Wireshark: IP

O texto original, em inglês, pode ser encontrado em

https://www-net.cs.umass.edu/wireshark-labs/Wireshark\_IP\_v7.0.pdf

Neste trabalho, será estudado o protocolo IP, com foco no datagrama IP. Faremos isso analisando um rastreamento de datagramas IP enviados e recebidos por uma execução do programa *traceroute*. Vamos investigar os vários campos do datagrama IP e estudar a fragmentação de IP em detalhes. Antes de iniciar, revise a seção 4.4 do livro do J. Kurose (6ª edição).

**Capturando pacotes de uma execução de *traceroute***

Para gerar um *trace* (rastreamento) de datagramas IP, usaremos o programa *traceroute* para enviar datagramas de tamanhos diferentes para um destino qualquer. Lembre-se que o *traceroute* opera enviando primeiro um ou mais datagramas com TTL, no cabeçalho IP, definido como 1; Em seguida, envia uma série de um ou mais datagramas para o mesmo destino com um valor TTL de 2; Em seguida, envia uma série de datagramas para o mesmo destino com um valor TTL de 3; e assim por diante. Lembre-se de que um roteador deve decrementar de uma unidade o TTL em cada datagrama recebido. Se o TTL atingir 0, o roteador retornará uma mensagem ICMP (tipo 11 –TTL-expirado) para o host que enviou o datagrama. Como resultado desse comportamento, um datagrama com um TTL igual a 1 (enviado pelo host) fará com que o roteador que está a um enlace do host envie uma mensagem ICMP (TTL expirado) de volta ao remetente; o mesmo acontecendo com o segundo, terceiro, ... roteadores no caminho. Dessa maneira, o host que executa o *traceroute* pode aprender as identidades dos roteadores entre ele e o destino X, observando os endereços IP de origem nos datagramas que contêm as mensagens ICMP TTL expirado. Vamos executar o *traceroute* e enviar datagramas de vários comprimentos.

**Windows**

O programa *tracert* fornecido com o Windows não permite alterar o tamanho da mensagem de solicitação de eco ICMP enviada pelo programa tracert. Um programa de rastreamento mais agradável do Windows é o ***pingplotter***, disponível nas versões gratuita e shareware em ***http://www.pingplotter.com***. Faça o download, instale o *pingplotter* e teste-o executando alguns traceroutes nos seus sites favoritos. O tamanho da mensagem de solicitação de eco ICMP pode ser explicitamente definido no pingplotter, selecionando o item de menu *Edit-> Options-> Packet* *Options* e preenchendo o campo de tamanho do pacote (*Packet Size*). O tamanho padrão do pacote é de 56 bytes. Depois que o pingplotter envia uma série de pacotes com os valores TTL crescentes, ele reinicia o processo de envio novamente com um TTL de 1, depois de aguardar um “intervalo de rastreio” (trace interval). O valor do intervalo de rastreio e o número de intervalos podem ser explicitamente definidos no pingplotter.

**Linux / Unix**

Com o comando ***traceroute***, o tamanho do datagrama UDP enviado para o destino pode ser explicitamente definido indicando o número de bytes no datagrama; este valor é inserido na linha de comando do traceroute imediatamente após o nome ou endereço IP do destino. Por exemplo, para enviar datagramas de 2000 bytes para http://gaia.cs.umass.edu, o comando seria:

**traceroute gaia.cs.umass.edu 2000**

Faça o seguinte:

Inicie o Wireshark e inicie a captura de pacotes (Capture-> Start) e então pressione OK na tela *Wireshark Packet Capture Options*. Se você estiver usando uma plataforma Windows, inicie o pingplotter e digite o nome de um destino na janela “Address to Trace”. Digite “3” no campo "# of times to Trace", para não coletar muitos dados. Selecione o item de menu Editar-> Opções Avançadas-> Opções de Pacotes, insira um valor de 56 no campo Packet Size e pressione OK. Em seguida, pressione o botão Trace. Você deve ver uma janela de pingplotter parecida com esta:

**Vide versão em inglês**

Em seguida, envie um conjunto de datagramas com um comprimento maior, selecionando Editar-> Opções Avançadas-> Opções de Pacotes, insira um valor de 2000 no campo *Packet Size* e pressione OK. Em seguida, pressione o botão *Resume*. Por fim, envie um conjunto de datagramas com um comprimento maior (3500) no campo PacketSize e pressione OK. Em seguida, pressione o botão *Resume*. Para rastrear o traçado Wireshark • Se você estiver usando uma plataforma Unix ou Mac, insira três comandos tracerout, um com um comprimento de 56 bytes, um com um comprimento de 2000 bytes e um com um comprimento de 3500 bytes.

