



计算机网络实验五

互联网控制报文协议 (ICMP)

信息学部 朱婉婷

主要内容

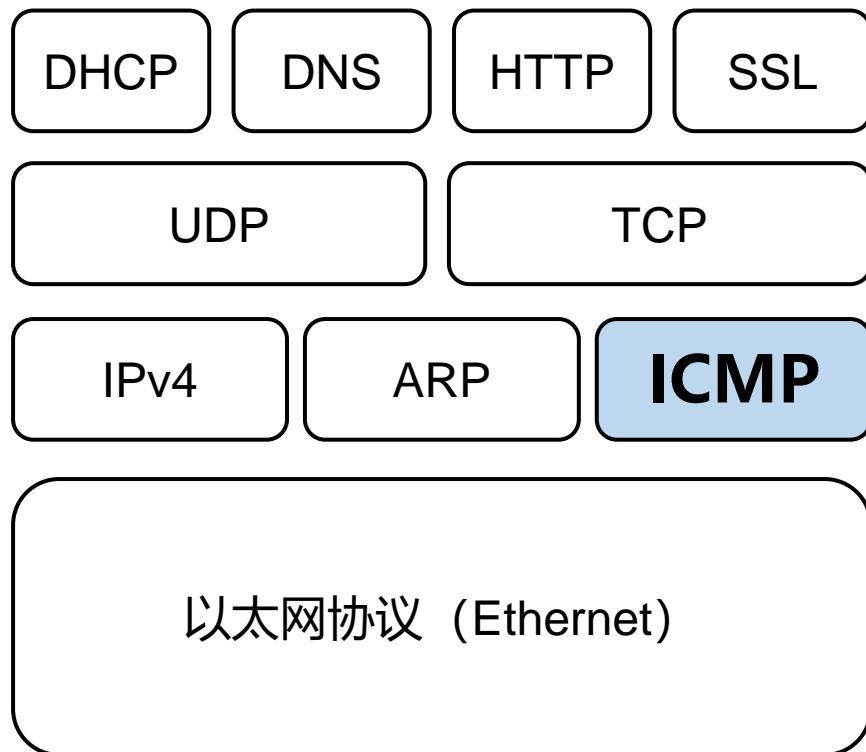
- 一、实验原理
- 二、实验步骤
- 三、实验结果及分析

ICMP简介

◆网际控制报文协议 ICMP

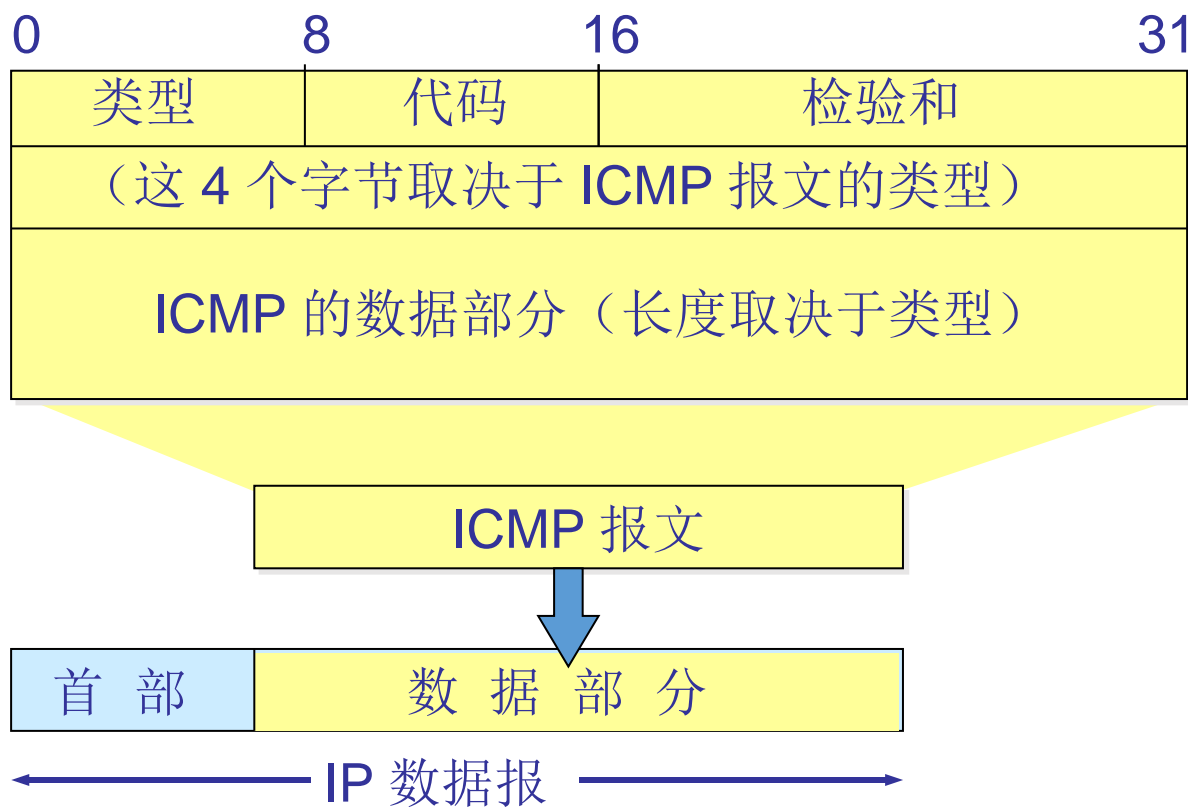
(Internet Control Message Protocol)

- 支持主机或路由器传递**控制消息**，提高 IP 数据报**交付成功**的机会。
- ICMP 允许主机或路由器报告**差错情况**和**异常情况**。
- ICMP 报文作为 IP 层数据报的**数据**，加上IP数据报的首部，组成 IP 数据报发送出去。



ICMP 报文的格式

- ICMP 报文的前 4 个字节是统一的格式，共有三个字段：即 **类型**、**代码**和**检验和**。
- 接着的 4 个字节的内容与 ICMP 的类型有关。



ICMP 报文的格式

类型(Type)	代码(Code)	描述
0	0	回送应答 (ping)
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-未用)
8	0	回送请求(ping)
9	0	路由通告
10	0	路由发现
11	0	TTL超时
12	0	IP首部错误

