

CISCONAT 配置

一、NAT简介

NAT(Network Address Translation) 的功能，就是指在一个网络内部，根据需要可以随意自定义的 IP 地址，而不需要经过申请。在网络内部，各计算机间通过内部的 IP 地址进行通讯。而当内部的计算机要与外部 internet 网络进行通讯时，具有 NAT功能的设备（比如：路由器）负责将其内部的 IP 地址转换为合法的 IP 地址（即经过申请的 IP 地址）进行通信。

二、NAT 的应用环境：

情况 1：一个企业不想让外部网络用户知道自己的网络内部结构，可以通过 NAT将内部网络与外部 Internet 隔离开，则外部用户根本不知道通过 NAT设置的内部 IP 地址。

情况 2：一个企业申请的合法 Internet IP 地址很少，而内部网络用户很多。可以通过 NAT功能实现多个用户同时公用一个合法 IP 与外部 Internet 进行通信。

三、设置 NAT所需路由器的硬件配置和软件配置：

设置 NAT功能的路由器至少要有一个内部端口（ Inside ），一个外部端口（ Outside ）。内部端口连接的网络用户使用的是内部 IP 地址。内部端口可以为任意一个路由器端口。外部端口连接的是外部的网络，如 Internet 。外部端口可以为路由器上的任意端口。

设置 NAT功能的路由器的 IOS 应支持 NAT功能（本文事例所用路

由器为 C isco2501 , 其 IOS 为 11.2 版本以上支持 NAT功能)。

四、关于 NAT的几个概念：

内部本地地址 (Inside local address)：分配给内部网络中的计算机的内部 IP 地址。

内部合法地址 (Inside global address)：对外进入 IP 通信时，代表一个或多个内部本地地址的合法 IP 地址。需要申请才可取得的 IP 地址。

五、NAT的设置方法：

NAT设置可以分为静态地址转换、动态地址转换、复用动态地址转换。

1、静态地址转换适用的环境

静态地址转换将内部本地地址与内部合法地址进行一对一的转换，且需要指定和哪个合法地址进行转换。如果内部网络有 E-mail 服务器或 FTP服务器等可以为外部用户提供的服务，这些服务器的 IP 地址必须采用静态地址转换，以便外部用户可以使用这些服务。

静态地址转换基本配置步骤：

(1)、在内部本地地址与内部合法地址之间建立静态地址转换。

在全局设置状态下输入：

```
ip nat inside source static      内部本地地址  内部合法地  
址
```

(2)、指定连接网络的内部端口 在端口设置状态下输入：

```
ip nat inside
```

(3) 指定连接外部网络的外部端口 在端口设置状态下输入：

```
ip nat outside
```

注：可以根据实际需要定义多个内部端口及多个外部端口。

实例 1：

本实例实现静态 NAT地址转换功能。将 2501 的以太网口作为内部端口，同步端口 0 作为外部端口。其中 10.1.1.2 ， 10.1.1.3 ， 10.1.1.4 的内部本地地址采用静态地址转换。其内部合法地址分别对应为 192.1.1.2 ， 192.1.1.3 ， 192.1.1.4 。

路由器 2501 的配置：

Current configuration ：

```
version 11.3
```

```
no service password-encryption
```

```
hostname 2501
```

```
ip nat inside source static 10.1.1.2 192.1.1.2
```

```
ip nat inside source static 10.1.1.3 192.1.1.3
```

```
ip nat inside source static 10.1.1.4 192.1.1.4
```

```
interface Ethernet0
```

```
ip address 10.1.1.1 255.255.255.0
```

```
ip nat inside
```

```
interface Serial0
```

```
ip address 192.1.1.1 255.255.255.0
```

```
ip nat outside
```

```
no ip mroute-cache

bandwidth 2000

no fair-queue

clockrate 2000000

interface Serial1

no ip address

shutdown

no ip classless

ip route 0.0.0.0 0.0.0.0 Serial0

line con 0

line aux 0

line vty 0 4

password cisco

end
```

