IPtables中SNAT、DNAT和MASQUERADE的区别   
  
IPtables中可以灵活的做各种网络地址转换（NAT）  
　　网络地址转换主要有两种：SNAT和DNAT  
  
　　SNAT是source network address translation的缩写，即源地址目标转换  
　　比如，多个PC机使用ADSL路由器共享上网，每个PC机都配置了内网IP  
　　PC机访问外部网络的时候，路由器将数据包的报头中的源地址替换成路由器的ip  
　　当外部网络的服务器比如网站web服务器接到访问请求的时候  
　　他的日志记录下来的是路由器的ip地址，而不是pc机的内网ip  
　　这是因为，这个服务器收到的数据包的报头里边的“源地址”，已经被替换了  
　　所以叫做SNAT，基于源地址的地址转换  
  
　　DNAT是destination network address translation的缩写  
　　即目标网络地址转换  
　　典型的应用是，有个web服务器放在内网配置内网ip，前端有个防火墙配置公网ip  
　　互联网上的访问者使用公网ip来访问这个网站  
　　当访问的时候，客户端发出一个数据包  
　　这个数据包的报头里边，目标地址写的是防火墙的公网ip  
　　防火墙会把这个数据包的报头改写一次，将目标地址改写成web服务器的内网ip  
　　然后再把这个数据包发送到内网的web服务器上  
　　这样，数据包就穿透了防火墙，并从公网ip变成了一个对内网地址的访问了  
　　即DNAT，基于目标的网络地址转换  
  
　　MASQUERADE，地址伪装，在iptables中有着和SNAT相近的效果，但也有一些区别  
　　但使用SNAT的时候，出口ip的地址范围可以是一个，也可以是多个，例如：  
　　如下命令表示把所有10.8.0.0网段的数据包SNAT成192.168.5.3的ip然后发出去  
　　iptables -t nat -A POSTROUTING -s 10.8.0.0/255.255.255.0 -o eth0 -j SNAT --to-source 192.168.5.3  
　　如下命令表示把所有10.8.0.0网段的数据包SNAT成192.168.5.3/192.168.5.4/192.168.5.5等几个ip然后发出去  
　　iptables -t nat -A POSTROUTING -s 10.8.0.0/255.255.255.0 -o eth0 -j SNAT --to-source 192.168.5.3-192.168.5.5  
　　这就是SNAT的使用方法，即可以NAT成一个地址，也可以NAT成多个地址  
但是，对于SNAT，不管是几个地址，必须明确的指定要SNAT的ip  
　　假如当前系统用的是ADSL动态拨号方式，那么每次拨号，出口ip192.168.5.3都会改变  
　　而且改变的幅度很大，不一定是192.168.5.3到192.168.5.5范围内的地址  
　　这个时候如果按照现在的方式来配置iptables就会出现问题了  
　　因为每次拨号后，服务器地址都会变化，而iptables规则内的ip是不会随着自动变化的  
　　每次地址变化后都必须手工修改一次iptables，把规则里边的固定ip改成新的ip  
　　这样是非常不好用的  
　　MASQUERADE就是针对这种场景而设计的，他的作用是，从服务器的网卡上，自动获取当前ip地址来做NAT  
　　比如下边的命令：  
　　iptables -t nat -A POSTROUTING -s 10.8.0.0/255.255.255.0 -o eth0 -j MASQUERADE  
　　如此配置的话，不用指定SNAT的目标ip了  
　　不管现在eth0的出口获得了怎样的动态ip，MASQUERADE会自动读取eth0现在的ip地址然后做SNAT出去  
　　这样就实现了很好的动态SNAT地址转换