

南开大学

网络技术与应用课程实验报告

实验 6: NAT 的配置



学院: 网络空间安全学院

专业: 信息安全-法学

学号: 2111954

姓名: 许积君

目录

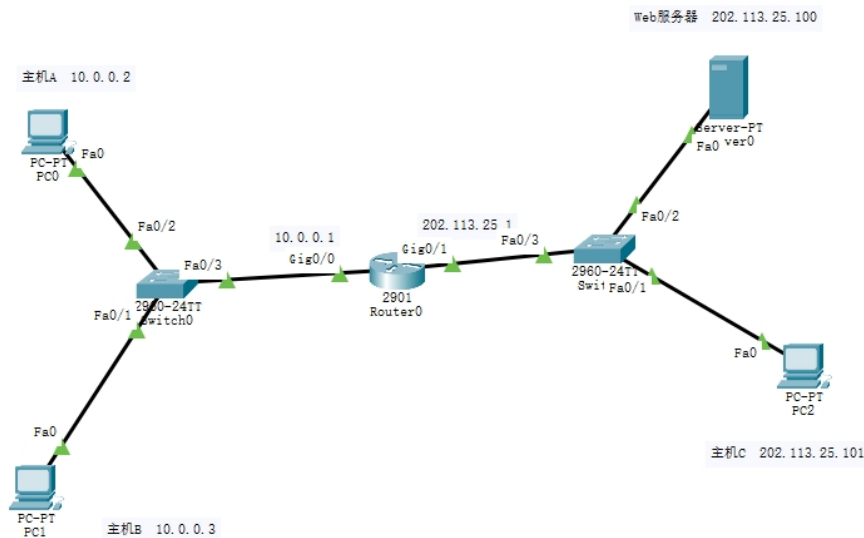
一、 相关知识	1
二、 仿真环境下的 NAT 服务器配置	1
(一) 网络配置	1
(二) 结果验证	3
(三) 模拟	3
三、 内部网络中放置 Web 服务器	4
(一) 结果验证	4
(二) 模拟	5

一、 相关知识

- 1. NAT 概念：NAT (Network Address Translation) 又称为网络地址转换，用于实现私有网络和公有网络的互访
- 2. NAT 的工作原理：NAT 用来将内网地址和端口号转换成合法的公网地址和端口号，建立一个会话，与公网主机进行通信。NAT 外部的主机无法主动跟位于 NAT 内部的主机通信，NAT 内部主机想要通信，必须主动和公网的一个 IP 通信，路由器负责建立一个映射关系，从而实现数据的转发
- 3. 路由器的表项
 - (a) 路由表：数据包通过目的 IP 查路由表转发
 - (b) ACL 访问控制列表：过滤数据包
 - (c) NAT 转换表：内网到外网转换源 IP 地址，外网到内网转换目的 IP 地址

二、 仿真环境下的 NAT 服务器配置

(一) 网络配置



主机 IP 如下图所示

主机号	IP 地址	掩码	默认路由
主机 A	10.0.0.2	255.0.0.0	10.0.0.1
主机 B	10.0.0.3	255.0.0.0	10.0.0.1
主机 C	202.113.25.101	255.255.255.0	-
外网服务器	202.113.25.100	255.255.255.0	-

路由器配置如下图所示

路由器号	端口	IP 地址	掩码
Router0	0/0	10.0.0.1	255.0.0.0
Router0	0/1	202.113.25.1	255.255.255.0

路由器 NAT 具体配置命令如下:

```
Router(config)#ip nat pool myNATPool 202.113.25.1 202.113.25.100 netmask
255.255.255.0
Router(config)#access-list 6 permit 10.0.0.0 0.255.255.255
Router(config)#ip nat inside source list 6 pool myNATPool overload
Router(config)#interface gig0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface gig0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
```

