lab2.1 利用wireshark观察网络层报文

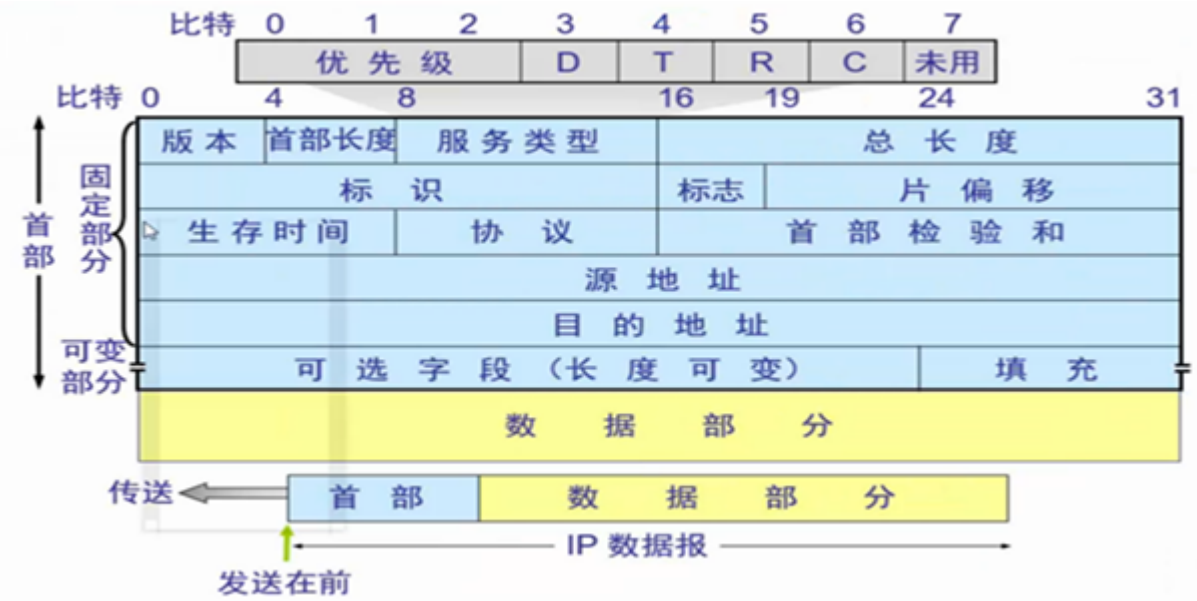
&实验步骤

利用 wireshark 和 PingPlotter 观察网络层数据包 (1) 下载并安装wireshark以及PingPlotter (2) 配置PingPlotter发包大小为3000Bytes (3) 启动wireshark (4) 启动PingPlotter追踪 gaia.cs.umass.edu，大约count值为3-4次时停止

