TCP协议的十一种状态集转换、子网划分过程

作者：Georgekai
归档：学习笔记
2018/1/17

网络运维基础（三）

1.1 TCP协议的十一种状态集转换

1.1.1 TCP三次握手状态集的转换

1.服务端：

1）服务端从closed状态转换为listen状态（在服务端开启相应服务），只有在listen才可以 接受客户端建立连接的请求

2）从colsed转变为listen，实际上就是创建了一个socket信息

netstat -an|grep -i es 可以看到socket条目信息

socker条目：tcp或udp协议——目标地址，端口——源地址，端口——状态

2.客户端：

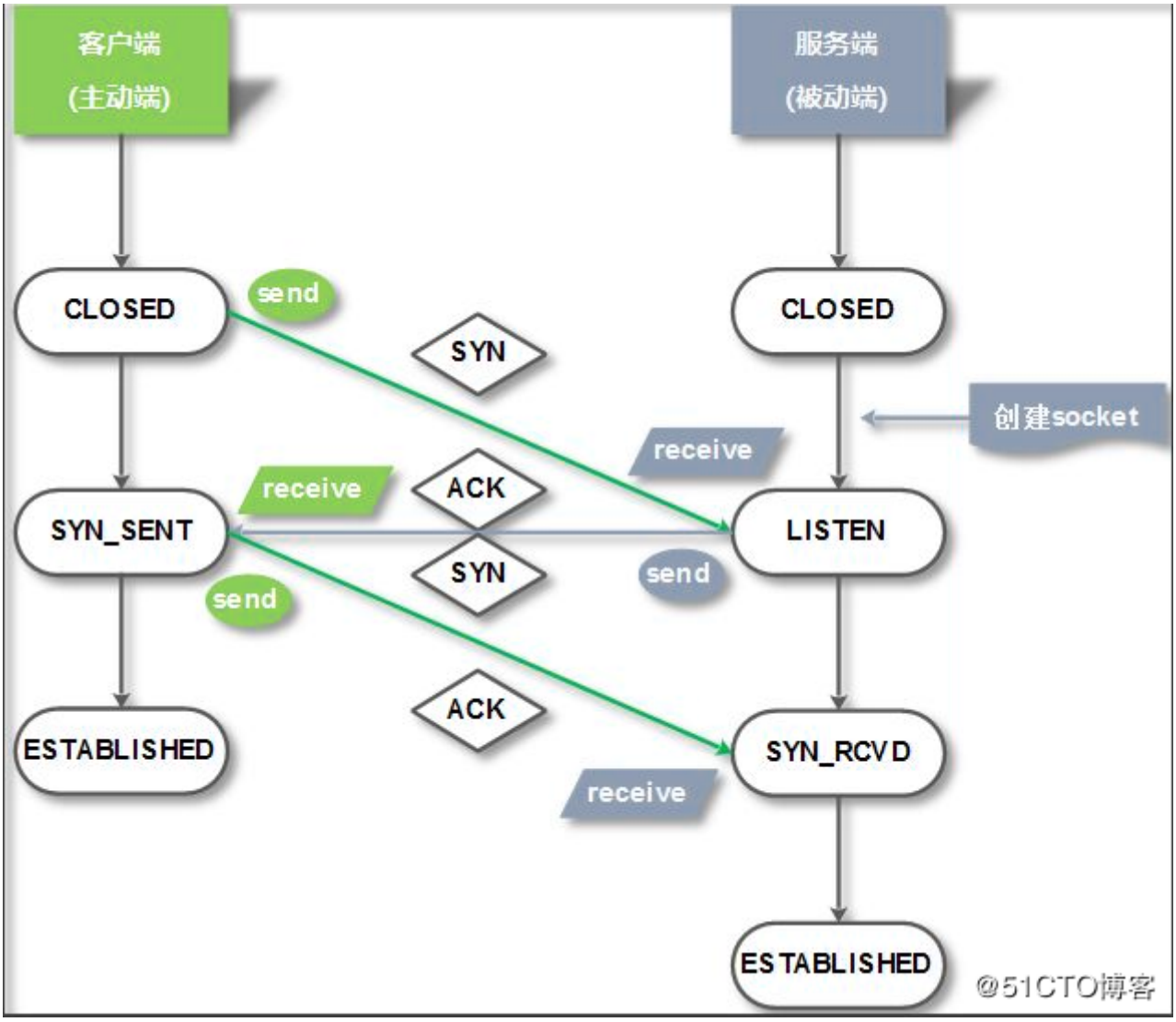
1）客户端发送syn信息给服务端，然后客户端从closed状态变为syn_send状态（三次握手 的第一次握手）

