IP/ICMP

一 实验目的

1. 深入理解 IP 协议的作用
2. 深入理解 IP 包的格式
3. 掌握 IP 的分片功能
4. 理解 ICMP 的作用

二 预备知识

1. IP 协议

IP 协议是将多个包交换网络连接起来，它在源地址和目的地址之间传送一种称之为数据包的东西，它还提供对数据大小的重新组装功能，以适应不同网络对包大小的要求。IP 不提供可靠的传输服务，它不提供端到端的或（路由）结点到（路由）结点的确认，对数据没有差错控制，它只使用报头的校验码，它不提供重发和流量控制。如果出错可以通过 ICMP 报告，ICMP 在 IP 模块中实现。

2. Ipv4 数据包格式

根据网络中的数据分层原理，在计算机网络中由于大都是使用 IP 进行网络互联，因此包的格式是有规律的，其中在当前公网中路由器支持的包也为 IP 格式包，因此我们通过分析抓取的 IP 包就可以得到包的部分信息。其中 IPV4 的包格式如下图示：

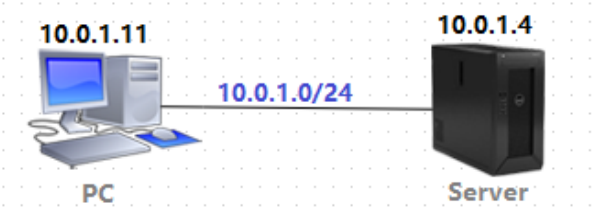
3. ICMP 协议

ICMP 全称 Internet Control Message Protocol（网际控制信息协议）。在网络体系结构的各层次中，都需要控制，而不同的层次有不同的分工和控制内容，IP 层的控制功能是最复杂的，主要负责差错控制、拥塞控制等，任何控制都是建立在信息的基础之上的，在基于 IP 数据报的网络体系中，网关必须自己处理数据报的传输工作，而 IP 协议自身没有内在机制来获取差错信息并处理。为了处理这些错误，TCP/IP 设计了 ICMP 协议，当某个网关发现

