

网络地址转换（NAT）配置实例 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/245/2021_2022__E7_BD_91_E7_BB_9C_E5_9C_B0_E5_c101_245613.htm

NAT包括有静态NAT、动态地址NAT和端口多路复用地址转换三种技术类型。静态NAT是把内部网络中的每个主机地址永久映射成外部网络中的某个合法地址；动态地址NAT是采用把外部网络中的一系列合法地址使用动态分配的方法映射到内部网络；端口多路复用地址转换是把内部地址映射到外部网络的一个IP地址的不同端口上。根据不同的需要，选择相应的NAT技术类型。由1994年NAT技术问世以来，NAT技术很快在企业LAN领域得到广泛应用。目前，NAT技术主要用于连接和安全方面。目前企业内部网络用户数量大，而能申请的合法的全球唯一IP地址有限。NAT能够有效的解决企业IP地址短缺问题，利用NAT技术能够实现多个用户共同使用一个合法的IP地址连接互联网。而另一种需要出于安全方面来考虑，在一定程度上防范网络攻击的发生。企业期望隐藏LAN内部网络结构，NAT可以将内部LAN与外部Internet隔离，使外部网络用户无法了解通过NAT设置的内部IP地址。NAT技术在企业中都采取两种技术类型结合应用，比较好的还是和端口复用地址转换。结合起来的如：端口复用地址转换、TCP/UDP端口NAT映射、静态地址转换 端口复用地址转换、动态地址转换 端口复用地址转换。如果ISP提供的合法IP地址数量较多，当然可以采用静态地址转换 端口复用动态地址转换技术得以完美实现。然而，如果只获得1个合法IP地址，虽然可以采用端口复用地址转换技术，实现整个网络

的Internet接入。但是，由于服务器也采用动态端口，Internet中的计算机将无法访问到网络内部的服务器。有没有好的解决问题的方案呢？当然，这就是TCP/UDP端口NAT映射。既然只有一个可用的合法IP地址，当然采用端口复用方式来实现NAT.不过，由于同时有要求网络内部的服务器要被Internet访问到，因此必须采用PAT创建TCP/UDP端口的NAT映射。我们知道，不同应用程序使用TCP/UDP端口是不同的，例如，WEB服务器使用80、FTP服务使用21、SMTP服务使用25、POP3服务使用110等。由于每种应用服务器都有自己默认的端口，所以这种NAT方式下，网络内部每种应用服务器成为Internet中的主机，例如，只能有一台WEB服务器、一台E-mail服务、一台FTP服务器。尽管可以采用改变默认端口的方式创建多台应用服务器，但这种服务器在访问时比较困难，要求用户必须先了解某种服务采用的新TCP端口。因此，可以将不同的TCP端口绑定至不同的内部IP地址，从而只使用一个IP地址，即可在允许内部所有服务器被Internet访问的同时，实现内部所有主机对Internet的访问。根据企业的网络环境利用TCP/UDP端口映射的应用，如企业网络采用1000Mbps光纤接入Internet.路由器选用拥有2个10/100/1000Mbps自适应端口的Cisco2821.内部网络使用的IP地址段为192.168.1.1 ~ 192.168.1.254（根据内部网络规模而定），局域网端口Ethernet 0的IP地址为192.168.1.1，子网掩码为255.255.255.0.网络分配的合法IP地址范围为202.99.16.128 ~ 202.99.160.135，子网掩码为255.255.255.248，连接ISP的端口Ethernet 1的IP地址为211.82.220.129，子网掩码为255.255.255.252，可用于转换IP地址为211.82.220.130.可以配

置相同类型的多个服务器，如多个WEB服务器，多个E-mail服务器等。具体配置文件如下：

```
Interface fastethernet 0/0 Ip address 192.168.100.1 255.255.255.0! - 定义本地端口IP地址 Ip nat inside! - 定义为本地端口 Interface fastethernet 0/1 Ip address 202.99.160.129 255.255.255.252! - 定义广域网端口IP地址 Ip nat outside! - 定义为广域网端口 Access-list 1 permit 192.168.100.0 0.0.0.255! - 定义本地访问列表 Ip nat pool multiip 202.99.160.130 202.99.160.134 netmask 255.255.255.248! - 定义multiip地址池的IP范围 Ip nat inside source list 1 mullitip overload Ip nat inside source static tcp 192.168.1.11 80 202.99.16.130 80 Ip nat inside source static tcp 192.168.1.12 80 202.99.16.131 80 Ip nat inside source static tcp 192.168.1.13 80 202.99.16.132 80! - 将80端口映射为192.168.1.11 ~ 13的80端口（WEB1-3） Ip nat inside source static tcp 192.168.1.14 21 202.99.16.130 21 Ip nat inside source static tcp 192.168.1.15 21 202.99.16.131 21! - 将21端口映射为192.168.1.14 ~ 15的21端口（FTP1-2） Ip nat inside source static tcp 192.168.1.16 25 202.99.16.133 25 Ip nat inside source static tcp 192.168.1.16 110 202.99.16.133 110 Ip nat inside source static tcp 192.168.1.17 25 202.99.16.134 25 Ip nat inside source static tcp 192.168.1.17 110 202.99.16.134 110! - 将25和110端口映射为192.168.1.16 ~ 17的25和110端口（mail1-2）
```

在企业中因根据具体的网络环境与条件选择相应的组合方式。在许多FTP网站考虑到服务器性能和Internet连接带宽的占用问题，都限制同一IP地址的多个进程访问。该选择动态地址转换 端口复用地址转换。在很多时候，服务器即为企业内部客户提供网络服务，同时又要为Internet中的用户提供访问服务，选择静态

地址转换 端口复用地址转换是一种比较好的方案。当ISP只提供一个合法 IP地址，网络又没有特殊需要，使用端口复用地址转换技术，既能节省了IP地址的同时，又可有效的保护网络内部计算机。除了在连接和隐藏方面的应用，NAT设备能实现负载均衡。DNS系列服务器群中多个IP地址公用一个域名，由于IP客户端会缓冲DNS/IP地址解析，从而使其后续申请延迟达到同一个IP地址，在一定程度上减弱了DNS系列服务器的作用。而基于NAT的负载均衡方案，可以有效的避免这类问题。NAT设备是把需要负载的平衡的多个IP地址翻译成一个公用的IP地址，每个TCP连接被NAT送到一个IP地址，使后续的TCP连接被NAT送到下一个IP地址来实现真正的负载均衡。除此之外，NAT技术能够在用户更改ISP时避免了对内部网络进行重新编址，同时减少用户网络接入的费用等问题。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com