3.服务端：

1）服务端在listen状态接收到客户端发送的syn请求，会响应syn和ack信息，并且从listen 状态装换为syn_rcvd状态（三次握手的第二次握手）

4.客户端：

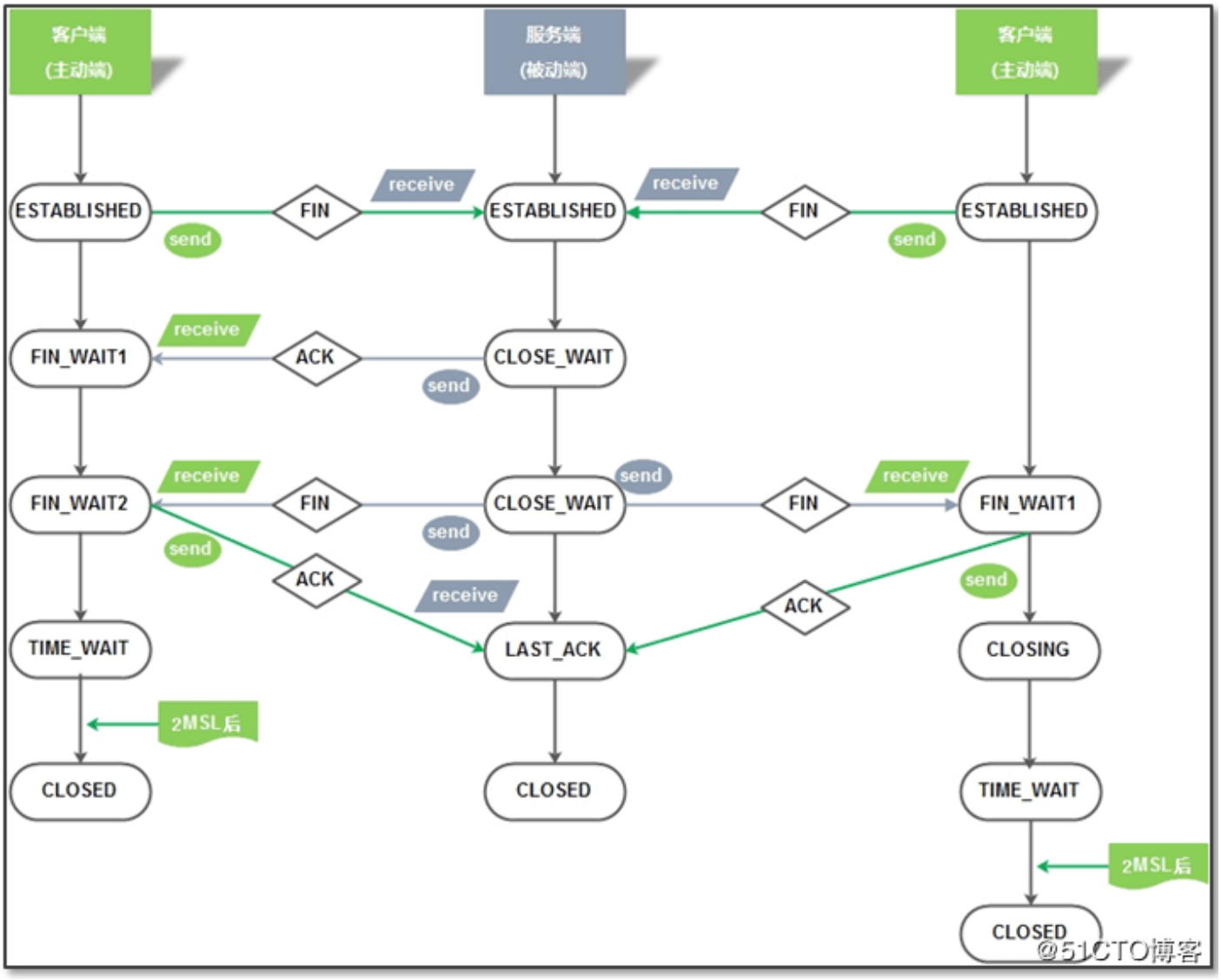
1）客户端在syn_send状态接收到服务端的syn和ack字段信息，然后回复ack确认信息（三 次握手的第三次），发送完后，从syn_send转换为established



