## Ethereal Lab: TCP



down Approach Featuring the Internet, 3<sup>rd</sup> edition.

Version: 1.0 © 2005 J.F. Kurose, K.W. Ross. All Rights Reserved

Neste laboratório, vamos investigar o comportamento do TCP em detalhes. Faremos isso através da análise de um trace de segmentos TCP enviados e recebidos na transferência de um arquivo de 150KB (contendo o texto de Alice no país das maravilhas, de Lewis Carrol) do seu computador para um servidor remoto. Vamos estudar no TCP a utilização da seqüência e números de confirmação para proporcionar a transferência de dados confiável; vamos ver o algoritmo de controle de congestionamento TCP em ação – partida lenta e como evitar o congestionamento; e veremos o mecanismo de controle fluxo do receptor TCP. Também vamos considerar brevemente a configuração da conexão TCP e investigar o desempenho (throughput e RTT – Round-trip time) da conexão entre seu computador e o servidor.

Antes de iniciar este laboratório, você provavelmente vai querer rever as seções 3.5 e 3.7 na text.<sup>1</sup>

## 1. Capturando uma transferência TCP em massa de seu computador para um computador servidor remoto

Antes de começar nossa exploração do TCP, vamos precisar usar o Ethereal para obter um arquivo para transferência do seu computador para um servidor remoto. Você vai fazê-lo acessando uma página da Web que permitirá que você digite o nome de um arquivo armazenado em seu computador (que contém o texto ASCII de Alice no País das Maravilhas), e depois transferir o arquivo para um servidor Web utilizando o método POST HTTP (ver secção 2.2.3 no texto). Utilizaremos o método POST em vez do método GET para transferir um grande quantidade de dados do seu computador para outro computador. É claro, vamos estar executando o Ethereal durante esse tempo para obter o rastreamento dos segmentos TCP enviados e recebidos.

<sup>1</sup> Todas as referências ao texto neste laboratório são apresentadas no livro Redes de Computadores e a Internet: Uma Nova Abordagem - 3 ª edição

Faça o seguinte:

- Inicie o seu browser web. Ir a <u>http://gaia.cs.umass.edu/ethereal-labs/alice.txt</u> e recuperar uma cópia ASCII de Alice no País das Maravilhas. Armazenar esse arquivo em algum lugar no seu computador.
- Em seguida vá para <u>http://gaia.cs.umass.edu/ethereal-labs/TCP-ethereal-file1.html</u>.
- Você deverá ver uma tela que se parece com:

🕅 Upload page for TCP Ethereal Lab - Netscape		
Ele Edit View <u>G</u> o <u>B</u> ookmarks Iools <u>W</u> indow <u>H</u> elp		
	Search	
🚬 🖉 🖼 Mail 🐔 Home 😱 Radio 🕅 Netscape 🔍 Search 🛱 Bookmarks		
Upload page for TCP Ethereal Lab Computer Networking: A Top Down Approach Featuring the Internet, 3rd edition Copyright 2004 J.F. Kurose and K.W. Ross, All Rights Reserved		
If you have followed the instructions for the TCP Ethereal Lab, you have <i>already</i> downloaded an ASCII copy of Alice and Wonderland from <a href="http://gaia.cs.umass.edu/ethereal-labs/alice.bd">http://gaia.cs.umass.edu/ethereal-labs/alice.bd</a> and you also <i>already</i> have the Ethereal packet sniffer running and capturing packets on your computer.		
Click on the Browse button below to select the directory/file name for the copy of alice.bt that is stored on yo	our computer.	
Browse		
Once you have selected the file, click on the "Upload alice.bt file" button below. This will cause your browser to send a copy of alice.bt over an HTTP connection (using TCP) to the web server at gaia.cs.umass.edu. After clicking on the button, wait until a short message is displayed indicating the the upload is complete. Then stop your Ethereal packet sniffer - you're ready to begin analyzing the TCP transfer of alice.bt from your computer to gaia.cs.umass.edu!!		
Upload alice:txt file		
🕲 🖂 🔏 💁 🗋 Document: Done (0.063 secs)	-11	

- Use o botão Browse (Procurar) para introduzir o nome do arquivo (nome completo do caminho) contendo Alice no País das Maravilhas (ou fazê-lo manualmente) em seu computador. Ainda não pressione o botão "Upload alice.txt file".
- Agora inicie Ethereal e comece a captura de pacotes (Capture-> Interface -> Start) e pressione OK na tela de Opções de Captura de Pacotes Ethereal (não vai ser necessário selecionar qualquer opção).
- Regressando ao seu navegador, pressione o botão "Upload alice.txt arquivo" para fazer o upload do arquivo para o servidor gaia.cs.umass.edu. Uma vez que o arquivo foi carregado, uma curta mensagem de parabéns será exibida na janela do browser.
- Pare a captura de pacotes do Ethereal. Sua tela Ethereal deve ser semelhante a mostrada abaixo.

