Universidade do Minho

Mestrado Integrado em Engenharia Informática

Redes de Computadores

TP4: Protocolo IPv4 (Parte I)

Datagramas IP e Fragmentação

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) endereçamento IP; (iii) encaminhamento IP; e (iv) fragmentação de pacotes 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.

Recomenda-se a leitura da bibliografia aconselhada, sobretudo aos alunos que estiveram ausentes na aula teórica sobre esta matéria.

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 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 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* n1 a um *router* n2; o *router* n2 a um *router* n3 que, por sua vez, se liga a um *host* n4.
    a. Active o *wireshark* ou o *tcpdump* no nó 1. Numa *shell* de n1, execute o comando *traceroute -I* para o endereço IP do *host* n4.
    b. Registe e analise o tráfego ICMP enviado por n1 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 n4? Qual o tempo médio de ida-e-volta (RTT - 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. Como alternativa, o programa *pingplotter* 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 2500

    Como tem sido recomendado, documente as suas respostas com a impressão do(s) outputs (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:
    Usando o *wireshark* capture o tráfego gerado pelo *traceroute* para os seguintes tamanhos de pacote: (i) tamanho por defeito e (ii) 3072 bytes. Utilize como máquina destino o *host* router-di.uminho.pt.
    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 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 com base no IP gerado na sua máquina. Quais os campos do datagrama IP cujo valor muda sempre na série de mensagens ICMP enviadas pelo seu computador?
f. Que campos se mantêm constantes? Que campos se devem manter, preferencialmente, constantes? Justifique.
g. Observa algum padrão nos valores do campo de Identificação do datagrama IP?
h. A seguir (com os pacotes ordenados por endereço destino) encontre a série de respostas ICMP TTL *exceeded* enviadas ao seu computador pelo primeiro router. Qual é o valor dos campos Identificação e TTL?
i. Esses valores permanecem constantes para todas as mensagens de resposta ICMP TTL *exceeded* enviados pelo primeiro *router* 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.

a. Localize a primeira mensagem ICMP depois do tamanho de pacote ter sido definido em 3072 *bytes*. A mensagem foi fragmentada? Porque é que houve (ou não) necessidade de o fazer?
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 verifique 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

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