

网络-网络层

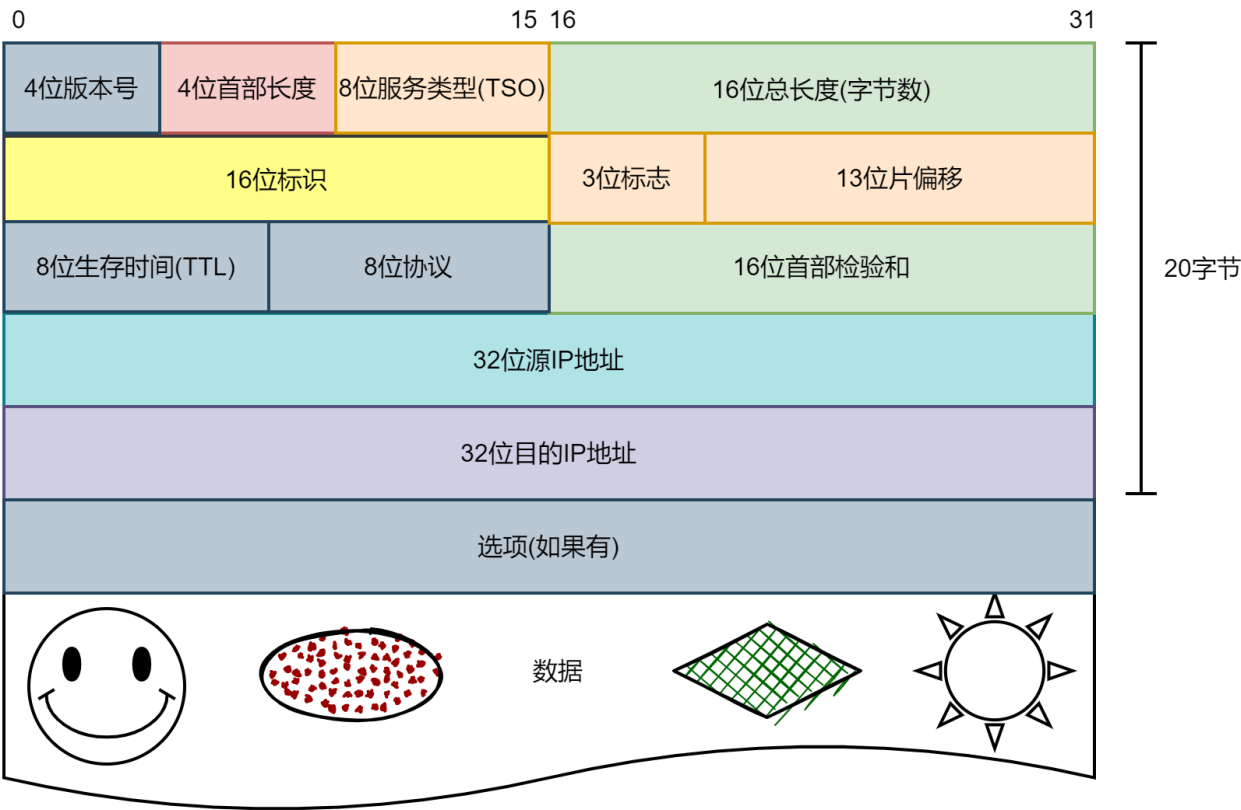
0 前言

- 1. 应用层http协议是进行构建和解析数据的，主要是请求request和响应response。
- 2. 传输层TCP/UDP协议不提供数据的运输。**传输层的作用主要是来进行做决策**，商量数据传输的这路数据怎么走？怎么保证数据不会丢失？怎样保证数据传输的效率更高？
- 3. 实际有数据传输能力的是网络层IP协议，**网络层的作用主要是来进行做执行**，提供了将数据从主机A跨网络送到主机B的能力。

1 基础

- 1. IP由两部组成：**网络号+主机号**
 - 网络号：保证相互连接的两个网段具有不同的标识
 - 主机号：同一网段内，主机之间具有相同的网络号。但是必须有不同的主机号
 - 子网(网络层概念)：就是将相同的网络号主机放在一起组成的网络
 - 局域网(数据链路层概念)
 - 网段(物理层概念)
- 2. IP协议提供了数据从主机A传输到主机B的能力，但是不能够保证数据正常的达到对端，也就是说**IP协议不能够保证可靠性**

