**Lab21\_IP 数据包分析实验项目**

学生姓名：苏家铭 合作学生：无

实验地点：济世楼 330 实验时间：2023 年 12 月 20 日

**【实验目的】**

IP 协议是 TCP/IP 模型的核心协议，IP 数据包是网际网上进行传输的网络数据包，所有的传输与处理都围绕 IP 数据包展开，因此，了解 IP 数据包格式，理解每一个数据域含义，对于网际网的传输机制理解至关重要。本实验将借助 Tcpdump 工具，捕获和分析 IP 数据包。

1. 了解 IP 数据包格式以及各个数据域含义。
2. 了解 IP 数据包传输原理。

**【实验原理】**



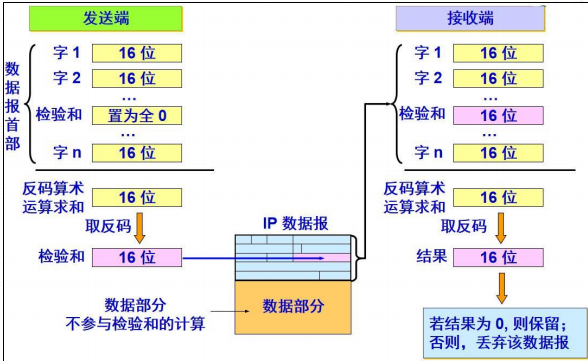
数据报文结构

1. IP 数据报文是在 IP 协议下进行传输的数据单位。它包含报头区和数据区两个主要部分。 报头区是 IP 数据报的头部信息，用于传输和处理数据的控制信息。报头区固定字段（20 字节）的格式如下：
2. 版本（Version）：指示 IP 协议的版本，通常为 IPv4 或 IPv6，占用 4 个位。
3. 首部长度（Header Length）：指示报头区的长度，以字节为单位，占用 4 个字节，可表示的最大数值为 15 个单位，一个单位为 4 位，因此 IP 的首部长度的最大值为 60。
4. 区分服务（Differentiated Services）：用于指定数据包的服务质量要求，如优先级、拥塞控制等，占用 8 个位，但实际上一直未被使用。
5. 总长度（Total Length）：指示整个 IP 数据报的总长度，包括报头区和数据区，以字节为单位，占 16 位，指首部和数据之和的长度，因此数据包的最大长度位 65535 字节。总长度必须不超过最大传送单元 MTU。
6. 标识（Identification）：用于标识和重组分片后的数据报，占 16 位，是一个计数器，用来产生 IP 数据报的标识。
7. 标志（Flags）：包含分片偏移和是否分片的标志位，标志只占 3 位，目前只有前两位有意义，标志字段的最低位是 MF（More Fragment）。MF = 1 表示后面还有分片；MF = 0 表示最后一个分片。标志字段中间的一位是 DF（Don’t Fragment）。只有当 DF = 0 的时候才允许分片。片偏移占 13 位，指出：较长的分组在分片后某片在原分组中的相对位置。片偏移以 8 个字节为偏移单位。
8. 生存时间（Time to Live）：指示数据包在网络中可以经过的最大路由跳数，每经过一个路由器该值减 1，当生存时间为 0 时数据报将被丢弃。
9. 协议（Protocol）：指示数据报的上一层——传输层的协议类型，如 TCP、UDP 等。
10. 首部校验和（Header Checksum）：用于检测报头区的传输错误。
11. 源地址（Source Address）：指示发送端的 IP 地址。
12. 目的地址（Destination Address）：指示接收端的 IP 地址。

IP 数据报的可选字段是在报头区的固定部分之后，长度可变的字段。这些可选字段提供了额外的功能和选项，根据需要选择性地添加到 IP 数据报中。这里支持排错、测量以及安全等措施，内容很丰富，选项字段的长度可变，从 1 字节到 40 字节不等，取决于所选择的项目。

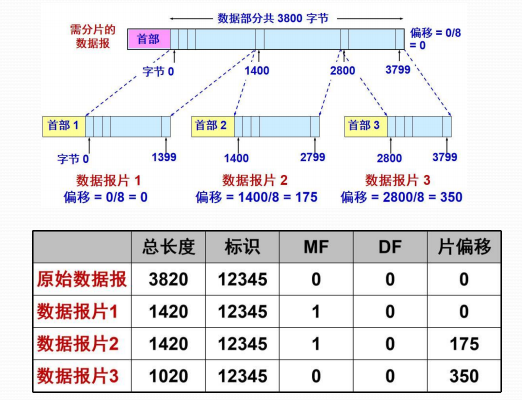
数据区包含高层协议传输的实际数据。它的格式和内容取决于上层协议，如 TCP 或 UDP。

