IP 地址详解

在 exam100 上，经常看到很多人问关于 IP 地址的问题。而且问的东西都很简单，可是会的人实在是很少。不说网络工程师，只说做为一个学习网络的人来说，如果不会这个东西，实在是说不过去。

IP 地址这个东西刚开始学确实觉得有些困难，不过当你抓住了原理以后，你会觉得原来是这么简单，这么容易。

我从来不讲什么技巧或者窍门之类的东西，我只说方法和原理。因为窍门有失灵的时候，但是会了方法和原理，只要是这类的东西，你都可以把它们砍的稀巴烂。

二进制基础（Binary）

二进制这个东西很简单，只有两种表示方法“0”和“1”。但是，很多变化就是在这“0”和“1”上面的。在二进制中，“0”和“1”代表的不是“0”和“1”本身，是代表这位有效或是无效（请注意，这里用的是位也就是bit）。每一个二进制位代表一个比特。八个二进制位就代表一个字节（byte）了。后面再说的时候，就只说位和字节了。

比如说，“0101”就代表“无效有效无效有效”。那么这个二进制如何快速的转换为十进制和十六进制呢？下面给一个对照表：1111 1111这八位1每一位分别代表的十进制的值

1	1	1	1	1	1	1	1
128	64	32	16	8	4	2	1

这个就是从右至左第 1 位到第 8 位的二进制位，有效时对应的十进制的值（第一位是 1 那位，第八位是128那位）。记下来这个很容易吧？最低位是1，然后前一位都是当前位的二倍。是不是？哈哈哈……

注：当然也可以通过2^{X-1}来计算当前位的十进制值，X是位数。

那么通过这个表很容易算了，比如“1010”，可以知道，是第四位和第二位是有效的。那么通过表，得到第四位是8，第二位是2。那么十进制就是将这些数相加，也就是10。十六进制表示就是A。

再举一个例子，“1110”，第四位，第三位和第二位都有效，那么就是8，4，2 这几个，相加的十进制就是14，十六进制就是E。

下面给出一个二进制，十进制，十六进制的转化表

十进制	二进制	十六进制
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

八位二进制的计算方法与四位的相同，只不过换算十六进制的方法不同。是把每四位做为一块，每块计算一次，都是从第一位到第四位的计算。

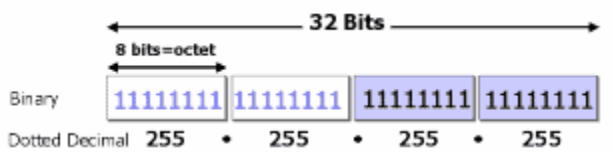
例如："1011 0001"计算十进制的时候是从第一位到第八位对应有效位的值，有效位的值分别是128，32，16，1。那么十进制应该是 177。而转化为十六进制的时候则是每四位为一个块来计算，块内是第一位到第四位，那么可以得到，第一块值是8，2，1。第二块值是1。所以，得到的十六进制是B1。

再举一个例子："1110 1101"十进制有效位的值是：128，64，32，8，4，1。十进制的值为237。十六进制每四位分成一块，第一块有效位的值是：8，4，2。第二块有效位的值是：8，4，1。那么十六进制值为ED。

