Redes de Computadores – 2011
Segundo Trabalho
Servidor Proxy HTTP

Prof. Ronaldo Alves Ferreira

1 Descrição do Trabalho

Neste trabalho você implementará um servidor Proxy para o protocolo HTTP de acordo com as RFCs 2616 e 3143. O seu servidor deve ser capaz de interagir com servidores web da Internet, tratando pelo menos os métodos GET, POST e HEAD.

2 Funcionamento Básico

Além dos métodos GET, POST e HEAD, o servidor proxy deve implementar mecanismos de cache para atender requisições que foram servidas recentemente. Você deve seguir as diretivas de cache estabelecidas na Seção 13 da RFC 2616.

O seu servidor deve receber como parâmetro na linha de comando o nome do arquivo de configuração do servidor. O arquivo deve conter, pelo menos, as seguintes opções de configuração:

- **PORT=port** – **port** especifica a porta em que o servidor receberá as conexões.
- **THREADS=threads** – **threads** indica o número de threads que devem ser criadas para o pool de threads.
- **CACHE_DIRECTORY=path** – **path** especifica o diretório onde os arquivos em cache serão mantidos.
- **CACHE_SIZE=size** – **size** tamanho do cache em MB. O seu servidor deve implementar uma política de substituição de páginas caso esse valor seja atingido.
- **ACCESS_LIST=file** – **file** especifica o caminho completo do arquivo com uma lista de URLs que devem ter o acesso bloqueado. Para cada URL bloqueado, o servidor proxy deve retornar um página HTML indicando que o URL solicitado foi bloqueada pelo administrador do sistema.

2.1 Conexões Persistentes

O servidor proxy deve tratar conexões persistentes como indicado na RFC 2616.

2.2 Access Lists

O servidor proxy deve bloquear URLs especificados em um arquivo de configuração. Segue, abaixo, um exemplo de arquivo de regras de bloqueio:

```
# Linha de comentário, deve ser ignorada
DENY=servidor.dominio/path           # URL deve ser bloqueado
DENY=*.dominio                       # URLs do dominio devem ser bloqueados
ALLOW=servidor.dominio/servidor/path # URL deve ser permitido. Esta regra
                                     # tem precedência sobre uma regra de
                                     # bloqueio de domínio
```

O seu servidor deve permitir que as regras de bloqueio sejam atualizadas enquanto o servidor estiver em execução, ou seja, você não precisa terminar e reiniciar o processo para que as regras passem a valer. Para implementar essa funcionalidade, o seu servidor deve interceptar o sinal SIGHUP e recarregar as regras de bloqueio no tratador do sinal.

3 Funcionalidades Adicionais

Os trabalhos serão avaliados comparativamente. Portanto, não há limite para funcionalidades adicionais, você pode implementar outras funcionalidades não descritas neste trabalho. Leia a RFC 2616 e decida as funcionalidades adicionais a serem implementadas.

4 Entrega do Trabalho

O trabalho deverá ser enviado por email até às **17h do dia 14 de outubro de 2011**.

Além do código fonte documentado, você deve entregar um relatório descrevendo o seu trabalho. Neste relatório, você deve incluir uma breve introdução, decisões de implementação, funcionalidades não implementadas, problemas enfrentados na implementação, etc. O relatório deve ser entregue em um arquivo PDF.

O trabalho pode ser feito em grupos de no máximo três alunos. Casos de plágio serão tratados com rigor. Caso você faça o trabalho em grupo, submeta apenas um trabalho e identifique os componentes do grupo no relatório e no código fonte.

5 Avaliação

Além da correção do programa, o professor fará uma entrevista com os membros do grupo. Na entrevista, o grupo deverá explicar o funcionamento do programa e responder a perguntas relativas ao projeto.