暨南大学本科实验报告专用纸

课程名称 《计算机网络实验》 成绩评定

实验项目名称 计算机网络协议分析 指导教师 雷小林 、魏林锋

实验项目编号 实验项目类型 综合 实验地点 N117

学生姓名 陈宇 学号 2020101642

学院 信息科学技术学院 系 计算机系 专业 软件工程

实验时间 2022 年 10 月 11 日下 午～10 月 11 日下午 温度 ℃湿度

实验目的

1.掌握 icmp 协议的报文格式

2.理解不同类型 icmp 报文的具体意义

3.了解常见的网络故障

实验原理

1.ICMP 协议介绍

ICMP（Internet Control Message Protocol）是因特网控制报文协议[RFC792]的缩写，是因特网的标准协议。ICMP 允许路由器或主机报告差错情况和提供有关信息，用以调试、监视网络。

（1）ICMP 的报文格式

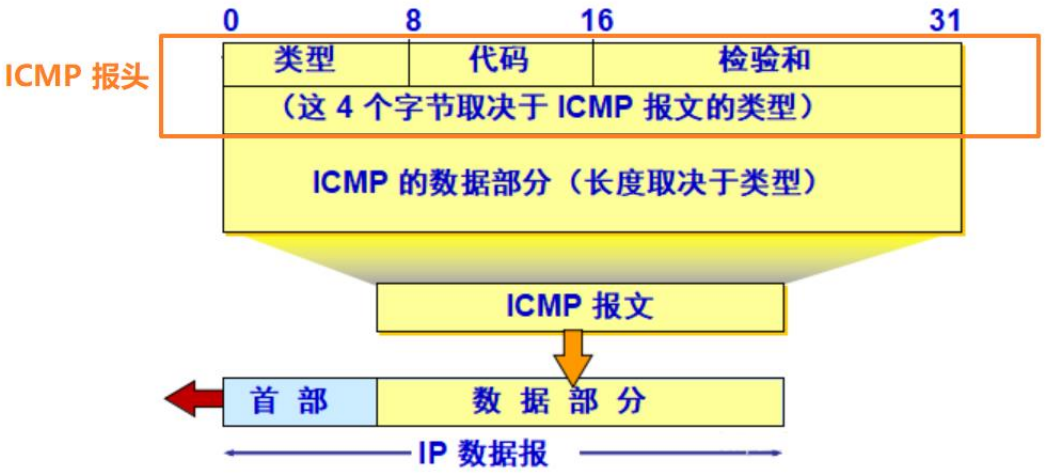


图 20　ICMP 回送请求和应答报文格式

在网络中，ICMP 报文将封装在 IP 数据报中进行传输。由于 ICMP 的报文类型很多，且又有各自的代码，因此，ICMP 并没有一个统一的报文格式供全部 ICMP 信息使用，不同的 ICMP 类别分别有不同的报文字段。

ICMP 报文只在前 4 个字节有统一的格式，即类型、代码和校验和 3 个字段。接着的 4 个字节的内容与 ICMP 报文类型有关。图 20 描述了 ICMP 的回送请求和应答报文格式，ICMP 报文分为首部和数据区两大部分。其中：

* 类型：一个字节，表示 ICMP 消息的类型，内容参见表 5；

* 代码：一个字节，用于进一步区分某种类型的几种不同情况；

* 校验和：两个字节，提供对整个 ICMP 报文的校验和；

表 5 ICMP 消息及类型码

类型	代码	说明	种类
0	0	回送回答。与回送请求成对被 ping 命令使用	信息查询
3		终点不可达	错误通知
	0	网络不可达	
	1	主机不可达	
	2	协议不可达	
	3	端口不可达	
	4	需要分片，但该数据包的 DF（不要分片）已设置	
	5	源点路由选择不能完成	
	6	目的网络未知	
	7	目的主机未知	
	8	源主机是孤立的	
	9	从管理上禁止与目的网络通信	
	10	从管理上禁止与目的主机通信	
	11	对指定的服务类型，网络不可达	
	12	对指定的服务类型，主机不可达	
	13	主机不可达，因为管理机构已经在该主机上放置了过滤器（由 RFC1812 追加）	
	14	主机不可达，因为主机的优先级被违背了（由 RFC1812 追加）	
	15	主机不可达，因为主机的优先级被删除了（由 RFC1812 追加）	
4	0	源点抑制。通知送信方抑制发送数据包	错误通知
5		改变路由	错误通知
	0	对特定网络路由的改变	
	1	对特定主机路由的改变	
	2	基于指明的服务类型对特定网络路由的改变	
	3	基于指明的服务类型对特定主机路由的改变	
6	0	回送请求。与回送回答成对被 ping 命令使用	信息查询
9		路由器通告（由 RFC1256 追加）	信息查询
	0	一般路由器通告（路由器向自己身边通告自己的存在）。	
	1	不能转发一般流量（由 RFC2002 追加）	
10	0	路由器询问（由 RFC1256 追加）	信息查询
11		超时	错误通知
	0	传送中生存时间变为了 0。被 traceroute 命令利用	
	1	规定时间内没有收到所有的分片	
12		参数问题	错误通知
	0	在 IP 首部的某个字段中有差错或两义性	
	1	缺少所需的选项部分（由 RFC1108 追加）	
	2	长度不对	
13	0	时间戳请求	信息查询
14	0	时间戳回答	信息查询

