

# 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 IP 数据报分片实验 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 专业 软件工程  
实验时间 2022 年 10 月 25 日 下午 ~ 10 月 25 日 下午 温度      °C 湿度     

## 实验目的

1. 理解 IP 分片过程

## 实验原理

### IP 数据报分片实验原理

我们已经从前边的实验中看到，IP 报文要交给数据链路层封装后才能发送。理想情况下，每个 IP 报文正好能放在同一个物理帧中发送。但在实际应用中，每种网络技术所支持的最大帧长各不相同。例如：以太网的帧中最多可容纳 1500 字节的数据；FDDI 帧最多可容纳 4352 字节的数据。这个上限被称为物理网络的最大传输单元（MTU, Maxium Transfer Unit）。这是由网络所使用的硬件与软件所决定的。每种网络的数据链路层都有自己的帧格式，其中有一个字段是“数据字段最大长度”。当数据包封装成帧时，数据包的总长度必须小于这个数据字段最大长度，如下图所示。



不同网络的 MTU 值

协议	MTU	协议	MTU
超级通道 (Hyperchannel)	65535	以太网	1500
令牌环 (16Mbps)	17914	X. 25	576
令牌环 (4Mbps)	4464	PPP	296
FDDI	4352	——	——

# 暨南大学本科实验报告专用纸(附页)

为了使 IP 协议与物理网络无关，IP 协议不考虑底层网络的 MTU，只是规定 IP 数据包的最大负载长度为 65535 字节。对于物理网络，如果数据包的长度超过了 MTU，就要把数据包进行分割，使它们能够通过这些网络，这就叫做分片。源主机的传输层会自动对数据包进行分片工作，把数据包划分成 IP 协议和数据链路层都可接受的大小。

当数据包被分片时，每一个数据包片有它自己的首部，其中大部分的字段都是重复的，但有些是不同的。如果已经分片的数据包要经过更小 MTU 的网络，那么这些已经分片的数据包还可再进行分片，数据包在到达最后终点之前可以经过多次的分片。

数据包可以被源主机或在其路径上的路由器进行分片。但是数据包的重装却只能在目的主机上进行。由于被分片的数据包可能会通过不同的路由到达目的主机，所以应当在最后的目的地主机上进行重装。当数据包被分片时，首部中的一些字段会被复制到所有的分片中（选项字段可以被复制，也可不被复制）。有三个字段是与数据包分片相关的，这三个字段是：标识字段、标志字段和偏移量字段。当然，不管是否进行分片，校验和的值总是要重新计算的。

对于最大传输单元（MTU）还可以理解为某层协议报文可携带数据的最大长度，对于不同协议，对应的 MTU 可能会有不同的值和计算方法。如我们常说的“以太网 MTU 为 1500”，说的是以太网 MAC 帧可封装的最大数据长度，其只包含 IP 报头及其上层协议数据的总长度。对于 IP 协议的 MTU 值应为 65535-20，也只是说一个 IP 数据报（包含 IP 包头的长度和 IP 上层协议数据的长度），最多可以携带 65535 个字节的数据。

与数据包的分片和重装有关的三个字段是：标识字段、标志字段和偏移量字段。

- 标识：IP 数据包的标识字段值与源 IP 地址唯一地确定了一个数据包。IP 协议使用一个计数器来保证每个数据包标识的唯一性。当 IP 协议发送数据包时，就把这个计数器的当前值复制到标识字段中，并把这个计数器的值加 1。当数据包被分片时，标识字段的值就复制到所有的分片中。这样所有的分片具有相同的标识。

这个标识号在终点重装数据包时很有用。终点会将所有具有相同标识号的分片组装成一个数据包。

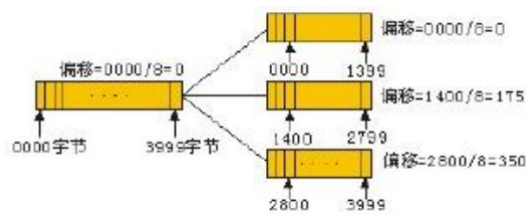
标志：这是一个长度为 3 位的字段。第一位保留。第二位是不分片位。若这个位为 1，就表示不能把该数据包进行分片。若无法把这个数据包通过任何可用的物理网络进行转发，就丢弃这个数据包，并向源主机发送 ICMP 差错报文（关于 ICMP 差错报文，参见实验 4）。若这个位为 0，则在需要时可把这个数据包进行分片。

# 暨南大学本科实验报告专用纸(附页)

- 第三位 是还有分片位。若这个位是 1，则表示这个数据包不是最后的分片，在这个分片后 面还有其它分片。若这个位是 0，则表示这是最后的分片。标志字段如下图所示：