注：在/etc/sysctl.conf中设置net.ipv4.tcp_syncookies=1来防止SYN Flood攻击

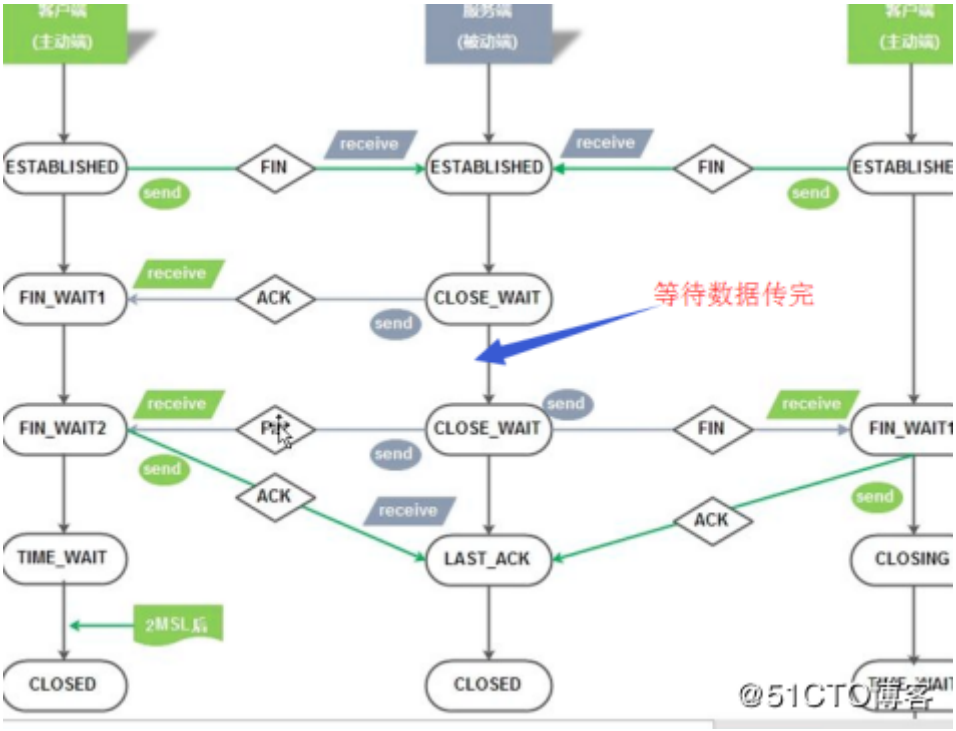
1.1.2 TCP的四次挥手状态集的转化

1. 客户端：
1）客户端在established状态发送fin字段信息给服务端（四次挥手的第一次挥手）
客户端状态转变为fin_wait1（第一次等待：服务端的确认ack信息）状态
2. 服务端：
1）服务端在established接收到客户端发送的fin字段信息，从established状态转换成close_wait状态
2）服务端在close_wait状态发送ack确认字段（四次挥手的第二次挥手）
3. 客户端：
1）客户端在fin_wait1状态接收到服务端的ack信息，进入到fin_wait2等待状态（第二次等待：等待服务端的fin信息）
4. 服务端：
1）服务端在close_wait状态发送fin断开连接字段给客户端（四次挥手的第三次挥手）
2）服务端从close_wait状态变为last_ack状态
5. 客户端：
