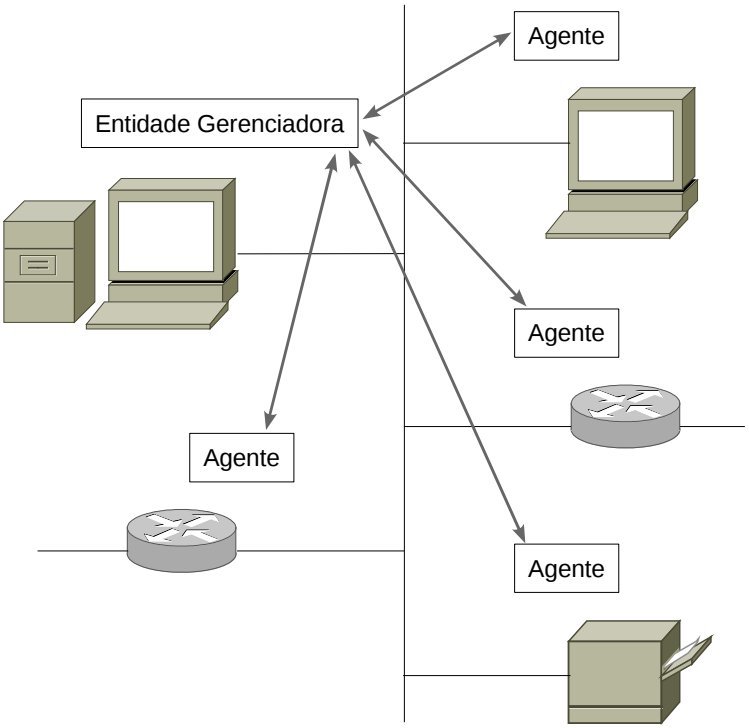

Figura 2.2: Arquitetura típica de gerenciamento de redes

- A entidade gerenciadora. Aplicação que em geral há um ser humano e é executada em uma estação central de gerência de rede. Esta entidade

é o núcleo da atividade de gerenciamento de rede. Por meio desta entidade são controladas as coletas de dados, o processamento, a análise e a apresentação de informações de gerenciamento da rede. É a partir da entidade gerenciadora que são iniciadas as ações para controlar o comportamento da rede.

- Dispositivo gerenciado. Equipamento de rede que esteja inserido em uma rede gerenciada. Um dispositivo gerenciado pode ser um computador de mesa ou portátil, um *tablet*, um roteador, um *switch*, um *hub*, uma impressora, ou seja, qualquer produto que tenha uma conexão ativa com a rede e esteja disponível, alcançável, e com permissão ao acesso da entidade gerenciadora.

- Objetos gerenciados. No interior de um dispositivo gerenciado pode haver diversos objetos gerenciados. Estes objetos são componentes de hardware que estão dentro do dispositivo, como por exemplo, uma placa de interface de rede e um sensor de temperatura. Estes objetos tem uma base de informações de gerenciamento com informações que são coletadas o tempo todo. Estas informações estão disponíveis para a entidade gerenciadora, e em algums casos, podem ser ajustadas remotamente pelo administrador da rede via entidade gerenciadora.

- Agente de gerenciamento de rede. É um programa de computador que é executado de forma independente no dispositivo gerenciado. Este programa é responsável por executar ações locais nos dispositivos gerenciados e recebe comandos da entidade gerenciadora que o controla.

- Protocolo de gerenciamento de rede. Este protocolo faz comunicação entre a entidade gerenciadora e o agente de gerenciamento de rede. Esta comunicação permite a entidade gerenciadora investigar a base de informações de gerenciamento e, indiretamente, executar ações sobre a base mediante o agente.

Capítulo 3

Principais Protocolos e Ferramentas utilizadas no Projeto

Neste capítulo serão descritos alguns protocolos fundamentais para monitoramento de redes. Todos os protocolos descritos nesta seção sustentam uma eficiente base para tomadas de decisões de redes de computadores. É importante observar que os protocolos ou as suas implementações em si não gerenciam a rede. Em vez disso, eles oferecerem uma ferramenta com a qual o administrador de rede pode ter acesso às informações e então sim, tomar decisões.

3.1 ICMP

Uma das principais finalidades do *Internet Control Message Protocol*, ICMP, é fornecer dentre outras informações, um suscinto relatório de testes básicos de conectividade e de detecção de erros de conexão entre dois *hosts*. A implementação mais comum do protocolo ICMP é a ferramenta ping, disponível em praticamente todas as distribuições de qualquer sistema operacional.

Um trabalho não muito recente mas relevante [32], apresenta uma proposta bem aceita de uma ferramenta de monitoramento baseada em ping, capaz de aferir a qualidade de conexões entre mais de 20 institutos de física do ramo das altas energias. Esta e outras referências [33, 34] reforçam a importância da ferramenta ping entre os administradores de redes.

A ferramenta ping, quando executada em direção a um endereço IP remoto, retorna uma pequena, mas muito útil informação. Uma sequência de respostas ping pode assegurar que o dispositivo está conectado, ativo, operacional e respondendo aos comandos básicos de rede.

Entretanto, há mais informações que o comando ping oferece. Atrelado ao número de sequências de sucesso do ping está o tempo em milissegundos exigidos para completar a ida e volta de informações entre o dispositivo origem e o destino. Este tempo provê a perspectiva de atrasos ou latências na rede. Latências podem ocorrer por diversos motivos, incluindo congestionamentos, e questões relacionadas aos meios físicos de conexões dos dispositivos origem e destino.

A velocidade de transferência de pacotes depende de uma série de fatores. Um dos fatores principais é o número de *hops*[1]. Desta forma, uma resposta ping bem sucedida fornece, dentre outras informações, o número de *hops* que estão entre os dispositivos origem e destino. Este número é apresentado em função de um fragmento das respostas ping chamado *Time To Live*, TTL, e é calculado subtraindo o TTL configurado no sistema pelo TTL apresentado pela resposta ping.

Outro fator comum que afeta a velocidade de transferência é o tamanho do dado transferido entre dispositivos de rede origem e destino. Dados maiores, normalmente são fragmentados buscando melhor performance na transferência entre dispositivos origem e destino. Em se tratando de tamanho de pacotes, cada sistema operacional possui uma implementação diferente do ping. No caso do sistema operacional Linux, a ferramenta ping envia uma sequência de dados de 56 bytes, que quando combinados com os 8 bytes referentes ao cabeçalho ICMP, formam pacotes de 64 bytes. É possível alterar

[1]Cada *hop* se refere a dispositivos intermediários, como roteadores e filtros de rede, entre o dispositivo origem e o destino.

os parâmetros da ferramenta e utilizar pacotes de tamanhos variados, com limite de 65507 bytes por pacote.

Finalmente, a parte final da sequência de respostas ping relata informações qualitativas a respeito da conexão entre os dispositivos origem e destino. As últimas linhas listadas no final de uma sequência bem sucedida da ferramenta ping informa sobre as perdas de dados na conexão. Dados transmitidos que não obtiveram sucesso na transmissão são considerados perdidos pela ferramenta ping. Altas taxas de perda indicam que um problema está ocorrendo dentro dos limites de conexão da rede como degradação do sinal, saturação na conexão, pacotes rejeitados por filtros, falhas em equipamentos ou outros problemas relacionados ao meio físico da rede. Embora as origens do problema sejam deixadas para outro protocolo ou outra técnica de detecção de falhas, a ferramenta ping oferece uma maneira simples de aferir a normalidade de uma conexão.

3.2 Protocolo SNMP

Embora o protocolo ICMP seja simples e bastante difundido, suas implementações resultam em ferramentas que retornam informações básicas a respeito da conectividade entre dois dispositivos. Consultas que utilizam este protocolo são, na maioria das vezes, utilizadas para verificação da disponibilidade de um dispositivo na rede. Para obter informações de mais alto nível é necessário a utilização de um protocolo com maior alcance ao interior dos dispositivos da rede.

O protocolo SNMP é um protocolo de gerência que está sendo amplamente utilizado atualmente. O SNMP basicamente permite a coleta de qualquer tipo de dado de um dispositivo de rede. Devido as suas diversas atualizações, no sentido de deixar o protocolo cada vez mais moderno, o SNMP pode ser utilizado em praticamente qualquer dispositivo de rede [13].

As raízes da atual estrutura do SNMP remonta a outro protocolo, o *Simple Gateway Monitoring*, SGMP, que sofreu diferentes ajustes até se tornar em 1993 o SNMP. Deste então o SNMP evoluiu do SNMPv1 para o SNMPv2 e chegou a sua versão mais recente, a SNMPv3 atualizada em

dezembro de 2002. Apesar da versão mais atual do protocolo ser a SNMPv3, grande parte da comunidade de desenvolvedores permanecem utilizando a versão SNMPv2.

Diversos trabalhos ressaltam o protocolo SNMP como protocolo fundamental para a gerência e monitoramento de redes. Explorando alguns destes trabalhos é possível encontrar várias referências interessantes, inclusive uma recente [35] que aponta a arquitetura típica de monitoramento web, representada pela Figura 3.4, como uma tecnologia de revolução para a gestão de redes de computadores, que uniu as facilidades do sistema baseado em *web* e as tradicionais ferramentas de aquisição de dados. Outra trabalho [36], também recente, sugere que este conjunto de tecnologias serão utilizados continuamente com adição de novas flexibilidades para se adaptar ao acesso de novos dispositivos de rede.

A estrutura de operação do SNMP é baseada em consultas e respostas por meio de operadores específicos para cada tipo de consulta. Estes operadores são comandos que habilitam um dispositivo origem acessar um banco de dados com informações que estão armazenadas em um disposivo destino.

Para acesso aos registros deste banco de dados, chamados de *Object Identifier*, OID, é necessário um identificador de objeto. Este identificador de objeto é único, basicamente é um endereço do registro dentro de uma estrutura organizada hierarquicamente. O protocolo SNMP utiliza notação decimal separada por pontos para indicar o identificador de um OID. Contudo, as últimas versões do protocolo permitem que o acesso aos registros OID seja feito por meio de nomes reservados associados ao identificador de objeto.

Certamente, a lista de OIDs para todos os dispositivos de rede é profundamente grande. Se preciso for, é possível realizar o *download* de OIDs opcionais e adicioná-los à estrutura armazenada nos dispositivos de rede.

A Figura 3.1 apresenta a organização da estrutura hierárquica onde se encontram as informações de registro OID. Nesta estrutura, os OIDs são organizados em um modelo de árvore que representa uma coletânea de objetos que juntos formam uma base de dados conhecida como *Management Information Base* MIB .

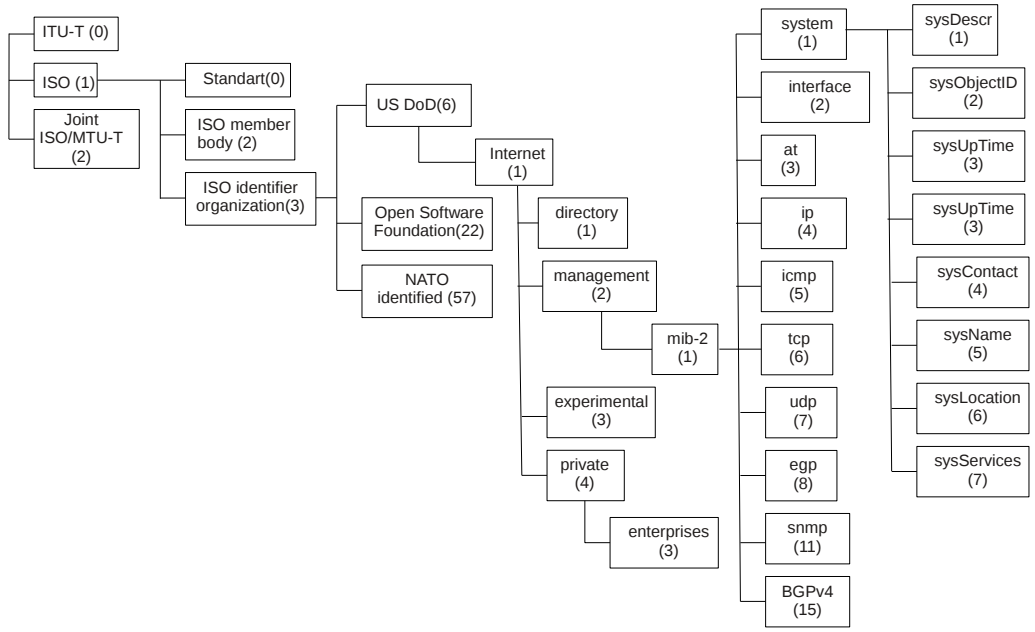

Figura 3.1: Trecho da árvore MIB

Um objeto MIB pode ser desde um contador de pacotes descartados por um roteador, até um conjunto de informações descritivas, como a versão do sistema operacional do dispositivo. Desta forma, os objetos MIB estão reunidos em módulos, cujos valores refletem o estado atual dos dispositivos na rede. Estes valores podem ser consultados e ou definidos por meio de mensagens SNMP.

Para acessar os pontos da árvore MIB é necessário adicionar às mensagens SNMP, o identificar de objeto, indicado pela sequência que especifica o trajeto da raiz até o ponto onde se pretende atingir.

O ramo mais baixo da árvore na Figura 3.1 mostra alguns módulos MIB voltados para os *hardwares* dos dispositivos como *system* e *interface*, e mais alguns módulos associados a protocolos importantes. Os OIDs que estão sob o módulo *system* contém informações gerais sobre o dispositivo com o qual estão sendo trocadas mensagens SNMP e os principais são apresentados na Tabela 3.1.

