# IP 协议分析实验

【实验目的】

1. 掌握 IP 数据报的报文格式
2. 掌握 IP 校验和计算方法
3. 掌握子网掩码和路由转发
4. 理解特殊 IP 地址的含义

【实验原理】

1. IP 协议介绍

IP（网际协议）是 TCP/IP 协议族中最核心的协议，它负责将数据包从源点交付到终点。所有的 TCP、UDP、ICMP 及 IGMP 数据都以 IP 数据报格式传输。IP 协议提供不可靠、无连接的数据报传送服务，即它对数据进行“尽力传输”，只负责将数据包发送到目的主机，不管传输正确与否，不做验证、不发确认、也不保证 IP 数据包到达顺序，将纠错重传问题交由传输层来解决。

（1）IP 地址的编址方法

IP 地址是为每个连接在互联网上的主机分配的唯一识别的 32 位标识符。IP 地址的编址方法共经历了三个阶段：

* 分类的 IP 地址

这是一种基于分类的两级 IP 地址编址的方法。

表 8 IP 地址的分类

| IP 地址<br>类型 | 第一字节<br>十进制范围 | 二进制<br>固定最高位 | 二进制<br>网络位 | 二进制<br>主机位 |
|---|---|---|---|---|
| A 类 | 1-126 | 0 | 8 位 | 24 位 |
| B 类 | 128 －191 | 10 | 16 位 | 16 位 |
| C 类 | 192 －223 | 110 | 24 位 | 8 位 |
| D 类 | 224 －239 | 1110 | 组播地址 | |
| E 类 | 240 －254 | 1111 | 保留试验使用 | |

如表 8 所示，IP 地址分为 A，B，C，D，E 五类，其中 A、B、C 类地址为可分配主机地址，而 D 类地址为组播地址，E 类地址保留以备将来的特殊使用。IP 地址采用点分十进制方式记录，每个地址表被视为 4 个以点分隔开的十进制整数，每个整数对应一个字节。

A、B、C 三类地址由两部分组成：网络地址和主机地址，这三类地址的网络地址部分的长度不一样。每个 A 类地址的网络中可以有 1600 万台主机；每个 B 类地址的网络中可以有 65534 台主机；每个 C 类地址的网络中可以有 254 台主机。

这样对于一个共有几十台计算机的局域网来说即使分配一个 C 类地址也是一种浪费。为此，提出了子网和子网掩码的概念。

* 划分子网的 IP 地址

子网就是将一个 A 类、B 类或 C 类网络分割成许多小的网络，每一个小的网络就称为子网。划分子网采用 “网络号”＋“子网号”＋“主机号”三级编址的方法。在划分了子网的网络地址中，子网掩码用于确定网络地址。

子网掩码是一个和 IP 地址对应的 32 位二进制数。子网掩码中与 IP 地址的网络地址对应的部分为 1，与主机地址对应的部分为 0。这样把网络接口的 IP 地址与该接口上的掩

码相与就得到该接口所在网络的网络地址，而把该 IP 地址与掩码的反码相与则可得到主机地址。

＊ 无分类域间路由选择 CIDR

无分类域间路由选择 CIDR 是根据划分子网阶段的问题提出的编址方法。IP 地址采用“网络前缀”＋“主机号”的编址方式。目前 CIDR 是应用最广泛的编址方法，它消除了传统的 A、B、C 类地址和划分子网的概念，提高了 IP 地址资源的利用率，并使得路由聚合的实现成为可能。