(2) ICMP 的报文类型

ICMP 报文的种类可以分为 ICMP 差错报告报文和 ICMP 询问报文两种，表 5 列出了已定义的几种 ICMP 消息。

其中差错报告报文主要有目的站点不可达、源站点抑制、超时、参数问题和路由重定向 5 种；ICMP 询问报文有回送请求和应答、时间戳请求和应答、地址掩码请求和应答以及路由器询问和通告 4 种。

(3) ICMP 常见的消息类型

下面介绍几种常用的 ICMP 消息类型。

* 目的站点不可达（3）

产生 “目的站点不可达”的原因有多种。在路由器不知道如何到达目的网络、数据报指定的源路由不稳定、路由器必须将一个设置了不可分段标志的数据报分段等情况下，路由器都会返回此消息。如果由于指明的协议模块或进程端口未被激活而导致目的主机的 IP 不能传送数据报，这时目的主机也会向源主机发送 “目的站点不可达”的消息。

为了进一步区分同一类型信息中的几种不同情况，在 ICMP 报文格式中引入了代码字段，该类型常见信息代码及其意义如下：

表 6 ICMP 类型 3 的常见代码

代码	描述	处理	代码	描述	处理
0	网络不可达；	无路由到达主机	1	主机不可达；	无路由到达主机
2	协议不可用；	连接被拒绝	3	端口不可达；	连接被拒绝
4	需分段但 DF 值为 0；	报文太长	5	源路由失败；	无路由到达主机

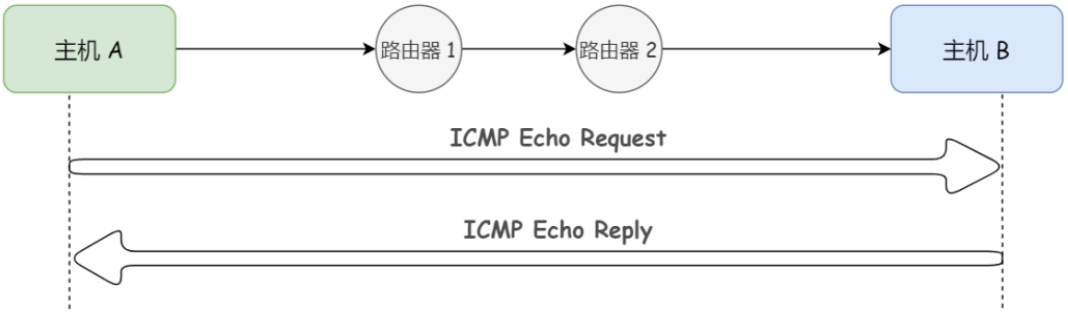
* 源站点抑制 （4）

此消息类型提供了流控制的一种基本形式。当数据报到达得太快，路由器或主机来不及处理时，这些数据报就必须被丢弃。丢弃数据报的计算机就会发一条 “源站点抑制”的 ICMP 报文。“源站点抑制”消息的接收者就会降低向该消息发送站点发送数据报的速度。

