

Universidade Federal de Ouro Preto - UFOP
Instituto de Ciências Exatas e Biológicas - ICEB
Departamento de Computação - DECOM

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

Aluno: Paulo Henrique Campos de Freitas
Matricula: 07.1.4050

Orientador: Daniel Fernandes Macedo

Ouro Preto
26 de outubro de 2010

Universidade Federal de Ouro Preto - UFOP
Instituto de Ciências Exatas e Biológicas - ICEB
Departamento de Computação - DECOM

Caracterização de Padrões de Uso da Rede 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 I (BCC390).

Aluno: Paulo Henrique Campos de Freitas
Matricula: 07.1.4050

Orientador: Daniel Fernandes Macedo

Ouro Preto
26 de outubro de 2010

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 dados 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

1	Introdução	1
2	Justificativa	3
2.1	Medindo a rede	3
2.2	Serviços da rede	3
3	Objetivos	4
3.1	Objetivo geral	4
3.2	Objetivos específicos	4
4	Metodologia	5
4.1	Revisão Bibliográfica	5
4.2	Desenvolvimento	5
5	Cronograma de atividades	7

Lista de Figuras

Lista de Tabelas

1	Cronograma de Atividades.	7
---	-----------------------------------	---

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 mouses, 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 desta.

Medir o tráfego da rede consiste em coletar e identificar os dados que trafegam por essa rede e, a partir destes, 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 desta 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 DO DECOM cujo 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, possibilitando detectar falhas na rede e a partir disso novas sugestões 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 trabalhos. 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 melhorias, pode-se analisar a segurança destes: A comunicação do usuário com o Moodle é segura? Os e-mails são protegidos contra interceptadores? O servidor WEB é capaz de defender os usuários contra vírus? Além da segurança, pode-se medir a eficiência de tais serviços, como a taxa de utilização, velocidade de resposta, entre outras características.

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*.
- Para proteger a privacidade dos usuários da rede os dados coletados devem ser anonimizados. A técnica que será adotada é a anonimização por preservação de prefixo. 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 que serão utilizadas. Em seguida são detalhadas as etapas do desenvolvimento.

4.1 Revisão Bibliográfica

A revisão bibliográfica apresentara uma revisão de conceitos de redes de computadores apresentados por Tanenbaum[3], uma vez que a disciplina de Redes de Computadores será cursada pelo autor em paralelo ao desenvolvimento do trabalho no próximo semestre.

A troca de dados entre computadores de uma rede é feita através de mensagens, estas 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* iguais.

4.2 Desenvolvimento

O primeiro passo para o desenvolvimento do trabalho será montar um ponto de acesso de teste e disponibiliza-lo para os alunos do DECOM, ou caso seja necessário devido a pouco acesso, para os demais alunos do ICEB.

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 recursos computacionais. 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.

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 transforma-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 dos mesmo usuário sejam agrupados e analisados, porém não pode permitir nenhuma inferência entre os dados anonimizados com dados reais.

No caso desse 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.

Após a etapa de anonimização dos dados, serão feitos os processamentos e análise dos dados. 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.

5 Cronograma de atividades

Na Tabela 1, abaixo é apresentado o cronograma referente ao desenvolvimento das atividades para a disciplina de Monografia 1. É apenas o início do desenvolvimento desse trabalho que será concluído no próximo semestre na disciplina de Monografia 2.

Atividades	Ago	Set	Out	Nov	Dez
Levantamento da Revisão Bibliográfica		X	X		
Estudo das Ferramentas a Serem Utilizadas			X	X	
Montagem do Ponto de Acesso				X	
Início da Coleta de Dados no Ponto de Acesso				X	
Escrita do Relatório das Atividades Desenvolvidas				X	
Apresentação do Relatório das Atividades Desenvolvidas				X	

Tabela 1: Cronograma de Atividades.

A etapa de levantamento da revisão bibliográfica e estudo das ferramentas a serem utilizadas já estão sendo desenvolvidas paralelamente a escrita da proposta. A montagem do ponto de acesso será executada em seguida e após todas as configurações acertadas será iniciada a coleta dos dados. O relatório será escrito abordando as ferramentas escolhidas com exemplos dos dados coletados. O relatório será apresentado no dia 27 de Novembro segundo programado pelo professor responsável pela disciplina de Monografia 1.

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.