传输错误时，立即向信源主机发送 ICMP 报文，报告出错信息，让信源主机采取相应处理措施，它是一种差错和控制报文协议，不仅用于传输差错报文，还传输控制报文。

三 实验环境

在右上方的实验拓扑图菜单中选择 **IP/ICMP**，点击连线设置子网网段：



然后点击**提交实验**，等待资源分配成功后，点击图标再点击全屏访问即可进入设备进行实验(注：Server 账户密码均为 **centos**)。

四 实验内容

1. 捕包

进入 PC，打开 Wireshark 开始捕包，接下来打开命令提示符，制作一个 8000 字节的 ip 包发送到 10.0.1.4（`ping -l 8000 10.0.1.4`）。

```
C:\Documents and Settings\admin>ping -l 8000 10.0.1.4

Pinging 10.0.1.4 with 8000 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.1.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

2. 分析

默认情况下 ping 会发送四次 8000 字节的 ip 包，我们只分析其中一次的执行过程：

7	8.203209	00 10.0.1.11	10.0.1.4	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0047) [R
8	8.203257	00 10.0.1.11	10.0.1.4	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=0047)
9	8.203288	00 10.0.1.11	10.0.1.4	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=0047)
10	8.203322	00 10.0.1.11	10.0.1.4	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=4440, ID=0047)
11	8.203370	00 10.0.1.11	10.0.1.4	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=5920, ID=0047)
12	8.203403	00 10.0.1.11	10.0.1.4	ICMP	642	Echo (ping) request id=0x0200, seq=512/2, ttl=128

我们知道链路层具有最大传输单元 MTU 这个特性，它限制了数据帧的最大长度，不同的网络类型都有一个上限值。如果 IP 层有数据包要传，而且数据包的长度超过了 MTU，那么 IP 层就要对数据包进行分段（fragmentation）操作，使每一片的长度都小于或等于 MTU。

由上图可知 8000 字节的 IP 包被分成 6 个分组发送。

IP 首部包含了分片和重组所需的信息：

1. 16 位的标识（Identification）：发送端发送的 IP 数据包标识字段都是一个唯一值，该值在分片时被复制到每个片中。
2. 3 位的标志字段分别是：

R：保留未用。

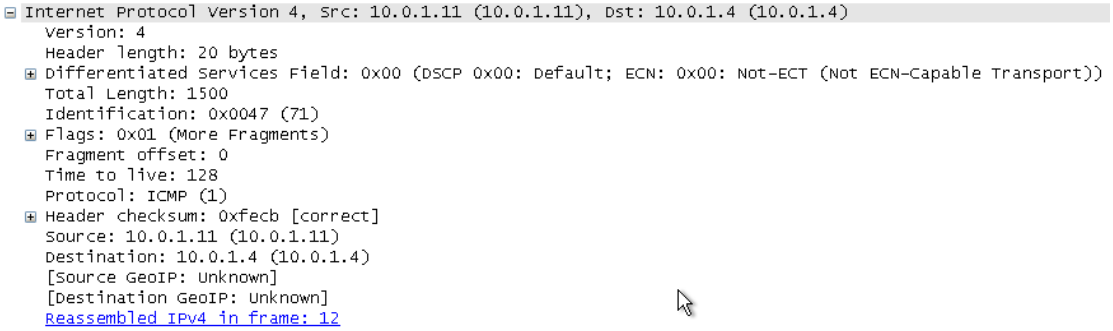
DF：Don't Fragment，“不分段”位，如果将这一比特置 1，IP 层将不对数据报进行分片。

MF：More Fragment，“更多的段”，除了最后一片外，其他每个组成数据报的片都要把该比特置 1。

3. Fragment Offset：该片偏移原始数据包开始处的位置。偏移的字节数是该值乘以 8。

另外，当数据报被分段后，每个片的总长度值要改为该片段的长度值。

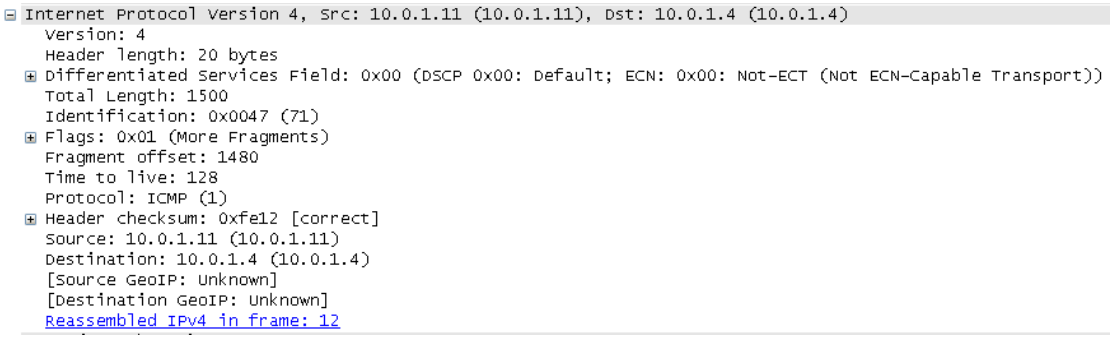
我们首先来分析第一个 IP 包:



由上图可知：

字段	值	备注
版本	4	IPV4
包头长度	5	报头长 20 字节
服务类型	0x00	正常时延、吞吐量、可靠性
总长度	1500	分组长度 1500 字节
标识	0x0047	序列号 71
标志	0x01	MF=1，DF=0，允许分片，此片不是最后一片
偏移值	0	偏移量为 0
生存周期	128	每跳生存周期为 128s
协议	1	携带的数据来自 ICMP 协议
头部校验和	0xfecb	IP 头部校验和为 fecb
源地址	10.0.1.11	源地址为 10.0.1.11
目的地址	10.0.1.4	目的地址为 10.0.1.4

上述为第一片，由于数据最长为 1500 字节，而 IP 头占据 20 字节，因此实际的数据只有 1480 字节，那么分组 2 偏移应该为 **1480**，实际我们采集到的 IP 分组 2 为：



由上图可知，分组的片偏移值为 1480，Flag 标志位值为 1 指明还有更多的分片。观察接下来的四个分组的片偏移值分别为 2960、4440、5920、7400。我们来查看最后一个分组后可以得到下列信息：

字段	值	备注
版本	4	IPV4
包头长度	20	报头长 20 字节
服务类型	0x00	正常时延、吞吐量、可靠性
总长度	**628**	分组长度 628 字节
标识	0x0047	序列号 71
标志	0x00	MF=0，DF=0，不允许分片，此片为最后一片
偏移值	7400	偏移量为 7400
生存周期	128	每跳生存周期为 128s
协议	1	携带的数据来自 ICMP 协议
头部校验和	0x1e97	IP 头部校验和为 1e97
源地址	10.0.1.11	源地址为 10.0.1.11
目的地址	10.0.1.4	目的地址为 10.0.1.2

分析以上分组分析可得：我们实际发送的有效数据的总长度 **8000=(1500-20)*5+(628-20-8)**。前五个分组都是由一个 IP 首部和有效数据区域组成，而最后一个分组实际上是由一个 IP 首部、一个 ICMP 首部(8 字节)及有效数据共同组成，所以有效数据的长度实际上为 628-20-8。