华东师范大学计算机科学技术系上机实践报告

课程名称： 计算机网络	**年级：** 2022 级	**上机实践成绩：**
指导教师： 洪道诚	**姓名：** 朱宇笑	**创新实践成绩：**
实验名称： 地址解析协议ARP	**学号：** 10225001410	**上机实践日期：** 2023/12/13
座位编号： F	**组号：** 6	**上机实践时间：** 2 学时

一、 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

二、 实验设备

1. PC机
2. 仿真编辑器
3. 协议分析器

三、 实验原理

一.ICMP 简介

IP 协议是一种不可靠无连接的协议，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、包拥塞和包丢失等问题。为了处理这些问题，在 IP 层引入了另一个协议 ICMP（Internet 控制报文协议）。ICMP 报文有两种类型：差错报文和查询报文。ICMP 报文封装在 IP 报文里传输。ICMP 报文可以被 IP 协议、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 的信息也可能丢失。为了防止 ICMP 报文无限制的连续发送,对于 ICMP 报文在传输中发生的问题,将不再发送 ICMP 差错报文。

二.ICMP 报文格式

ICMP 数据包由 8 字节的首部和可变长度的数据部分组成。如下图所示，第一个字段是 ICMP 的类型，它定义了报文类型。第二个字段是代码字段，它指明了发送这个特定报文类型的原因。校验和字段为 ICMP 数据包提供差错校验。对于不同类型的 ICMP 数据包，首部的最后 4 个字节的格式是不同的，具体的格式将在下面讨论。

差错报文的数据部分携带引起差错的原始数据。查询报文的数据部分携带了基于查询类型的额外信息。

类型（8 位）	代码（8 位）	校验和（16 位）

首部的其余部分
数据部分

图 4-1 ICMP 报文的一般格式

1

●类型：8 位字段，用于描述特定类型的 ICMP 报文。

●代码：8 位字段，进一步描述某些 ICMP 报文的具体说明。

●校验和：16 位字段，覆盖这个 ICMP 报文的校验和。

三. ICMP 封装

ICMP 报文封装在 IP 数据报中，具体的封装方法如下图所示：

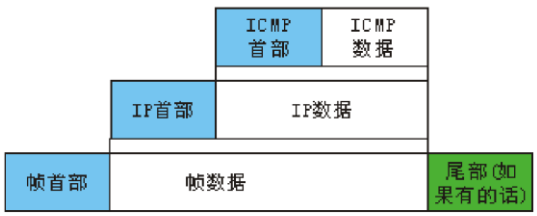


图 4-2 ICMP 封装

四. ICMP 报文类型

ICMP 报文可分为两大类：差错报文和查询报文，如下图所示：

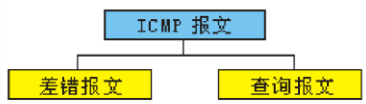


图 4-3ICMP 报文类型

差错报文报告路由器或主机在处理 IP 数据报时遇到的问题。

查询报文是成对出现的，它帮助主机或网络管理员从一个路由器或另一个主机得到特定的信息。例如，主机使用 ICMP 回显请求和回显应答报文发现它们的邻站。下表列出了每一类 ICMP 报文。

表 4-1 ICMP 报文

种类	类型	报文
差错报文	3	目的端不可达
	4	源点抑制
	11	超时
	12	参数问题
	5	改变路由
查询报文	8 或 0	回显请求或应答

	13 或 14	时间戳请求或应答
	17 或 18	地址掩码请求或应答
	10 或 9	路由器询问和通告

五. ICMP 查询报文

ICMP 查询报文能够获得特定主机或路由器的信息，能够对某些网络问题进行诊断。ICMP 查询报文包括 4 对不同类型的报文，分别为回显请求和应答报文、时间戳请求和应答报文、地址掩码请求和应答报文以及路由器询问和通告报文，如下图所示。

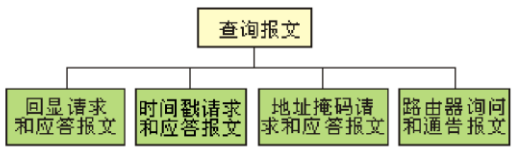


图 4-4 查询报文

1. 回显请求和应答

回显请求报文和回显应答报文用来确定了两个节点（主机或路由器）之间是否能够正常通信。用户可以使用这对报文来发现网络问题。

主机或路由器可以发送回显请求报文给另一个主机或路由器。收到回显请求报文的主机或路由器产生回显应答报文，并将其返回给原来的发送端。

回显请求和回显应答报文可用来确定是否在 IP 这级能够通信。因为 ICMP 报文被封装在 IP 数据报中，发送回显请求的主机在收到回显应答报文时，就证明了在发送端和接收端之间能够使用 IP 数据报进行通信。另外，这还证明了链路中的路由器能够接收、处理和转发数据报。

