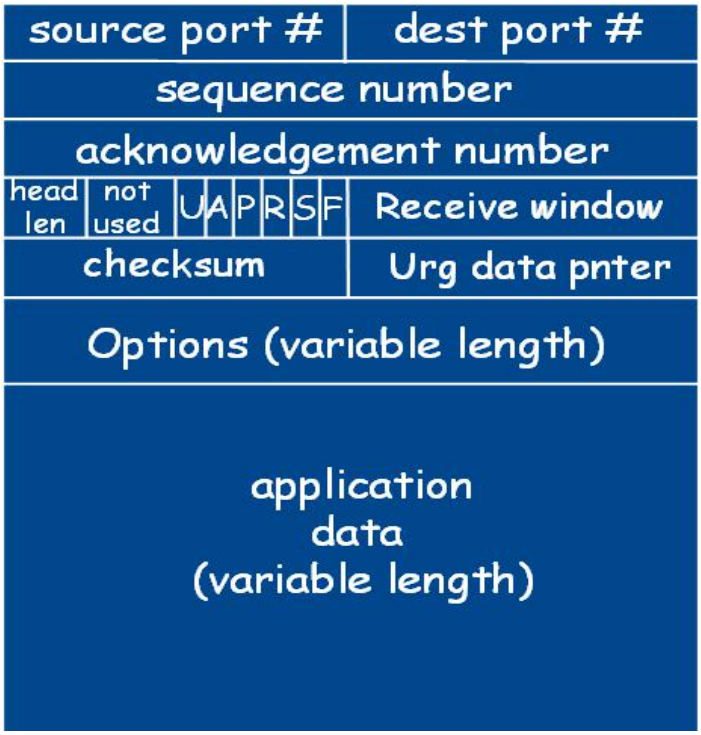
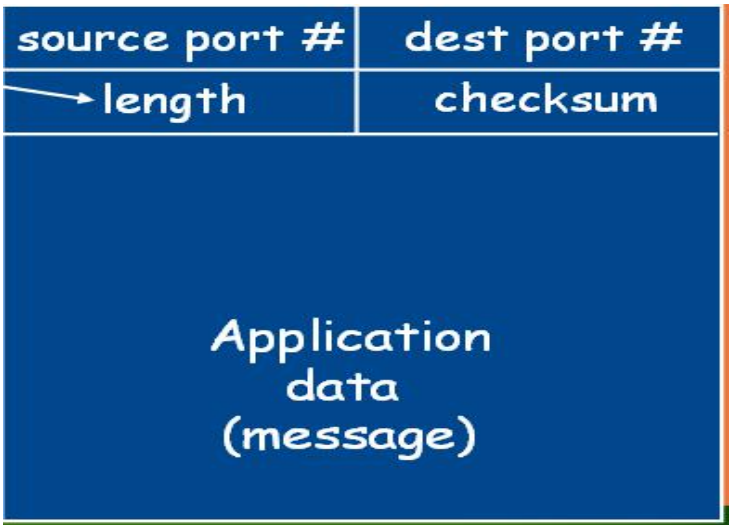
实验二：利用分组嗅探器分析传输层与网络层协议

