Universidade de Aveiro

departamento de electrónica, telecomunicações e informática

Desempenho e Dimensionamento de Redes

NETWORK AWARENESS

Metodologias de Aquisição de Dados

8240 - mestrado integrado em engenharia de computadores e telemática

Bernardo Ferreira
NMec: 67413 | P4G1

Bruno Silva
NMec: 68535 | P4G1

Docente: Susana Sargento

Março de 2016
2015-2016

Conteúdos

1 Introdução

Este relatório explica as metodologias e os resultados obtidos das experiências realizadas nas aulas práticas sobre os conceitos de SNMP, NetFlow e Pcap.

1.0.0.1 A rede utilizada para a realização das experiências foi a seguinte:

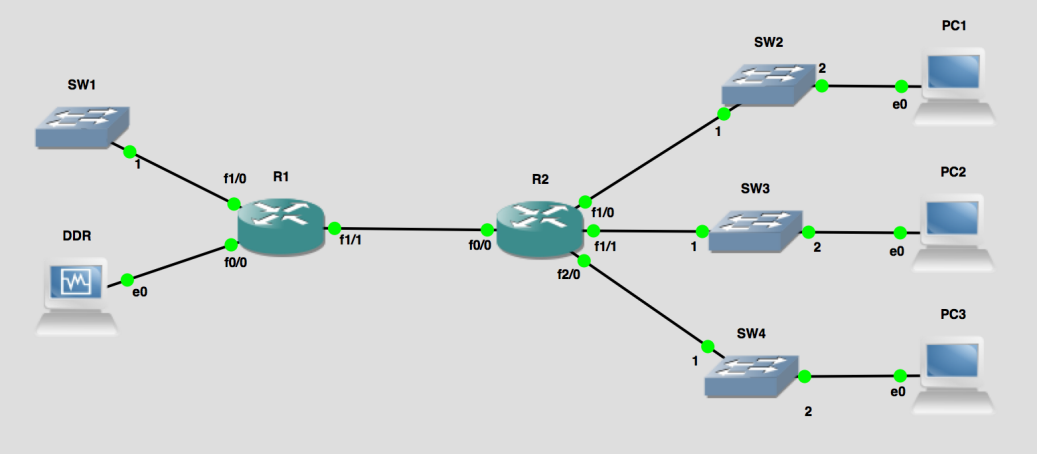

Figura 1: Topologia da rede

Bernardo Ferreira nmec: 67413
Bruno Silva nmec: 68535

2 Aquisição de dados com SNMP

2.1 Descrição

2.1.0.1 O primeiro trabalho realizado foi relativo ao uso do SNMP para aquisição de dados dos routers. Para isso foi configurada uma rede no simulador GNS3 conforme era pedido no enunciado e os routers foram configurados com o utilizador "*uDDR*".

2.1.0.2 Para aceder a informação disponibilizada por SNMP pelo router, foi utilizado um script escrito em python baseado no exemplo que foi fornecido. O script recebe 2 argumentos que permitem escolher o router do qual obter informações, assim como o tempo de intervalo entre amostras. Era ainda pedido, e está implementado, que o script pode-se permitir a escrita de um ficheiro de log onde eram guardados os valores que iam ser escritos no terminal, assim como mostrar uma representação visual dos valores através de gráficos.