&IP数据报/ICMP协议简介

IP数据报

IP数据报的数据部分一般是TCP/UDP报文段或ICMP协议内容



ICMP协议

ICMP报文承载在IP分组中，其首部占8个字节。

ICMP可用于网络层差错报告，其报文类型如下

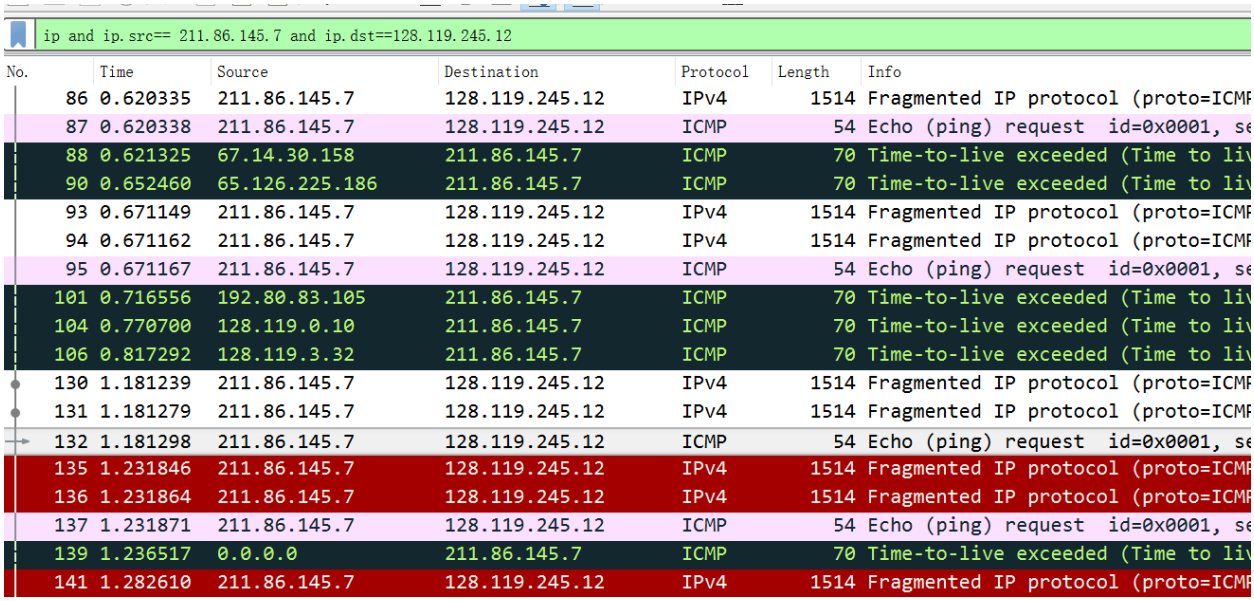
ICMP 类型	编码	描述
0	0	回显回答（对 ping 的回答）
3	0	目的网络不可达
3	1	目的主机不可达
3	2	目的协议不可达
3	3	目的端口不可达
3	6	目的网络未知
3	7	目的主机未知
4	0	源抑制（拥塞控制）
8	0	回显请求
9	0	路由器通告
10	0	路由器发现
11	0	TTL过期
12	0	IP 首部损坏

&抓包结果分析

1.显示过滤器过滤出本机到目的主机的所有IP和ICMP数据包

- **IP数据包**

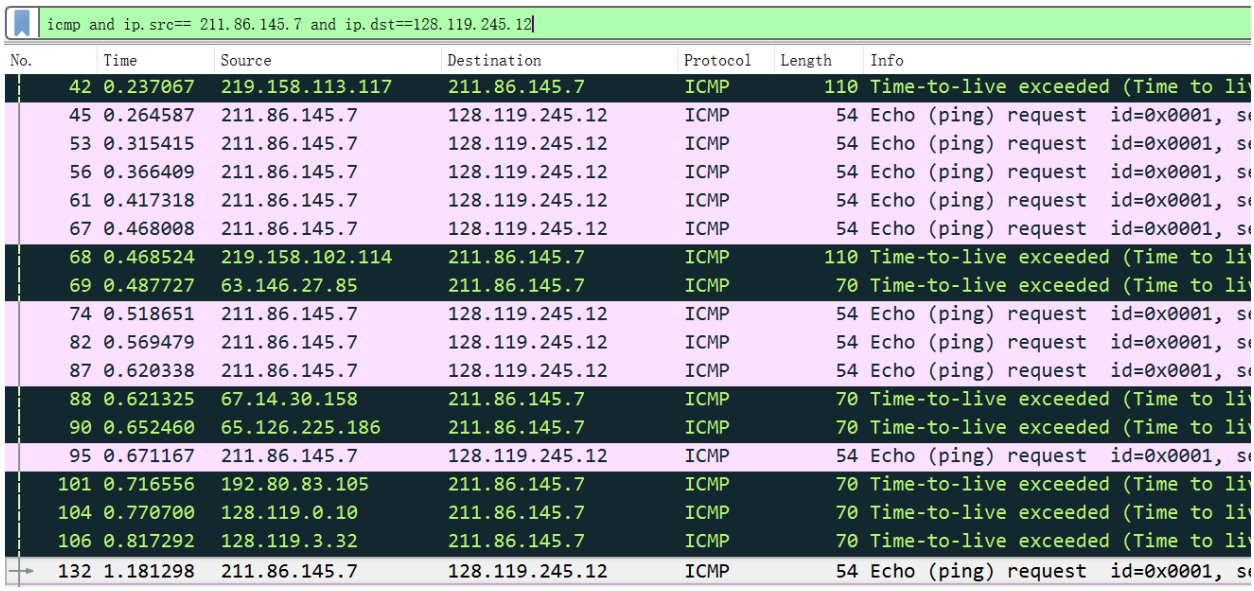
  显示过滤器：ip and ip.src== 211.86.145.7 and ip.dst==128.119.245.12