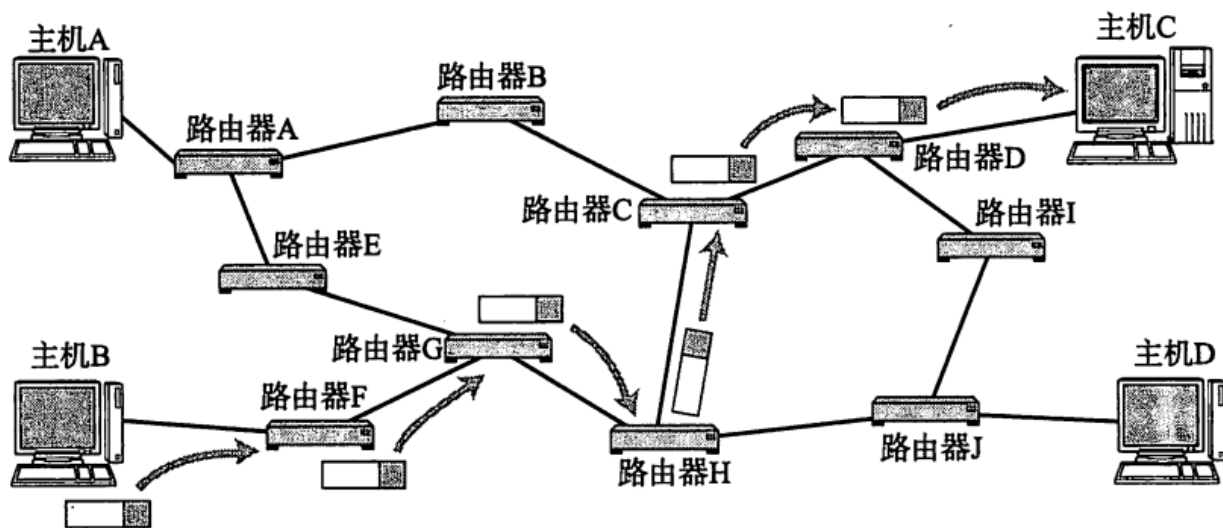
2 IP报文

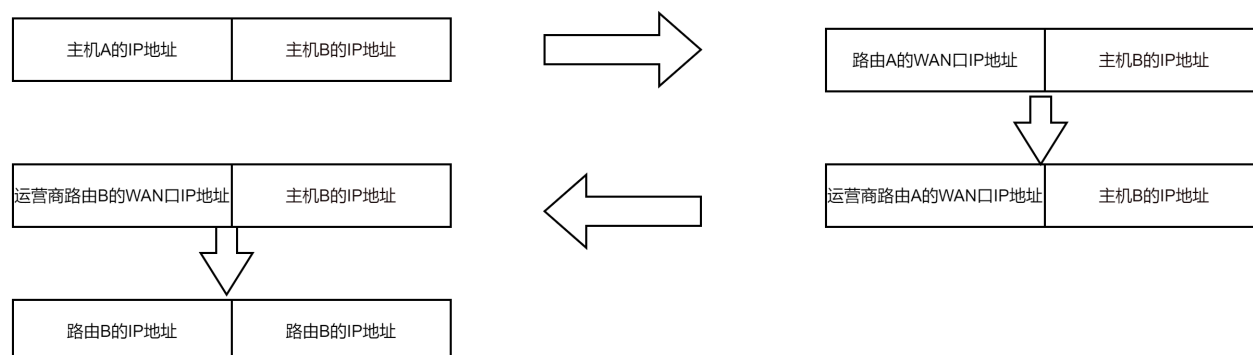
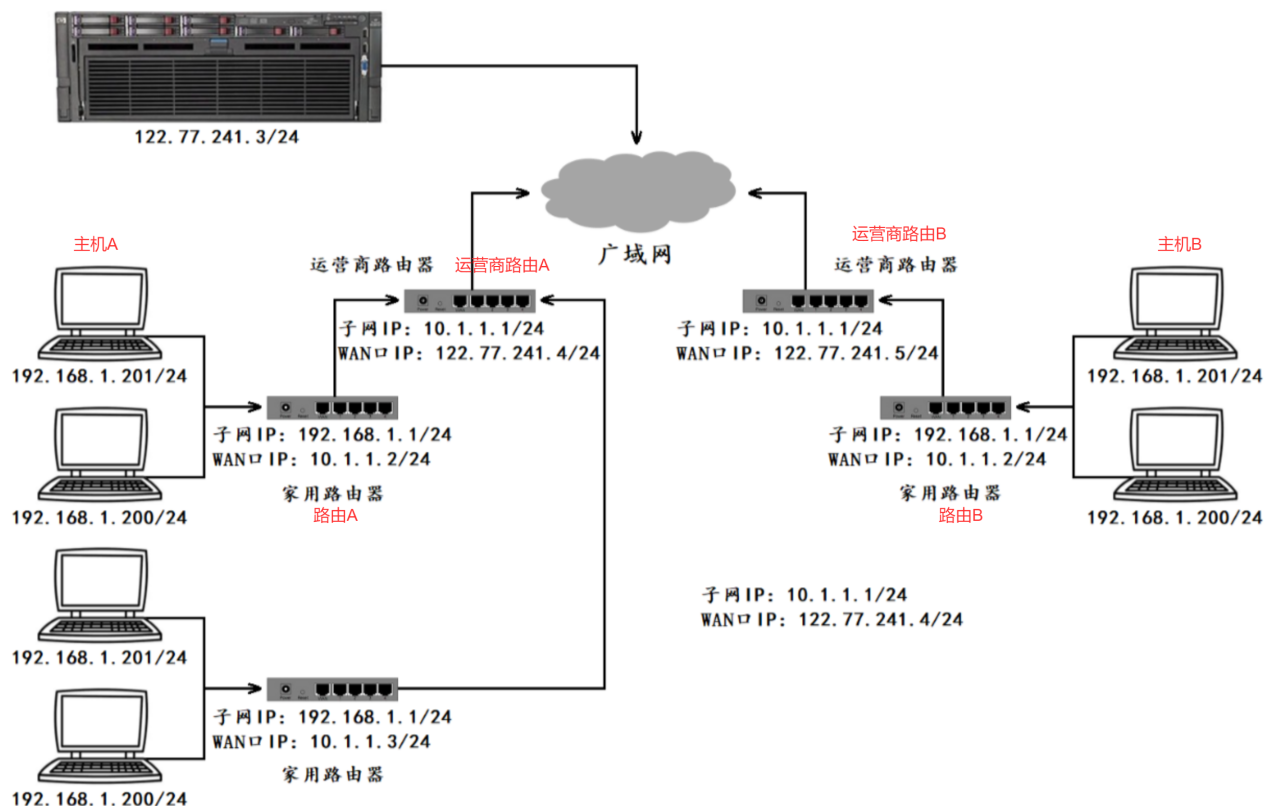


