XV INIC Encontro Latino Americano de Iniciação Científica
XI EPG Encontro Latino Americano de Pós Graduação
V INIC Jr Encontro Latino Americano de Iniciação Científica Júnior

NETZ – SISTEMA DE APOIO À GERÊNCIA DE REDES

Alana de Almeida Brandão, Frederico Ferreira Costa, Profª Crishna Irion

Universidade do Vale do Sapucaí/Sistemas de Informação, alana.brandao@yahoo.com.br
Universidade do Vale do Sapucaí/Sistemas de Informação, fredericoferreira@live.com
Universidade do Vale do Sapucaí/Sistemas de Informação, crishnairion@gmail.com

Resumo- O gerenciamento, em qualquer área, é essencial para que os serviços exigidos a um determinado sistema funcionem corretamente e satisfaçam as necessidades de seus usuários. Este trabalho apresenta a construção de um sistema de apoio ao gerenciamento de redes de computadores, que além de fornecer gráficos e tabelas exibindo a situação da rede, também será capaz de alertar aos gestores através de *e-mail* e SMS sobre as mudanças e eventos ocorridos no ambiente computacional.

Palavras-chave: sistema, gerência, redes
Área do Conhecimento: Sistemas de Informação

Introdução

As redes de dados, que segundo Tanenbaum (2003) são um conjunto de computadores autônomos, interconectados por uma única tecnologia, se encontram em um número muito grande de instituições e fornecem maneiras para que estas economizem e compartilhem recursos. O gerenciamento das redes é um processo importante, pois pode possibilitar maior controle, garantir desempenho e a prover uma ampliação do aproveitamento dos recursos das redes.

Uma empresa não pode perder o controle de sua rede, nem correr o risco de seus usuários utilizarem exageradamente os recursos. Não pode se arriscar na ocorrência de possíveis invasões ou uso indevido de seus dados. Portanto, a gerência não pode parar, e os *softwares* de apoio à gerência devem prover maneiras para que o gestor conheça o que ocorre no ambiente computacional mesmo não estando conectado à ela. S*oftwares* de apoio à gerência de redes geralmente são ferramentas caras e muitas empresas deixam de utilizar um produto deste tipo por não poderem fazer tal investimento financeiro. O sistema desenvolvido, neste trabalho, será um *software* livre e *open source*, de forma que qualquer pessoa ou empresa poderá utilizá-lo gratuitamente e seu código fonte poderá servir para que acadêmicos de qualquer instituição possam compreender as tecnologias que foram empregadas e utilizá-las para outros fins.

Este trabalho tem como objetivo geral desenvolver um sistema de informação que apóie a gerência de redes, permitindo a visualização e acompanhamento, em tempo real, das atividades que ocorrem dentro da rede de computadores. Para que se consiga a realização do objetivo geral, os objetivos específicos são: analisar os conceitos de redes e seu gerenciamento; construir uma ferramenta de análise com relatórios e gráficos sobre as ações e tráfego de informações; e apresentar a utilização de sistema *workflow*, com notificações via SMS e *e-mail* sobre o estado e possíveis problemas existentes no ambiente computacional.

Metodologia

O tipo de pesquisa deste trabalho classifica-se como sendo aplicada, que é aquela no qual o pesquisador utilizará os conhecimentos obtidos durante a pesquisa para aplicá-la em um projeto real e conhecer os seus resultados. Barros e Lehfeld (1986) citam que esse tipo visa aplicar soluções aos problemas do cotidiano.

O *software* desenvolvido, neste projeto, será capaz de apoiar a gerência da rede, ajudando a prover um maior controle do que ocorre no ambiente computacional. Empresas de qualquer segmento poderão utilizar este sistema, desde que possuam uma infraestrutura de computadores conectados em rede, a presença de um aparelho centralizador de nós (como, por exemplo, um roteador, *hub* ou *switch*) e um computador que funcione como um servidor, no qual o *software* será instalado e passará a funcionar.

Para compreender o funcionamento das redes de computadores foram estudados seus conceitos e modelos de referência. Os modelos de referência são importantes, pois atuam como uma diretriz funcional para que fornecedores criem produtos compatíveis e para que o desenvolvimento das tecnologias de rede sigam o mesmo padrão.