Os OIDs que correspondem às informações do módulo *interfaces*, um dos

Tabela 3.1: Principais objetos gerenciados no módulo *system*, este módulo provê informações administrativas sobre o *host*.

Identificador de objeto	Nome	Descrição (segundo RFC1213)
1.3.6.1.2.1.1.1	sysDescr	Nome, versão e data da instalação do sistema operacional no dispositivo
1.3.6.1.2.1.1.3	sysUptime	Tempo desde a última inicialização.
1.3.6.1.2.1.1.4	sysContact	Informações de contatos configuradas pelo administrador de redes.
1.3.6.1.2.1.1.5	sysName	Nome atribuído administrativamente para o dispositivo.

Tabela 3.2: Principais objetos gerenciados no módulo *ifEntry*. Este módulo é único para cada interface disponível no *host* e provê informações relacionadas a configuração e ao tráfego de dados da interface.

Identificador de objeto	Nome	Descrição (segundo RFC1213)
1.3.6.1.2.1.2.2.1.7	ifAdminStatus	Indica o estado da interface, 1 *up* e 2 *down*.
1.3.6.1.2.1.2.2.1.5	ifSpeed	Estimativa da largura de banda em bits por segundo.
1.3.6.1.2.1.2.2.1.10	ifInOctets	Número total de octetos transmitidos para dentro da interface.
1.3.6.1.2.1.2.2.1.16	ifOutOctets	Número total de octetos transmitidos para fora da interface.

módulos mais importantes para o monitoramento de tráfego de rede estão agrupados em MIBs distintas, ou seja, um módulo MIB para cada interface de rede disponível no dispositivo, que por sua vez, estão localizadas dois níveis abaixo da MIB *interfaces*: módulo *ifEntry* representados na Tabela 3.2.

Um detalhe importante deve ser observado caso o objeto gerenciado, *ifSpeed* apresentado na Tabela 3.2 reportar o valor 4.294.967.295. Nesta situação, considerada de erro, os contadores de 32 bits associados ao objeto não foram capazes de apresentar o valor correto da velocidade da interface. Recomenda-se então, a utilização de outro módulo MIB, específico para interfaces de alta capacidade [37].

Para interfaces que operam na faixa entre 20Mbps e 100Mbps podem ser utilizados, tanto os contadores de 32 bits previstos na RFC1213, quanto os contadores, de alta capacidade, de 64 bits previstos na RFC2233, e para interfaces que operam acima de 100Mbps devem ser utilizados somente os contadores de 64bits, cujo módulo MIB encontra-se sobre o nome *ifXTable*.

Pelo fato do protocolo SNMP estar padronizado em praticamente qualquer dispositivo de rede, é possível acessar por meio de uma única entidade gerenciadora dispositivos de diferentes fabricantes. Isto resulta em uma unidade central de monitoramento capaz de criar imagens, em tempo real, a respeito do comportamento interno de uma rede. Esta imagem pode incluir desde informações sobre a performace dos dispositivos, como também detalhes adicionais como configurações, temperatura e estatísticas de fluxo de dados nas interfaces de redes dos dispositivos.

O modo de utilização mais comum do SNMP é em modo comando resposta, no qual a entidade gerenciadora envia uma requisição a um agente SNMP, que a recebe, realiza as ações requisitadas e envia uma resposta de volta à entidade gerenciadora. Normalmente, estas requisições são utilizadas para consultar ou escrever algum valor no OID associado a um dispositivo gerenciado.

Sempre que for necessário, é possível atualizar as informações em alguns OIDs, especialmente aqueles que disponibilizam informações de configurações. Isto é possível por meio de uma opção de escrita disponível pelo protocolo SNMP.

Para todos os casos, tanto de coleta de dados ou configuração/atualização de informações, o dispositivo de rede destino deve ser configurado com um par de senhas, chamadas SMNP *Community Strings*. Estas *Strings*, normalmente são distintas e aplicadas separadamente para leitura e para escrita nos dispositivos, e ainda, devem ser sempre informadas nas requisições SNMP.

3.2.1 Operações SNMP

O protocolo SNMP é capaz de realizar vários tipos de operações. Estas operações se resumem em trocas de mensagens SNMP entre a entidade

gerenciadora e um agente e pode ser representada pela Figura 3.2. As mensagens SNMP contém a versão do protocolo SNMP utilizada na operação, a community, ou senha de acesso para a entidade gerente acessar informações no agente de gerenciamento e o SNMP PDU (*Protocol Data Units*).

O protocolo SNMP tem um formato padrão de PDU para os principais tipos de operações SNMP como segue:

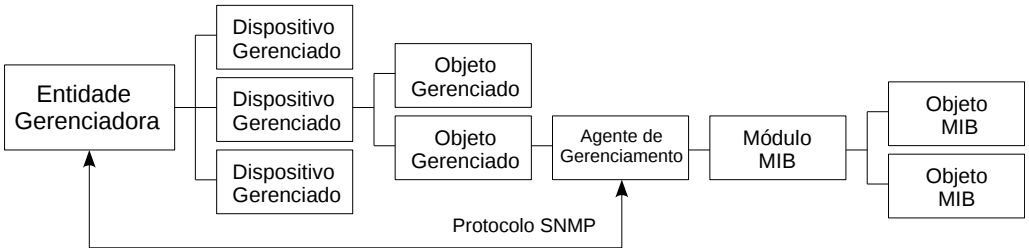

Figura 3.2: Processo de troca de mensagens do Protocolo SNMP

- Operação *get*: A requisição *get* é iniciada pela entidade gerenciadora, que envia uma requisição ao agente. Alguns dispositivos que estão sobrecarregados podem não responder às operações de *get*, descartando-a. Entretanto, se o agente for bem sucedido em reunir as informações solicitadas, ele envia uma resposta, *get-response*, à entidade gerenciadora. As respostas submetidas à entidade gerenciadora pelos agentes são vinculadas à variáveis associadas ao OID solicitado pela entidade gerenciadora, chamada *variable binding* ou simplesmente *varbind*. Sendo assim, o formato de uma operação *get* deve conter necessariamente: A identificação do dispositivo na rede, a *string* de acesso ao dispositivo e OID requisitado. E a resposta, se bem sucedida deve retornar os valores das variáveis *varbind* associados ao OID requisitado.

- Operação *get-next* ou *snmpwalk*: Esta operação permite emitir uma sequência de comandos para recuperar um grupo de valores de uma MIB. Esta operação parte do princípio que, uma vez que um OID é uma sequência de números inteiros, um agente é capaz de percorrer toda árvore MIB, desde a raiz até encontrar o OID que está sendo requisitado. Quando a entidade gerenciadora recebe do agente a resposta

do primeiro *get-next*, outro *get-next* é emitido e este processo continua enquanto o agente não retornar um erro, o que significa que o final da MIB foi alcançado e que não há mais consultas a serem feitas.

- Operação *get-bulk*: A operação *get-bulk* pode obter mais de um OID de uma vez, mas os tamanhos das mensagens são limitados pela capacidade do agente. Se o agente não pode retornar todas as respostas solicitas, ele retorna somente um erro. A operação *get-bulk* pode, por meio de parâmetros, informar o agente para enviar o máximo de respostas de volta, ou seja o máximo de informação que couber no PDU. Este recurso pode acarretar em respostas incompletas. A operação *get-bulk* está disponível nas versões 2 e 3 do protocolo SNMP.

- Operação *set*: Esta operação é utilizada para atualizar, apagar ou escrever algum valor nos campos da MIB que a entidade gerenciadora tenha permissão. Neste tipo de operação é possível uma entidade gerenciadora realizar vários valores por vez.

No aspecto confiança, as implementações do protocolo SNMP são soluções não confiáveis para coleta de informações nos dispositivos de uma rede. Esta característica é detectada pela baixa prioridade do protocolo sobre outros protocolos de rede e também pelo descarte dos pacotes SNMP por alguns dispositivos de redes quando estes estão operando com carga de processamento acima de 60%.

No aspecto segurança, as versões mais populares do protocolo SNMP são inseguras. Esta característica se dá pelo fato do protocolo operar com suas *Community Strings* em texto aberto pela rede. Existem métodos que visam atenuar esta celeuma característica do protocolo atuando sobre a transmissão das *Community Strings* no momento da requisição SNMP.

3.3 Telnet

O protocolo telnet é considerado pela comunidade de administradores de redes um dos protocolos de uso comum mais antigo. Atualmente, a utilização

do telnet baseia-se na conexão via acesso remoto, por linha de comandos, a dispositivos de redes com sistemas operacionais habilitados a permitir este acesso. A partir de uma conexão telnet é possível realizar qualquer comando remotamente.

Para questões voltadas ao monitoramento de dispositivos e testes de conexão, o telnet é utilizado com frequência para verificar se o dispositivo destino está apto a receber conexões em determinado canal ou porta. Sendo assim, um comando telnet deve ser composto na origem pelo endereço IP do dispositivo destino seguido de um número que indica a porta. O dispositivo destino pode responder de duas formas. A primeira pode ser a rejeição do comando seguido de uma mensagem de erro e a segunda forma, acompanhada do sucesso da conexão: uma janela em modo texto.

No ambiente telnet, os dados e comandos são passados do dispositivo origem para o destino em texto aberto. Uma das características deste protocolo é a falta de encriptação que garanta a passagem segura da informação pela rede.

3.4 SSH

SSH *Secure Shell* é um programa de computador que implementa toda a funcionalidade do procoloco telnet e oferece um ambiente seguro para comunicação remota entre dispositivos. O programa SSH oferece diferentes mecanismos de autenticação, sendo o mais utilizado pela comunidade o sistema de chaves públicas criptografadas para autenticar no dispositivo origem o dispositivo destino.

Neste mecanismo, baseado em uma arquitetura cliente-servidor, o dispositivo origem, um cliente SSH, é autenticado em um dispositivo destino ou servidor SSH, comprovando sua identidade com base em cálculos matemáticos avançados. Concluída a autenticação, uma conexão segura é criada, esta conexão propõe garantir a integridade e confidencialidade dos dados trocados entre dois dispositivos de rede.

Segundo alguns trabalhos publicados pela comunidade, [38, 39], o SSH é um importante mecanismo de autenticação que resolveu um grave problema

de segurança na comunicação entre dois *hosts*. Desde meados de 90 o SSH é difundido na internet, sendo utilizado em todos os seguimentos da internet, incluindo universidades, centros de pesquisa, grandes e pequenas companhias e usuários em geral.

Do ponto de vista das possíveis aplicações e implementações que o SSH pode oferecer, há algumas que se ajustam à gerência e monitoramento de redes:

- Transferência de arquivos por meio das implementações SSH: SCP, SFTP e rsync. O protocolo *Secure Copy*, SCP, e *Secure File Transfer Protocol*, SFTP, promovem a transferência segura de arquivos de rede baseando-se nas regras, padrões e especificações do SSH. Rsync é um modelo de transferência de arquivos que pode ser operado via SSH. A utilização mais comum deste modelo é a conexão do dispositivo origem ao dispositivo destino via SSH e a cópia por rsync somente dos arquivos recém-adicionados ou modificados no dispositivo destino. porta

- Deslocamento de porta e tunelamento: O deslocamento da porta SSH interfere sensivelmente no método de conexão entre dispositivos. Deslocando-se a porta SSH, automaticamente a porta padrão de conexão se fecha evitando desta forma ataques direcionados a porta padrão SSH. O túnel SSH é um método de conexão SSH entre dois dispositivos de rede cujos dados são redirecionados por um terceiro dispositivo. Este método pode ser aplicado por administradores e usuários de forma a proteger os dados de comunicação entre dispositos por meio de uma conexão SSH segura.

- Montagem remota de diretórios via SSH *Filesystem* ou SSHFS: Esta implementação do SSH permite que a partir de uma conexão seja feita também a montagem de diretórios. Este recurso exige a autenticação, assim como em todas as conexões SSH, e permite ao administrador e usuário autorizado acessar pastas e arquivos presentes em outros dispositivos de redes de modo transparente.

3.5 RRDtool

RRDtool (*Round Robin Database tool*) é um programa de computador de propósito específico, uma ferramenta importante, direcionada para armazenamento de dados e visualização gráfica de estatísticas de monitoramento de dispositivos de rede, e está disponível sob os termos da licença pública GNU(GNU GPL). É um projeto de iniciativa de Tobias Oetiker, do Instituto Federal de Tecnologia da Suíça. O projeto foi concluído no final da década de 90 e até os dias de hoje recebe atualizações e suporte.

O termo "*Round Robin*", utilizado na ciência da informação, serve para caracterizar bancos de dados lineares com número fixo de registros, em que os dados mais antigos são subscritos por novos dados que são inseridos no banco [40].

Em bancos de dados lineares convencionais, as tabelas possuem crescimento regular. Nos banco de dados RRD o tamanho é determinado no momento da criação do banco. Analogamente, um banco de dados RRD pode ser considerado o perímetro de um círculo e os registros são inseridos ao longo deste perímetro, partindo de um ponto inicial. Quando novos registros alcançam o ponto inicial, os dados antigos começam a ser subscritos. Assim, o tamanho de um banco de dados RRDtool sempre se mantém constante. O nome "*Round Robin*" deriva deste atributo [41].