（2）IP 报文格式

IP 报文由报头和数据两部分组成，如图 23 所示：

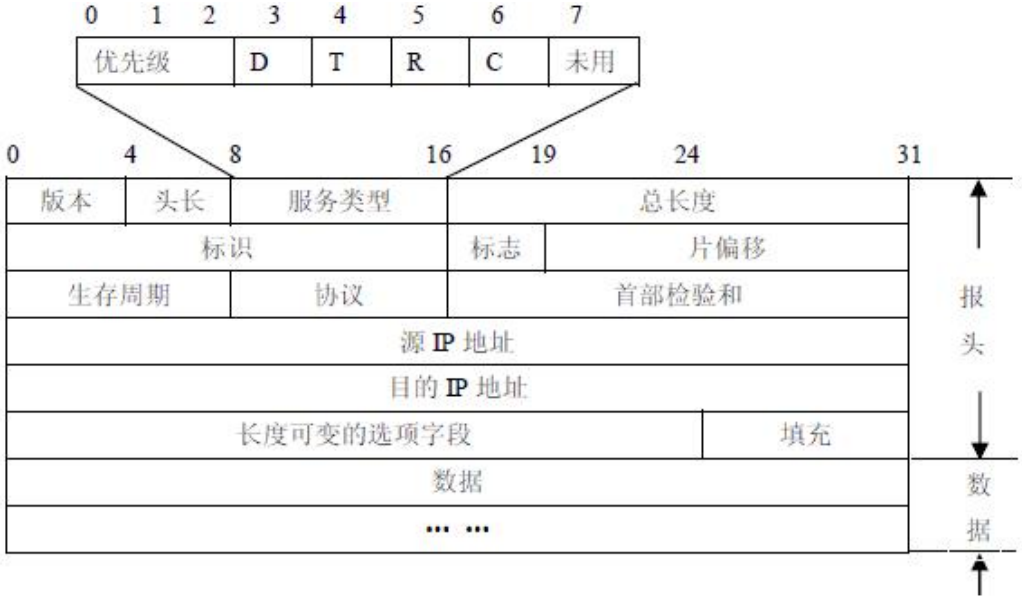


图 23　IP 报文格式

其中主要字段的意义和功能如下：

＊ 版本：指 IP 协议的版本；

＊ 头长：是指 IP 数据报的报头长度，它以 4 字节为单位。IP 报头长度至少为 20 字节，如果选项部分不是 4 字节的整数倍时，由填充补齐；

＊ 总长度：为整个 IP 数据报的长度；

＊ 服务类型：规定对数据报的处理方式；

＊ 标识：是 IP 协议赋予数据报的标志，用于目的主机确定数据分片属于哪个报文；

＊ 标志：为三个比特，其中只有低两位有效，这两位分别表示该数据报文能否分段和是否该分段是否为源报文的最后一个分段；

＊ 生存周期：为数据报在网络中的生存时间，报文每经过一个路由器时，其值减 1，当生存周期变为 0 时，丢弃该报文；从而防止网络中出现循环路由；

＊ 协议：指 IP 数据部分是由哪一种协议发送的；

＊ 校验和：只对 IP 报头的头部进行校验，保证头部的完整性；

＊ 源 IP 地址和目的 IP 地址：分别指发送和接收数据报的主机的 IP 地址。

（3）IP 数据报的传输过程

在互联网中，IP 数据报根据其目的地址不同，经过的路径和投递次数也不同。当一台主机要发送 IP 数据报时，主机将待发送数据报的目的地址和自己的子网掩码按位“与”，判断其结果是否与其所在网络的网络地址相同，若相同，则将数据报直接投递给目的主机，

否则，将其投递给下一跳路由器。

路由器转发数据报的过程如下：

① 当路由器收到一个数据报文时，对和该路由器直接相连的网络逐个进行检查，即用目的地址和每个网络的子网掩码按位 “与”，若与某网络的网地址相匹配，则直接投递；否则，执行 2。

② 对路由表的每一行，将其中的子网屏蔽码与数据报的目的地址按位“与”，若与该行的目的网络地址相等，则将该数据报发往该行的下一跳路由器；否则，执行 3。

③ 若路由表中有一个默认路由，则将数据报发送给路由表所指定的默认路由器。否则，报告转发出错。

2．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数据报，用 Wireshark 截获数据报，分析 IP 数据报的格式，理解 IP V4 地址的编址方法，加深对 IP 协议的理解。

（2）实验设备和连接

实验设备和连接图如图 24 所示，一台锐捷 R1760 路由器连接 2 台 PC 机，分别命名为主机 A、主机 B。

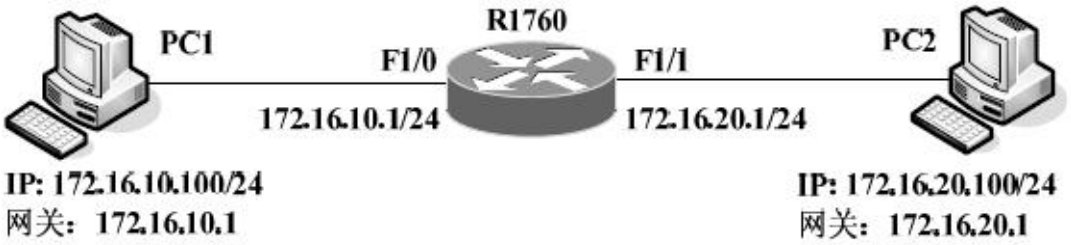


图 24 IP 协议分析实验连接图

（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。

3．实验步骤

【注】按照指导老师的要求配置好网络结构及 IP 地址，网络拓朴验证正确后，在主机 B 在命令行方式下输入 staticroute_config 命令，开启静态路由服务。

