实验五 ICMP 互连控制报文协议分析

【实验目的】

1、了解 ICMP 协议的功能与应用。
2、掌握常用 ICMP 报文格式和响应方式及作用。
3、熟悉常见的网络故障。

【实验学时】

4 学时

【实验环境】

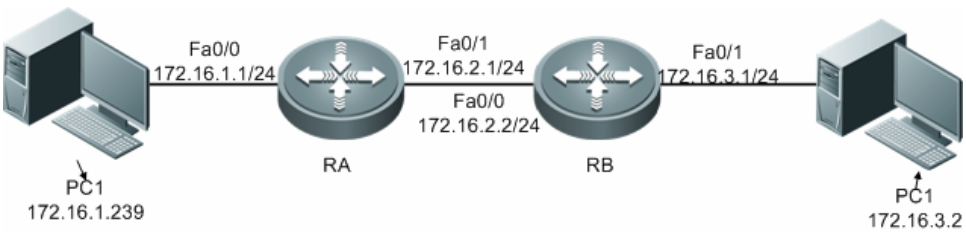

图 3-23 实验拓扑图

【实验内容】

1、学习和掌握 ICMP 协议的基本作用。
2、掌握 ICMP 报文的格式。
3、理解 ICMP 协议与 IP 协议的封装关系。
4、学会根据各种响应信息进行出错分析的方法。

【实验流程】

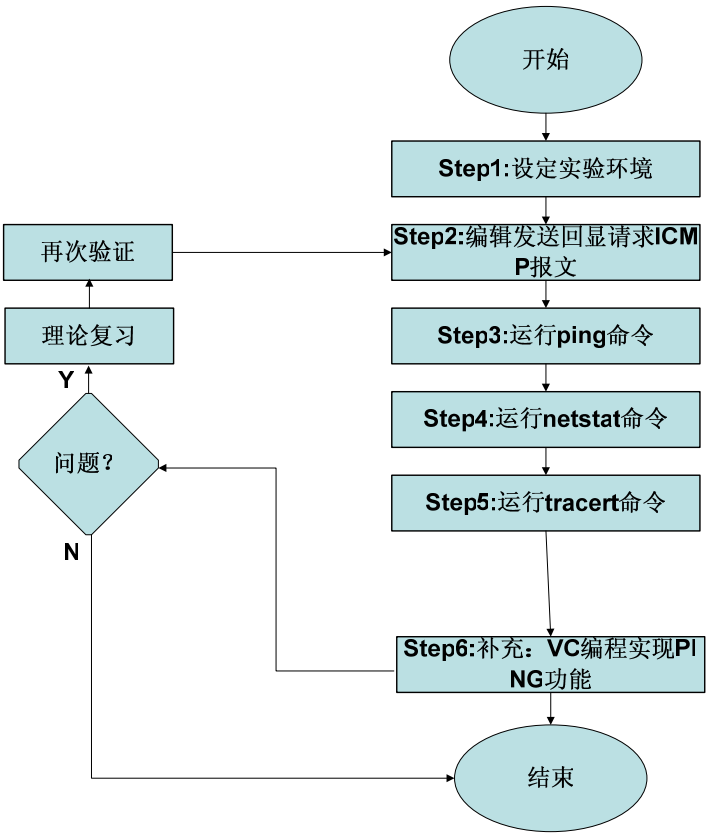

图 3-24 实验流程图

【实验原理】

IP 协议是一种不可靠无连接的包传输，当数据包经过多个网络传输后，可能出现错误、目的主机不响应、包拥塞和包丢失等。为了处理这些问题，在 IP 层引入了一个子协议 ICMP(Internet Control Message Protocol)。该协议是 TCP/IP 协议集中的一个子协议，属于网络层协议，主要用于在网络设备与网络设备之间传递控制信息，包括报告错误、交换受限控制和状态信息等。当遇到 IP 数据无法访问目标、IP 路由器无法按当前的传输速率转发数据包等情况时，会自动发送 ICMP 消息。

ICMP 数据报文有两种形式：差错数据报文和查询数据报文。ICMP 数据报文封装在 IP 数据报文里传输。ICMP 报文可以被 IP 协议层、传输层协议(TCP 或 UDP)和用户进程使用。ICMP 与 IP 一样，都是不可靠传输，ICMP 的信息也可能会丢失。为了防止 ICMP 信息无限制的连续发送，对 ICMP 数据报文传输中问题不能再使用 ICMP 传输。