Se você estiver usando uma plataforma Linux, insira três comandos traceroute, um com um comprimento de 56 bytes, um com um comprimento de 2000 bytes e outro com um comprimento de 3.500 bytes.

Pare o rastreamento do Wireshark (*Stop Wireshark Tracing*).

**Analisando o *trace (rastreamento)***

No seu rastreamento, você poderá ver a série de solicitações de Eco ICMP (no caso da máquina Windows) ou o segmento UDP (no caso do Unix) enviado pelo seu computador e as mensagens de ICMP (TTL expirado) retornadas ao seu computador pelos roteadores intermediários. Nas perguntas abaixo, vamos supor que você esteja usando uma máquina Windows (equivalentes para o caso de uma máquina Linux). Sempre que possível, ao responder uma pergunta abaixo, você deve entregar uma impressão da tela do(s) *trace(s)* realizado(s) (a qual(is) pacote(s) corresponde(m) o rastreamento usado para responder à pergunta). Anote a saída para que fique claro de onde você está obtendo as informações para sua resposta (por exemplo, marque a cópia em papel com uma caneta ou arquivo ou use *File -> Print e Select Packet Only*), escolha *Packet Summary Line* e selecione a quantidade mínima de detalhes do pacote que você precisa para responder à pergunta.

1. Selecione o primeiro pacote ICMP Echo enviado pelo seu computador e expanda a parte do protocolo IP na janela de detalhes do pacote. Qual é o endereço IP do seu computador?

**Vide figura na versão em inglês**

1. Dentro do cabeçalho do datagrama IP, qual é o valor no campo “protocolo da camada superior”?
2. Quantos bytes têm o cabeçalho IP? Quantos bytes têm na carga útil do datagrama IP? Explique como você determinou o número de bytes de carga útil.
3. Este datagrama IP foi fragmentado? Explique como você determinou se o datagrama foi ou não fragmentado.

Em seguida, ordene os pacotes rastreados de acordo com o endereço IP de origem, clicando na coluna *Source*; uma pequena seta apontando para baixo deve aparecer ao lado da palavra Source. Selecione a primeira mensagem ICMP Echo Request enviada pelo seu computador e expanda a parte do IP na janela “detalhes do cabeçalho do pacote selecionado”. Na janela “listagem de pacotes capturados”, você deve ver todas as mensagens ICMP subseqüentes (talvez com pacotes intercalados adicionais enviados por outros protocolos em execução no seu computador) abaixo deste primeiro pacote ICMP. Percorra as mensagens ICMP enviadas pelo seu computador.

1. Quais campos do datagrama IP sempre mudam de um datagrama para o próximo nesta série de mensagens ICMP enviadas pelo seu computador?
2. Quais campos permanecem constantes? Qual dos campos deve permanecer constante? Quais campos devem mudar?
3. Descreva o padrão que você vê nos valores do campo “Identificação do datagrama IP”.

A seguir (com os pacotes ainda classificados por endereço de origem) encontre a série de respostas “ICMP TTL expirado” enviadas ao seu computador pelo roteador de primeiro salto.

1. Qual é o valor no campo Identificação e no campo TTL?
2. Esses valores permanecem inalterados para todas as respostas ICMP enviadas ao seu computador pelo roteador mais próximo (primeiro salto)? Por que?

**Fragmentação**

Ordene a listagem de pacotes de acordo com o tempo novamente, clicando na coluna *Time*.

1. Encontre a primeira mensagem ICMP Echo Request que foi enviada pelo seu computador depois de ter alterado o tamanho do pacote para 2000. Essa mensagem foi fragmentada em mais de um datagrama IP? (Obs: Se o seu computador tiver uma interface Ethernet, um tamanho de pacote de 2000 deve causar a fragmentação)
2. Imprima o primeiro fragmento do datagrama IP fragmentado. Que informação no cabeçalho IP indica que o datagrama foi fragmentado? Que informação no cabeçalho IP indica se este é o primeiro fragmento versus um último fragmento? Qual o tamanho do datagrama IP?
3. Imprima as informações do segundo fragmento do datagrama IP. Que informação no cabeçalho IP indica que este não é o primeiro fragmento de datagrama? Existem mais fragmentos? Como você pode saber?
4. Quais campos mudam no cabeçalho IP do primeiro para o segundo fragmento?

Agora encontre a primeira mensagem ICMP Echo Request que foi enviada pelo seu computador depois que você alterou o tamanho do pacote para 3500.

1. Quantos fragmentos do datagrama original foram criados?
2. Quais campos mudam no cabeçalho IP entre os fragmentos?