

华东师范大学数据科学与工程学院实验报告

课程名称：计算机网络与编程

年级：2021 级

上机实践成绩：

指导教师：张召

姓名：彭一琿

学号：10215501412

上机实践名称：UDP 协议分析

上机实践日期：2023.5.19

上机实践编号：12

组号：

上机实践时间：9:50

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、使用环境

Wireshark

Windows11

四、实验过程

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。

```
> Frame 8207: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on interface \Device\NPF_{77D02574-...}
> Ethernet II, Src: Tp-LinkT_f4:11:f0 (f8:8c:21:f4:11:f0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 1024, Dst Port: 5001
  Source Port: 1024 源端口
  Destination Port: 5001 目的端口
  Length: 139 长度
  Checksum: 0xf1d9 [unverified] 校验和
  [Checksum Status: Unverified]
  [Stream index: 3]
  > [Timestamps]
    UDP payload (131 bytes)
  > Data (131 bytes)
```

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。

真首部数据长度（8bytes）+数据长度。因为数据字段的长度在一个 UDP 段中不同于在另一个段中，因此需要一个明确的长度。如上图所示，数据长度为 131bytes，而 header 里面的 length 字段值为 139，是头部长度加数据长度。

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。

Length 数据段的长度是 2bytes，共有 16 位，能保存的最大数字是 $2^{16}-1=65535$ ，因此有效负载中包含的最大字节数是 65527

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。

7851	281.175866	192.168.1.111	222.94.109.159	UDP	89 55818 → 8000 Len=47
7852	281.226993	222.94.109.159	192.168.1.111	UDP	97 8000 → 55818 Len=55

选取这两个包作为观察对象。发送包的端口如下：

```
Source Address: 192.168.1.111
Destination Address: 222.94.109.159
v User Datagram Protocol, Src Port: 55818, Dst Port: 8000
  Source Port: 55818
  Destination Port: 8000
```

响应包的端口如下：

```
Source Address: 222.94.109.159
Destination Address: 192.168.1.111
User Datagram Protocol, Src Port: 8000, Dst Port: 55818
  Source Port: 8000
  Destination Port: 55818
```

响应包和发送包的源端口和目的端口正好相反，说明 UDP 协议传送的数据包是在两个主机的两个应用程序之间传递的，而响应也是由收到数据包的应用程序进行。

五、总结

本次实验的目的是了解 UDP 协议的工作原理，通过使用 Wireshark 软件快速了解和分析 UDP 协议。通过选择跟踪数据包并识别其 UDP 首部字段，可以深入了解 UDP 协议的结构和设计。

在本次实验中，选择一个 UDP 数据包进行分析，从中识别出 UDP 首部字段并进行命名。UDP 首部由四个字段组成，分别为源端口号、目的端口号、长度和校验和。其中，源端口号指当前传输数据的应用程序所使用的端口号，而目的端口号则表示接收方应用程序所使用的端口号。长度字段指整个 UDP 数据报的长度，包括首部和有效负载。校验和字段用于检测数据是否发生了错误。

需要注意的是，UDP 首部中的长度字段指的是整个 UDP 数据包的长度，包括首部和有效负载。这样设计是为了让接收方能够正确地识别整个 UDP 数据包的长度，并将其正确地提取出来。通过捕获 UDP 数据包进行验证，可以发现 UDP 首部中的长度字段确实指示了整个数据包的长度。

此外，UDP 有效负载中可包含的最大字节数是 65507 字节。这是因为 UDP 首部占用了 8 个字节的空间，而 IP 数据报的最大长度为 65535 字节，因此 UDP 的有效负载最多只能占用 $65535 - 8 = 65527$ 字节的空间。在实验中验证后，得出的结果也与理论值相符。

观察发送 UDP 数据包后接收响应的 UDP 数据包，可以发现这是对发送的 UDP 数据包的回复。在这两个数据包中，端口号之间的关系是目的端口号和源端口号交换了位置，即响应包的源端口号与请求包的目标端口号相同，响应包的目标端口号与请求包的源端口号相同。