ICMP 报文的种类

◆询问报文(2种)

- 回送(Echo)请求与应答报文
- 时间戳请求与应答报文

◆差错报告报文(5种)

- 目的不可达
- 源抑制(Source Quench)
- TTL超时/超期
- 参数问题
- 重定向 (Redirect)

回送(Echo)请求与应答报文

- **回送请求** (echo-request) 与**回送应答** (echo-reply) 报文属于ICMP询问报文，两者是为了网络诊断而设计的。
- 回送请求和回送应答组合起来确定了两个系统（主机或路由器）之间**能否彼此通信**。

类型：8或0（请求报文为8,应答报文为0）	代码：0	检验和
标识符（由主机设定，一般设置为进程号，回送应答消息与回送请求消息中identifier保持一致）		序号（由主机设定，一般设为由0递增的序列，回送应答消息与回送请求消息中Sequence Number保持一致）
可选数据 由请求报文发送，被应答报文重复		

ICMP的应用举例——PING命令

◆PING (Packet InterNet Groper)

- PING 使用了 ICMP 回送请求与回送应答报文。
- PING 用来测试两个主机之间的连通性。
- PING 是应用层直接使用网络层 ICMP 的例子，它没有通过运输层的 TCP 或UDP。

PING命令示例

```
C:\Users\zwt717>ping www.baidu.com
```

```
正在 Ping www.a.shifen.com [39.156.66.14] 具有 32 字节的数据:
```

```
来自 39.156.66.14 的回复: 字节=32 时间=27ms TTL=52
```

```
来自 39.156.66.14 的回复: 字节=32 时间=39ms TTL=51
```

```
来自 39.156.66.14 的回复: 字节=32 时间=21ms TTL=52
```

```
来自 39.156.66.14 的回复: 字节=32 时间=17ms TTL=52
```

```
39.156.66.14 的 Ping 统计信息:
```

```
数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
```

```
往返行程的估计时间(以毫秒为单位):
```

```
最短 = 17ms, 最长 = 39ms, 平均 = 26ms
```

```
C:\Users\zwt717>ping www.bjut.edu.cn
```

```
正在 Ping bjut-edu-cn.cname.saaswaf.com [27.221.108.54] 具有 32 字节的数据:
```

```
请求超时。
```

```
请求超时。
```

```
请求超时。
```

```
请求超时。
```

```
27.221.108.54 的 Ping 统计信息:
```

```
数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```

ICMP超时报文

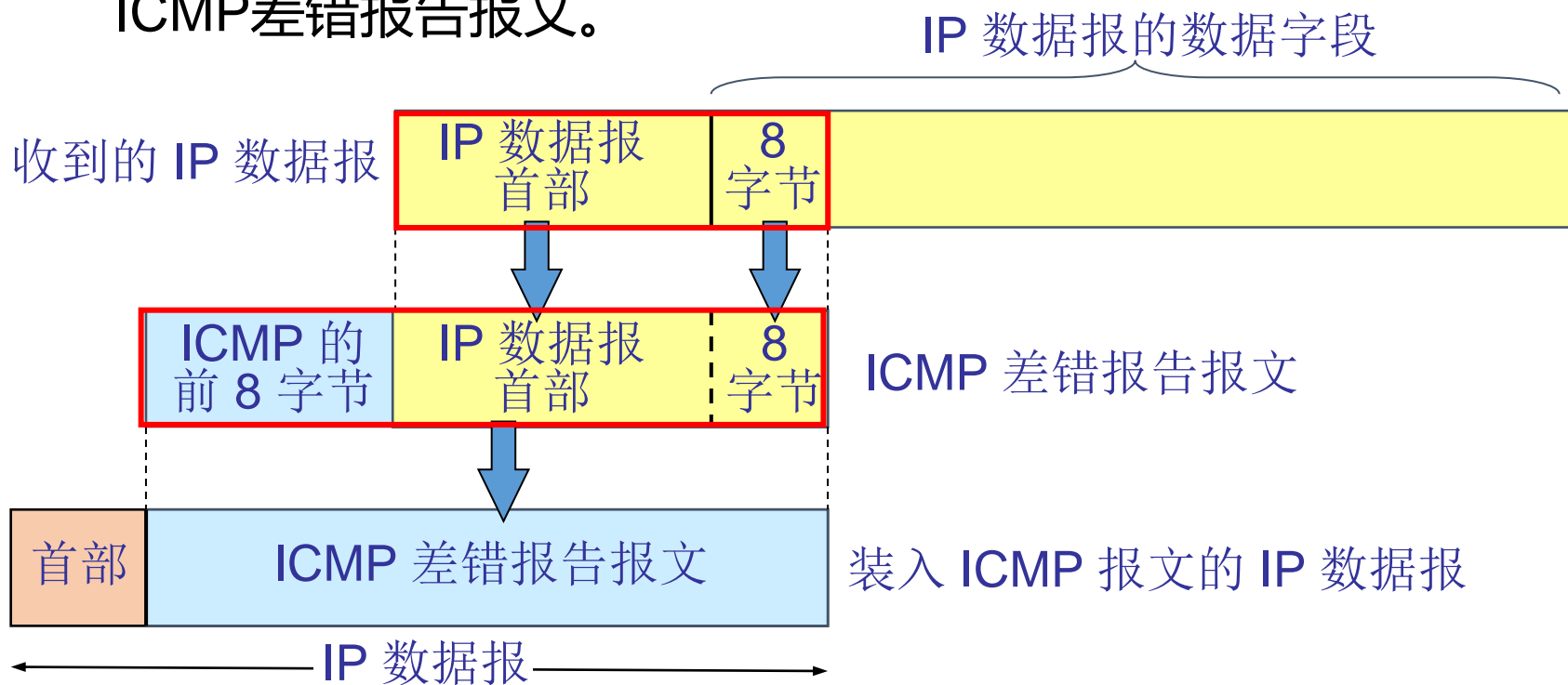
◆超时报文在以下两种情况下产生：

- **代码0**：当网络结点发现某数据报的**TTL域为零**，需要丢弃此数据报时，需要向该数据报的源主机告知超时出错；
- **代码1**：当目的主机在分段重组时，规定时间内由于分段丢失**未完成重组**，需要发送超时报文。

类型： 11	代码： 0或1	检验和
未使用（全为0）		
收到的IP数据报的一部分，包括IP首部 以及数据报数据的前8个字节		

ICMP 差错报告报文的数据字段的内容

- 将收到的需要进行差错报告IP数据报的首部和数据字段的前8个字节提取出来，作为ICMP报文的数据字段。
- 再加上响应的ICMP差错报告报文的前8个字节，就构成了ICMP差错报告报文。



Traceroute (tracert) 命令示例

