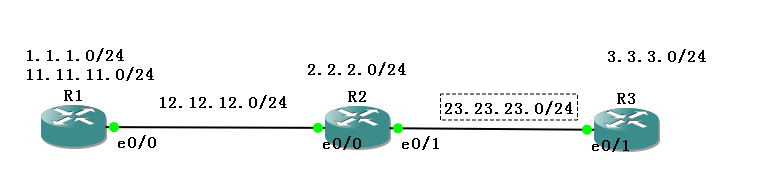
ACL,NAT,DHCP未完成版（gns模拟器）

该实验最后一步有问题，过两天改善后再出完整版——JK

**实验出现问题：为什么设置完了pat ,R7还能ping通R5，R4??**

ACL

实验拓扑：



实验要求：

1.1.1.1 🡪3.3.3.3 不通

11.11.11.11🡪3.3.3.3 通

2.2.2.2🡪3.3.3.3 通

实验步骤：

步骤一：基本配置

R1：

R1#conf t

R1(config)#int lo0

R1(config-if)#ip add 1.1.1.1 255.255.255.0

R1(config-if)#int lo1

R1(config-if)#ip add 11.11.11.11 255.255.255.0

R1(config-if)#int e0/0

R1(config-if)#ip add 12.12.12.1 255.255.255.0

R1(config-if)#no shut

R1(config-if)#end

R2：

R2#CONF T

R2(config)#int lo0

R2(config-if)#ip add 2.2.2.2 255.255.255.0

R2(config-if)#no shut

R2(config-if)#int e0/0

R2(config-if)#ip add 12.12.12.2 255.255.255.0

R2(config-if)#no shut

R2(config)#int e0/1

R2(config-if)#ip add 23.23.23.2 255.255.255.0

R2(config-if)#no shut

R2(config-if)#end

R3:

