Universidade Federal de Ouro Preto - UFOP

Instituto de Ciências Exatas e Biológicas - ICEB

Departamento de Computação - DECOM

Caracterização de Padrões de Uso da Rede Sem Fio do DECOM
Proposta de Projeto de Monografia.

Aluno: Paulo Henrique Campos de Freitas
Matrícula: 07.1.4050

Orientador: Daniel Fernandes Macedo

Ouro Preto
15 de setembro de 2011

Universidade Federal de Ouro Preto - UFOP

Instituto de Ciências Exatas e Biológicas - ICEB

Departamento de Computação - DECOM

Caracterização de Padrões de Uso da Rede Sem Fio do DECOM
Proposta de Projeto de Monografia.

Proposta de monografia apresentada ao curso de Bacharelado em Ciência da Computação, Universidade Federal de Ouro Preto, como requisito parcial para a conclusão da disciplina Monografia II (BCC391).

Aluno: Paulo Henrique Campos de Freitas
Matrícula: 07.1.4050

Orientador: Daniel Fernandes Macedo

Ouro Preto
15 de setembro de 2011

Resumo

As redes sem fio são cada vez mais comuns hoje em dia. Uma rede mal projetada pode ser lenta e não satisfazer seus usuários à medida em que eles aumentam. Para melhorar seu desempenho, uma rede deve ser medida a fim de identificar pontos críticos em sua implementação. O trabalho a seguir visa medir os pacotes trafegados pela rede sem fio do Departamento de Ciência da Computação da Universidade Federal de Ouro Preto. A partir da medição será possível identificar pontos de melhorias para a rede, assim como avaliar os serviços oferecidos por ela.

Palavras-chave: Rede sem fio. Coleta de dados. Mikrotik. Anonimização.

Sumário

Lista de Figuras

Lista de Tabelas

1 Introdução

Nos últimos anos, o número de alunos do Departamento de Computação (DECOM) da Universidade Federal de Ouro Preto que possuem notebooks cresceu consideravelmente. Consequentemente, o uso destes nos laboratórios da universidade propiciou um significativo aumento de perdas de mouse, cabos de redes, e outros periféricos que causaram prejuízos à universidade. Para minimizar essas perdas, foi proibido pelo DECOM o uso de notebooks nos laboratórios.

De forma a não prejudicar os alunos, foi implantado pelo DECOM, sob a coordenação do professor Ricardo Rabelo, uma rede sem fio. Esta é restrita aos alunos e professores, os quais podem acessá-la através de pontos de acesso espalhados pelo departamento e no Centro Acadêmico de Ciência da Computação (CACIC), mediante autenticação.

A topologia da rede sem fio consiste em uma máquina servidora e vários pontos de acesso. Existem ainda dois roteadores Mikrotik [2], porém ainda não estão em uso e futuramente serão instalados.

Os pontos de acesso são basicamente compostos por computadores simples, sem grandes quantidades de processamento e memória, e com discos rígidos razoáveis, de modo a possibilitar a reciclagem de máquinas consideradas ultrapassadas. Estas máquinas possuem um sistema operacional Mikrotik RouterOS, que oferece algumas ferramentas para monitorar a rede, como geração de arquivos de *log*, e um *sniffer* para rastrear os pacotes trafegados na rede, além de outras que possibilitam transformá-las em roteadores. A máquina servidora possui configurações melhores, uma vez que máquinas similares aos pontos de acesso queimaram quando utilizadas para esta finalidade.

A instalação da rede é uma experiência recente, e ainda não foi realizada nenhuma medição de tráfego dessa.

Medir o tráfego da rede consiste em coletar e identificar os dados que trafegam por essa rede além de analisá-los e caracterizá-los de forma a identificar padrões. Os dados que não se encaixem nos possíveis padrões identificados também devem ser separados e analisados. Os dados podem ser separados entre conexões HTTP, serviços de e-mail, conexões peer-to-peer, entre outras possíveis categorias que podem ser identificadas durante a análise dos resultados. A caracterização da rede será feita a partir desses dados, e se faz necessária para que seja possível identificar pontos de melhoria dessa e propor soluções para tais. A análise dos dados propiciará também um balanço a respeito do uso da rede e de seus serviços.

