

## 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：21 级

上机实践成绩：

指导教师：张召

姓名：杨茜雅

学号：10215501435

上机实践名称：Lab12

上机实践日期：2023.5.26

上机实践编号：12

组号：

上机实践时间：5.26

## 一、实验目的

了解 UDP 协议的工作原理

## 二、实验任务

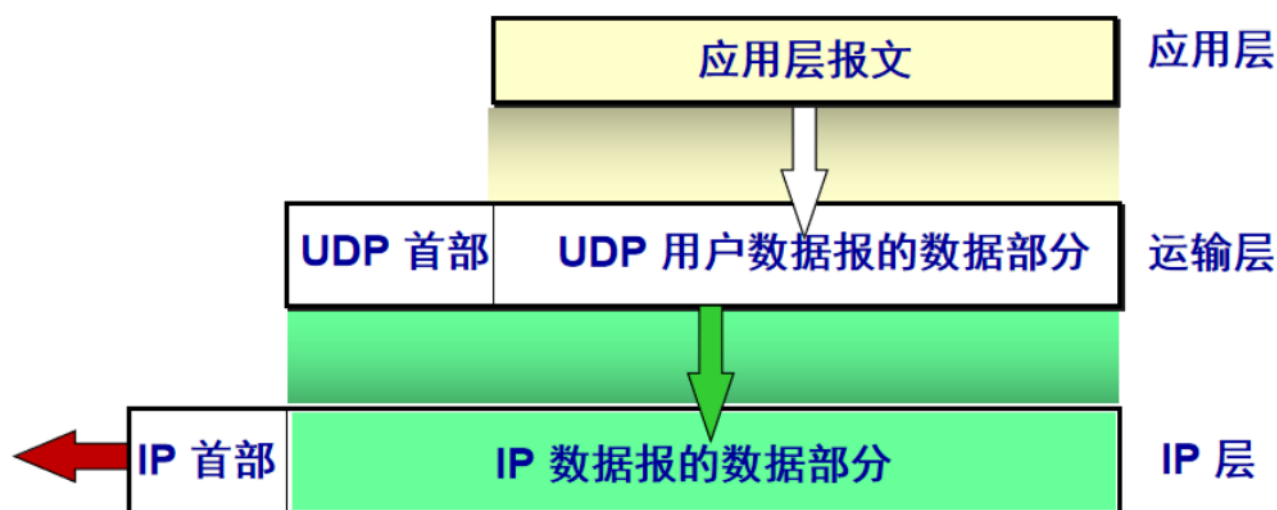
使用 Wireshark 快速了解 UDP 协议

## 三、使用环境

Wireshark

## 四、实验过程

**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。



**Task 1: 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。**

利用 Wireshark 抓取一个 UDP 包

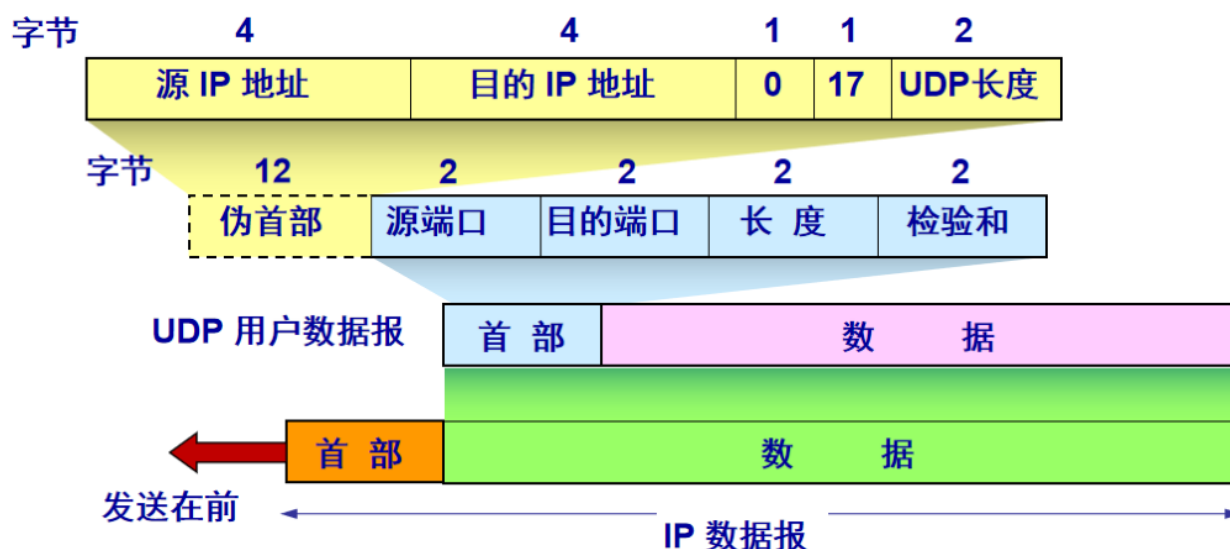
1. 在 Wireshark 中捕获数据包，然后执行一些会导致主机发送和接收多个 UDP 数据包的操作。也可以什么也不做，仅执行 wireshark 捕获以便获取其他程序发给您的 UDP 数据包。有一种特殊情况：简单网络管理协议 (SNMP) 在 UDP 内部发送 SNMP 消息，因此可能会在跟踪中找到一些 SNMP 消息 (以及 UDP 数据包)。