```
C:\Users\zwt717>tracert www.baidu.com
```

通过最多 30 个跃点跟踪

到 www.a.shifen.com [39.156.66.18] 的路由:

1	3 ms	3 ms	7 ms	192.168.1.1
2	42 ms	24 ms	180 ms	100.79.128.1
3	*	42 ms	*	211.136.60.225
4	*	*	*	请求超时。
5	*	*	*	请求超时。
6	24 ms	31 ms	*	111.13.188.114
7	8 ms	6 ms	*	111.13.188.38
8	16 ms	5 ms	17 ms	39.156.67.1
9	12 ms	*	6 ms	39.156.67.33
10	*	*	*	请求超时。
11	*	*	*	请求超时。
12	*	*	*	请求超时。
13	6 ms	6 ms	*	39.156.66.18
14	7 ms	7 ms	11 ms	39.156.66.18

跟踪完成。

ICMP的应用举例——Tracert命令

◆ Tracert (Traceroute)

- 利用报文的TTL信息实现路由的获取。
- 首先主机会向目的主机发送一个TTL=1的数据报，当数据报到达第一个路由器时，TTL减1变为0，这时路由器会发送一个ICMP差错报告报文返回给主机说明数据报超时。由此得到第一个路由地址。
- 然后令TTL=2,再次发送一个数据报，会得到第二个路由返回的ICMP差错报告报文。
- 由此一次次增加TTL就可以得到主机到目的主机之间所经过的路由信息。
- 因此，当执行tracert命令并且抓取ICMP时，抓取的ICMP报文当中就会有超时报文。

Traceroute (tracert) 命令示例

```
C:\Users\zwt>tracert www.bjut.edu.cn
```

通过最多 30 个跃点跟踪

到 bjut-edu-cn.cname.saaswaf.com [116.211.138.205] 的路由:

1	2 ms	2 ms	1 ms	192.168.1.1
2	5 ms	5 ms	5 ms	101.39.218.185
3	18 ms	37 ms	6 ms	101.39.218.65
4	5 ms	5 ms	4 ms	10.255.38.133
5	5 ms	7 ms	5 ms	10.255.125.209
6	5 ms	5 ms	5 ms	218.241.253.241
7	*	*	5 ms	218.241.245.177
8	*	6 ms	*	218.241.244.189
9	4 ms	4 ms	4 ms	218.241.166.242
10	5 ms	5 ms	*	218.241.166.253
11	6 ms	*	*	218.241.244.65
12	5 ms	5 ms	5 ms	218.241.244.141
13	11 ms	14 ms	17 ms	211.153.2.249
14	10 ms	*	11 ms	103.216.40.43
15	*	*	*	请求超时。
16	*	*	*	请求超时。
17	*	8 ms	*	36.110.63.237
18	*	*	*	请求超时。
19	29 ms	34 ms	32 ms	202.97.65.254
20	28 ms	32 ms	28 ms	116.211.130.10
21	*	*	*	请求超时。
22	28 ms	28 ms	28 ms	116.211.112.254
23	*	*	*	请求超时。
24	*	*	*	请求超时。
25	*	*	*	请求超时。
26	*	*	*	请求超时。
27	*	*	*	请求超时。
28	*	*	*	请求超时。
29	*	*	*	请求超时。
30	*	*	*	请求超时。

跟踪完成。

主要内容

- 一、实验原理
- 二、实验步骤
- 三、实验结果及分析

实验环境搭建

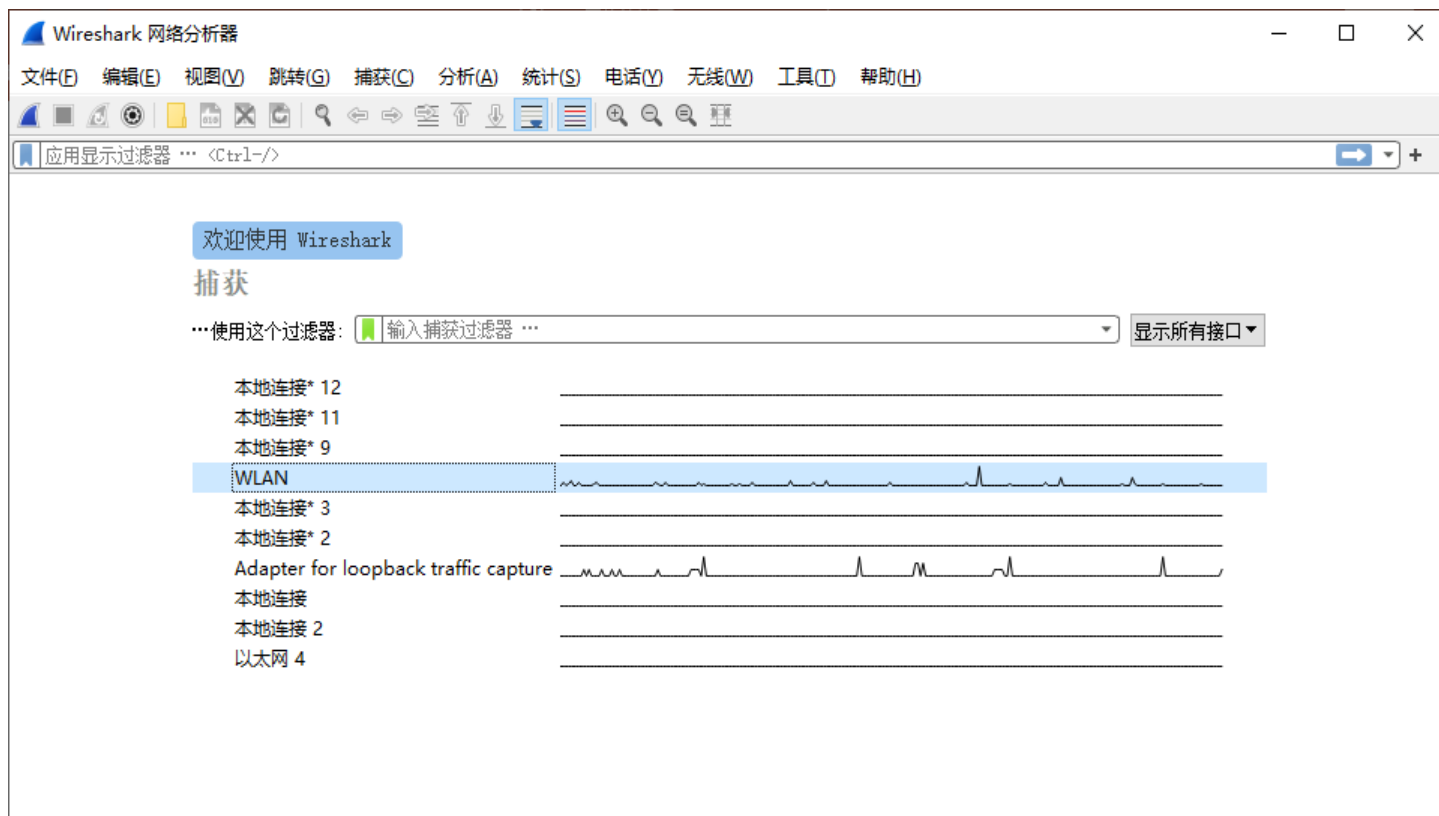
列出本次实验所使用的平台和相关软件，以下为例：

(打开cmd指令窗口，输入指令 “ipconfig /all”查看)

- 1、主机：联想笔记本（Win10系统）；主机IP地址：192.168.1.106；子网掩码：255.255.255.0；主机网卡MAC地址：34-F6-4B-C0-90-40。
- 2、网络连接方式：无线连接；默认网关地址：192.168.1.1。
- 3、抓包工具：Wireshark（v3.6.2）。

实验具体步骤

1、打开Wireshark软件，双击本次实验正在使用的网络接口，开始进行抓包。



实验具体步骤

- 2、在Windows命令模式下利用ping命令来抓取ICMP请求和应答报文。输入命令 “ping www.baidu.com”。
- 3、记录目的地IP地址， “39.156.66.18” 。