No.	Time	Source	Destination	Protocol	Length	Info
86	0.620335	211.86.145.7	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP
87	0.620338	211.86.145.7	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, se
88	0.621325	67.14.30.158	211.86.145.7	ICMP	70	Time-to-live exceeded (Time to liv
90	0.652460	65.126.225.186	211.86.145.7	ICMP	70	Time-to-live exceeded (Time to liv
93	0.671149	211.86.145.7	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP
94	0.671162	211.86.145.7	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP
95	0.671167	211.86.145.7	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, se
101	0.716556	192.80.83.105	211.86.145.7	ICMP	70	Time-to-live exceeded (Time to liv
104	0.770700	128.119.0.10	211.86.145.7	ICMP	70	Time-to-live exceeded (Time to liv
106	0.817292	128.119.3.32	211.86.145.7	ICMP	70	Time-to-live exceeded (Time to liv
130	1.181239	211.86.145.7	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP
131	1.181279	211.86.145.7	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP
132	1.181298	211.86.145.7	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, se
135	1.231846	211.86.145.7	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP
136	1.231864	211.86.145.7	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP
137	1.231871	211.86.145.7	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, se
139	1.236517	0.0.0.0	211.86.145.7	ICMP	70	Time-to-live exceeded (Time to liv
141	1.282610	211.86.145.7	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP

- **ICMP数据包**

  显示过滤器：icmp and ip.src== 211.86.145.7 and ip.dst==128.119.245.12

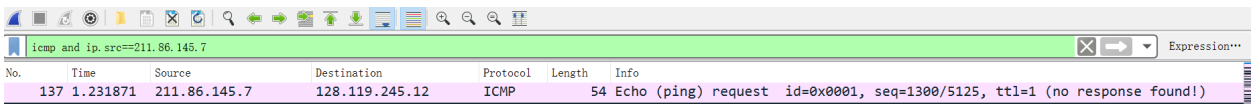


No.	Time	Source	Destination	Protocol	Length	Info
42	0.237067	219.158.113.117	211.86.145.7	ICMP	110	Time-to-live exceeded (Time to liv
45	0.264587	211.86.145.7	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, se
53	0.315415	211.86.145.7	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, se
56	0.366409	211.86.145.7	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, se
61	0.417318	211.86.145.7	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, se
67	0.468008	211.86.145.7	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, se
68	0.468524	219.158.102.114	211.86.145.7	ICMP	110	Time-to-live exceeded (Time to liv
69	0.487727	63.146.27.85	211.86.145.7	ICMP	70	Time-to-live exceeded (Time to liv
74	0.518651	211.86.145.7	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, se
82	0.569479	211.86.145.7	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, se
87	0.620338	211.86.145.7	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, se
88	0.621325	67.14.30.158	211.86.145.7	ICMP	70	Time-to-live exceeded (Time to liv
90	0.652460	65.126.225.186	211.86.145.7	ICMP	70	Time-to-live exceeded (Time to liv
95	0.671167	211.86.145.7	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, se
101	0.716556	192.80.83.105	211.86.145.7	ICMP	70	Time-to-live exceeded (Time to liv
104	0.770700	128.119.0.10	211.86.145.7	ICMP	70	Time-to-live exceeded (Time to liv
106	0.817292	128.119.3.32	211.86.145.7	ICMP	70	Time-to-live exceeded (Time to liv
132	1.181298	211.86.145.7	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, se

2.查找本机发送的第一个 TTL等于1 的 ICMP Echo Request 消息

- **显示过滤器输入ip.src==211.86.145.7 and icmp**

  查找到第一个TTL=1的ICMP Echo Request 消息



No.	Time	Source	Destination	Protocol	Length	Info
137	1.231871	211.86.145.7	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, seq=1300/5125, ttl=1 (no response found!)