IP 数据报首部检验和的计算采用 16 位二进制反码求和算法



IP 数据报分段

给出一数据报的总长度为 3820 字节，其数据部分的长度为 3800 字节（使用固定首部），需要分片为长度不超过 1420 字节的数据报片。因固定首部长度为 20 字节，因此每个数据报片的数据部分长度不能超过 1400 字节。于是分为 3 个数据报片，其数据部分的长度分别为 1400、1400 和 1000 字节。 原始数据报首部被复制为各数据报片的首部，但必须修改有关字段的值（如标志字段）。



IP 数据报文格式传输

注意，上图表示的数据，最高位在左边，记为 0 位；最低位在右边，记为 31 位。在网络中传输数据时，先传输 0～7 位，其次是 8～15 位，然后传输 16～23 位，最后传输 24～31 位。



IP 数据报文上层协议

IP 数据报文的 TOS：

服务类型（TOS、type of service）：占用 8 位二进制位，用于规定本数据报的处理方式。服务类型字段的 8 位分成了 5 个子域：

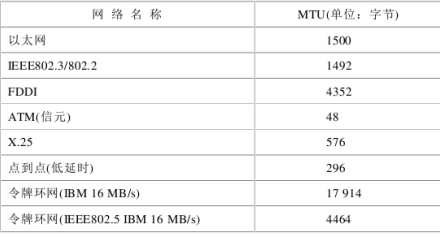
1. 优先权（0-7）数越大，表示该数据报优先权越高。网络中路由器可以使用优先权进行拥塞控制，如当网络发生拥塞时可以根据数据报的优先权来决定数据报的取舍。
2. 短延迟位 D（Delay）：该位置 1 时，数据报请求以短延迟信道传输，0 表示正常延时。
3. 高吞吐量位 T（Throughput）：该位置 1 时，数据报请求以高吞吐量信道传输，0 表示普通。
4. 高可靠位 R（Reliability）：该位置 1 时，数据报请求以高可靠性信道传输，0 表示普通。
5. 保留位。

目前在 Internet 中使用的 TCP/IP 协议大多数情 况下网络并未对 TOS 进行处理，但在实际编程时，有专门的函数来设置该字段的各域。一些重要的网际应用协议中都设置了建议使用的 TOS 值：



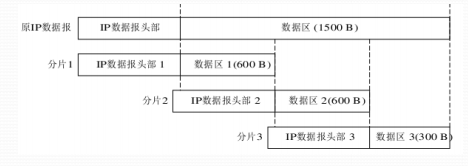
最大传输单元：

IP 数据报在互联网上传输时，可能要经过多个物理网络才能从源端传输到目的端。不同的网络由于链路层和介质的物理特性不同，因此在进行数据传输时，对数据帧的最大长度都有一个限制，这个限制值即最大传输单元 MTU（Maximum Transmission Unit）。同一个网络上的两台主机之间通信时，该网络的 MTU 值是确定的，不存在分片问题。分片问题一般只存在于具有不同 MTU 值的互联网中。由于现在互联网主要使用路由器进行网络连接，因此分片工作通常由路由器负责。当两台主机之间的通信要通过多个具有不同 MTU 值的网络时，MTU 的瓶颈是通信路径上最小的 MTU 值，它被称为路径 MTU。由于路由选择不一定是对称的（从 A 到 B 的路由可能与从 B 到 A 的路由不同），因此，路径 MTU 在两个方向上不一定是一致的，下表是几种常用网络的 MTU 值：



分片：

把一个数据报为了适合网络传输而分成多个数据报的过程称为分片，被分片后的各个 IP 数据报可能经过不同的路径到达目标主机。IP 数据报在传输过程中可能被分片，也可能不被分片。如果被分片，分片后的 IP 数据报和原来没有分片的 IP 数据报结构是相同的，即也是由 IP 头部和 IP 数据区两个部分组成：分片后的 IP 数据报，数据区是原 IP 数据报数据区的一个连续部分，头部是原 IP 数据报头部的复制，但与原来未分片的 IP 数据报头部有两点主要不同：标志和片偏移： 片偏移：IP 数据报被分片后，各片数据区在原来 IP 数据区中的位置用 13 位片偏移来表示。上图中分片 1 的偏移为 0；分片 2 的偏移为 600；分片 3 的偏移为 1200 实际在 IP 地址中，由于偏移是以 8 个字节为单位进行计算的，因而在 IP 数据报中分片 1 的偏移是 0；分片 2 的偏移是 75；分片 3 的偏移是 150



