

实验 4 ICMP 协议分析

4. 1 实验目的

掌握 ICMP 协议的工作原理，理解 ICMP 分组结构。

4. 2 实验环境

1. 安装科来网络分析系统的连网的 Windows XP 主机两台。
2. 实验分组：两名同学一组，轮流进行实验。

4. 3 实验内容

用 ping 命令和科来网络分析系统分析 ICMP 包的基本结构以及回显请求与应答消息、目标不可达、超时等消息的 ICMP 报文的异同。

4. 4 实验步骤

在两台 PC 机上启动科来网络分析系统，开始抓包。

1. 回显请求及应答消息。

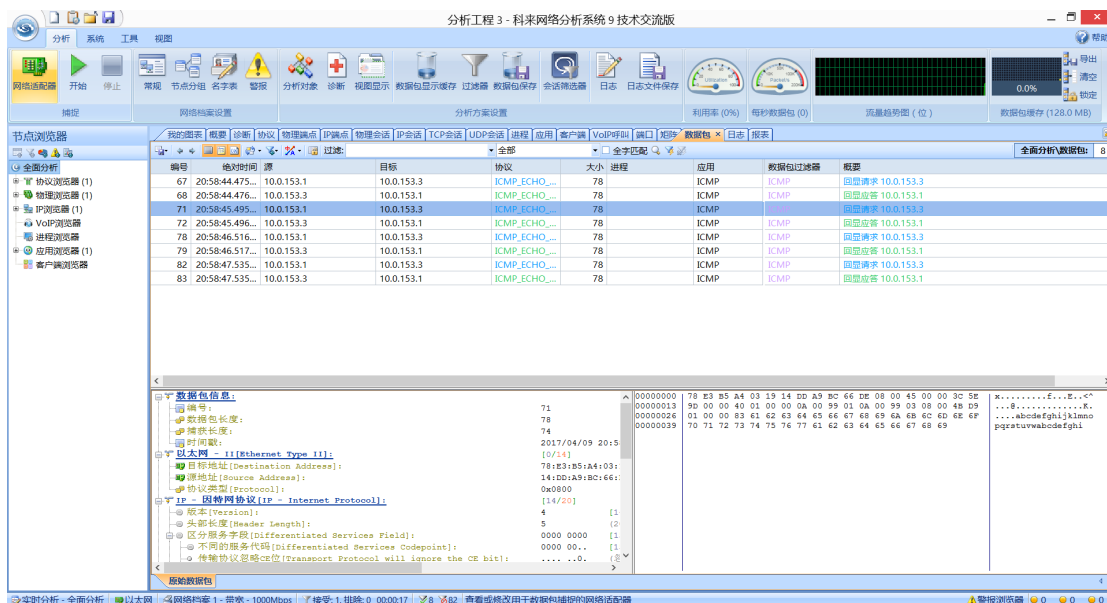
- 1) 在 PC1 上运行命令：ping 临机 IP。

```
C:\WINDOWS\system32>ping 10.0.153.3

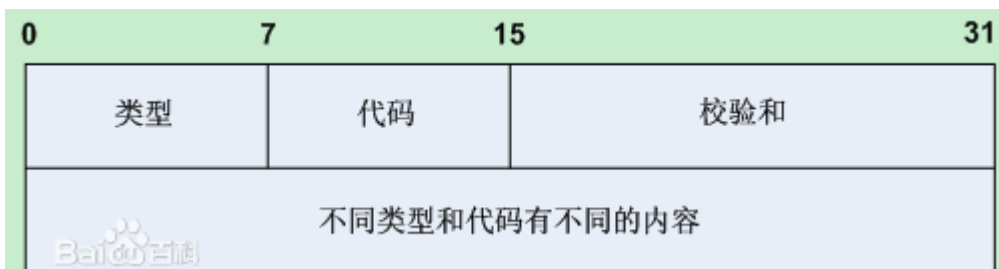
正在 Ping 10.0.153.3 具有 32 字节的数据:
来自 10.0.153.3 的回复: 字节=32 时间=1ms TTL=64
来自 10.0.153.3 的回复: 字节=32 时间=1ms TTL=64
来自 10.0.153.3 的回复: 字节=32 时间=1ms TTL=64
来自 10.0.153.3 的回复: 字节=32 时间=1ms TTL=64

10.0.153.3 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 = 1ms, 最长 = 1ms, 平均 = 1ms
```