```
C:\Users\zwt717>ping www.baidu.com
```

```
正在 Ping www.a.shifen.com [39.156.66.18] 具有 32 字节的数据:
```

```
来自 39.156.66.18 的回复: 字节=32 时间=6ms TTL=52
```

```
来自 39.156.66.18 的回复: 字节=32 时间=7ms TTL=53
```

```
来自 39.156.66.18 的回复: 字节=32 时间=6ms TTL=52
```

```
来自 39.156.66.18 的回复: 字节=32 时间=8ms TTL=53
```

```
39.156.66.18 的 Ping 统计信息:
```

```
数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),  
往返行程的估计时间(以毫秒为单位):
```

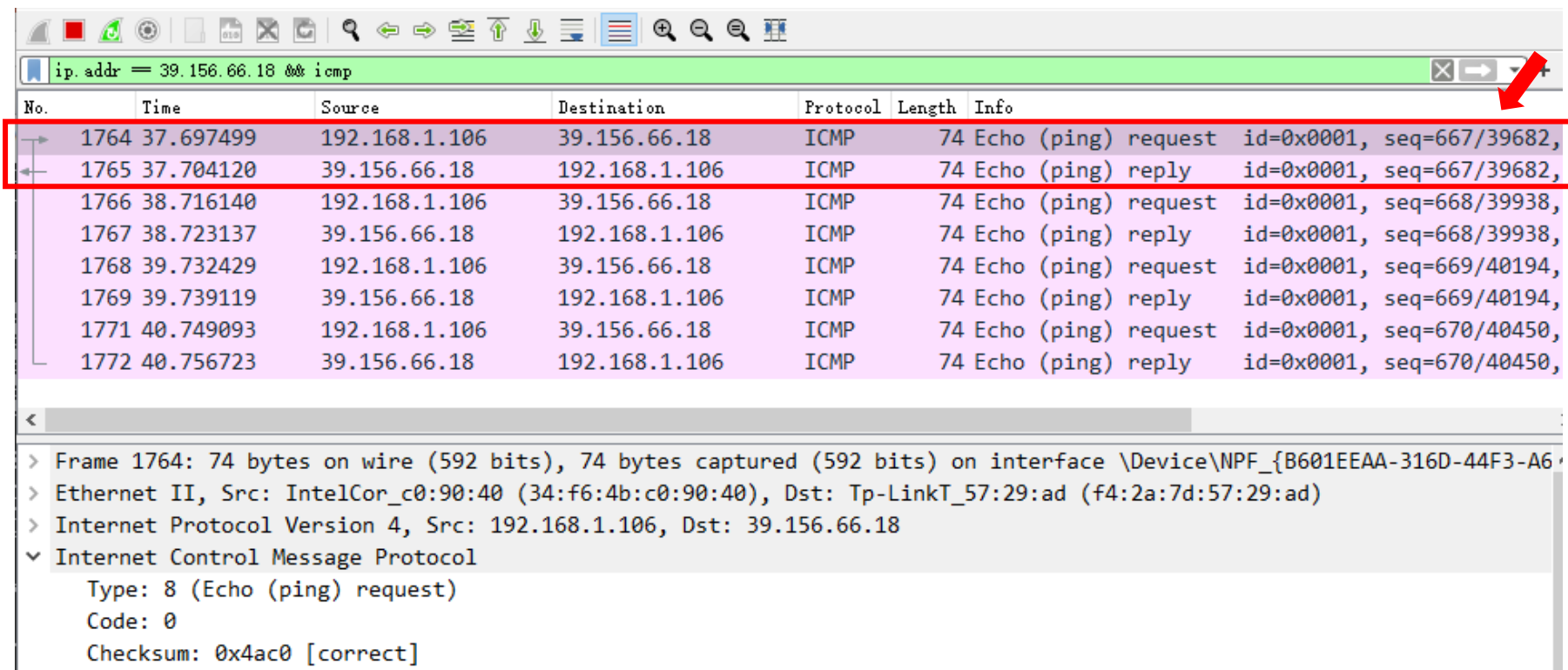
```
最短 = 6ms, 最长 = 8ms, 平均 = 6ms
```

实验具体步骤

4、使用过滤表达式 “icmp” 对捕获的数据包进行初步筛选。

或：ip.addr == 39.156.66.18 && icmp （目的地IP地址）

5、从中选取一组回送(Echo)请求与应答报文数据包。



The screenshot shows the Wireshark network protocol analyzer interface. The filter bar at the top contains the expression `ip.addr == 39.156.66.18 && icmp`. The packet list pane displays a series of ICMP Echo (ping) request and reply packets between 192.168.1.106 and 39.156.66.18. Packets 1764 and 1765 are highlighted with a red box, representing a request and its corresponding reply. A red arrow points to the filter bar. The packet details pane for packet 1764 is expanded, showing the Ethernet II header, Internet Protocol Version 4 header, and Internet Control Message Protocol (ICMP) details, including the Echo (ping) request type, code 0, and a correct checksum.

No.	Time	Source	Destination	Protocol	Length	Info
1764	37.697499	192.168.1.106	39.156.66.18	ICMP	74	Echo (ping) request id=0x0001, seq=667/39682,
1765	37.704120	39.156.66.18	192.168.1.106	ICMP	74	Echo (ping) reply id=0x0001, seq=667/39682,
1766	38.716140	192.168.1.106	39.156.66.18	ICMP	74	Echo (ping) request id=0x0001, seq=668/39938,
1767	38.723137	39.156.66.18	192.168.1.106	ICMP	74	Echo (ping) reply id=0x0001, seq=668/39938,
1768	39.732429	192.168.1.106	39.156.66.18	ICMP	74	Echo (ping) request id=0x0001, seq=669/40194,
1769	39.739119	39.156.66.18	192.168.1.106	ICMP	74	Echo (ping) reply id=0x0001, seq=669/40194,
1771	40.749093	192.168.1.106	39.156.66.18	ICMP	74	Echo (ping) request id=0x0001, seq=670/40450,
1772	40.756723	39.156.66.18	192.168.1.106	ICMP	74	Echo (ping) reply id=0x0001, seq=670/40450,

> Frame 1764: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B601EEAA-316D-44F3-A6...}

> Ethernet II, Src: IntelCor_c0:90:40 (34:f6:4b:c0:90:40), Dst: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad)

> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 39.156.66.18

▼ Internet Control Message Protocol

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0x4ac0 [correct]

实验具体步骤

6、观察回送(Echo)请求报文，并进行分析。

ip.addr = 39.156.66.18 && icmp

No.	Time	Source	Destination	Protocol	Length	Info
1764	37.697499	192.168.1.106	39.156.66.18	ICMP	74	Echo (ping) request id=0x0001, seq=66
1765	37.704120	39.156.66.18	192.168.1.106	ICMP	74	Echo (ping) reply id=0x0001, seq=66

Internet Control Message Protocol

Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x4ac0 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 667 (0x029b)
Sequence Number (LE): 39682 (0x9b02)
[\[Response frame: 1765\]](#)

Data (32 bytes)
Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
[Length: 32]

0000 f4 2a 7d 57 29 ad 34 f6 4b c0 90 40 08 00 45 00 .*}W).-4. K..@..E.
0010 00 3c 58 56 00 00 40 01 f6 aa c0 a8 01 6a 27 9c .<XV..@.j'.
0020 42 12 08 00 4a c0 00 01 02 9b 61 62 63 64 65 66 B...J... ..abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

实验具体步骤

7、观察回送(Echo)应答报文，并进行分析。

ip.addr = 39.156.66.18 && icmp

No.	Time	Source	Destination	Protocol	Length	Info
1764	37.697499	192.168.1.106	39.156.66.18	ICMP	74	Echo (ping) request id=0x0001, seq=667/
1765	37.704120	39.156.66.18	192.168.1.106	ICMP	74	Echo (ping) reply id=0x0001, seq=667/

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x52c0 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 667 (0x029b)
Sequence Number (LE): 39682 (0x9b02)
[\[Request frame: 1764\]](#)
[Response time: 6.621 ms]

Data (32 bytes)
Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
[Length: 32]

```
0000 34 f6 4b c0 90 40 f4 2a 7d 57 29 ad 08 00 45 04 4-K-..@.* }W)...E-
0010 00 3c 58 56 00 00 34 01 02 a7 27 9c 42 12 c0 a8 -<XV..4. ...'.B...
0020 01 6a 00 00 52 c0 00 01 02 9b 61 62 63 64 65 66 -j...R... ..abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi
```

实验具体步骤

8、利用输入命令 “tracert www.baidu.com”，并记录IP地址。

