

Universidade do Minho
Mestrado Integrado em Engenharia Informática
Redes de Computadores
TP2: Protocolo IPv4 (Parte I)

Datagramas IP e Fragmentação

(Nota importante: O trabalho é para ser realizado nas aulas PL correspondentes.

Não serão aceites trabalhos "resolvidos em casa".)

1. Objectivos

O principal objectivo deste trabalho é o estudo do *Internet Protocol* (IP) nas suas principais vertentes, nomeadamente: (i) estudo do formato de um pacote ou datagrama IP; (ii) fragmentação de pacotes IP; (iii) endereçamento IP; e (iv) encaminhamento IP.

Na primeira parte deste estudo é realizado o registo de datagramas IP enviados e recebidos através da execução do programa *traceroute*. São analisados os vários campos de um datagrama IP e detalhado o processo de fragmentação realizado pelo IP. Para tal, o seu computador deve estar conectado à rede Ethernet da sala de aula.

2. Captura de tráfego IP

Com o objectivo de obter um registo de tráfego IP, pretende-se usar o programa *traceroute* para descobrir uma rota IP, enviando pacotes de diferentes tamanhos para um determinado destino X.

O comando *traceroute* permite descobrir a rota (salto-a-salto) desde uma origem IP até um determinado destino IP, tirando partido da escolha de valores adequados para o "tempo-de-vida" indicado no cabeçalho IP dos datagramas enviados. O *traceroute* opera da seguinte forma: inicialmente, é enviado um ou mais datagramas com o campo TTL (*Time-To-Live*) igual 1; seguidamente, é enviado um ou mais datagramas com o TTL a 2; depois com o TTL a 3; e assim sucessivamente. Todos os pacotes são enviados para o mesmo destino que é especificado no comando *traceroute*.

Recorda-se que cada *router* no percurso até ao destino deve decrementar de 1 o TTL de cada datagrama recebido¹. Se o TTL atinge o valor 0, o *router* descarta o datagrama e devolve uma mensagem de controlo ICMP (*Internet Control Message Protocol*) ao *host* de origem, indicando que o TTL foi excedido (ICMP Type=11 - *TTL exceeded*). Como resultado deste comportamento, o *datagrama* com o TTL=1 (enviado pelo *host* que executa o *traceroute*) faz com que o *router* a um salto de distância envie uma mensagem ICMP para a origem. O datagrama com TTL=2 provoca esse comportamento no *router* a 2 saltos de distância e assim sucessivamente.

Desta forma, um *host* que execute o comando *traceroute* pode obter a identificação dos *routers* no percurso para o destino X, extraindo o endereço IP fonte dos datagramas que contenham mensagens ICMP do tipo TTL excedido.

¹ O RFC 791 diz que um *router* deve decrementar o TTL de pelo menos uma unidade.

1. Prepare uma **topologia CORE** para verificar o comportamento do *traceroute*. Ligue um *host (pc)* h1 a um *router* r2; o *router* r2 a um *router* r3, que por sua vez, se liga a um *host (servidor)* s4. (Note que pode não existir conectividade IP imediata entre h1 e s4 até que o routing estabilize). Ajuste o nome dos equipamentos atribuídos por defeito para a topologia do enunciado.
 - a. Active o *wireshark* ou o *tcpdump* no *pc* h1. Numa *shell* de h1, execute o comando *traceroute -I* para o endereço IP do *host* s4.
 - b. Registe e analise o tráfego ICMP enviado por h1 e o tráfego ICMP recebido como resposta. Comente os resultados face ao comportamento esperado.
 - c. Qual deve ser o valor inicial mínimo do campo TTL para alcançar o destino s4? Verifique na prática que a sua resposta está correta.
 - d. Qual o valor médio do tempo de ida-e-volta (Round-Trip Time) obtido?
2. Pretende-se agora usar o *traceroute* **na sua máquina nativa**, e gerar de datagramas IP de diferentes tamanhos.

Windows. O programa *tracert* disponibilizado no Windows não permite mudar o tamanho das mensagens a enviar. Como alternativa, o programa *pingplotter* (ou equivalente) na sua versão livre ou *shareware* (<http://www.pingplotter.com>) permite maior flexibilidade para efetuar *traceroute*. Descarregue, instale e experimente o *pingplotter* face ao objectivo pretendido.

O tamanho da mensagem enviada (ICMP *Echo Request*) pode ser estabelecido no *pingplotter* no menu Edit-> Options->Packet. Uma vez enviado um conjunto de pacotes com valores crescentes de TTL, o programa recomeça com TTL=1, após um determinado intervalo. Quer o valor do intervalo de tempo como o número de intervalos podem ser configurados.

Linux/Unix. O comando *traceroute* permite indicar o tamanho do pacote ICMP (opção -I) através da linha de comando, a seguir ao *host* de destino (ver *man traceroute*).

Exemplo: `%traceroute -I router-di.uminho.pt 512`

Documente as suas respostas com a impressão do(s) output(s) (e.g. pacote(s)) que as suportam. Para esse feito use, por exemplo, File->Print, selecione *packet only*, e coloque o mínimo de detalhe suficiente para responder à pergunta e identificar o seu computador.

Procedimento a seguir:

Usando o *wireshark* capture o tráfego gerado pelo *traceroute* para os seguintes tamanhos de pacote: (i) sem especificar, i.e., usando o tamanho por defeito; e (ii) 35XX bytes, em que XX é o seu número de grupo. 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 em resposta a esses pedidos.

Selecione a primeira mensagem ICMP capturada (referente a (i) tamanho por defeito) e centre a análise no nível protocolar IP (expanda o *tab* correspondente na janela de detalhe do *wireshark*). Através da análise do cabeçalho IP diga:

- a. Qual é o endereço IP da interface ativa do seu computador?
 - b. Qual é o valor do campo protocolo? O que identifica?
 - c. Quantos *bytes* tem o cabeçalho IP(v4)? Quantos *bytes* tem o campo de dados (*payload*) do datagrama? Como se calcula o tamanho do *payload*?
 - d. O datagrama IP foi fragmentado? Justifique.
 - e. Ordene os pacotes capturados de acordo com o endereço IP fonte (e.g., selecionando o cabeçalho da coluna *Source*), 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.
 - f. Observa algum padrão nos valores do campo de Identificação do datagrama IP e TTL?
 - g. 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 35XX *bytes*.
- a. Localize a primeira mensagem ICMP. Porque é que houve necessidade de fragmentar o pacote inicial?
 - b. 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?
 - c. 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?
 - d. Quantos fragmentos foram criados a partir do datagrama original? Como se detecta o último fragmento correspondente ao datagrama original?
 - e. 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.

(Fim da Parte I)

Bibliografia

Internetworking - Protocolo IP (Notas de Apoio das Aulas Teóricas)

traceroute: <http://tools.ietf.org/html/rfc2151> (secção 3.4)

Internet Protocol (IP): <http://tools.ietf.org/html/rfc791>

Internet Message Control Protocol (ICMP): <http://tools.ietf.org/html/rfc792>

Nota: Parte deste trabalho é baseado no Wireshark Lab 802.11 [J. Kurose e K. Ross].