Os modelos de referência mais utilizados são o modelo OSI e o TCP/IP. Soares, Guido e Colcher (1995) ressaltam que o modelo OSI por si

só não define a arquitetura de uma rede, pois ele não especifica os serviços e protocolos exatos que devem ser usados em cada camada, ele apenas informa o que cada camada deve fazer, sendo apenas um modelo teórico. O modelo TCP/IP é amplamente utilizado na internet, na criação de grandes conjuntos de redes privadas e em inúmeros produtos de *software* usados em várias plataformas de comunicação (Microsoft, 2011). Por esse motivo o escolhido para o desenvolvimento do *software* neste trabalho foi o TCP/IP.

Este trabalho encontra-se em desenvolvimento, e para isso estão sendo seguidas as fases da metodologia ICONIX, que segundo Rosenberg e Scott (1999), é uma metodologia incremental, iterativa e que utiliza técnicas da *Unified Modeling Language* (UML). Primeiro foram identificados os requisitos com base na análise das normas 10164-1 a 10164-13 da ISO, que ditam como devem ser os sistemas de gerenciamento de redes. Logo após foi criado um modelo de domínio e um protótipo com as principais telas do sistema. Os casos de uso foram identificados e detalhados através de fluxos de eventos. Os diagramas de robustez e de sequência foram elaborados e após esses passos foi iniciado o desenvolvimento do projeto, juntamente com a criação de testes unitários.

O desenvolvimento do projeto está sendo realizado através da linguagem de programação Java, que foi criada pela Sun Microsystems e teve sua primeira versão lançada em 1995 (Costa, 2008). Por causa do seu grande potencial e usabilidade, se tornou uma das mais utilizadas no mundo. Para coletar as informações da rede, está sendo utilizado, neste trabalho, o conceito de *sniffers*, também conhecidos como analisadores de pacotes, que são programas que tem a habilidade de interceptar o tráfego que passa pela rede. Através do estudo deste tráfego capturado é feita uma análise para identificar problemas e ações ocorridas no ambiente computacional, e, a partir disto, são criados gráficos, tabelas e mecanismos de notificações via *e-mail* e SMS. A captura de pacotes na rede está sendo realizada através da API JPcap, que é uma biblioteca *open source* que captura e envia pacotes na rede, identificando seus tipos e gerando objetos correspondentes em Java (Fujii, 2007). A criação de gráficos está sendo feita através da JFreeChart, uma biblioteca criada em 2000 por David Gilbert (JFreeChart, s.d.). O envio das mensagens SMS é realizado pelo *software* a partir de *gateways* SMS e o envio de *e-mail* através da biblioteca Commons Email.

Resultados

O projeto ainda está em fase de desenvolvimento, mas já existem alguns resultados que podem ser observados com o que já foi criado. A construção do *software* está se baseando no conceito de captura de pacotes que trafegam na rede, de forma que a análise do tráfego está permitindo a criação de gráficos e tabelas.

Existem duas maneiras de se receber os pacotes da rede utilizando a API do Jpcap: abrir uma interface de rede e aguardar que os pacotes sejam capturados, chamado de método de *call-back*, ou capturá-los manualmente, chamado de método *one-by-one*. Foi testado primeiramente o *call-back* e verificou-se que ele não funciona corretamente, pois como cita Fujii (2007), nesse método deve-se esperar que a função que captura os pacotes seja chamada pelo Jpcap. No método *one-by-one* a aplicação criada é quem chama a função de captura e recebe os pacotes – sua desvantagem é que ela deve ser chamada o tempo todo, mas são capturados todos os pacotes de forma correta. O segundo método foi o escolhido para ser usado nesse *software*.

Para salvar o tráfego capturado foi feito uso do gerenciador de banco de dados PostgreSQL, que foi escolhido por ser uma ferramenta *open source* e oferecer armazenamento ilimitado. Outro fator que influenciou na escolha deste banco de dados é que ele funciona em várias plataformas de sistemas operacionais, sendo capaz de gerenciar uma quantidade muito grande de dados (PostgreSQL, s.d.)

Após a captura dos pacotes, foi criado um gráfico através da API JFreeChart, que mostra o nível do tráfego de dados. Ele é do tipo *TimeSeries*, que exibe mudança dados em relação ao tempo. A figura 1 apresenta o gráfico, que exibe a quantidade de tráfego capturado em bytes (eixo y), de acordo com o horário no relógio do sistema (eixo x).