2.2 Analise de Resultados

2.2.0.1 Em baixo é possível visualizar os dados obtidos da execução do script SNMP sobre a rede pedida no enunciado.

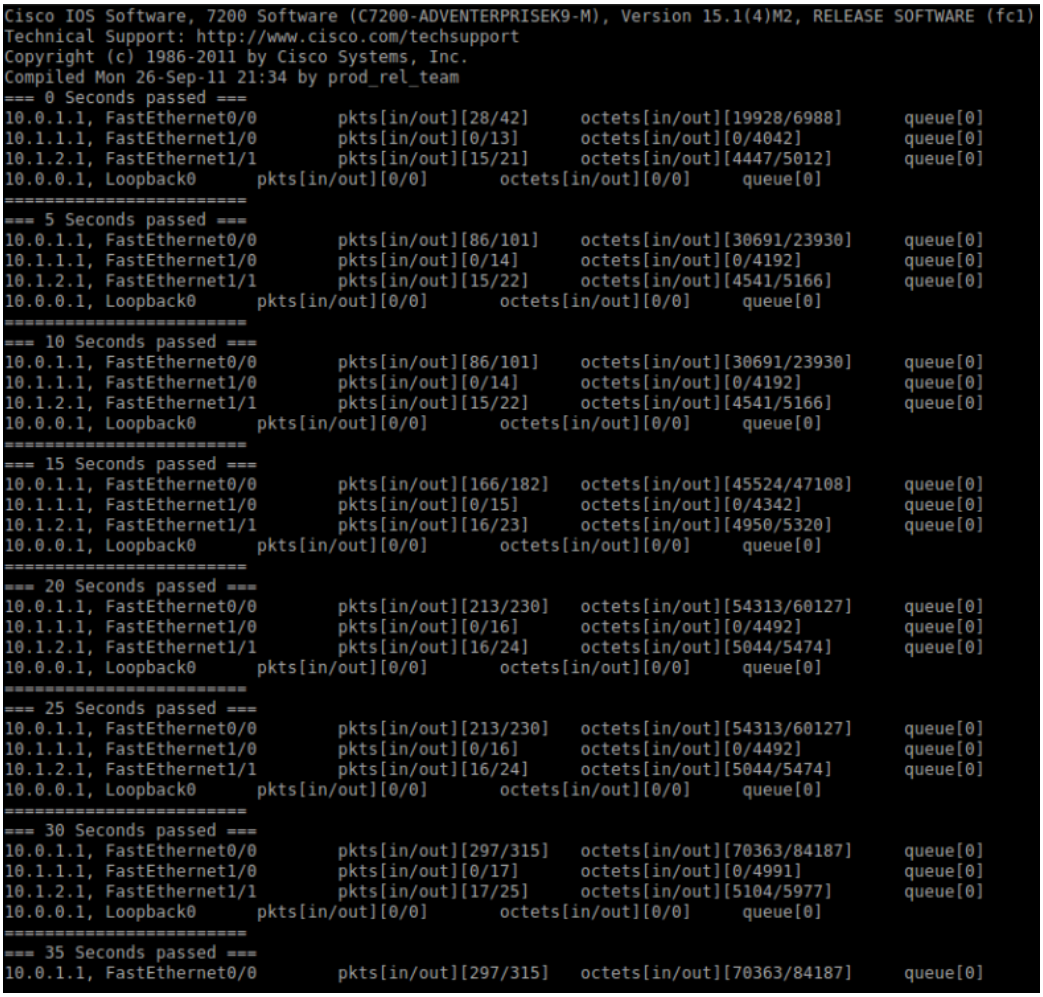

Figura 2: Captura da aquisição de dados por SNMP

2.2.0.2 Na imagem acima pode-se observar a listagem das diferentes interfaces do router que contem endereços IP's assim como, para cada uma temos ainda informação referente ao número de pacotes e octetos enviados e recebidos e o tamanho da fila de espera de cada interface. Esta informação aparece periodicamente, com o intervalo definido pelo utilizador como argumento, e é ao mesmo tempo gravada para um ficheiro com o nome "*router_<router-ip>*".

2.2.0.3 Na figura a baixo é mostrado o gráfico resultante da execução do script onde é possível ver de forma mais comparativa os valores recolhidos.