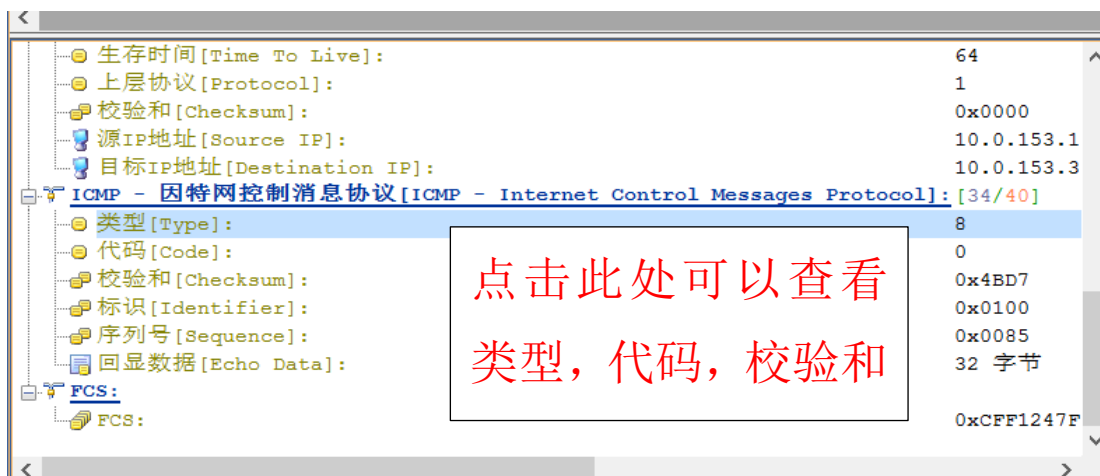
- 2) 命令执行后，停止抓包，分析 ICMP 报文，查看报文结构和首部格式以及首部中各字段的内容。