- 偏移量：偏移量字段表示一个分片在整个数据包中的相对位置。以 8 字节为度量单 位。下图表示具有 4000 字节长度的数据包被划分为三个分片。在原始数据包 中的 数据编号是 0~3999。第一个分片携带的数据是字节 0~1399。对于这个数 据包， 偏移量是  $0 / 8 = 0$ 。第二个分片携带的数据是字节 1400~2799；对于这个 数据包， 偏移量是  $1400 / 8 = 175$ 。最后，第三个分片携带的数据是字节 2800~ 3999。对于 这个数据包，偏移量是  $2800 / 8 = 350$ 。如下图：



偏移量字段的长度只有 13 位，它不能表示超过 8191 的字节数，所以偏移量是以 8 字节为单位的。因此，把数据包进行分片的主机或路由器必须选择一个能够被 8 整除的长度来为数据包分片。

TCP/IP 协议在发送 IP 数据报文时，一般选择一个合适的初始长度。当这个报文要从一个 MTU 大的子网发送到一个 MTU 小的网络时，IP 协议就把这个报文的数据部分分割成能被目的子网所容纳的较小数据分片，组成较小的报文发送。每个较小的报文被称为一个分片（Fragment）。每个分片都有一个 IP 报文头，分片后的数据报的 IP 报头和原始 IP 报 头除分片偏移、MF 标志位和校验字段不同外，其他都一样。图 25 显示了 Wireshark 捕获 的 IP 数据报分片的分析情况，可参考。

# 暨南大学本科实验报告专用纸(附页)

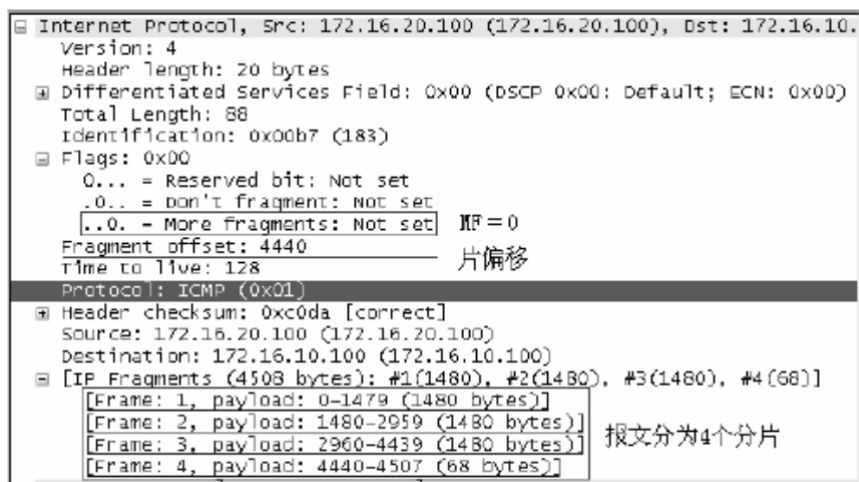


图 25 IP 数据报分片示例

重组是分片的逆过程，分片只有到达目的主机时才进行重组。当目的主机收到 IP 报文时，根据其片偏移和标志 MF 位判断其是否是一个分片。若 MF 为 0，片偏移为 0，则表明它是一个完整的报文；否则，则表明它是一个分片。当一个报文的全部分片都到达目的主机时，IP 就根据报头中的标识符和片偏移将它们重新组成一个完整的报文交给上层协议处理。

## 实验环境与说明

### (1) 实验目的

使用 Ping 命令在两台计算机之间发送大于 MTU 的数据报，验证分片过程，加深对 IP 协议的理解。

### (2) 实验设备和连接

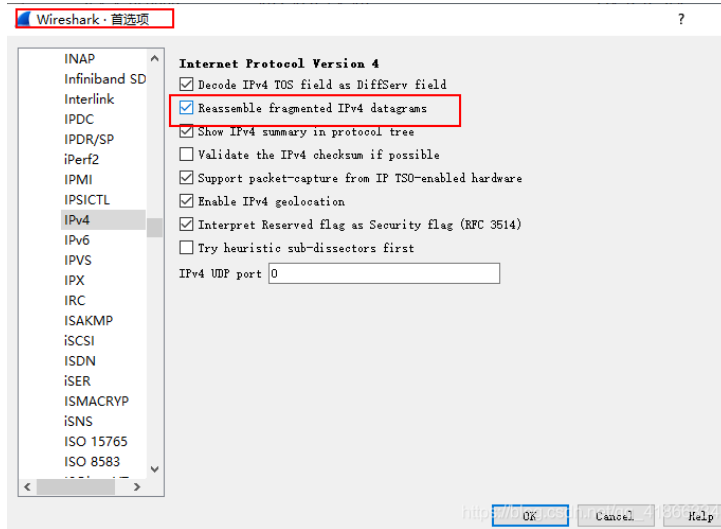
与 4.3.1 和 4.3.2 实验完全相同。

### (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。

注：为了更好地观察 IP 分片过程，本实验需要取消 Wireshark 自动组装分片的设置，操作如下：

# 暨南大学本科实验报告专用纸(附页)



## 实验步骤

### 练习一、运行 ping 命令分析 IP 分片情况

步骤 1:

在主机 A、主机 B 两台计算机上运行 Wireshark，为了只截获和实验有关的数据报，设置 Wireshark 的截获条件为对方主机的 IP 地址，开始截获报文；

步骤 2:

在主机 A 上执行如下 Ping 命令，向主机 B 发送 4500B 的数据报文：

Ping -l 4500 -n 1 主机 B IP 地址

步骤 3:

停止截获报文，分析截获的报文，回答下列问题：

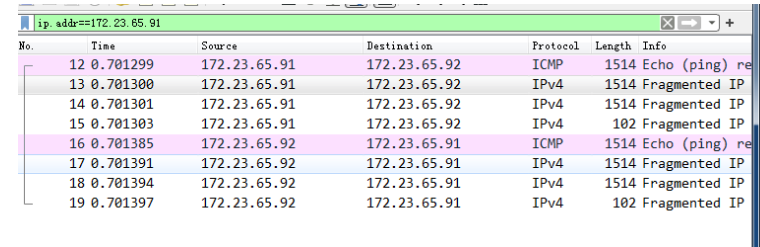
1) 以太网的 MTU 是多少？

答：1500 bytes。

2) 对截获的报文分析，将属于同一 ICMP 请求报文的分片找出来，主机 A 向主机 B 发送的 ICMP 请求报文分成了几个分片？

# 暨南大学本科实验报告专用纸(附页)

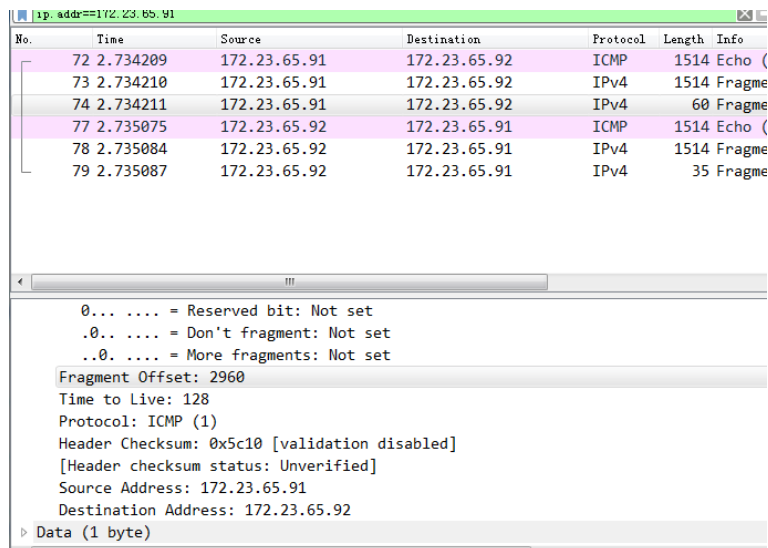
答：四片；



No.	Time	Source	Destination	Protocol	Length	Info
12	0.701299	172.23.65.91	172.23.65.92	ICMP	1514	Echo (ping) request
13	0.701300	172.23.65.91	172.23.65.92	IPv4	1514	Fragmented IP
14	0.701301	172.23.65.91	172.23.65.92	IPv4	1514	Fragmented IP
15	0.701303	172.23.65.91	172.23.65.92	IPv4	102	Fragmented IP
16	0.701385	172.23.65.92	172.23.65.91	ICMP	1514	Echo (ping) response
17	0.701391	172.23.65.92	172.23.65.91	IPv4	1514	Fragmented IP
18	0.701394	172.23.65.92	172.23.65.91	IPv4	1514	Fragmented IP
19	0.701397	172.23.65.92	172.23.65.91	IPv4	102	Fragmented IP

3) 若要让主机 A 向主机 B 发送的数据分为 3 个分片，则 Ping 命令中的报文长度应大于多少？为什么？

答：应该 $\geq 2952$ bytes，因为第一片数据最大长度为 1472 字节，第二片数据最大长度为 1480 字节，所以需要分三片报文总长度应大于 2952 字节。