1）客户端在fin_wait2状态接受服务端的fin信息，然后响应ack信息给服务端，并将自己的fin_wait2状态time_wait状态
6. 服务端：
1）服务端在last_ack状态接受到客户端发送的ack字段信息后，就会进入最终的closed状态
7. 客户端：
1）在time_wait状态会等待120秒钟的时间，才会进入到closed状态



注：传输层发送fin（请求断开连接），是接收到了会话层的断开连接请求（这样一层层的转发）

那么问题来了：1. 为什么会有四次挥手过程，ack 和fin要分开发送?
答：服务端接受到了客服端的FIN时会向应用层汇报，并回应ACK给客户端，
然后会等数据传输完毕后，在发送FIN请求断开连接。



2. 客户端为什么要有time_wait状态
答：为了确保服务端能收到ack，客户端会在time_wait不断给服务端发送ack。

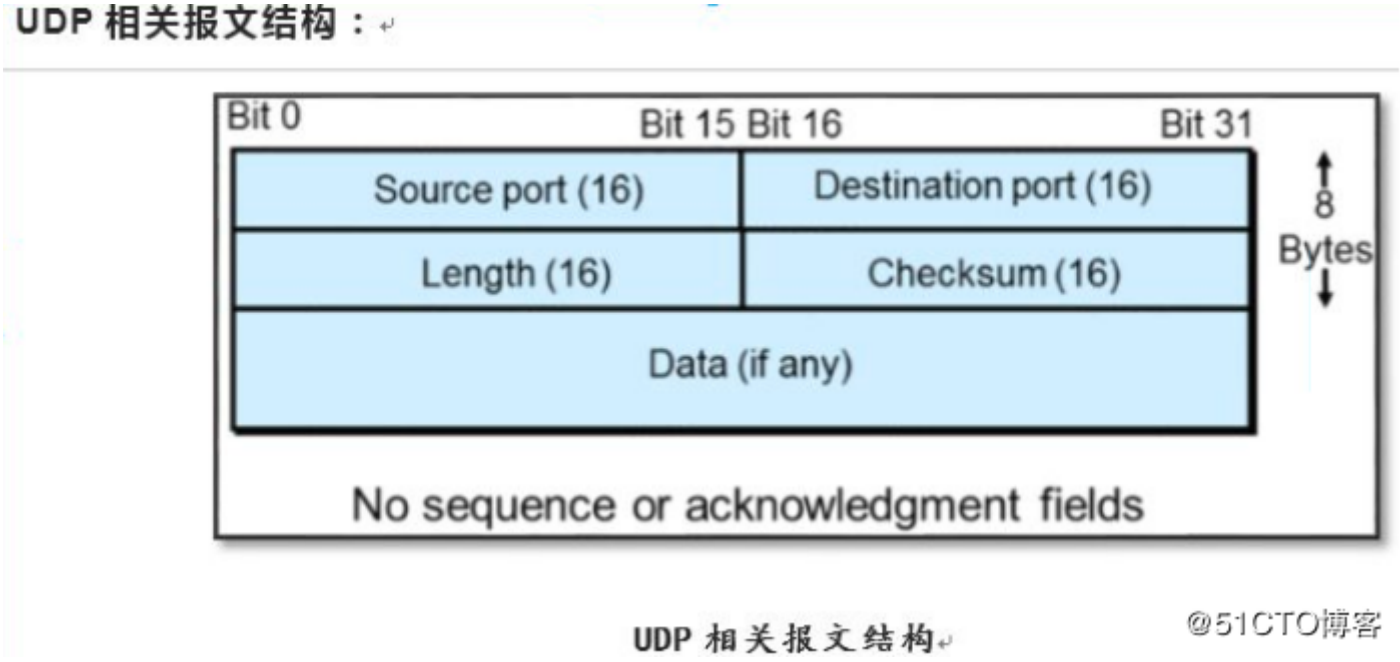
3. 总结closing状态的由来：
答：在第二次挥手的时候，客户端没收到服务端发送的ack，但收到了fin字段信息，按理说收到fin后应该转换为time_wait，所以加了colsing起一个缓存时间（过程很快）

