

## 华东师范大学数据科学与工程学院上机实践报告

课程名称：计算机网络原理与编程

年级：2018

上机实践成绩：

指导教师：张召

姓名：孙秋实

学号：10185501402

上机实践名称：UDP 协议分析

上机实践日期：2020/5/11

上机实践编号：Exp5

组号：

上机实践时间：

### Part 1

#### 实验目的

- 快速简单了解 UDP 协议
- 了解 UDP 的标头数据，报文段数据结构

### Part 2

#### 实验任务

- 使用已被抓取的数据分析 UDP 协议

### Part 3

#### 使用环境

- Wireshark Version 3.2.3

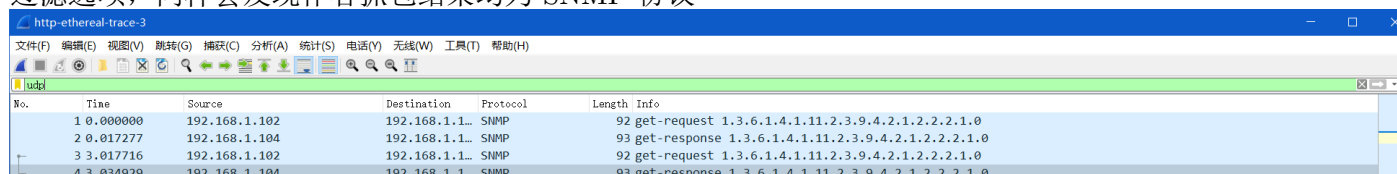
### Part 4

#### 实验过程

#### Task 1

Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn't look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.

首先，SNMP 采用 UDP 协议在管理端和 agent 之间传输信息，所以我们分析 SNMP 协议，使用 UDP 过滤选项，同样会发现作者抓包结果均为 SNMP 协议



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	192.168.1.1...	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
2	0.017277	192.168.1.104	192.168.1.1...	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
3	0.017716	192.168.1.102	192.168.1.1...	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
4	0.034929	192.168.1.104	192.168.1.1...	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0

上图为使用过滤器获得基于 (SNMP)UDP 协议的数据传输

UDP 协议头较为简单，包括以下四个部分，每个部分由两个字节构成：

- (1) 源端口号 (Source Port)
- (2) 目标端口号 (Destination Port)
- (3) 报文长度 (Length)
- (4) 校验和 (Checksum)

如下图所示

```

User Datagram Protocol, Src Port: 161, Dst Port: 4271
  Source Port: 161
  Destination Port: 4271
  Length: 59
  Checksum: 0x8e31 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 3]
  > [Timestamps]

```

## Task 2

By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

如 Task1 所示 UDP 报文共有四个部分，每个部分有两个字节构成 (2Bytes=16Bits)

$$\therefore \text{Sizeof}(\text{Header}) = 8\text{Bytes} = 64\text{Bits}$$

## Task 3

The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.

UDP 报文中的长度字段指的是数据长度与报文头长度之和，在这个 trace 的分析中为

$$\text{Length} = 59\text{bytes} = 8\text{bytes}(\text{Header}) + 51\text{bytes}(\text{Data})$$

如下图所示，传输数据长度为 51bytes

```

Simple Network Management Protocol
  version: version-1 (0)
  community: public
  data: get-response (2)
    > get-response
      [Response To: 3]
      [Time: 0.017213000 seconds]

```

0000	00 08 74 4f 36 23 00 30 c1 61 eb ed 08 00 45 00	..t06#..0.a...E.
0010	00 4f ed 68 00 00 3c 11 0d 17 c0 a8 01 68 c0 a8	.O.h...<.....h..
0020	01 66 00 a1 10 af 00 3b 8e 31 30 31 02 01 00 04	.f.....;..101...
0030	06 70 75 62 6c 69 63 a2 24 02 02 18 c1 02 01 00	.public.\$.....
0040	02 01 00 30 18 30 16 06 11 2b 06 01 04 01 0b 02	...0.0...+.....
0050	03 09 04 02 01 02 02 02 01 00 04 01 10	.....

Simple Network Management Protocol (snmp), 51 byte(s)

总长度 (Length) 为 69Bytes

```

User Datagram Protocol, Src Port: 161, Dst Port: 4270
  Source Port: 161
  Destination Port: 4270
  Length: 59
  Checksum: 0x8f32 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 1]
  > [Timestamps]

```

**Task 4**

What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your answer to 2. above)

考虑 UDP 包内的 Header 内的总长度字段，同样为 2Bytes，因此 UDP 数据包的总长度被限制为  $2^{16} - 1 = 65535$ ，但有效载荷还需考虑 Header 占据的字段大小，即 65535 再减去 UDP Header 本身所占用的 8 个字节，因此基于 UDP 协议的服务中的最大有效负载长度为  $65535 - 8 = 65527$  Bytes

**Task 5**

What is the largest possible source port number? (Hint: see the hint in 4.)