重组：

当分了片的 IP 数据报到达最终目标主机时，目标主机对各分片进行组装，恢复成源主机发送时的 IP 数据报，这个过程叫做 IP 数据报的重组。在 IP 数据报头部中，标识用 16 位二进制数表示，它唯一地标识主机发送的每一份数据报。在一个数据报被分片时，每个分片仅把数据报“标识”字段的值原样复制一份，所以一个数据报的所有分片具有相同的标识。目标端主机重组数据报的原理是：

1. 根据“标识”字段可以确定收到的分片属于原来哪个 IP 数据报；
2. 根据“标志”字段的“片未完 MF”子字段可以确定分片是不是最后一个分片；
3. 根据“偏移量”字段可以确定分片在原数据报中的位置。

IP 数据报选项：

IP 数据报“选项”主要有两大功能：

1. 用来实现对数据报传输过程中的控制，如规定数据报要经过的路由；
2. 进行网络测试，如一个数据报传输过程中经过了哪些路由器。IP“选项“域共分为四大类，每类分为若干个选项，每个选项有确定的编号：



IP 数据报“选项”由三个部分组成：选项码、选项长度和选项数据。选项码和选项长度各占一个字节，中，选项长度用于确定整个选

项部分的长度；选项码又分为复制、选项类和选项号：复制：占一位，用来控制一个带有选项的 IP 数据报被分片后对选项的处理方式。该位置 1 时将选项复制到所有分片中；置 0 时将选项仅复制到第一个分片中。选项类和选项号用于确定该选项是哪类选项中的哪个选项，其实就是确定该选项的功能。

1. 源路由选择：是指 IP 数据报在互联网中传输时，所经过的路由是由发出 IP 数据报的源主机指定的，以区别于数据报在互联网中传输时由路由器的 IP 层自动寻径所得到的路由。通过设置源路由选择选项，可以测试网络中指定路由的连通性，以使数据报绕开出错的网络，也可用于测试特定网络的吞吐量。源路由选择可分为两类：严格源路由选择和宽松源路由选择。
2. 严格源路由选择有发送端规定 IP 数据报必须经过的路径上的每一个路由器，相邻路由器之间不得有中间路由器，并且所经过的路由器的顺序不可更改。如果一个路由器发送源路由所指定的下一个路由器不在其直接连接的网络上，那么它就返回一个“源路由失败”的 ICMP 差错报文。严格源路由选择选项格式如下：

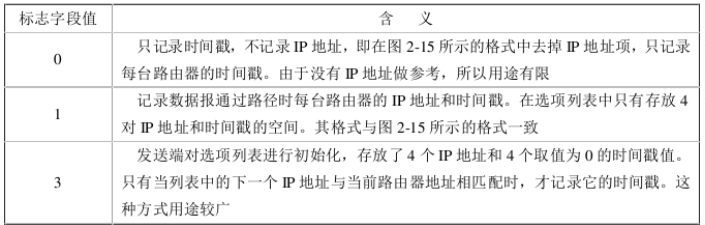


1. —宽松源路由选择：由发送方指明一个数据报经过的 IP 地址清单，但是在数据报传输的路径上，在选项中指定的两个 IP 地址之间可以有其他 IP 地址的路由器。格式与严格的相同，只是选项码字段值为 0x83。
2. 记录路由：通过设置记录路由选项，IP 数据报就可以记录数据报从源主机传输到目标主机时，所经过路径上的各个路由器的 IP 地址。记录路由选项的数据格式和严格源路由选择格式相同，但选项码字段值为 0x87，指针初值为 4，指向存放第一个 IP 地址的位置。每个路由器的 IP 地址存入选项的数据区中，指针字段的值也随着增加（从 4 开始到 8，12，16，最大到 36），它始终指向下一个存放 IP 地址的位置。当记录了 9 个 IP 地址后，指针字段的值为 40，表示数据区已满。
3. 记录时间戳：就是 IP 数据报每经过一个路由器都记下它的 IP 地址和时间。时间戳中的时间以 ms 为单位，时间戳取值一般为格林威治时间（UT，Universal Time）自午夜开始计时的毫秒数时间戳选项格式如下：