1、ICMP 报文的封装

ICMP 有两种报文：差错报文和查询报文。两种报文都是封装在 IP 报文中进行传输的，具体的封装格式见下图：

图 3-25 ICMP 报文封装

2、ICMP 报文格式

图 3-26 ICMP 报文格式

字段说明：ICMP 类型和代码字段：8 位的类型字段有 15 个不同值，它与 8 位代码字段共同决定各种类型的 ICMP 报文。

校验和字段：对 ICMP 整个报文中每个 16bit 进行二进制反码求和。

3、ICMP 报文的主要类型

ICMP 报文可以分为两大类：差错报告和查询报文。差错报告报文是用于当路由器或主机在处理数据过程出现问题的时候进行报告。查询报文用于帮助网络管理员从一个网络设备上得到特定的信息，例如到达某个主机是否可达，中间经过那些路由等等。基于功能的不同，ICMP 报文分成很多类型，各类 ICMP 报文如下表所示。

表 3-1 ICMP 报文类型

种类	类型	报文
差错报告报文	3	目的端不可达
	4	源端抑制
	11	超时
	12	参数问题
	5	改变路由
查询报文	8 或 0	回送请求或回答
	13 或 14	时间戳请求或回答
	17 或 18	地址掩码请求或回答
	10 或 19	路由器查询和通告

由于 ICMP 报文类型过多并且很多报文极少使用，因此本书只介绍常用的 ICMP 报文类型及其作用。

4、目的端不可达

当路由器在发送数据的时候无法送达目的地，或者目的主机无法将数据交付相应程序时就丢弃这个数据包，并想源主机发送一个目的端不可达报文。目的端不可达报文格式如下所示。

图 3-27 ICMP 目的端不可达报文

在目的端不可达 ICMP 报文中，不同的代码值表示了不同的目的端不可达的原因。

- 代码 0：网络不可达，这类报文只能有路由器产生。
- 代码 1：主机不可达，只能由路由器产生。
- 代码 2：协议不可达，原因可能为目标主机的的相关协议未开启，此类报文只能由主机产生。
- 代码 3：端口不可达，数据报要交付的应用程序未运行。
- 代码 4：需要进行分段，但此数据的不分段字段被置位，导致数据无法送至目的端。
- 代码 5：源路由选择不能完成，数据中源路由选项定义的一个或多个路由器无法通过。
- 代码 6：目的网络未知，路由器不知道目的网络的存在。
- 代码 7：目的主机未知，路由器不知道目的主机的存在。
- 代码 8：源主机是孤立的。
- 代码 9：从管理上进制与目的网络通信。
- 代码 10：从管理上禁止与目的主机通信。
- 代码 11：对指明的服务类型，网络不可达。
- 代码 12：对指明的服务类型，主机不可达。
- 代码 13：主机不可达，由于管理机构在主机处配置了过滤器。
- 代码 14：主机不可达，由于主机的优先级被破坏。
- 代码 15：主机不可达，由于其优先级被删除。

5、超时 ICMP 报文

两种情况下会产生超时 ICMP 报文：

- 1、当路由器收到一个生存时间字段值为 0 的数据报时，就丢弃这个数据报，并向源端发送超时报文。
- 2、一个 IP 报文被分片后，所有的分片没有能够在一定时间内到达目的主机时，目的主机就将所有分片都丢弃掉，并向源端发送超时报文。

超时 ICMP 报文格式如下图所示：

图 3-28 超时 ICMP 报文格式

代码为 0 时，此报文只由路由器产生，表示生存时间字段值为 0，代码为 1 时，此报文只有主机产生，表示在规定时间内没有收到所有的分片。

6、改变路由 ICMP 报文

当主机连接到多个路由器的时候，它发送一个数据包到另一个网络，通常主机的做法是将其交给自己的默认路由，但是其实这个数据报本应当发给另一个路由器，这时收到此报文的路由器会将数据报转发给正确的路由器，并想主机发送一个改变路由 ICMP 报文，此后主机再发送数据报的时候会发给正确的路由器。

