**IP地址简介**

这里主要介绍在网络上传输数据时候所需要的IP地址的相关信息。相关内容主要包括：IP地址分类、子网划分、子网掩码、无分类编址（CIDR）、使用子网掩码时分组的转发过程。可做为日常划分子网设置时的参考。

**1、IP地址**

**=========================================**

IP地址是一个32位的二进制数，用来在网络中唯一标识一台计算机。IP地址由因特网名字与号码指派公司（ICANN，即：Internet Corporation for Assigned Names and Numbers）分配。我国用户可向亚太网络信息中心（APNIC，即：Asia Pacific Network Information Center）申请IP地址（需缴费）。

IP地址的编址方法共经历了三个阶段：（1）分类的IP地址（1981）。（2）子网的划分（1985）。（3）构成超网（1993，也叫无分类编址方法，简称CIDR）。后面在适当之处会详细介绍。

**2、分类的IP地址**

**=========================================**

为了方便IP寻址，将所有IP地址所在的网络划分为A、B、C、D和E五类，IP地址由网络ID（也叫网络号）和主机ID（也叫主机号）两部份组成。每种类型的网络对其IP地址中用来表示网络ID和主机ID的位数作了明确的规定。

A类地址用IP地址前8位表示网络ID，后24位表示主机ID。表示网络ID的第一位必须以0开始，其他7位可以是任意值，当其他7位全为0是网络ID最小，即为0；当其他7位全为1时网络ID最大，即为127。网络ID不能为0，它有特殊的用途，用来表示所有网段，所以网络ID最小为1；网络ID也不能为127；127用来作为网络回路测试用。所以A类网络网络ID的有效范围是1-126共126个网络，每个网络可以包含224-2台主机。

B类地址用IP地址前16位表示网络ID，后16位表示主机ID。表示网络ID的前两位必须以10开始，其他14位可以是任意值，当其他14位全为0是网络ID最小，即为128；当其他14位全为1时网络ID最大，第一个字节数最大，即为191。B类IP地址第一个字节的有效范围为128－191，共16384个B类网络；每个B类网络可以包含216-2台主机（即65534台主机）。

C类地址用IP地址前24位表示网络ID，后8位表示主机ID。表示网络ID的前三位必须以110开始，其他22位可以是任意值，当其他22位全为0是网络ID最小，IP地址的第一个字节为192；当其他22位全为1时网络ID最大，第一个字节数最大，即为223。C类IP地址第一个字节的有效范围为192－223，共2097152个C类网络；每个C类网络可以包含28-2台主机（即254台主机）。

D类地址用来多播使用，没有网络ID和主机ID之分，其第一个字节前四位必须以1110开始，其他28位可以是任何值，则D类IP地址的有效范围为224.0.0.0到239.255.255.255。

E类地址保留实验用，没有网络ID和主机ID之分，其第一字节前四位必须以1111开始，其它28位可以是任何值，则E类IP地址的有效范围为240.0.0.0至255.255.255.254。其中255.255.255.2555表示广播地址。

在实际应用中，只有A、B和C三类IP地址能够直接分配给主机，D类和E类不能直接分配给计算机。

**3、公共IP和私有IP地址**

**=========================================**

IP地址由IANA（Internet地址分配机构后来被ICANN掌管）管理和分配，任何一个IP地址要能够在Internet上使用就必须由IANA分配，IANA分配的能够在Internet上正常使用的IP地址称之为公共IP地址；同时IANA也保留了一部份IP地址，这部份IP地址不能在让个人和机构在Internet上使用，此类IP地址就称之为私有IP地址，这些非注册的私有IP地址可供组织个人内部使用。因为Internet上没有私有IP地址的路由，所以，私有IP地址不能在Internet上使用。私有IP地址范围包括：