回显请求和回显应答报文还可以用于检查另一个主机是否可达。用户可以调用数据包因特网搜寻器（ping）命令做到这一点。现在，大多数系统都提供 ping 命令，它可以产生一连串的回显请求或回显应答报文。

回显请求和回显应答报文也可以用来验证某个节点是否正常工作。可以向被测试的节点发送回显请求报文，该报文的数据字段包含一段信息，如果这段信息被测试的节点在回显应答报文中完全一样地重复，则说明该节点工作正常；否则说明该节点出了问题。下图给出了回显请求和回显应答报文的格式。类型值为 8 表示回显请求报文，类型值为 0 表示回显应答报文。标识符和序号字段在协议中没有正式定义，可以由发送端任意使用。

类型：8 或 0	代码：0	校验和
标识符		序号
回请求报文发送 由应答报文重复		

图 4-5 ICMP 回显请求和应答报文

2. 时间戳请求和应答

两个机器（主机或路由器）可使用时间戳请求和时间戳应答报文来确定 IP 数据报在这两个机器之间传输所需要的时间，也可以用作两个机器时钟的同步。这两个报文的格式如下图所示。其中，类型值为 13 表示时间戳请求报文，类型值为 14 表示时间戳应答报文。

类型：13 或 14	代码：0	校验和
标识符		序号
原始时间戳		
接收时间戳		
发送时间戳		

图 4-6 时间戳请求和应答报文

在报文格式中 3 个时间戳字段的长度都是 32 位。每一个字段都保存一个整数，代表从通用时间（格林尼治标准时间）的午夜起测量出的时间，以毫秒为单位。

源节点在时间戳请求报文的原始时间戳字段填入它的时钟所显示的通用时间。其它两个时间戳字段都填入零。

收到时间戳请求报文后，终点将生成时间戳应答报文。终点把请求报文中的原始时间戳字段值复制到应答报文的同一个字段中。然后在接收时间戳字段中填入收到这个请求报文时其时钟所显示的通用时间。最后，终点在应答报文将要发送时在发送时间戳字段中填入其时钟所显示的通用时间。

时间戳请求和时间戳应答报文可以用来计算数据报从源点到终点所需的时间，还可以用于计算数据报再返回到源点所需的时间。

3. 地址掩码请求和应答

要得到掩码，主机应该向局域网上的路由器发送地址掩码请求报文。若主机知道路由器的地址，它就把请求直接发送给该路由器。若主机不知道路由器的地址，则它就广播地址掩码请求报文。路由器收到地址掩码请求报文后，用地址掩码应答报文进行响应，向主机提供所需的掩码。

地址掩码请求和地址掩码应答报文的格式如下图所示。其中，类型值为 17 表示地址掩码请求报文，类型值为 18 表示地址掩码应答报文。在请求报文中，地址掩码字段填入全 0。当路由器把地址掩码应答发回给主机时，这个字段就包含真正的掩码。

类型：17 或 18	代码：0	校验和
标识符		序号
地址掩码		

图 4-7 地址掩码请求和应答报文

无盘工作站在启动时是需要地址掩码的，它会使用 RARP 协议查找完整的 IP 地址，在收到 IP 地址以后，无盘工作站就可使用地址掩码请求报文找出地址掩码，从而确定 IP 地址的哪一部分定义了子网号，哪一部分定义了主机号。

4.路由器询问和通告

主机若想把数据发送给另一个网络上的主机，就需要知道连接到该网络上的路由器的地址。此外，这个主机还需要知道这些路由器是否正常工作。路由器询问报文和路由器通

告报文可以完成这项工作。主机可把路由器询问报文进行广播（或多播）。收到询问报文的一个或几个路由器就使用路由器通告报文广播其路由选择信息。甚至在没有主机询问时，路由器也可周期性地发送路由器通告报文。路由器发送出通告报文时，它不仅通告了自己的存在，而且也通告了它所知道的所有在这个网络上的路由器。下图给出了路由器询问报文的格式。

类型：10	代码：0	校验和
标识符		序号

图 4-8 路由器询问报文

下图给出了路由器通告报文的格式。生存期字段表示这个报文在多长时间内是有效的。在通告报文中每一个路由器的项目有两个字段：路由器地址和地址优先级。地址优先级定义了路由器的等级。优先级用来选择某个路由器作为默认路由器。若地址优先级为零，则这个路由器就被认为是默认路由器。若地址优先级是 0x80000000，则这个路由器永远不能被选为默认路由器。

类型：9	代码：0	校验和
地址数	地址项目长度	生存期
路由器地址 1		
地址优先级 1		
路由器地址 2		
地址优先级 2		
……		

图 4-9 路由器通告报文

六. ICMP 差错报文

ICMP 差错报文用来报告差错。虽然现代的技术已经制造出很可靠的传输媒体，但差错仍然存在，因而必须进行处理。正如在实验三中所讨论的，IP 是个不可靠的协议。这就表示 IP 不考虑差错校验和差错控制。ICMP 就是为了补偿这个缺点而设计的。然而 ICMP 不能纠正差错，它只是报告差错，差错纠正留给高层协议去做。ICMP 使用源 IP 地址把差错报文发送给数据报的源点（发出者）。