二进制只要把这些都搞懂了，看IP 地址的二进制的时候就不会晕了。

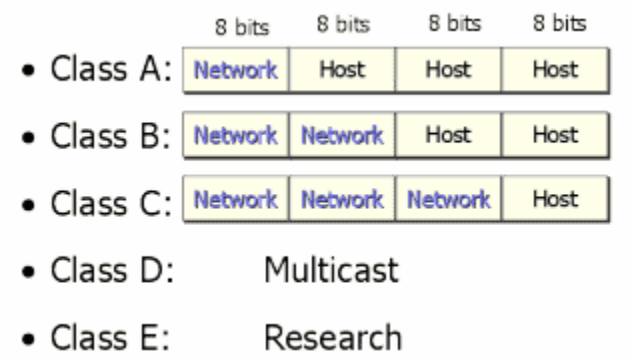
IP 地址（IP Addressing）

IP 地址是由32 位（bit），8字节（byte）组成的。作用就是给每个设备定义一个逻辑地址，以方便查找。



为了寻址方便，所以把这 32 位又分为网络号和主机号两部分。在同一个网络中的设备共享相同的网络号，并且以不同的主机号来进行标识。

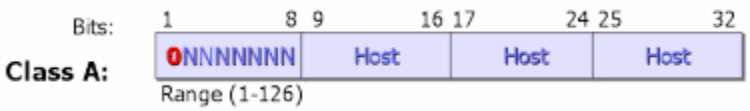
IP 地址的类



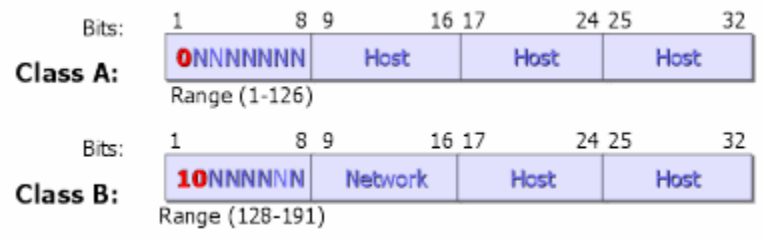
IP 地址设计出来的时候是分类的，这样看上去很好，很有条理，也很美观。A、B、C 类地址用于日常使用。D类用于多播（有的叫组播）。E 类用于研究实验用。

不过，在实际应用中，这些优点似乎没有什么作用。因为A 类网网络太少主机太多，不可能把所有的主机都放在一个A类网中，那样的话，仅仅是广播的流量就足以是整个网络瘫痪。而C 类网网络太多，主机数量却不够用。是个矛盾的问题，所以，才有后面会说到的CIDR和VLSM 的产生。当然，CIDR 和VLSM 最主要的意义还是用来解决IP 地址不够的问题。

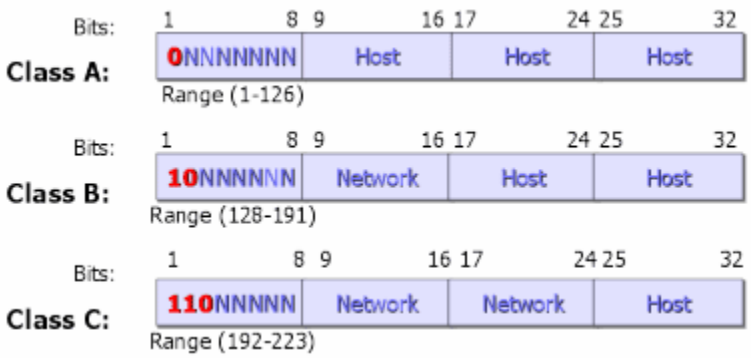
A 类网：第一个字节的第八位是“0”。整个第一个字节是网络号，后面三个字节是主机号。IP 地址以1 - 126 开头的都是 A 类地址。（实际是到 127，不过 127 有特殊作用）



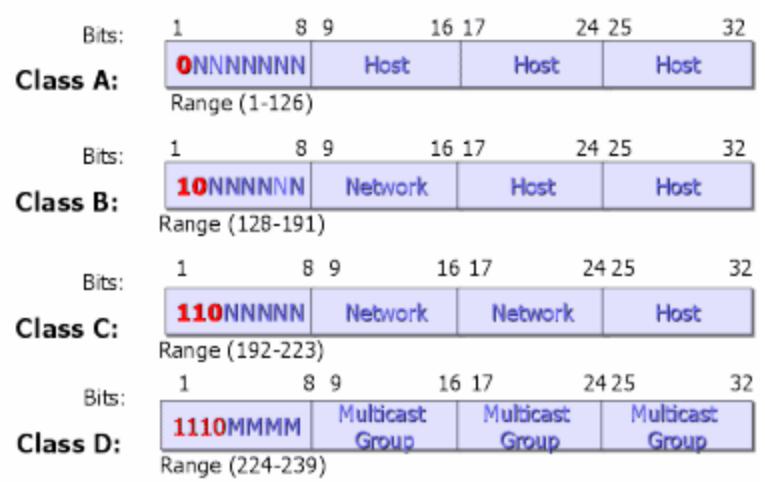
B 类网：第一个字节的第八位和第七位是“1”和“0”。前两个字节为网络号，后两个字节为主机号。IP 地址以128 - 191开头的都是B类地址。



