

学号：	姓名：	班级：
实验题目： 实验八 ICMP		
实验学时：2h	实验日期： 2023. 04. 17	
实验目的： 学习 ICMP 的相关内容		
硬件环境： Windows10 家庭版		
软件环境： Wireshark		
实验步骤与内容： 实验内容： <ol style="list-style-type: none"> 1. What is the IP address of your host? What is the IP address of the destination host? 2. Why is it that an ICMP packet does not have source and destination port numbers? 3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields? 4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields? 5. What is the IP address of your host? What is the IP address of the target destination host? 6. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be? 7. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so? 8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields? 9. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different? 10. Within the tracert measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in Figure 4, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this 		

link?

实验步骤:

先在 CMD 命令行中输入 `ping -n 10 www.ust.hk` 表示向香港科技大学的 Web 服务器发送 10 个查询数据包, 之后再输入 `tracert www.inria.fr` 表示跟踪路由。

```
C:\Users\sdu.wzl>ping -n 10 www.ust.hk

正在 Ping www.ust.hk [143.89.12.134] 具有 32 字节的数据:
来自 143.89.12.134 的回复: 字节=32 时间=54ms TTL=47
来自 143.89.12.134 的回复: 字节=32 时间=54ms TTL=47
来自 143.89.12.134 的回复: 字节=32 时间=56ms TTL=47
来自 143.89.12.134 的回复: 字节=32 时间=56ms TTL=47
来自 143.89.12.134 的回复: 字节=32 时间=54ms TTL=47
来自 143.89.12.134 的回复: 字节=32 时间=54ms TTL=47
来自 143.89.12.134 的回复: 字节=32 时间=55ms TTL=47
来自 143.89.12.134 的回复: 字节=32 时间=54ms TTL=47
来自 143.89.12.134 的回复: 字节=32 时间=54ms TTL=47
来自 143.89.12.134 的回复: 字节=32 时间=55ms TTL=47
```

1. 本机的 IP 地址为 172.25.193.66, 目标主机的 IP 地址为 143.89.12.134。

738	13.681...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
746	13.736...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply
802	14.697...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
808	14.751...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply
849	15.714...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
852	15.770...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply
909	16.724...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
912	16.780...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply
966	17.728...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
967	17.783...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply
1016	18.743...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
1017	18.797...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply
1053	19.759...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
1058	19.814...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply
1109	20.771...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request

2. ICMP 包没有源端口号和目的端口号, 因为它设计的目的在于主机和路由器之间交换网络层信息, 而不是在应用层进程之间交换信息。传输层才有端口号的概念, ICMP 报文仅传送到主机。

3. ICMP 类型为 8, 代码编号为 0, ICMP 数据包还具有 Checksum、Identifier、Sequence Number 和 Data 字段, 其中校验和、序列号和标识符字段各两个字节。

738	13.681...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
746	13.736...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply
802	14.697...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
808	14.751...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply
849	15.714...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
852	15.770...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply
909	16.724...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
912	16.780...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply
966	17.728...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
967	17.783...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply
1016	18.743...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
1017	18.797...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply
1053	19.759...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
1058	19.814...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply
1109	20.771...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
1114	20.826...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply

> Frame 738: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF...
 > Ethernet II, Src: LiteonTe_1f:d7:61 (14:5a:fc:1f:d7:61), Dst: JuniperN_f6:12:a0 (28:a2:4b:f6:12:a0)
 > Internet Protocol Version 4, Src: 172.25.193.66, Dst: 143.89.12.134
 > Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0x4d54 [correct]
 [Checksum Status: Good]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence Number (BE): 7 (0x0007)
 Sequence Number (LE): 1792 (0x0700)
 [\[Response frame: 746\]](#)
 > Data (32 bytes)

4. ICMP 类型为 0, 代码编号为 0, ICMP 数据包还具有 Checksum、Identifier、Sequence Number 和 Data 字段, 其中校验和、序列号和标识符字段各两个字节。

746	13.736...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply
802	14.697...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
808	14.751...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply
849	15.714...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
852	15.770...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply
909	16.724...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
912	16.780...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply
966	17.728...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
967	17.783...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply
1016	18.743...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
1017	18.797...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply
1053	19.759...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
1058	19.814...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply
1109	20.771...	172.25.193.66	143.89.12.134	ICMP	74 Echo (ping) request
1114	20.826...	143.89.12.134	172.25.193.66	ICMP	74 Echo (ping) reply