由于数据链路层传输数据有一定的大小要求，MTU=1500字节，因此对于网络层传输下来的数据，如果有效载荷加上报头20字节小于1500字节，那么数据链路层对于该数据包就不会进行分片操作，但是加上报头的20字节大于1500字节的话，那么数据链路层就会对该数据包进行分片处理，将原先的数据包分成几个满足MTU要求的数据包

1. 4位版本号：IPv4与IPv6两个，但是由于IPv6有他自己独特的报文，因此这四位版本号一般指的就是IPv4，这个地方填的就是4
2. 4位首部长度：这里和TCP报文那里的含义是一样的，0000-1111(0-15),单位是4字节，因此这里的取值范围也就是0-60字节，但是IP报文的长度一般都是20字节，因此这里的4位首部长度填的都是0101
3. 8位服务类型(TSO):3位优先级字段(已经弃用)，4位TOS字段和1位保留字段(必须置为0)，其中4位TOS分别表示最大延时，最大吞吐量，最高可靠性，最小成本，这4者是相互冲突的，只能够选择一个，对于ssh/telnet这样的应用程序，最小延时最重要，对于ftp这样的程序，最大的吞吐量最重要。
4. 16位总长度：代表的是该报文实际的有效载荷大小，是以字节为单位
5. 16位标识：如果数据包被分成了n个数据包，那么这n个数据包的16位标识是一样的，不然每个不同的报文16位标识是不一样的
6. 3位标志：这里面存在3个比特位，有一位暂时不用，第二位标识是否允许进行分片(TCP决定)，如果是1则表明该数据包是禁止进行分片，那怕这个数据包的有效载荷是超过1480字节时，这时该数据包由于是禁止分片的，因此该数据包会被丢弃，第三位则是用来表示该数据包后面存在已经分片的数据包，1就代表后面还有分片的数据包，0就表示没有分片的数据包
7. 13位片偏移：这个和分片的数据包有关，如果一个数据包被分成了2片，那么第一片数据包的13位片偏移就是0，第二片数据包的13位片偏移就是1480
8. 8位生存时间TTL：数据报到达目的地的最大报文数，一般是64，，每次经历一个路由，TTL-=1，一直减到0都还没有到达，那么就丢弃，这个字段主要是用来防止出现路由循环
9. 8位协议：这个由上面的传输层进行填写，上面如果是TCP协议这里就填TCP协议，如果是UDP协议的话，就需要填写UDP协议
10. 16位首部校验和：检验该报文在传输的过程当中是否又被修改，如果有修改就会报错
11. 32位源IP地址：也就是该数据包不忘初心的起始点
12. 32位目的IP地址：也就是该数据包经历千难万险需要奔赴的终点
 - 由于网络各层之间的解耦，因此如果数据包进行分片处理时，网络将数据分成几个然后对端的网络层又如何进行组装分片的数据包，传输层是不关心的，他只关心数据我给你了，你给我时是一个完整的数据报就行
 - IP数据包分片不是经常进行的，因为数据分片会增加数据传输过程当中数据丢失的风险，因此一般会减少分片，这就需要TCP控制数据段的大小了
 - 接收端如何知道自己接收的数据包是否被分片了？
 - a. 先看报文里面的13位片偏移是否为0，如果不为0，那就表明该数据包一定是分片的数据包
 - b. 如果13位片偏移为0，那么就需要看3位标志，如果第三位标志不为0时，那就表明该数据包一定也是被分片了
 - 一个路由器会配备两个IP地址，分别是WAN的地址和LAN的地址
 - WAN:WAN的接口也称作广域网接口，用来连接外部的网络也就是连接运营商的设备