配置完成后可以用以下语句进行查看：

```
show ip nat statistics

show ip nat translations
```

2、动态地址转换适用的环境：

动态地址转换也是将本地地址与内部合法地址一对一的转换，但是动态地址转换是从内部合法地址池中动态地选择一个未使用的地址对内部本地地址进行转换。

动态地址转换基本配置步骤：

(1) 在全局设置模式下，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  子网掩  
码
```

其中地址池名称可以任意设定。

(2) 在全局设置模式下，定义一个标准的 access-list 规则以允许哪些内部地址可以进行动态地址转换。

```
Access-list    标号 permit    源地址  通配符
```

其中标号为 1-99 之间的整数。

(3) 在全局设置模式下，将由 access-list 指定的内部本地地址与指定的内部合法地址池进行地址转换。

```
ip nat inside source list          访问列表标号 pool  内部合法地  
址池名字
```

(4) 指定与内部网络相连的内部端口在端口设置状态下：

```
ip nat inside
```

(5) 指定与外部网络相连的外部端口

```
Ip nat outside
```

实例 2：

本实例中硬件配置同上，运用了动态 NAT地址转换功能。将 2501 的以太口作为内部端口，同步端口 0 作为外部端口。其中 10.1.1.0 网段采用动态地址转换。对应内部合法地址为 192.1.1.2~192.1.1.10

Current configuration :

version 11.3

no service password-encryption

hostname 2501

ip nat pool aaa 192.1.1.2 192.1.1.10 netmask 255.255.255.0

ip nat inside source list 1 pool aaa

interface Ethernet0

ip address 10.1.1.1 255.255.255.0

ip nat inside

interface Serial0

ip address 192.1.1.1 255.255.255.0

ip nat outside

no ip mroute-cache

bandwidth 2000

no fair-queue

clockrate 2000000

interface Serial1

no ip address

shutdown

no ip classless

ip route 0.0.0.0 0.0.0.0 Serial0

access-list 1 permit 10.1.1.0 0.0.0.255

line con 0

line aux 0

```
line vty 0 4  
  
password cisco  
  
end
```

3、复用动态地址转换适用的环境：

复用动态地址转换首先是一种动态地址转换，但是它可以允许多个内部本地地址共用一个内部合法地址。只申请到少量 IP 地址但却经常同时有多于合法地址个数的用户上外部网络的情况，这种转换极为有用。

注意：当多个用户同时使用一个 IP 地址，外部网络通过路由器内部利用上层的如 TCP或 UDP端口号等唯一标识某台计算机。

复用动态地址转换配置步骤：

在全局设置模式下，定义内部合法地址池

```
ip nat pool 地址池名字 起始 IP 地址 终止 IP 地址 子网掩码
```

其中地址池名字可以任意设定。

在全局设置模式下，定义一个标准的 access-list 规则以允许哪些内部本地地址可以进行动态地址转换。

```
access-list 标号 permit 源地址 通配符
```

其中标号为 1 - 99 之间的整数。

在全局设置模式下，设置在内部的本地地址与内部合法 IP 地址间建立复用动态地址转换。

```
ip nat inside source list 访问列表标号 pool 内部合法地址池名字 overload
```

在端口设置状态下，指定与内部网络相连的内部端口

```
ip nat inside
```

在端口设置状态下，指定与外部网络相连的外部端口

```
ip nat outside
```

实例：应用了复用动态 NAT地址转换功能。将 2501 的以太网口作为内部端口，同步端口 0 作为外部端口。 10.1.1.0 网段采用复用动态地址转换。假设企业只申请了一个合法的 IP 地址 192.1.1.1 。

2501 的配置

Current configuration :

```
version 11.3
```

```
no service password-encryption
```

```
hostname 2501
```

```
ip nat pool bbb 192.1.1.1 192.1.1.1 netmask 255.255.255.0
```

```
ip nat inside source list 1 pool bbb overload
```

```
interface Ethernet0
```

```
ip address 10.1.1.1 255.255.255.0
```

```
ip nat inside
```

```
interface Serial0
```

```
ip address 192.1.1.1 255.255.255.0
```

```
ip nat outside
```

```
no ip mroute-cache
```

```
bandwidth 2000
```


no fair-queue

clockrate 2000000

interface Serial1

no ip address

shutdown

no ip classless

ip route 0.0.0.0 0.0.0.0 Serial0

access-list 1 permit 10.1.1.0 0.0.0.255

line con 0

line aux 0

line vty 0 4

password cisco

end