一共有 5 种差错报文：目的端不可达、源点抑制、超时、参数问题以及改变路由，如下图所示。

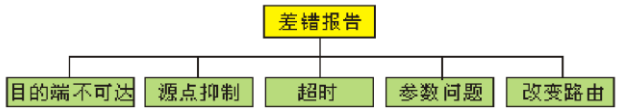


图 4-10 差错报文

差错报文的数据字段包括原始数据报（引起差错的报文）的首部和原始数据报数据部分的前 8 个字节。包括原始数据报首部的目的是为了向差错报文的原始信源给出关于数据

报本身的信息。包括数据的前 8 个字节是因为这前 8 个字节提供了关于端口号(UDP 和 TCP)和序号（TCP）的信息。根据这些信息，源点可以把差错情况通知给上层协议。

1. 目的端不可达

当路由器不能够为数据报找到路由或主机，就丢弃这个数据报，然后向发出这个数据报的源主机发送目的端不可达报文。下图给出了目的端不可达报文的格式。这种类型的代码字段指明了丢弃该数据报的原因。

类型：3	代码：0 至 15	校验和
未使用（全 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		

图 4-11 目的端不可达报文

2. 源点抑制

IP 协议是无连接协议，因此通信缺乏流量控制。ICMP 源点抑制报文就是为了给 IP 增加一种流量控制而设计的。当路由器或主机因拥塞而丢弃数据报时，它就向数据报的发送端发送源点抑制报文。第一，它通知发送端，数据报已被丢弃。第二，它警告发送端，在路径中的某处出现了拥塞，因而源端必须放慢发送过程。源点抑制报文的格式如下图所示：

类型：4	代码：0	校验和
未使用（全 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		

图 4-12 源点抑制报文

3. 超时

超时报文是在以下两种情况下产生的：

●数据报的生存时间字段值被减为 0 时，路由器丢弃这个数据报，并向发送端发送超时报文。

●当组成报文的所有分段未能在某一时限内到达目的主机时，也要产生超时报文。当第一个分段到达时，目的主机就启动计时器。当计时器的时限到了，目的主机就将所有分段丢弃，并向发送端发送超时报文。超时报文格式如下图所示：

类型：11	代码：0 或 1	校验和
未使用（全 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		

图 4-13 超时报文

4. 参数问题

当数据报在 Internet 上传送时，如果路由器或目的主机发现数据报首部中出现了二义性问题，或在数据报的某个字段中缺少某个值，它就丢弃这个数据报，并向发送端发送参数问题报文。下图给出了参数问题报文格式。代码字段指明了丢弃数据报的原因。

类型：12	代码：0 或 1	校验和
指针	未使用（全 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		

图 4-14 参数问题报文

●代码为 0 时表示在首部的某个字段中有差错或二义性。指针字段值指向有问题的字节。

●代码为 1 时表示缺少所需的选项部分。这种情况下不使用指针。

5. 重定向

为了提高效率，主机不参与路由选择更新过程，因此，主机可能会把某数据报发送给一个错误的路由器。这时，收到这个数据报的路由器会把数据转发给正确的路由器，同时向主机发送重定向报文，告诉主机正确路由器的地址。下图给出了重定向报文的格式。

类型：5	代码：0 到 3	校验和
目标路由器 IP 地址		
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		

