Universidade do Minho

Licenciatura em Ciências da Computação

Sistemas de Comunicações e Redes

TP2: Protocolo IPv4 (Parte I – 2 aulas)

Datagramas IP e Fragmentação

1. Objetivos

O principal objetivo 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 wireless da sala de aula.

2. Captura de tráfego IP

Com o objetivo 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 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, especificado no comando *traceroute*.

Recorda-se que cada *router* no percurso até ao destino deve decrementar de 1 o TTL de cada datagrama recebido[1]. 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 TTL *exceeded* - Type=11). Como resultado, 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. Quando a mensagem *ICMP Echo request* atinge o host destino, este responde com a mensagem *ICMP Echo Reply* (Type=0).

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. (Nota: outros comandos que permitem traçar rotas são o *mtr* e o *pathping*).

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

Para verificar o comportamento do *traceroute*, implemente no **CORE** uma topologia retangular com um router em cada vértice. Ligue a cada um dos routers um *host* (*pc*) e atribua à rede de cada *host* os endereços 192.<nº do grupo+N>.<nº do grupo+N>.X/24, com N=0,1,2,3. Atribua ao decimal X um valor adequado. Atribua a este *host* o nome PC1. Ao *host* que está ligado ao router diametralmente oposto do do PC1 atribua o nome PC2. Coloque esses nomes nos respetivos *hosts* da topologia e arranque a rede. Active o *wireshark* no *host* PC1. Numa *shell* do PC1, execute o comando *traceroute –I* para o endereço IP do PC2. (*Note que pode não existir conectividade IP imediata entre os hosts até que o anúncio de rotas estabilize*).

a. Registe e analise o tráfego ICMP enviado pelo PC1 e o tráfego ICMP recebido como resposta. Comente os resultados face ao comportamento esperado.
b. Qual deve ser o valor inicial mínimo do campo TTL para alcançar o PC2? Verifique na prática que a sua resposta está correta.
c. Calcule o valor médio do tempo de ida-e-volta (*Round-Trip Time*) obtido? (Para melhorar a média, convém alterar o número de *probe packets* com a opção -q).

2. Pretende-se agora usar o *traceroute* **na sua máquina nativa**. (Nota: o *tracert* disponibilizado no Windows não permite mudar o tamanho das mensagens a enviar. Porém, no Linux/Unix, o *traceroute* permite indicar o tamanho do pacote ICMP através da linha de comando, a seguir ao *host* de destino (ver *man traceroute*). Por 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.* Coloque apenas o detalhe necessário para sustentar a resposta e identificar o seu computador.

   Usando o *wireshark*, capture o tráfego gerado pelo *traceroute -I/tracert* usando 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 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 IPv4? 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 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. Indique o padrão observado 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. Capture com o *Wireshark* o tráfego gerado pelo comando *ping <opção> 52XY marco.uminho.pt*, onde a opção *–l* (Windows) ou *–s* (Linux) define o número de bytes enviados no campo de dados do pacote ICMP, X representa as dezenas e Y as unidades do número do grupo. Por exemplo, X=2 e Y=4 para os grupos G24 e G124. Observe o tráfego capturado.

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 primeiro 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? Estabeleça um filtro no *Wireshark* que permita listar o último fragmento do datagrama IP segmentado.
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.
f. Sabendo que a opção *-f* (Windows) ou *-M do* (Linux) ativa a flag "*Don't Fragment*" (DF) no cabeçalho do IPv4, usando *ping <opção DF> <opção pkt size> SIZE marco.uminho.pt*, (opção *pkt size = –l* (Windows) ou *–s* (Linux)), determine o valor máximo de *SIZE* sem que ocorra fragmentação do pacote? Justifique o valor obtido.

(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