# Wireshark Laboratório: IP

Neste laboratório investigaremos o protocolo IP, focando na análise de datagramas IP enviados e recebidos capturados durante a execução do programa traceroute. Investigaremos os diversos campos do datagrama IP e estudaremos a fragmentação IP em detalhes.

Antes de iniciar este laboratório, você provavelmente desejará revisar as seções 1.63 do texto e a seção 3.4 da RFC 2151[1] para se atualizar sobre a operação do programa traceroute. Você também desejará ler a seção 4.4 no texto, e provavelmente a RFC 791[2] em mãos também, para uma discussão do IP.

## 1. Capturando pacotes a partir de uma execução do traceroute

Para gerar um registro dos datagramas IP para este laboratório, usaremos o programa traceroute para enviar datagramas de diferentes tamanhos para algum destino, X. O traceroute opera através do envio de um ou mais datagramas com o campo de tempo de vida (TTL) no cabeçalho do IP com valor 1; depois envia uma série de um ou mais datagramas para o mesmo destino com um valor do TTL igual a 2; depois ele envia uma série de datagramas para o mesmo destino com um valor do TTL igual a 3; e assim por diante. Lembre-se de que um roteador deve decrementar o campo TTL em 1 para cada datagrama recebido (atualmente, a RFC 791 diz que o roteador deve decrementar o TTL em cada datagrama recebido por pelo menos um). Se o TTL chega a 0, o roteador retorna uma mensagem ICMP (tipo 11 – TTL excedido) para o hospedeiro transmissor. Como resultado deste comportamento, um datagrama com um TTL igual a 1 (enviado pelo hospedeiro que está executando o traceroute) fará com que o roteador a um salto do transmissor envie uma mensagem ICMP de TTL excedido de volta ao transmissor; o datagrama enviado com TTL 2 fará com que o roteador a dois saltos envie uma mensagem ICMP de volta ao transmissor; o datagrama enviado com TTL 3 fará com que o roteador a três saltos envie uma mensagem ICMP de volta para o transmissor; e assim por diante. Desta forma, o hospedeiro que executa o traceroute pode aprender as identidades dos roteadores entre ele mesmo e o destino X olhando os endereços IP de origem dos datagramas que contêm as mensagens ICMP de TTL excedido.

Nós iremos executar o traceroute e fazer com que ele envie datagramas de diversos comprimentos.

Observações com relação aos sistemas operacionais executando o traceroute:

- **Windows.** No entanto, o programa tracert fornecido com o Windows não nos permite alterar o tamanho da mensagem ICMP de solicitação de eco. Um programa de traceroute melhor é o pingplotter, disponível em versões gratuitas em http://www.pingplotter.com/. Faça o download e instale o pingplotter, e faça alguns testes executando alguns traceroutes para os seus sites favoritos. O tamanho da mensagem de pedido de eco ICMP pode ser modificado explicitamente no pingplotter através da seleção do item do menu Edit→Options→Packet options e preenchendo o campo de Packet Size (tamanho do pacote). O tamanho de pacote default é de 56 bytes. Uma vez que o pingplotter tenha enviado uma série de pacotes com valores crescentes de TTL, ele reinicia o processo de envio de novo com TTL 1, depois de aguardar um intervalo de

1 ftp://ftp.rfc-editor.org/in-notes/rfc2151.txt
2 ftp://ftp.rfc-editor.org/in-notes/rfc791.txt

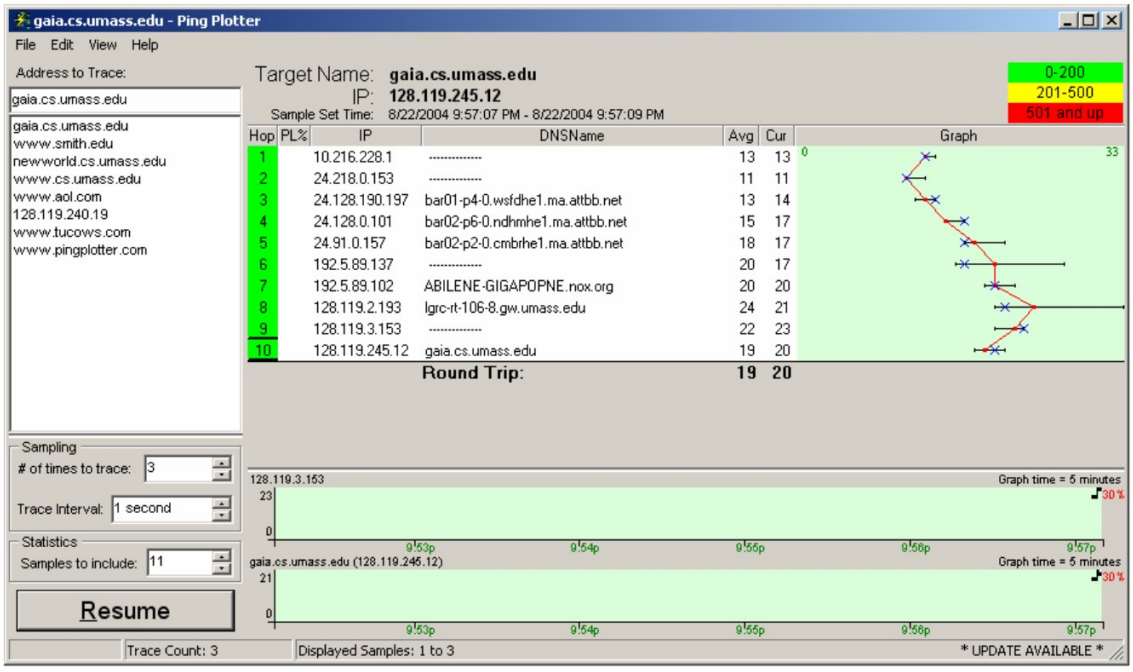
tempo dado por Trace Interval. O valor do Trace Interval e o número de intervalos podem ser estabelecidos explicitamente no pingplotter.

