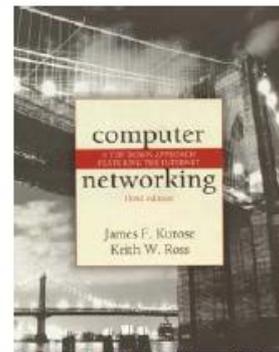


Ethereal Lab: IP



Computer Networking: A Top-down Approach Featuring the Internet, 3rd edition.

Version: 1.0

© 2005 J.F. Kurose, K.W. Ross. All Rights Reserved

Neste laboratório, iremos investigar o protocolo IP, focando o datagrama IP. Vamos fazê-lo através da análise de um trace de datagramas IP enviados e recebidos por uma execução do programa traceroute (o programa Traceroute será explorado em mais detalhe no Ethereal ICMP laboratório). Nós vamos investigar os vários campos no datagrama IP estudar a fragmentação em detalhe.

Antes de iniciar este laboratório, você provavelmente vai querer rever o item 1.63 no texto e o item 3.4 da RFC 2151 [<ftp://ftp.rfc-editor.org/in-notes/rfc2151.txt>] para atualizar-se sobre o funcionamento do programa traceroute. Você também vai querer ler o item 4,4 do texto, e provavelmente também ter a RFC 791 [<ftp://ftp.rfc-editor.org/in-notes/rfc791.txt>] a mão, para uma discussão do protocolo IP.¹

1. Capturando pacotes a partir da execução do traceroute

A fim de gerar um trace de datagramas IP para este laboratório, vamos usar o programa traceroute para enviar datagramas de tamanhos diferentes para algum destino, X. Lembre-se que traceroute funciona através do envio de um ou mais datagramas com o time-to-live (TTL) no cabeçalho IP definido como 1, seguido do envio de outras séries de datagramas com TTL=2, 3, 4 e assim por diante. Lembre-se que em cada roteador que o datagrama alcança o TTL é decrementado em 1 (na verdade, a RFC 791 diz que o roteador deve diminuir o TTL de pelo menos um). Se o TTL que chega estiver em 0 (zero), o router volta uma mensagem ICMP (tipo 11 - TTL excedido) para o host que originou o datagrama. Como resultado deste comportamento, um datagrama enviado com um TTL=1 (enviado pelo host executando traceroute) a um host distante, será decrementado em 1 no roteador local (próximo) e provocará o envio da mensagem ICMP TTL excedido de volta para o remetente, o datagrama enviado com um TTL=2 fará com que o segundo roteador (dois saltos) envie uma mensagem ICMP para o remetente, o datagrama enviado com um TTL=3 fará com que terceiro roteador (três saltos) envie uma mensagem ICMP para o remetente, e assim por diante. Desta forma, o host executando traceroute pode aprender as identidades dos roteadores entre sua rede e a rede do host destino X, olhando para os endereços IP de origem no datagramas contendo as mensagens ICMP de TTL excedido.

Queremos executar o traceroute para enviar datagramas de vários comprimentos. Assim:

No Windows: O programa tracert usado com o Windows não permite alterar o tamanho do echo request ICMP, mensagem PING, enviada pelo programa tracert (usado para o nosso laboratório Ethereal ICMP). Uma bom programa traceroute, em Windows, é o *pingplotter*, disponível na versão gratuita em <http://www.pingplotter.com>. Baixe e instale *pingplotter*, para testá-lo realizando traceroutes para os seus sites favoritos.

¹ Todas as referências ao texto neste laboratório são a Computer Networking: A Top-down Approach Featuring the Internet, 3a edição.