时间戳选项的选项码是 0x44。选项长度表示选项的总长度（一般为 36 或 40），指针指向下一个可用空间的指针（值为 5、9、13 等）。3）记录时间戳“溢出 OF”字段表示因时间戳选项数据区空间不够而未能记录下来的时间戳个数；“标志 FL”字段用于控制时间戳选项的格式。

取值如下：



**【实验内容】**

1. 一个终端，启用 Tcpdump 工具软件﹐并设置相应过滤条件，从指定网卡捕获 IP 数据包，并进行分析。
2. 另一个终端触发产生 IP 数据包。输入 ping 命令，向 Windows 节点发出 ICMP 消息，该消息封装在 IP 数据包中进行传输。

**【实验设备】**

实验环境主要由一台计算机组成，使用 ubuntu 系统。

**【实验步骤】**

启动捕获 IP 数据包监听。创建终端 1，进人捕获 IP 数据包监听状态。

输入捕获 IP 数据包监听命令： sudo tcpdump - ex - i enp0s3 ip 口令：123456789，处于监听状态。

触发产生 IP 数据包。创建终端 2，向 Windows 节点发出 ICMP 消息。

输入“ping 192.168.1.254”。

分析捕获 IP 数据包。终端 1，捕获了一个 IP 数据包。

IP 数据包头部分成五行，每行对应两组数字，共计 20 个字节，按照 IP 数据包格式对 IP 数据包进行分析。

**【实验现象】**

1 个数字代表半个字节，每组 8 个数字刚好对应 IP 数据包格式中一行，特意用矩形框分隔，下面按照格式中行顺序来分析数据含义。

第一行，version=0x4，标识 IP 版本号，表示第四版 IP；h.len=0x5，表示 IP 头部长度为 5 行，每行长 32 位，总计 20 字节； Service Type=0x00，空缺；Total Length=0x54，表示 IP 数据包总长度，当前为 84 个字节。

第二行，分段数据，不讨论。

第三行，TTL=0x80，表示生存时间，折合成十进制为 128；type=0x01，表示封装的上层协议，1 表示 ICMP 协议；Header checksum=0x4e99，表示 IP 数据包头部的校验和补码。

第四行，源地址=0xc0a8 01fe，表示源节点 IP 地址，折合成十进制是 192.168.1.254。

第五行，目标地址=OxcOa8 0113，表示目标节点 IP 地址，折合成十进制是 192.168.1.19。

**【分析讨论】**

通过这次实验，我不仅学会了使用工具进行抓包，还深入了解了 IP（Internet Protocol）数据包的格式，使我能够对获取到的包进行深入分析，尤其是对 IP 数据包头部的格式有了更为深刻的理解。

在实验过程中，我观察到在数据包的发送过程中，起始和目的地的 IP 地址始终保持不变，分别是起始 PC 与目标服务器。然而，MAC 地址却以路由器为中转。在发送到路由器之前，目的地的 MAC 地址是路由器端口的 MAC 地址，到达后，起始 MAC 地址又变成了路由器的端口 MAC 地址，而目的地则变成了目标 PC 的 MAC 地址。这表明了路由器的重要功能，包括了在以太网中负责 MAC 地址的中转。这同时也说明了数据包在到达路由器之前并不清楚自己会以怎样的方式传播，展示了路由器连接不同子网的关键功能。相比之下，交换机在中转数据包时并不影响其内容，只是起到中转的作用，因此在报告中没有详细列出它们的功能。

到达路由器后，除了 MAC 地址外，TTL（Time To Live）也减少了 1，表明经过了一个子网的中转。这是因为每经过一个路由器，TTL 都会减少，以防止数据包在网络中无限循环。

对于经过路由器中转后的数据包，我发现虽然其内容有些许变化，但本质上仍然是同一个包。然而，到达服务器后发出的回应则本质上是另一个包。观察到回应数据包中，长度、检验和、生存周期等全部被重置，同时 MAC 地址和 IP 地址也发生了颠倒。这展示了在网络通信中，每个路由器都会对数据包进行处理，而回应数据包的本质是产生了一个全新的包，而不是简单地对原始数据包进行修改。

我深入理解了网络中路由器的重要作用以及它与交换机的区别，对数据包在网络中的传输过程和经过不同设备时的变化有了更为清晰的认识。这对于理解网络通信的机制以及进行网络故障排除将有着实质性的帮助。