```
C:\Users\zwt717>tracert www.baidu.com
```

```
通过最多 30 个跃点跟踪
```

```
到 www.a.shifen.com [39.156.66.14] 的路由:
```

1	3 ms	1 ms	1 ms	192.168.1.1
2	4 ms	4 ms	3 ms	100.109.128.1
3	6 ms	*	4 ms	211.136.66.205
4	*	*	*	请求超时。
5	*	*	*	请求超时。
6	6 ms	*	7 ms	111.13.188.114
7	7 ms	331 ms	6 ms	39.156.27.1
8	6 ms	5 ms	8 ms	39.156.67.1
9	*	*	*	请求超时。
10	*	*	*	请求超时。
11	*	*	*	请求超时。
12	*	*	6 ms	39.156.66.14

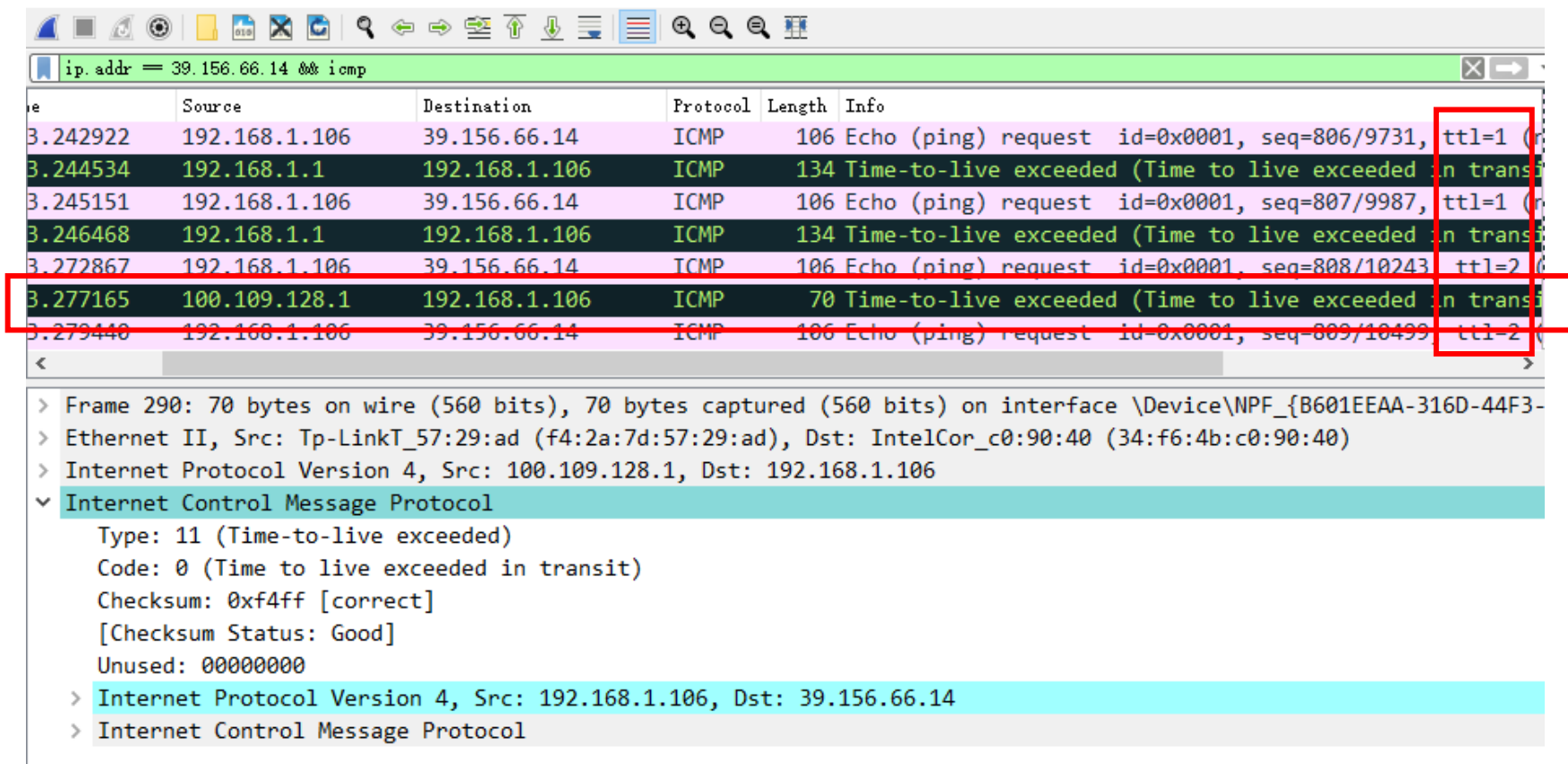
```
跟踪完成。
```

实验具体步骤

9、使用过滤表达式 “icmp” 对捕获的数据包进行初步筛选。

或：ip.addr == 39.156.66.14 && icmp （目的地IP地址）

10、从中选取一个超时报文数据包。



The screenshot shows the Wireshark network protocol analyzer interface. The filter bar at the top is set to `ip.addr == 39.156.66.14 && icmp`. The packet list pane displays several ICMP packets. The packet at offset 3.277165 is highlighted with a red box. The packet details pane shows the structure of the ICMP Time-to-live exceeded message.

Time	Source	Destination	Protocol	Length	Info
3.242922	192.168.1.106	39.156.66.14	ICMP	106	Echo (ping) request id=0x0001, seq=806/9731, ttl=1
3.244534	192.168.1.1	192.168.1.106	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
3.245151	192.168.1.106	39.156.66.14	ICMP	106	Echo (ping) request id=0x0001, seq=807/9987, ttl=1
3.246468	192.168.1.1	192.168.1.106	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
3.272867	192.168.1.106	39.156.66.14	ICMP	106	Echo (ping) request id=0x0001, seq=808/10243, ttl=2
3.277165	100.109.128.1	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
3.279440	192.168.1.106	39.156.66.14	ICMP	106	Echo (ping) request id=0x0001, seq=809/10499, ttl=2

Frame 290: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{B601EEAA-316D-44F3-...}

Ethernet II, Src: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad), Dst: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)

Internet Protocol Version 4, Src: 100.109.128.1, Dst: 192.168.1.106

Internet Control Message Protocol

- Type: 11 (Time-to-live exceeded)
- Code: 0 (Time to live exceeded in transit)
- Checksum: 0xf4ff [correct]
- [Checksum Status: Good]
- Unused: 00000000

Internet Protocol Version 4, Src: 192.168.1.106, Dst: 39.156.66.14

Internet Control Message Protocol

实验具体步骤

11、观察超时报文，并进行分析。

ip.addr = 39.156.66.14 && icmp

Time	Source	Destination	Protocol	Length	Info
3.285626	192.168.1.106	39.156.66.14	ICMP	106	Echo (ping) request id=0x0001, seq=810/10755, ttl=2
3.289240	100.109.128.1	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Internet Control Message Protocol

Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0xf4ff [correct]
[Checksum Status: Good]
Unused: 00000000

Internet Protocol Version 4, Src: 192.168.1.106, Dst: 39.156.66.14

Internet Control Message Protocol

Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf4d4 [unverified] [in ICMP error packet]
[Checksum Status: Unverified]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 810 (0x032a)
Sequence Number (LE): 10755 (0x2a03)

0000 34 f6 4b c0 90 40 f4 2a 7d 57 29 ad 08 00 45 c0 4-K-..@.* }W)...E-
0010 00 38 03 a7 00 00 fe 01 11 dd 64 6d 80 01 c0 a8 -8-.....-dm....
0020 01 6a 0b 00 f4 ff 00 00 00 00 45 00 00 5c 8d 55 -j.....-E-.\-U
0030 00 00 01 01 00 90 c0 a8 01 6a 27 9c 42 0e 08 00-j'-.B...
0040 f4 d4 00 01 03 2a*