TCP的十一种状态总结：

TCP 的十一种状态转移总结：

状态出现方式	状态出现环境	状态名称	状态描述
TCP 建立过程 涉及 5 种状态	服务端/客户端	CLOSED	默认初始化状态
	服务端	LISTEN	建立 socket，进入监听状态
	客户端	SYN_SENT	发送 syn 报文，进入 syn 发送状态
	服务端	SYN_RCVD	接收 syn 报文，并回复 ack 及 syn 报文
	客户端/服务端	ESTABLISHED	接收 syn 报文，回复 ack，建立连接(客户端) 接收 ack 报文，建立连接(服务端)
TCP 断开过程 涉及 6 种状态	服务端/客户端	ESTABLISHED	默认断开前初始化状态
	客户端	FIN_WAIT1	发送断开请求 FIN 报文
	服务端	CLOSE_WAIT	收到 FIN 后向客户端发生 ACK
	客户端	FIN_WAIT2	收到服务端返回的 ACK 报文，等待数据传输
	服务端	LAST_ACK	发送 FIN 断开请求报文
	客户端	TIME_WAIT	回复 FIN 断开请求，发送 ack 报文
	服务端/客户端	CLOSED	收到 ack 报文，立即转变为断开状态(服务端) 等待 2MSL 后，进入断开状态（客户端）
	客户端	CLOSEING	没有收到第二次挥手的 ack 信息，但接受到了第三次挥手的 fin 字段，就会由 FIN_WAIT1 变为 CLOSE

1.2 UDP相关报文结构



1.3 IP地址分类与子网划分基础

1.3.1 什么是IP地址（常见的IP的地址为ipv4和ipv6）

1. IPV4：有32位二进制组成，采用点分十进制分为4段，每段为8位二进制
2. IPV4和IPV6的总数：用awk计算了一下，大约这么多

```
[root@georgekai ~]# awk 'BEGIN{print 2^128}'
340282366920938463463374607431768211456
[root@georgekai ~]# awk 'BEGIN{print 2^32}'
4294967296
```
@51CTO博客

注：seq -w 10　让数字补齐

```
[root@georgekai ~]# seq -w 10
01
02
03
04
05
06
07
08
09
10
```
@51CTO博客

1.3.2 IP地址分类

A	1.0.0.0	到	126.0.0.0	（0.0.0.0 和 127.0.0.0 保留）
B	128.0.0.0	到	191.254.0.0	（128.0.0.0 和 191.255.0.0 保留）
C	192.0.1.0	到	223.255.254.0	（192.0.0.0 和 223.255.255.0 保留）
D	224.0.0.0	到	239.255.255.255	用于多点广播
E	240.0.0.0	到	255.255.255.254	保留（255.255.255.255 用于广播）

类别	8Bits	8Bits	8Bits	8Bits	IP取值范围
A类型	0NNNNNNN	Host	Host	Host	1.0.0.0-126.255.255.254
B类型	10NNNNNN	Network	Host	Host	128.0.0.1-191.255.255.254
C类型	110NNNNN	Network	Network	Host	192.0.0.1-223.255.255.254
D类型	1110NNNN	Multicast group	Multicast group	Multicast group	224.0.0.1—239.255.255.254
E类型	Research				