转换表如下图:

```
show ip nat translations ——显示 NAT 转换
show ip nat statistics ——显示 NAT 统计信息
```

```
Router#show ip nat statistics
Total translations: 1 (0 static, 1 dynamic, 1 extended)
Outside Interfaces: GigabitEthernet0/1
Inside Interfaces: GigabitEthernet0/0
Hits: 17 Misses: 12
Expired translations: 11
Dynamic mappings:
-- Inside Source
access-list 6 pool myNATPool refCount 1
pool myNATPool: netmask 255.255.255.0
start 202.113.25.1 end 202.113.25.100
type generic, total addresses 100 , allocated 1 (1%), misses 0
Router#
tcp 202.113.25.1:1025 10.0.0.2:1025 202.113.25.100:80 202.113.25.100:80

Router#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 202.113.25.1:18 10.0.0.2:18 202.113.25.101:18 202.113.25.101:18
icmp 202.113.25.1:19 10.0.0.2:19 202.113.25.101:19 202.113.25.101:19
icmp 202.113.25.1:20 10.0.0.2:20 202.113.25.101:20 202.113.25.101:20
icmp 202.113.25.1:24 10.0.0.2:24 202.113.25.101:24 202.113.25.101:24
icmp 202.113.25.1:25 10.0.0.2:25 202.113.25.101:25 202.113.25.101:25
icmp 202.113.25.1:26 10.0.0.2:26 202.113.25.101:26 202.113.25.101:26
icmp 202.113.25.1:30 10.0.0.2:30 202.113.25.100:30 202.113.25.100:30
icmp 202.113.25.1:31 10.0.0.2:31 202.113.25.100:31 202.113.25.100:31
icmp 202.113.25.1:32 10.0.0.2:32 202.113.25.100:32 202.113.25.100:32
tcp 202.113.25.1:1025 10.0.0.2:1025 202.113.25.100:80 202.113.25.100:80
```

(二) 结果验证

```
Pinging 202.113.25.100 with 32 bytes of data:

Reply from 202.113.25.100: bytes=32 time<1ms TTL=127
Reply from 202.113.25.100: bytes=32 time<1ms TTL=127
Reply from 202.113.25.100: bytes=32 time<1ms TTL=127
Reply from 202.113.25.100: bytes=32 time<1ms TTL=127

Ping statistics for 202.113.25.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

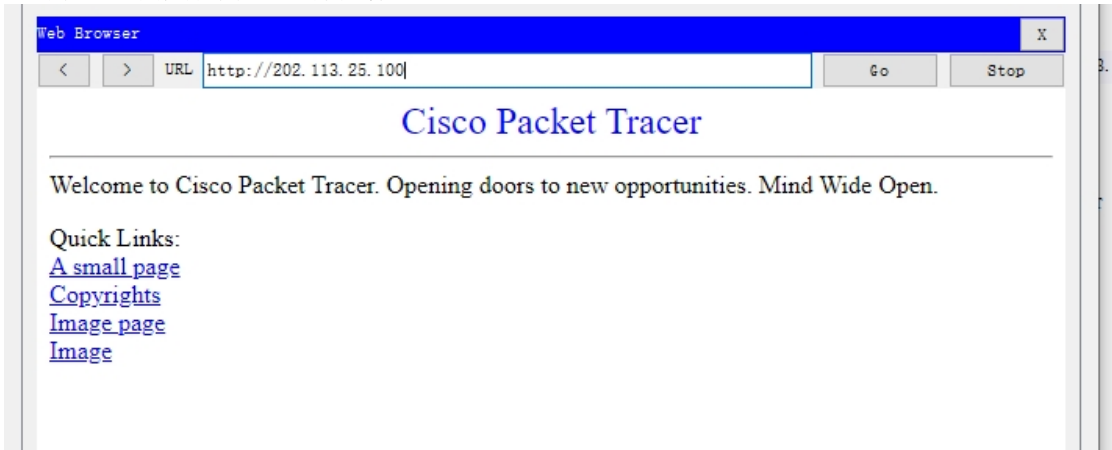
C:\>tr
C:\>tracert 202.113.25.100

Tracing route to 202.113.25.100 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms    10.0.0.1
  1  0 ms    0 ms    0 ms    202.113.25.100

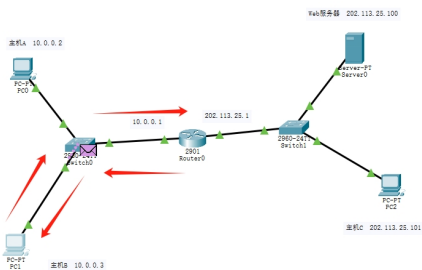
Trace complete.
```