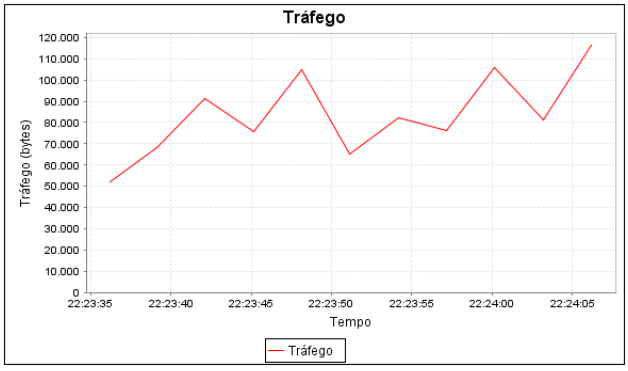

Figura 1- Gráfico de tráfego de pacotes.

Após a criação do gráfico, foi criada uma tabela com a lista do tráfego de dados na rede, conforme mostra a figura 2.

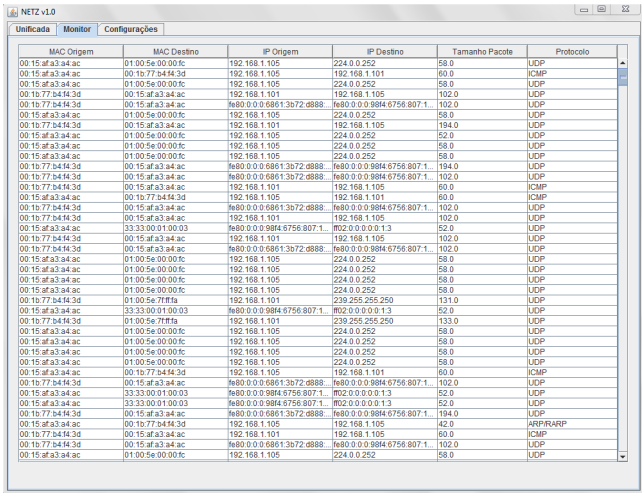

Figura 2- Tabela de captura de tráfego.

A tabela exibe os detalhes dos pacotes capturados, com os MACs e IPs de origem e de destino, além do tamanho do pacote e do protocolo utilizado.

Para exibir os *hosts* que estão *online* na rede foi criada uma lista que mostra o nome e o IP. Os *hosts* são exibidos com um ícone verde, representando que estão *online*, e o texto com o nome e o IP pode aparecer na cor preta ou na cor vermelha. Caso esteja na cor preta, quer dizer que é um computador conhecido na rede e cadastrado no banco; caso esteja na cor vermelha, quer dizer que aquele é um *host* desconhecido, podendo ser um novo computador na rede ou um possível intruso. Ao clicar na lista pode-se também visualizar os detalhes do host, como exibido na figura 3.

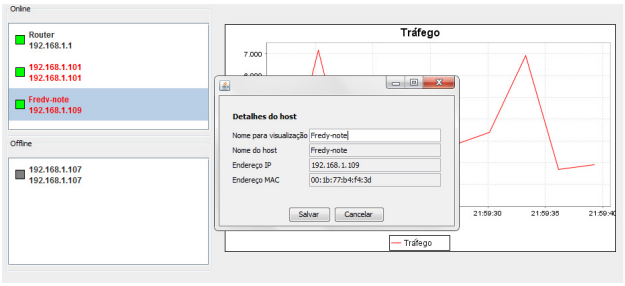

Figura 3- Lista de hosts.

Quando o usuário do sistema clica em um *host* desconhecido, que aparece na lista de com a fonte de cor vermelha, ele tem a opção de salvar esse *host* como conhecido na rede, e ele passa a ser apresentado com fonte preta, informando que aquele é um dispositivo confiável.

Foram criados sistemas de *workflow*, de forma que ocorrências na rede, como a entrada de um novo *host* ou a mudança do nível do tráfego desencadeiam tarefas que são executadas seguindo a esses fluxos de trabalho.

