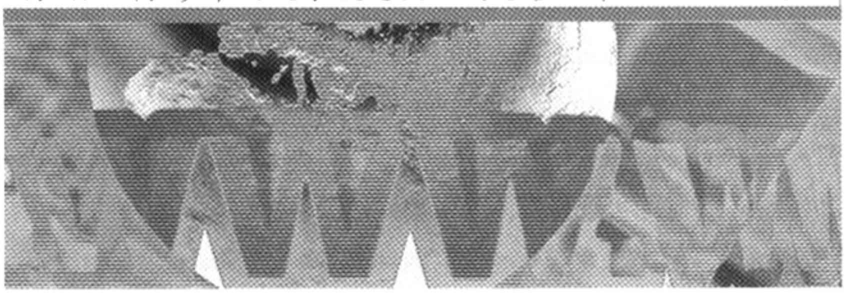
网络地址翻译(NAT)技术及应用

杨 林 （长沙中南大学铁道校区网络管理中心 410075）



摘要：本文介绍了网络地址翻译（NAT）技术的概念、应用和配置方法，并以Cisco路由器为例做了介绍。

关键词：IP NAT ACCESS-LIST 路由器

1 引言

随着Internet的日益普及和飞速发展，上网已经成为一种流行趋势，连入Internet的局域网数量日益增长，造成目前Internet IP地址严重短缺，为每一台访问Internet的网络工作站分配一个全球唯一的IP全局地址几乎是不可能的。为了解决这个问题，出现了许多解决方案，网络地址翻译(NAT)技术是较为突出的一种解决方案。用一句简单的话来描述NAT，它就是在内部网络的私有地址需要与外部网络通信时，利用1个或几个IP地址来实现局域网上的所有主机都可以访问Internet。使用NAT技术时，好像NAT设备根本就不存在，面向用户这个技术完全是透明的。

2 网络地址翻译（NAT）的相关概念

(1) 内部本地地址（Inside Local Address）：分配给内部网络中的工作站保留的IP地址。

(2) 内部合法地址（Inside Global Address）：对外部进入IP通信时，代表一个或多个内部本地地址的合法Internet IP地址。

(3) 外部本地地址（Outside Local Address）：对于内部网络工作站可见的外部主机地址，可以使用保留的IP地址。

(4) 外部合法地址（Outside Global Address）：分配给外部网络主机的IP地址，该地址由全局可达地址或网络空间中获取。

(5) 简单翻译入口（Simple Translation Entry）：映射一个IP地址到另外一个IP地址的入口列表。

(6) 扩展翻译入口（Extended Translation Entry）：映射一个IP地址和端口号到另外一个IP地址和端口号的入口列表。

3 网络地址翻译（NAT）的主要特性

3.1 静态地址翻译

用户可以在本地和全局地址之间建立一个一对一的映射，这个需要网络管理员定义。如果内部网络中有E-Mail或FTP服务器等可以为外部用户使用的服务器，这些服务器IP地址必须采用静态地址转换，以便外部用可以使用这些服务。

3.2 动态地址翻译

用户可以在本地和全局地址之间建立一个动态的映射，这时必须建立一个全局地址池，由路由器从合法地址池中动态地选择一个未使用的地址对内部保留地址进行转换。

3.3 复用动态地址翻译

首先是一种动态地址翻译，但是它可以允许多个内部保留地址共用一个内部合法地址，路由器内部会利用上层的如TCP或UDP端口号来唯一标识某台IP主机，是一对多的关系。当申请到少量IP地址，但是却经常同时有多于合法地址个数的用户访问外部网络时，这种翻译极为有用。