也可以通过网页访问 Web 服务器



(三) 模拟

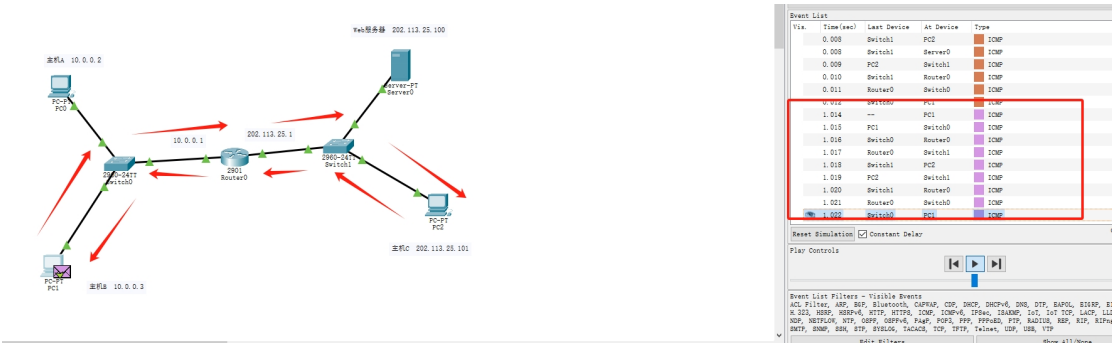
分为两部分，第一部分为 ARP 包的发送



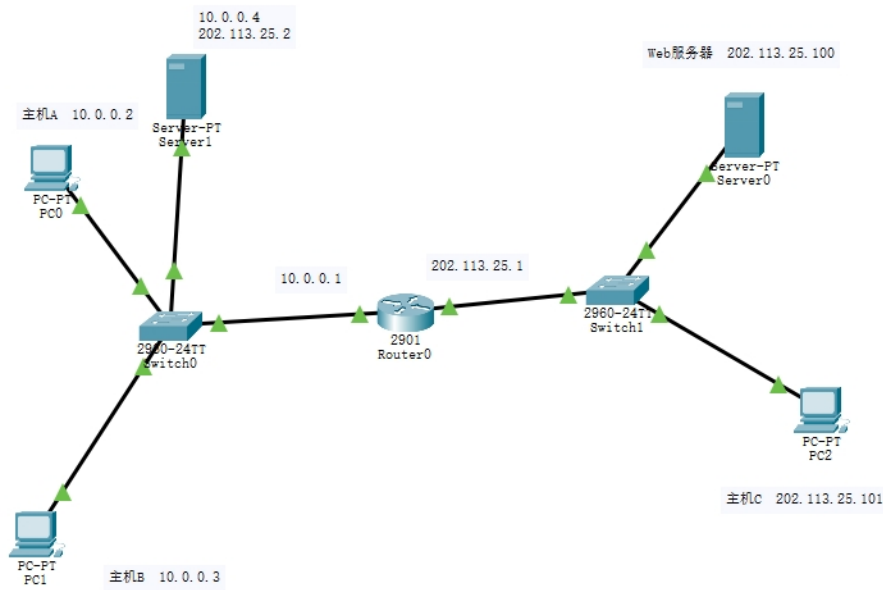
ARP传递过程

Time	Time(s)	Last Device	At Device	Type
0.000	--	PC1	PC1	ARP
0.001	PC1	Switch0	ARP	
0.002	Switch0	Router0	ARP	
0.003	Router0	Switch1	ARP	
0.004	Switch1	Server0	ARP	
0.005	PC1	Switch0	ICMP	
0.006	Switch0	Router0	ICMP	
0.007	Router0	Switch1	ICMP	
0.008	Switch1	Server0	ICMP	
0.009	PC1	Switch0	ICMP	
0.010	Switch0	Router0	ICMP	

第二部分才是真正的数据包的发送，主要分析数据包到达路由器时的信息，具体如下：当数据包从内部网络转到外部网络时，设备查找其 NAT 表以进行必要的转换。当该数据包与内部源列表匹配，则对源本地 IP 地址进行转换，从而实现内外主机的连接