3) 说明 ICMP 报文首部各字段的含义以及所捕获的数据报属于什么报文。

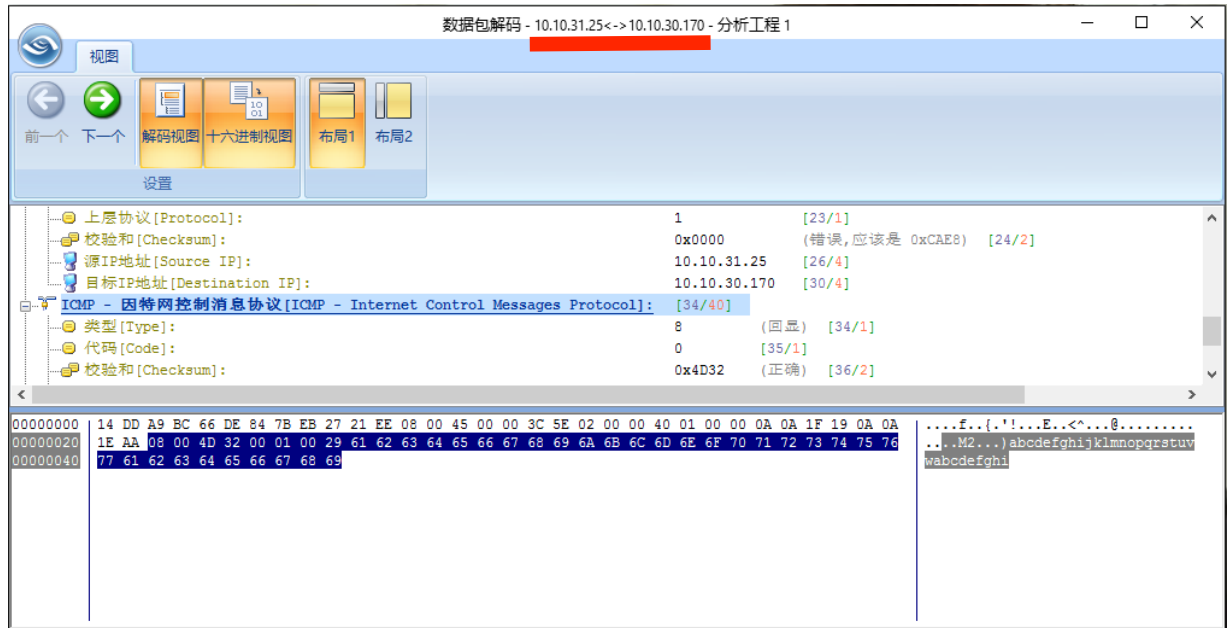


1. 类型: 占 8 位
2. 代码: 占 8 位
3. 校验和: 占 16 位



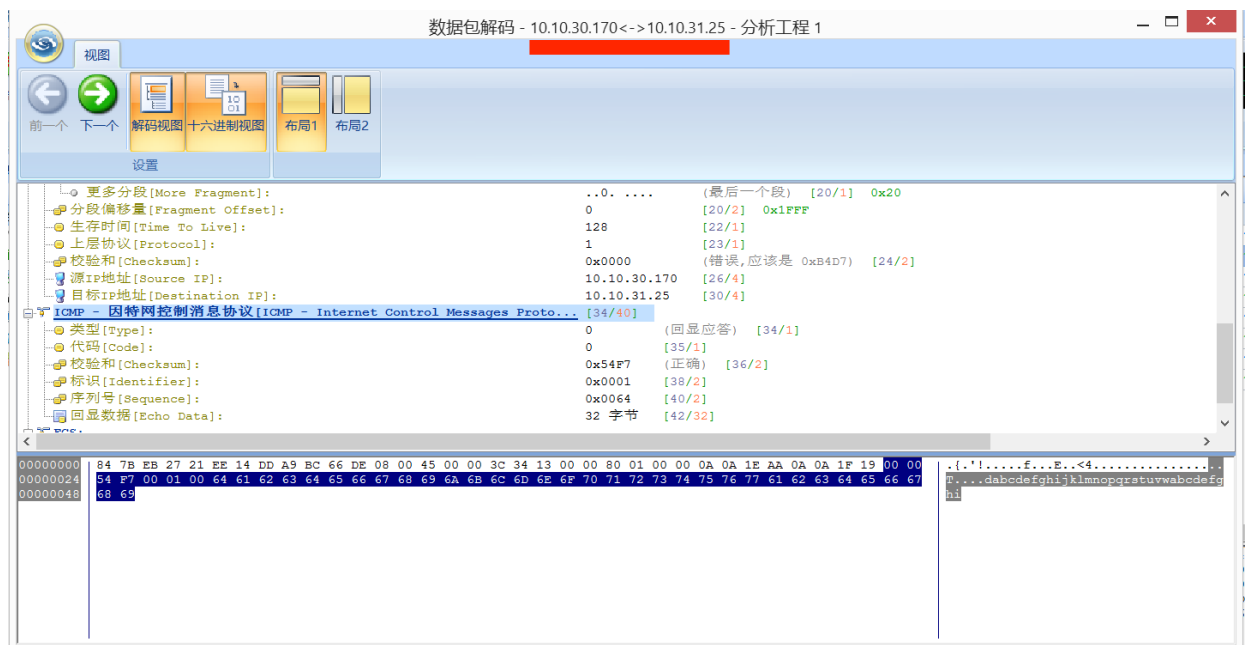
常用的 ICMP 报文如下表

ICMP 报文种类	类型的值	ICMP 报文的类型
差错报告报文	3	终点不可达
	4	源点抑制 (Source quench)
	11	时间超时
	12	参数问题
	5	改变路由 (Redirect)
询问报文	8 或 0	会送 (Echo) 请求或回答
	13 或 14	时间戳 (Timestamp) 请求或回答



