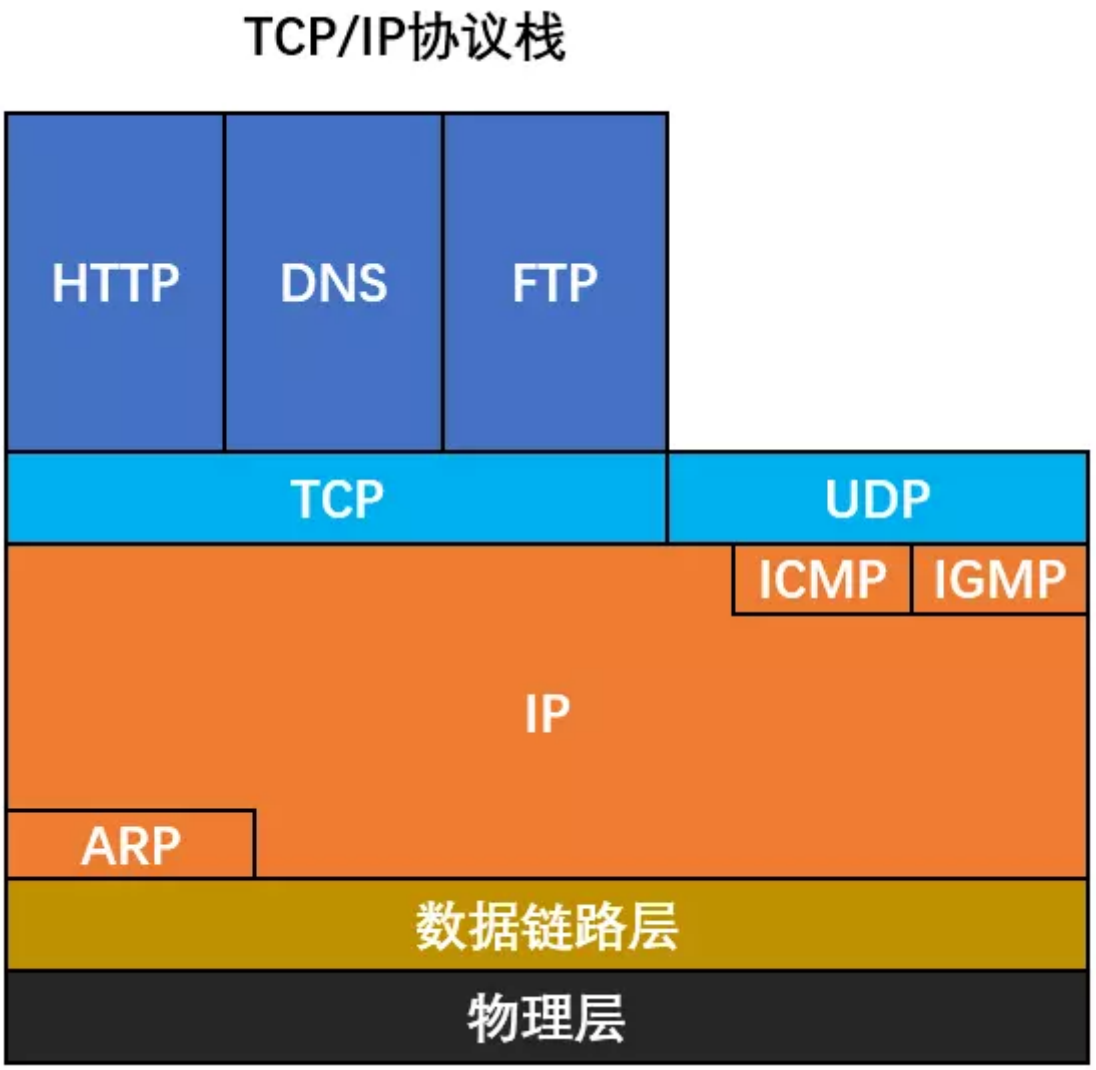
IP数据报格式

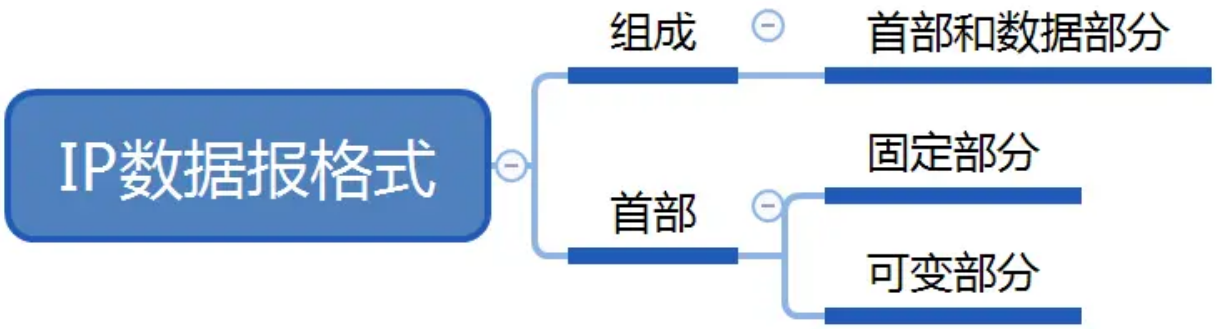
前言

先回顾一下TCP/IP协议栈

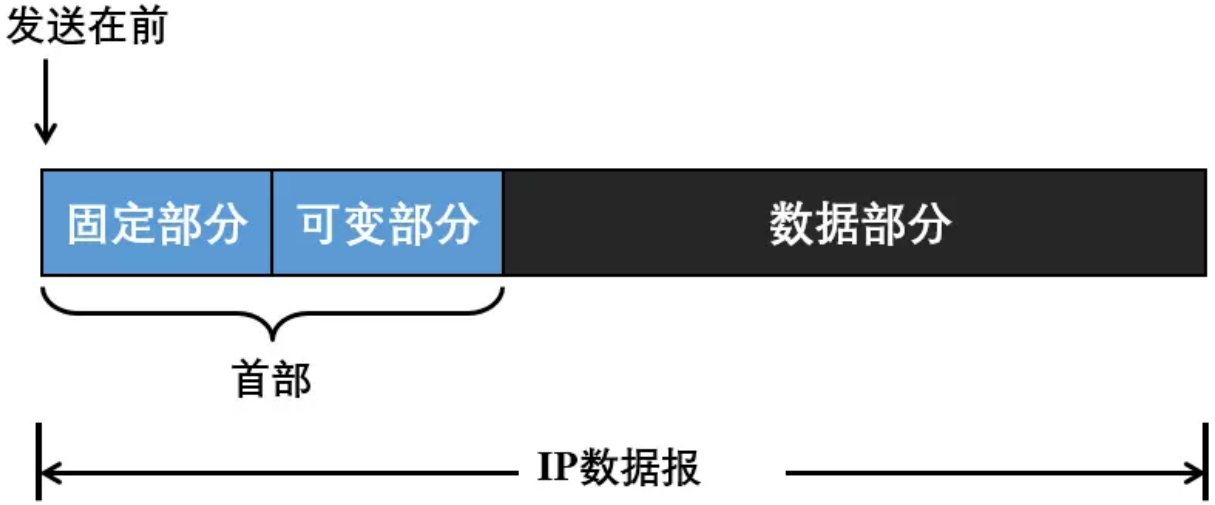


网络层的协议有IP协议、ARP协议、ICMP协议和IGMP协议。其中IP协议是最主要也是最重要的协议，所以本文先从IP数据报的格式开始介绍。

内容总览



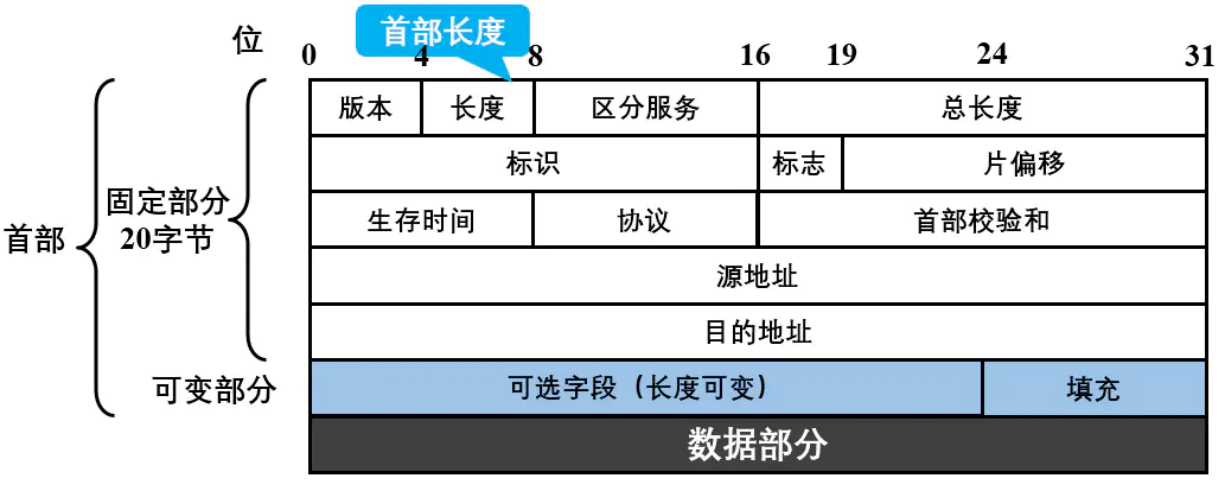
1.IP数据报格式



一个IP数据报由**首部和数据**两个部分组成。

其中首部的前一个部分是**固定部分**，长度固定共**20字节**，这是所有IP数据报必须具有的。后一部分是**可变部分**，其长度是可变的，不是必须的。

2.IP数据报首部格式



2.1.固定部分

(1) **版本**：占4位，指**IP协议的版本。**目前广泛使用的IP协议版本有两种IPv4和IPv6。