- **此IP数据报是否被分片?**

  查看此数据报详细IP报文段，可知其在链路层帧中分片为三个片段,数据包编号分别为No.135，No.136，No.137

```
[3 IPv4 Fragments (2980 bytes): #135(1480), #136(1480), #137(20)]
    [Frame: 135, payload: 0-1479 (1480 bytes)]
    [Frame: 136, payload: 1480-2959 (1480 bytes)]
    [Frame: 137, payload: 2960-2979 (20 bytes)]
    [Fragment count: 3]
    [Reassembled IPv4 length: 2980]
```

3.分析碎片IP数据报的第一个片段

- **打印出碎片IP数据报的第一个片段**

  No.135数据包的IPv4数据报文如下图

```
Internet Protocol Version 4, Src: 211.86.145.7, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x7db3 (32179)
  v Flags: 0x2000, More fragments
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..1. .... .... .... = More fragments: Set
      ...0 0000 0000 0000 = Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x3c8c [validation disabled]
    [Header checksum status: Unverified]
    Source: 211.86.145.7
    Destination: 128.119.245.12
    Reassembled IPv4 in frame: 137
Data (1480 bytes)
```

- **IP 头中的哪些信息表明数据报已碎片化?**

  标志(flags)字段为1，说明已碎片化，且不为最后一个片段。

  Total Length=1500, 说明此数据报已达到最大长度，这不能确定已碎片化，只能说明很可能已碎片化。

- **IP报头中的哪些信息表明这是第一个片段还是后一个片段?**

  标志(flags)字段为1，说明已碎片化，且不为最后一个片段。

  偏移字段(offset)为0，说明是第一个片段。

- **这个 IP 数据报header有多少个字节?**

  Header Length= 20 bytes， 即header有20字节

- **有效负载有多少个字节?**

  Total Length=1500，1500-20=1480，即数据段为1480字节

4.分析碎片IP数据报的第二个片段

- **打印出碎片 IP 数据报的第二个片段。**

  No.136数据包的IPv4数据报文如下图

```
Internet Protocol Version 4, Src: 211.86.145.7, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x7db3 (32179)
  v Flags: 0x20b9, More fragments
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..1. .... .... .... = More fragments: Set
      ...0 0000 1011 1001 = Fragment offset: 185
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x3bd3 [validation disabled]
    [Header checksum status: Unverified]
    Source: 211.86.145.7
    Destination: 128.119.245.12
    Reassembled IPv4 in frame: 137
v Data (1480 bytes)
```

- **IP 报头中的哪些信息表明这不是第一个数据报片段?**

  偏移字段(offset)为185，说明这不是第一个数据报片段。

- **是否还有更多的片段?**

  标志(flags)字段为1，说明已碎片化，且不为最后一个片段，故还有更多片段。

5.分析碎片IP数据报的最后一个片段

- **打印出碎片 IP 数据报的最后一个片段**

  在第一个片段的数据包中，蓝色字段说明最后一个片段是编号为No.137的数据包，其IPv4数据报文如下图

```
Internet Protocol Version 4, Src: 211.86.145.7, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x7db3 (32179)
  v Flags: 0x0172
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..0. .... .... .... = More fragments: Not set
      ...0 0001 0111 0010 = Fragment offset: 370
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x60ce [validation disabled]
    [Header checksum status: Unverified]
    Source: 211.86.145.7
    Destination: 128.119.245.12
  v [3 IPv4 Fragments (2980 bytes): #135(1480), #136(1480), #137(20)]
      [Frame: 135, payload: 0-1479 (1480 bytes)]
      [Frame: 136, payload: 1480-2959 (1480 bytes)]
      [Frame: 137, payload: 2960-2979 (20 bytes)]
      [Fragment count: 3]
      [Reassembled IPv4 length: 2980]
      [Reassembled IPv4 data: 08007870000105142020202020202020202020202020202020...]
```

- **从原始数据报创建了多少个片段?**

  Fragment count=3 ,说明从原始数据报创建了3个片段

- **如何判断是最后一个片段?**

  标志(flags)字段为0，说明是最后一个片段

- **最后一个 IP数据报负载有多少个字节?**

  总长度：40 字节

  首部长度：20 字节

  负载长度：40-20=20 字节

- **TTL的值**

  TTL=1

- **上层协议字段**

  三个分段的IP数据报组装成一个完整的IP数据报，组装得到IP数据报文，其上层协议字段为ICMP，故把组装后的有效载荷提供给ICMP协议

- **下层协议**

  网络层的下层即为链路层协议，其信息如下图

```
Ethernet II, Src: RivetNet_e1:41:91 (9c:b6:d0:e1:41:91), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
  > Destination: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
  > Source: RivetNet_e1:41:91 (9c:b6:d0:e1:41:91)
    Type: IPv4 (0x0800)
```