* 回送请求 （8）和回送应答 （0）

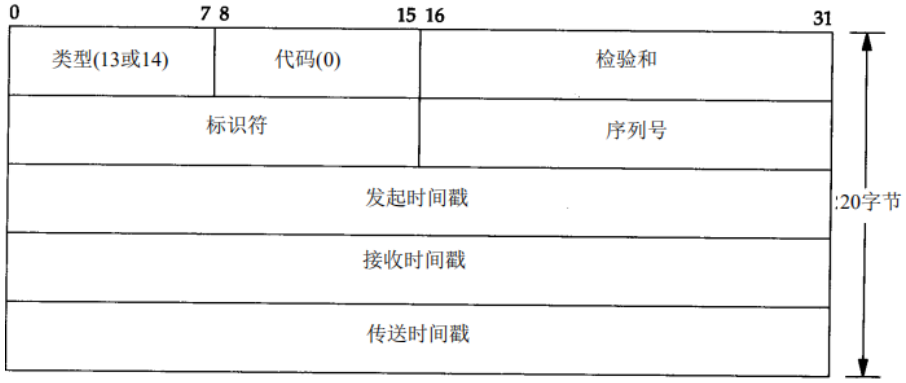
这两种 ICMP 消息提供了一种用于确定两台计算机之间是否可以进行通信

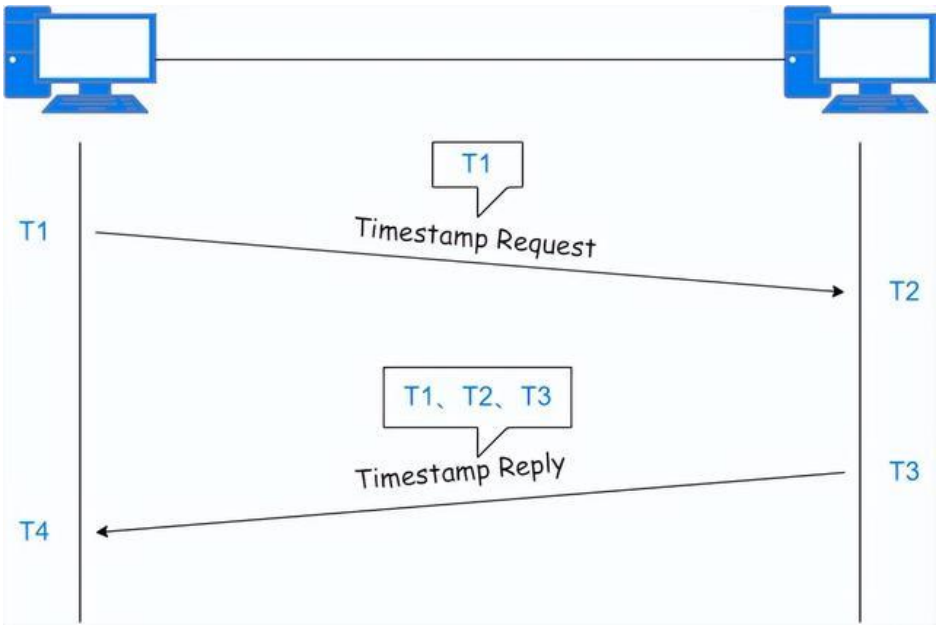
的机制。当一个主机或路由器向一个特定的目的主机发出 ICMP 回送请求报文时，该报文的接收者应当向源主机发送 ICMP 回送应答报文。



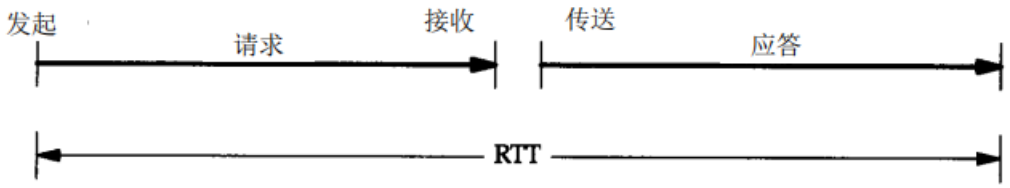
* 时间戳请求 （15）和时间戳应答 （16）

这两种消息提供了一种对网络延迟进行取样的机制。时间戳请求的发送者在其报文的信息字段中写入发送消息的时间。接收者在发送时间戳之后添加一个接收时间戳，并作为时间戳应答消息报文返回。





请求端填写发起时间戳，然后发送报文。应答系统收到请求报文时填写接收时间戳，在发送应答时填写发送时间戳。但是，实际上，大多数的实现把后面两个字段都设成相同的值(提供三个字段的原因是可以让发送方分别计算发送请求的时间和发送应答的时间)。



上图中往返时间（RTT）的值是收到应答时的时间值减去发送请求时的时间值。发送方和接收方的偏差值是接收时间戳值减去发起时间戳值。如果我们相信 RT T 的值，并且相信 RTT 的一半用于请求报文的传输，另一半用于应答报文的传输，那么为了使本机时钟与查询主机的时钟一致，本机时钟需要进行调整，调整值是发送方和接收方之间的偏差值减去 RTT 的一半。

* 地址掩码请求 （17）和地址掩码应答 （18）

主机可以用 “地址掩码请求”消息来查找其所连接网络的子网掩码。主机在网络上广播

请求，并等待路由器的包含子网掩码的 “地址掩码应答”消息报文的到来。

* 超时报告 （11）

当一个数据报的 TTL 值到达 0 时，路由器将会给源主机发送超时报文。

2.基于 ICMP 的应用程序

目前网络中常用的基于 ICMP 的应用程序主要有 ping 命令和 tracert 命令。

（1）ping 命令

Ping 命令是调试网络常用的工具之一。它通过发出 ICMP Echo 请求报文并监听其回应来检测网络的连通性。图 21 显示了 Wireshark 捕获的 ICMP Echo 请求报文和应答报文。

