

实验 28 配置动态 NAT

【实验名称】

配置动态 NAT。

【实验目的】

配置网络地址变换，为私有地址的用户提供到外部网络的资源的访问。

【背景描述】

某 IT 企业因业务扩展，需要升级网络，他们选择 172.16.1.0/24 作为私有地址，并用 NAT 来处理和外部网络的连接。

【需求分析】

ISP 提供商给 IT 企业的一段公共 IP 地址的地址段为 200.1.1.200~100.1.1.210，需要内网使用这段地址去访问 Internet，考虑到包括安全在内的诸多因素，公司希望对外部隐藏内部网络。

【实验拓扑】

实验的拓扑图，如图 28-1 所示。

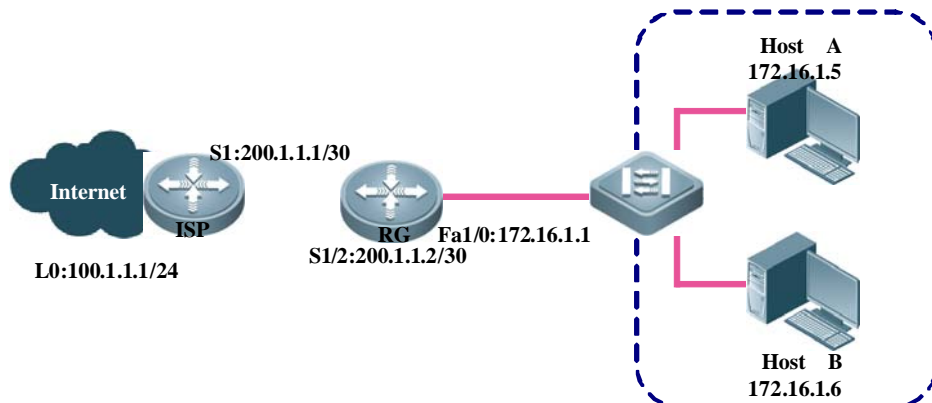


图 28-1

【实验设备】

路由器 2 台
交换机 1 台
PC 机 2 台

【预备知识】

路由器基本配置知识、IP 路由知识、NAT 原理。

【实验原理】

在路由器上定义内网与外网接口，利用 NAT 地址池实现内网对外网的访问，并把内网隐藏起来。

【实验步骤】

步骤 1 在路由器上配置 IP 路由选择和 IP 地址。

```
RG#config t
RG(config)#interface serial 1/2
RG(config-if) #ip address 200.1.1.2 255.255.255.252
RG(config-if) #clock rate 64000
RG(config)#interface FastEthernet 1/0
RG(config-if) #ip address 172.16.1.1 255.255.255.0
RG(config)#ip route 0.0.0.0 0.0.0.0 serial 1/2
```

步骤 2 定义一个 IP 访问列表。

```
RG(config)#access-list 10 permit 172.16.1.0 0.0.0.255
```

步骤 3 配置静态 NAT。

```
RG(config)# ip nat pool ruijie 200.1.1.200 200.1.1.210 prefix-length 24
RG(config)#ip nat inside source list 10 pool ruijie
```

步骤 4 指定一个内部接口和一个外部接口。

```
RG(config)#interface serial 1/2
RG(config-if)#ip nat outside
RG(config)#interface FastEthernet 1/0
RG(config-if)#ip nat inside
```

步骤 5 验证测试。

用两台主机 telnet 登录远程主机 100.1.1.1 来测试 NAT 的转换。

```
C:\>telnet 100.1.1.1
User Access Verification
Password:
[root@lab ~]# telnet 100.1.1.1
Trying 100.1.1.1...
Connected to 100.1.1.1 (100.1.1.1).
Escape character is '^]'.
User Access Verification
Password:
```

```
RG#sh ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 200.1.1.201:1174    172.16.1.6:1174   100.1.1.1:23       100.1.1.1:23
tcp 200.1.1.204:1026    172.16.1.5:1026   100.1.1.1:23       100.1.1.1:23
RG#debug ip nat
RG#NAT: [A] pk 0x03f553ec s 172.16.1.6->200.1.1.201:1176 [4082]
NAT: [B] pk 0x03f56d44 d 200.1.1.201->172.16.1.6:1174 [363]
NAT: [A] pk 0x03f560a4 s 172.16.1.6->200.1.1.201:1174 [4083]
NAT: [B] pk 0x03f4d044 d 200.1.1.201->172.16.1.6:1174 [364]
NAT: [A] pk 0x03f50620 s 172.16.1.6->200.1.1.201:1174 [4084]
NAT: [B] pk 0x03f4f968 d 200.1.1.201->172.16.1.6:1174 [365]
```

```

NAT: [A] pk 0x03f55580 s 172.16.1.6->200.1.1.201:1174 [4085]
.....
NAT: [A] pk 0x03f54d84 s 172.16.1.5->200.1.1.204:1026 [52337]
NAT: [B] pk 0x03f56238 d 200.1.1.204->172.16.1.5:1026 [372]
NAT: [A] pk 0x03f56888 s 172.16.1.5->200.1.1.204:1026 [52339]
NAT: [A] pk 0x03f56560 s 172.16.1.5->200.1.1.204:1026 [52341]
NAT: [B] pk 0x03f566f4 d 200.1.1.204->172.16.1.5:1026 [373]
NAT: [A] pk 0x03f5b6d4 s 172.16.1.5->200.1.1.204:1026 [52343]
NAT: [B] pk 0x03f51c50 d 200.1.1.204->172.16.1.5:1026 [374]

```

【参考配置】

```

RG#sh run
Building configuration...
Current configuration : 789 bytes
version 8.4 (building 15)
hostname RG
enable secret 5 $1$yLhr$s2r9y5lxyE7yFA12
access-list 10 permit 172.16.1.0 0.0.0.255
no service password-encryption
!
interface serial 1/2
 ip nat outside
 ip address 200.1.1.2 255.255.255.252
 clock rate 64000
!
interface FastEthernet 1/0
 ip nat inside
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet 1/1
 duplex auto
 speed auto
!
interface Null 0
 ip nat pool ruijie 200.1.1.200 200.1.1.210 prefix-length 24
 ip nat inside source list 10 pool ruijie
 ip route 0.0.0.0 0.0.0.0 serial 1/2
 line con 0
 line aux 0
 line vty 0
 login
 password 7 093d12
 line vty 1 4
 login
!

```