No.	Time	Source	Destination	Protocol	Length	Info
72	2.734209	172.23.65.91	172.23.65.92	ICMP	1514	Echo (ping) request
73	2.734210	172.23.65.91	172.23.65.92	IPv4	1514	Fragmented IP
74	2.734211	172.23.65.91	172.23.65.92	IPv4	60	Fragmented IP
77	2.735075	172.23.65.92	172.23.65.91	ICMP	1514	Echo (ping) response
78	2.735084	172.23.65.92	172.23.65.91	IPv4	1514	Fragmented IP
79	2.735087	172.23.65.92	172.23.65.91	IPv4	35	Fragmented IP

Field	Value
0... .. = Reserved bit:	Not set
.0... .. = Don't fragment:	Not set
..0. .... = More fragments:	Not set
Fragment Offset:	2960
Time to Live:	128
Protocol:	ICMP (1)
Header Checksum:	0x5c10 [validation disabled]
[Header checksum status:	Unverified]
Source Address:	172.23.65.91
Destination Address:	172.23.65.92
Data (1 byte)	

3) 片段中 IP 标头中的哪些字段发生了变化？

答：标志位 偏移值 检验字段

5) 将第二个 ICMP 请求报文的分片信息填入下表中：

分片序号	标识(Identification)	标志(Flag)	片偏移(Fragment Offset)	数据长度
1	0x0273 (627)	0x20	0	1472
2	0x0273 (627)	0x20	1480	1480
3	0x0273 (627)	0x21	2960	1480
4	0x0273 (627)	0x02	4440	68

# 暨南大学本科实验报告专用纸(附页)

思考问题:

1. Ping 的数据部分为 3000 字节, 回显请求报文为何被分为 3 片而不是 2 片?

答: 由第三问可知, 两片分组最多只能装 2952 个 byte; 所以 3000byte 的报文只能被分为 3 片。

2. 数据部分长度为多少时报文正好被分为 2 片?

答: 当长度为 1473byte 时

序	时间	源地址	目标地址	协议	长度	应用
52	1.959223	172.23.65.91	172.23.65.92	ICMP	1514	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 56)
53	1.959227	172.23.65.91	172.23.65.92	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=0290)

## 练习二、执行 ping 命令观察不分片标志位对 IP 分片的影响

步骤 1:

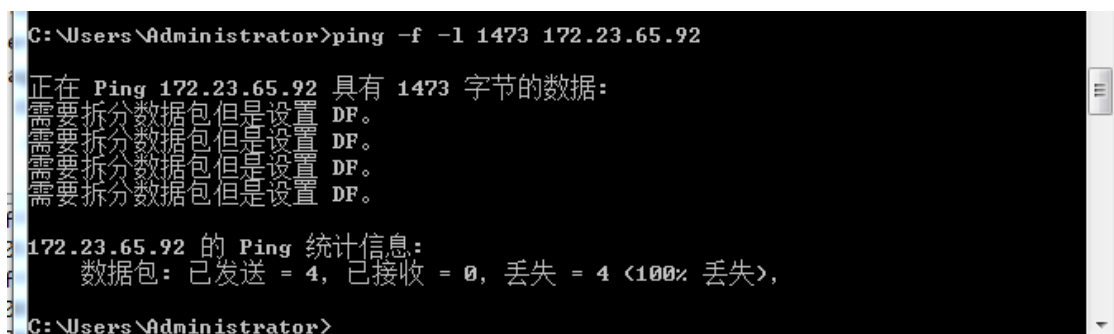
在主机 A 上执行“ping -f -l 1472 主机 B IP 地址”命令, 其中参数-l 是设置 ping 命令的数据的大小; 参数-f 是将该 IP 报文设置为不可分片。观察记录执行结果。

步骤 2:

在主机 A 上执行“ping -f -l 1473 主机 B IP 地址”命令, 观察记录执行结果。回答下列问题:

1) 将数据包长度设置为 1472 能正常发送, 而 1473 就不能, 为什么?

答: 因为由练习一可以知道, 第一片报文长度数据部分只能发送 1475byte (总长度 1514 - 以太网首部 14 - ip 首部 20 - icmp 首部 8); 而-f 参数限定不能分组发送, 所以该数据包不能正常发送。



```
C:\Users\Administrator>ping -f -l 1473 172.23.65.92

正在 Ping 172.23.65.92 具有 1473 字节的数据:
需要拆分数据包但是设置 DF。
需要拆分数据包但是设置 DF。
需要拆分数据包但是设置 DF。
需要拆分数据包但是设置 DF。

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

C:\Users\Administrator>
```

## 实验总结

了解了 IP 数据报的分片发送的特点



# 暨南大学本科实验报告专用纸(附页)

---