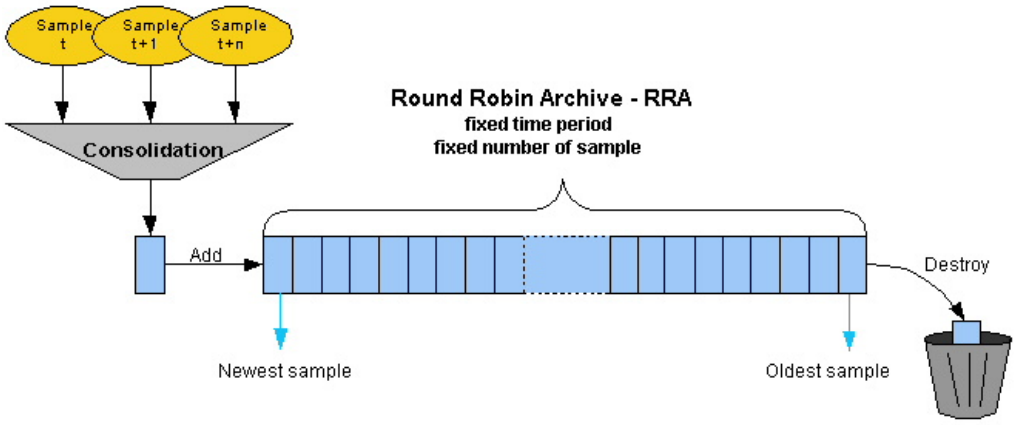

Figura 3.3: Esquema de funcionamento de bancos dos dados do tipo Round Robin, (Figura retirada do sítio: http://www.luteus.biz, Mai/2013)

Observando sua documentação, o projeto RRDtool foi direcionado exclusivamente para aplicação em dispositivos de rede [42]. Ou seja, é um programa de computador de propósito específico.

Em sistemas de monitoramento de redes, os bancos RRDs são utilizados para acumulação de dados referentes a diversos parâmetros de monitoramento. Para cada parâmetro deve ser criado um banco RRD, configurado de forma a acumular dados durante espaços de tempo que satisfaçam os requisitos da aplicação. Nesta etapa são declarados os detalhes sobre o número de amostras que os bancos RRD deverão acumular.

Na questão desta acumulação de dados, para cada parâmetro de monitoramento, por exemplo, a quantidade de bits que adentram determinada interface, são gerados dois conjuntos de quatro arquivos. Quatro para valores médios e quatro para valores máximos, ambos conjuntos seguindo a mesma estrutura. Considerando apenas os valores médios, cada um destes arquivos abrange um período de tempo diferente. O primeiro armazena os dados a medida que eles chegam, ou seja, a cada 5 minutos. Na ocasião da criação dos arquivos foram previstas 600 amostras, portanto cada arquivo deste tipo pode armazenar dados por 50 horas. Após 50 horas, novas amostras substituem amostras mais antigas.

O segundo arquivo calcula a média de seis amostras para armazenar uma amostra a cada 30 minutos. Como este arquivo possui espaço para 700 amostras, é possível a cobertura de 14,5 dias. O terceiro arquivo armazena a média de 24 amostras do arquivo de 5 minutos. Neste arquivo, a matemática se comporta da seguinte forma: 5 minutos x 24 médias x 775 amostras = 93000 minutos = 1550 horas = 64,5 dias. O último arquivo armazena a média de 288 amostras de 5 minutos. Este arquivo cobre exatos 797 dias.

Atribuindo seu propósito a seu recurso de encapsulamento via *scripts* Shell, PHP e outras linguagens de programação, muitos desenvolvedores da comunidade científica, utilizam o RRDtool de base para outros programas, desta maneira foram criados os programas MRTG [14], Cacti [43], Zenoos [44] entre outros, todos específicos para aplicação em redes de computadores.

A ferramenta RRDtool possui uma vasta documentação, a seguir serão abordadas algumas características técnicas:

- Atualizações: O banco de dados RRDtool é estruturado de modo que ele precisa de atualizações em um intervalo de tempo predefinido. As atualizações também devem estar dentro de um limite (*treshold*) configurado. Caso não haja novos valores válidos durante o intervalo, ele armazena um valor *unknow* para este intervalo

- Funções de consolidação: Antes de um novo dado ser inserido no banco, há uma verificação que agrega o dado em determinado parâmetro de configuração. Estes parâmetros podem ser: média, máximo, mínimo e último. Por meio destas funções é possível recuperar dados específicos de um determinado período de tempo. Por exemplo, o histórico do tráfego máximo em uma determinada interface de rede nos últimos 30 dias ou no último ano

3.6 LAMP

Um grande número de *web-sites* são desenvolvidos utilizando as linguagens de programação PHP em conjunto com banco de dados MySQL em uma plataforma como sistema operacional Linux e servidor *web* Apache.

Desde que este conjunto passou a ser adotado pela comunidade *open source*, houve muitas contribuições em vários aspectos, desde as disponibilidades gratuitas de aplicativos até a preocupação dos desenvolvedores em tornar as tecnologias cada vez melhores e seguras [45, 46].

- Linux - Segundo a Netcraft (`www.netcraft.com`), apesar de não ser maioria entre os usuários da internet, o sistema operacional Linux se mantém no topo dos sistemas operacionais menos vulneráveis a falhas e com melhores históricos de disponibilidade entre as maiores organizações de hospedagens de *web-sites*. As vantagens do Linux são inúmeras, que vão desde vantagens econômicas [47], porque a implementação do sistema Linux pode sair muito menos onerosa do que a implementação de sistemas proprietários [48], até a agilidade em que os famosos *bugs* (falhas no código-fonte) são corrigidos. No caso do Linux, quando um *bug* é descoberto, o mesmo é rapidamente corrigido,

porque há uma comunidade envolvida em todas as fases do processo de desenvolvimento do sistema e manutenção [49].

- Apache - Atualmente, estima-se que 50% dos servidores *web* são Apache [50]. Esse número é resultado de desenvolvimento e atualizações do servidor, no sentido de torná-lo cada vez mais seguro, e capaz de suportar a integração de outras tecnologias. Esta afirmação é reforçada por trabalhos que apresentam boa performance do Apache no consumo de recursos computacionais como CPU, acesso a disco e memória [51, 52], e também por trabalhos que ressaltam a vantagem econômica do Apache. Entretanto, há preocupações no nível de aplicações, ou seja, descuidos dos programadores que podem causar problemas no Apache. Para minimizar estas falhas, recomenda-se melhorar a segurança utilizando recursos como *firewalls* [45].

- MySQL - Este gerenciador de banco de dados oferece a maioria dos recursos de bancos de dados de alta performance. Segundo sua documentação, MySQL suporta a gerência de bancos de dados com Terabytes de dados. Na internet há vasta documentação e aplicabilidade do MySQL.

- PHP - A primeira versão do PHP foi lançada em 1995. Em 2001, segundo um *survey* da Netcraft, estimou-se 1,8 milhão de *web-sites* com aplicações PHP. Em 2013, segundo nova estimativa [53], há cerca de 244 milhões de *web-sites* com aplicações PHP, sendo 78% destas aplicações hospedadas em servidores com sistema operacional Linux.

  Assim como o MySQL, o PHP e outras linguagens de programação, que não fazem parte do conjunto LAMP mas também são amplamente utilizadas, o principiante desenvolvedor encontra com facilidade todos os manuais e discussões a respeito, pois todas estas tecnologias são bastante difundidas na comunidade de desenvolvedores.

3.7 Protocolo BGP

3.7.1 Sistemas Autônomos

A internet passa por um gigantesco crescimento em tamanho e complexidade desde o início da sua comercialização, na década de 90. Nela, se conectam milhares de Sistemas Autônomos (ASs). De acordo com a RFC4271, o termo AS pode se definido, classicamente, sob o seguinte conceito: Um conjunto de redes locais e roteadores operados pelo mesmo grupo de administradores de rede e submetidos a uma mesma política de operação.

Cada AS é identificado por um número, ASN, entre 1 e 65536. Este número é fornecido por um órgão de controle e é utilizado nas configurações dos roteadores que farão as conexões entre ASs e será a sua assinatura para toda a internet. Os dados para o desenvolvimento do repositório RIB- BGP descrito neste trabalho foram obtidos no AS 2715.

O número de sistemas autônomos cresce diariamente, até 1994 este número não chegava a 5000, em 2012 este número ultrapassou a casa dos 40.000, Figura 3.4.

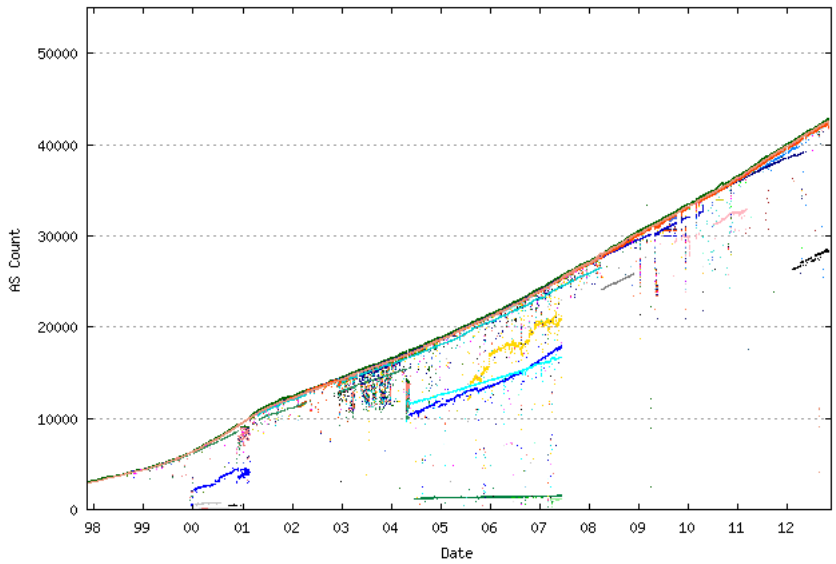

Figura 3.4: Crescimento do número de ASs, (dados da Universidade de Oregon) http://bgp.potaroo.net/bgprpts/rva-index.html, Nov/2012.

Cada AS tem um conjunto de roteadores que agrega uma ou mais redes locais. Este conjunto de roteadores distribuem o tráfego de informação internamente entre suas redes locais. Estes roteadores internos trocam informações através de protocolos que tem a função principal de informar aos demais roteadores do AS quais as redes locais cujo o acesso é feito por meio deles. Estes protocolos são conhecidos também como protocolos intradomínio como por exemplo: *Router Information Protocol* - RIP e *Open Shortest Path First* - OSPF.

Em cada AS está contido pelo menos um roteador com características interdomínio, ou seja, um roteador que se comunica com roteadores de outros ASs que faz a comunicação externa ao AS. Este roteador é chamado de roteador de borda e se comunica por meio do protocolo BGP [54].

O protocolo BGP é o protocolo de roteamento que opera no interior da internet e atualmente se encontra na versão 4. Sua função é manter uma tabela de rotas, RIB-BGP, que aponta o alcance das redes entre os ASs. É um protocolo do tipo *vector path*. Em outras palavras, o BGP implementa um algoritmo que seleciona o menor caminho em termos de AS. E para tomar esta decisão, o protocolo BGP lida com diversos atributos, os quais serão citados neste documento: peso, origem, AS_*path*, e *next_hop*.

O meio mais simples de um protocolo *vector path* decidir sobre o menor caminho, seria admitir, com base nos atributos, a rota com o caminho mais curto. No entanto, o BGP permite uma série de diretrizes, de forma que o administrador de redes possa controlar o seu tráfego com liberdade. Ao receber uma atualização, a decisão de usar ou não o caminho sugerido é do administrador de redes por meio das configurações de diretrizes do roteador. As diretrizes são definidas via manipulação de atributos e serão discutidas na sessão seguinte.

3.7.2 Diretrizes

Os relacionamentos entre ASs acontecem após o estabelecimento de um acordo de troca de tráfego com ou sem compromisso financeiro (*peering*) entre dois ou mais ASs. Uma vez definido este acordo, os roteadores de

borda começam a anunciar para seus vizinhos, os blocos de redes (prefixos) que estão ao seu alcance. Em seguida são montadas e atualizadas as tabelas com os prefixos, seguidos de seus caminhos via ASs. Desta forma, configura-se um caminho de ASs para cada rede, partindo do AS origem até o AS destino, onde se encontra a rede em questão.

A função primária do BGP é trocar informações de redes de computadores alcançáveis entre roteadores BGP vizinhos. Entretanto, ASs podem aplicar diferentes diretrizes para a importação e exportação de rotas quando utilizam BGP. As diretrizes definem como serão tomadas as decisões de roteamento na internet.

A diretriz atua quando um AS decide anunciar blocos de redes (prefixos), para outro AS. As diretrizes de importação permitem que um AS negue ou aceite uma atualização, atribuindo, em caso de aceite, dependendo da origem do AS vizinho, e dos caminhos dos seus vizinhos (AS_*path*), uma rota de preferência. As diretrizes de exportação permitem um AS determinar se envia uma atualização para um vizinho e se, em caso positivo, envia esta atualização de forma resumida ou completa. Mais sobre diretrizes em [55].

3.7.3 Tabela de Rotas

As trocas de mensagens entre os roteadores de borda de cada AS permitem que cada um destes roteadores construa uma RIB-BGP que contém o caminho de acesso, via ASs para cada rede local acessível.