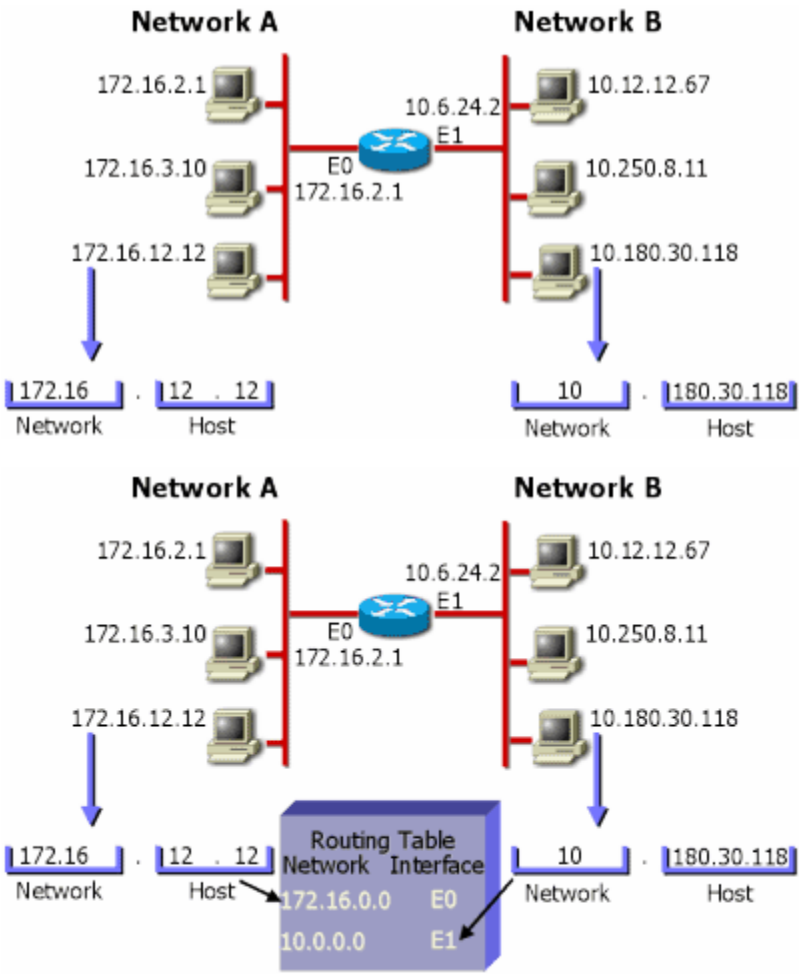
C 类网：第一个字节的第八位，第七位和第六位分别是“1”“1”“0”。前三个字节是网络号，最后一个字节是主机号。IP 地址以192 - 223 开头的都是C 类地址。



D 类网：第一字节的第八位，第七位，第六位和第五位分别是“1”“1”“1”“0”。D类地址是没有网络号和主机号之分的。整个地址组成了一个多播组的地址。



下面是一个网络号和主机号关系的图例



上面这个就是这两个网络在路由表中的情况。一般情况下，路由表中只记录某个网络如何走，而不会具体到某个主机的。具体的路由以及路由表方面的东西，在下一个笔记中会写到。这里就不详细解释了。