A类：10.0.0.0/8

B类：172.16.0.0/12 即172.16.0.1-172.31.255.254共16个B类网络

C类：192.168.0.0/16即192.168.0.1-192.168.255.254共256个C类网络

在我们组建局域网的时候（例如在家中将多个机器组成一个局域网，可以共享同一个宽带口上网，还可实现局域网内机器的数据共享），可以使用私有IP做为局域网内机器的IP地址。另外我们需要注意的是，以上和后面讨论的网络间机器通信的路由过程，都是不同网段具有公共IP机器的路由，而不是到这样的只有私有地址的局域网机器的路由（但是两者路由时候的基本原理是一样的）。像这样的私有地址局域网内的机器，在公共网络上是不可见的，虽然这个局域网内的机器能够通过网关访问到外面，但是通过一般手段，外面无法访问到这个局域网中的特定机器，在外边的公网看来，这个局域网内所有的机器连同它们的网关共同组成了一个“机器”，即网络节点，节点的IP就是网关暴漏给外面的公网IP，这点不在本文讨论范围内。

**4、子网的划分**

**=========================================**

前面介绍的“分类的IP地址”，不利于根据企业需要灵活分配IP地址。比如，一个企业有2000台计算机，那么根据前面对各类IP地址规定，要么为其分配一个B类的网络地址，这样该网络可包含65534台计算机，将造成63534个IP地址的浪费；要么为其分配8个C类网络地址，那么必须用路由器连接这个8个网络，造成公司网络管理和维护的负担。

以上问题的根源就在于早期建立的IP地址结构，只有“网络号+主机号”这样的两级结构，且长度固定（即A类、B类、C类等几种网络的网络字段长度和主机字段长度是固定的）。为解决上述问题，1985年在原有IP地址的两级结构中增加了一个“子网号”，这样原来的两级IP地址变成了“网络号+子网号+主机号”三级结构，其中“网络号”就是原来两级结构中的网络号，“子网号+主机号”就是原来两级结构中的“主机号”。

通过对原来网络中固定长度的“主机号部分”，划分为可变的“子网号+主机号”两部分（但是两者总长还是固定的），可以实现将原有网络号对应的网络（一般是A类、B类或C类的网络）中再次划分子网，原来两级结构中的“主机号”部分不再固定不变，增加了灵活性，节省了IP地址的浪费。

**5、IP寻址简述**

**=========================================**

这里IP寻址的意思就是根据一个IP地址，找到相应的机器，也就是路由的过程。 无论是划分了子网的网络，还是没有划分子网的网络，各个不同网络之间，都是通过路由器相连接的。

对于前面的描述，我们把IP地址中“网络号+子网号”共同组成的部分，称作IP地址对应的网络地址部分，网络地址部分再加上全零的主机地址便成了网络地址。这样我们很容易算出一个IP地址对应的网络地址。例如：

IP地址：168.169.170.171

是一个B类地址，我们没有给它划分子网，于是它的网络地址为：168.169.0.0。若划分子网了，那么就将"170.171"中相应于的子网位也换算成二进制，并表示出来，这里不详细说明了。

假设A主机给B主机发送IP数据包，当知道了网络地址的长度之后，A主机便可通过根据IP包中的目的地址（B主机的IP地址），知道的其相应的网络地址是否和自己的网络地址相同，如果相同那么两者就在同一网段，于是，A直接发送数据给B；如果网络地址不同，那么两者不在同一个网络中，所以需要由路由器负责位于不同网络的机器之间的通信。

总之，发送数据时：（1）发送主机先检查IP包中目的IP地址的网络地址，如果和自己相同则直接发送给主机（2）如果不同，则通过路由器将包发送到目的网络，再到达主机。（3）路由器中的路由表，记录了它所知的所有IP网络地址对应的目的网络，目的网络中的机器（路由）会将发给它网络中机器的数据包传达给正确的主机。

**6、子网掩码**

**=========================================**

前面所述的路由过程，有一个关键的地方就是要确定目的地址的“网络地址”的长度。虽然没有划分子网的分类IP地址其网络地址长度是固定的，但是经过了“子网的划分”之后，由于网络地址的长度变得不固定了，所以需要一种新的方法，以便确定一个IP地址对应的网络地址的位数。我们可以用子网掩码来实现这点。

