**TP3 - PL19**

**Tiago Matos Guedes**

**Eduardo Manuel Sousa Pereira - A70619**

Questões e respostas

1. Prepare uma topologia CORE para verificar o comportamento do traceroute. Ligue um host (pc) *Cliente1* a um router *R2*; o router *R2* a um router *R3*, que por sua vez, se liga a um host (servidor) *Servidor1*. Ajuste o nome dos equipamentos atribuídos por defeito para a topologia do enunciado.



* Ative o Wireshark no *Cliente1*. Numa shell do *Cliente1*, execute o comando traceroute -I para o endereço IP do *Servidor1*.



* Registe e analise o tráfego ICMP enviado pelo *Cliente1* e o tráfego ICMP recebido como resposta. Comente os resultados face ao comportamento esperado.



Como era esperado, o resultado é a comunicação entre o Cliente1 e o Servidor1, sendo que o Cliente1 faz requests ao Servidor1, e este dá reply.

* Qual deve ser o valor inicial mínimo do campo TTL para alcançar o *Servidor1*? Verifique na prática que a sua resposta está correta.

O valor inicial de TTL deve ser TTL = 3, porque como se pode verificar na imagem abaixo, com TTL = 1 ou com TTL = 2, o pacote não chega ao Servidor1, que, por sua vez não retorna resposta. Ou seja, o pacote só consegue chegar ao Servidor1, com TTL igual ou superior a 3.



* Calcule o valor médio do tempo de ida-e-volta (*Round-Trip Time*) obtido.

  
O tempo médio de ida-e-volta pode-se saber calculando:

(0.024+0.013+0.013+0.012+0.019+0.012)/6 = 0.016ms

2. Usando o Wireshark, capture o tráfego gerado pelo traceroute para os seguintes tamanhos de pacote: (i) sem especificar, ou seja, o tamanho por defeito; (ii) 3219 bytes. Utilize como máquina destino o host marco.uminho.pt . Pare a captura. Com base no tráfego capturado, identifique os pedidos ICMP Echo Request e o conjunto de mensagens devolvidas como resposta.

Selecione a primeira mensagem ICMP capturada referente a (i) e centre a análise no nível protocolar IP. Através da análise do cabeçalho IP diga:

* Qual é o endereço IP da interface ativa do seu computador?
* Qual é o valor do campo protocolo? O que identifica?
* Quantos bytes tem o cabeçalho IP(v4)? Quantos bytes tem o campo de dados (payload) do datagrama? Como se calcula o tamanho do payload?
* O datagrama IP foi fragmentado? Justifique.
* Ordene os pacotes capturados de acordo com o endereço IP fonte e analise a sequência de tráfego ICMP gerado a partir do endereço IP atribuído à interface da sua máquina. Para a sequência de mensagens ICMP enviadas pelo seu computador, indique que campos do cabeçalho IP variam de pacote para pacote.
* Observa algum padrão nos valores do campo de identificação do datagrama IP e TTL?
* Ordene o tráfego capturado por endereço destino e encontre a série de respostas ICMP TTL *exceeded* enviadas ao seu computador. Qual é o valor do campo TTL? Esse valor permanece constante para todas as mensagens de resposta ICMP TTL *exceeded* enviados ao seu host? Porquê?

3. Pretende-se agora analisar a fragmentação de pacotes IP. Reponha a ordem do tráfego capturado usando a coluna do tempo de captura. Observe o tráfego depois do tamanho de pacote ter sido definido para 3219 bytes.

* Localize a primeira mensagem ICMP. Porque é que houve necessidade de fragmentar o pacote inicial?
* Imprima o primeiro fragmento do datagrama IP segmentado. Que informação no cabeçalho indica que o datagrama foi fragmentado? Que informação no cabeçalho IP indica que se trata do primeiro fragmento? Qual é o tamanho deste datagrama IP?
* Imprima o segundo fragmento do datagrama IP original. Que informação do cabeçalho IP indica que não se trata do 1º fragmento? Há mais fragmentos? O que nos permite afirmar isso?
* Quantos fragmentos foram criados a partir do datagrama original? Como se detecta o último fragmento correspondente ao datagrama original?
* Indique. Resumindo, os campos que mudam no cabeçalho IP entre os diferentes fragmentos, e explique a forma como essa informação permite reconstruir o datagrama original.