类型: 08
 代码: 00
 校验和: 4D 32
 报文: ICMP 询问报文

4) 对 PC2 上捕获到的包进行分析, 说明 ICMP 报文首部各字段的含义以及所捕获的数据报属于什么报文。



类型: 00
 代码: 00
 校验和: 54 F7
 报文: ICMP 询问报文

2. 超时消息。

1) 在 PC1 上运行命令: ping 不存在的或者没有开机的计算机的 IP。

```
管理员: 命令提示符

Microsoft Windows [版本 10.0.10586]
(c) 2015 Microsoft Corporation。保留所有权利。

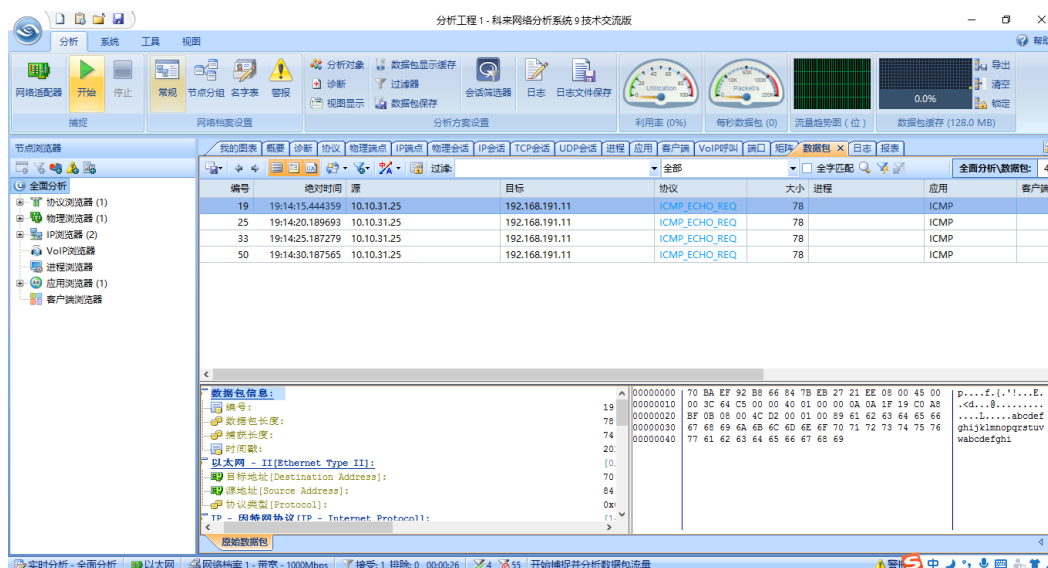
C:\WINDOWS\system32>ping 192.168.191.11

正在 Ping 192.168.191.11 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

192.168.191.11 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),

C:\WINDOWS\system32>
```