【实验前需要学习掌握的知识】

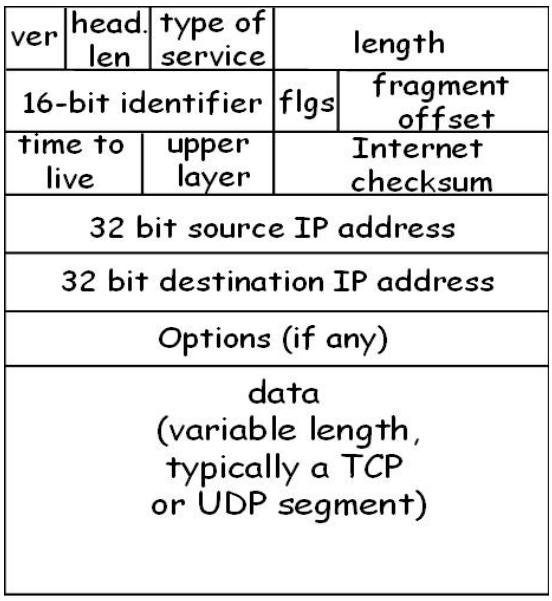
1、详细掌握 TCP 段结构。



2、详细掌握 UDP 段结构。



3、IP 数据报结构



【实验目的】

1、了解传输层 TCP/UDP 协议构造；

2、了解网络层 IP 协议构造；

【实验内容】

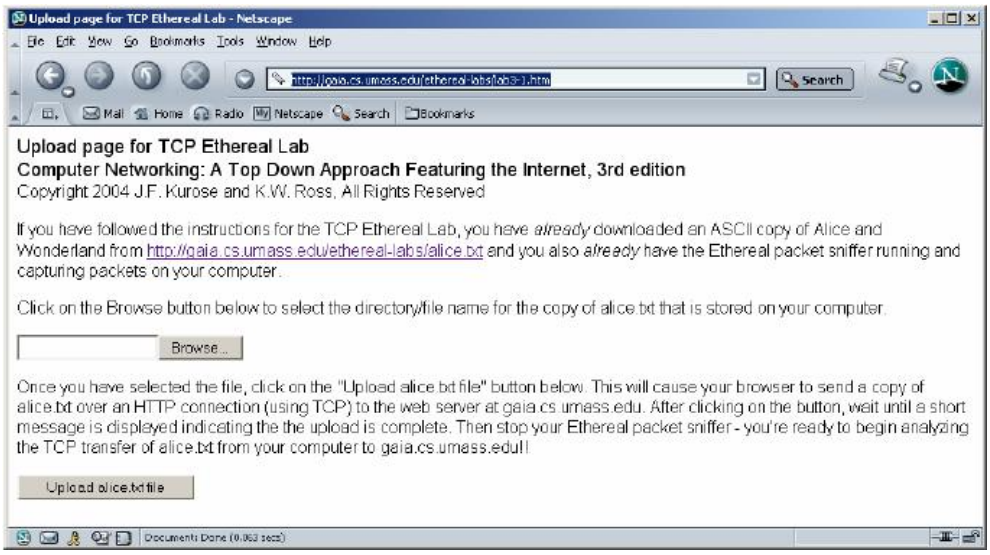
1、对传输层协议 TCP/UDP 进行捕包分析并回答问题

俘获大量的由本地主机到远程服务器的 TCP 传输

(1) 启动浏览器，打开http://gaia.cs.umass.edu/wireshark-labs/alice.txt网页，得到ALICE'S ADVENTURES IN WONDERLAND文本，将该文件保存到你的主机上。

(2)打开http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html

窗口如下所示。



在Browse按钮旁的文本框中输入保存在你的主机上的文件ALICE'S ADVENTURES IN WONDERLAND的全名（含路径），此时不要按“*Upload alice.txt file*”按钮

(3)启动Ethereal，开始分组俘获。

(4)在浏览器中，单击“*Upload alice.txt file*”按钮，将文件上传到gaia.cs.umass.edu服务器，一旦文件上传完毕，一个简短的贺词信息将显示在你的浏览器窗口中。

(5)停止俘获。

浏览追踪信息

(1)在显示筛选规则中输入“tcp”,你可以看到在你的主机和服务器之间传输的一系列的tcp 和 http 报文，你应该能看到包含 SYN 报文的三次握手。也可以看到有你的主机向服务器发送的一个 HTTP POST 报文和一系列的“http continuation”报文。

(2)根据操作回答“实验报告”中的 1-2 题。

TCP 基础

根据操作回答“实验报告”中的 3-9 题

2、对网络层协议 IP 进行捕包分析

注意分析网络层发送方和接收方 IP 地址关系，推荐采用对 tracert 命令进行捕包分析。

【实验方式】实验指导教师讲解演示，每位同学上机实验，并与指导教师讨论。

【实验地点】学院实验室。

下载共享版本 http://www.pingplotter.com/安装 pingplotter 标准版（你有一个 30 天的试用期），通过对你所喜欢的站点执行一些 traceroute 来熟悉这个工具。ICMP 回复请求消息的大小可以在 pingplotter 中设置：Edit->Options->Packet，在 packet size 字段中默认包的大小是 56 字节。pingplotter 发送一系列 TTL 值渐增的包时，Trace 时间间隔的值和间隔的个数在 pingplotter 中能够设置。按下面步骤做：

1．打开 Ethereal，开始包捕获，然后在 Ethereal 包捕获的选择屏幕上点击 OK；

2．开启 pingplotter，然后在“Address to Trace”窗口输入目的地目标的名字：

在“#of times to Trace”区域输入 3。然后选择 Edit->Options->Packet，确认在 packet size 字段的值为 56，点 OK。然后按下 Trace 按钮。

3.接下来，发送一组具有较长长度的数据包，通过 Edit->Options->Packet 在包大小区域输入值为 2000，点 OK。接着按下 Resume 按钮；

4.再发送一组具有更长长度的数据包，通过 Edit->Options->Packet 在包大小区域输入值为 3500，点 OK。接着按下 Resume 按钮；

5.然后我们停止 Ethereal tracing；

根据操作回答“实验报告”中的 10-23 题

在实验的基础上，回答以下问题：(请在实验报告中 TCP 与 IP 各 5 道题回答)