子网掩码的位数和IP地址相同，格式是将主机部分全置为0，网络地址部分全置为1。例如：A类地址的子网掩码就是255.0.0.0；B类地址的子网掩码为255.255.0.0；划分了两个子网的B类网址其子网的子网掩码为255.255.128.0。

因此可知，网络地址就是IP地址与子网掩码进行与运算获得，即将IP地址中表示主机ID的部份全部变为0，表示“网络ID+子网ID”的部份保持不变。再次强调，网络地址的格式与IP地址相同都是32位的二进制数；主机号就是表示主机号的部份。

例1：IP地址:192.168.23.130 子网掩码：255.255.255.192

则：这是划分了子网的C类网络中的IP地址；网络地址为192.168.23.0；网络号为192.168.23；子网号：2；主机ID:2。

例2：IP地址:192.168.23.130 子网掩码：255.255.255.0

则：这是没划分子网的C类网络中的IP地址；网络地址为192.168.23.0，网络号为192.168.23，主机ID:130。

现在的标准规定，所有的网络都必须有一个子网掩码。

**7、使用子网掩码进行IP寻址**

**=========================================**

在不划分子网的两级IP地址下，从IP地址很容易得到相应的网络地址。划分子网之后，仅从IP地址无法得到相应的网络地址，而且IP数据包中也没有关于网络地址的信息，所以还需要通过子网掩码来尝试得到一个IP地址的网络信息，而这个子网掩码则是预先在发送端配置好了的。举例说明一下发送IP数据包时，使用子网掩码寻址的过程。

例1，假设位于同一个子网的A向B发送IP包。大致过程是：

（1）A要有一个待发送的IP包，其中包含B的IP地址以及A本身的IP地址；还要有一个在A上面配置的自己的本地子网掩码（通过这个“本地子网掩码”，A会以为自己所在的网络其网络地址位数是本地子网掩码中1的个数）。

（2）A将B的IP地址和本地子网掩码相与，得到自己理解的B的IP地址所属的网络地址netb；A再将自己的IP和本地子网掩码相与，得到自己理解的自己的IP地址所属的网络地址neta；

（3）将netb和neta比较，两者相同，则A认为B与它在同一个网络中，所以不经过其它机器（例如路由器），直接将IP包转发给B。

例2，当A和B位于不同子网，则前面的netb和neta不相同，这时候需要经过路由进行转发。大致过程是：

（1）A上面一般会事先配置一个网关R，这个网关的IP地址应当和A在同一个网络中。当A发送的IP包目标地址B不属于A的网络时会将这个IP包发送给网关R（注意，这个时候，IP包中的目的地址并没有变成R的IP地址，A只是通过它本身的网关配置，知道了R的IP地址并在IP层下面的网络接口层中将目标的MAC地址变成了R的MAC地址发送给R；而R在转发时，目的IP仍旧不变，也会在MAC帧中重写目标MAC地址，这期间涉及到使用ARP协议根据机器IP查询其MAC地址，以及网络接口层的内容，这里不详细叙述了）；另外，一台机器应该可以设置多个网关，指定它们用转发特定外网中的目的地址，或者配置一个无论哪个外网地址都会转发给这个网关的默认网关地址。

（2）R上面有一个路由表，其中的每项记录包含了它所知的所有网络的网络地址、子网掩码、以及对应的路由（如果目的地址B在另外一个路由连接的不同网络中）或者主机B所连网络的接口（如果目的地址B在同一个R路由器所连接的不同网络中）。注意，因为路由器是可以连接不同的网络的，所以路由器上面有至少两个网络接口，每个网络接口对应一个网络地址，而相应地，主机却只有一个网络地址。

（3）R根据自己的路由表和IP中的目的地址B所在的位置并发送。具体过程是：将路由表中第一项的子网掩码与目标地址B进行与，得到网络地址如果匹配相应表项的地址则转发到相应的网络接口或者路由，否则对下一项进行同样的匹配，直到出现匹配的情况并且将数据发送出去。