2) 停止抓包, 分析 ICMP 报文, 查看报文结构和首部格式以及首部中各字段的内容。



3) 说明 ICMP 报文首部各字段的含义以及所捕获的数据报属于什么报文。

类型: 00

代码: 00

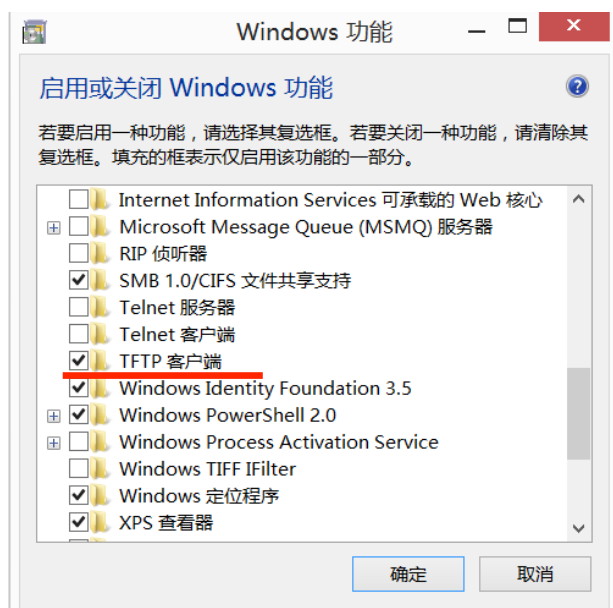
校验和: 54 F7

报文: ICMP 询问报

3. 端口不可达消息。

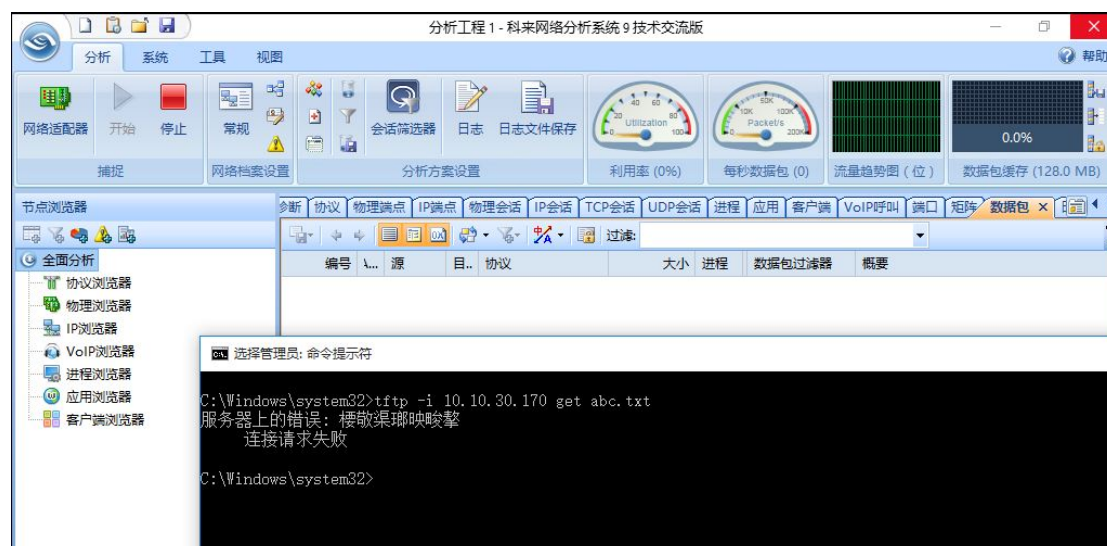
在 PC2 上启动 TFTP 服务器软件。

控制面板——程序——启动或关闭 windows 功能



在 PC1 上启动科来网络分析系统，开始抓包。

在 PC1 的命令窗口运行命令: tftp -I PC2 的 IP get 文件名 (该文件可能不存在);
停止抓包可以看到如图所示结果:



文件存在:

```
C:\WINDOWS\system32>tftp -i 10.10.30.170 put f:\xsw.txt
传输成功: 1 秒 0 字节, 0 字节/秒
```

编号	绝对时间	源	目标	协议	大小	进程	应用	数据包过滤器	概要
2467	12:13:26.047...	10.10.30.170	10.0.15.11	ICMP_DESTU...	571		ICMP	...	目标端口不可达

数据包解码 - 10.10.30.170<->10.0.15.11 - 分析工程 1

视图: 前一个 下一个 解码视图 十六进制视图 布局1 布局2

设置

- 分段标志 [Fragment Flags]:
 - 保留 [Reserved]: 0000... [20/1] 0x00
 - 分段 [Fragment]: 0... [20/1] 0x00
 - 更多分段 [More Fragment]: 0... [20/1] 0x00
 - 分段偏移量 [Fragment Offset]: 0... [20/2] 0x0000
 - 生存时间 [Time To Live]: 128 [22/1]
 - 上层协议 [Protocol]: 1 [23/1]
 - 校验和 [Checksum]: 0x0000 (错误, 应该是 0xC8B3) [24/2]
 - 源IP地址 [Source IP]: 10.10.30.170 [26/4]
 - 目标IP地址 [Destination IP]: 10.0.15.11 [30/4]
- ICMP - 因特网控制消息协议 [ICMP - Internet Control Messages Proto...]: [34/8]
 - 类型 [Type]: 3 (目的不可达) [34/1]
 - 代码 [Code]: 3 (端口不可达) [35/1]
 - 校验和 [Checksum]: 0x40C6 (正确) [36/2]
- IP - 因特网协议 [IP - Internet Protocol]: [42/20]
 - 版本 [Version]: 4 [42/1] 0xF0
 - 头部长度 [Header Length]: 5 (20 字节) [42/1] 0x0F
 - 区分服务字段 [Differentiated Services Field]: 0000 0000 [43/1] 0xFF
 - 不同的服务代码 [Differentiated Services Codepoint]: 0000 00.. [43/1] 0xFC
 - 传输协议忽略CE位 [Transport Protocol will ignore the CE bit]: 0.. (忽略) [43/1] 0x02