4 NAT在路由器中的配置

4.1 静态地址翻译基本配置步骤

(1) 在内部保留地址与外部合法地址之间建立静态地址翻译

ip nat inside source static 内部保留地址 内部合法地址

例如：ip nat inside source static 10.10.10.1 202.197.40.80

(2) 指定连接网络的内部端口

在端口配置状态下 ip nat inside

例如：interface Ethernet 0

ip address 10.10.10.1 255.255.255.0

ip nat inside

(3) 指定连接外部网络的端口

在端口配置状态下 ip nat outside

例如：interface serial 0

ip address 10.10.10.1 255.255.255.0

ip nat outside

4.2 动态地址翻译基本配置步骤

(1) 在全局配置模式下，定义内部合法地址池

ip nat pool 地址池名称 起始IP地址 终止IP地址 [掩码]

例如：ip nat pool nat1 202.197.33.1 202.197.33.26 255.255.255.0

(2) 在全局配置模式下，定义一个标准的访问表，允许哪些内部本地地址进行动态翻译

access-list 标识号 permit 源地址 通配符

例如：access-list 1 permit 202.197.40.80 0.0.0.255

(3) 建立动态源地址翻译

ip nat inside source list 访问列表标识号 pool 地址池名

例如：ip nat inside source list 1 pool nat1

(4) 说明内部接口

在端口配置状态下 ip nat inside

例如：interface Ethernet 0

ip address 10.10.10.1 255.255.255.0

ip nat inside

(5) 说明外部接口

在端口配置状态下 ip nat outside

例如：interface serial 0

ip address 10.10.10.1 255.255.255.0

ip nat outside

4.3 复用动态地址翻译配置步骤

(1) 在全局配置模式下，定义内部合法地址池

ip nat pool 地址池名称 起始IP地址 终止IP地址 [掩码]

(2) 在全局配置模式下，定义一个标准的访问表，允许哪些内部本地地址进行动态翻译

(3) 在全局配置模式下，建立复用动态地址翻译

ip nat inside source list 访问列表标识号 pool 地址池名 overload

例如：ip nat inside source list 1 pool nat1 overload

(4) 说明内部接口

在端口配置状态下 ip nat inside

(5) 说明外部接口

在端口配置状态下 ip nat outside

5 NAT的具体应用

图1 网络结构图

如图1所示，我们给出一个配置实例，图中的路由器具有一个局域网接口和一个广域网接口。广域网接口利用DDN与Internet连接，内部局域网有一台主机，使用内部保留地址（10.10.10.1）。

路由器配置如下（有些其他无关信息省去）：

.....

!

ip nat pool NET 202.197.40.20 202.197.40.30 netmask 255.255.255.0

ip nat pool OVL 202.197.40.50 202.197.40.50 netmask 255.255.255.0

//这里定义IP地址池，地址复用地址池只用了一个IP地址

!

ip nat inside source list 1 pool NET

//将访问控制列表与地址池对应，上面是动态地址翻译的例子

!

ip nat inside source list 2 pool OVL

//将访问控制列表与地址池对应，上面是复用动态地址翻译的例子

!

ip nat inside source static 10.10.10.1 202.197.40.10

//将访问控制列表与地址池对应，上面是静态地址翻译的例子

!

interface Ethernet 0

（下转第66页）

(上接第 26 页)

```
    ip address 10.10.10.2 255.255.255.0
    ip nat inside      //定义为内部端口
    !
interface Serial 0
ip address 202.197.40.1 255.255.255.0
ip nat outside     //定义为网络的外部端口
!
ip route 0.0.0.0 0.0.0.0 serial 0 // 定义缺省路由
!
access-list 1 permit 10.10.10.0 0.0.0.255
access-list 2 permit 10.10.20.0 0.0.0.255
//内部网访问地址表，指出内部网络中可以进行地址翻译的网段，分别定义对应不同的地址池
!
... ...
end ■
```


参考文献

1 Bassam Halabi，因特网的路由选择技术，北京电子工业出版社。

2 Egevang R.Francis P,The IP Network Address Tranclator (NAT).RFC1631,1994(5)。

3 Tanenbaum AS,Computer Network Third Edition. Pretice-Hall,1996。