R3#conf t

R3(config)#int e0/1

R3(config-if)#ip add 23.23.23.3 255.255.255.0

R3(config-if)#no shut

R3(config-if)#int lo0

R3(config-if)#ip add 3.3.3.3 255.255.255.0

R3(config-if)#no shut

R3(config-if)#end

步骤二：静态路由设置

R1(config)#ip route 0.0.0.0 0.0.0.0 e0/0 12.12.12.2 //目标ip不在路由表中时就走e0/0到R2

R2(config)#ip route 1.1.1.0 255.255.255.0 e0/0 12.12.12.1

R2(config)#ip route 11.11.11.0 255.255.255.0 e0/0 12.12.12.1

R2(config)#ip route 3.3.3.0 255.255.255.0 e0/1 23.23.23.3

R3(config)#ip route 0.0.0.0 0.0.0.0 e0/1 23.23.23.2

//直连网络本身就存在在路由表中，不用配静态

检验：

R1#ping 3.3.3.3

R3#ping 1.1.1.1

步骤三：

编写ACL语句：

R2#conf t

R2(config)#ip access-list extended IT //命名acl叫IT（扩展acl）

R2(config-ext-nacl)#deny ip 1.1.1.1 0.0.0.0 3.3.3.3 0.0.0.0

R2(config-ext-nacl)#permit ip host 2.2.2.2 host 3.3.3.3

R2(config-ext-nacl)#permit ip host 11.11.11.11 host 3.3.3.3

检验：

R2#show access-list

Extended IP access list IT

10 deny ip host 1.1.1.1 host 3.3.3.3

20 permit ip host 2.2.2.2 host 3.3.3.3

30 permit ip host 11.11.11.11 host 3.3.3.3

步骤四：

接口下引用ACL

R2#conf t

R2(config)#int e0/1

R2(config-if)#ip access-group IT out

R2(config-if)#end

检验：

R1#ping 3.3.3.3 so 1.1.1.1 不通 //修改源就是该标签，同下

R1#ping 3.3.3.3 so 11.11.11.11 通

R2#ping 3.3.3.3 通

R2#ping 1.1.1.1 通

!!补充

自反ACL

实验拓扑：同上（R1——R2为内网，R3为外网）

实验要求：

内网到外网 OK

外网到内网 NO

实验步骤：

R2#conf t

R2(config)#ip access-list extended inside

R2(config-ext-nacl)#permit ip any any reflect CHINA

//抓取内网去向外网的流量产生临时条目 放入 CHINA

R2(config)#ip access-list extended outside

R2(config-ext-nacl)#evaluate CHINA

//将所有源自外网流量做匹配

R2(config)#int e0/0

R2(config-if)#ip access-group inside in

R2(config-if)#int e0/1

R2(config-if)#ip access-group outside in

现象：

11.11.11.11🡪3.3.3.3 可通

3.3.3.3🡪11.11.11.11 不可通

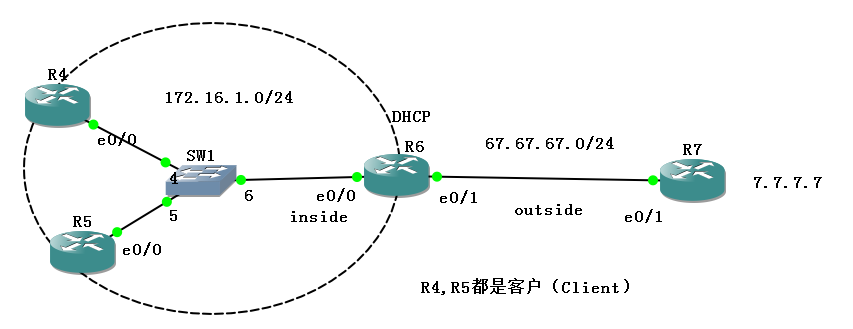
2.2.2.2🡪3.3.3.3 不通

3.3.3.3🡪2.2.2.2 不通

DHCP

——最后一步含有PAT（有疑问）

实验拓扑：



实验步骤：

步骤一：基本配置

R4#conf t

R4(config)#no ip routing

R4(config)#ip default-gateway 172.16.1.1

R4(config)#int e0/0

R4(config-if)#ip add dhcp

R5#conf t

R5(config)#no ip routing

R5(config)#ip default-gateway 172.16.1.1

R5(config)#int e0/0

R5(config-if)#ip add dhcp

R6#conf t

R6(config)#int e0/0

R6(config-if)#ip add 172.16.1.1 255.255.255.0

R6(config-if)#no shut

R6(config-if)#int e0/1

R6(config-if)#ip add 67.67.67.6 255.255.255.0

R6(config-if)#no shut

R7#conf t

R7(config)#int e0/1

R7(config-if)#ip add 67.67.67.7 255.255.255.0

R7(config-if)#no shut

R7(config-if)#int lo0

R7(config-if)#ip add 7.7.7.7 255.255.255.0

R7(config-if)#end

步骤二：R6，R7设置静态路由

R6(config)#ip route 7.7.7.0 255.255.255.0 e0/1 67.67.67.7

R7(config)#ip route 0.0.0.0 0.0.0.0 e0/1 67.67.67.6

步骤三：配置地址池

R6(config)#ip dhcp pool CHINA-Telecom

R6(dhcp-config)#network 172.16.1.0 /24

R6(dhcp-config)#default-router 172.16.1.1

R6(dhcp-config)#dns-server 172.16.1.1

R6(dhcp-config)#lease 7

R6(dhcp-config)#exit

R6(config)#ip dhcp excluded-address 172.16.1.1

R5#conf t

R5(config)#int e0/0

R5(config-if)#no shut

R4#conf t

R4(config)#int e0/0

R4(config-if)#no shut

检验：

R4#show ip int br

Interface IP-Address OK? Method Status Protocol

Ethernet0/0 172.16.1.2 YES DHCP up up

Ethernet0/1 unassigned YES unset administratively down down

Ethernet0/2 unassigned YES unset administratively down down

Ethernet0/3 unassigned YES unset administratively down down

R5#show ip int br

Interface IP-Address OK? Method Status Protocol

Ethernet0/0 172.16.1.3 YES DHCP up up

Ethernet0/1 unassigned YES unset administratively down down

Ethernet0/2 unassigned YES unset administratively down down

Ethernet0/3 unassigned YES unset administratively down down

R4：ping 7.7.7.7 通

R5：ping 7.7.7.7 通

R7：ping 172.16.1.2通

ping 172.16.1.3通

步骤四：

方法一：R6设置自反ACL 保证 172.16.1.0/24网段内部网络安全

R6#conf t

R6(config)#ip access-list extend inside

R6(config-ext-nacl)#permit ip any any reflect Greatwall

R6(config-ext-nacl)#exit

R6(config)#ip access-list extend outside

R6(config-ext-nacl)#evaluate Greatwall

R6(config-ext-nacl)#exit

R6(config)#int e0/0

R6(config-if)#ip access-group inside in

R6(config-if)#int e0/1

R6(config-if)#ip access-group outside in

R6(config-if)#exit

检验：

R4：ping 7.7.7.7 通

R5：ping 7.7.7.7 通

R7：ping 172.16.1.2不通

ping 172.16.1.3不通

方法二：R6设置PAT（port address translation 端口地址转换）

多对一的转换：多个内网地址对应到一个公网地址(有问题，亟待解决)

R6(config)#int e0/0

R6(config-if)#ip nat inside

R6(config-if)#int e0/1

R6(config-if)#ip nat outside

R6(config)#access-list 99 per 172.16.1.0 0.0.0.255

R6(config)#ip nat inside source list 99 interface e0/1 overload