- **Linux/Unix.** Com o comando traceroute do Unix. O tamanho de um datagrama UDP enviado para um destino específico pode ser explicitamente definido indicando o numero de bytes do datagrama. Esse valor deve ser colocado no comando logo após o endereço do destinatário. Por exemplo, para executar um traceroute com datagramas de 2000 bytes para gaia.cs.umass.edu, o comado deve ser:

%traceroute gaia.cs.umass.edu 2000

Faça o seguinte:

- Inicie o Wireshark e comece a captura de pacotes (Capture → Start), selecione a placa de rede e aperte OK na tela de Opções de Captura de Pacotes do Wireshark.
- Se você está utilizando windows**,** inicialize o pingplotter e entre o nome de um destino alvo no campo de “Address to Trace”. Tecle 3 no campo de “# of times to Trace”, de modo que você não capturará dados excessivos. Selecione o item Edit→Options→Packet e entre com o valor de 56 no campo de Packet Size e aperte OK. Depois aperte o botão “Trace”. Você deverá ver uma janela do pingplotter que se parece com a imagem a seguir.




Depois, envie um conjunto de datagramas com um comprimento maior, selecionando Edit → Options → Packet e entre o valor 2000 no campo de Packet Size e depois aperte OK. Depois aperte o botão Resume.

Finalmente, envie um conjunto de datagramas com um comprimento ainda maior, selecionando Edit→Options→Packet e entre o valor 3500 no campo de Packet Size e depois aperte OK. Depois aperte o botão Resume.

Pare o trace do wireshark.

- Se você está utilizando uma plataforma Unix, execute 3 comandos traceroute, um com tamanho de 56 bytes, outro com 2000 bytes e o último com 3500 bytes

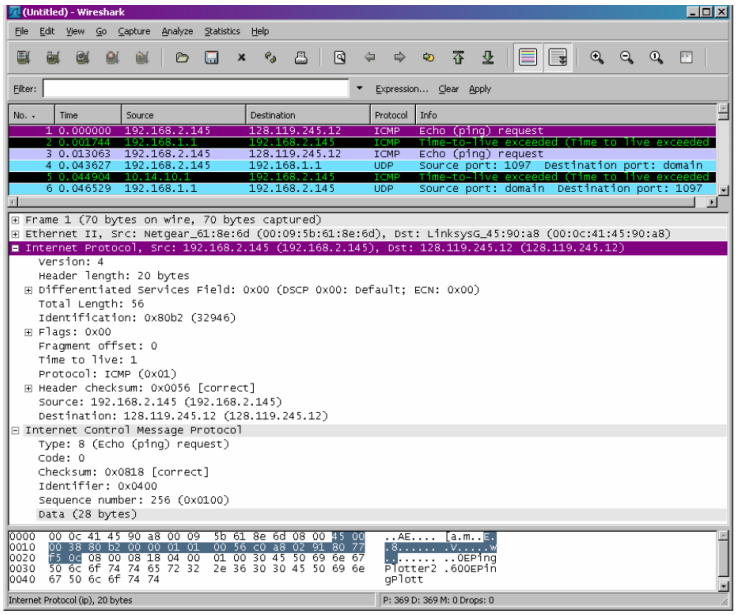
Pare o trace do wireshark.

Se você não pode executar o wireshark conectado a internet. Você pode baixar um arquivo de trace de pacotes o qual foi capturado enquanto seguia os passos acima no computador windows de um dos autores[3]. Você pode achar interessante baixar esse trace, mesmo se você capturou o seu próprio, e utilizá-lo para responder as questões abaixo.

## 2. Analisando no registro capturado

No seu registro, você deve ser capaz de ver uma série de pedidos de eco do ICMP (no caso do windows) ou segmentos UDP (no caso do Unix) enviados pelo seu computador e as mensagens TTL-exceeded do ICMP retornadas ao seu computador pelos roteadores intermediários. Sempre que possível, quando responder uma questão você deve mostrar o(s) pacote(s) do trace que foram necessários para responder a pergunta. Uma maneira de facilitar esta visualização é inserir “icmp or udp”, sem as aspas, na caixa de textos de filtros (Filter) e pressionar o botão Apply. Isso deixa apenas o que importa na tela. Para mostrar um pacote, use File -> Print, escolha apenas o(s) pacote(s) selecionado(s), escolha packet summary line e selecione o mínimo de detalhe que foi preciso para responder a questão.