IP 地址类型表 @51CTO博客

1. 按IP的数值范围划分：A B C D E 五类地址
常用地址为ABC三类地址：
A类地址==网络位+主机位+主机位+主机位
B类地址==网络位+网络位+主机位+主机位
C类地址==网络位+网络位+网络位+主机位
D类地址为组播地址：每一个地址都作为一个网段
E类地址为科学研究使用

2 按IP地址的用途分类：公网地址，私网地址
私网地址：每个局域网都可以使用的地址信息，并局域网内唯一，跨越不同局域网可以重复 使用，因此私网地址有效缓解了地址枯竭问题
私网地址的范围：
A类：10.0.0.0 —— 10.0.0.255
B类：172.16.0.0 —— 172.31.255.255
C类：192.168.0.0 —— 192.168.2

10.0.0.0/8	(10.0.0.0	到	10.255.255.255)
172.16.0.0/12	(172.16.0.0	到	172.31.255.255)
192.168.0.0/16	(192.168.0.0	到	192.168.255.255)
169.254.0.0/16	(169.254.0.0	到	169.254.255.255)

@51CTO博客

公网地址：是互联网上可以识别的地址信息，并且是全球唯一
1.3.3 ABC三类地址的可用主机数计算：
公式：2的**N**次方**-2**
注：N为每类地址的主机位数（二进制），最后一个2：表示主机位

```
[root@georgekai ~]# awk "BEGIN{print 2^24-2}"
16777214
[root@georgekai ~]# awk "BEGIN{print 2^16-2}"
65534
[root@georgekai ~]# awk "BEGIN{print 2^8-2}"
254
[root@georgekai ~]#
```
@51CTO博客

1.3.4 ABC三类地址的可用网段数计算：

公式：2的N次方

注：N表示每类地址的网络位数（二进制）

1.3.5 特殊地址

特殊 IP 地址说明：

- 127.0.0.1
  表示回环地址，进行测试使用，验证本地的 TCP 协议簇安装的是否正确。
- 0.0.0.0
  主机位全为 0 的称为是网络地址
- 255.255.255.255
  主机位全为 1 的称为是广播地址，即向所有人发出信息。 @51CTO博客

1.3.6 三种常见的网络通讯类型

8.9.5 IP 地址的类别-按网络通信方式划分

三种常见的网络通讯类型：

- 单播(点到点)
  就是点到点的通讯，例如 A-B 的通信方式
- 组播
  也是一对多的方式，但是可以根据需要进行接收，如果不想接收可以进行过滤掉
- 广播(广播域)
  在一定的范围内，所有成员都会收到的信息，称为广播信息，并且每个成员都要收取，都要进行处理。