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。

22141 22.180891	fe80::1	fe80::1	168 Standard query response 0x0004 AAAA content-autofill.googleapis.com
22142 22.182609	fe80::1	fe80::a1f7:c6a2:9f2...	175 Standard query response 0x0014 A content-autofill.googleapis.com
22143 22.182795	fe80::1	fe80::a1f7:c6a2:9f2...	168 Standard query response 0x0004 HTTPS content-autofill.googleapis.com
22145 22.205795	192.168.1.7	111.20.4.14	250 8062 → 8829 Len=208
22147 22.253701	111.20.4.14	192.168.1.7	163 8829 → 8062 Len=121
22161 24.116133	39.156.132.106	192.168.1.7	129 OICQ Protocol

## 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。



UDP 首部有 8 个字节，由源端口、目的端口、长度以及校验和 4 个字段构成，每个字段都是两个字节。

> Frame 22145: 250 bytes on wire (2000 bits), 250 bytes captured (2000 bits) on interface \Device\NPF_{90CB2279-4FDD-49D7-8293-23DC64008BEA}, id 0	
> Ethernet II, Src: IntelCor_9a:dc:a6 (10:3d:1c:9a:dc:a6), Dst: zte_ae:b5:e8 (34:24:3e:ae:b5:e8)	
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 111.20.4.14	
▼ User Datagram Protocol, Src Port: 8062, Dst Port: 8829	
Source Port: 8062	源端口: 源端口号, 需要对方回信时选用, 不需要时全部置为0
Destination Port: 8829	目的端口: 目的端口号
Length: 216	长度: UDP的数据报文的长度 (包括首部和数据), 其最小值为8 (只有首部。这里为216)
Checksum: 0x35bb [unverified] [Checksum Status: Unverified] [Stream index: 13]	校验和: 检测UDP数据报在传输中是否有错, 有错则丢弃
> [Timestamps]	
UDP payload (208 bytes)	
▼ Data (208 bytes)	数据部分长度, 等于Length216-首部的长度8

**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。**

UDP 的数据报文的长度包括首部长度和数据长度，其最小值为8，即只有首部。这样设计是为了防止路由错误。

```

User Datagram Protocol, Src Port: 8062, Dst Port: 8829
  Source Port: 8062
  Destination Port: 8829
  Length: 216
  Checksum: 0x35bb [unverified]
  [Checksum Status: Unverified]
  [Stream index: 13]
  > [Timestamps]
  UDP payload (208 bytes)
  Data (208 bytes) 208=Length 216 - header 8
0000 34 24 3e ae b5 e8 10 3d 1c 9a dc a6 08 00 45 00 4$>.....= .....E
0010 00 ec 0c 2d 00 00 80 11 00 00 c0 a8 01 07 0f 14 0
0020 04 0e 1f 7e 22 7d 00 d8 35 bb c9 85 e0 3d 64 69 ...~"}5....=di
0030 f0 40 00 10 40 06 02 00 00 03 00 00 c1 00 40 f0 @...@... ..@

```

**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。

因为UDP 首部中，长度字段只有2 个字节即16 位。所以能表示的最大数为 $2^{16}-1=65535$ 。又因为UDP 首部占据了8 字节，所以有效负载中可包含的最大字节数是 $65535-8=65527$  字节。

**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。**

对于这组发送的 UDP 数据包和响应的 UDP 数据包。

22143	22.182795	fe80::1	fe80::a1f7:c6a2:9f2...	DNS	168 Standard query response 0xatec HTTP
22145	22.205795	192.168.1.7	111.20.4.14	UDP	250 8062 → 8829 Len=208
22147	22.253781	111.20.4.14	192.168.1.7	UDP	163 8829 → 8062 Len=121
22161	24.116133	39.156.132.106	192.168.1.7	OICQ	129 OICQ Protocol

编号为22145 和22147。No. 22145 包的源地址是：192.168.1.7 即我本地的电脑地址，目的地址是111.20.4.14，源端口是8062，目的端口是8829。No. 22147包的原地址是111.20.4.14，而目的地之是192.168.1.7，源端口是8829，目的端口8062。

所以我们可以发现：

发送UDP 数据包的源端口号等于响应的UDP 数据包的目的端口号。

响应UDP 数据包的源端口号等于发送的UDP 数据包的目的端口号。

✓ User Datagram Protocol, Src Port: 8062, Dst Port: 8829

Source Port: 8062

Destination Port: 8829

Length: 216

Checksum: 0x35bb [unverified]

[Checksum Status: Unverified]

[Stream index: 13]

> [Timestamps]

UDP payload (208 bytes)

✓ Data (208 bytes)

✓ User Datagram Protocol, Src Port: 8829, Dst Port: 8062

Source Port: 8829

Destination Port: 8062

Length: 129

Checksum: 0xde35 [unverified]

[Checksum Status: Unverified]

[Stream index: 13]

> [Timestamps]

UDP payload (121 bytes)

## 五、总结

通过本次实验，使用Wireshark 了解到了UDP 协议，明确了UDP 协议的作原理，更直观地认识到了UDP发送数据包和响应数据包之间的联系以及UDP数据包的结构，对UDP 协议有了更深刻的理解。