图 4-15 改变路由报文

七. ICMP 校验和

ICMP 的校验和的计算覆盖了整个 ICMP 报文（首部和数据）。

1. 校验和的计算

发送端按以下步骤使用反码算术运算计算校验和：

(1)把校验和字段置为零。

(2)把报文按照 16 位长度分段，使用反码算术运算计算所有分段之和。

(3)把得到的和求反码，得到校验和。

(4)把校验和存储在校验和字段中。

2. 校验和的测试

接收端按以下步骤使用反码算术运算来测试校验和的正确性：

(1)把报文按照 16 位长度分段，使用反码算术运算计算所有分段之和。

(2)把得到的和求反码。

(3)若结果是全 0，则接受这个报文；否则就拒绝这个报文。

【实验步骤】

练习 1 运行 Ping 命令

首先按照附录 A 关于网络拓扑结构二的要求为每组的 A～F 各主机设置 IP 地址、子网掩码、默认网关等参数。

本练习将主机 A、B、C、D、E、F 作为一组进行实验。

实验开始前主机 B 首先执行命令“staticroute_config”启动静态路由。

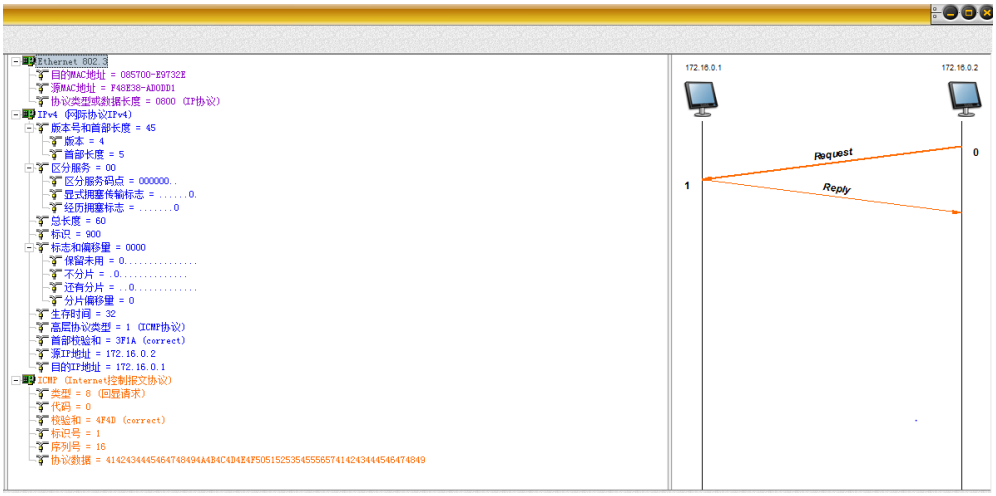
1. 主机 B、E、F 启动协议分析器，打开捕获窗口进行数据捕获并设置过滤条件（提取 ICMP 协议）。
2. 主机 A ping 主机 E（172.16.0.2）。

