Week 12: UDP协议分析

一、实验目的

- 了解 UDP 协议的工作原理

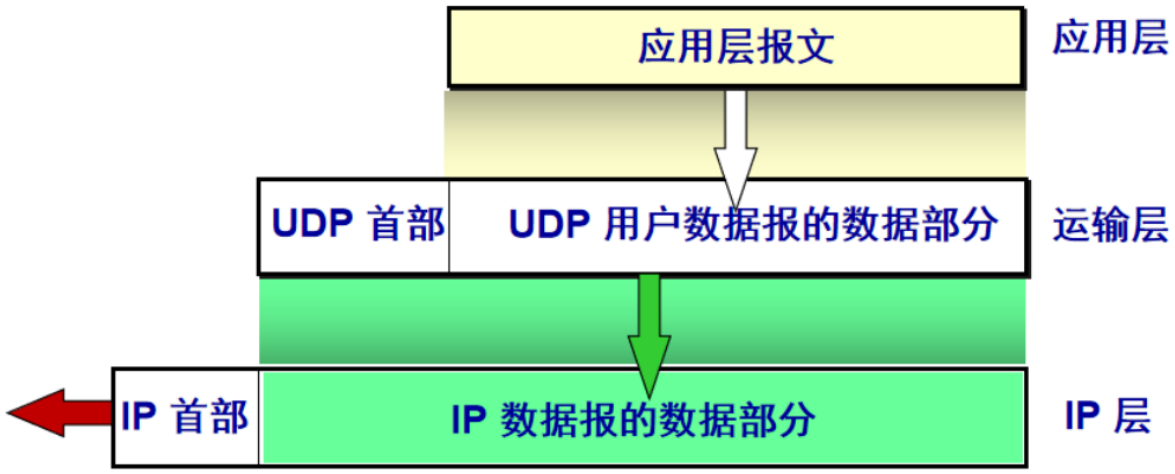
二、实验任务

- 使用Wireshark快速了解UDP协议

三、实验过程

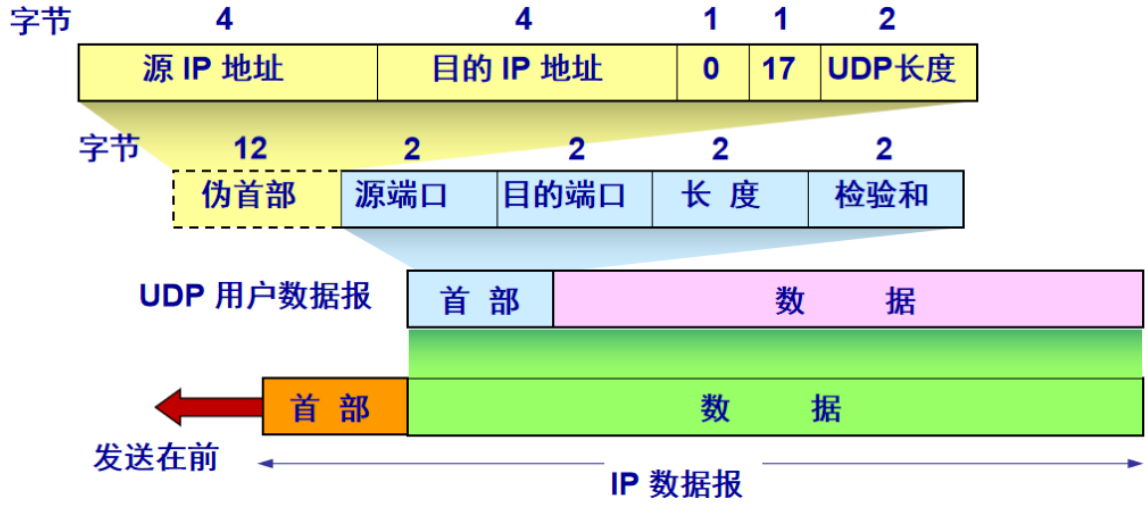
3.1 UDP 协议

用户数据报(UDP)协议是运输层提供的一种最低限度的复用/分解服务，可以在网络层和正确的用户即进程间传输数据。UDP 是一种不提供不必要服务的轻量级运输协议，除了**复用/分用**功能和简单的**差错检测**之外，几乎就是 IP 协议了，也可以说它仅提供**最小**服务。UDP 是**无连接**的，因此在两个进程通信前**没有握手过程**。UDP 协议提供一种不可靠数据传输服务，也就是说，当一个进程讲一个报文发送进 UDP 套接字时，UDP 协议**并不保证**该报文将到达接收进程。也正是由于 UDP 不修复错误，因此到达接收进程的报文也可能是乱序到达的。UDP 是面向报文的，这是因为 UDP 并不会对应用层传递下来的报文进行任何处理，对于报文的边界信息都会保存，向下交付时交付的是完整报文。



