

## Análise de Tráfego IP

O registo (log, traço) de pacotes a analisar neste trabalho foi obtido usando um monitor de tráfego passivo e tem uma duração de cerca de 45 s. O registo contém todos os pacotes observados nos 2 sentidos de um *link*.

O registo de pacotes encontra-se em `traco.gz`, comprimido com `gzip`. Depois de descomprimido o ficheiro fica com cerca de 11 Mbytes, em formato ASCII.

Cada linha do ficheiro corresponde a um pacote. Para cada pacote os campos do cabeçalho do pacote são descritos da seguinte forma:

- interface-id (1 ou 2, para cada sentido do *link*);
- tempo de captura do pacote, em segundos com uma resolução de 100 ns;
- endereço IP de origem cifrado;
- endereço IP de destino cifrado;
- número do protocolo (consulte `/etc/protocolos`);
- comprimento do pacote, em bytes;
- porta de origem, se TCP ou UDP (consulte `/etc/services`);
- porta de destino, se TCP ou UDP;
- flags TCP: URG, ACK, PSH, RST, SYN, FIN. Estas flags estão codificadas num número hexadecimal de 6 bits. URG é representado pelo bit mais significativo e FIN pelo bit menos significativo. Por exemplo, o número 18, em hexadecimal,

```
- - urg ack      psh rst syn fin
0 0 0 1          1 0 0 0
```

indica que apenas as flags ACK e PSH se encontram activas;

- Número de sequência (válido apenas para os pacotes TCP);
- Número de confirmação, ACK (pacotes TCP, apenas);
- Advertised window (pacotes TCP, apenas).

Analise o traço oferecido de modo a responder às questões que a seguir são colocadas. A análise deste registo requer o desenvolvimento de um programa numa linguagem de programação à sua escolha. Para a elaboração dos gráficos recomenda-se a utilização do programa Excel.

1. Calcule a percentagem de pacotes de cada um dos 3 protocolos mais frequentes no registo. Faça o mesmo para os bytes. Existe alguma diferença entre os valores obtidos. Se sim, explique essa diferença.
2. Calcule e represente graficamente a função densidade de probabilidade do comprimento dos pacotes. Comente a forma e os valores da curva.
3. Calcule a percentagem de pacotes SMTP, HTTP, FTP e DNS. Calcule também a percentagem de pacotes que não usam uma "porta-bem-

- conhecida". Calcule a percentagem de pacotes que são ACKs puros (sem dados).
4. Assuma que um fluxo de pacotes é uma sequência de pacotes com o mesmo endereço de origem, endereço de destino, porta de origem, porta de destino e número de protocolo. Assuma que um fluxo deve ter pelo menos 5 pacotes. Calcule o número de fluxos no registo. Quantos usam o protocolo TCP? E o protocolo UDP?
  5. Construa uma figura em que, no eixo das abcissas (Xs) representa o número de ordem de cada fluxo por ordem decrescente de bytes transferidos. Para cada fluxo representado, o valor no eixo das ordenadas (Ys) deve representar a percentagem de bytes de todos os fluxos com ordem menor ou igual a X (função distribuição de probabilidade). O que observa? De quantos fluxos precisa o router de se recordar para manter registo de pelo menos 80% do tráfego?
  6. Isole no traço todos os pacotes da ligação HTTP que começa no instante  $t=990048367.932311$ . Inclua os pacotes dos 2 sentidos (cliente-servidor e servidor-cliente). Represente os números de sequência dos dados transferidos do servidor para o cliente como uma função do tempo. O que observa? Explique.
  7. Represente a função densidade de probabilidade do tempo entre chegada de pacotes consecutivos na interface 1. Represente sobre a mesma curva a função densidade de probabilidade exponencial com a mesma média. Comente o que observa.