练习一、分析真实的 IP 报文

步骤 1：分别在主机 A 和主机 B 上运行 Wireshark，开始截获报文，为了只截获和实验内容有关的报文，将 Wireshark 的 Captrue Filter 设置为 “icmp”；

步骤 2：截获主机 A 上 ping 主机 B 的报文，结果保存为 IP-学号；

步骤 3：任取一个数据报，分析 IP 协议的报文格式，完成下列各题：

1）分析 IP 数据报头的格式，完成表 9；

表 9 IP 协议报文分析

| 字段 | 报文信息 | 说明 |
|---|---|---|
| 版本 | | |
| 头长 | | |
| 服务类型 | | |

| | | |
|---|---|---|
| 总长度 | | |
| 标识 | | |
| 标志 | | |
| 片偏移 | | |
| 生存周期 | | |
| 协议 | | |
| 校验和 | | |
| 源地址 | | |
| 目的地址 | | |

2）查看该数据报的源 IP 地址和目的 IP 地址，他们分别是哪类地址？体会 IP 地址的编址方法。

3）说明 IP 地址与硬件地址的区别，为什么要使用这两种不同的地址？

练习二、特殊的 IP 地址

本练习将主机 A、B、C、D、E、F 作为一组进行实验。

1. 直接广播地址

(1) 主机 A 编辑 IP 数据报 1，其中：

目的 MAC 地址：FFFFFF-FFFFFF。

源 MAC 地址：A 的 MAC 地址。

源 IP 地址：A 的 IP 地址。

目的 IP 地址：172.16.1.255。

自定义字段数据：填入大于 1 字节的用户数据。

校验和：在其它字段填充完毕后，计算并填充。

- 记录实验结果

| | 主机号 |
|---|---|
| 收到主机 A 发送的 IP 数据报 | |
| 未收到主机 A 发送的 IP 数据报 | |

结合实验结果，简述直接广播地址的作用。

2. 受限广播地址

(1) 主机 A 编辑一个 IP 数据报，其中：

目的 MAC 地址：FFFFFF-FFFFFF。

源 MAC 地址：A 的 MAC 地址。

源 IP 地址：A 的 IP 地址。

目的 IP 地址：255.255.255.255。

自定义字段数据：填入大于 1 字节的用户数据。

校验和：在其它字段填充完毕后，计算并填充。

(2) 主机 B、C、D、E、F 运行 Wireshark，开始截获报文，设置过滤条件（提取 IP 协议，捕获 源IP地址为172.16.1.2接收和发送的所有 IP 数据包）。

(3) 主机 A 同时发送这两个数据报。

(4) 主机 B、C、D、E、F 停止捕获数据。

- 记录实验结果

| | 主机号 |
|---|---|
| 收到主机 A 发送的 IP 数据报 | |
| 未收到主机 A 发送的 IP 数据报 | |

结合实验结果，简述受限广播地址的作用。

---

练习三、编辑并发送 IP 数据报

主机 A 再编辑 IP 数据报 2，其中：

目的 MAC 地址：主机 B 的 MAC 地址（对应于 172.16.1.1 接口的 MAC）。

源 MAC 地址：A 的 MAC 地址。

源 IP 地址：A 的 IP 地址。

目的 IP 地址：E 的 IP 地址。

自定义字段数据：填入大于 1 字节的用户数据。

校验和：在其它字段填充完毕后，计算并填充。

(3) 主机 B、C、D、E、F 运行 Wireshark，开始截获报文，设置过滤条件（提取 IP 协议，捕获 源IP地址为172.16.1.2接收和发送的所有 IP 数据包）。

(5) 主机 A 同时发送这两个数据报。

(6) 主机 B、C、D、E、F 停止捕获数据。

- 记录实验结果

| | 主机号 |
|---|---|
| 收到主机 A 发送的 IP 数据报 | |
| 未收到主机 A 发送的 IP 数据报 | |

结合实验结果，简述该数据报在发送端到接收端的传输过程，并指定哪些字段在传输过程中发生变化，为什么会这样？

---