主要内容

- 一、实验原理
- 二、实验步骤
- 三、实验结果及分析

ICMP回送(Echo)请求与应答

请求

应答

ip.addr == 39.156.66.18 && icmp						
No.	Time	Source	Destination	Protocol	Length	Info
1764	37.697499	192.168.1.106	39.156.66.18	ICMP	74	Echo
1765	37.704120	39.156.66.18	192.168.1.106	ICMP	74	Echo
Internet Control Message Protocol						
Type: 8 (Echo (ping) request)						
Code: 0						
Checksum: 0x4ac0 [correct]						
[Checksum Status: Good]						
Identifier (BE): 1 (0x0001)						
Identifier (LE): 256 (0x0100)						
Sequence Number (BE): 667 (0x029b)						
Sequence Number (LE): 39682 (0x9b02)						
[Response frame: 1765]						
Data (32 bytes)						
Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869						
[Length: 32]						
0000	f4 2a 7d 57 29 ad 34 f6 4b c0 90 40 08 00 45 00	.*}W).4. K..@..E.				
0010	00 3c 58 56 00 00 40 01 f6 aa c0 a8 01 6a 27 9c	.XV. @ . j.				
0020	42 12 08 00 4a c0 00 01 02 9b 61 62 63 64 65 66	B...J.... ..abcdef				
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv				
0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi				

ip.addr == 39.156.66.18 && icmp						
No.	Time	Source	Destination	Protocol	Length	Info
1764	37.697499	192.168.1.106	39.156.66.18	ICMP	74	Echo
1765	37.704120	39.156.66.18	192.168.1.106	ICMP	74	Echo
Internet Control Message Protocol						
Type: 0 (Echo (ping) reply)						
Code: 0						
Checksum: 0x52c0 [correct]						
[Checksum Status: Good]						
Identifier (BE): 1 (0x0001)						
Identifier (LE): 256 (0x0100)						
Sequence Number (BE): 667 (0x029b)						
Sequence Number (LE): 39682 (0x9b02)						
[Request frame: 1764]						
[Response time: 6.621 ms]						
Data (32 bytes)						
Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869						
[Length: 32]						
0000	34 f6 4b c0 90 40 f4 2a 7d 57 29 ad 08 00 45 04	4.K..@.* }W)...E.				
0010	00 3c 58 56 00 00 34 01 02 a7 27 9c 42 12 c0 a8	.<XV..4. ...'.B...				
0020	01 6a 00 00 52 c0 00 01 02 9b 61 62 63 64 65 66	.j...R.... ..abcdef				
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv				
0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi				

ICMP回送(Echo)请求

实验结果:

ip.addr == 39.156.66.18 && icmp

No.	Time	Source	Destination	Protocol	Length	Info
1764	37.697499	192.168.1.106	39.156.66.18	ICMP	74	Echo (ping) request id=0x0001, seq=66
1765	37.704120	39.156.66.18	192.168.1.106	ICMP	74	Echo (ping) reply id=0x0001, seq=66

Internet Control Message Protocol

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0x4ac0 [correct]
- [Checksum Status: Good]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence Number (BE): 667 (0x029b)
- Sequence Number (LE): 39682 (0x9b02)
- [\[Response frame: 1765\]](#)

Data (32 bytes)

Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

[Length: 32]

注: wireshark考虑到window系统与Linux系统发出的ping报文(主要指ping应用字段而非包含IP头的ping包)的字节顺序不一样(windows为LE: little-endian byte order, Linux为BE: big-endian), 为了体现wireshark的易用性, 开发者将其分别显示出来。

Offset	Hex	ASCII
0000	f4 2a 7d 57 29 ad 34 f6 4b c0 90 40 08 00 45 00	. *}W) -4. K..@..E.
0010	00 3c 58 56 00 00 40 01 f6 aa c0 a8 01 6a 27 9c	.<XV..@.j'.
0020	42 12 08 00 4a c0 00 01 02 9b 61 62 63 64 65 66	B...J... ..abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi

实验结果与分析

实验分析：

- 类型Type: 8 (Echo (ping) request), 回送请求报文类型为8