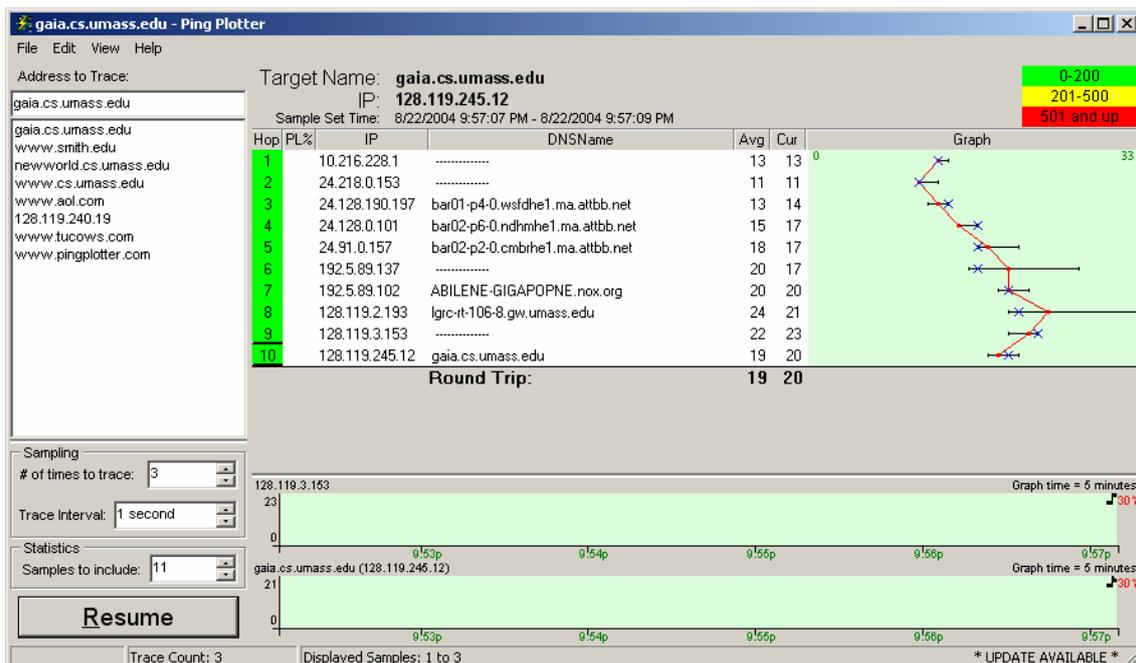
O tamanho da mensagem ICMP echo request pode ser explicitamente definida no *pingplotter* selecionando o item de menu *Edit-> Advanced Options-> Packet Options* e, em seguida, preenchendo o tamanho do campo *Packet Size* O tamanho do pacote padrão é 56 bytes. Então *pingplotter* enviará uma série de pacotes com valores TTL incrementados de um. Ele reiniciará o processo de envio de novo com um TTL=1, depois de esperar uma quantidade de Traces em um intervalo de tempo. O valor do Intervalo entre Traces e o número de intervalos podem ser explicitamente definidos em *pingplotter*.

No Linux / Unix: Com o comando *traceroute* do Unix, o tamanho do datagrama UDP enviado para o destino pode ser explicitamente definido, indicando o número de bytes do datagrama na linha de comando do *traceroute* imediatamente após o nome ou do endereço do destino. Por exemplo, para enviar no *traceroute* com datagramas de 2000 bytes para *gaia.cs.umass.edu*, o comando seria:

```
% traceroute gaia.cs.umass.edu 2000
```

Faça o seguinte:

- No Ethereal inicie a captura de pacotes (*Capture-> Start*) e pressione OK na tela de opções Ethereal Packet Capture (não precisa selecionar todas as opções aqui)
- Se você estiver usando uma plataforma Windows, inicie *pingplotter* e introduza um nome de um destino alvo no campo "*Address to Trace*". Digite 3 no campo "*# of times to trace*", assim você não coletará muitos dados. Selecione o item de menu *Edit -> Advanced Options-> Packet Options* e introduza um valor de 56 no campo *Packet Size* e pressione OK. Em seguida, pressione o botão *Resume*. Você deverá ver uma janela *pingplotter* parecida com esta:



Em seguida, enviar um conjunto de datagramas com um comprimento maior, escolhendo *Edit-> Advanced Options-> Packet Options* e introduza um valor de 2000 bytes no campo de *Packet Size* e pressione OK. Em seguida, pressione o botão *Resume*.

Finalmente, envie um conjunto de datagramas com um comprimento maior, escolhendo *Edit-> Advanced Options-> Packet Options* e introduzindo um valor de 3500 no campo de *Packet Size* e pressionando OK Em seguida, pressione o botão *Resume*.

Pare o rastreamento Ethereal.

Se você estiver usando uma plataforma Unix, digite três comandos *traceroute*, sendo um com

comprimento de 56 bytes, um com comprimento de 2000 bytes e um com comprimento de 3500 bytes.

Pare o rastreamento Ethereal.

Se você não conseguir executar o Ethereal numa rede conectada, você pode baixar o arquivo de rastreamento de pacotes que foi capturado quando o autor estava seguindo os passos acima, em seu computador Windows². Você pode usar o trace do autor ou o seu próprio trace, quando você for explorar as perguntas abaixo.