Todos os dados coletados serão anonimizados de forma a ocultar o usuário e preservar sua identidade, afinal não é objetivo do trabalho apontar quais usuários estão erroneamente utilizando a rede.

As seções seguintes apresentarão a proposta para o trabalho de Monografia

CARACTERIZAÇÃO DE PADRÕES DE USO DA REDE SEM FIO DO DECOM. Seu objetivo é montar um ponto de acesso de teste, medir e analisar o tráfego da rede do DECOM, assim como os serviços disponibilizados por ela como o Moodle, o servidor Web, entre outros. Desta forma será possível detectar falhas na rede e indicar soluções para melhorar a velocidade e disponibilidade da rede e seus serviços para todos os seus usuários. A Seção 2 explica as justificativas para a escolha do trabalho. Em seguida a Seção 3 apresenta os objetivos gerais e específicos do trabalho. Na Seção 4 se encontra a metodologia a ser utilizada para a execução deste e por fim, a Seção 5 apresenta o cronograma para seu desenvolvimento.

2 Justificativa

A motivação para o desenvolvimento deste trabalho é conhecer melhor a rede sem fio, de modo que seja possível indicar melhorias para a mesma e para seus serviços.

2.1 Medindo a rede

Antes de poder sugerir qualquer adaptação para a rede sem fio, é necessário conhecer como ela funciona, o que é transmitido através dela. De modo geral, é preciso analisar o ponto de acesso para identificar possíveis melhorias.

A forma adotada para conhecer o ponto de acesso será a medição dos pacotes trafegados por ele. Depois de feita a coleta, os dados serão separados e analisados, possibilitando identificar pontos de melhoria na rede e até possíveis ataques à rede.

2.2 Serviços da rede

São vários os serviços disponibilizados pela rede sem fio. Medir esses serviços é a maneira adequada de identificar melhorias viáveis. Entre as possíveis melhorias podem-se classificar as senhas de acordo com o nível de segurança oferecido, fazer um balanço dos protocolos mais utilizados na rede. Também é interessante identificar horários de pico dos usuários além de tentativas de ataques e contaminações de vírus.

3 Objetivos

3.1 Objetivo geral

- Estudar os dados trafegados pela rede sem fio é fundamental para identificar seus pontos críticos. Uma vez identificados, será possível sugerir melhorias. Este trabalho irá estudar a rede sem fio e os serviços disponibilizados por ela e propor melhorias.

3.2 Objetivos específicos

- Redes de computadores são cada vez mais frequentes no dia a dia, principalmente agora com a expansão da internet. Este trabalho irá revisar conceitos relacionados à construção e administração de redes de computadores.

- Surgem a cada dia diversas ferramentas para gerenciar redes de computadores. Neste trabalho será possível conhecer melhor algumas destas que o Mikrotik RouterOS oferece.

- O Mikrotik RouterOS é um sistema operacional desenvolvido pela empresa Mikrotik [2] que permite transformar um simples computador em um poderoso roteador. Ele será apresentado com suas ferramentas ao longo desse trabalho.

- Para analisar o tráfego da rede é necessário medir todas as informações trafegadas pelo ponto de acesso desta. Para isso será montado um ponto de acesso de teste na rede sem fio e desta forma obter os arquivos de *log*. Caso não seja viável montar este ponto, pode-se utilizar os *logs* históricos já existentes, deixando como proposta de trabalho futuro a análise dos dados recentes.

- Para proteger a privacidade dos usuários da rede os dados coletados devem ser anonimizados. A técnica que será adotada é a anonimização com preservação de prefixo proposta por [6]. Ela será detalhada e apresentada ao longo do trabalho.