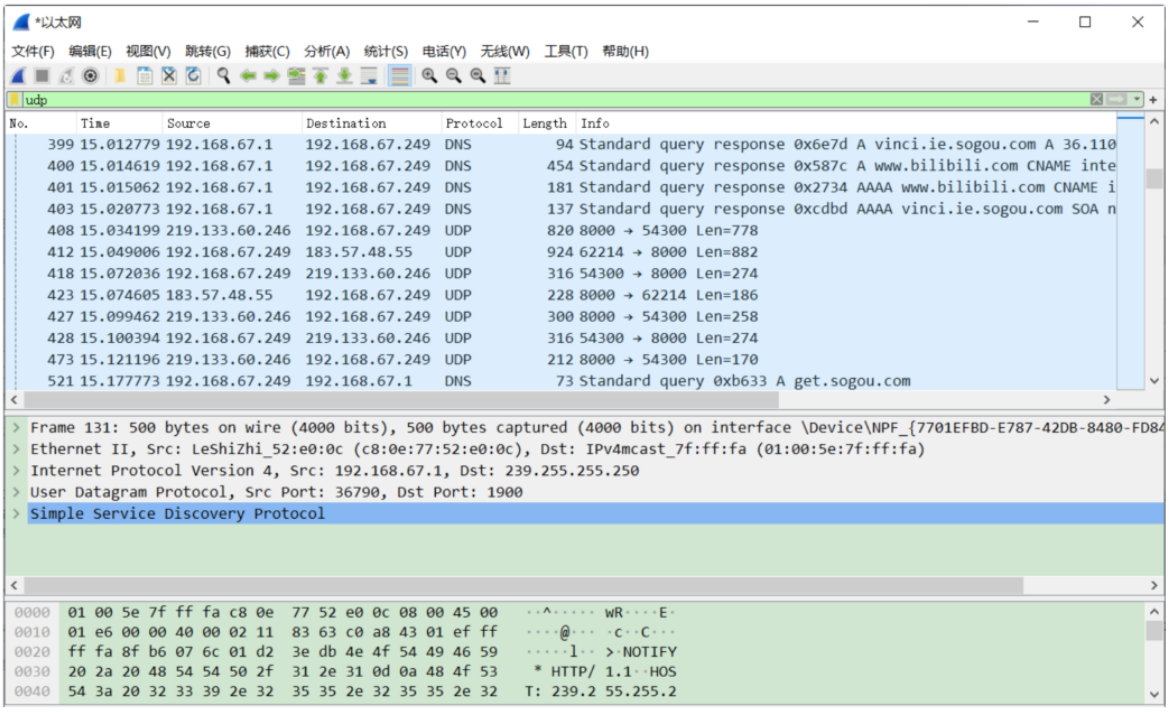
3.2 UDP 报文结构

UDP 首部只有 4 个字段：源端口号、目的端口号、长度、校验和，其中每个字段由 2 个字节组成。



3.3 实验操作

1. 在 Wireshark 中捕获数据包，然后执行一些会导致主机发送和接收多个 UDP 数据包的操作。也可以什么也不做，仅执行 wireshark 捕获以便获取其他程序发给您的 UDP 数据包。有一种特殊情况：简单网络管理协议（SNMP）在 UDP 内部发送 SNMP 消息，因此可能会在跟踪中找到一些 SNMP 消息（以及 UDP 数据包）。
2. 停止数据包捕获后，设置数据包筛选器，以便 Wireshark 仅显示在主机上发送和接收的 UDP 数据包。 选择其中一个 UDP 数据包并在详细信息窗口中展开 UDP 字段。



task1: 从跟踪中选择一个 UDP 数据包。从此数据包中，识别并确定 UDP 首部字段，请为这些字段命名并将实验结果附在实验报告中。

task2: UDP首部中的长度字段指的是什么，以及为什么需要这样设计？使用捕获的 UDP 数据包进行验证，请将实验结果附在实验报告中。

task3: UDP 有效负载中可包含的最大字节数是多少？请将实验结果附在实验报告中。

首先先认识下**有效负载**：

> 有效负载是被传输数据中的一部分，而这部分才是数据传输的最基本的目的，和有效负载一同被传送的数据还有：数据头或称作元数据，有时候也被称为开销数据，这些数据用来辅助数据传输。
> ——百度百科

task4: 观察发送 UDP 数据包后接收响应的 UDP 数据包，这是对发送的 UDP 数据包的回复，请描述两个数据包中端口号之间的关系。(提示：对于响应 UDP 目的地应该为发送 UDP 包的地址。）请将实验结果附在实验报告中。