00000000 70 BA EF 92 B8 66 14 DD A9 BC 66 DE 08 00 45 00 02 29 2B 92 00 00 80 01 00 00 0A 0A 1E AA 0A 00 0F 0B 0B
00000008 03 40 C6 00 00 00 00 45 00 02 0D 3D 96 00 00 3C 11 FD 8B 0A 00 0F 0B 0A 0A 1E AA 00 35 ED 75 01 F9 49 E8
00000016 20 A6 81 80 00 01 00 02 00 0D 0B 0A 6E 65 78 75 73 72 75 6C 65 73 0A 6F 66 66 69 63 65 61 70 70 73 04
00000024 6C 69 76 65 03 63 6F 6D 00 00 01 00 01 C0 0C 00 05 00 01 00 09 FF 00 25 04 70 72 6F 64 0A 6E 65 78 75
00000032 73 72 75 6C 65 73 04 6C 69 76 65 03 63 6F 6D 06 61 6B 61 64 6E 73 03 6E 65 74 00 C0 3C 00 01 00 01 00 00
00000040 01 37 00 04 28 71 0E 9F 00 00 02 00 01 00 04 16 0E 00 11 01 67 0C 72 6F 6F 74 2D 73 65 72 76 65 72 73 C0

```
F:\Windows\system32>tftp -i 10.10.30.170 get xsw.txt
传输成功: 1 秒 0 字节, 0 字节/秒
```

分析工程 1 - 科来网络分析系统 9 技术交流版

分析 系统 工具 视图

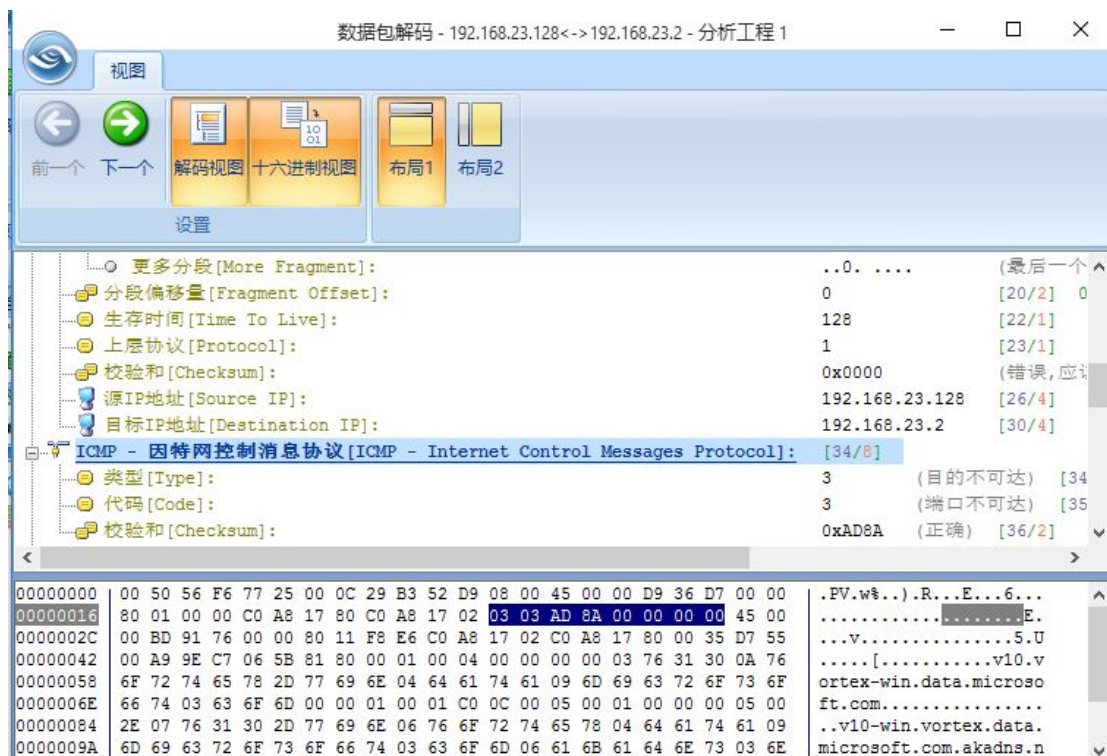
网络适配器 开始 停止 常规 会话筛选器 日志 日志文件保存

捕捉 网络档案设置 分析方案设置

利用率 (0%) 每秒数据包 (0) 流量趋势图 (位) 数据包缓存 (128.0 MB)

节点浏览器: 全面分析 协议浏览器 (1) 物理浏览器 (1) IP浏览器 (1) VoIP浏览器 进程浏览器 应用浏览器 (1) 客户端浏览器

编号	源	目标	协议	大小	进程	数据包过滤器	概要
303	192.1...	192.1...	ICMP_DESTUNR...	235		...	目标端口不可达
435	192.1...	192.1...	ICMP_DESTUNR...	583		...	目标端口不可达
463	192.1...	192.1...	ICMP_DESTUNR...	224		...	目标端口不可达