Eventualmente, a pedido dos administradores, a RIB-BGP pode conter informações de mais redes locais provenientes de segundos e terceiros vizinhos. No caso extremo, todos os prefixos das redes locais da internet e os seus respectivos caminhos de acesso em termos do ASN podem ser armazenados e atualizados. Neste caso, esta tabela deixa de ser sintetizada a um conjunto resumido de ASs e passa a ser uma tabela completa de rotas (*Full Route*) da internet global.

Na Tabela 3.3 pode-se observar um fragmento do resultado do comando que exibe a tabela de rotas BGP no roteador de borda do AS 2715. Esta tabela que na realidade é uma RIB-BGP *Full Route* contém mais de 470 mil

Tabela 3.3: Trecho de uma tabela BGP retirado da RedeRio de Computadores.

Network	Next hop	LocPrf	Weight	Path
* >4.2.24.0/24	200.255.243.174			3549 i
*	200.143.254.138			3549 5413 i
*	200.255.243.50			3549 702 702 701 i
*	200.255.243.51			1916 1144 i
*	200.255.243.175			3549 3549 701 i

linhas e é constituída de cinco colunas relacionadas a seguir:

- A primeira coluna contém os prefixos (redes locais acessíveis, anunciadas pelos ASs).
- A segunda coluna contém o endereço da interface do roteador por onde devem trafegar os pacotes de informação para a rede de destino definida na coluna 1.
- Na terceira coluna o atributo *local_pref*, se assim for configurado.
- Na quarta coluna o peso do caminho que neste caso é nulo e igual para todas as entradas.
- A quinta coluna apresenta o AS_*path* identificados por seus números, ASN.

Por exemplo, a RIB-BGP mostrada na Tabela 3.3, apresenta o acesso eleito para destino do prefixo 4.2.24.0/24, indicada pelo símbolo ">". Este acesso foi decidido pelo critério do menor caminho, a linha de menor comprimento no AS_*path*. Entretanto, o AS tinha cinco rotas candidatas para 4.2.24.0/24, a saber: AS_*path* (3549) via *next_hop* 200.255.243.174, AS_*path* (3549 5413) via *next_hop* 200.143.254.138, e assim por diante. É possível notar na terceira rota candidata, AS_*path* (3549 702 702 701), que o AS 702 aparece duplicado. Isto ocorreu porque o AS 702 fez um *prepend* deste número antes de exportá-lo para o AS 3549. Fazendo uso do recurso *prepend* o AS foi repetido no AS_*path*, aumentando seu comprimento, a fim de desencorajar o tráfego de entrada em sua rede.

3.7.4 Aplicações da RIB-BGP

Uma vez que o interesse deste trabalho é a descrição das principais características de um repositório RIB-BGP específico cabe acrescentar algumas aplicações interessantes que envolvem a tabela de rotas.

Uma tabela de rotas BGP (RIB-BGP), apresenta uma série de informações, que se resumem em caminhos, através dos quais é possível alcançar uma rede local na internet [56]. Esta tabela é um importante ingrediente para o processo que envolve o envio de pacotes em um roteador BGP. A RIB-BPG contém ainda métricas associadas aos caminhos, ou seja, variáveis de custo que são usadas para decidir o melhor caminho (rota), de acordo com as diretrizes do AS, configuradas no roteador de borda pelo administrador de redes.

As informações na RIB-BGP podem ser utilizadas, para monitorar aspectos da internet como:

- A quantidade de endereços IP (o limite do IPv4 é aproximadamente 4,3 bilhões)
- A quantidade de ASs (o limite é aproximadamente 64.412)
- Identificadores de redes, limitado pelo tamanho da memória do equipamento.
- O tamanho da RIB-BGP, limitado pelo tamanho da memória e configurações do equipamento.
- O processamento de atualizações BGP, que podem interferir na capacidade de envio de pacotes, se as atualizações forem muito frequentes.
- Banda consumida pelas mensagens BGP

E ainda responder questões interessantes como:

- Quais são os principais ASs da internet ?
- Como a internet tem evoluído nos últimos anos? E nos últimos meses?

Certos trabalhos [56, 57] procuram responder as questões anteriores. E outros trabalhos [58, 59, 60, 61, 62] sugerem que os dados para as análises sejam coletados em repositórios RIB-BGP espalhados pelo globo. Um dos repositórios RBI-BGP mais citados na literatura [56, 62, 60] é o *Oregon Route View* [16] . Outros autores [61] sugerem que para uma análise mais completa da RIB-BGP global, os dados devessem ser coletados também em outros repositórios RIB-BGP relacionados como IRL, Exodus Comm Asia, Opentransit entre outros.

Seguindo esta linha, este repositório poderia contribuir de maneira positiva em pelo menos três trabalhos [59, 54, 61]. Dois deles [59, 54] têm o objetivo de descrever propriedades relacionadas à topologia, conectividade e outras características de redes de conexões. Neste caso, os autores poderiam fazer uso desta ferramenta desenvolvida no sentido de alimentar sua base de dados com informações provenientes de uma outra perspectiva, ou seja, uma visão "local" da internet no globo.

Um segundo estudo de caso para este repositório poderia ser aplicado em um terceiro trabalho [61]. Neste trabalho, os autores associaram diferentes RIB-BGPs oferecidas por repositórios ao redor da internet. Neste caso, os autores encontrariam uma visão "global" com mais informações da internet mundial.

Na seção seguinte serão apresentadas as tecnologias e os procedimentos que foram utilizados no desenvolvimento do repositório RIB-BGP.

Capítulo 4

RRLG - Principais características

Servidores do tipo *Looking Glass* disponibilizam na internet uma variedade de consultas sobre roteamento na internet, testes de alcance e de tempo de resposta. O sistema RRLG (Rede Rio *Looking Glass*) além de permitir diversas consultas a partir do roteador BGP da RedeRio de Computadores oferece também, um mecanismo de repositório das Tabelas *Full Route* BGP, organizado cronologicamente em arquivos compactados e disponibilizado livremente em um servidor na internet.

O sistema RRLG ainda disponibiliza os seguintes recursos:

Capacidade de fazer comandos BGP preestabelecidos: Os comandos BGP são recursos considerados indispensáveis para o desenvolvimento de um sistemas *Looking Glass*. A pré definição dos comandos atribui velocidade na decisão do comando e evita falhas na sintaxe do comando.

Capacidade de fazer comandos ping IPv4 e traceroute IPv4: Estes comandos são essenciais para teste de alcance e tempo de resposta.

Capacidade de fazer comandos ping IPv6 e traceroute IPv6: O Brasil possui cerca de 600 alocações IPv6, segundo informações do site `www.ipv6.br` . Esta tecnologia prevê a ampliação do mecanismo de endereçamento na internet mundial e está descrita na RFC1752.

Capacidade de gerenciar *upload* e *download* de documentos: Esta funcionalidade oferece aos usuários, documentos técnicos sobre o sistema e outros assuntos.

Basicamente, o sistema RRLG é composto por diferentes tecnologias de *software* que serão apresentadas nas próximas seções. A escolha por estas tecnologias, foi decidida pelo custo zero de investimento, pois o projeto foi desenvolvido a partir de ferramentas de licença livre, e também pelo baixo custo computacional requerido pelas tecnologias.

As ferramentas desenvolvidas para o sistema, em particular para o repositório RIB-BGP tiveram o objetivo de manter a sistemática de extrair do roteador de borda as tabelas RIB-BGP e mantê-las organizadas cronologicamente em diretórios diários, mensais e anuais. Para o armazenamento das tabelas RIB-BGP foi implantado um servidor *web* que permite a navegação entre esses diretórios e fornece permissão para a transferência (*download*) das tabelas RIB-BGP para outros dispositivos conectados a internet.

Para compor a sistemática do repositório RIB-BGP, foram desenvolvidas ferramentas computacionais em diferentes linguagens de programação objetivando desde a estruturação de diretórios, passando pela conexão remota, extração e tratamento das tabelas RIB-BGP e encerrando na transferência para o servidor *web* implantado.

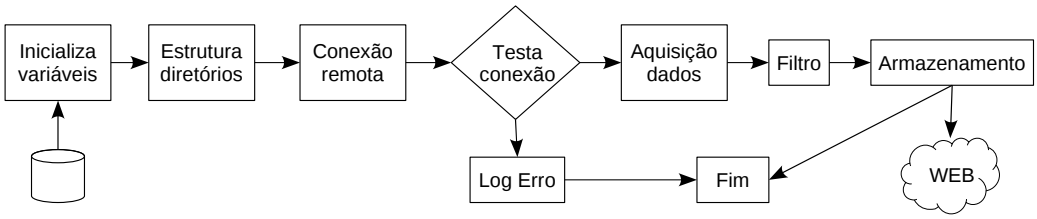

Figura 4.1: Representação esquemática do algoritmo desenvolvido para a criação do repositório RIB-BGP.

A Figura4.1 apresenta um fluxograma, que faz uma representação esquemática do trabalho desenvolvido. O fluxograma contribui para o entendimento do trabalho antes e após o seu desenvolvimento.

Nos itens a seguir será feita uma abordagem aos principais módulos que compõem o repositório RIB-BGP.

Módulo de conexão remota: Este módulo apresentou uma lógica de programação intuitiva e simples. Intuitiva e simples porque foram seguidos padrões de desenvolvimento de sistemas. Estas qualidades facilitam a manutenção da ferramenta e a possibilidade de adaptação da ferramenta para comunicação com outros equipamentos.

Módulo de aquisição de dados: Apresenta um robusto mecanismo de extração de dados do roteador de borda BGP. Robustez é a capacidade do sistema de continuar adquirindo dados mesmo em condições anormais de operação. Apesar da robustez, o módulo de aquisição de dados seguiu a simplicidade de codificação dos demais módulos e pode ser facilmente alterado e adaptado a outros cenários.

Módulo de armazenamento e transferência de dados para a *web*: Este módulo presenta uma metodologia dinâmica de aplicação de funções específicas aos dados adquiridos. Estas funções são compostas de outros dois módulos, compactação e aplicação de filtros, que seguem o mesmo padrão de desenvolvimento dos demais módulos.

4.1 O Repositório BGP

O repositório está em operação deste o dia 29 de Fevereiro de 2012 e pode ser acessado livremente, por meio do endereço eletrônico *http://lg.rederio.br*. A Figura4.2 apresenta uma imagem da interface de navegação. Esta interface é dividida em três regiões a saber:

- A região superior com o título da página *web* e um menu com dois *links*: o da esquerda aponta para a página que oferece acesso ao repositório da tabelas de rotas e o da direita que oferece acesso a documentos referentes ao projeto.
- A região lateral direita há um link para a página do Centro Brasileiro de Pesquisas Físicas.

- E a região central, que apresenta os conteúdos referentes aos *links* do menu superior. Nesta região, o *link download* aponta para uma página que contém uma lista de diretórios contendo as tabelas RIB-BGP. E o *link* Nota Técnica aponta para o *download* deste documento.

Figura 4.2: Interface com o usuário, acessada por meio do endereço http://lg.rederio.br

A seguir, na Figura 4.3, um trecho de uma lista contendo as tabelas RIB-BGP retirada da página de *download* do servidor. Cada um destes arquivos contém uma tabela RIB-BGP, cada qual identificada por quatro campos comuns a todas: o identificador *route-info*, o ASN2715 de onde foram coletados os dados, a identificação *full* por se tratar de uma tabela de rotas do tipo *Full Routing*, o formato de arquivo dat, e o formato de compactação *.gz*, respectivamente. O campo de distinção é o horário de aquisição. Ainda são apresentados outros três campos que não fazem parte do arquivo e sim da estrutura de diretório: a data da aquisição, a hora da gravação e o tamanho do arquivo.

No rodapé da página é possível perceber o endereço completo de *download* (*link* direto) do arquivo requisitado, que está relacionado com o arquivo selecionado pelo ponteiro do *mouse*. A disponibilidade do *download* via *link* direto é interessante pois possibilita de forma simplificada o *download* das tabelas de rotas. O *download* pode ser feito diretamente pela página de internet, como indica a figura, ou por meio de outras ferramentas como *wget*, *rsync* ou por meio de *scripts* PHP e Shell.

Grande parte da funcionalidade do repositório foi obtida por meio do uso do conjunto oferecido pela tecnologia LAMP, acrônimo para sistema

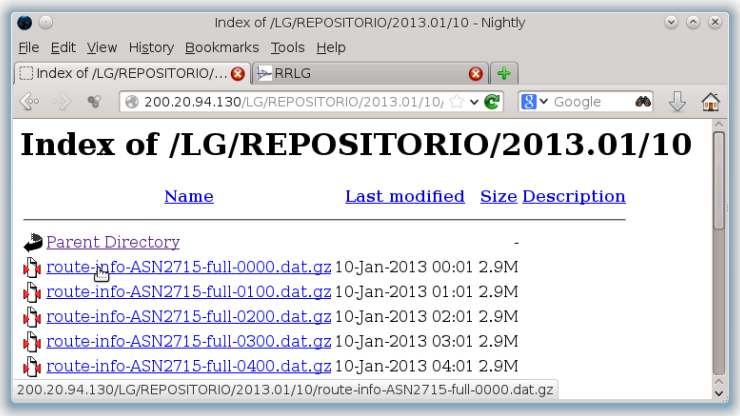

Figura 4.3: Lista contendo *links para download* das tabelas RIB-BGP.

operacional Linux, servidor *web* Apache, banco de dados MySQL e linguagem de programação PHP.