子网掩码

子网掩码的作用就是协助 IP 地址计算出网络号。子网掩码和 IP 地址一样，是由 32 位二进制组成的。子网掩码最大的特点就是，所有的网络号的部分，在子网掩码中都表示为“1”，而主机号部分都表示为“0”。比如：B类地址的网络号是前两个字节，后两个字节是主机号。172.16.10.8。其中，172.16 这两个字节就是网络号，10.8 这两个字节是主机号。那么对应的子网掩码就是255.255.0.0。二进制如下表：

十进制	二进制
172.16.10.8	1010 1100 . 0001 0000 . 0000 1010 . 0000 1000
255.255.0.0	1111 1111 . 1111 1111 . 0000 0000 . 0000 0000

仔细看看，是不是对应的网络号的位置上，子网掩码都是“1”？那么如何通过子网掩码和IP 地址计算网络号呢？是通过做“与运算”来实现的。与运算的规则就是“1与1等于1”，“1与0等于0”，“0 与1 等于0”，“0与0 等于0”。计算的方法就是按位做与运算。

从与运算的规则上可以看出，1 和任何数做与运算都等于任何数。0 和任何术做与运算都等于0。所以，子网掩码和IP 地址做与运算以后，由于网络号的地方，子网掩码全是1。所以，网络号的地方都不变，原来是什么，与运算后还等于什么。而主机号的地方，子网掩码全是 0，所以，与运算后全都等于 0。也就是说 172.16.10.8 和255.255.0.0这个子网掩码，与运算后得到的是172.16.0.0，而这个正是172.16.10.8 这个IP 地址所在的网段。

一些特殊地址

127.x.x.x：这个地址是用于本地回路测试的；

255.255.255.255：有限广播地址；

主机号全为0：表示一个网络；

主机号全为1：直接广播地址；

网络号全1 的广播也分为两种，一种是全子网广播，一种是本地子网广播。全子网广播是可以跨越路由器的（本地子网广播不能跨越路由器的原因是路由器的不同端口必须在不同的子网网段，所以，同一个子网的IP 地址不可能分配在两个路由器端口上）。我们常说的路由器可以隔离广播，是指的隔离掉255.255.255.255这种。这种也是应用最广的，比如：ARP和DHCP 都是使用255.255.255.255 这种广播。

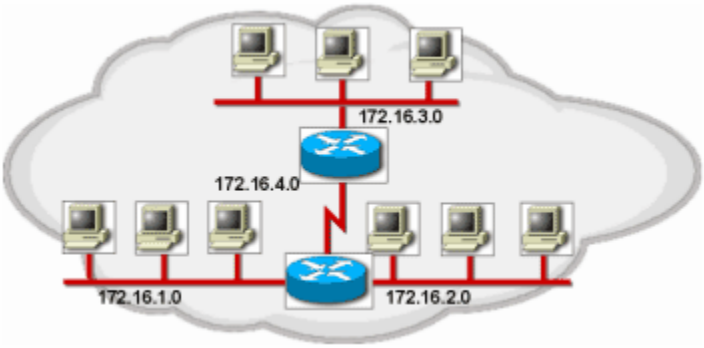
常见的私有地址：10.0.0.0 - 10.255.255.255，172.16.0.0 - 172.31.255.255，192.168.0.0-192.168.255.255；

这些地址都是不可以做为有效的全球唯一的单播地址的。当然还包括 D 类和 E 类的 IP 地址。私有地址中还应该包括169和192 的一个网段，不过不常用，我给忘了，大家有兴趣就上网查查吧。

划分IP 子网和使用可变长子网掩码（IP Subnetting and VLSM）

基于类（classful）的网络看起来很不错，格式也很工整，很美观。不过一个很明显问题就是 A 类主机太多，网络太少。而C 类网络太多，主机太少。这个时候，大家就想，可不可以不受子网掩码的束缚。于是就发明了可

变长子网掩码（Variable Length Subnet Masks，VLSMs）。



由于路由器要求每一个端口上都有一个IP 地址，而且在同一个路由器上，不可以在接口上配置两个相同网段的IP 地址。如果以前使用172.16.0.0 这个网络，只能是所有的机器都放在同一个广播域中。不过为了保证带宽和控制广播对于网络的影响，就需要加入路由器。这个时候使用172.16.0.0 就没有办法用了。所以，划分为几个子网，然后连接到路由器上是一个比较好的选择。