As formas de alertas são apresentadas através do envio de *e-mails* e SMS. Para enviar uma mensagem SMS é criada uma conexão HTTP com um *gateway*. Os *gateways* de SMS funcionam como intermediários entre as aplicações que querem fazer uso dos serviços de mensagens de texto e as operadoras de telefonia móvel, fazendo as conversões necessárias frente à grande quantidade de tipos de aparelhos e protocolos utilizados para o envio (Firtman, 2010). Para fazer uso desses serviços é preciso comprar os pacotes de mensagens providos pelos servidores de *gateways*. Foram realizadas diversas pesquisas sobre vários provedores, e percebeu-se que todos eles utilizam estruturas parecidas, fornecendo uma URL que servirá de requisição ao envio das mensagens. Desta forma o *software* foi criado para que o gerente de redes use qualquer *gateway* que desejar, configurando apenas esta URL. Para o envio de *e-mail* foram utilizados elementos da API *Commons Email,* que é uma biblioteca desenvolvida para ser utilizada junto ao Java que permite o envio de mensagens de *e-mail,* que podem ser simples ou mais bem trabalhadas (Apache, 2010).

O desenvolvimento do sistema incluiu a criação dos módulos de captura e análise de tráfego, notificações, e configurações, partindo posteriormente para as interfaces gráficas, que ainda estão em desenvolvimento. Todo o desenvolvimento ocorreu em conjunto com a criação de testes unitários. Após estas etapas serem finalizadas o sistema deverá passar por um teste de integração, que verificará o funcionamento de todos os seus componentes em um ambiente de redes e já estará pronto para uso e divulgação de seu código fonte.

Discussão

Para compreender e analisar o tráfego que transita na rede foi preciso estudar a arquitetura TCP/IP e como são os pacotes e seus cabeçalhos em cada camada do modelo. Após este estudo foi possível identificar características como a quantidade de tráfego e quais *hosts* estão utilizando a rede. Os objetivos estão sendo concluídos ao longo do desenvolvimento do trabalho, como o estudo das teorias de redes e gerenciamento, primeira etapa realizada no projeto, a criação de um sistema *workflow* de notificações através do envio de *e-mails* e SMS e a exibição das ações que ocorrem na rede, como a entrada e saída de hosts e o tráfego de pacotes.

Conclusão

As redes de dados estão presentes em vários locais, como empresas, escolas, hospitais e diversas organizações. Gerenciá-la é um processo importante, de forma que o gerente de redes deve estar atento para garantir que ela esteja funcionando corretamente, atendendo as necessidades dos usuários. Um sistema que apóia a gerência da rede é uma forma de auxiliar na manutenção e funcionamento correto dos serviços que ela provê e a proposta deste trabalho é a criação de um sistema de informação para apoiar a realização das tarefas de manutenção e controle da rede. Gerenciar é um processo trabalhoso, de forma que um *software* de apoio torna as tarefas menos cansativas e mais produtivas.

Referências

- APACHE**. Commons Email.** 2010. Disponível em http://commons.apache.org/email/index.html. Acesso em 24 julho de 2011.

- BARROS, A. J. P; LEHFELD, N. A. S. **Fundamentos de Metodologia**. Um guia para a iniciação científica. São Paulo: McGraw-Hill, 1986.

- COSTA, D. G. **Java em Rede:** recursos avançados de programação. Rio de Janeiro: Brasport, 2008.

- FIRTMAN, M. **Programming the Mobile Web**. O'Reilly, 2010.

- FUJII, K. **Jpcap Tutorial**. 2007. Disponível em: http://netresearch.ics.uci.edu/kfujii/Jpcap/doc/tutorial/index.html Acesso em 09 janeiro de 2011.

- JFREECHART. **Welcome to JFreeChart!** Disponível em: http://www.jfree.org/jfreechart Acesso em 26 janeiro de 2011.

- MICROSOFT. **O modelo TCP/IP**. Disponível em: http://technet.microsoft.com/pt-br/library/cc786900%28WS.10%29.aspx. Acesso em 07 de Abril de 2011.

- SOARES, L. F.G; GUIDO, L; COLCHER, S. **Redes de Computadores:** das LANs, MANs e WANs às redes ATM. Rio de Janeiro: Campus, 1995.

- TANENBAUM, A. S. **Redes de Computadores.** Trad. Vandeberg D. De Souza. 4. ed. Rio de Janeiro: Elsevier, 2003.