(2) **首部长度**：**占4位**，其单位是**4B。**所以首部长度**必须是4B的整数倍。**如首部长度字段的4个二进制位分别是1111（对应十进制是15），则IP协议首部的长度是15 × 4B = 60B（字节）。由于IP数据报首部的固定部分长度固定是20，所以首部字段最小从0101开始。

(3) **区分服务**：**占8位**，一般情况下不使用该字段。只有使用区分服务时，这个字段才起作用，如要求当前的数据报设置高优先级优先发送。

(4) **总长度**：**占16位**，表示首部和数据部分长度之和，**单位是1字节。**

(5) **标识、标志、片偏移是关于IP数据报分片的**，见下文。

(6) **生存时间**：**占8位**，表示数据报在网络中的寿命。由发送数据报的源点设置这个字段，其目的是为了防止那些无法交付的数据报无限制的在互联网中兜圈子（例如从路由器R1转发到R2，再转发到R3，然后又转发到R1），因而白白浪费网络资源。数据报每经过一个路由器，这个值就会减1，当减至0时，就丢弃该数据报。

(7) **协议**：占8位，协议字段是指出次数据报所携带的数据是使用的协议。这里记两个协议字段的值：**6表示TCP协议，17表示UDP协议。**

(8) **首部校验和**：占16位，**只校验数据报的首部，不检验数据部分。**数据报每经过一个路由器都要重新计算一下首部校验和（一些字段，如生存时间、标志、片偏移可能发生了变化）。

(9) **源地址和目的地址：各占32位。**

2.2.可变部分

(1) **可选字段**：长度可变，从1字节~40字节。可变部分是为了**增加IP数据报的功能**，如用来支持排错、测量以及安全等措施。

(2) **填充**：IP数据报的首部长度必须是4B的整数倍，所以如果首部长度不满足4B整数倍时，就使用填充字段将首部填充到4B的整数倍。

3.IP数据报分片

数据链路层将网络层传送的数据报添加头部和尾部封装成以太网帧，数据链路层封装数据帧长度是有限制的，以太网规定其最大传送单元MTU的值是1500字节，如果从网络层传输下来的数据报长度超过MUT值，就必须把过长的数据报进行分片处理。