1. Selecione o primeiro pedido de eco do ICMP mandado pelo seu computador e expanda a parte Internet Protocol do pacote na janela de detalhes do pacote. Qual é o endereço de IP do seu computador?




2. Dentro do cabeçalho IP do pacote, qual é o valor no campo de protocolo da camada superior.
3. Quantos bytes estão no cabeçalho IP? Quantos bytes de carga útil tem o datagrama IP? Explique como você determinou o número de bytes da carga útil.

---

3 Baixe o arquivo zip http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip e extraia o arquivo ip-ethereal-trace-1. Os traces dentro do arquivo zip foram coletados pelo wireshark executado no computador de um dos autores, enquanto seguia os passos indicados no wireshark lab. Após ter baixado o trace, você pode carregar ele no wireshark através do menu Open e selecionando o arquivo de trace ip-ethereal-trace-1 trace file.

4. Esse datagrama IP foi fragmentado? Explique como você determinou se o datagrama foi ou não fragmentado.

Em seguida, classifique os pacotes rastreados de acordo com o endereço de IP de origem, clicando no botão Source do cabeçalho da coluna; uma pequena seta apontando para baixo deve aparecer ao lado da palavra Source. Se a seta apontar para cima, clique no cabeçalho da coluna source novamente. Selecione a primeira mensagem de solicitação de eco ICMP enviada pelo seu computador e expanda a parte internet protocol da janela "detalhes do cabeçalho do pacote selecionado". Na "lista de pacotes capturados" janela, você deverá ver todas as mensagens ICMP subsequentes (talvez com pacotes intercalados enviados por outros protocolos em execução no seu computador) abaixo deste primeiro ICMP. Use a seta para baixo no teclado para percorrer as mensagens ICMP enviadas pelo seu computador.

5. Quais campos no datagrama IP sempre mudam de um datagrama para o próximo dentro desta série de mensagens ICMP enviadas pelo seu computador?

6. Quais campos permanecem constantes? Qual dos campos devem permanecer constante? Quais campos deve mudar? Por quê?

7. Descreva o padrão que você vê nos valores no campo Identificação do Datagrama IP. Depois (com os pacotes ainda classificados por endereço de origem) encontre a série de respostas ICMP TTL- exceeded enviadas ao seu computador pelo roteador mais próximo (primeiro salto).

8. Qual é o valor no campo Identificação e no campo TTL?

9. Esses valores permanecem inalterados para todas as respostas ICMP TTL-exceeded enviadas ao seu computador pelo roteador mais próximo (primeiro salto)? Por quê?

## Fragmentação

Classifique a lista de pacotes de acordo com o horário novamente, clicando na coluna Hora.

10. Localize a primeira mensagem de solicitação de eco ICMP que foi enviada pelo seu computador após você ter alterado o tamanho do pacote para 2000. Essa mensagem foi fragmentado em mais de um datagrama IP?[4]

11. Mostre o primeiro fragmento do datagrama IP fragmentado. Que informação no cabeçalho IP indica que o datagrama foi fragmentado? Quais informações no cabeçalho IP indicam se este é o primeiro fragmento ou o último fragmento? Quanto tempo dura esse datagrama IP?

---

4 Se você achar que seu pacote não foi fragmentado, você deve baixar o arquivo zip http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip e extraia o ip- ethereal-trace-1packet trace. Se o seu computador tiver uma interface Ethernet, um pacote tamanho de 2000 deve causar fragmentação.Os pacotes no arquivo de rastreamento ip-ethereal-trace-1 em http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip tem menos de 1500 bytes. Isso ocorre porque o computador no qual o rastreamento foi coletado possui um Placa Ethernet que limita o comprimento do pacote IP máximo a 1500 bytes (40 bytes do cabeçalho TCP / IP dados e 1460 bytes de carga útil do protocolo da camada superior). Esse valor de 1500 bytes é o valor máximo padrão comprimento permitido pela Ethernet. Se o seu rastreamento indicar um datagrama com mais de 1500 bytes e o computador estiver usando uma conexão Ethernet, o Wireshark está relatando o comprimento incorreto do datagrama IP; provavelmente também mostra apenas um datagrama IP grande em vez de vários datagramas menores. Essa inconsistência no relatório comprimentos é devido à interação entre o driver Ethernet e o software Wireshark. Nós recomendamos que, se você tiver essa inconsistência, execute este laboratório usando o arquivo de rastreamento ip-ethereal-trace-1.

12. Mostre o segundo fragmento do datagrama IP fragmentado. Que informação em o cabeçalho IP indica que este não é o primeiro fragmento de datagrama? Existem mais fragmentos? Como você pôde saber?

13. Quais campos são alterados no cabeçalho IP entre o primeiro e o segundo fragmento?

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

14. Quantos fragmentos foram criados a partir do datagrama original?

15. Quais campos são alterados no cabeçalho IP entre os fragmentos?