- As informações úteis para a análise estarão registradas nos arquivos de *log*. Para auxiliar a análise será desenvolvido um protótipo responsável por processar os arquivos e extrair deles as informações desejadas

4 Metodologia

Nesta seção será apresentada primeiramente uma revisão da bibliografia utilizada para o desenvolvimento do trabalho, definindo os algoritmos e ferramentas utilizados durante a disciplina de Monografia I (BCC 390). Em seguida são detalhadas as etapas do desenvolvimento para a disciplina de Monografia II (BCC 391).

4.1 Revisão Bibliográfica

A revisão bibliográfica apresentará uma revisão de conceitos de redes de computadores encontrados em [3].

A troca de dados entre computadores de uma rede é feita através de mensagens. Essas estão encapsuladas dentro de pacotes, que nada mais são do que uma sequência de *bytes* [3]. Uma mensagem pode ser subdividida em vários pacotes, e são inúmeros os pacotes trocados em uma comunicação. Para medir uma rede, é necessário fazer uma coleta dos dados trafegados por ela. A coleta pode ser feita de diversas maneiras, entre elas a por interceptação. Esse modelo apenas adiciona uma funcionalidade ao ponto de acesso, que é a de registrar os pacotes que passam por ele.

Existem ferramentas desenvolvidas para executar a coleta dos pacotes no ponto de acesso. Uma delas é o Ethereal desenvolvida pela Ethereal [1]. Ela é uma ferramenta de código livre desenvolvida para executar nos principais sistemas operacionais existentes no mercado, entre eles Unix, Linux e Windows. Existe também o Wireshark [5], que é a evolução do Ethereal.

A empresa Mikrotik desenvolveu um sistema operacional chamado Mikrotik RouterOS. Ele é baseado em linux e possui inúmeras ferramentas para auxiliar na construção e administração da rede. O site da Mikrotik disponibiliza uma seção wiki [4] para apresentar o Mikrotik RouterOS e todas as ferramentas oferecidas por ele. Nela também é possível encontrar todas as especificações para o WinBox.

Para proteger a privacidade do usuário deve-se anonimizar o pacote coletado. Essa anonimização pode ser feita nos campos IPs de destino e origem. Para mascarar um IP existe a técnica de anonimização com preservação de prefixo descrita em [6]. Nesta técnica, se temos dois endereços IP com *bits* iniciais iguais, após anonimizados, eles terão a mesma quantidade de *bits* ligados iguais. Dados pessoais dos usuários também serão mascarados a fim de proteger a privacidade desses.

4.2 Desenvolvimento

O primeiro passo para o desenvolvimento do trabalho será montar um ponto de acesso de teste e disponibilizá-lo para os alunos do DECOM, ou caso seja inviável montá-lo, obter um registro histórico dos *logs* da rede..

O ponto de acesso será constituído de um computador com quantidade razoável de memória RAM e espaço de armazenamento. Seu papel será transmitir os pacotes da

máquina servidora para os possíveis clientes que estejam conectados. Não é uma tarefa que demanda muito poder de processamento, porém caso queira processar os pacotes *online*, é necessário um pouco mais de recurso computacional. Para esse trabalho iremos gerar um arquivo de *log* no ponto de acesso e processar esse arquivo em outra máquina, de modo a exigir do ponto de acesso apenas uma quantidade significativa de memória de armazenamento. Todos os pontos de acesso já fazem registros de *log*, portanto os usuários finais não serão prejudicados com perda de desempenho desse.

Cada ponto de acesso executa o sistema operacional Mikrotik RouterOS. O sistema é desenvolvido para gerenciar as Mikrotik RouterBoards, porém se instalado em qualquer computador, possibilita transformá-lo em um roteador. A interface com o usuário é através de linha de comando, porém existe ainda uma ferramenta chamada WinBox que permite acessar todas as funcionalidades oferecidas pelo Mikrotik por meio de interfaces gráficas. A vantagem em se usar esta ferramenta é que ela facilita monitorar os dados que trafegam pela rede, e não precisa ser executada na própria máquina, podendo ser acessada em qualquer computador que esteja conectado à rede. Por motivos de segurança toda a comunicação entre o Mikrotik e o WinBox é criptografada.