改变路由报文格式如下图所示。

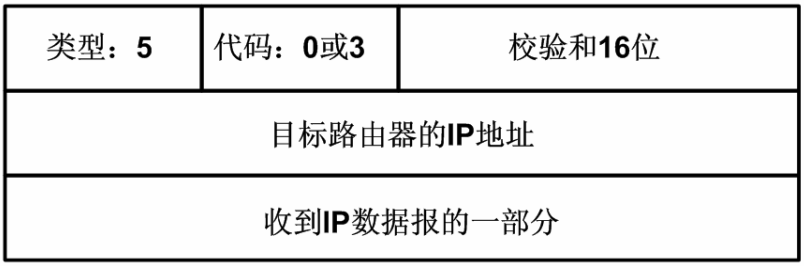

图 3-29 改变路由报文格式

7、回显请求和回答

回显请求和回答是为查询网络连通性而设计的 ICMP 查询报文。回显请求和回答报文可以用来确定在源端和目的端时候可以实现 IP 级的通信。主机或路由器发送一个回显请求给另一个主机或路由器，收到回显请求的主机或路由器创建回显应答 ICMP 报文，发送给源端，源端收到回显应答报文后可以判断目的主机是否可达。

回显请求及应答报文如下图所示。

图 3-30 回显请求和应答报文

类型为 8 时为回显请求报文，类型为 0 时为回显应答报文。

8、时间戳请求和回答

两台设备之间可以使用时间戳请求和时间戳回答报文确定 IP 数据报在这两个机器之间往返所需的时间，可以用用于两台设备的时钟的同步。时间戳的报文格式如下图所示。

图 3-31 时间戳请求和时间戳回答报文格式

源端创建时间戳请求报文，源端在报文离开源端时在原始时间戳填入自己时钟显示的时间，其他两个时间戳中填入 0。

目的端收到时间戳请求后创建时间戳应答报文，其中，原始时间戳与发送端相同，接受时间戳填入自己接收到时间戳请求报文的时间，发送时间戳填入目的端在发送时间戳应答报文的时间。

由此可以计算出从源端到目的端发送时间=接收时间戳的值—原始时间戳的值，接收时间=返回时间—发送时间戳的值，往返时间=发送时间+接收时间。

当准确的单向时间可以确定，时间戳请求和回答报文可以用来同步双方机器的时钟。

【实验步骤】

步骤一：设定实验环境

1、按照实验拓扑连接拓扑。

2、配置主机和路由接口地址，注意，在路由器上只配置接口地址不配置路由。

```
RA(config)#interface FastEthernet 0/0
RA(config-if)#ip address 172.16.1.1 255.255.255.0
RA(config)#interface FastEthernet 0/1
RA(config-if)#ip address 172.16.2.1 255.255.255.0
RB(config)#interface FastEthernet 0/0
RB(config-if)#ip address 172.16.2.2 255.255.255.0
RB(config)#interface FastEthernet 0/1
RB(config-if)#ip address 172.16.3.1 255.255.255.0
```

步骤二：捕获分析目的端不可达 ICMP 报文

1、在 PC1 中开启协议分析软件进行数据包捕获。

2、在 PC1 中的命令行窗口 ping PC2 的地址 172.16.3.2，如下图所示。

```
G:\Documents and Settings\Administrator>ping 172.16.3.2

Pinging 172.16.3.2 with 32 bytes of data:
```

图 3-32 ping 主机 PC2

3、PC1 中捕获到的目的不可达 ICMP 报文如下图所示。

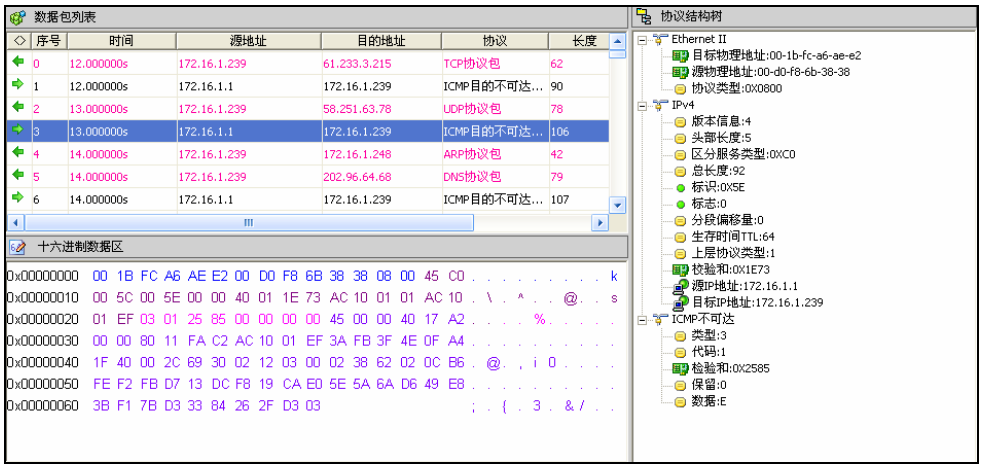

图 3-33 目的不可达 ICMP 报文

上图为目的不可达 ICMP 报文，从源地址可以看到发送此目的不可达报文由路由器 R1 发出，因为 R1 路由查找不到目标网段 172.16.3.0 的路径，因此丢弃 PC1 发送的 ICMP 回显请求，并发送目的不可达 ICMP 报文。