Estas tecnologias são bastante conhecidas e a literatura a respeito está amplamente disponível. Entretanto cabe destacar neste projeto o desenvolvimento e implementação de duas importantes tecnologias:

- A fim de evitar tráfegos entre redes, o servidor *web* foi alocado na mesma rede do roteador de borda e algumas configurações e serviços disponíveis no servidor foram alteradas ou desativadas, buscando reservar os recursos computacionais da máquina para as tarefas contidas no projeto.
- Um pequeno banco de dados MySQL foi implementado para armazenar o login e senhas dos roteadores. Isto reforça a segurança de acesso ao equipamento, pois as senhas desta forma são passadas via scripts, em variáveis especiais extraídas no banco de dados.

4.2 Características Técnicas

Esta sessão apresenta de forma sucinta as principais características do Repositório RIB-BGP desenvolvido.

4.2.1 Módulo de conexão remota

Telnet é atualmente, um dos principais protocolos da internet para estabelecer a conexão remota entre computadores. Através dessa conexão remota, pode-se, havendo permissão, executar programas e comandos em outra máquina.

O Telnet pode ser usado para a pesquisa de informações e transferência de arquivos. Conhecendo o protocolo e fazendo uso de linguagens de programação adequadas é possível desenvolver ferramentas computacionais similares, entretanto mais específicas, e que atinjam melhores resultados.

No sentido de desenvolver uma função específica para o estabelecimento de conexões remotas com o roteador de borda foi desenvolvida uma função em PHP, feita por meio de aberturas de *sockets*, semelhante ao telnet. Este modelo foi escolhido pela praticidade do protocolo e a sua ampla utilização entre os desenvolvedores e administradores de rede.

A principal diferença entre esta função desenvolvida e o protocolo Telnet propriamente dito é que a função utiliza acesso ao banco de dados e passa as senhas por meio de variáveis, reforçando desta forma a segurança das senhas. Esta função também está agregada a um arquivo de *log* que aponta eventuais erros de conexão.

4.2.2 Módulo de aquisição de dados

A função para comunicação remota, explicada na seção anterior, utiliza um método de conexão em que os parâmetros são passados, todos de uma única vez. Caso a conexão seja bem sucedida, é reservado na memória do computador, espaço necessário para a gravação de dados em uma variável privada do tipo texto. Esta variável, intuitivamente, armazena a RIB-BGP em texto puro. Sendo necessário, posteriormente, o tratamento de filtragem de informações reservadas à RedeRio via filtros e em seguida a compactação.

4.2.3 Modulo de armazenamento e disponibilidade na *web*

Os arquivos compactados requerem espaço de armazenamento significativamente menor do que os arquivos não compactados, embora um ou outro método de compactação resulte na perda de alguns dados porque a compactação de arquivo se destina a reduzir os requisitos de armazenamento de dados que não fornecem informações adicionais, como por exemplo páginas em branco e repetições de bits em uma palavra binária [63].

O principal resultado da compactação, é a velocidade da transferência do arquivo compactado. Mesmo um computador que pode lidar com grandes quantidades de transferência de dados pode ficar lento quando muitos usuários se conectam a ele de uma só vez. Outro resultado importante da compactação é a integridade do arquivo enviado. A transferência corre menos risco de sofrer alguma interrupção e o arquivo acabar sendo corrompido.

O método utilizado para compactar as tabelas de rotas RIB-BGP foi o *GNU zip*, conhecido como *gzip*. Este método, popular na comunidade de desenvolvedores, é suportado pelo Apache e diversos navegadores da internet também suportam sua extensão *.gz*. As RIB-BGP quando transferidas do roteador de borda, têm cerca de 47 Mb de tamanho, e após compactadas atingem cerca de 3 Mb de tamanho.

Foi feita uma suscinta comparação entre as ferramentas *gzip* e *bzip*, as duas ferramentas comuns de compactação encontradas em repositórios RIB-BGP na internet, apresentada na Tabela 4.1. Esta comparação levou em consideração os tempos de compactação, de descompactação e tamanho do arquivo compactado. A ferramenta *gzip* leva pouca desvantagem no requisito tamanho de arquivo mas possui ampla vantagem no tempo de compactação e descompactação, por este motivo foi adotado o formato *.gz*, já que o sistema RRLG preza pela leveza computacional e velocidade entre os módulos. Outro motivo que pesou para a adoção da ferramenta é o *gzip* ser nativo em praticamente todas as distribuições do sistema operacional Linux.

Tabela 4.1: Comparação entre as ferramentas Gzip e Bzip.

	Tempo de compressão (s)	Tamanho do arquivo (Mb)	Tempo de descompressão (s)
Gzip	1.48	3	0.7
Bzip	16.17	2.7	2.09
Diferença	14.7	0.3	1.39

4.2.4 Interface Gráfica

Foi atribuído ao repositório RIB-BGP uma interface gráfica com o usuário. Esta interface foi desenvolvida com tecnologias descritas anteriormente e se resume a páginas de internet amigáveis que são moldadas pelo módulo de estrutura de diretórios. O objetivo previa a estrutura de diretórios organizada hierarquicamente em diretórios diários, mensais e anuais.

4.3 Carga computacional

Com o auxílio de ferramentas de monitoramento, foram realizadas medidas de consumo durante a execução da ferramenta desenvolvida. Tendo em vista que o *hardware* disponibilizado para o projeto é o mesmo para os dois sistemas descritos neste trabalho, um computador comum com um processador de 3.4 GHz e 1 GB de mémoria, o consumo de CPU e de memória durante a execução da ferramenta são os mesmos apresentados no capítulo seguinte, na página 57.

Capítulo 5

GRRWX - Principais características

Nesta seção serão apresentadas as principais características técnicas do Sistema de Gerência da RedeRio Linux, GRRWX, desenvolvido. Ao final será feita uma abordagem aos principais módulos e ferramentas que compõem o sistema

Basicamente, o GRRWX é composto por diferentes tecnologias de *software* que serão apresentadas nas próximas seções. A escolha por estas tecnologias, foi decidida pelo custo zero exigido pelas licenças de tecnologias de *software* e também pela boa eficiência computacional que cada tecnologia contribuiu para o sistema.

O sistema GRRWX foi desenvolvido com a finalidade de atender as necessidades dos administradores da RedeRio de Computadores. A RedeRio de Computadores é um importante projeto que tem o objetivo de interconectar instituições acadêmicas, centros de ensino e pesquisa e órgãos públicos do estado do Rio de Janeiro.

As principais características do sistema GRRWX é disponibilizar os seguintes recursos e informações por meio de uma interface *web* com o usuário:

- Funções de manipulação (*insert, delete e update*) do banco de dados relativos aos equipamentos de rede (roteadores, comutadores, etc) que compõem o projeto Rederio.

- Funções de manipulação (*insert, delete e update*) do banco de dados relativos aos dados corporativos das instituições filiadas à RedeRio.
- Capacidade de obtenção de parâmetros variados dos equipamentos através do protocolo SNMP .
- Banco de dados de imagens/gráficos da taxa de utilização da banda das interfaces dos equipamentos com a ferramenta RRDTool.
- Uma visão geral da topologia da rede através do sistema Network Weathermap.

5.1 Inserção de Informações no Sistema

Em um primeiro momento, o operador do sistema deve apontar por meio de uma interação com a interface *web*, quais dispositivos de rede serão inseridos no sistema. Caso todos os apontamentos tenham sido informadas corretamente, tal como endereço IP do dispositivo e senha *community* SNMP, a base do sistema é atualizada e um novo dispositivo é disponibilizado na base de dados e então apresentado ao operador. Em seguida, o sistema automaticamente, informa a taxa percentual de uso de CPU do dispositivo recém-adicionado, identifica a quantidade de interfaces de rede e retorna para o operador uma lista com cinco colunas, explicadas a seguir:

- A primeira indica o tipo de tecnologia da interface, como por exemplo *TenGigabitEthernet*, *GigabitEhernet*, etc...
- A segunda informa se a interface já foi cadastrada no sistema e já está sendo monitorada ou se está disponível para receber cadastro.
- A terceira informa a velocidade de conexão da interface
- A seguinte indica o *status* administrativo da interface, por exemplo *up* ou *down*.
- E a última informa o IP utilizado na interface caso a interface já tenha sido cadastrada no sistema anteriormente e esteja sendo monitorada.

Em um segundo momento, o operador do sistema pode escolher no menu principal a opção cadastrar. Esta opção permite que o operador escolha qual interface dentre todos os dispositivos de rede deverá receber as informações de cadastro e iniciar o processo de monitoramento.

Por meio de uma terceira interação com a interface *web* do sistema, o operador insere os dados corporativos e técnicos pertinentes à interface associada a uma instituição ou associada a outro equipamento de rede presente no domínio da RedeRio de Computadores. Estas informações são, resumidamente as seguintes:

- Sigla da instituição ou acrônimo para a conexão associada a interface.
- Contato(s) do(s) responsável(is) técnico(s) associado a instituição filiada à RedeRio de Computadores.
- Em alguns casos, o provedor de internet associado a instituição.

Ao confirmar a operação, o operador do sistema receberá um aviso positivo caso todas as informações essencias tenham sido inseridas corretamente ou um aviso negativo. Em caso de aviso negativo, o sistema retorna o motivo da operação não ter sido concluída. No caso de aviso positivo, a base de dados do sistema é atualizada e uma nova instituição é apresentada ao operador, conforme Figura5.1, na página 52.

Uma funcionalidade que se destaca no GRRWX é a capacidade do sistema de permitir ao operador transferir informações associadas às instituições de um equipamento para o outro sem a perda de dados, ou seja, permite a edição de informações operacionais, conforme mostra a Figura 5.2, na página 52.

5.2 Aquisição de dados

O sistema GRRWX foi desenvolvido com um mecanismo de aquisição de dados que permite a coleta periódica de parâmetros de monitoramento das interfaces dos diversos dispositivos de rede apontados no sistema por meio da interface *web* do sistema. Dentre estes dispositivos, a maioria são roteadores,

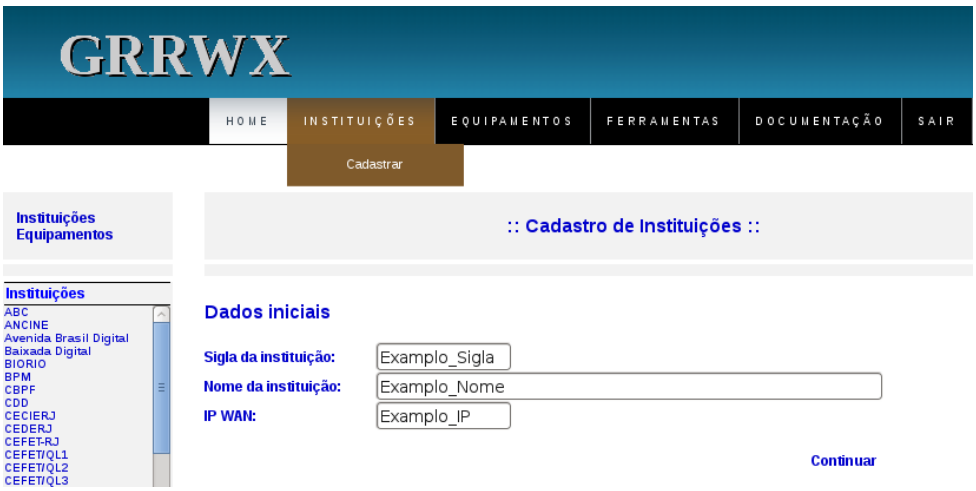

Figura 5.1: GRRWX - Tela de inserção de dados corporativos e técnicos pertinentes à interface associada a uma instituição ou associada a outro *host* presente no domínio da rede.

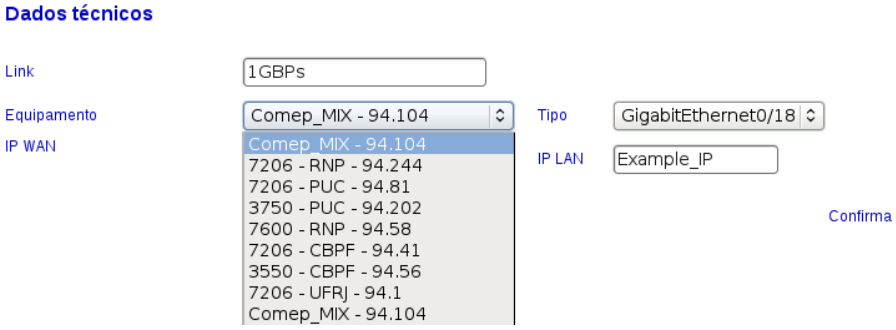

Figura 5.2: GRRWX - Tela de edição de informações de instituições associadas ao equipamento. É permitido ao operador trocar as informações relativas ao equipamento sem perda dos dados corporativos cadastrados.

switchs e comutadores que se encontram espalhados em diferentes pontos operacionais da RedeRio no estado do Rio de Janeiro.

Este mecanismo de aquisição de dados faz uso de algumas tecnologias de *software*, descritas adiante:

5.2.1 Integração PHP, SQL, RRDTool e SNMP

Integrando as tecnologias linguagens de programação PHP, linguagem descritiva de banco de dados SQL e o conjunto RRDtool e o protocolo SNMP foi possível desenvolver um mecanismo para automatizar a aquisição de dados procedentes dos parâmetros de monitoramento de dispositivos de redes. Esta técnica é amplamente difundida na comunidade e está implementada em diferentes sistemas [14, 43].