- LAN:用来连接内网(局域网)的设备, 连接电脑, 交换机, 打印机等设备(一般一个路由器有多个LAN接口)
- 以太网是一种总线型局域网, 但是局域网的类型不一定是总线型, 还有可能是星型, 环形
- 将IP地址与子网掩码进行“按位与”操作, 得到的结果就是网络号
- 将IP地址当中的主机地址全部设置成0也就是成了网络号, 代表这个局域网
- 将IP地址当中的主机地址全部设置1, 就成了广播地址, 用于给同一链路中相互连接的所有主机发送数据包
- 127.*通常代表本机环回地址测试, 一般是127.0.0.1, 就只会从本机的应用层到传输层到网络层然后再到传输层到应用层, 目的主要是测试本机网络的连通情况
- 不同的路由器其子网的IP地址(LAN地址)其实都是一样的, 一般都是192.168.1.1, 但是子网内的主机地址中主机号是不同的





1. 当主机A发送数据到主机B，由于内网的IP不能进入到公网里面，因此在子网里面，主机A发送数据经过跳一跳到达该子网的路由器当中，到达该路由器之后，由于路由器两个IP地址，因此它会将该数据帧的源地址改成该路由器的WAN口的地址，然后进入到下一个局域网里面，经过相同的过程将数据最终达到主机B当中
2. 私网的IP是不能够进入到公网当中的，因为不同的私网里面可能会有相同的IP地址，如果私网中的IP进入到公网，就会分不清这个私网是来自那个具体的主机
3. 不同的局域网是需要经过运营商那层局域网才能够进行通信的。

```
[Jolly.Roger@VM-16-9-centos ~]$ route
```

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	gateway	0.0.0.0	UG	0	0	0	eth0
10.0.16.0	0.0.0.0	255.255.252.0	U	0	0	0	eth0
link-local	0.0.0.0	255.255.0.0	U	1002	0	0	eth0

- Destination代表的是目的网络地址。
- Gateway代表的是下一跳地址。
- Genmask代表的是子网掩码。
- Flags中，U标志表示此条目有效（可以禁用某些条目）G标志表示此条目的下一跳地址是某个路由器的地址，没有G标志的条目表示目的网络地址是与本机接口直接相连的网络，不必经路由器转发。

- Iface代表的是发送接口。

1. 当IP数据包到达路由器时，路由器就会用该数据的目的IP地址，依次与路由表中的子网掩码 Genmask进行“按位与”操作，然后将结果与子网掩码对应的目的网络地址Destination进行比对，如果匹配则说明该数据包下一跳就应该跳去这个子网，此时就会将该数据包通过对应的发送接口Iface发出。
2. 如果将该数据包的目的IP地址与子网掩码进行“按位与”后，没有找到匹配的目的网络地址，此时路由器就会将这个数据包发送到默认路由，也就是路由表中目标网络地址中的default。可以看到默认路由对应的Flags是UG，实际就是将该数据转给了另一台路由器，让该数据在另一台路由器继续进行路由。
3. 数据包不断经过路由器路由后，最终就能到达目标主机所在的目标网络，此时就不再根据该数据包目的IP地址当中的网络号进行路由了，而是根据目的IP地址当中的主机号进行路由，最终根据该数据包对应的主机号就能将数据发送给目标主机了。

IP地址不够用的三种缓解方案

1. 动态分配IP地址：只给接入网络的设备分配IP地址，因此同一个MAC地址设备，在不同的时间接入互联网，所分配的地址是不一样的
2. 使用NAT技术
3. 采用IPv6技术，IPv6在根本上增加了地址的个数，但是由于v4与v6是不兼容的两种IP地址方案，短时间内是无法大面积使用v6技术的