@51CTO博客

1.3.7 子网划分

1. 为什么要划分子网？

1）会出现大量的局域网地址，向同一个网关请求，造成网关负载过高

2）会引起局域网内的大量广播数据传送，形成广播风暴

3）浪费地址

2. 子网划分的优点：

1）将一个大的广播域划分为几个小的广播域

2）减少网关设备锁承载的负载量

3）有效避免ip地址的浪费，使一个大的地址空间更加灵活的分配

3. 掩码作用：

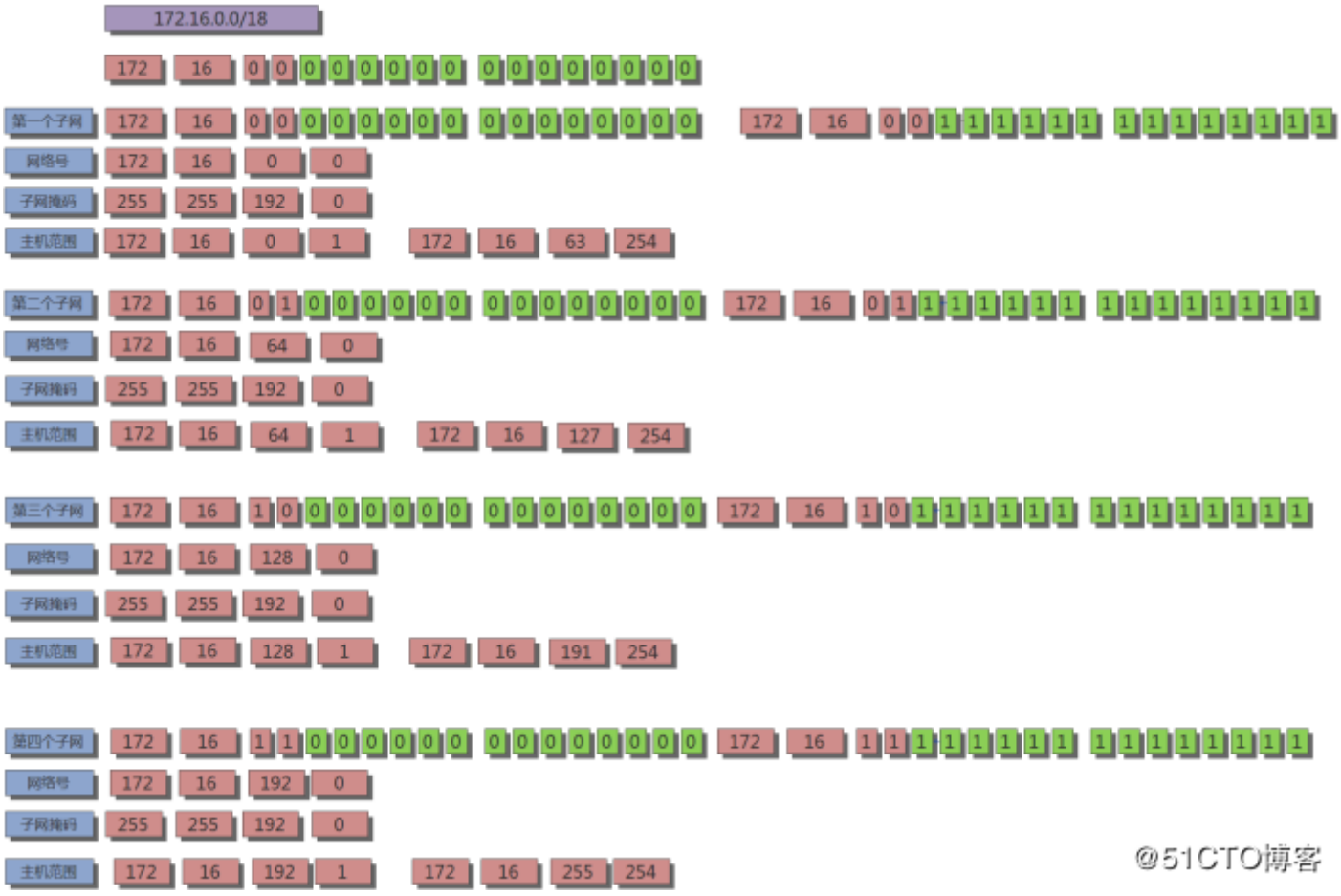
1）利用掩码快速得知是A类地址，还是B类，C类？

2）利用掩码定位网络位信息

4. 掩码表现形式：

1）用十进制表示，分为四组，也是32为二进制数组成
2）A类默认掩码：255.0.0.0 或/8
B类默认掩码：255.255.0.0 或/16
C类默认掩码：255.255.255.0 或/24

实例**1-1** 子网划分计算过程：



小伙伴们可以关注我的微信公众号：linux运维菜鸟之旅

关注“中国电信天津网厅”公众号，首次绑定可免费领2G流量，为你的学习提供流量！