实验 6 分析 TCP 特性

1. 实验目的

1)深入理解 TCP 的如下重要机制的工作原理：利用序号和确认号实现可靠数据传输，TCP 拥塞控制算法(慢启动和拥塞避免)，接收方通告的流量控制。

2)掌握用 Wireshark 分析 TCP 踪迹文件的技能。

2. 实验环境

1)运行 Windows 2008 Server/Windows XP/Windows 7 操作系统的 PC 一台。

2)PC 具有以太网卡一块，通过双绞线与校园网相连；或者具有适合的踪迹文件。

3)每台 PC 运行程序协议分析仪 Wireshark。

3. 实验步骤

1)俘获本机与远程服务器的 TCP 踪迹文件

在开始研究 TCP 工作机制之前，需要使用 Wireshark 来俘获从本机到远程服务器之间的 TCP 踪迹文件。为此，可以从本机浏览器打开某 Web 网站上的网页，用 HTTP 协议下载包括文本文件在内的对象。与此同时，在本机上运行 Wireshark 俘获本机收发的 TCP 报文段并存入踪迹文件 tcp.cap 中。为了便于比较，可以从因特网上下载现成的踪迹文件进行分析，相关 URL 是 http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip。

2)熟悉 TCP 踪迹文件

打开 tcp-ethereal-trace-1.pcap 文件，可以看到俘获机器与 gaia.cs.umass.edu 的 Web 服务器之间交互的 TCP 和 HTPP 报文序列(参见图 40)。

选择一个报文，观察其各层次协议间的包含关系。观察 HTTP 与 TCP 之间关系是如何体现的？从俘获报文列表窗口右侧，可以发现发起三次握手的 SYN 报文，也可以发现一系列交互的 HTTP 报文。

回答下列问题：

(1) 与 gaia.cs.umass.edu 传输文件的源主机所使用 IP 地址和端口号是什么？

(2) gaia.cs.umass.edu 服务器所使用 IP 地址和端口号是什么？

(3) 前 6 个 TCP 报文段的每个长度各为多长？

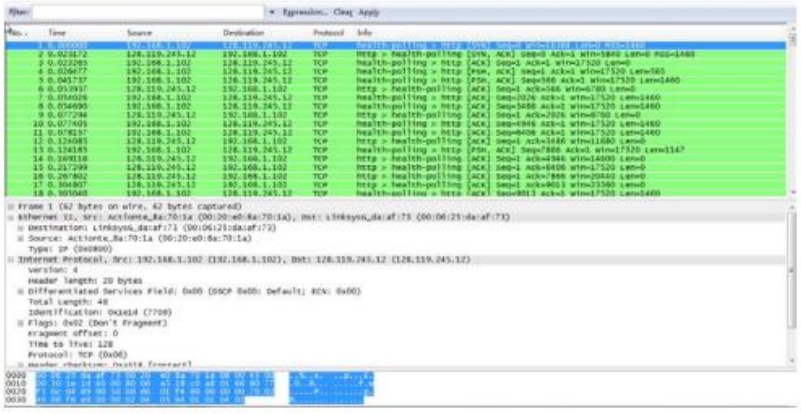

图 40 分析 TCP 踪迹文件

3)分析 TCP 序列/应答编号和流量控制

为分析 TCP 序号和确认号，可以从分组列表中观察，也可以点击“Statitics/Flow Graph”，出现如图 41 所示的本机与服务器之间的图分析结果。

观察该图，回答下列问题：

(4) 用于发起与服务器 TCP 连接的 TCP SYN 报文段的序号是多少？在该报文段中标识其为 SYN 报文段的标志是什么？

(5) 服务器应答上述 TCP SYN 报文段的 SYN ACK 报文段的序号是什么？在该 SYN ACK 报文段的 ACK 应答字段中的值是多少？服务器是怎样确定这个 ACK 值的？在该报文段中标识其作为 SYN ACK 报文段的标志是什么？