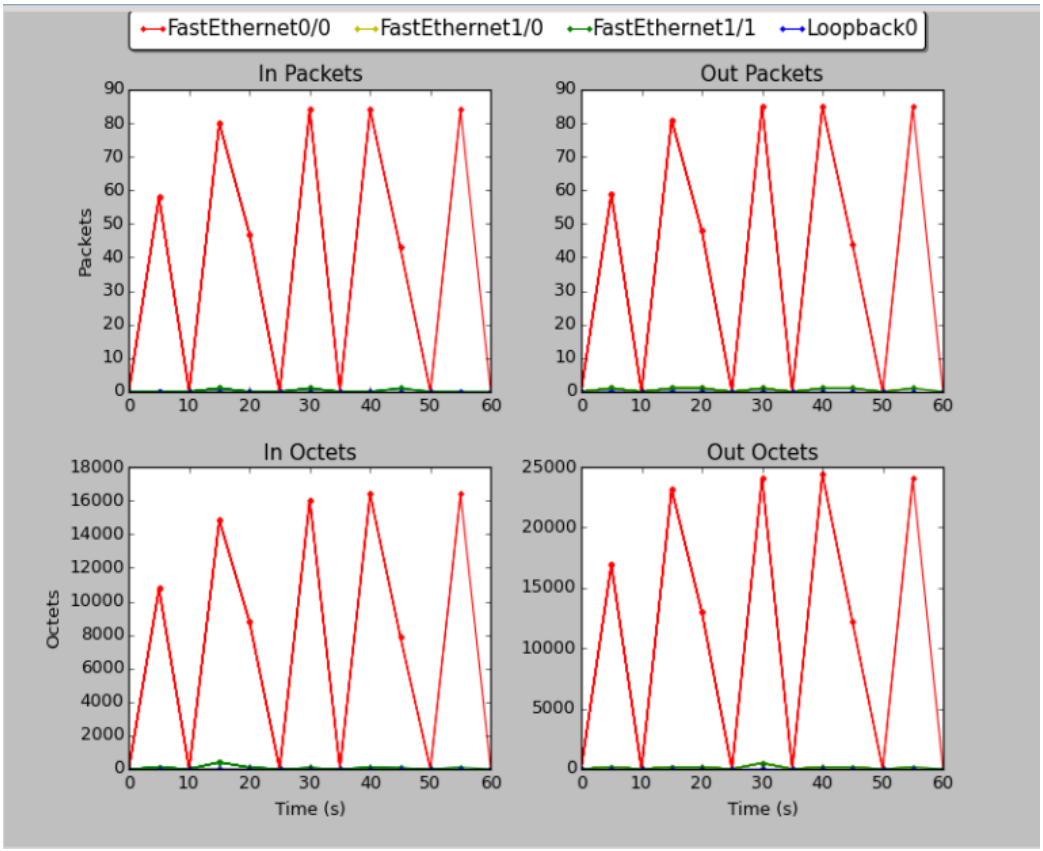

Figura 3: Gráfico da aquisição de dados por SNMP

2.2.0.4 Na janela dos gráficos, representámos em tempo real o número de octetos e packets de entrada e de saída para as 4 interfaces. Neste caso, utilizou-se intervalos de 5 segundos em que o valor apresentado é a diferença do número de pacotes/octetos recebidos até ao instante atual e os recebidos até ao instante anterior. Como é possível verificar, no primeiro gráfico, na interface FastEthernet0/0 entre 0 a 5 segundos, foram recebidos cerca de 60 pacotes, no entanto, de 5 a 10 segundos não foi recebido qualquer pacote.

3 Aquisição de dados com NetFlow/IPFIX

3.1 Descrição

3.1.0.1 O segundo trabalho realizado foi relativo ao uso do NetFlow para aquisição de dados dos routers. Para isso foi configurada uma rede no simulador GNS3 conforme era pedido no enunciado e os routers foram configurados nas interfaces necessárias para exportarem os fluxos de dados por Netflow.

3.1.0.2 Relativamente aos dados recebidos pelo Netflow era pedido para construir e mostrar a matriz de tráfego para as interfaces utilizadas tendo para cada uma os valores de fluxos existentes, o número de pacotes e de bytes. Era ainda pedido para suportar ambas as versões 1 e 5 do Netflow.

3.2 Analise de Resultados

3.2.0.1 Em baixo é possível ver uma captura da matriz de tráfego após serem capturados alguns fluxos.

```
|||(src/dst)|||||----others-----|--10.0.2.0/24--|--10.0.3.0/24--|--10.0.4.0/24--|
|----others-----| [0, 0, 0]       [1, 5, 500]       [0, 0, 0]       [0, 0, 0]
|--10.0.2.0/24--| [1, 5, 420]       [0, 0, 0]       [0, 0, 0]       [0, 0, 0]
|--10.0.3.0/24--| [0, 0, 0]       [0, 0, 0]       [0, 0, 0]       [1, 5, 420]
|--10.0.4.0/24--| [0, 0, 0]       [2, 10, 840]       [1, 5, 420]       [0, 0, 0]
```

Figura 4: Matriz de tráfego construida a partir da informação do Netflow

3.2.0.2 Olhando para a matriz produzida podemos observar o número de fluxos que ocorreram entre as diferentes redes, assim como o número de pacotes e bytes. Olhando por exemplo para os fluxos originados com origem na rede "*10.0.2.0/24*" com um destino que não está a ser monitorizado "*others*" vemos que existiu um fluxo que originou 5 pacotes e 420 bytes. Olhando para outro exemplo como por exemplo a rede de origem "*10.0.4.0/24*" com um destino que não está a ser monitorizado "*10.0.2.0/24*" vemos que existiram dois fluxos que originaram 10 pacotes e 840 bytes.