（4）R的路由表中若有一个默认的路由，则当所有项都不匹配的时候将数据发送到这个路由。

（5）如果以上过程全都没有匹配，则报告转发分组出错。

通过以上描述我们可知：（1）子网掩码是在发送端上的，而不是在网络中传输的。（2）发送端发送的时候会根据自己的子网掩码来确定（它所认为的）目标IP的网络地址，而不是通过某个事先公共协商好的子网掩码；（3）发送端的子网掩码虽然理论上可以随意配置，但是应当和自己所属的子网对应的网关的接口子网掩码一致，否则很可能会有问题。

**8、一些概念**

**=========================================**

至此，在讲述CIDR（无分类编址）之前，为便于理解，我们将遇到过的“子网掩码、网络地址、网络类别、IP地址、网络号、子网、子网号、主机号”这几个比较容易混淆的概念再进行一下总结：

（1）IP地址是在发送IP包时，用于标识网络节点（例如某个特定主机）的具体位置，目前长度固定为32位；

（2）IP地址中分为“网络部分”和“主机号”，网络部分是IP地址的“左”边，“主机号”在IP地址的“右”边；

（3）网络地址其格式和IP地址格式几乎一样，用于标识一个IP地址究竟属于哪个网络；

（4）计算一个IP地址的网络地址的方法是将IP地址仅保留“网络部分”，而将“主机号”部分全部置零；

（5）网络类别是指对所有IP地址按某种策略分类，得到的A、B、C、D、E等这些网络，一个IP地址一定属于其中的一类，也可理解为“分类编址”（与CIDR的无分类编制相对）；

（6）划分子网之后，IP地址中的“网络部分”从左到右又可划分为“网络号+子网号”，如果没有划分子网则没有“子网号”部分。

（7）一种类别的网络，如果划分了子网，那么其中的IP地址“网络号”部分的位数是固定的，“子网号”部分位数是不固定的（位数越少则子网越“大”，包含的主机数也越多），而后面的“子网号+主机号”总和是固定的位数（32位-“网络号”位数）；

（8）一种类别的网络，如果没有划分子网，则其中的IP地址“网络部分”没有“子网号”部分，并且网络位数是固定的，等于其“网络号”部分，因此“主机号”部分也是固定的（32位-“网络号”）。

以上这些概念不是严格如此的，但是尝试用这里的方式，应该能助于理解相关的内容。

**9、无分类编址**

**=========================================**

（1）无分类编址的提出

划分子网在一定程度上解决了Internet发展中遇到的许多困难，但是随着因特网的普及，仍然面临着两个重要的问题：

（a）IP地址面临耗尽的问题。

（b）路由表项目急剧增长。

第一个问题属于长远的问题，将由IETF（即Internet Engineering Task Force，互联网工程任务组，主要任务是负责互联网相关技术规范的研发和制定）成立的IPv6工作组研究新版本IP协议时解决；第二个问题采用无分类编制（即CIDR，Classless Inter-Domain Routing）来解决。

（2）CIDR最重要的两个特点

（a）CIDR消除了传统A、B、C等分类，以及在分类的IP中进行子网划分的概念。

CIDR不用子网，而直接使用网络前缀，这样IP地址又变回了两级结构，即IP地址={网络前缀，主机}。但是这里的网络前缀直接就是IP地址中除主机部分的网络地址部分，这个网络地址已经没有A、B、C之类的区别。IP地址采用“斜线记法”（又称CIDR记法），即在IP地址后面加上一个"/"，在加上网络前缀的位数。

例如：128.15.68.36/20，表示这个32位的IP地址中，前20 bit表示网络前缀，后12 bit表示主机号。

（b）CIDR将连续的、网络前缀相同的IP地址组成“CIDR地址块”。

由于没有IP地址分类的概念（即A、B、还是C等类的网络）了，所以，一个地址块可能包含多个某种类型的网络（例如一个“/18 地址块”相当于64个C类的网络），通过这个方式，CIDR使得路由器中的路由表项目，比包含分类IP概念的路由表项目少了很多。这个我们可以称作“路由聚合(route aggregation)”或者“构成超网（supernetting）”。地址块包含如下信息：起始地址+地址块中的地址数。它也采用和IP地址一样的“斜线记法”。