(6) 接收方的 ACK 报文应答的数据一般为多长？如何确定接收方是对哪个报文段进行应答的？

(7) 观察 TCP SYN 报文段达到的时间以及 SYN ACK 报文段回复的时间。它们与后继请求和应答报文对之间的时间差一样吗？

(8) 接收方通常的可用缓存的量是一样大的吗？最小量是多少？出现了为抑制发送方而减少接收缓存空间的情况吗？

(9) 在踪迹文件中有重传报文段吗？如何检查是否出现了这种情况？

(10) 对该 TCP 连接，吞吐量是多大？解释计算所使用的方法。

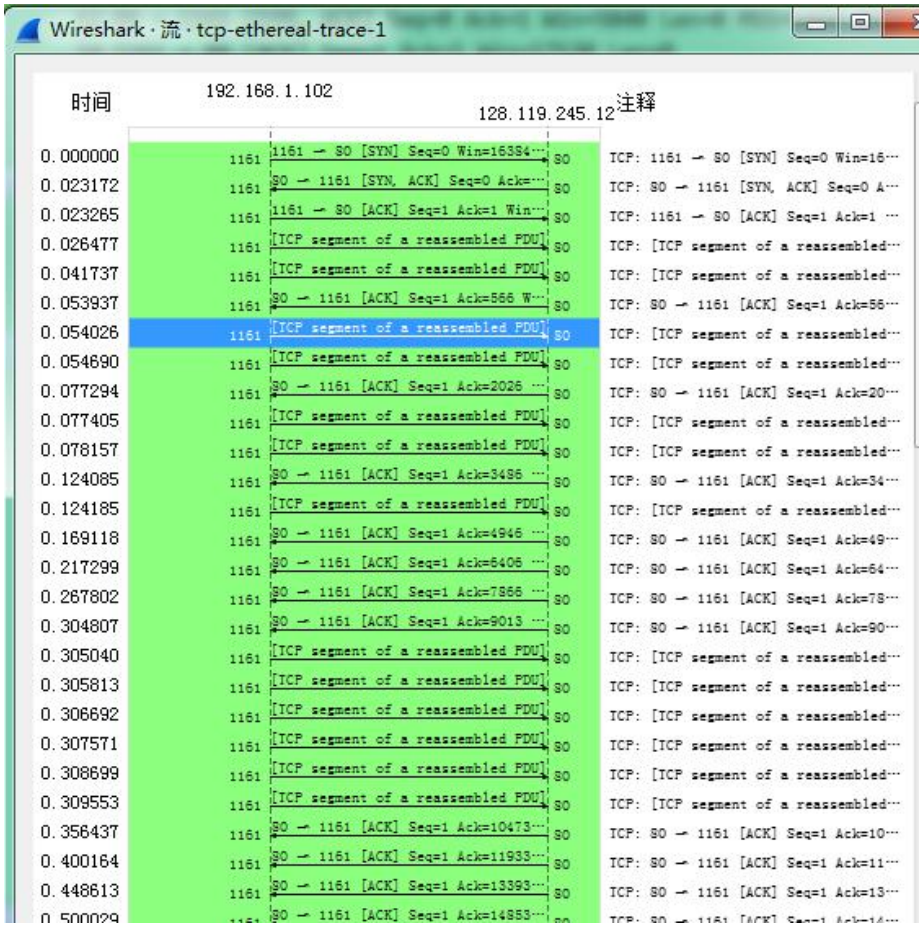

图 41 TCP 流图分析

4)分析应用层内容

本实验中的应用层是 HTTP，该协议的可靠传输基于 TCP 得到的。通过分析 TCP 报文序列可以得到 HTTP 传输的内容。为此，点击 TCP 三次握手之间的第 4 号报文，发现它是一条从本机向服务器发送 HTTP POST 命令的报文，请求 Web 服务器发送特定的页面对象。对于后继报文，也可以发现以 ASCII 明文发送的应用层内容。

对于分析应用层内容，Wireshark 提供了一个很好的工具。点击“Analyze/Follow TCP Stream”，可打开如图 42 所示界面，显示了该 TCP 流的应用层相关信息。

(11) 分析一下 HTTP 传输的是大约什么内容？

(12) 如果 Web 页面传输的是图片或视频对象，会出现什么情况？

图 42　Follow TCP Stream 界面

5)分析 TCP 拥塞控制

前面实验已经为你用 Wireshark 分析报文序列打下了有用的基础。应当说它是一件枯燥(尽管十分有用)的工作，下面使用 Wireshark 提供的分析大量 TCP 报文时的图形工具。

点击“Statistics/TCP Stream Graph/Throughput Gragh)”，得到如图 43 所示的界面。图中的每个点表示在某时刻该 TCP 连接的吞吐量。