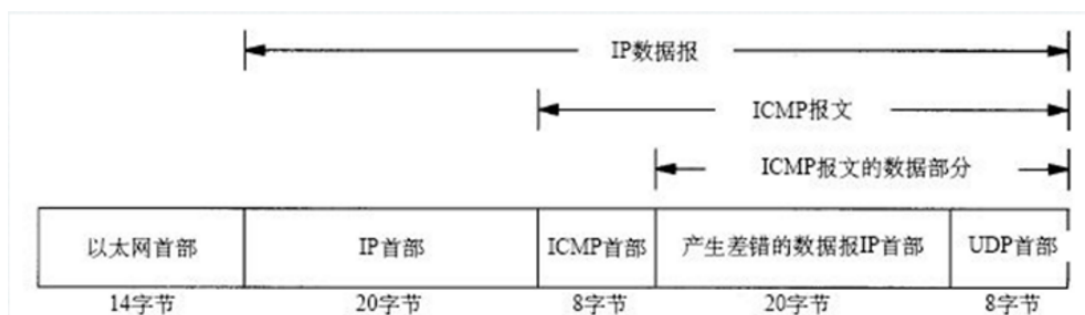


4. 5 实验要求

完成本次实验后，通过查找资料，整理并总结 ICMP 报文的各字段的意义，ICMP 各种消息的作用，进一步掌握网络连通性的测试方法。

4. 6 思考与讨论

1. 通过查资料，请描述协议不可达报文的结构以及首部字段的含义。



2. 总结 ICMP 类型与代码，简单描述其含义。

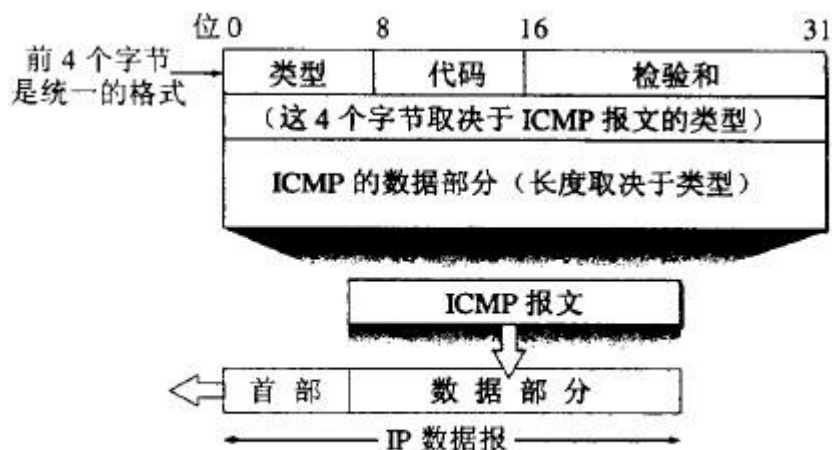


图 4-27 ICMP 报文的格式

Type	Code	类别	含义
0	0	查询	回送应答
3	0	差错	网络不可抵达
	1	差错	主机不可抵达
	2	差错	协议不可抵达
	3	差错	端口不可抵达
	4	差错	需要重新分片但设置了不分片比特
	5	差错	源路由失败
	6	差错	目的网络未知
	7	差错	目的主机未知
	8	差错	源主机被隔离
	9	差错	目的网络被禁止
	10	差错	目的主机被禁止
	11	差错	对所请求的服务类型, 网络不可达
	12	差错	对所请求的服务类型, 主机不可达
	13	差错	由于过滤, 通信被禁止
	14	差错	主机越权
	15	差错	优先级失效
4	0	差错	源端被关闭

5	0	差错	对网络重定向
	1	差错	对主机重定向
	2	差错	对服务类型和网络重定向
	3	差错	对服务类型和主机重定向
8	0	查询	请求回显
9	0	查询	路由器通告
10	0	查询	路由器请求
11	0	差错	传输期间数据报超时
	1	差错	数据报组装期间超时
12	0	差错	IP报头损坏
	1	差错	缺少必要的选项
13	0	查询	时间戳请求
14	0	查询	时间戳回复
15	0	查询	信息请求（已过时）
16	0	查询	信息回复（已过时）
17	0	查询	地址掩码请求
18	0	查询	地址掩码回复