查看 ICMP 报头各字段内容。

- 类型：3，表示此报文为目的不可达 ICMP 报文。
- 代码：1，主机不可达，只能由路由器产生，产生原因为 R1 路由器不知道目的主机 172.16.3.2 的路由。
- 校验和：0X2585，校验和字段为 ICMP 报文和数据部分的校验和数据。
- 保留：0，ICMP 目标不可达报文中保留字段全为 0。
- 数据：数据部分为被丢弃报文的 IP 报头的部分。

步骤三：捕获分析超时 ICMP 报文

1、在路由器 R1 和 R2 上配置静态路由，使得 PC1 和 PC2 可以互相通信。静态路由参开配置如下所示。

```
R1(config)#ip route 172.16.3.0 255.255.255.0 172.16.2.2
R2(config)#ip rout 172.16.1.0 255.255.255.0 172.16.2.1
```

2、在 PC1 中开启协议编辑软件，编辑 IP 包。如下图所示。

图 3-34 编辑 IP 包

在编辑的 IP 包中，以太网分装中：

- 目的物理地址：通过地址本填入网关 172.16.1.1 的物理地址。
- 源物理地址：通过地址本填入 PC1 的物理地址。
- 类型：0800。
- 在 IP 封装中：
- 版本：4。
- IP 头长度（32 比特数）：5，IP 头长度为 20 字节。
- 服务类型：00，不使用。
- 总长度：60 字节，为 IP 报头加数据部分。
- 标识：0000。
- 标志：0，允许分片。
- 分段偏移：0，无分片。
- 生存时间：1，从 PC1 到达 PC2 跳数为两跳。将生存时间定义为 1 后，在路由器 R1 会由于生存时间减为 0 发送超时 ICMP 报文。
- 协议类型：0。
- 校验和：IP 报头和数据的校验和数据。
- 发送 IP 地址：PC1 的 IP 地址。
- 目标 IP 地址：PC2 的 IP 地址。

3、在 PC1 上开启协议分析软件进行数据包捕获。

4、在 PC1 中的协议编辑软件中点击”发送”，发送编辑好的 IP 数据包。

5、捕获到的超时 ICMP 报文如下图所示。

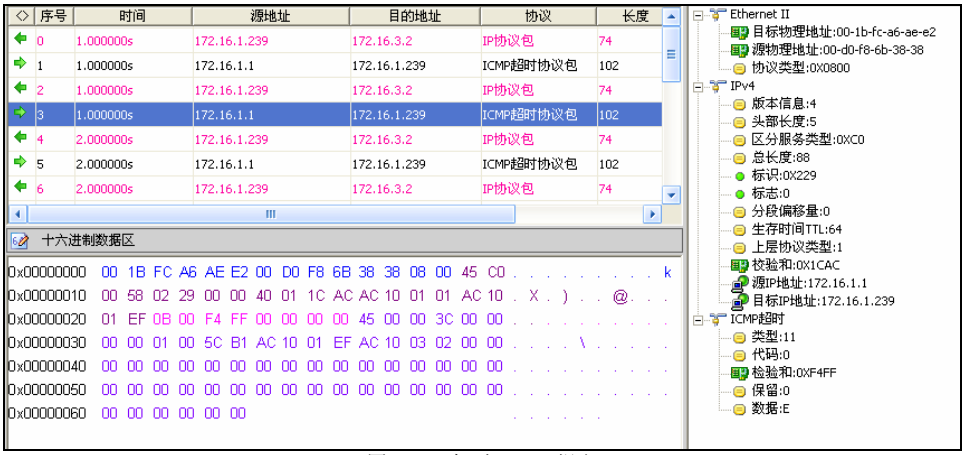

图 3-35 超时 ICMP 报文

从捕获到的超时 ICMP 报文可以看到，发送报文的源端为路由器 R1。查看 ICMP 报头。

- 类型：11，说明此报文为 ICMP 超时报文。
- 代码：0，说明此报文为生存时间到期 ICMP 报文，当代码为 1 时，说明此报文为分片 IP 包未能在规定时间内全部到达目的端的超时报文。
- 校验和：ICMP 报头和数据部分的校验和数据。
- 保留：0，保留字段在超时报文中未使用，全 0。
- 数据：数据部分为由于超时被报文的部分 IP 报头。

