实验二

UDP

**实验目的**

本次实验是为了熟悉UDP传输协议。如课本的第3章中所述，UDP是一种简洁高效、不加修饰的协议。在做这个实验之前请先复习一下课本第3.3节。正因UDP简洁而芬芳，使得我们能够简短地完成这个实验。

到了这个阶段，你应该已经是一个Wireshark专家了。因此，我们不会像以前的实验那样明确地阐述每个步骤。特别是，我们将不再提供所有步骤的示例屏幕截图。

**实验步骤**

在Wireshark中启动分组捕获，然后执行一些会导致主机发送和接收多个UDP分组的操作。也有可能不需要做任何事情（除了通过Wireshark捕获分组），其它进程发送的一些UDP数据包就会出现在你的跟踪中。特别是象简单网络管理协议（SNMP–请参阅课本的第5.7节）其发送的SNMP消息嵌入在UDP内，因此你也可能会在捕获的分组中找到一些SNMP消息（以及UDP数据包）。

停止分组捕获后设置分组筛选器，以便Wireshark仅显示在主机上发送和接收的UDP分组。选择其中一个UDP分组并在详细信息窗口中展开UDP字段。

如果可能请提交分组捕获跟踪的打印输出，用于回答下面问题。并请加上注解以解释你的答案。要打印分组，请使用“文件”→“打印到文件”，选择“仅选定分组”，选择“分组摘要行”，然后选择回答问题所需的分组详细信息。

1. 从追踪中选择一个UDP分组，确定其UDP首部中有多少字段，给出这些字段的名称
2. 通过查看Wireshark捕获分组内容字段显示的信息，确定UDP首部字段的长度信息（字节单位）
3. 长度字段中的值是什么的长度? (你可以参考课本内容作答)。用捕获的UDP分组验证你的答案
4. UDP负载中可以包含的最大字节数是多少?（提示：这个问题的答案可以从上面问题2的答案来确定）
5. 最大可能的源端口号是多少?（提示：参见问题4的提示）
6. UDP的协议号是多少？分别用十六进制和十进制来表示。要回答这个问题，需要查看包含UDP报文段的IP数据报的Protocol字段（参见课本图4.13和IP首部字段的讨论）
7. 检查一对UDP分组，其中你的主机发送了第一个UDP分组，而第二个UDP分组是对第一个UDP分组的回复。（提示：为响应第一个分组而发送的第二分组，第一个分组的发送者应该是第二个分组的目的地）。描述两个分组端口号之间的关系