   主机 C ping 主机 F（172.16.0.3）。
3. 主机 B、E、F 停止捕获数据，察看捕获到的数据，并回答以下问题：

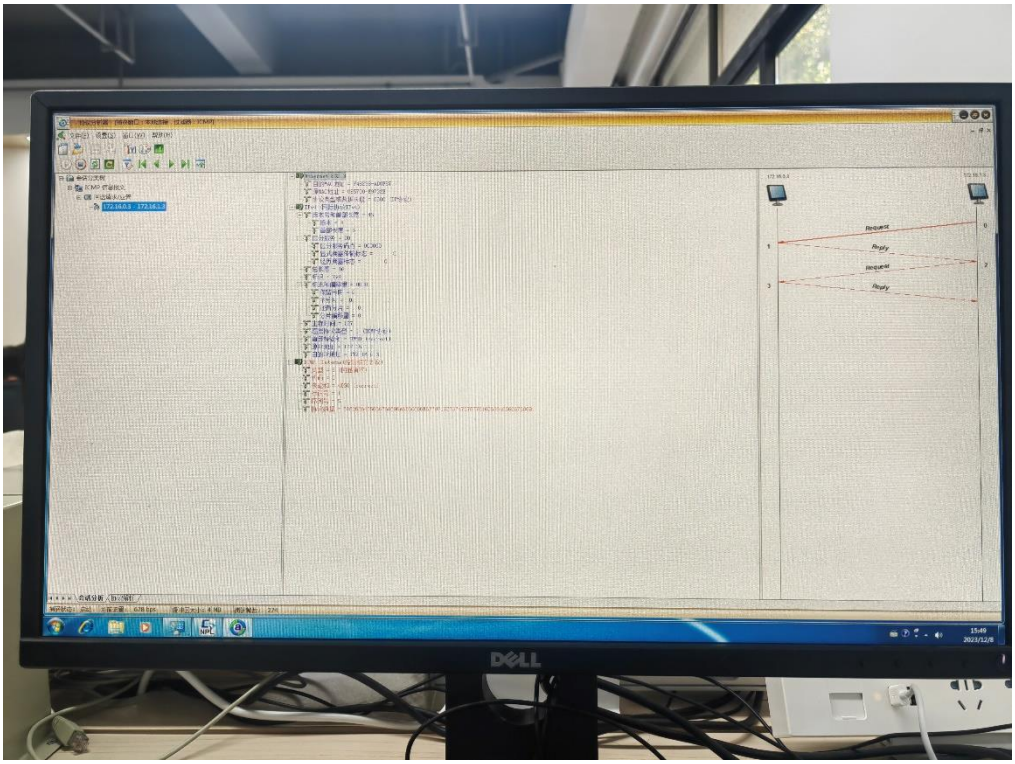
   ●捕获的报文对应的“类型”和“代码”字段分别是什么？

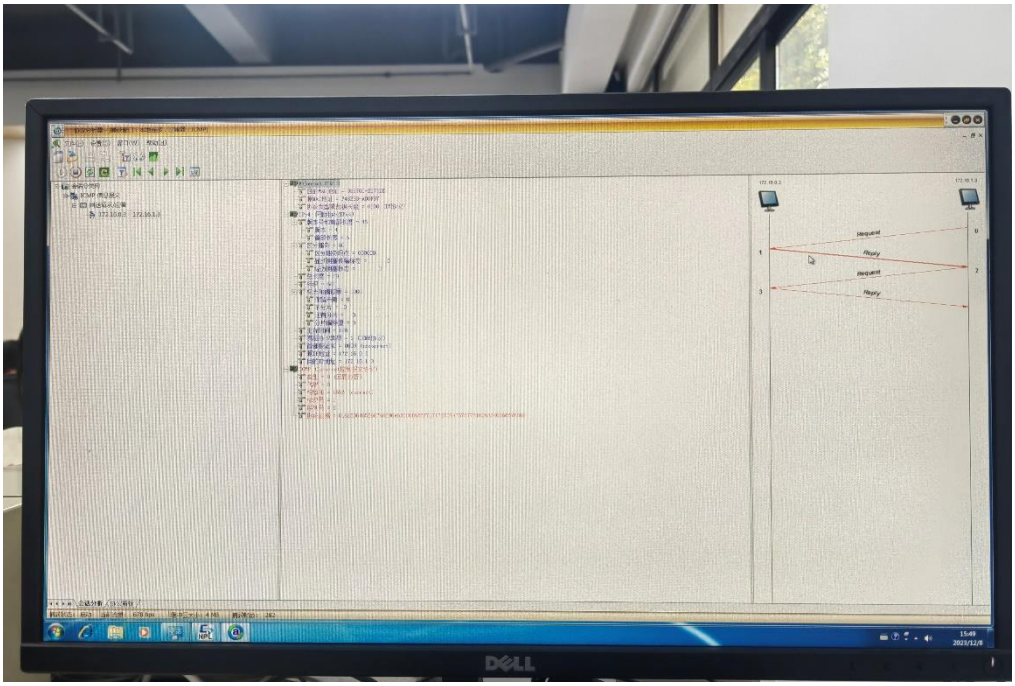
   ●分析报文中的哪些字段保证了回显请求报文和回显应答报文的一一对应？

主机 B:


Ethernet 802.3
目的MAC地址 = 085700-E9732E
源MAC地址 = F48E38-AD0DD1
协议类型或数据长度 = 0800 (IP协议)
IPv4 (网际协议IPv4)
版本号和首部长度 = 45
版本 = 4
首部长度 = 5
区分服务 = 00
区分服务码点 = 000000..
显式拥塞传输标志 = ...0.
经历拥塞标志 = ...0
总长度 = 60
标识 = 900
标志和偏移量 = 0000
保留未用 = 0...............
不分片 = .0..............
还有分片 = ..0.............
分片偏移量 = 0
生存时间 = 32
高层协议类型 = 1 (ICMP协议)
首部校验和 = 3F1A (correct)
源IP地址 = 172.16.0.2
目的IP地址 = 172.16.0.1
ICMP (Internet控制报文协议)
类型 = 8 (回显请求)
代码 = 0
校验和 = 4F4D (correct)
标识号 = 1
序列号 = 16
协议数据 = 41424344454647484849
172.16.0.1
172.16.0.2
Request
Reply
0
1

主机 F:


DELL



报文中的标识号和序列号保证了回送请求报文和回送应答报文一一对应。

练习 2 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。

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：先清 0，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。

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）。

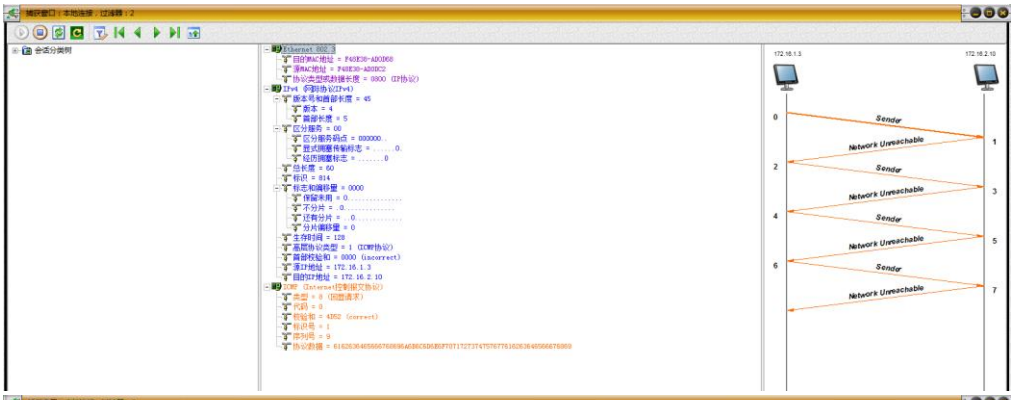
3. 主机 A 发送已编辑好的数据帧。

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	0	标识号	0
序列号	0	序列号	0
发起时间戳	0	发起时间戳	0
接收时间戳	0	接收时间戳	1887418625
传送时间戳	0	传送时间戳	1887418625