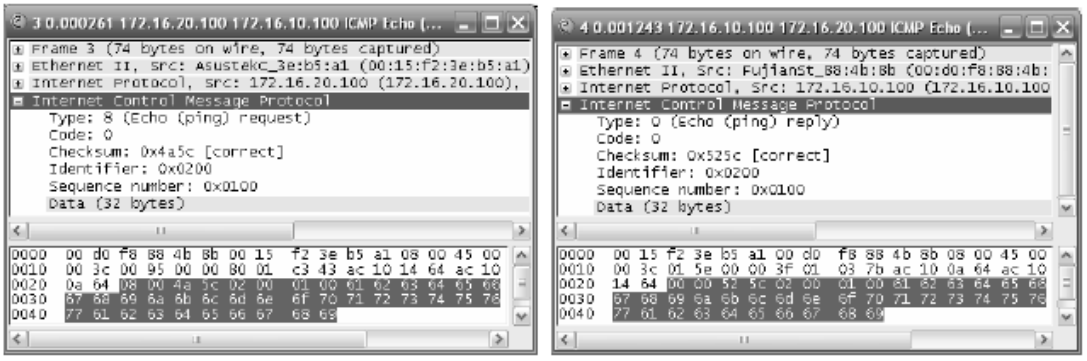


图 21 ICMP Echo 请求报文和应答报文

Ping 命令只有在安装了 TCP/IP 协议之后才可以使用，其命令格式如下：

ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count]

[[-j host-list] | [-k host-list]] [-w timeout] target_name

这里对实验中可能用到的参数解释如下：

* -t ： 用户所在主机不断向目标主机发送回送请求报文，直到用户中断；

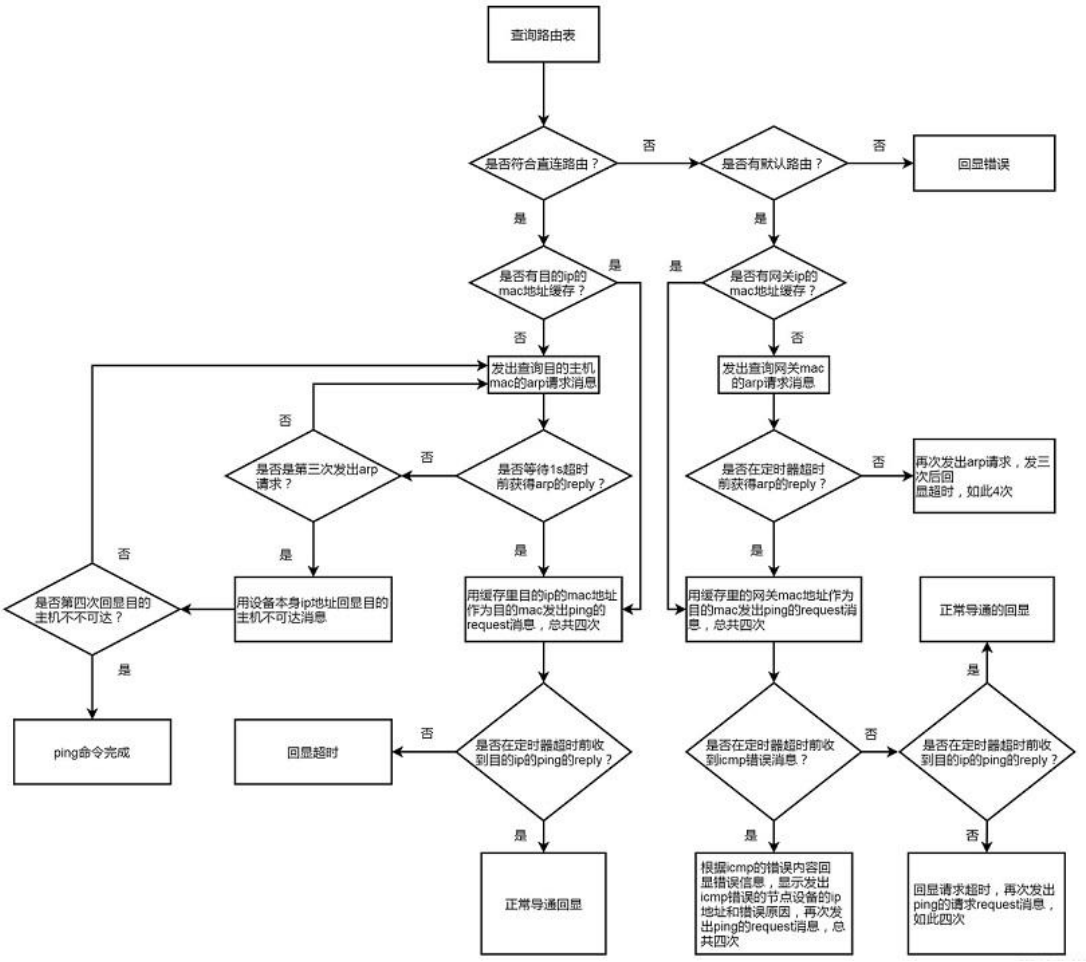
* -n count：指定要 Ping 多少次，具体次数由后面的 count 来指定 ， 缺省值为 4；