Para implementar este mecanismo, foram desenvolvidos *scripts* nas linguagens de programação PHP que encapsulam comandos SQL, SNMP e RRDTool. Neste modelo de aquisição, comandos SQL recuperam do banco de dados MySQL os registros necessários para desenvolver as requisições SNMP, cujas respostas alimentam a base de dados RRDTool. Este mecanismo é todo implementado no mesmo *script* cujo principal objetivo é realizar as consultas de monitoramento SNMP aos dispositivos inseridos no sistema pela interface *web* e gravar as respostas das consultas na base de dados RRDTool.

Caso haja falha em alguma consulta, um valor especial chamado *unknow* é gravado no banco. Este recurso permite uma normalização de valores no banco de dados, suprimindo gravações de valores muito fora da média ou valores zerados. Uma taxa limite *treshold* deve ser informada no momento da configuração do banco de dados RRDtool para definir os limites para os valores *unknow* e a quantidade de valores *unknow* que poderão ser gravados em sequência no banco.

Estes *scripts* são executados automaticamente a cada cinco minutos, por meio de uma ferramenta especial chamada *crontab*. Esta ferramenta nativa de alguns sistemas operacionais é um recurso que permite a execução automática de tarefas em datas e horários predeterminados.

5.2.2 Weathermap

Weathermap é uma ferramenta para visualização gráfica de redes de computadores. Uma característica importante desta ferramenta é a capacidade de utilização sobre bancos de dados RRDtool [64]. Desta forma, ela pode ser utilizada como uma funcionalidade complementar para o GRRWX.

O mapa de rede pode ser construído a partir de um arquivo de configuração. Neste método, o desenvolvedor por meio de *scripts*, informa todos os parâmetros necessários para o desenvolvimento do mapa, como por exemplo as coordenadas no mapa onde serão inseridos os nós da rede e as conexões entre esses nós. Em seguida, o desenvolvedor associa cada nó a um equipamento da rede e cada conexão a um par de interfaces dos equipamentos. Neste momento o desenvolvedor pode associar cada conexão do mapa a um arquivo *.RRD* presente no banco de dados RRDtool.

Ao final, o desenvolvedor pode publicar o mapa sensitivo de rede na internet, fornecendo ou não, permissão para usuários terem acesso ao mapa. Caso seja configurado, o usuário pode ter acesso às estatísticas de tráfego de rede quando clicar sobre as conexões de rede no mapa.

A comunidade de operadores de internet mencionam a importância do weathermap para o monitoramento de redes de computadores em vários trabalhos [65, 66]. Um trabalho recente [65] ressaltou a importância da ferramenta no auxilio do reparo de uma importante rede da Ásia que foi atingida por um desastre natural.

Desta forma, foi desenvolvido um mapa da RedeRio, Figura 5.3, que pode ser acessado por meio de um *link*, presente no GRRWX. Neste mapa é possível identificar os roteadores, em azul, os *swtches* em cinza, as conexões da RedeRio com a internet, representadas pelas nuvens e as instituições associadas a RedeRio, representadas pelas suas siglas. Cada conexão está associada a uma cor, que como informa a legenda, representa a taxa de bits atual que trafega pelas interfaces dos equipamentos. Ao passar o *mouse* sobre cada conexão, o operador terá acesso às estatísticas de tráfego, cujo comentário será feito na seção seguinte, referentes às últimas doze horas.

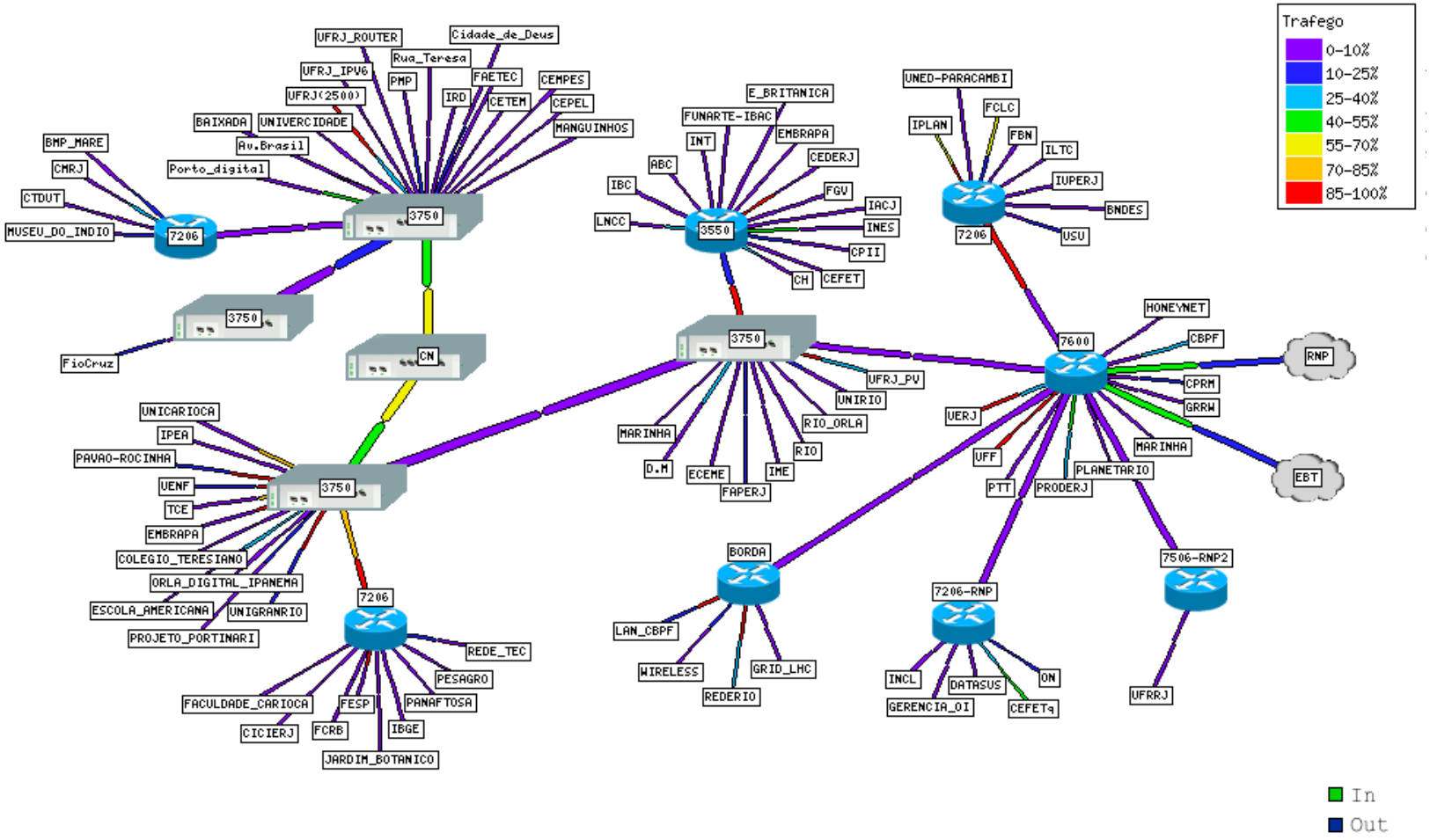

Figura 5.3: Mapa sensitivo da RedeRio de Computadores. Neste mapa é possível identificar os roteadores, os *swtches*, as conexões da RedeRio com a internet, e as instituições associadas a RedeRio.

5.2.3 Estatísticas de Tráfego

Sempre que o operador do sistema consultar informações associadas a determinada instituição cadastrada no sistema, um *script* é executado. Tecnicamente, este *script* recupera da base de dados RRDtool uma série histórica das respostas às requisições SNMP feitas a interface de rede associada a instituição.

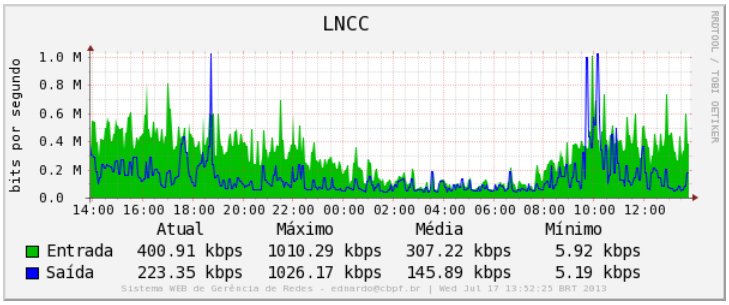

Figura 5.4: GRRWX - Gráfico de estatística de tráfego gerado pelo sistema. As cores diferenciam os fluxos de entrada e saída de dados. No topo, a sigla associada a instituição e abaixo as legendas com indicações de valores variados da taxa de bits

A partir desta série histórica, uma imagem é processada e apresentada ao operador do sistema. A Figura 5.4 apresenta a visualização do fluxo de entrada e saída de dados associados à uma instituição cadastrada no sistema.

As estatísticas são apresentas em modo gráfico, onde o eixo horizontal representa frações de tempo e o eixo vertical representa o fluxo de dados, em unidade de bits por segundo.

O gráfico foi configurado para apresentar as estatísticas de tráfego em um período de 12 horas divididas em grades que representam janelas de tempo de 30 minutos. Cada linha contida em uma janela é resultado de uma média aritmética entre 6 amostras recuperadas da base de dados RRDtool. Caso haja entre os valores recuperados, um valor *unknow* ele é descartado e a média aritmética passa a ser entre 5 amostras e assim sucessivamente. Se todas as amostras recuperadas forem valores *unkown*, a janela do gráfico é preenchida com linhas em branco.

Ainda foram adicionados ao gráfico legendas de indicação rápida com os valores atuais, médios, máximos e mínimos do fluxo de dados e ao rodapé uma marca d'água com data, identificação do gráfico e *e-mail* para contato.

O sistema GRRWX ainda disponibiliza mais uma funcionalidade para visualização das estatísticas de tráfego. Ao clicar sobre a imagem de consulta às informações associadas às instituições, uma nova janela é apresentada ao operador do sistema. Nesta janela estão contidas quatro outras imagens. A primeira representa as estatísticas de tráfego compreendidas em um período de dois dias, a segunda em um período de três dias, a terceira uma semana e a quarta, 1 mês.

5.3 Desempenho

Com a utilização de ferramentas que calculam o tempo de execução de determinados processos computacionais foi possível aferir que o tempo médio gasto pelo sistema para realizar as consultas SNMP e gravação das respostas nos arquivos RRDs foi de menos de um minuto. Este tempo foi aferido quando os dispositivos de redes operavam com a carga computacional abaixo de 60%.

Com o auxílio da ferramenta de monitoramento de recursos computacionais *top*, foram realizadas medidas de consumo durante a execução do sistema GRRWX. O *hardware* disponibilizado para o projeto é um computador com um processador de 3.4 GHz e 1 Gb de memória e o seu *load average* durante a execução da ferramenta não ultrapassa 0.8%, conforme Figura 5.5 e o consumo de memória se mantém da faixa de 15%, Figura 5.6, na página 58.

É aconselhável que o servidor que hospeda o sistema esteja na mesma rede de computadores dos dispositivos que serão monitorados. Testes indicaram que algumas configurações de filtros e *firewall* podem forçar o descarte de pacotes SNMP nos dispositivos. Outra forma de descarte é que alguns fabricantes indicam, nos manuais de seus produtos, que o descarte de pacotes acorrem quando a CPU atinge carga a partir de 60 porcento.

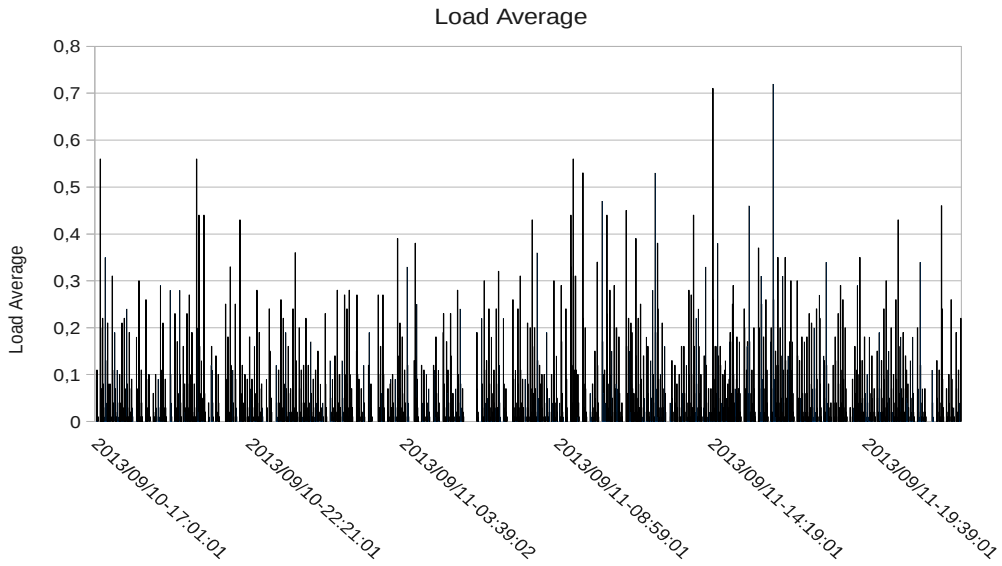

Figura 5.5: GRRWX - Gráfico de *Load Average* gerado pelo sistema

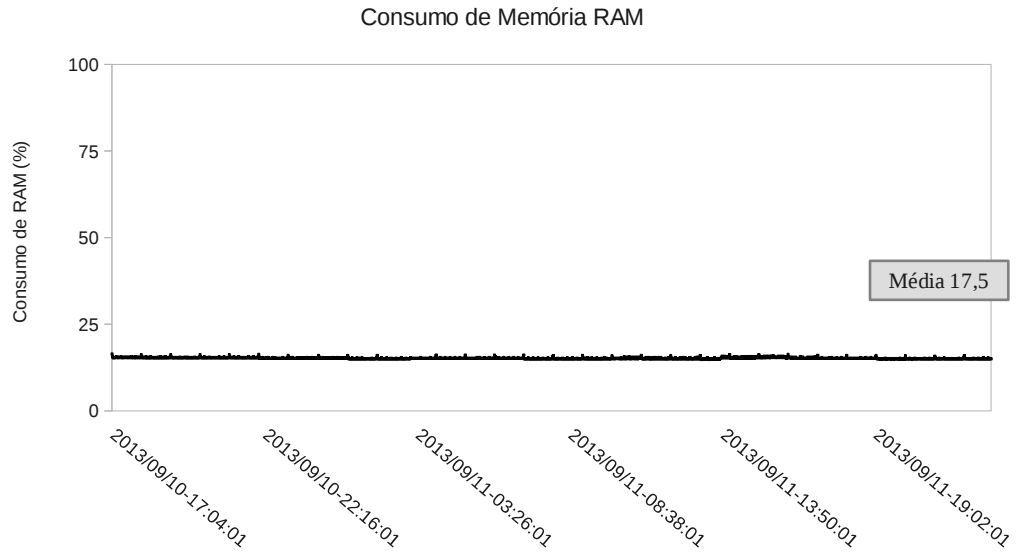

Figura 5.6: GRRWX - Gráfico do consumo percentual de mémoria.

