Universidade do Minho - Dep.to Informática
1º Semestre, 2016/2017
Gestão de Redes

Trabalho Prático Nº3 – Parte I

Servidor de números aleatórios

Objectivos:

- Consolidação da utilização prática do modelo de gestão preconizado pelo *Internet-standard Network Management Framework* (INMF), dando especial relevo ao *Simple Network Management Protocol* (SNMP) e às *Management Information Bases* (MIBs).
- Utilização de APIs SNMP para construção de ferramentas de gestão (agentes e gestores).
- Investigação da aplicação do SNMP em sistemas de gestão nos mais variados ramos da engenharia aplicacional.

Observações:

- O trabalho deverá ser realizado em cerca de 70 horas efetivas de trabalho.

Requisitos:

- Sistema com um agente SNMPv2c instalado (preferencialmente o NET-SNMP) e pacote de desenvolvimento numa linguagem de programação que disponibilize APIs para construção de gestor e agente SNMPv2c (como por exemplo o SNMP4J).

AVISOS:

- Não serão tolerados atropelos aos direitos de autor de qualquer tipo de *software*...

Bibliografia específica e material de apoio

Material de apoio:

- Manuais do *ucd-snmp* e *scottty*
- MIBs em `/usr/share/snmp/mibs` e `/aplicacoes/MIBs`
- Recurso `http://net-snmp.sourceforge.net/wiki/index.php/Tutorials/`
- Recurso `http://www.simpleweb.org/`
- Recurso `http://www.snmplinks.org/`
- Recurso `http://www.agentpp.com/`

Bibliografia:

- M. Rose, *The Simple Book*, Second Edition, Prentice Hall, 1996.
- W. Stallings, *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*, Addison-Wesley, 2000.
- D. Mauro, K. Schmidt, *Essential SNMP*, O'Reilly, 2001.

- Ver outros recursos na secção da *Bibliografia* na página da disciplina e no CD fornecido no início do semestre.

Servidor de números aleatórios

O objetivo principal deste trabalho é o desenvolvimento de um agente SNMP que seja um servidor de geração de números aleatórios. Este tipo de serviço remoto através da internet estaria assim disponível a outros sistemas que precisem formas de obter números aleatórios não controlados por processos internos ao seu próprio sistema computacional. Já existem serviços parecidos, como random.org, mas pretende-se que este serviço tenha um interface comunicacional através de SNMPv2c e não através de HTTP.

O primeiro passo do trabalho deve ser a definição dos requisitos funcionais, isto é, que tipo de resultados são esperados tendo em conta as possíveis parametrizações que os utilizadores podem fazer. Depois deve definir-se uma MIB com os grupos de objetos com a semântica e sintaxe adequadas à correta abstração dos requisitos funcionais pré-estabelecidos. Por fim, deve construir-se e testar-se o *software* do agente que implemente o serviço num agente SNMPv2c. Este *software* pode ser desenvolvido na linguagem e ambiente de programação que achar mais adequados.

Definições Prévias

Dada uma matriz $M_{T,K}$ de T linhas e K colunas, cada elemento $d_{i,j}$ é um dígito hexadecimal e os índices são números inteiros tal que $1 \leq i \leq T$ e $1 \leq j \leq K$ (T é o tamanho da dimensão vertical e K o tamanho da dimensão horizontal). Defina-se $L_{N,D}(p,q,M)$ como sendo a sub-matrix de $M_{T,K}$ (com $N \leq T$ e $D \leq K$) com os elementos $d_{a,b}$ em que $p \leq a < p+N$ e $q \leq b < q+D$; quando $p+N > T+1$, então $p \leq a \leq T$ e $1 \leq a \leq p+N-T$; quando $q+D > K+1$, então $q \leq b \leq K$ e $1 \leq b \leq q+D-K$. Defina-se refrescamento vertical $v(i,j,M_{T,K})$ duma matriz $M_{T,K}$ como o deslocamento/circulação vertical dos elementos da coluna i, j vezes; e refrescamento horizontal $h(i,j,M_{T,K})$ duma matriz $M_{T,K}$ como o deslocamento/circulação horizontal dos elementos da linha i, j vezes. Defina-se como substituição $s(i,j,M_{T,K})$ duma matriz $M_{T,K}$ como a substituição da linha i pelo resultado da operação binária XOR entre a linha i-1 (ou T se i=1) e a linha i+1 (ou 1 se i=T), seguida da substituição da coluna j pelo resultado da operação binária XOR entre a coluna j-1 (ou K se j=1) e a coluna j+1 (ou 1 se j=K).