* -l size：指定发送到目标主机的数据包的大小 ， 默认为 32 字节，最大值是 65,527；

* -w timeout：指定超时间隔，单位为毫秒；

* target_name：指定要 ping 的远程计算机。

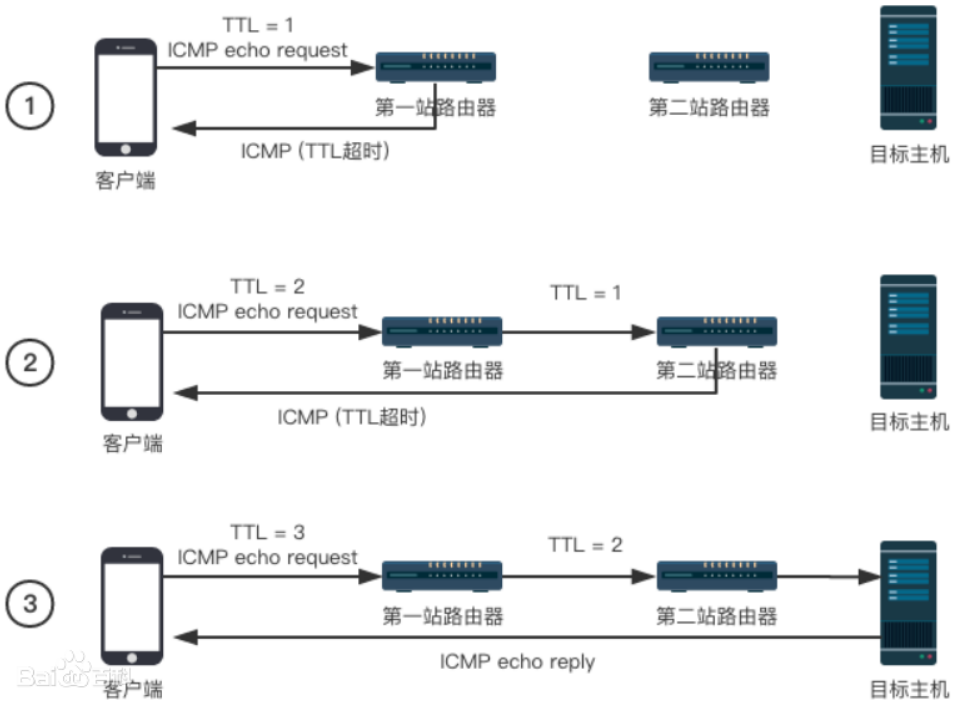
ping 的过程流程图如下：



(2) Traceroute 命令

Traceroute 命令用来获得从本地计算机到目的主机的路径信息。在 MS Windows 中该命令为 Tracert，而 UNIX 系统中为 Traceroute。

Tracert 先发送 TTL 为 1 的回显请求报文，并在随后的每次发送过程将 TTL 递增 1，直到目标响应或 TTL 达到最大值，从而确定路由。它所返回的信息要比 ping 命令详细得多，它把您送出的到某一站点的请求包，所走的全部路由均告诉您，并且告诉您通过该路由的 IP 是多少，通过该 IP 的时延是多少。



Tracert 命令同样要在安装了 TCP/IP 协议之后才可以使用，其命令格式为：tracert [-d] [-h maximum_hops] [-j computer-list] [-w timeout] target_name