> Frame 746: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF...
 > Ethernet II, Src: JuniperN_f6:12:a0 (28:a2:4b:f6:12:a0), Dst: LiteonTe_1f:d7:61 (14:5a:fc:1f:d7:61)
 > Internet Protocol Version 4, Src: 143.89.12.134, Dst: 172.25.193.66
 > Internet Control Message Protocol
 Type: 0 (Echo (ping) reply)
 Code: 0
 Checksum: 0x5554 [correct]
 [Checksum Status: Good]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence Number (BE): 7 (0x0007)
 Sequence Number (LE): 1792 (0x0700)
 [\[Request frame: 738\]](#)
 [Response time: 54.589 ms]
 > Data (32 bytes)


```

C:\Windows\system32\cmd.exe
C:\Users\sdu.wzl>tracert www.inria.fr

通过最多 30 个跃点跟踪
到 www.inria.fr [128.93.162.83] 的路由:

 1  1 ms    1 ms    1 ms    192.168.250.250
 2  3 ms    3 ms    1 ms    192.168.249.178
 3  1 ms    1 ms    1 ms    192.168.249.201
 4  11 ms   10 ms   11 ms   58.194.164.65
 5  10 ms   10 ms   10 ms   58.194.164.77
 6  *      *      *      请求超时。
 7  11 ms   11 ms   11 ms   202.194.96.213
 8  11 ms   11 ms   14 ms   101.4.115.33
 9  16 ms   15 ms   16 ms   101.4.116.118
10  17 ms   17 ms   17 ms   101.4.112.69
11  *      *      16 ms   101.4.118.214
12  18 ms   26 ms   17 ms   210.25.189.65
13  21 ms   18 ms   17 ms   210.25.187.50
14  253 ms  244 ms  245 ms  orientplus-gw.mxl.lon.uk.geant.net [62.40.125.101]
15  244 ms  244 ms  244 ms  ae2.mxl.lon2.uk.geant.net [62.40.98.65]
16  251 ms  251 ms  251 ms  ae8.mxl.par.fr.geant.net [62.40.98.107]
17  259 ms  260 ms  261 ms  renater-lbl-gw.mxl.par.fr.geant.net [62.40.124.70]
18  *      *      *      请求超时。
19  *      *      *      请求超时。
20  *      *      *      请求超时。
21  263 ms  264 ms  267 ms  193.55.200.26
22  287 ms  277 ms  279 ms  xe1-0-6-marseille1-rtr-131.noc.renater.fr [193.51.177.184]
23  256 ms  257 ms  258 ms  xe-1-1-7-ren-nr-lyon1-rtr-131.noc.renater.fr [193.55.204.111]
24  256 ms  259 ms  258 ms  et-3-1-7-ren-nr-paris1-rtr-131.noc.renater.fr [193.51.180.166]
25  279 ms  280 ms  280 ms  tel-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
26  265 ms  265 ms  270 ms  inria-roquencourt-gi3-2-inria-rtr-021.noc.renater.fr [193.51.184.177]
27  275 ms  276 ms  268 ms  unit240-reth1-vfw-ext-dcl.inria.fr [192.93.122.19]
28  266 ms  265 ms  267 ms  prod-inriafr-cms.inria.fr [128.93.162.83]

```

5. 主机 IP 地址是 172.25.193.66，目标 IP 地址是 128.93.162.83。

No.	Time	Source	Destination	Protocol	Len
734	13.732...	172.25.193.66	128.93.162.83	ICMP	
735	13.733...	192.168.250.250	172.25.193.66	ICMP	
736	13.734...	172.25.193.66	128.93.162.83	ICMP	
737	13.735...	192.168.250.250	172.25.193.66	ICMP	
738	13.735...	172.25.193.66	128.93.162.83	ICMP	
739	13.737...	192.168.250.250	172.25.193.66	ICMP	
1266	23.783...	172.25.193.66	128.93.162.83	ICMP	
1267	23.786...	192.168.249.178	172.25.193.66	ICMP	
1268	23.786...	172.25.193.66	128.93.162.83	ICMP	
1269	23.790...	192.168.249.178	172.25.193.66	ICMP	
1270	23.790...	172.25.193.66	128.93.162.83	ICMP	
1271	23.791...	192.168.249.178	172.25.193.66	ICMP	
1776	33.851...	172.25.193.66	128.93.162.83	ICMP	
1777	33.853...	192.168.249.201	172.25.193.66	ICMP	
1778	33.853...	172.25.193.66	128.93.162.83	ICMP	
1779	33.855...	192.168.249.201	172.25.193.66	ICMP	