Tomem-se como exemplos as seguintes matrizes $M_{3,3}$ e $B_{3,3}$:

```
M          B
1 2 3      1 0 0
4 5 6      0 1 1
7 8 9      1 0 1
```

Então, a matriz resultante dum refrescamento $v(2,2,M)$, seguido dum refrescamento $h(1,1,M)$ é igual a:

```
3 1 5
4 8 6
7 2 9
```

E, a matriz resultante duma substituição $s(2,2,B)$, é igual a:

```
1 1 0
0 1 1
1 0 1
```

Finalmente, a sub-matriz $L_{2,2}(3,3,M)$ é igual a:

```
1 3
7 9
```

Requisitos Funcionais Genéricos

Quando executado, o agente SNMP deve consultar um ficheiro de configuração contendo os seguintes parâmetros de inicialização, um por linha, nesta ordem, todos obrigatórios:

- Porta UDP de atendimento de pedidos;
- Nome de comunidade SNMPv2c;
- Frequência R de refrescamento da tabela de números aleatórios (em Hz);
- Número N de entradas na tabela de números aleatórios;
- Número de D dígitos hexadecimais de cada entrada na tabela de números aleatórios;
- Caminho para o ficheiro com as T sementes iniciais (uma por linha, com K dígitos cada).

Em conjunto com o ficheiro deste enunciado são disponibilizados dois ficheiros adicionais, um com um exemplo de configuração e outro com um conjunto de sementes iniciais correspondente.

Como argumento do programa (na linha de comandos ou através dum interface dinâmico) deve ser indicada a chave de configuração para autorização da operação de *reset* do agente através do SNMP.

Exemplo do comando para executar o agente:

```
unpredictable-agent dfh8ty3t-4rq8549
```

Assim que é arrancado, o agente deve construir uma matriz $M_{T,K}$ com as sementes do ficheiro indicado no ficheiro de configuração (cada semente será uma linha da matriz). A matriz $M_{T,K}$ será usada para construir a tabela de números aleatórios a implementar como instância da MIB no agente. Ou melhor, a tabela da MIB conterá N linhas a que equivalem N números aleatórios (um número de D dígitos por cada linha). Cada número aleatório i da tabela da MIB corresponde à concatenação circular de D elementos de cada linha i da sub-matriz $L_{N,D}(p,q,M)$, em que p e q são calculados dinamicamente a cada refrescamento da tabela de números aleatórios.

***Unpredictable* MIB**

A *Unpredictable* MIB, a implementar no agente SNMP, deve conter dois grupos:

- `unpredictableParam(1)` – grupo com objetos escalares que representem os parâmetros de funcionamento; além dos parâmetros de inicialização R, N, e D (apenas com permissões de leitura) deve incluir-se um objeto escalar especial (do tipo *string* e apenas com permissões de escrita) que sirvará para verificar autorizações para a operação *reset* do agente.
- `unpredictableTable(2)` – grupo com a tabela de N números aleatórios; a tabela deve incluir apenas duas colunas, uma para o índice da entrada (que é chave da tabela) e outra para o número aleatório (sequência de D dígitos hexadecimais).

Requisitos - FASE A

Para a primeira fase os alunos devem especificar a *Unpredictable* MIB e confirmar a sua sintaxe e semântica junto do docente antes de continuar para a Fase B.

Requisitos - FASE B

Para a segunda fase os alunos devem construir e testar um agente SNMP que leia o ficheiro de configuração e implemente apenas o grupo `unpredictableParam(1)` da *Unpredictable* MIB (o ficheiro com as sementes iniciais indicado no ficheiro de configuração deve ser ignorado). Os alunos devem confirmar com o docente a correção do desenvolvimento do agente.

Requisitos - FASE C

Na terceira fase os alunos devem acrescentar a implementação do grupo `unpredictableTable(2)` da *Unpredictable* MIB. Devem considerar que N=T, D=K e p=q=1 são constantes. Ainda não devem implementar a operação de refrescamento da tabela de números aleatórios nem a operação de *reset*, ou seja, a tabela que construírem no arranque do agente a partir da matriz $M_{T,K}$ do ficheiro de sementes deve manter-se fixa (a própria matriz é constante/fixa). No final desta fase os alunos devem confirmar com o docente a correção do desenvolvimento do agente.

Requisitos - FASE D

Implementação do refrescamento da matriz $M_{T,K}$ e da tabela de números aleatórios.
Nota: detalhes na Parte II do enunciado.

Requisitos - FASE E

Implementação da operação de *reset* da matriz $M_{T,K}$ e da tabela de números aleatórios.
Nota: detalhes na Parte II do enunciado.

Relatório

Elabore o relatório do trabalho para ser entregue fisicamente e por *e-mail*.
Nota: detalhes na Parte II do enunciado.