划分子网

划分子网其实很简单，我就不明白为啥搞的这么困难。估计是国内的书写的太垃圾了。建议大家看看国外的书，人家能把很深奥的东西用很浅显的语言表达出来，比老雷的东西不知道精辟多少。那才叫有水平，有含金量了。我尽量也用最浅显方式给大家讲述，当然肯定不如人家洋鬼子了。不过我尽量多的举例子来帮助大家理解。大家记住原理和规则就可以了。开始正题。所谓的划分子网，首先就要明白这个“子”字。所谓的“子”，就是指在原先的基于类的网络上，再次分出来的网络。也就是说 C 类网是 24 位掩码，那么一个 C 类网的子网的掩码是肯定要大于 24 的。同理，A 类网的子网掩码是8 位，那么A 类网的子网的掩码就肯定大于8 位。

下面举几个例子：一个标准的C类IP地址：192.168.1.0/24，那么192.168.1.0/26就表示192.168.1.0/24的一个子网（/24代表的就是这个地址具有24位的网络前缀。网络前缀的意思就是网络号，说明这个地址的前24位都是网络号。也就是说，它的子网掩码的前24位都是1。同理，/26就是指这个IP 地址具有26位的网络前缀，前26 位都是网络号，子网掩码的前26位都是1）。一个标准的B类IP：172.16.0.0/16，那么172.16.5.0/24就表示172.16.0.0/16 的一个子网。

子网都是在主类网的基础上划分的。而且要明确一点就是，子网都是从主机位借位来当做网络位的。那么我们

可以知道，A类网的网络号为8 位，主机号为24位，那么可以用来划分子网的位数就应该是24 位（理论上24 位，实际上要比这个少。B 类和C 类也是这样）。B 类网的网络号为16 位，主机号也是16 位，那么可以用来划分子网的位数就应该是16位。C类网的网络号为24位，主机号为8 位，那么可以用来划分子网的就应该是8 位。

那么我们看看借位的规则。借位的规则是，从左面第一位不是网络号的位开始借，而且借位必须是连续的不能跳跃。而这个位的概念前面也说过了，就是转化成二进制以后的每一个二进制数字就是一位。

例如，一个标准的B类IP 网段172.16.0.0/16，如果要从主机号中借出4位划分子网，那么会从16后面的那个0中借出四位。0表示成二进制应该是0000 0000，借出四位做为网络号的话，就应该是0000 0000。红色部分代表借出成为网络号的位。那么这个172.16.0.0/16 这个网段就被划分为16 个子网（2^4=16）。假设其中一个网段172.16.48.0/20（以前是16 位网络号，再加上刚才借的4 位就是20位了），要求借出3 位再次划分子网，这个时候从哪里划分呢？还是那个规则，从左面第一位不是网络号的位开始借，而且借位必须是连续的不能跳跃。这个时候左边第一位不是网络号的就应该是0011 0000 了。所以，再借三位就应该是0011 0000 了。在表示的时候就应该使用172.16.48.0/23（刚才20 位，现在又借了3 位）。

再举例，这次全用二进制表示，以达到直观的效果。不过大家不要被搞晕就好。IP 网段使用的是：192.168.1.0/24，从中借3位作为网络号。

IP 十进制：192 .168 .1 .0

IP 二进制：1100 0000 .1010 1000 .0000 0001 .0000 0000

如果借出三位，那么应该从左面第一为不是网络号的位开始借位。那就应该是这里：

IP 十进制：192 .168 .1 .0

IP 二进制：1100 0000 .1010 1000 .0000 0001 .0000 0000

那么借位后就应该是：

IP 十进制：192 .168 .1 .0

IP 二进制：1100 0000 .1010 1000 .0000 0001 .0000 0000

这里可能会问，这不都一样吗？没有什么变化，只是把有些位作为网络号部分了。其它的没什么变化。其实还

有一个最关键的东西也是在变化的。那就是子网掩码。是否划分了子网，从子网掩码一眼就可以看出来。为什么呢？前面已经说了，子网掩码就是用来和IP 地址配合计算网络号的。所以，在子网掩码中，所有的网络号的部分都是1，而主机号的部分都是0。