参数含义为：

* -d：不解析目标主机的名称；

* -h：指定搜索到目标地址的最大跳跃数；

* -j：按照主机列表中的地址释放源路由；

* -w：指定超时时间间隔，程序默认的时间单位是毫秒。

实验环境与说明

1.实验目的

掌握 ping 和 tracert 命令的使用方法，了解 ICMP 协议报文类型及其作用。

执行 ping 和 tracert 命令，分别截获报文，分析截获的 ICMP 报文类型和 ICMP 报文格式，理解 ICMP 协议的作用。

2.实验设备和连接

实验设备和连接图如图 22 所示，一台锐捷 R1760 路由器连接 2 台 PC 机，分别命名为 主机 A、主机 B。

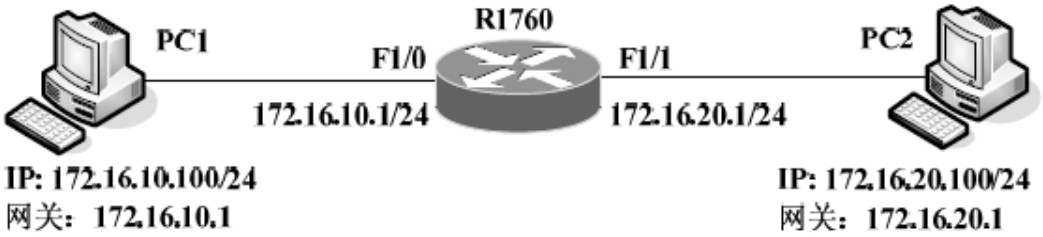


图 22 ICMP 协议分析实验连接图

3.实验分组

每六名同学为一组，其中每两人一小组，每小组各自独立完成实验。将主机 A 和

B 作为一组，主机 C 和 D 作为一组，主机 E 和 F 作为一组。现仅以主机 A、B 所在组为例，其它组的操作参考主机 A、B 所在组的操作。将主机 A 和 B 作为一组，主机 C 和 D 作为一组，主机 E 和 F 作为一组。现仅以主机 A、B 所在组为例，其它组的操作参考主机 A、B 所在组的操作。

实验步骤

练习一、运行 Ping 命令

步骤 1：

分别在主机 A 和主机 B 上运行 Wireshark，开始截获报文，为了只截获和实验内容有关的报文，将 Wireshark 的 Captrue Filter 设置为 “icmp”；