思考问题：

1. 能否根据时间戳计算出当前的时间？
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？



1. 能
2. 时间戳得到的时间更加精准。

练习 3 ICMP 差错报文

本练习将主机 A、B、C、D、E、F 作为一组进行实验。

1.目的端不可达

(1)主机 A、B、C、D、E、F 启动协议分析器捕获数据，并设置过滤条件（提取 ICMP）。

(2)主机 A、C、D、E、F ping 172.1.2.3（一个不存在的 IP 地址）。

(3)主机 A、B、C、D、E、F 停止捕获数据。察看捕获到的数据，并回答以下问题：

●捕获到的是哪一种目的端不可达报文？

2.超时

(1)主机 A、C、D 分别启动协议编辑器，编写一个发送给主机 F（172.16.0.3）的 ICMP 数据帧。其中：

MAC 层：

目的 MAC 地址：主机 B 的 MAC 地址（Intel I219 接口的 MAC）。

源 MAC 地址：本机的 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。

生存时间（TTL）：0。

高层协议类型：1。

校验和：先清 0，在其它字段填充完毕后，计算并填充。

源 IP 地址：本机的 IP 地址。

目的 IP 地址：F 的 IP 地址。

ICMP 层：

类型：8。

代码字段：0。

校验和：在 ICMP 其它字段填充完毕后，计算并填充。

其它字段使用默认值。

(2)主机 E、F 分别启动协议编辑器，编写一个发送给主机 D（172.16.1.4）的 ICMP 数据帧。其中：

MAC 层：

目的 MAC 地址：主机 B 的 MAC 地址（Realtek RTL8139 接口的 MAC)。

源 MAC 地址：本机的 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。

TTL：0。

高层协议类型：1。

校验和：先清 0，在其它字段填充完毕后，计算并填充。

源 IP 地址：本机的 IP 地址。

目的 IP 地址：D 的 IP 地址。

ICMP 层：

类型：8。

代码字段：0。

校验和：在 ICMP 其它字段填充完毕后，计算并填充。

其它字段使用默认值。

(3)主机 B 启动协议分析器，网卡 Intel I219(172.16.1.1)、网卡 Realtek RTL8139（172.16.0.1）分别捕获数据，并设置过滤条件（提取 ICMP 协议)。