- 代码位Code: 0
- 检验和Checksum: 0x4ac0 [correct], 检验和状态：良好
- 标识符Identifier (BE): 1 (0x0001)
- 标识符Identifier (LE): 256 (0x0100)
- 序列号Sequence number (BE): 667 (0x029b)
- 序列号Sequence number (LE): 39682 (0x9b02)
- 数据Data (32 bytes) : 数据信息 (32字节)

ICMP回送(Echo) 应答

实验结果:

ip.addr == 39.156.66.18 && icmp

No.	Time	Source	Destination	Protocol	Length	Info
1764	37.697499	192.168.1.106	39.156.66.18	ICMP	74	Echo (ping) request id=0x0001, seq=667/
1765	37.704120	39.156.66.18	192.168.1.106	ICMP	74	Echo (ping) reply id=0x0001, seq=667/

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0x52c0 [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence Number (BE): 667 (0x029b)

Sequence Number (LE): 39682 (0x9b02)

[Request frame: 1764]

[Response time: 6.621 ms]

Data (32 bytes)

Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

[Length: 32]

0000 34 f6 4b c0 90 40 f4 2a 7d 57 29 ad 08 00 45 04 4-K..@.* }W)...E.

0010 00 3c 58 56 00 00 34 01 02 a7 27 9c 42 12 c0 a8 .<XV..4. ..'.B...

0020 01 6a 00 00 52 c0 00 01 02 9b 61 62 63 64 65 66 .j..R... ..abcdef

0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv

0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

实验结果与分析

实验分析：

- 类型Type: 0 (Echo (ping) reply), 回送应答报文类型为0
- 代码位Code: 0
- 检验和Checksum: 0x52c0 [correct], 检验和状态：良好
- 标识符Identifier (BE): 1 (0x0001), 和请求报文的标识符一致
- 标识符Identifier (LE): 256 (0x0100), 和请求报文的标识符一致
- 序列号Sequence number (BE): 667 (0x029b), 和请求报文的序列号一致
- 序列号Sequence number (LE): 39682 (0x9b02), 和请求报文的序列号一致
- 数据Data (32 bytes) : 数据信息 (32字节), 和请求报文的数据信息一样

实验结果与分析

绘制回送(Echo)请求报文格式:

Type: 8 (Echo (ping) request)	Code: 0	Checksum: 0x4ac0 [correct]
Identifier (BE): 1 (0x0001) Identifier (LE): 256 (0x0100)		Sequence number (BE): 667 (0x029b) Sequence number (LE): 39682 (0x9b02)
Data:6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869		

绘制回送(Echo)应答报文格式:

Type: 0 (Echo (ping) reply)	Code: 0	Checksum: 0x52c0 [correct]
Identifier (BE): 1 (0x0001) Identifier (LE): 256 (0x0100)		Sequence number (BE): 667 (0x029b) Sequence number (LE): 39682 (0x9b02)
Data:6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869		

ICMP超时报文

实验结果：

ip. addr = 39.156.66.14 icmp					
Time	Source	Destination	Protocol	Length	Info
3.285626	192.168.1.106	39.156.66.14	ICMP	106	Echo (ping) request id=0x0001, seq=810/10755, ttl=2 (
3.289240	100.109.128.1	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transi

> Ethernet II, Src: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad), Dst: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)
> Internet Protocol Version 4, Src: 100.109.128.1, Dst: 192.168.1.106
v Internet Control Message Protocol

Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0xf4ff [correct]
[Checksum Status: Good]
Unused: 00000000



ICMP报文首部的前8个字节；
类型字段为11，表示此报文为超时报文。

> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 39.156.66.14



原始IP数据报的首部

v Internet Control Message Protocol

Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf4d4 [unverified] [in ICMP error packet]
[Checksum Status: Unverified]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 810 (0x032a)
Sequence Number (LE): 10755 (0x2a03)



原始IP数据报数据字段的前8个字节。由于原始数据报内的数据是上一个ICMP的报文，因此此处就是上一个ICMP报文首部的前8个字节。