在之前的实验中我们知道，有两个 Bytes 用于源端口号 (Source Port)

$$\therefore 2\text{Bytes} = 16\text{Bits} \Rightarrow 2^{16} - 1 = 65535$$

即最大源端口号为 65535

**Task 6**

What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. To answer this question, you'll need to look into the Protocol field of the IP datagram containing this UDP segment (see Figure 4.13 in the text, and the discussion of IP header fields)

查询协议号列表可知，UDP 协议号在十进制下为 17，在 16 进制下为 0x11

十进制	十六进制	关键字	协议	引用
0	0x00	HOPOPT	IPv6 逐跳选项	RFC 2460
1	0x01	ICMP	互联网控制消息协议 (ICMP)	RFC 792
2	0x02	IGMP	因特网组管理协议 (IGMP)	RFC 1112
3	0x03	GGP	网关对网关协议	RFC 823
4	0x04	IPv4	IPv4 (封装)	RFC 791
5	0x05	ST	因特网流协议	RFC 1190, RFC 1819
6	0x06	TCP	传输控制协议 (TCP)	RFC 793
7	0x07	CBT	有核树组播路由协议	RFC 2189
8	0x08	EGP	外部网关协议	RFC 888
9	0x09	IGP	内部网关协议 (任意私有内部网关 (用于思科的 IGRP))	
10	0x0A	BBN-RCC-MON	BBN RCC 监视	
11	0x0B	NVP-II	网络语言协议	RFC 741
12	0x0C	PUP	Xerox PUP	
13	0x0D	ARGUS	ARGUS	
14	0x0E	EMCON	EMCON	
15	0x0F	XNET	Cross Net Debugger	IEN 158
16	0x10	CHAOS	Chaos	
17	0x11	UDP	用户数据报协议 (UDP)	RFC 768
18	0x12	MUX	多路复用	IEN 90
19	0x13	DCN-MEAS	DCN Measurement Subsystems	
20	0x14	HMP	Host Monitoring Protocol	RFC 869
21	0x15	PRM	Packet Radio Measurement	

分析 UDP 协议传输的数据包时也可以得到其协议号即其在 10 进制和 16 进制下的表示

```

Internet Protocol Version 4, Src: 192.168.1.104, Dst: 192.168.1.102
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 79
    Identification: 0xed67 (60775)
    > Flags: 0x0000
      Fragment offset: 0
      Time to live: 60
      Protocol: UDP (17)
      Header checksum: 0x0d18 [validation disabled]
      [Header checksum status: Unverified]
      Source: 192.168.1.104
      Destination: 192.168.1.102

```

```

0000  00 08 74 4f 36 23 00 30 c1 61 eb ed 08 00 45 00
0010  00 4f ed 67 00 00 3c 11 0d 18 c0 a8 01 68 c0 a8
0020  01 66 00 a1 10 ae 00 3b 8f 32 30 31 02 01 00 04
0030  06 70 75 62 6c 69 63 a2 24 02 02 18 c0 02 01 00
0040  02 01 00 30 18 30 16 06 11 2b 06 01 04 01 0b 02
0050  03 09 04 02 01 02 02 02 01 00 04 01 10

```

**Task 7**

Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). Describe the relationship between the port numbers in the two packets.

## 分析一组发送——接收捕捉记录

3	3.017716	192.168.1.102	192.168.1.1...	SNMP	92	get-request	1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0
4	3.034929	192.168.1.104	192.168.1.1...	SNMP	93	get-response	1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0

```

> Frame 4: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)
> Ethernet II, Src: HewlettP_61:eb:ed (00:30:c1:61:eb:ed), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 192.168.1.104, Dst: 192.168.1.102
v User Datagram Protocol, Src Port: 161, Dst Port: 4271
  Source Port: 161
  Destination Port: 4271
  Length: 59
  Checksum: 0x8e31 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 3]
> [Timestamps]
> Frame 3: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: HewlettP_61:eb:ed (00:30:c1:61:eb:ed)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.104
v User Datagram Protocol, Src Port: 4271, Dst Port: 161
  Source Port: 4271
  Destination Port: 161
  Length: 58
  Checksum: 0xa037 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 3]
> [Timestamps]

```

如上图所示，数据发送者在接收返回的 UDP 协议数据包时，会变成接收端口号。同样地，数据接收者发送返回 UDP 时候用于接收的端口号会变成发送端口号。