(4)主机 A、C、D、E、F 各自发送已编辑好的数据帧。

(5)主机 B 停止捕获数据，察看并分析捕获到的数据。

(6)主机 B 在命令行方式下输入“recover_config”命令，停止静态路由服务。

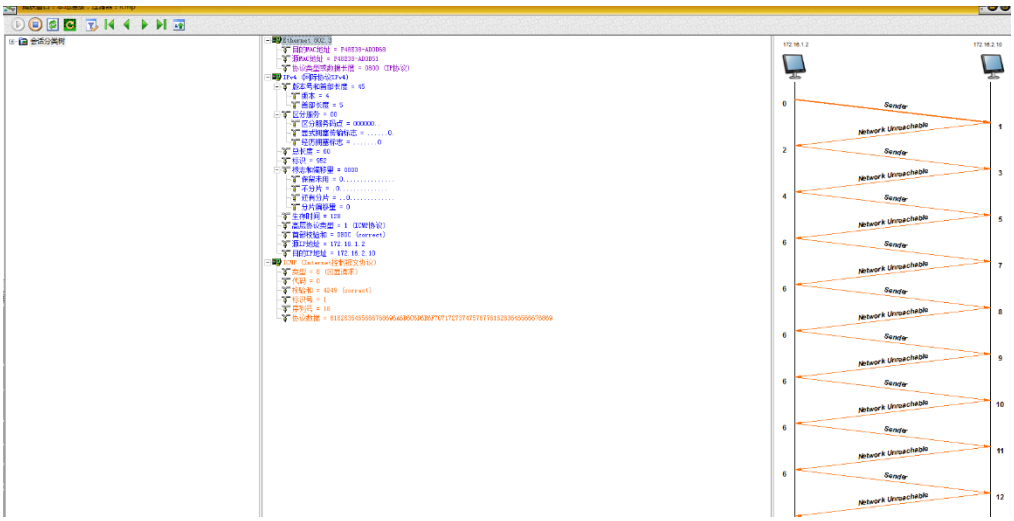
思考问题：

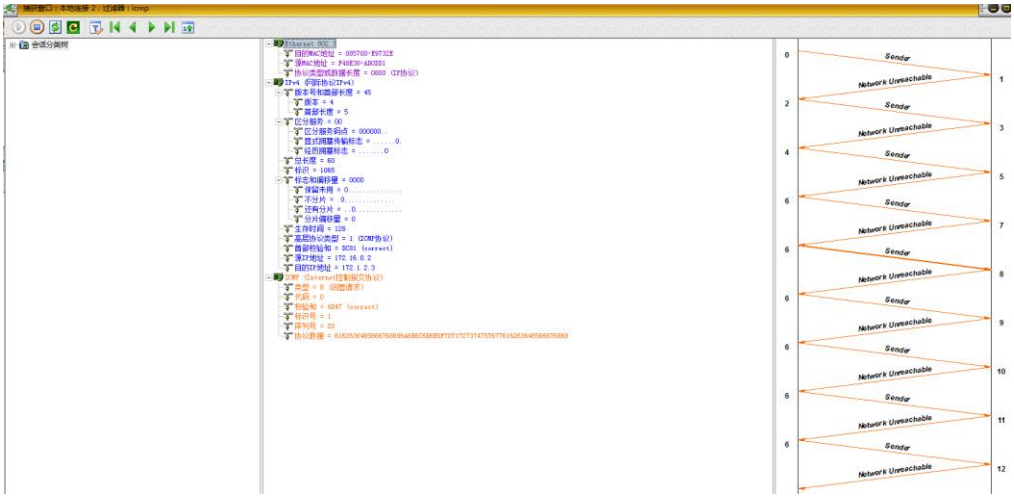
1.为什么要设置 TTL 字段？

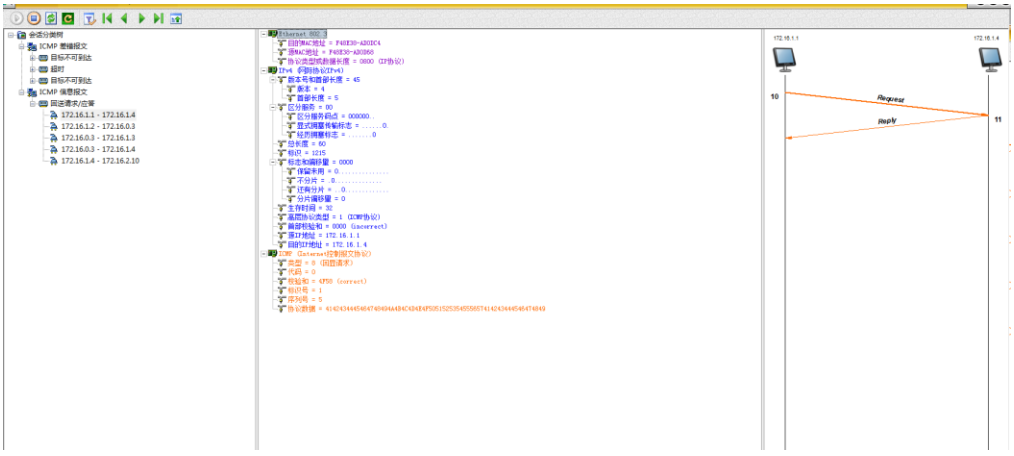
2.为什么要限制由失效的 ICMP 差错报文再产生一个 ICMP 报文？

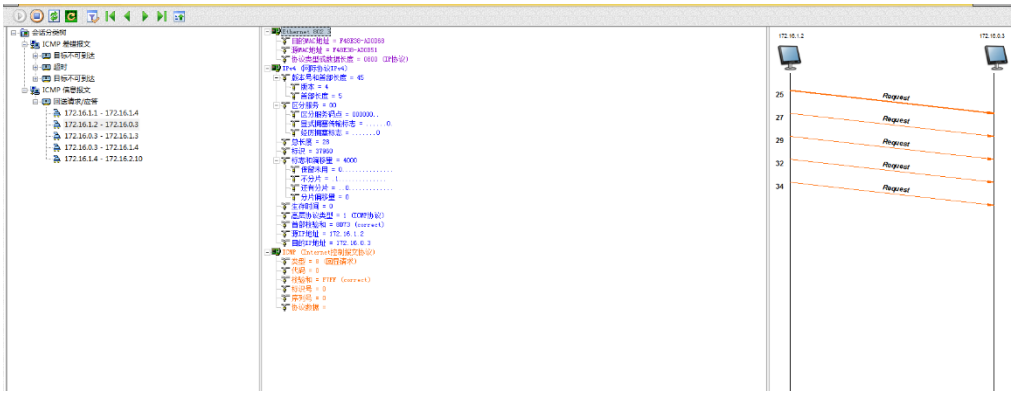
3.什么样的 ICMP 报文是由路由器发送出的？什么样的 ICMP 报文是由目的主机发送出的？

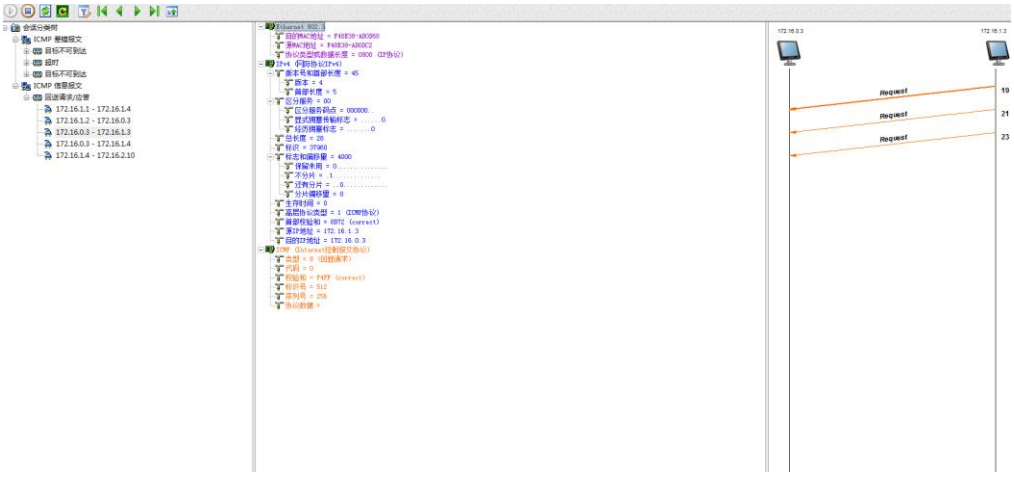
4.主机 A 向主机 B 发送数据报，主机 B 从未收到该数据报，而主机 A 也从未收到出问题的通知。试给出可能发生情况的两种不同解释。