步骤四：捕获分析回显请求和应答 ICMP 报文

1、在 PC1 中开启协议分析软件进行数据包捕获。

2、在 PC1 中的命令行窗口中 pingPC2 的地址 172.16.3.2，如下图所示。

```
G:\Documents and Settings\Administrator>ping 172.16.3.2

Pinging 172.16.3.2 with 32 bytes of data:

Reply from 172.16.3.2: bytes=32 time<1ms TTL=126
Reply from 172.16.3.2: bytes=32 time<1ms TTL=126
Reply from 172.16.3.2: bytes=32 time<1ms TTL=126
Reply from 172.16.3.2: bytes=32 time<1ms TTL=126

Ping statistics for 172.16.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图 3-36 ping 操作

3、在 PC1 中捕获到 ICMP 回显请求报文如下图所示。

图 3-37 ICMP 回显请求报文

此报文源地址为 172.16.1.239，目的地址为 172.16.3.2，为 PC1 发送给 PC2 的 ICMP 回显请求报文。

在 ICMP 回显请求报头中，

- 类型：8，表示此报文为 ICMP 回显请求报文。
- 类型：0，ICMP 回显请求和应答报文类型均为 0。
- 校验和：校验和部分为 ICMP 报头及数据部分的校验数据。
- 标识符：512，帮助确认 ICMP 回显应答报文，即正对此请求的应答报文中的标识符也为 512。
- 序列号：8448，帮助确认 ICMP 会显应答报文。
- 数据：填充数据。

捕获到的 ICMP 回显应答报文如下图所示。

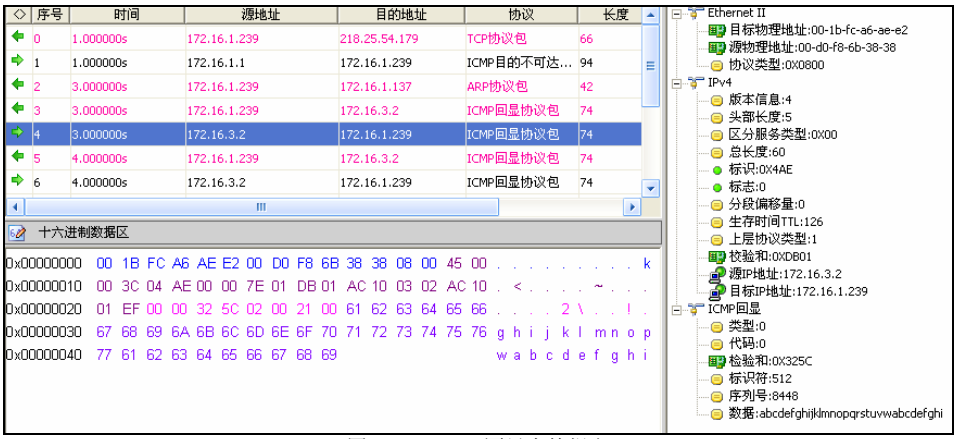

图 3-38 ICMP 回显应答报文

此报文的源 IP 地址为 172.16.3.2，目的 IP 地址为 172.16.1.239，为 PC2 发送给 PC1 的 ICMP 回显应答报文。

查看上图中的 ICMP 报头中

- 类型：0，ICMP 回显应答报文类型为 0；
- 代码：0，ICMP 回显报文代码均为 0；
- 校验和：此部分为 ICMP 报头和数据的校验和数据；
- 标识符：512，与 PC1 发送 ICMP 回显请求报文的标识符相同；
- 序列号：8448，与 PC1 发送的 ICMP 回显请求报文的标识符相同；
- 数据：填充数据部分。

【思考问题】

结合实验过程中的实验结果，回答下列问题：

1、根据实验结果说明：实验室环境所使用操作系统默认的 TTL 值是多少？

2、运行 ping 127.0.0.1，再运行 ping 本机名(或本机 IP 地址)。在监测机端是否捕获到相应的 ICMP 回显请求报文？