2. Um olhar sobre o trace capturado

Em seu trace, você deve ser capaz de ver a série de mensagens ICMP Echo Request (no caso de Máquina Windows) ou o segmento UDP (no caso do Unix), enviado pelo seu computador e as mensagens ICMP TTL exceeded retornadas ao seu computador pelos roteadores. Nas perguntas abaixo, vamos supor que você está usando uma máquina Windows, as questões correspondentes para o caso de uma máquina Unix devem ser idênticas. Sempre que possível, ao responder uma pergunta entregue uma cópia impressa do trace de pacote (s) que você usou para responder. Sobre a impressão explique sua resposta. Para imprimir um pacote, use *File-> Print*, escolha *Selected packet only*, escolha *Packet summary line*, e selecione a quantidade mínima de detalhes do pacote que você precisa para responder à pergunta.

1. Seleciona a primeira mensagem ICMP Echo Request enviada pelo seu computador, e expanda o pacote do Protocolo Internet na janela de detalhes do pacote.

The screenshot shows the Ethereal interface with a list of captured packets. Packet 9 is selected, showing an ICMP Echo Request from 10.216.228.1 to 192.168.1.102. The details pane shows the IP header and ICMP payload. The hex dump at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Telebit_73:8d:ce	Broadcast	ARP	who has 192.168.1.117? Tell 192.168.1.104
2	4.866867	192.168.1.100	192.168.1.1	SSDP	M-SEARCH * HTTP/1.1
3	4.868147	192.168.1.100	192.168.1.1	SSDP	M-SEARCH * HTTP/1.1
4	5.363536	192.168.1.100	192.168.1.1	SSDP	M-SEARCH * HTTP/1.1
5	5.364799	192.168.1.100	192.168.1.1	SSDP	M-SEARCH * HTTP/1.1
6	5.864428	192.168.1.100	192.168.1.1	SSDP	M-SEARCH * HTTP/1.1
7	5.865461	192.168.1.100	192.168.1.1	SSDP	M-SEARCH * HTTP/1.1
8	6.163045	192.168.1.102	128.59.23.100	ICMP	Echo (ping) request
9	6.176326	10.216.228.1	192.168.1.102	ICMP	Time-to-live exceeded
10	6.188629	192.168.1.102	128.59.23.100	ICMP	Echo (ping) request
11	6.202957	24.218.0.153	192.168.1.102	ICMP	Time-to-live exceeded
12	6.208597	192.168.1.102	128.59.23.100	ICMP	Echo (ping) request
13	6.234505	24.128.190.197	192.168.1.102	ICMP	Time-to-live exceeded
14	6.238695	192.168.1.102	128.59.23.100	ICMP	Echo (ping) request
15	6.257672	24.128.0.101	192.168.1.102	ICMP	Time-to-live exceeded
16	6.258750	192.168.1.102	128.59.23.100	ICMP	Echo (ping) request

Frame 9 (70 bytes on wire, 70 bytes captured)
Ethernet II, Src: 00:06:25:da:af:73, Dst: 00:20:e0:8a:70:1a
Internet Protocol, Src Addr: 10.216.228.1 (10.216.228.1), Dst Addr: 192.168.1.102 (192.168.1.102)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00)
Total Length: 56
Identification: 0x9d7c (40316)
Flags: 0x00
Fragment offset: 0
Time to live: 255
Protocol: ICMP (0x01)
Header checksum: 0x6ca0 (correct)
Source: 10.216.228.1 (10.216.228.1)
Destination: 192.168.1.102 (192.168.1.102)
Internet Control Message Protocol
.....
0000 00 20 e0 8a 70 1a 00 06 25 da af 73 08 00 45 c0P...%.S..E.
0010 00 38 9d 7c 00 00 ff 01 6c a0 0a d8 e4 01 c0 a88.....I.....
0020 01 66 0b 00 d9 46 00 00 00 00 45 00 00 54 32 d0f...F...E..T2.
0030 00 00 01 01 f6 16 c0 a8 01 66 80 3b 17 64 08 00:f.;d..
0040 f7 ca 03 00 50 03P.
Internet Protocol (ip), 20 bytes P: 380 D: 380 M: 0

² Baixe o arquivo zip <http://gaia.cs.umass.edu/ethereal-labs/ethereal-traces.zip> e extraia o arquivo ip-ethereal-trace-1. Os traces deste arquivo zip foram coletados pelo Ethereal rodando em um dos computadores do autor, quando executava os passos indicados neste laboratório Ethereal. Depois de ter baixado o arquivo trace, você pode carregá-lo no Ethereal e visualizar o rastreamento usando o menu suspenso, Abrir e, em seguida selecionando o arquivo de rastreamento ip-ethereal-trace-1.