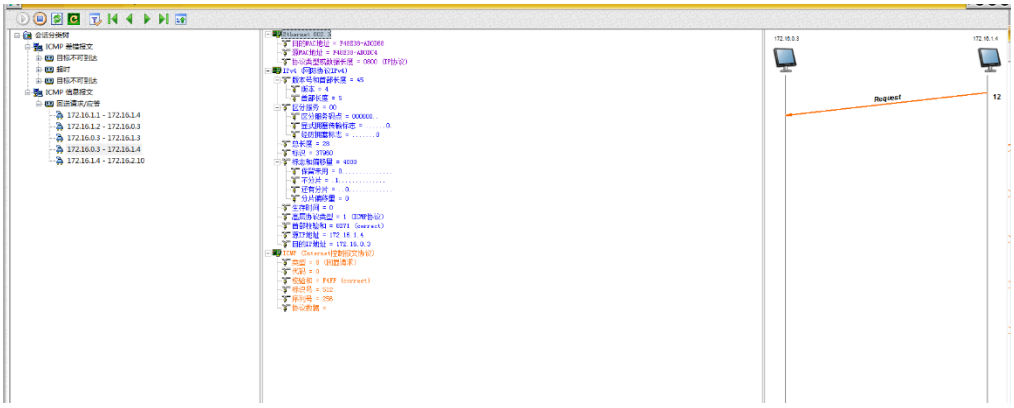

会话分类树
Ethernet 802.3
IPv4 (网际协议IPv4)
ICMP (Internet控制报文协议)
172.16.1.2
172.16.2.10
Sender
Network Unreachable

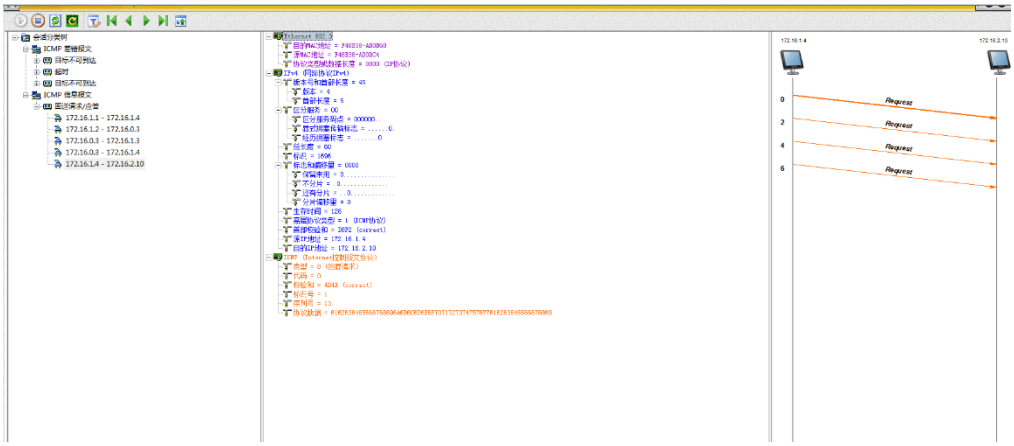

会话分类树
Ethernet 802.3
IPv4 (网际协议IPv4)
ICMP (Internet控制报文协议)
Sender
Network Unreachable


会话分类树
ICMP 错误报文
目标不可到达
超时
目标不可到达
ICMP 信息报文
回送请求/应答
172.16.1.1 - 172.16.1.4
172.16.1.2 - 172.16.0.3
172.16.0.3 - 172.16.1.3
172.16.0.3 - 172.16.1.4
172.16.1.4 - 172.16.2.10
Ethernet 802.3
IPv4 (网际协议IPv4)
ICMP (Internet控制报文协议)
172.16.1.1
172.16.1.4
Request
Reply









1、答:设置生存时间字段，限制通过的路由数。这一规则是为了防止过去允许 ICMP 差错报文对)播分组相应带来的广播风暴。

2、答:限制由失效的 ICMP 差错报文再产生一个 ICMP 报文从而减少网络的流量

3、答:路由器:网络不可达、主机不可达、对主机重定向等。目的主机:回显应答、端口不可达。