Capítulo 6

Conclusões

O objetivo deste trabalho é o desenvolvimento de um sistema de monitoramento de redes. Este sistema se divide em duas partes, RRLG e GRRWX, que recebem destaque neste documento nos capítulos 4 e 5, respectivamente. Diante disto, este capítulo de conclusões será dividido nas seguintes seções:

- RRLG
- GRRWX
- Perspectivas futuras

6.1 RRLG

Inicialmente, o sistema RRLG permite qualquer usuário conectado a internet, executar comandos predefinidos no roteador de borda da RedeRio de Computadores.

Os sistemas LG estão disponíveis em toda a internet. Normalmente, as informações prestadas por sistemas deste tipo são disponibilizadas pelas próprias organizações que respondem pelos roteadores de borda [67, 68] ou são divulgados por portais públicos [69], que relacionam vários LGs em um único sítio da internet.

Além da funcionalidade de oferecer alguns comandos BGP predefinidos, comum à maioria dos sistemas deste tipo, o RRLG oferece um repositório

RIB-BGP. Este repositório é composto de uma série de tabelas de rotas BGP organizadas cronologicamente, adquiridas do roteador de borda da RedeRio de Computadores. Estas tabelas recebem tratamento por meio de filtros para preservar informações internas da RedeRio e em seguida são alocadas em um servidor *web*.

O repositório RIB-BGP é composto de alguns módulos, que se resumem em ferramentas computacionais que também foram desenvolvidas durante o projeto. Destacam-se no repositório RIB-BGP as seguintes ferramentas:

a) Módulo de conexão remota.

b) Módulo de aquisição de dados.

c) Módulo de armazenamento e transferência de dados para a *web*.

As ferramentas computacionais implementadas neste sistema receberam destaque pela simplicidade do código e velocidade no desenvolvimento. Os resultados obtidos mostram que a metodologia implementada nos módulos desenvolvidos aproximam-se dos resultados vistos em repositórios semelhantes. Além disso, no sentido de análise técnica da ferramenta, a mesma não proporciona um alto custo computacional, conforme foi observado na seção 4.3, na página 48. Este resultado indica que o sistema desenvolvido é leve e não depende de computadores com alta capacidade de processamento.

a) A função utilizada para conexão remota, comentada na seção 4.2.1, página 46, utiliza um método simples para conexão com equipamentos de rede, baseado em telnet e bastante difundido pela comunidade de desenvedores. Este método pode ser facilmente adaptado a novos cenários sem a necessidade de grande alteração no código.

b) Caso a conexão remota seja bem sucedida, o módulo de aquisição de dados assume a tarefa de reservar espaço em memória proporcional ao tamanho da tabela de rotas no roteador de borda e em seguida, tranferir esta tabela do equipamento para o repositório. A metodologia utilizada neste módulo, envolve técnicas tradicionais de manipulação de arquivos desenvolvidas em linguagens de programação PHP e Shell Script.

c) O módulo de armazenamento e transferência de dados para a *web* recebe os dados adquiridos pelo módulo anterior e assume a fase seguinte, composta de duas partes: i) compactação das tabelas de rotas e ii) interface gráfica para acesso ao repositório.

i) Foi feita uma breve análise entre as ferramentas *gzip* e *bzip*, duas ferramentas comuns encontradas en repositórios semelhantes. Nesta análise, que se encontra na seção 4.2, na página 45, foi verificado que o modelo de compactação de arquivos *gzip* reduzem em 93% o tamanho das tabelas exportadas para o repositório RIB-BGP em menos de 2 segundos enquanto *bzip* demora mais de 16 segundos para atingir quase o mesmo resultado. Tendo em vista que o sistema RRLG preza pela leveza e velocidade entre os módulos, foi adotado o formato *.gz* como padrão.

ii) No sentido de organizar e oferecer uma interface adequada para o *download* das tabelas RIB-BGP foi atribuído ao repositório uma estrutura de diretórios diários, mensais e anuais, onde o interessado pode acessar e baixar as tabelas RIB-BGP do seu interesse por meio de um *link* direto. A disponibilidade do *download* via *link* direto é interessante pois possibilita o *download* diretamente pela página de internet, conforme mostrado na Figura 4.3, na página 45, e também por meio de outras ferramentas como *wget*, *rsync* entre outras, conforme explicado na seção 4.1, página 43.

6.2 GRRWX

Outro sistema desenvolvido, com o mesmo nível de importância do RRLG, é o sistema de Gerência da RedeRio *web* versão linuX, que atualmente está em operação na RedeRio de Computadores auxiliando os administradores no controle, operação, administração e manutenção da rede.

Destacam-se neste sistema:

a) Módulo de interface com o usuário: foi desenvolvido para este sistema, uma interface *web*, apresentada na seção 5.1, na página 50. Por meio

desta interface, o operador do sistema pode definir, em poucas etapas, quais *hosts* deseja monitorar. Uma das funcionalidades em destaque é a facilidade de transferir informações associadas a instituições de um equipamento para outro equipamento sem perdas de dados.

b) Mecanismo de geração de gráficos: outro aspecto que destacou-se no sistema GRRWX é o mecanismo de geração de imagens/gráficos. Comparado a mecanismos de outros sistemas relacionados, este apresentou vantagem, visto que o processamento de imagens, no sistema GRRWX, ocorre somente no momento que o operador faz consultas às informações do sistema.

c) Mapa sensitivo da rede: Com a integração da ferramenta *Weathermap* ao sistema, tornou-se possível associar as conexões de rede monitoradas pelo sistema a uma única imagem, apresentada pela Figura 5.3, na página 55. Nesta imagem, as conexões são exibidas em determinadas cores, que representam o fluxo de dados entre os *hosts* da rede. Esta e outras funcionalidades oferecem ao operador do sistema uma visão panorâmica da rede e configura uma solução de fácil visualisação das conexões e do fluxo de dados na rede.

d) SNMP: Este protocolo foi de essencial importância para o desenvolvimento deste sistema. Na tentativa de melhorar a velocidade de comunicação entre as diferentes tecnologias de *software*, foram configurados módulos do SNMP no servidor *web* para que os comandos SNMP pudessem ser executados diretamente pelo Apache, sem a necessidade de fazer chamadas a *scripts* externos. Esta configuração, além de eficiente, trouxe também menos dependência ao sistema.

6.3 Perspectivas Futuras

O sistema GRRWX foi desenvolvido de forma a receber atualizações e adição de novos recursos de acordo com a necessidade dos administradores da RedeRio de Computadores. O próximo passo é adaptar mais funcionalidades ao sistema, algumas sugeridas pelo próprio desenvolvedor do trabalho e

outras pelos próprios administradores, como:

a) Gerência das redes de conexão: Automação do mecanismo de configuração das redes de conexão que são atribuídas aos equipamentos do projeto RedeRio de Computadores. Esta funcionalidade irá melhorar a fase de cadastro das instituições que atualmente é realizada em três passos. Consequentemente, esta melhoria irá atender também a organização dos diversos blocos de redes administrados pela RedeRio.

b) Integração com outros sistemas de gerência da RedeRio: Esta etapa futura prevê o compartilhamento das informações entre os diferentes sistemas ativos da RedeRio, dentre eles, o mapa da RedeRio disponibilizado para as instituições associadas ao projeto e o sistema utilizado pela equipe de segurança de redes da RedeRio.

c) Envio de alertas em caso de falhas: Utilizando ferramentas de correio eletrônico e envio de mensagem de texto, é possível criar um sistema de alertas que possa auxiliar os administradores em suas tarefas em caso de falhas nas redes.

A perspectiva futura em relação ao RRLG é a comparação e análise entre as tabelas de rotas BGP adquiridas pelo repositório RIB-BGP, e várias tabelas BGP coletadas em diferentes repositórios da internet. Pretende-se com isto, reunir todos os objetos destas tabelas em uma nova tabela BGP. Um trabalho semelhante [61], publicado há cerca de 10 anos, mostra uma tabela resultante da união de outras seis, coletadas em diferentes repositórios RIB-BGP. Esta nova tabela apresentou um incremento de 16% no número de conexões e 0.7% no número de ASs. Este fenômeno ocorre principalmente porque algumas destas conexões e ASs acabam sendo escondidos nas tabelas de rotas devido a políticas de roteamento. Nesta nova etapa, as diversas tabelas de rotas adquiridas no roteador de borda da RedeRio e em roteadores de borda distintos, serão consideradas diferentes perspectivas da internet. O objetivo é desenvolver uma visão "holográfica" da internet mundial. Esta "holografia" será resultante da reunião destas perspectivas e o interessado poderá observar a internet de uma perspectiva mais completa.

Bibliografia

[1] Alexander Clemm. *Network management fundamentals*, volume 800. Cisco Press Indianapolis, 2006.

[2] Ademarlaudo França Barbosa; et al. *Projeto Conceitual do Laboratório de Instrumentação Científica* - LIC. Centro Brasileiro de Pesquisas Físicas, 2008.

[3] Artur Batista VILAR. *Instrumentação para Observação de Fluorescência de Raios Cósmicos com Fotomultiplicadora Multianódica*. PhD thesis, dissertação de Mestrado do CBPF, 2009.

[4] Rafael Gonçalves Gama. *Desenvolvimento de instrumentaçao baseada em lógica programável para aquisiçao de dados no Projeto Neutrinos Angra*. PhD thesis, Dissertaçao de Mestrado/CBPF, 2011.

[5] RF Neumann, M Bahiana, LG Paterno, MAG Soler, JP Sinnecker, JG Wen, and PC Morais. Morphology and magnetism of multifunctional nanostructured gamma fe _2 films: Simulation and experiments. *arXiv preprint arXiv:1108.6099*, 2011.

[6] Márcio Portes de Albuquerque, Andrea Murari, M Giovani, Nilton Alves, and F Romanelli. A 10 000-image-per-second parallel algorithm for real-time detection of marfes on jet. *Plasma Science, IEEE Transactions on*, 41(2):341–349, 2013.

[7] Genildo Nonato Santos. *CARACTERIZAÇÃO DO REGISTRADOR MULTIPROPÓSITO MODULAR PARA MONITORAMENTO REMOTO (CAIPORA)*. PhD thesis.

[8] Fernando Marcio Barcellos de Sousa. *Lógica programável aplicadaa aquisiçao e transmissao serial de dados em alta velocidade via barramento PCI Express*. PhD thesis.

[9] Antonio Matheus Benaion Esteves. *Sistema de monitoramento de redes com STP*. PhD thesis.

[10] Embrapa Informática. *Equipamentos do Laboratório Multiusuário de Bioinformática*. http://www.lmb.cnptia.embrapa.br/web/lmb/parque-computacional1, 2013.

[11] Universidade Estadual de Campinas. *Novo parque computacional de alto desempenho*. http://www.unicamp.br/unicamp/noticias/unicamp-inaugura-novo-parque-computacional-de-alto-desempenho-0, 2008.

[12] Rede Nacional de Pesquisa. *Redes Comunitárias de Educação e Pesquisa*. http://www.redecomep.rnp.br, 2013.

[13] Kevin Schmidt Douglas Mauro. *Essential SNMP*. O'Reilly Media, 2001. ISBN 978-0-596-00020-2.

[14] Steve Shipway. *Using MRTG with RRDtool and Routers2*. Cheshire Cat Computing, 3ª edition, 2010.

[15] Felipe Costa. *Ambiente de Rede Monitorado com Nagios e Cacti*. Ciência Moderna, 2008. 9788573936858.

[16] www.routeviews.org. visitado em 20/11/2012.

[17] Xiaoqiao Meng, Zhiguo Xu, Beichuan Zhang, Geoff Huston, Songwu Lu, and Lixia Zhang. Ipv4 address allocation and bgp routing table evolution. *ACM SIGCOMM Computer Communication Review (CCR) special issue on Internet Vital Statistics*, January 2005.