3.2.0.3 Embora o Netflow seja uma ferramenta útil para fornecer este tipo de informação, olhando para a matriz de tráfego ficamos um pouco limitados sem ser possível perceber no último exemplo dado quantos pacotes pertencem a cada fluxo.

4 Aquisição de dados com pcap

4.1 Descrição

4.1.0.1 O terceiro trabalho realizado foi relativo à captura de pacotes de entrada e saída durante a visualização de um vídeo no YouTube. Para isso, configurou-se a placa de rede da VM em modo Bridge e com o modo Promíscuo a permitir tudo. De seguida foi necessário colocar um vídeo em reprodução e descobrir o endereço de IP do YouTube a ser usado. Para o exercício foi pedido para guardar num ficheiro o tráfego de Download e Upload gerado a cada milissegundo.

4.2 Analise de Resultados

4.2.0.1 O comando usado para executar o programa foi o seguinte: "*python basePCap.py -i eth0 -c <IP pessoal>/32 -s <IP do Youtube>/24* " Em baixo é possível ver uma captura do fim do programa.

```
1457390628.951670000: IP packet from 213.30.18.143 to 192.168.1.178 (UDP:64427) 1378
1457390628.951672000: IP packet from 213.30.18.143 to 192.168.1.178 (UDP:64427) 1378
1457390628.951673000: IP packet from 213.30.18.143 to 192.168.1.178 (UDP:64427) 1378
^C
2031 packets captured! Done!
 Download: 1850354 Bytes
 Upload: 47657 Bytes
```

Figura 5: Estatísticas acerca do tráfego gerado durante a execução do programa

4.2.0.2 Os ficheiros gerados têm em cada linha o número de Bytes recebidos durante cada milissegundo. Em baixo encontra-se um exemplo dos ficheiros gerados de Download e Upload

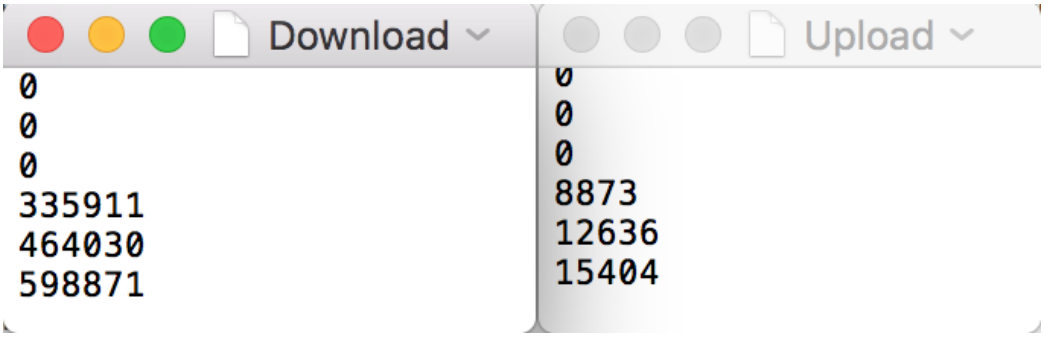

Figura 6: Exemplo dos ficheiros criados depois de terminar o programa

4.2.0.3 Analisando os resultados, podemos verificar que o YouTube utiliza um sistema de bursts, ou seja, envia muitos pacotes em curtos intervalos de tempo, havendo longos intervalos de tempo em que não há qualquer troca de pacotes.

5 Conclusão

Com este trabalho podemos conhecer e utilizar ferramentas importantes para a análise de tráfego. Houve oportunidade para conhecermos diferentes formas com diferentes níveis de detalhe de recolha de dados. Começámos por recolher dados com SNMP e concluímos que este era o método mais simples e em que não era exigido tanto poder de processamento aos routers, mas também tinha as suas limitações, não fornecendo tanto detalhe como as restantes opções. No caso do pcap, como capturava e permitia a análise dos campos de cada pacote enviado, torna-se uma solução bastante computacionalmente exigente para os routers. Por fim, com o NetFlow, obtia-se um equilíbrio entre a informação disponibilizada e a capacidade computacional dos routers.