> Frame 734: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
 > Ethernet II, Src: LiteonTe_1f:d7:61 (14:5a:fc:1f:d7:61), Dst: Juniper_08:00:27:00:00:00
 > Internet Protocol Version 4, Src: 172.25.193.66, Dst: 128.93.162.83
 > Internet Control Message Protocol

6. 不是，ICMP 如果发送了 UDP 数据包，那么 IP 协议号应为 11（十六进制数），因为 UDP 协议号是 11（十六进制数）。

7. ICMP 响应数据包与 ICMP ping 查询数据包中包含的字段是相同，但响应数据包中的类型是 0，而查询数据包的类型是 8。

ICMP 响应数据包：

112...	217.97...	128.93.162.83	172.25.193.66	ICMP	106	Echo (ping) reply	id=0x0001, seq=98/25088, ttl=40
112...	217.98...	172.25.193.66	128.93.162.83	ICMP	106	Echo (ping) request	id=0x0001, seq=99/25344, ttl=28
112...	218.24...	128.93.162.83	172.25.193.66	ICMP	106	Echo (ping) reply	id=0x0001, seq=99/25344, ttl=40
112...	218.24...	172.25.193.66	128.93.162.83	ICMP	106	Echo (ping) request	id=0x0001, seq=100/25600, ttl=28
112...	218.51...	128.93.162.83	172.25.193.66	ICMP	106	Echo (ping) reply	id=0x0001, seq=100/25600, ttl=40

> Frame 11252: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NP ^	0000	14	5a
> Ethernet II, Src: JuniperN_f6:12:a0 (28:a2:4b:f6:12:a0), Dst: LiteonTe_1f:d7:61 (14:5a:fc:1f:d7:61)	0010	00	5c
> Internet Protocol Version 4, Src: 128.93.162.83, Dst: 172.25.193.66	0020	c1	42
▼ Internet Control Message Protocol	0030	00	00
Type: 0 (Echo (ping) reply)	0040	00	00
Code: 0	0050	00	00
Checksum: 0xff9c [correct]	0060	00	00
[Checksum Status: Good]			
Identifier (BE): 1 (0x0001)			
Identifier (LE): 256 (0x0100)			
Sequence Number (BE): 98 (0x0062)			
Sequence Number (LE): 25088 (0x6200)			
[Request frame: 11231]			
[Response time: 265.829 ms]			
▼ Data (64 bytes)			

ICMP ping 查询数据包：

738	13.681...	172.25.193.66	143.89.12.134	ICMP	74	Echo (ping) request
746	13.736...	143.89.12.134	172.25.193.66	ICMP	74	Echo (ping) reply
802	14.697...	172.25.193.66	143.89.12.134	ICMP	74	Echo (ping) request
808	14.751...	143.89.12.134	172.25.193.66	ICMP	74	Echo (ping) reply
849	15.714...	172.25.193.66	143.89.12.134	ICMP	74	Echo (ping) request
852	15.770...	143.89.12.134	172.25.193.66	ICMP	74	Echo (ping) reply
909	16.724...	172.25.193.66	143.89.12.134	ICMP	74	Echo (ping) request
912	16.780...	143.89.12.134	172.25.193.66	ICMP	74	Echo (ping) reply
966	17.728...	172.25.193.66	143.89.12.134	ICMP	74	Echo (ping) request
967	17.783...	143.89.12.134	172.25.193.66	ICMP	74	Echo (ping) reply
1016	18.743...	172.25.193.66	143.89.12.134	ICMP	74	Echo (ping) request
1017	18.797...	143.89.12.134	172.25.193.66	ICMP	74	Echo (ping) reply
1053	19.759...	172.25.193.66	143.89.12.134	ICMP	74	Echo (ping) request
1058	19.814...	143.89.12.134	172.25.193.66	ICMP	74	Echo (ping) reply
1109	20.771...	172.25.193.66	143.89.12.134	ICMP	74	Echo (ping) request
1114	20.826...	143.89.12.134	172.25.193.66	ICMP	74	Echo (ping) reply

> Frame 738: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NP ^
> Ethernet II, Src: LiteonTe_1f:d7:61 (14:5a:fc:1f:d7:61), Dst: JuniperN_f6:12:a0 (28:a2:4b:f6:12:a0)
> Internet Protocol Version 4, Src: 172.25.193.66, Dst: 143.89.12.134
▼ Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x4d54 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 7 (0x0007)
Sequence Number (LE): 1792 (0x0700)
[Response frame: 746]
▼ Data (22 bytes)