(1) 向 gaia.cs.umass.edu 服务器传送文件的客户端主机的 IP 地址和 TCP 端口号是多少？

(2) Gaia.cs.umass.edu 服务器的 IP 地址是多少？对这一连接，它用来发送和接收 TCP 报文段的端口号是多少？

(3) 客户服务器之间用于初始化 TCP 连接的 TCP SYN 报文段的序号（sequence number）是多少？在该报文段中，是用什么来标示该报文段是 SYN 报文段的？

(4) 服务器向客户端发送的 SYNACK 报文段序号是多少？该报文段中，ACKnowledgement 字段的值是多少？Gaia.cs.umass.edu 服务器是如何决定此值的？在该报文段中，是用什么来标示该报文段是 SYNACK 报文段的？

(5) 包含 HTTP POST 命令的 TCP 报文段的序号是多少？

(6) 考虑在 TCP 连接中含有 HTTP POST 并把它作为第一个片段的 TCP 片段。在 TCP 连接（包括含有 HTTP POST 的片段）中最先的六个片段的序列号是多少？每一个片段是什么时候发送的？每一个片段接收到 ACK 是什么时候？请给出每一个 TCP 片段发送和确认被收到时的间隔，即六个片段中的每一个 RTT 值是多少？当接收到每一个 ACK 时的 EstimatedRTT 值是多少？假设对于第一个片段来说，EstimatedRTT 值和标准的 RTT 值相同。

EstimatedRTT=(1-α)*EstimatedRTT+α*SampleRTT （假设α=0.125）可以知道如何计算即可

(7) 前六个 TCP 报文段的长度各是多少？

(8) 在整个跟踪过程中，接收端公示的最小的可用缓存空间是多少？限制发送端的传输以后，接收端的缓存是否仍然不够用？

(9) 在跟踪文件中是否有重传的报文段？进行判断的依据是什么？

(10)选择你的电脑所发送的第一个 ICMP 请求消息，在包详细信息窗口扩展包的 Internet 协议部分。你的电脑的 IP 地址是多少？

(11)在 IP 包头部，上层协议区域的值是多少？

(12)IP 头部有多少字节？IP 数据包的有效载荷是多少字节？解释你是怎样确定有效载荷的数量的？

(13)这个 IP 数据包被分割了吗？解释你是怎样确定这个数据包是否被分割？

接下来单击列名按 IP 源地址排序数据包，选择你的电脑发送的第一个 ICMP 请求消息，扩展显示 IP 协议的数据。

(14)在包捕获列表窗口，你能看到在第一个 ICMP 下的所有并发的 ICMP 消息吗？

(15)往同一 IP 的数据包哪些字段在改变,而且必须改变？为什么？哪些字段是保持不变的，而且必须保持不变？

(16)描述一下在 IP 数据包的 Identification 字段的值是什么样的？

接下来找到通过最近的路由器发送到你的电脑去的 ICMP 的 TTL 溢出回复的系列，回答以下问题：

(17)Identification 字段和 TTL 字段的值是多少？

(18)所有的通过最近的路由器发送到你的电脑去的 ICMP 的 TTL 溢出回复是不是值都保持不变呢？为什么？

接下去研究一下分片，先按时间顺序排序数据包，找出在 pingplotter 中把包的大小改成 2000 后，你的电脑所发送的第一个 ICMP 请求消息。回答以下问题：

(19)那个消息是否传送多于一个 IP 数据包的分片？看第一个被分割的 IP 数据包的片段,在 IP 头部有什么信息指出数据包已经被分割？在 IP 头部有什么信息指出这是否是第一个与后面片段相对的片段？这个 IP 数据包的长度是多少？

(20)看被分割的 IP 数据包的第二个片段。在 IP 头部有什么信息指出这不是第一个数据包片段？有更多的片段吗？你是怎么知道的？和上一个分片的长度加起来是 2000 吗？

(21)哪个字段在第一个和第二个片段之间的 IP 头部改变了？Identification 变了吗

再找出在 pingplotter 中把包的大小改成 3500 后，你的电脑所发送的第一个 ICMP 请求消息。回答以下问题：

(22)从原始的数据包中产生了多少片段？片偏移分别为多少？

(23)在片段之中 IP 头部哪些字段改变了？Identification 变了吗？

计算机网络与通信实验报告（二）

学　号	姓　名	班　级	报告日期
实验内容	**网络常用命令的使用**		
实验目的			
实验预备知识			
实验过程描述			
实验结果			

实验当中问题 及解决方法	1、 2、			
成绩（教师打分）	优秀	良好	及格	不及格