用上面这个例子来说，划分子网前：

IP 网段十进制：192 .168 .1 .0

IP 网段二进制：1100 0000 .1010 1000 .0000 0001 .0000 0000

掩码的十进制：255 .255 .255 .0

掩码的二进制：1111 1111 .1111 1111 .1111 1111 .0000 0000

划分子网后：

IP 网段十进制：192 .168 .1 .0

IP 网段二进制：1100 0000 .1010 1000 .0000 0001 .0000 0000

掩码的十进制：255 .255 .255 .224

掩码的二进制：1111 1111 .1111 1111 .1111 1111 .1110 0000

红色部分是划分子网前后变化的部分。所以，在划分子网的时候必须也把子网掩码做相应的变化，否则，无法计算出子网的网络号。这点很重要。

在VLSM中子网掩码的使用

如何使用IP 地址和子网掩码计算网络号在前面已经说过了，这里就不再重复了，这里只给出一个计算子网网络号的例子。IP 地址：192.168.1.169，子网掩码为：255.255.255.224。以二进制进行计算：

地址：1100 0000 . 1010 1000 . 0000 0001 . 1010 1001

掩码：1111 1111 . 1111 1111 . 1111 1111 . 1110 0000

红色部分就是划分的子网部分（因为这是一个 C 类网络，所以前 24 位肯定已经是网络号了，子网只能是在

二十四位以后的网络号部分），而网络号则是整个彩色部分，黑色部分就是主机号了。子网掩码就是标识出所有的网络号的部分，因为网络号的部分在子网掩码中都使用 1 来表示。使用 IP 地址和子网掩码对应的位做与运算。与运算的规则就是任何数和1进行与的时候都等于任何数。这里子网掩码都是1 的部分都是网络号，所以和子网掩码做与运算以后的结果还是原来的任何数。而和0 做与运算的部分就都等于0 了。这样就可以达到屏蔽掉主机号部分的作用。屏蔽掉主机号剩下的自然就是网络号了。从例子中很容易知道这个 IP 地址所在的网络号就是：1100 0000 .1010 1000 . 0000 0001 . 1010 0000，转换为十进制就是：192.168.1.160。

题型实例

1、给定IP 网段：192.168.1.0/24，要求划分子网。子网的要求是：每个网络可以容纳下35 台主机。所有划分子网的题都使用同样的公式，计算网络数量：2x=Y（X 是借用的位数，Y 是网络数量），计算主机数目：2x-2=Y（X 是借位后剩下的主机位的位数，Y 是主机数量）。

这个题计算方法很简单，每个网络容纳35台主机，所以有等式：2x-2> = 35。那么可以得出X = 6（5是不行的，如果 X 等于 5 的时候，主机数量只有 30 台。虽然使用 6 可以容纳 62 台主机，对于 35 来说很浪费，但是没办法，只能等于6）。那么就可以知道需要有6 位要当做网络号。那有多少位可以用来借位呢？看题目，网络前缀是24位，所以用总位数减去网络前缀就是可以借位的数量，也就是32-24=8。有8 位可以用来借位，需要剩下6位做主机号，那么也就是说要借出来两位。那么用二进制表示为：1100 0000 . 1010 1000 . 0000 0001 . 0000.0000。所以，可以划分出四个子网。这四个子网的网络号分别是：192.168.1.0/26，192.168.1.64/26，192.168.1.128/26，192.168.1.192/26（就是红色那两位的四种组合：00，01，10，11）。

2、给定IP 网段：192.168.1.0/24，要求划分子网。子网的要求是：划分出11 个子网。这个时候，就要应用这个公式了：2x> = 11。于是可以得出 X = 4。从而知道了应该从主机位中借出 4 位当做网络号。用二进制表示为：1100 0000 . 1010 1000 . 0000 0001 . 0000 0000。