8. 比正常的响应数据包多了 ICMP 请求数据包的内容
错误 ICMP 数据包

11150	216.97...	192.93.122.19	172.25.193.66	ICMP	70 Time-to-live exceeded
11231	217.71...	172.25.193.66	128.93.162.83	ICMP	106 Echo (ping) request i
11252	217.97...	128.93.162.83	172.25.193.66	ICMP	106 Echo (ping) reply i
11253	217.98...	172.25.193.66	128.93.162.83	ICMP	106 Echo (ping) request i
11274	218.24...	128.93.162.83	172.25.193.66	ICMP	106 Echo (ping) reply i
11275	218.24...	172.25.193.66	128.93.162.83	ICMP	106 Echo (ping) request i
11291	218.51...	128.93.162.83	172.25.193.66	ICMP	106 Echo (ping) reply i

> Frame 11150: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\N

> Ethernet II, Src: JuniperN_f6:12:a0 (28:a2:4b:f6:12:a0), Dst: LiteonTe_1f:d7:61 (14:5a:fc:1f:1

> Internet Protocol Version 4, Src: 192.93.122.19, Dst: 172.25.193.66

✓ 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: 172.25.193.66, Dst: 128.93.162.83

✓ Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0xf79d [unverified] [in ICMP error packet]

[Checksum Status: Unverified]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence Number (BE): 97 (0x0061)

Sequence Number (LE): 24832 (0x6100)

原始 ICMP 数据包

11127	216.70...	192.93.122.19	172.25.193.66	ICMP	70 Time-to-live exceeded
11128	216.70...	172.25.193.66	128.93.162.83	ICMP	106 Echo (ping) request i
11150	216.97...	192.93.122.19	172.25.193.66	ICMP	70 Time-to-live exceeded
11231	217.71...	172.25.193.66	128.93.162.83	ICMP	106 Echo (ping) request i
11252	217.97...	128.93.162.83	172.25.193.66	ICMP	106 Echo (ping) reply i
11253	217.98...	172.25.193.66	128.93.162.83	ICMP	106 Echo (ping) request i
11274	218.24...	128.93.162.83	172.25.193.66	ICMP	106 Echo (ping) reply i
11275	218.24...	172.25.193.66	128.93.162.83	ICMP	106 Echo (ping) request i
11291	218.51...	128.93.162.83	172.25.193.66	ICMP	106 Echo (ping) reply i

> Frame 11128: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device

> Ethernet II, Src: LiteonTe_1f:d7:61 (14:5a:fc:1f:d7:61), Dst: JuniperN_f6:12:a0 (28:a2:4b:f6:1

> Internet Protocol Version 4, Src: 172.25.193.66, Dst: 128.93.162.83

✓ Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0xf79d [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence Number (BE): 97 (0x0061)

Sequence Number (LE): 24832 (0x6100)

> [No response seen]

> Data (64 bytes)

9. 最后三个 ICMP 数据包的消息类型是 0，之前错误数据包的类型是 11，这是因为 ICMP 查询数据包的 TTL 是逐渐递增的，最后的 ICMP 的查询数据包的 TTL 已经大于到达目的地的路由跃点数，所以不会被目标主机丢弃。

10.

```
12  18 ms   26 ms   17 ms  210.25.189.65
13  21 ms   18 ms   17 ms  210.25.187.50
14  253 ms  244 ms  245 ms  orientplus-gw.mx1.lon.uk.geant.net [62.40.125.101]
15  244 ms  244 ms  244 ms  ae2.mx1.lon2.uk.geant.net [62.40.98.65]
16  251 ms  251 ms  251 ms  ae8.mx1.par.fr.geant.net [62.40.98.107]
17  259 ms  260 ms  261 ms  renater-lbl-gw.mx1.par.fr.geant.net [62.40.124.70]
```

其中 IP 地址为 210.25.187.50 在北京，IP 地址为 62.40.125.101 在英国伦敦。

IP地址查询

本服务由百度智能云和埃文科技联合提供

210.25.187.50

免费查询

IPv4 : 210.25.187.50

归属地: 中国 北京市 --

运营商: 中国教育网

邮编: 100005

区号: 110000

IP地址查询

本服务由百度智能云和埃文科技联合提供

62.40.125.101

免费查询

IPv4 : 62.40.125.101

归属地: 英国 伦敦 --

运营商: IP allocation for GEANT
network infrastructure

邮编: WC2B 5QZ

区号: --

结论分析与体会:

通过本次实验，对网络层有了进一步的了解，先是使用 ping 向目标 IP 地址发送数据包，再对路由进行跟踪，通过本实验对 ICMP 数据包有了更清楚的认知。