🙆 lab3-1-trace - Ethereal			
Elle Edit View Go Capture Analyze Statistics Help			
Elter: Science Apply			
No Time Source Destination	Protocol Info		
1 0.000000 192.168.1.102 128.119.245.12	TCP 1161 > http [SYN] Seq=232129012 Ack=0 Win=16384 Len=0 MSS=1460		
2 0.023172 128.119.245.12 192.168.1.102 3 0.023265 192.168.1.102 128.119.245.12	TCP NTTD > 1161 [SYN, ACK] Seq=883061785 ACK=232129013 W1N=5840 Len= TCP 1161 > http [ACK] Seq=232129013 Ack=883061786 Win=17520 Len=0		
4 0.026477 192.168.1.102 128.119.245.12	HTTP POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1		
5 0.041737 192.168.1.102 128.119.245.12	HTTP Continuation		
6 0.053937 128.119.245.12 192.168.1.102	TCP http > 1161 [ACK] Seq=883061786 Ack=232129578 Win=6780 Len=0		
	HILP COntinuation		
9 0.077294 128.119.245.12 192.168.1.102	TCP bttp > 1161 [ACK] Seg=883061786 Ack=232131038 win=8760 Len=0		
10 0.077405 192.168.1.102 128.119.245.12	HTTP Continuation		
11 0.078157 192.168.1.102 128.119.245.12	HTTP Continuation		
12 0.124085 128.119.245.12 192.168.1.102	TCP http > 1161 [ACK] seq=883061786 Ack=232132498 win=11680 Len=0		
13 0.124185 192.168.1.102 128.119.245.12	HTTP Continuation		
	TCP http > 1161 [ACK] Seq=883061/86 ACK=232133958 W1n=14600 Len=0		
	TCP http > 1161 [ACK] Seq=883001780 ACK=232133418 Win=17320 Len=0		
17 0 304807 128 119 245 12 192 168 1 102	TCP http > 1161 [ACK] Seq=883061786 Ack=232138075 Win=23360 Len=0		
18 0.305040 192.168.1.102 128.119.245.12	HTTP Continuation		
19 0.305813 192.168.1.102 128.119.245.12	HTTP Continuation		
20 0.306692 192.168.1.102 128.119.245.12	HTTP Continuation		
21 0.307571 192.168.1.102 128.119.245.12	HTTP Continuation		
22 0.308699 192.168.1.102 128.119.245.12	HTTP Continuation		
	HTTP Continuation		
	TCP N(LP > 1161 [ACK] Seq=883061/86 ACK=232139485 W(n=26280 Len=0		
	TCP http > 1161 [ACK] Seq=883061786 Ack=232140943 Win=32120 Len=0		
27 0.500029 128.119.245.12 192.168.1.102	TCP http > 1161 [ACK] Seq=883061786 Ack=232143865 win=35040 Len=0		
28 0.545052 128.119.245.12 192.168.1.102	TCP http > 1161 [ACK] Seg=883061786 Ack=232145325 win=37960 Len=0		
29 0.576417 128.119.245.12 192.168.1.102	TCP http > 1161 [ACK] Seq=883061786 Ack=232146217 Win=37960 Len=0		
30 0.576671 192.168.1.102 128.119.245.12	HTTP Continuation		
Askerul adament sumbana 993061796			
Acknowledgement number: 883061/86			
N Flage: 0x0018 (DEH ACK)			
A Pridus, VAUULO (PDR. ACK)			
10000 00 06 25 da at 73 00 20 e0 8a 70 1a 08 00 45 00	%SpE.		
0020 f5 0c 04 89 00 50 0d d6 01 f5 34 a2 74 1a 50 18	P4.t.P.		
0030 44 70 1f bd 00 00 50 4f 53 54 20 2f 65 74 68 65	DpPO ST /ethe		
0040 72 65 61 6c 2d 6c 61 62 73 2f 6c 61 62 33 2d 31	real-lab s/lab3-1		
T0050 24 (2 65 70 66 70 26 69 74 64 20 49 54 54 50 2F	PODD(D TH HTTD/		
Therefore a destriction of the state of the			

Se você não conseguir executar o Ethereal numa rede conectada, você pode baixar um trace que foi capturado pelo autor quando seguia os passos acima em seus experimentos. Você pode muito bem baixar esse trace, mesmo que você tenha capturado seu próprio rastreamento, e usá-lo como opção ao seu próprio rastreamento, quando você for explorar as perguntas abaixo.