看了这两题大家就应该知道了，其实这样的题目很简单，就是计算网络的时候用网络的公式，计算主机的时候使用主机的公式。其余的类似题目都是在这两题的基本形式上做了一些变化。万变不离其宗，所有的计算子网的题

目只需要这两个公式即可搞定。只不过有些题需要注意一些细小的地方。比如，已经分过子网了，还要你再次划分子网。这个时候就需要注意从哪里开始划了。只要记住：从左面第一位不是网络号的位开始借，而且借位必须是连续的不能跳跃。

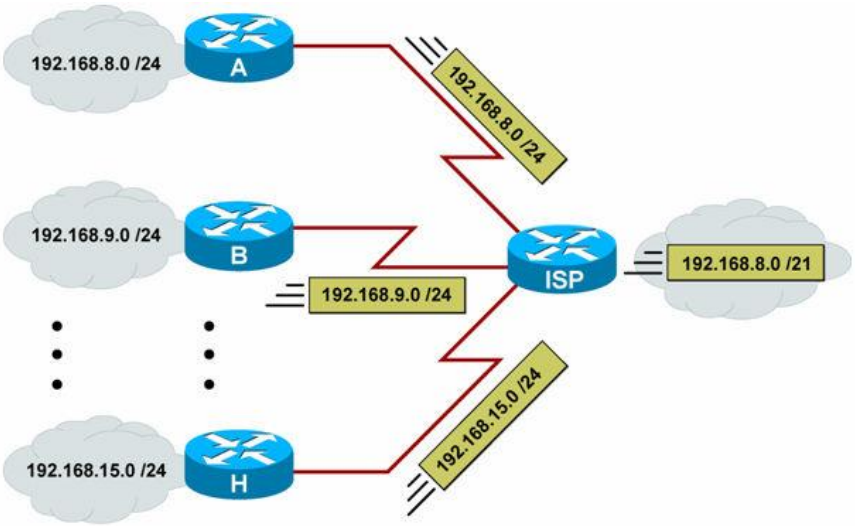
3、计算哪些是非法主机地址。这类题目不要看见IP 地址里面很多0 或者有255 就选。有0 和255不见得就是非法地址，需要看子网掩码。使用子网掩码和IP 地址来计算，看看是不是主机号的部分是全0 和全1。如果不是，即使有0 和 255，也是一个合法的IP 地址（计算方法前面说了）。还有就是前面说的几种特殊的IP 地址也不是合法的IP 地址（私有地址是合法的IP 地址，但是不是全球唯一的单播地址，也就是公网地址）。

4、计算出选项中哪个地址和题目中给出的 IP 地址是同一个网段（或者是可以相互通信）。这个和 3 的做法基本相同。先使用题目中给出的IP 地址和子网掩码计算出其所在网段的网络号。然后分别使用选项中的IP 地址和子网掩码计算出他们所在网段的网络号。与题目中IP 地址的网络号相同的就是选项。

我所说的题型只是举个例子。不过考试中能遇到的这类的题也就是这几种类型的。基本上都大同小异，只不过表述的方式跟我写的不太一样。这几种类型都会了，那么其余的应该也没问题了，最多是其中几种类型的合起来使用。学到网络工程师了，举一反三的能力都应该是有的吧？不要把东西学死，要灵活运用。

路由汇总和无类域间路由（Route Summarization and CIDR）

无类域间路由（Classless Inter-Domain Routing）



无类域间路由技术一般都是使用在ISP 供应商的。CIDR 技术的意义在于，可以把数个主机数量很少的网络，合并成一个主机数量比较多的网络，以便使用。并且可以减小ISP 供应商那边路由表条目的减小。