A coleta dos dados será feita por meio da ferramenta Traffic Flow [4], disponibilizada pelo Mikrotik Router OS. Essa ferramenta é capaz de coletar todos os pacotes que trafegam através do ponto de acesso. Traffic Flow é baseado na ferramenta Cisco NetFlow e proporciona todas as utilidades desta. A partir da coleta dos dados, é necessário anonimizar os dados, de forma a proteger a privacidade dos usuários da rede.

Anonimizar um dado consiste em mascarar sua identidade, de forma a tornar impossível a identificação de seu autor. Existem leis que se referem ao fato de preservar a privacidade e segurança do usuário, portanto é necessário escolher cautelosamente qual ferramenta utilizar e qual política adotar. A ferramenta de anonimização escolhida deve garantir que os dados do mesmo usuário sejam agrupados e analisados, porém não pode permitir nenhuma inferência entre os dados anonimizados com dados reais.

No caso deste trabalho, iremos usar a anonimização de endereço IP. O endereço IP permite identificar a origem de um pacote e seu fluxo na rede, sendo de grande valia na análise a ser feita. A técnica de anonimização utilizada será a preservação de prefixos, pois permite agrupar os dados pertencentes a uma mesma sub-rede porém preservando a privacidade do usuário.

Juntamente ao processo de anonimização, será selecionado e mascarado toda forma de dado pessoal como senhas, nomes, etc. Para auxiliar este trabalho as senhas serão testadas quanto a sua segurança e classificadas como fracas, médias e fortes. O ideal seria classificá-las entre criptografadas ou não, porém a primeira proposta de classificação é fácil de ser obtida com apenas uma função de teste de *string* . Todas as senhas criptografadas serão classificadas como fortes devido a sua composição de *caracteres*, desta forma evita-se o contato do autor com as senhas dos usuários e ainda satisfaz um dos objetivos do trabalho.

Um protótipo será gerado para analisar os arquivos de *log* gerado pela ferramenta Traffic Flow e agrupar os pacotes similares. O protótipo irá gerar as estatísticas de todo o tráfego, levando em conta qual serviço está sendo utilizado, possibilitando deduzir quais desses serviços podem ser otimizados.

Depois que todos os arquivos de *log* forem analisados deverão ser confeccionados gráficos e tabelas de forma a ilustrar os resultados obtidos. Com esses resultados prontos, será possível identificar um padrão de uso da rede sem fio do DECOM e o comportamento dos usuário da rede. É desejável descobrir gargalos que causem lentidão à rede e sugerir métodos para contorná-los. A segurança da rede é mais um ponto a ser analisado, afinal é possível identificar alguns tipos de ataques através dos pacotes trafegados. Para todos os problemas identificados pela análise serão feitas sugestões de melhorias ou formas de tentar contorná-los. Todos os resultados serão devidamente documentados durante a redação da monografia.

5 Cronograma de atividades

Na Tabela 1, será apresentado o cronograma para o desenvolvimento da disciplina Monografia 2.

Atividades	**Ago**	**Set**	**Out**	**Nov**	**Dez**
Coleta do dados		X			
Análise dos dados			X	X	
Apresentação dos resultados				X	
Redigir a Monografia		X	X	X	
Apresentação do Trabalho					X

Tabela 1: Cronograma de Atividades.

Referências

[1] Site oficial do ethereal. `http://www.ethereal.com`.

[2] Site do mikrotik. `http://www.mikrotik.com`.

[3] Andrew S. Tanenbaum. *Redes de Computadores*. Campus, 4 edition, 2003.

[4] Site wiki do mikrotik. `http://wiki.mikrotik.com/wiki`.

[5] Site do wireshark. `http://www.wireshark.org`.

[6] Jun Xu, Jinliang Fan, Mostafa Ammar, and Sue B. Moon. On the design and performance of prefix-preserving ip traffic trace anonymization. In *ACM SIGCOMM Internet Measurement Workshop*, pages 263–266, San Francisco, USA, 2001.