步骤 2：

在主机 A 上以主机 B 为目标主机，在命令行窗口执行 Ping 命令；

请写出执行的命令：ping 172.23.65.71

步骤 3：

停止截获报文，将截获的结果保存为 ICMP-1-学号，分析截获的结果，回答下列问题：

1）您截获几个 ICMP 报文？分别属于那种类型？

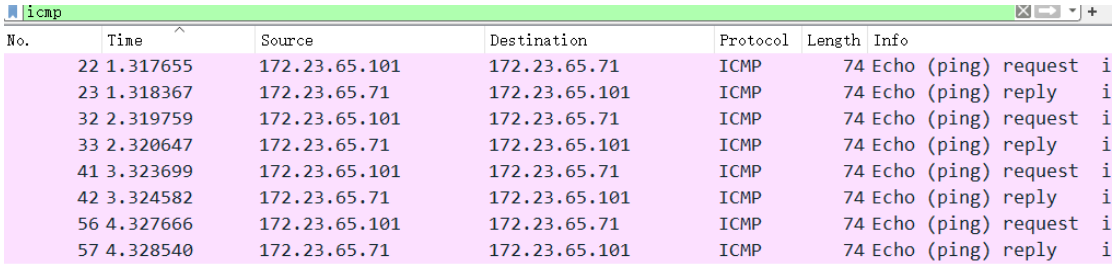
答：

截获了 8 个报文其中 4 个为请求报文，另外 4 个为应答报文。

请求报文的 ICMP 类型为 08

应答报文的 ICMP 类型为 00

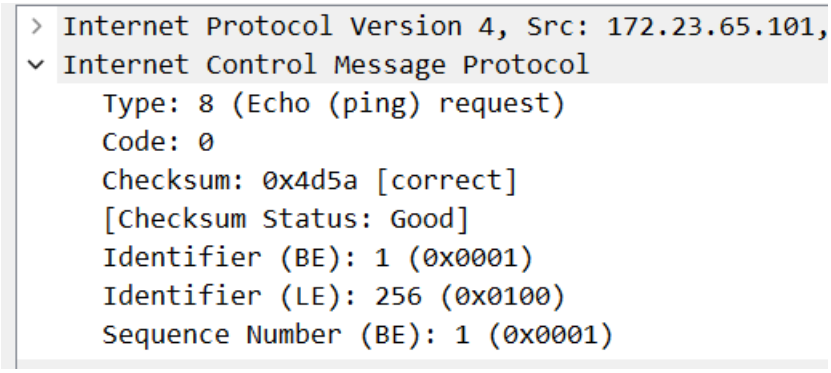
8 个报文：



icmp

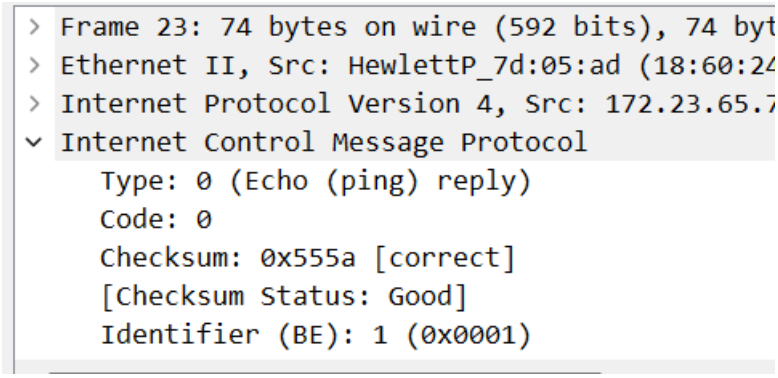
No.	Time	Source	Destination	Protocol	Length	Info
22	1.317655	172.23.65.101	172.23.65.71	ICMP	74	Echo (ping) request i
23	1.318367	172.23.65.71	172.23.65.101	ICMP	74	Echo (ping) reply i
32	2.319759	172.23.65.101	172.23.65.71	ICMP	74	Echo (ping) request i
33	2.320647	172.23.65.71	172.23.65.101	ICMP	74	Echo (ping) reply i
41	3.323699	172.23.65.101	172.23.65.71	ICMP	74	Echo (ping) request i
42	3.324582	172.23.65.71	172.23.65.101	ICMP	74	Echo (ping) reply i
56	4.327666	172.23.65.101	172.23.65.71	ICMP	74	Echo (ping) request i
57	4.328540	172.23.65.71	172.23.65.101	ICMP	74	Echo (ping) reply i

请求报文的类型：



```
> Internet Protocol Version 4, Src: 172.23.65.101,
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d5a [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1 (0x0001)
```

应答报文的类型：



```
> Frame 23: 74 bytes on wire (592 bits), 74 byt
> Ethernet II, Src: HewlettP_7d:05:ad (18:60:24
> Internet Protocol Version 4, Src: 172.23.65.7
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x555a [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
```

2）分析截获的 ICMP 报文，查看表 7 中要求的字段值，填入表中。

表 7 ICMP 报文分析

报文号	源 IP	目标 IP	ICMP 报文格式			
			类型	代码	标识	序列号
4	172.23.65.101	172.23.65.71	08	00	01	01
4	172.23.65.71	172.23.65.101	00	00	01	01
4	172.23.65.101	172.23.65.71	08	00	01	02
4	172.23.65.71	172.23.65.101	00	00	01	02
4	172.23.65.101	172.23.65.71	08	00	01	03
4	172.23.65.71	172.23.65.101	00	00	01	03

3）分析在上表中哪个字段保证了回送请求报文和回送应答报文的一一对应，仔细体会 Ping 命令的作用。

答：序列号字段保证了请求报文和应答报文的一一对应。

练习二、ICMP 查询报文

本练习将主机 A、B、C、D、E、F 作为一组进行实验。

步骤1：

主机 A启动协议编辑器，编辑一个 ICMP 时间戳请求数据帧发送给主机 C（172.16.1. 3）。

MAC 层:

目的 MAC 地址：C 的 MAC 地址。

源 MAC 地址：A 的 MAC 地址。

协议类型或数据长度：0800。

IP 层:

总长度：包含 IP 层和 ICMP 层长度。

高层协议类型：1。

校验和：在其它字段填充完毕后计算并填充。
源 IP 地址：A 的 IP 地址。
目的 IP 地址：C 的 IP 地址。

ICMP 层:

类型：13。
代码字段：0。
校验和：在 ICMP 层其它字段填充完毕后，计算并填充。

其它字段使用默认值。

步骤2:

主机 C 启动协议分析器进行数据捕获，并设置过滤条件（提取 ICMP 协议）。

步骤3:

主机 A 发送已编辑好的数据帧。

步骤4:

主机 C 停止捕获数据。察看主机 C 捕获到的数据，并填写下表

时间戳请求报文		时间戳应答报文	
ICMP 字段名	字段值	ICMP 字段名	字段值
类型	13	类型	14
标识号	4	标识号	4
序列号	5	序列号	5
发起时间戳	1633837924	发起时间戳	1633837923
接收时间戳	1701209960	接收时间戳	809649920
传送时间戳	1768581996	传送时间戳	809649920

1、 能否根据时间戳计算出当前的时间?

答：由于时间戳的值是自午夜开始计算的毫秒数，所以可以。

2、 使用时间戳得到的时间比从系统得到的时间有什么好处?