CIDR计算的方法也是很简单的，观察下表：

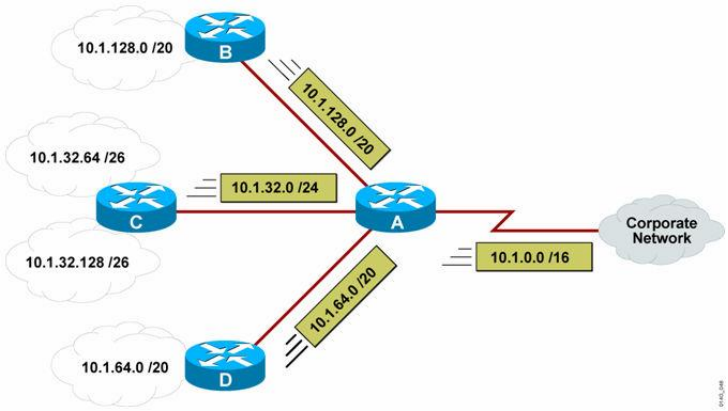
192.168.0.0/24	1100 0000 . 1010 1000 . 0000 0000 . 0000 0000
192.168.1.0/24	1100 0000 . 1010 1000 . 0000 0001 . 0000 0000
192.168.2.0/24	1100 0000 . 1010 1000 . 0000 0010 . 0000 0000
192.168.3.0/24	1100 0000 . 1010 1000 . 0000 0011 . 0000 0000
192.168.4.0/24	1100 0000 . 1010 1000 . 0000 0100 . 0000 0000
192.168.5.0/24	1100 0000 . 1010 1000 . 0000 0101 . 0000 0000
192.168.6.0/24	1100 0000 . 1010 1000 . 0000 0110 . 0000 0000
192.168.7.0/24	1100 0000 . 1010 1000 . 0000 0111 . 0000 0000

可以观察到这些IP 网段的规律。彩色部分都是网络号。在网络号中蓝色部分都是始终不变的，红色的部分是变化的。而这种变化也是有规律的，共有三位在变化，那我们应该知道这个变化的种类应该共有八种（2 的 X 次方，这里X是3，所以八种）。也就是说上表中的红色部分包含了所有这八种的变化。当蓝色部分始终保持不变，且红色部分呈上述规律变化的时候，就可以进行 CIDR 了。而 CIDR 后的网络号部分应该是蓝色部分，所以应该是 21 位前缀。那么CIDR 的结果应该是192.168.0.0/21。

其实 CIDR 就是划分子网的一个逆运算。划分子网是网络不够用，需要从主机号部分借位做网络号。而CIDR则是主机不够使用，需要从网络号部分借位作为主机号。

还想多写一点，不过 CIDR 这块就这点东西。只要知道如何把这些地址汇聚起来就可以了。实在没有什么好说的，很基础的东西。按照规律多多练习一下应该没问题的。

路由汇总（Route Summarization）



路由汇总一般是使用在路由器上的技术。路由汇总的意义在于，可以在通告上层路由器的时候，进行地址的汇聚，使得上层路由器的路由表更小。这样，可以占用更小的内存，节省路由器的资源开销。并且可以把问题限制在本地化（这个到后面的路由协议部分会讲到）。

路由汇总的方法和 CIDR 相同。不过有一个不同点：CIDR 后的网段是需要把所有这个汇聚后网段应该有的网段都包括进来。就像上面的表格，CIDR需要有表格中所有的IP 网段的时候才能汇聚成192.168.0.0/21。而路由汇总则不必须。只要保证在除了你以外，别人不再有IP 网段是属于你汇总的网段内就可以了。比如上图中，C路由器汇总了一条10.1.32.0/24 的路由，发送给A。那么A 的右侧就不可以再有路由器通告属于10.1.32.0/24这个网段中的网段了。

总结一下，IP 地址的计算实际上就是二进制的计算，所以，一定要把二进制搞清楚。否则很难学好 IP 地址方面的东西的。还有就是记住各种规律和方法。剩下的事就是把这些规律和方法套在题目上，把题目搞定！

由于水平有限，错误在所难免，欢迎大家批评指正！

Written by 研究僧 kldsh2002

2005-7-10

E-mail address kldsh2002@126.com