## 2. Uma primeira visão do o trace capturado

Antes de analisar o comportamento da conexão TCP em detalhes, vamos dar uma olhada, em alto nível, no trace.

 Primeiro, filtrar os pacotes exibidos na janela Ethereal, digitando "tcp" (em letras minúsculas, sem aspas, e não se esqueçer de pressionar APPLY) na janela de especificação do filtro na parte superior da tela do Ethereal.

O que você deve ver é uma série de mensagens TCP e HTTP entre seu computador e gaia.cs.umass.edu. Você deverá ver o three-way handshake inicial contendo mensagens com o bit SYN setado.

<sup>&</sup>lt;sup>2</sup> Baixe o arquivo zip de http://gaia.cs.umass.edu/ethereal-labs/ethereal-traces.zip e extraia o arquivo tcpethereal-trace-1. Os traces desse arquivo zip foram coletados através da execução Ethereal em um dos computadores do autor, enquanto realizava os passos indicados no laboratório Ethereal. Depois de ter baixado o trace, você pode carregá-lo no Ethereal e exibir o rastreamento usando a opção Arquivo/Abrir no menu suspenso, e em seguida, selecionando o arquivo de rastreamento tcp-ethereal-trace-1.

Você deverá ver uma mensagem HTTP POST e uma série de mensagens de "Continuação HTTP" (TCP segment of a reassembled PDU) enviadas do seu computador para o servidor gaia.cs.umass.edu. Lembre-se da nossa discussão no laboratório anterior Ethereal HTTP, que existe uma Mensagem de continuação HTTP – essa é a forma do Ethereal indicar que há vários segmentos TCP sendo usados para levar uma única mensagem HTTP. Você também deve ver segmentos TCP ACK sendo retornados de gaia.cs.umass.edu para o seu computador.

Responder às seguintes perguntas, abrindo o arquivo de pacotes capturados do Ethereal tcp-ethereal-trace-1 em <u>http://gaia.cs.umass.edu/ethereal-labs/ethereal-traces.zip</u> (que você pode baixar e abrir no Ethereal, conforme nota <sup>2</sup>). Sempre que possível, ao responder uma pergunta, imprimir os pacote(s) dentro do trace que você usou para responder. Para imprimir um pacote, use File-> Imprimir, marque "*selected packet only* ", "*Packet summary line*", e selecione uma quantidade mínima de detalhes do pacote que você precisará para responder a questão.

- 1. Qual é o endereço IP e número da porta TCP usados pelo computador do cliente (fonte) que está transferindo o arquivo para gaia.cs.umass.edu? Para responder a esta pergunta, provavelmente é mais fácil selecionar uma mensagem HTTP e explorar os detalhes do pacote TCP usado para transmitir a mensagem HTTP, usando os detalhes do pacote selecionado na janela de cabeçalho "(veja a Figura 2 na" Introdução ao Ethereal Lab "se você está incerto sobre as janelas Ethereal.
- 2. Qual é o endereço IP de gaia.cs.umass.edu? E o número da porta de envio e de recebimento de segmentos TCP para esta conexão?

Se você foi capaz de criar seu próprio rastreamento (trace), responda a seguinte pergunta:

3. Qual é o endereço IP e número da porta TCP usada pelo seu computador cliente (fonte) para transferir o arquivo para gaia.cs.umass.edu?

Já que este laboratório é sobre o TCP, em vez de HTTP, vamos mudar na *"janela de pacotes capturados"* do Ethereal para que sejam mostradas informações sobre os segmentos TCP que contém as Mensagens HTTP, em vez de HTTP. Para isso, selecione *Analize-> Enablead Protocols*. Em seguida, desmarque a caixa de HTTP e selecione OK. Você deverá ver uma janela do Ethereal parecida com:

🕝 lab3-1-trace - Ethereal		
Elle Edit View Go Capture Analyze Statistics Help		
	⊻ [ • • • • • • • • • • • • • • • • • •	
Eilter: tcp	Expression Suclear V Apply	
No.     Time     Source     Destination       1     0.000000     192.168.1.102     128.119.245.12       2     0.023172     128.119.245.12     128.119.245.12       3     0.023255     192.168.1.102     128.119.245.12       4     0.026477     192.168.1.102     128.119.245.12       5     0.041737     192.168.1.102     128.119.245.12       6     0.053937     128.119.245.12     192.168.1.102       7     0.054026     192.168.1.102     128.119.245.12       8     0.054691     192.168.1.102     128.119.245.12	Protocol     Info	
9     0.077294     128.119.245.12     192.168.1.102       10     0.077405     192.168.1.102     128.119.245.12       11     0.078157     192.168.1.102     128.119.245.12       12     0.124085     128.119.245.12     192.168.1.102       13     0.124185     192.168.1.102     128.119.245.12       14     0.169118     128.119.245.12     192.168.1.102       15     0.217299     128.119.245.12     192.168.1.102       16     0.267802     128.119.245.12     192.168.1.102       17     0.304807     128.119.245.12     192.168.1.102       18     0.305040     192.168.1.102     128.119.245.12       19     .305813     192.168.1.102     128.119.245.12       19     0.305813     192.168.1.102     128.119.245.12       20     0.306592     192.168.1.102     128.119.245.12       21     0.307571     192.168.1.102     128.119.245.12       22     0.308699     192.168.1.102     128.119.245.12       22     0.306591     192.168.1.102     128.119.245.12 <td><math display="block">\begin{array}{llllllllllllllllllllllllllllllllllll</math></td>	$\begin{array}{llllllllllllllllllllllllllllllllllll$	
23.0.309553   192.168.1.102   128.119.245.12   TCP   1161 > http://PSH. ACK1 Sep=232145325 Ack=883061786 win=17520 Len     > Frame 7 (1514 bytes on wire, 1514 bytes captured)   >   b   thernet II, Src: 00:20:e0:8a:70:1a, Dst: 00:06:25:da:af:73     > Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 128.119.245.12 (128.119.245.12)   >     > Transmission Control Protocol, Src Port: 1161 (1161), Dst Port: http (80), Seq: 232131038, Ack: 883061786, Len: 1460     Source port: 1161 (1161)     Destination port: http (80)     Sequence number: 232131038     [Next sequence number: 232132498]     Acknowledgement number: 883061786		
Header length: 20 bytes > Flags: 0x0010 (ACK) 0000 00 00 10 40 40 10 10 10 10 10 10 10 10 10 10 10 10 10		
DUDU     UU     U		

Isso é o que estamos procurando - uma série de segmentos TCP enviados entre o seu computador e gaia.cs.umass.edu. Vamos usar o traço de pacotes que você capturou (e / ou o traço de pacotes *tcp-ethereal-trace-1* em <u>http://gaia.cs.umass.edu/ethereal-labs/ethereal-traces.zip</u> ; ver nota <sup>2</sup>) para estudar o comportamento do TCP neste laboratório.

3. O Básico do TCP

Responder às seguintes perguntas para os segmentos TCP:

4. Qual é o número de seqüência do segmento TCP SYN que é usado para iniciar a conexão TCP entre o computador do cliente e gaia.cs.umass.edu?

O que é no segmento que identifica o segmento como um segmento SYN?

5. Qual é o número de seqüência do segmento SYNACK enviado por gaia.cs.umass.edu para o computador cliente em resposta ao SYN?

Qual é o valor do campo ACK no segmento SYNACK? Como gaia.cs.umass.edu determinou esse valor

O que é no segmento que identifica o segmento como um Segmento SYNACK?

6. Qual é o número de següência do segmento TCP que contém o comando HTTP POST? Note que, a fim de encontrar o comando POST, você precisará abrir o campo de conteúdo do pacote na parte inferior da janela do Ethereal, procurando um segmento com um "POST" dentro de seu campo de dados.

7. Considere o segmento TCP que contém o POST HTTP como o primeiro segmento da conexão TCP. Quais são os números de següência dos seis primeiros segmentos da conexão TCP (incluindo o segmento que contém o POST HTTP)? Em que tempo foi cada segmento enviado?

Quando ocorreu o ACK para cada segmento recebido?

Dada a diferença entre quando cada segmento TCP foi enviado, e quando sua confirmação foi recebida, gual é o valor RTT para cada um dos seis segmentos?

Qual é o valor do RTT estimado (ver página 237 no texto) após a recebimento de cada ACK? Suponha que o valor do RTT estimado é igual ao RTT medido para o primeiro segmento e em seguida calcule o RTT estimado usando a equação na página 237 para todos os segmentos subseqüentes.