答：这种ＩＣＭＰ报文的好处是它提供了毫秒级的分辨率，而利用其他方法从别的主机获取的时间（如某些 Ｕｎｉｘ系统提供的ｒｄａｔｅ命令）只能提供秒级的分辨率。

练习三、运行 tracert 命令

步骤1：
打开 windows 的控制面板，将IP改成自动获取，打开浏览器完成校园网上网验证。

步骤2：
打开 windows 的命令提示符。

步骤3：
启动 Wireshark 数据包嗅探器，并开始 Wireshark 数据包捕获。

步骤4：
在命令提示符中输入“tracert hostname” 或 “c:windowssystem32 tracert hostname”。其中 hostname 是要测试的主机名，选择麻省理工学院官网 www.mit.edu来测试。

思考问题：

1. 你主机的 IP 地址是多少？目标主机的 IP 地址是多少？Traceroute 对每一个节点默认发出几个探测报文，每个报文的传输路径是否相同?

答：主机 IP 地址为：172.23.12.112，目标主机的 IP 地址为：104.79.117.240

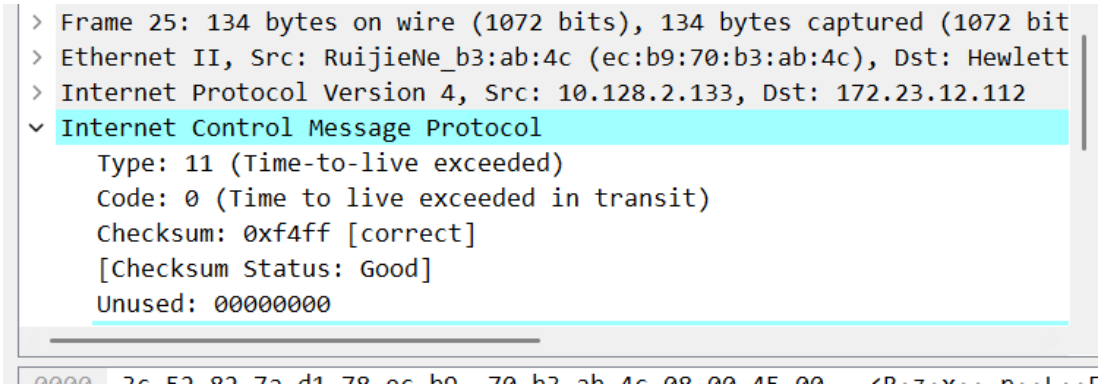
Traceroute 对每一个节点默认发出 3 个探测报文，每个报文的传输路径不相同。

2. 检查屏幕截图中的 ICMP 响应数据包。这与本实验的练习一中的 ICMP ping 数据包不同吗？如果不同，请解释为什么？

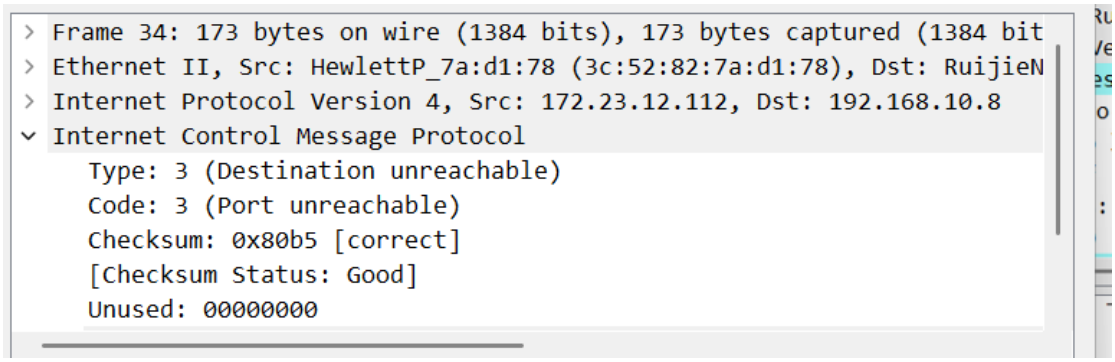
答：不同，ICMP 报文的类型为 11，表示网络不可达

还有一类 ICMP 报文的类型为 03，表示端口不可达

类型为 11：



类型为 03：



3. 检查源主机收到的最后三个 ICMP 数据包。这些数据包与 ICMP 错误数据包有何不同？他们为什么不同？

答： 最后收到的三个响应报文都是成功回复的，ICMP 类型均为 0。说明最后三次请求，目的主机均收到，在传递时没有丢包且源主机也收到了目的主机发出的响应报文。

```
106 Echo (ping) request  id=0x0001, seq=39/9984, ttl=11 (reply in 698)
106 Echo (ping) reply    id=0x0001, seq=39/9984, ttl=54 (request in 697)
106 Echo (ping) request  id=0x0001, seq=40/10240, ttl=11 (reply in 700)
106 Echo (ping) reply    id=0x0001, seq=40/10240, ttl=54 (request in 699)
106 Echo (ping) request  id=0x0001, seq=41/10496, ttl=11 (reply in 702)
106 Echo (ping) reply    id=0x0001, seq=41/10496, ttl=54 (request in 701)
```