Qual é o endereço IP do seu computador?

2. Dentro do cabeçalho do pacote IP, qual é o valor no campo do protocolo da camada superior?

3. Quantos bytes possui o cabeçalho IP?

Quantos bytes possui o campo de dados da Datagrama IP?

Explique como você determinou o número de bytes de do campo de dados (Pay load - carga útil).

4. Esse datagrama IP foi fragmentado?

Explique como você determinou se o datagrama foi fragmentado ou não.

Em seguida, classificar os pacotes traçado de acordo com o endereço IP de origem, clicando na coluna do cabeçalho *Source*; uma pequena seta apontando para baixo deve aparecer ao lado da palavra *Source*. Se a seta aponta para cima, clique na coluna do cabeçalho *Source* novamente. Selecione a primeira mensagem ICMP Echo Request enviada pelo seu computador, e expanda as informações do Protocolo Internet na janela "details of selected packet header". Na janela "*listagem de pacotes capturados*", você verá todas as mensagens ICMP subseqüentes (talvez com pacotes adicionais, enviados por outros protocolos em execução no seu computador, intercalados). Use a seta para baixo para mover através das mensagens ICMP enviadas pelo seu computador.

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

6. Quais os campos permanecem constantes?

Qual dos campos devem permanecer constante?

Quais os campos deve mudar?

7. Descreva o padrão que você vê nos valores no campo *Identification* do datagrama IP.

Em seguida, com os pacotes ainda ordenadas por endereço de origem, encontre a série de ICMP TTL exceeded enviados como respostas para o computador pelo roteador mais próximo (primeiro salto).

8. Quais são os valores dos campos Identificação e TTL?

9. Será que esses valores permanecem inalterados para todas as respostas ICMP - TTL excedido enviadas para o seu computador pelo roteador mais próximo (primeiro salto)?

Por quê?

Fragmentação

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

10. Encontre a primeira mensagem ICMP Echo Request que foi enviada por seu computador após você ter alterado o tamanho do pacote em *pingplotter* para 2000. A mensagem foi fragmentada em mais de um datagrama IP? [Nota: se você não encontrar um pacote que foi fragmentado, você deve baixar o arquivo zip <http://gaia.cs.umass.edu/ethereal-labs/ethereal-traces.zip> e extrair o rastreamento ip-ethereal-trace-1. Se o seu

computador tem uma interface Ethernet, um pacote tamanho de 2000 deve causar fragmentation.^{3]}

11. Imprima o primeiro fragmento do datagrama IP fragmentado. Quais são as informações no cabeçalho do IP que indicam que o datagrama foi fragmentado?

Quais são as informações no cabeçalho do IP que indicam se este é o primeiro fragmento, um fragmento intermediário ou o último fragmento?

Qual o tamanho desse datagrama IP?

12. Imprima o segundo fragmento do datagrama IP fragmentado. Quais são as informações no cabeçalho do IP que indicam que esse não é o primeiro fragmento do datagrama?

Existem mais fragmentos?

Como você pode explicar?

13. Que campos se alteram no cabeçalho do IP entre o primeiro e segundo fragmento?

Agora, localize a primeira mensagem ICMP Echo Request que foi enviado por seu computador depois que você mudou o tamanho do pacote em pingplotter para 3500.

14. Como muitos fragmentos foram criados a partir do datagrama original?

15. Quais campos mudaram no cabeçalho IP entre os fragmentos?

³ Os pacotes no arquivo zip [ip-ethereal-trace-1](http://qaia.cs.umass.edu/ethereal-labs/etherealtraces) rastreado s em <http://qaia.cs.umass.edu/ethereal-labs/etherealtraces> são todos menores que 1500 bytes. Isso ocorre porque o computador no qual o trace foi recolhida tem uma Placa Ethernet, que limita o tamanho dos pacotes IP ao máximo de 1500 bytes (40 bytes do cabeçalho TCP / IP e 1460 bytes de dados na carga útil do protocolo da camada superior). Este valor de 1500 bytes é o padrão de comprimento máximo permitido pela Ethernet. Se o seu trace indicar um datagrama maior que 1500 bytes, e o seu computador está usando uma conexão Ethernet, então Ethereal está relatando o comprimento do datagrama IP errado, ou provavelmente mostrando apenas uma grande datagrama IP ao invés de vários pequenos datagramas .. Esta inconsistência no relato de comprimentos é devido à interação entre o driver Ethernet e o software Ethereal. Recomendamos que se você tiver essa incoerência, executar este laboratório utilizando o arquivo de rastreamento ip-ethereal-trace-1.