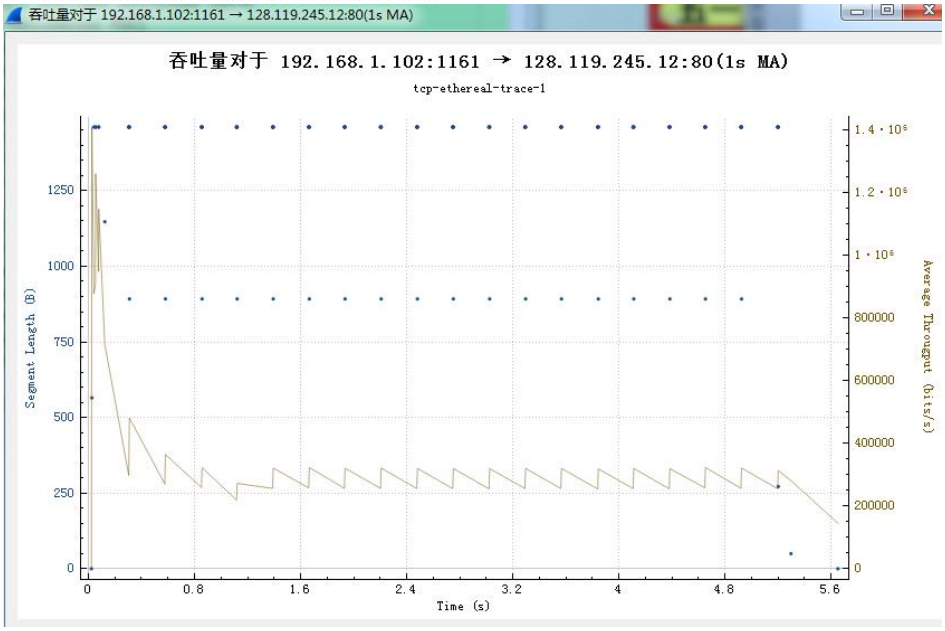

图 43　分析 TCP 序列吞吐量的时序图

(13) 根据图 43 分析的吞吐量分布曲线，解释哪部分对应的是 TCP 慢启动阶段和拥塞避免阶段。

(14) 图示曲线是否与课文中的理论分析曲线一致？为什么？

4. 相关概念

1)传输控制协议报文段结构。TCP(Transmission Control Protocol，TCP) [RFC 793]是TCP/IP 体系中面向连接的运输层协议，它提供全双工的和可靠交付的服务。TCP 报文段结构如图 44 所示。TCP 与 UDP 最大的区别就是 TCP 是面向连接的，而 UDP 是无连接的。

2)TCP 拥塞控制算法。通常包括 3 个主要部分：(1)加性增(additive-increase)，乘性减(multiplicative-decrease)，即每发生一次丢失事件时就将当前的拥塞窗口 CongWin 值减半，每当它收到一个ACK后就把CongWin增加一个MSS(最大报文段长)。(2)慢启动(slow start)，即 TCP 发送方在初始阶段不是线性地增加其发送速率，而是以指数的速度增加，即每过一个 *RTT* 将 CongWin 值翻倍，直到发生一个丢包事件为止，此时 CongWin 将被降为一半，然后就会像上面所讲的那样线性地增长。(3)对超时事件作出反应。对于收到 3 个冗余 ACK 后，TCP 将拥塞窗口减小一半，然后线性地增长。但是超时事件发生时，TCP 发送方进入一个慢启动阶段，即它将拥塞窗口设置为 1 *MSS*，然后窗口长度以指数速度增长。拥塞窗口持续以指数速度增长，直到 CongWin 达到超时事件前窗口值的一半为止。此后，CongWin 以线性速度增长，就像收到 3 个冗余 ACK 一样动作。

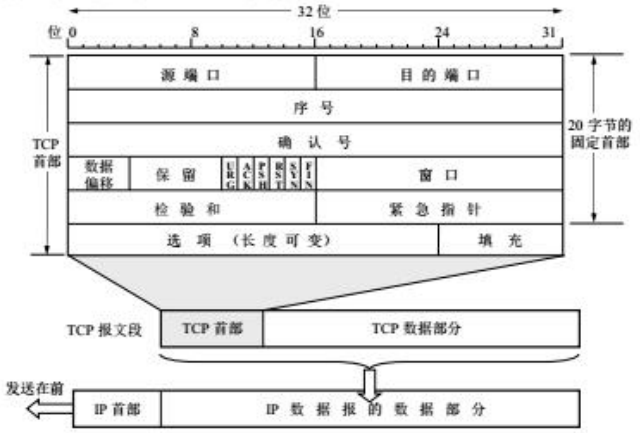

图 44　TCP 报文段结构

5. 注意事项

由于 TCP 较为复杂，在实验前应当熟悉 TCP 及其工作过程。