```
0000 34 f6 4b c0 90 40 f4 2a 7d 57 29 ad 08 00 45 c0 4 -K...@.* }W)...E-
0010 00 38 03 a7 00 00 fe 01 11 dd 64 6d 80 01 c0 a8 .8.....dm....
0020 01 6a 0b 00 f4 ff 00 00 00 00 45 00 00 5c 8d 55 .j.....E..U
0030 00 00 01 01 00 90 c0 a8 01 6a 27 9c 42 0e 08 00 .....j'.B...
```


实验结果与分析

实验分析：

- 类型Type: 11 (Time-to-live exceeded) , 超时报文类型为 11
- 代码位Code: 0 (Time to live exceeded in transit)
- 检验和Checksum: 0xf4ff [correct], 检验和状态：良好
- 未使用字段Unused: 00000000
- 原始IP数据报的首部：IPv4数据报首部，20字节
- 原始IP数据报数据字段的前8个字节： ICMP回送请求报文的前8个字节。

实验结果与分析

绘制ICMP超时报文格式:

Type: 11 (Time-to-live exceeded)	Code: 0 (Time to live exceeded in transit)	Checksum: 0xf4ff [correct]
全0		
<p>Data:</p> <p>原始IP数据报的首部: Internet Protocol Version 4, Src: 192.168.1.106, Dst: 39.156.66.14</p> <p>原始IP数据报数据字段的前8个字节: Internet Control Message Protocol</p> <p>Type: 8 (Echo (ping) request)</p> <p>Code: 0</p> <p>Checksum: 0xf4d4 [unverified] [in ICMP error packet]</p> <p>[Checksum Status: Unverified]</p> <p>Identifier (BE): 1 (0x0001)</p> <p>Identifier (LE): 256 (0x0100)</p> <p>Sequence Number (BE): 810 (0x032a)</p> <p>Sequence Number (LE): 10755 (0x2a03)</p>		

实验说明（目的地不可达报文）

由于校内网管理员可能会对默认网关进行特殊设置，导致默认网关拒绝转发回送请求报文，并向主机返回目的地不可达报文。同学们可根据实际的实验情况，将实验步骤7往后的实验替换为，观察目的地不可达报文，并进行分析。目的地不可达报文与超时报文同属于差错报告报文，分析方法相同。

```
7672 327.334531 172.18.3.66 182.61.200.6 ICMP 74 Echo (ping) request id=0x0001, seq=0x00000001
7673 327.336885 172.18.3.254 172.18.3.66 ICMP 70 Destination unreachable (Communication failure)
7676 328.338600 172.18.3.66 182.61.200.6 ICMP 74 Echo (ping) request id=0x0001, seq=0x00000001

> Frame 7664: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{210F48BF-F314-4319-AA
> Ethernet II, Src: Cisco_03:d8:c4 (00:16:c7:03:d8:c4), Dst: LiteON_f9:bb:66 (6c:4b:90:f9:bb:66)
> Internet Protocol Version 4, Src: 172.18.3.254, Dst: 172.18.3.66
▼ Internet Control Message Protocol
  Type: 3 (Destination unreachable)
  Code: 13 (Communication administratively filtered)
  Checksum: 0xa796 [correct]
  [Checksum Status: Good]
  Unused: 00000000
> Internet Protocol Version 4, Src: 172.18.3.66, Dst: 182.61.200.6
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4d4a [unverified] [in ICMP error packet]
  [Checksum Status: Unverified]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 17 (0x0011)
  Sequence Number (LE): 4352 (0x1100)
```

实验要求

◆ 本次实验二选一：

- 回送请求报文+回送应答报文+ICMP超时报文；
- 回送请求报文+ICMP目的地不可达报文。

思考题

思考题：抓取ICMPv6报文，观察其报文格式与ICMP报文是否不同。