例如：128.15.32.0/20表示一个包含2^12个主机的地址块（因为网络前缀20位，所以主机数目是2的12次方个），其起始地址为128.15.32.0。有时候，我们可能不必关心起始地址，那么可以省略起始地址部分，例如：“/20 地址块”表示有20位网络前缀的某个地址块。因为地址块的记录方法和IP地址一样，所以，有时候，需要根据上下文来确定，一个用斜线记法表示的地址是IP地址，还是CIDR的IP地址块。

（3）其它注意

另外，CIDR中虽然没有子网概念了，但是还有掩码的概念，掩码也可用斜线记法表示。CIDR的斜线记法还有以下等效的方式：

10.0.0.0/10，可简写为10/10（即点分10进制的IP部分中低位连续的0省略）。

0000101000xxxxxx xxxxxxxx xxxxxxxx，这里的"x"表示任意主机地址，非"x"的部分是网络前缀。

0000101000\*，这里的"\*"表示任意主机地址，非"\*"部分是网络前缀。

注意，在配置基于CIDR的网络时候，可能有的主机以前就是基于分类的IP地址的（无论有无子网划分），他们可能不允许将网络前缀设置为比原来分类地址的子网掩码1比特长度更短。例如：200.25.16.0/20这样的配置就不行，因为在它看来这是一个C类网络，其子网掩码长度至少为24位。所以，只有主机软件支持CIDR之时，网络前缀才能比原来的分类IP地址掩码长度更短。

由上面我们可以看出，使用CIDR可以减少路由表项目，也可以更有效的利用IP地址。通过下面两个例子可以有助了解：

（a）假设有一个ISP，它拥有地址块206.0.64.0/18。在采用CIDR之前，这个ISP其实相当于拥有64个C类网络，每个和此ISP通信的网络都需要在其路由内部有至少64个与此ISP相关的路由表项；采用CIDR地址聚合之后，这个ISP的相关表项就致用一个"/18 地址块"即可。可见，采用CIDR大大减少了路由表中的表项数目。

（b）假设有一个大学需要向上面提到的ISP申请800个IP地址。在采用CIDR之前，ISP或者为这个学校分配1个B类地址（这将浪费64734个IP地址），或者分配4个C类地址（这样各个相关路由表中会有4个该大学的表项），而且这个大学给其各系分配子网之时，也会比较复杂；采用CIDR之后，ISP只需要给这个大学分配一个"/22 地址块"，大学也可以给其各个系分配相应大小的地址块。可见，采用CIDR大大提高了IP的利用率和管理复杂度。

当采用CIDR之时，IP地址由“网络前缀+主机号”组成，路由表项目则相应地改成了“网络前缀+下一跳路由”，这样在查找路由的时候，一个IP地址可能得到不止一个匹配结果，这是采用最长匹配原则，确认网络前缀最长匹配的一项。

例如：前面的ISP给大学分配了206.0.68.0/22地址块，该大学又给其某个系分配了206.0.71.128/25地址块，这样，ISP中就有了这两个路由表项。当ISP收到一个数据报目的IP为D=206.0.71.130之时，查找表项将D与前面两表项中的子网掩码与目标地址相与，发现都匹配，但是由于206.0.71.128/25的网络前缀更长，所以会采用这个更长的路由表项（因为网络前缀越长，信息越具体）。

虽然现在很难将已经分配出去的IP重新收回，再采用CIDR的策略重新规划IP分配，但是CIDR已经推迟了IP地址将要耗尽的日期。

**10、补充**

**=========================================**

以上内容，基本是对教科书和网络资料以及在一些实践基础上的总结，其中有描述不够准确的地方，希望读者能够联系我，相互交流和学习。^\_^

**作者：QuietHeart**

**EMail：quiet\_heart000@126.com**

**日期：2012年6月23日**