而上节IP数据报首部固定部分的标识、标志和片偏移就是用于数据报分片的。

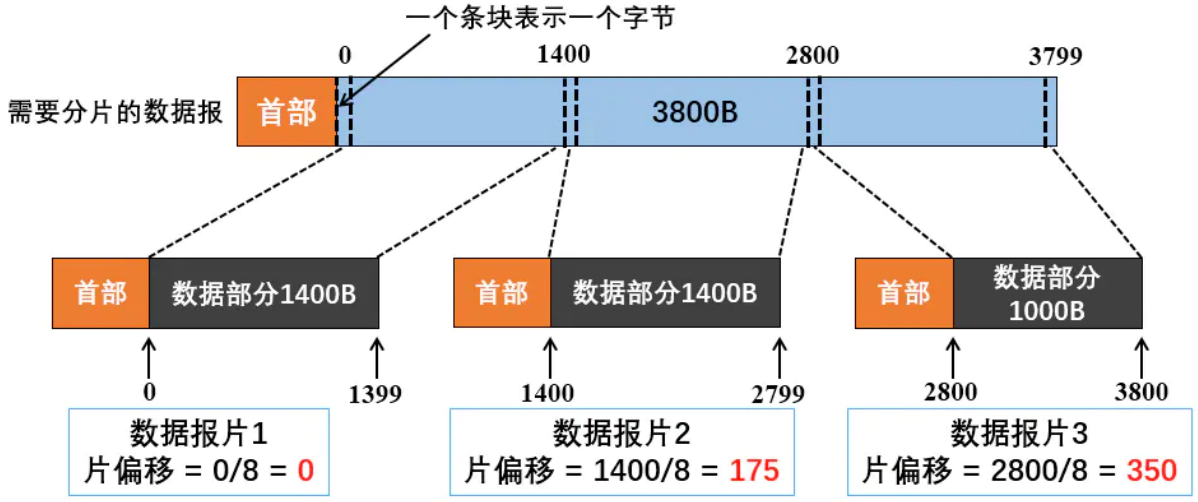
(1) **标识**：**占16位，所有分片的数据报的标识必须要和原数据报的标识相同。**假如一个数据报的标识是12345，这个数据报过大，分片后将它分为3个小的数据报，这3个较小的数据报的标识也必须是12345，可以理解这3个数据报是一个家族的。**相同的标识字段的值可以使分片后的各个数据报最后能正确的重装成原来的数据报。**

(2) **标志：占3位，目前只有两位有意义。**

> 1. **最低位即第3位记为MF**（More Fragment），意思是是否还有更多分片。当值为1时，表示该分片不是最后一片，后面还有分片，当值为0时，表示这是原数据报分片后的最后一片数据报，后面已经没有更多的分片了。
> 2. **中间位即第2位记为DF**（Don't Fragment），意思是原数据报能否分片。当值为1时，表示该数据报不允许分片，当值为0时，表示该数据报允许分片。

(3) **片偏移**：占13位，以8B为单位。其表示较长分组分片后，某一片在原分组中的相对位置，也就是说相对于**用户数据字段的起点**，该片从何处开始。这也就是说，**除了最后一个分片，每个分片的长度一定是8B的整数倍。**

> **举个栗子：**
> 假设一个数据报的总长度是3820个字节，其数据部分为3800字节长（首部仅仅使用固定部分），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长度不超过1400字节。于是分为3个报片，其数据部分的长度分别为1400、1400、1000字节。原始数据报首部被复制为各个数据报的首部，但是必须修改有关字段。



对于原始数据报、数据报片1、2、3的首部部分信息如下图，（原始数据报的标识取12345）

	总长度	标识	MF	DF	片偏移
原始数据报	**3820**	**12345**	**0**	**0**	**0**
数据报片1	1420	12345	1	0	0
数据报片2	1420	12345	1	0	175
数据报片3	1020	12345	0	0	350

注意区分几个字段的单位：

> (1) 首部长度：单位是4B，表示数据报的首部的长度。
> (2) 总长度：单位是B，标识整个数据报的长度。
> (3) 片偏移量：单位是8B，表示某一分片相对于用户数据字段的起点。

4.总结


IP数据报
组成
首部
固定部分（20B）、可选部分。
数据部分
首部
版本：IP协议版本，IPv4/IPv6。
首部长度：数据报首部长度，单位是4B。
区分服务：一般情况下不用。
总长度：数据报总长度，首部+数据部分。
标识：分片的标识要和原数据报的标识一致。
标志：MF（是否还有分片），DF（能否分片）。
片偏移：分片相对于用户数据字段的起点，单位是8B。
生存时间：数据报寿命，每经一个路由器生存时间减1。
协议：数据部分使用的协议类型，6->TCP，17->UDP。
首部检验和：只校验数据报首部。
源地址&目的地址
可变部分
可选字段：用于增加IP数据报功能，1~40字节。
填充：使数据报首部长度是4B的整数倍。