Nota: Ethereal tem um recurso interessante que permite traçar o RTT para cada um dos segmentos TCP enviados. Selecione um segmento TCP na listagem da " janela de captura dos pacotes "que está sendo enviado a partir do cliente para o servidor gaia.cs.umass.edu. Em seguida, selecione: Statistics-> TCP Stream Graph-> Round Trip Time Graph.

8. Qual é o comprimento de cada um dos seis primeiros segmentos TCP?<sup>3</sup>

9. Qual é a quantidade mínima de espaço de buffer disponível anunciado pelos receptores no rastreamento inteiro?

Será que o espaço de buffer no receptor regula a tansmissão do remetente?

10. Há algum segmentos retransmitidos no arguivo de rastreamento?

O que o você verificou no traçe para responder a esta pergunta?

11. Qual a quantidade de dados que o receptor normalmente reconhece em um ACK?

Você pode identificar casos em que o receptor está reconhecendo todos os demais segmentos recebidos (ver Tabela 3.2 na página 245 no texto).

12. Qual é a taxa de transferência (throughput - bytes transferidos por unidade de tempo) para a conexão TCP?

Explique como você calculou este valor.

## 4. Controle de congestionamento TCP em ação

Vamos agora examinar a quantidade de dados enviados por unidade de tempo do cliente para o servidor.

Ao invés do tedioso trabalho de calcular isso a partir dos dados brutos na janela Ethereal, vamos utilizar a facilidade gráfica do Ethereal para TCP - *Time-Sequence-Graph (Stevens)* – para plotar os dados.

 Selecione um segmento TCP na janela "*lista de pacotes capturados*," do Ethereal. Em seguida, selecione o menu: *Statistics-> TCP Stream Graph-> Time-Sequence-Graph (Stevens)*. Você deverá ver uma tela que se parece com o seguinte gráfico, que foi criado a partir dos pacotes capturados no rastreamento de pacotes *tcp-ethereal-trace-1* em <u>http://gaia.cs.umass.edu/ethereallabs/ethereal-traces.zip</u> (ver nota 2):

<sup>&</sup>lt;sup>3</sup> Os segmentos TCP no arquivo de rastreamento tcp-ethereal-trace-1 estão todos com menos de 1460 bytes. Isso ocorre porque o computador em que o trace foi recolhida tem uma placa Ethernet que limita o comprimento máximo do pacote IP em 1500 bytes (40 bytes dos dados do cabeçalho do TCP / IP e 1460 bytes de payload do segmento TCP). Este valor de 1500 bytes é o comprimento máximo permitido pelo padrão Ethernet. Se o seu trace indicar segmento TCP maior que 1500 bytes, e seu computador estiver usando uma conexão Ethernet, então Ethereal estará relatando o comprimento do segmento TCP, mas provavelmente também mostra apenas um segmento TCP grande, em vez de várias segmentos menores. Seu computador, na verdade, provavelmente, estará enviando vários segmentos menores, como indicado pela ACKs que recebe. Esta inconsistência em comprimentos de segmentos é devido à interação entre a driver Ethernet e o software Ethereal. Recomendamos que se você tiver essa inconsistência, executar este laboratório usando o arquivo de rastreamento fornecido.



Aqui, cada ponto representa um segmento TCP enviado, plotando o número de seqüência do segmento em relação ao tempo em que foi enviado. Note-se que um conjunto de pontos empilhados acima de si representa uma série de pacotes que foram enviados de volta ao remetente.

Responder às seguintes perguntas para os segmentos TCP do trace de pacotes tcp-etherealtrace-1 em <u>http://gaia.cs.umass.edu/ethereal-labs/ethereal-traces.zip</u>.

13. Use a ferramenta *Time-Sequence Graph (Stevens)* para ver, em lote, a seqüência de números de segmentos versus tempo enviados do cliente para o servidor gaia.cs.umass.edu. Você pode identificar onde a fase de partida lenta do TCP começa e termina, e onde evitar o congestionamento? Note que num trace do"mundo real", nem tudo é tão limpo e arrumado como na Figura 3.51 (também note que os rótulos do eixo y para a plotagem *Time-Sequence-Graph (Stevens)* e a ferramenta de Figura 3.51 são diferentes).

14. Comente sobre as formas em que os dados medidos diferem do comportamento idealizado da TCP que foi estudado no texto.

15. Responda cada uma das duas perguntas acima para o rastreamento capturado quando você transferiu um arquivo de seu computador para gaia.cs.umass.edu.