[18] Geoff Huston. Ipv4-how long have we got? In *IEPG meeting*, 2003.

[19] Xiaoqiao Meng, Zhiguo Xu, S Lu, and L Zhang. An analysis of bgp routing table evolution. *Techincal Report*, 30046, 2003.

[20] Qian Chen, Hyunseok Chang, Ramesh Govindan, and Sugih Jamin. The origin of power laws in internet topologies revisited. In *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 2, pages 608–617. IEEE, 2002.

[21] Cliff C Zou, Don Towsley, Weibo Gong, and Songlin Cai. Routing worm: A fast, selective attack worm based on ip address information. In *Proceedings of the 19th Workshop on Principles of Advanced and Distributed Simulation*, pages 199–206. IEEE Computer Society, 2005.

[22] Zesheng Chen, Chuanyi Ji, and Paul Barford. Spatial-temporal characteristics of internet malicious sources. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pages 2306–2314. IEEE, 2008.

[23] Daniel J. Power. Web-based decision support systems. volume 2. The On-Line Executive Journal for Data-Intensive Decision Support, 1998.

[24] Jim Gray Daniel and Daniel P. Siewiorek. High availability computer systems. *IEEE Computer*, 24:39–48, 1991.

[25] Yair Amir, Danny Dolev, Shlomo Kramer, and Dalia Malki. Transis: A communication subsystem for high availability. In *Fault-Tolerant Computing, 1992. FTCS-22. Digest of Papers., Twenty-Second International Symposium on*, pages 76–84. IEEE, 1992.

[26] James F. Kurose; Keith W. Ross. *Computer Networking: a Top-Down Approach Featuring the Internet.* Addison-Wesley, 2006. ISBN 8588639181.

[27] Products and services network management system: Best practices. White Paper, Cisco, 2007. Document ID:15114.

[28] Andrew S. Tanenenbaum. *Modern Operating Systems.* Makron Books, 2007. ISBN 0130313580.

[29] David L Tennenhouse, Jonathan M Smith, W David Sincoskie, David J Wetherall, and Gary J Minden. A survey of active network research. *Communications Magazine, IEEE*, 35(1):80–86, 1997.

[30] Ann Chervenak, Ian Foster, Carl Kesselman, Charles Salisbury, and Steven Tuecke. The data grid: Towards an architecture for the distributed management and analysis of large scientific datasets. *Journal of network and computer applications*, 23(3):187–200, 2000.

[31] Ian Foster, Carl Kesselman, Craig Lee, Bob Lindell, Klara Nahrstedt, and Alain Roy. A distributed resource management architecture that supports advance reservations and co-allocation. In *Quality of Service, 1999. IWQoS'99. 1999 Seventh International Workshop on*, pages 27–36. IEEE, 1999.

[32] Warren Matthews and Les Cottrell. The PingER project: active internet performance monitoring for the HENP community. *Communications Magazine, IEEE*, 38(5):130–136, 2000.

[33] Vassilis Prevelakis. A secure station for network monitoring and control. In *Information Security Management & Small Systems Security*, pages 103–116. Springer, 1999.

[34] Luca Deri and Stefano Suin. Ntop: Beyond ping and traceroute. In *Active Technologies for Network and Service Management*, pages 271–283. Springer, 1999.

[35] Lishen Yang and Qiang Wang. Analysis of network management technology and development trend in the future. In *Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering*. Atlantis Press, 2013.

[36] Zhaung Wu. The principe and realization of computer network management. In *Eletronic Industry Press*, pages 15–20, 2009.

[37] Snmp counters: Frequently asked questions. White Paper, Cisco, 2007. Document ID:26007.

[38] Tatu Ylonen. SSH–secure login connections over the Internet. In *Proceedings of the 6th USENIX Security Symposium*, pages 37–42, 1996.

[39] Daniel J Barrett and Richard E Silverman. *SSH, the Secure Shell: the definitive guide*. O'Reilly Media, Inc., 2001.

[40] Shamkant B. Elmasri, Ramez; Navathe. *Fundamentais of Database Systems*. Pearson Education, 2004.

[41] S. Sudarshan; Silberschatz, Avi; Hank Korth. *Database System Concepts*. McGramHill, 2006. ISBN 0-07-295886-3.

[42] http://oss.oetiker.ch/rrdtool/. visitado em 20/07/2011.

[43] www.cacti.net/. visitado em 25/07/2011.

[44] www.zenoss.com/. visitado em 25/07/2011.

[45] Shann-Chiuen Wu, Yung-Chung Ku, and Tzao-Lin Lee. Zero-configuration security module for LAMP application system. In *Asia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE*, pages 113–116. IEEE, 2008.

[46] UV Ramana and TV Prabhakar. Some experiments with the performance of LAMP architecture. In *Computer and Information Technology, 2005. CIT 2005. The Fifth International Conference on*, pages 916–920. IEEE, 2005.

[47] Andrea Bonaccorsi and Cristina Rossi. Why open source software can succeed. *Research policy*, 32(7):1243–1258, 2003.

[48] Arianne Vivian de Souza Figueiredo, Diogo Dias Santos, Eduardo Massao Tomimori, Frank César Silva, and Isabella Tamine Parra Miranda. Softwares livres: Vantagens. *Maringá Management*, 2(1), 2006.

[49] http://www.linuxfoundation.org/. visitado em 10/07/2013.

[50] http://news.netcraft.com/archives/category/web-server survey, 05 2011. visitado em 26/05/2011.

[51] Cristina Duarte Murta, Virgılio Almeida, and Wagner Meira Jr. Analyzing performance of partitioned caches for the WWW. In *Proceedings of the 3rd International WWW Caching Workshop*, 1998.

[52] Yiming Hu, Ashwini Nanda, and Qing Yang. Measurement, analysis and performance improvement of the apache web server. In *Performance, Computing and Communications Conference, 1999 IEEE International*, pages 261–267. IEEE, 1999.

[53] http://news.netcraft.com/archives/2013/01/31/php-just-grows grows.html. visitado em 05/03/2013.

[54] Nilton ALves Jr. *Caracterização de Redes Complexas - Aplicação à Modelagem Relacional entre Sistemas Autônomos da Internet.* PhD thesis, UERJ - IPRJ, 2007.

[55] Geoff Huston. Exploring autonomous system numbers. *The Internet Protocol Journal*, 9(1), 2006.

[56] Andre Broido; KC Claffy. Analysis of routeviews BGP data: policy atoms. Santa Barbara, CA, 2001. Network Resource Data Management Workshop.

[57] Xenofontas Dimitropoulos; KC Claffy; et al. Classifying the types of autonomous systems in the internet. Philadelphia, PA, 2005. SIGCOMM.

[58] Tian Bu; Don Towsley. On distinguishing between internet power law topology generators. volume 2, pages 638–647, New York, NY, 2002. IEEE INFOCOM.

[59] Rodrigo Augusto Alves; Cristina Duarte Murta. Análise da topologia dos sistemas autônomos: Evolução e predição. Rio de Janeiro, RJ, 2008. 26º Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos.

[60] Hyunseok Chang; Ramesh Govindan; et al. On inferring AS-level connectivity from BGP routing tables. New York, NY, 2002. IEEE INFOCOM.

[61] José M. Barceló; Juan I. Nieto-Hipólito; Jorge García-Vidal. Study of internet autonomous system interconnectivity from BGP routing tables. (45):333–344, 2004.

[62] Lixin Gao. On inferring autonomous system relationships in the internet. *IEEE/ACM Transactions on Networking*, Vol 9(6), 2001.

[63] http://techtips.salon.com/file-compression-important-internet 11385.html. visitado em 20/11/2012.

[64] http://www.network weathermap.com. visitado em 19/08/2012.

[65] Yasuichi Kitamura, LEE Youngseok, Ryo Sakiyama, and Koji Okamura. Experience with restoration of asia pacific network failures from taiwan earthquake. *IEICE transactions on communications*, 90(11):3095–3103, 2007.

[66] Edwin D Vinas and T Baba. Characterization, analysis, and visualization of traffic in the asian internet interconnection initiatives (ai3) satellite-based research network test bed. In *Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on*, pages 41–45. IEEE, 2003.

[67] http://www.rnp.br/servicos/lg/. visitado em 22/07/2013.

[68] http://lg.cern.ch/. visitado em 22/07/2013.

[69] http://www.bgp4.com.br/. visitado em 22/07/2013.

Apêndice A

Publicação

Foi publicado uma Nota Técnica intitulada Repositório BGP, cuja página de rosto é apresentada na página seguinte. Esta Nota Técnica foi publicada dia 02 de agosto de 2013 na revista Notas Técnicas do CBPF e pode ser acessada por meio do seguinte endereço eletrônico: dx.doi.org/10.7437/NT2236-7640/2013.02.001

dx.doi.org/10.7437/NT2236-7640/2013.02.001
Notas Técnicas, v. 3, n. 2, p. 1–6, 2013

Desenvolvimento de um Repositório RIB-BGP

Ednardo F. Miranda, Nilton Alves Jr. e Marcelo Giovani M. Souza*
Centro Brasileiro de Pesquisas Fisicas - Rio de Janeiro - RJ - Brasil - CEP:22290-180
(Dated: 2 de Agosto de 2013)

Repositórios RIB-BGP (*Route Information Base - Border Gateway Protocol*) são servidores distribuídos na internet que disponibilizam cópias da tabela de informação de rotas BGP em determinados momentos de observação. Estas tabelas de informações de rotas são ingredientes essenciais para o processo que envolve as relações entre os sistemas autônomos e podem ser utilizadas para monitorar aspectos importantes da internet. O objetivo deste trabalho é apresentar e descrever as principais características de um repositório RIB-BGP implantado anteriormente que adquire e armazena tabelas de rotas e disponibiliza estes dados para consultas na internet. A análise de alguns parâmetros de desempenho da ferramenta e a forma de armazenamento dos dados fazem parte do escopo deste trabalho.

BGP Full Rounting Tables; Internet; Desenvolvimento de software; Aquisição de dados; Análise de desempenho.

1. INTRODUÇÃO

Repositórios RIB-BGP (*Route Information Base-Border Gateway Protocol*) foram inicialmente criados para oferecer, aos operadores de internet, uma ferramenta para obter informações em tempo real a respeito do sistema de rotas sobre diferente perspectivas na internet [1]. Com o passar do tempo, vários autores descreveram diferentes metodologias para medir, inferir e modelar o crescimento da internet, tendo como base tabelas de rotas BGP, que será referida neste documento como RIB-BGP.

Certos autores [2, 3], revelaram que o comportamento da distribuição da internet é baseado em leis de potência e assim associados a curvas exponenciais, outros autores [4] desenvolveram um conjunto de métricas para caracterizar a topologia da internet, outros recentes [5], revelaram que estas análises devem ser feitas ao longo do tempo, pois acredita-se que a internet vem experimentando uma nova fase de evolução atualmente. Embora os resultados procurem responder questões diferentes, a base de dados é semelhante a todos: a tabela de rotas BGP.

O objetivo deste trabalho é apresentar e descrever as principais características de um repositório RIB-BGP desenvolvido e implantado que adquire e armazena tabelas de rotas RIB-BGP e disponibiliza estes dados para consulta na internet. Observações sobre o desempenho do repositório desenvolvido e considerações sobre a forma de armazenamento utilizada também fazem parte do escopo deste trabalho.

2. BGP

2.1. Sistemas Autônomos

A internet passa por um gigantesco crescimento em tamanho e complexidade desde o início da sua comercialização, na década de 90. Nela, se conectam milhares de Sistemas Autônomos (ASs). ASs podem ser definidos sob o seguinte conceito: Um conjunto de redes locais e roteadores operados pelo mesmo grupo de administradores de rede e submetidos a uma mesma política de operação.

Cada AS é identificado por um número, ASN, entre 1 e 65536. Este número é fornecido por um órgão de controle e é utilizado nas configurações dos roteadores que farão as conexões entre ASs e será a sua assinatura para toda a internet. Os dados para o desenvolvimento do repositório RIB- BGP descrito neste trabalho foram obtidos no AS 2715.

O número de sistemas autônomos cresce diariamente, até 1994 este número não chegava a 5000, em 2012 este número ultrapassou a casa dos 40.000, Figura 1.

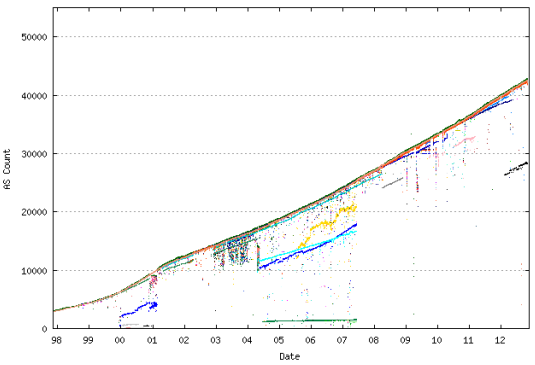

Figura 1: Crescimento do número de ASs, (dados da Universidade de Oregon) http://bgp.potaroo.net/bgprpts/rva-index.html, Nov/2012

Cada AS tem um conjunto de roteadores que agrega uma ou mais redes locais. Este conjunto de roteadores distribuem o tráfego de informação internamente entre suas redes locais. Estes roteadores internos trocam informações através de protocolos que tem a função principal de informar aos demais roteadores do AS quais as redes locais cujo o acesso é

*ednardo@cbpf.br; naj@cbpf.br; mgm@cbpf.br

Índice