三、 内部网络中放置 Web 服务器

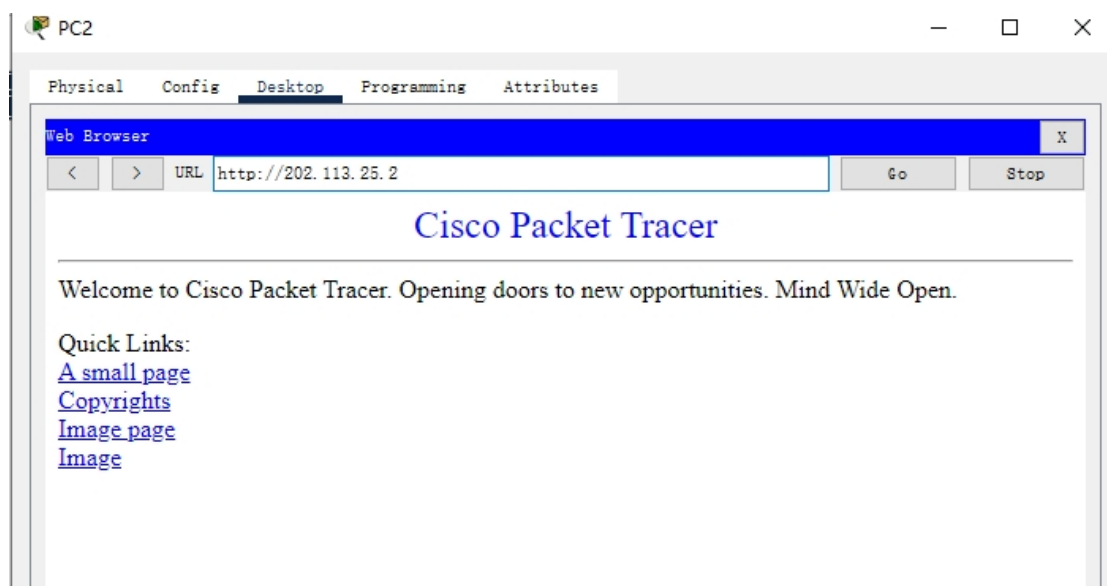


将内部 Web 服务器的 IP 设为 10.0.0.4，掩码为 255.0.0.0，对应外网地址为 202.113.25.2
在路由器中通过添加静态 NAT 的方式使其联通

```
ip nat inside source static tcp 10.0.0.4 80 202.113.25.2 80
```

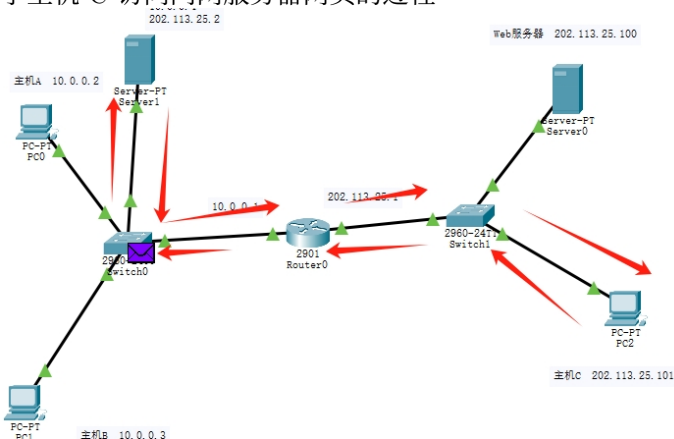
(一) 结果验证

通过主机 C 访问内网 Web 服务器



(二) 模拟

本次模拟了主机 C 访问内网服务器网页的过程



可以看到在刚开始打开网页的时候，网页并没有任何数据，直到第一个通信建立完成，开启 HTTP 协议进行通信，当关闭网页时，又会传输报文安全断开连接

1. 三次握手建立连接
2. HTTP 协议进行通信
3. 四次挥手断开连接

Vis.	Time(sec)	Last Device	At Device	Type
	0.003	Router0	Switch0	TCP
	0.004	Switch0	Server1	TCP
	0.005	Server1	Switch0	TCP
	0.006	Switch0	Router0	TCP
	0.007	Router0	Switch1	TCP
	0.008	Switch1	PC2	TCP
	0.008	--	PC2	HTTP
	0.009	PC2	Switch1	TCP
	0.009	--	PC2	HTTP
	0.010	PC2	Switch1	HTTP
	0.010	Switch1	Router0	TCP
	0.011	Switch1	Router0	HTTP
	0.011	Router0	Switch0	TCP
	0.012	Router0	Switch0	HTTP
	0.012	Switch0	Server1	TCP
	0.013	Switch0	Server1	HTTP
	0.014	Server1	Switch0	HTTP
	0.015	Switch0	Router0	HTTP
	0.016	Router0	Switch1	HTTP
	0.017	Switch1	PC2	HTTP
	0.017	--	PC2	TCP
	0.018	PC2	Switch1	TCP