



南开大学
Nankai University

实验6：IPv6组网与NAT的配置

- 姓名：陈睿颖
- 学号：2013544
- 专业：计算机科学与技术

1. 实验内容

1.1 仿真环境下的NAT服务器配置

在仿真环境下完成NAT服务器的配置实验，要求如下：

1. 学习路由器的NAT配置过程。
2. 组建由NAT连接的内网和外网。
3. 测试网络的连通性，观察网络地址映射表。
4. 在仿真环境的“模拟”方式中观察IP数据报在互联网中的传递过程，并对IP数据报的地址进行分析。

1.2 在仿真环境下完成如下实验

将内部网络中放置一台Web服务器，请设置NAT服务器，使外部主机能够顺利使用该Web服务。

1.3 IPv6组网实验（选做）

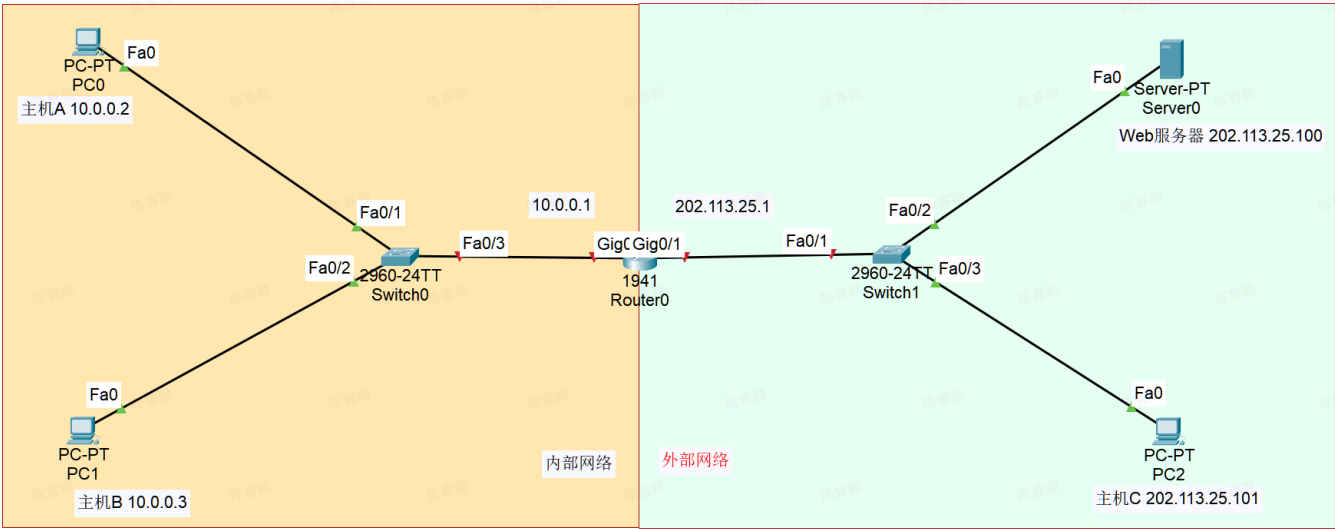
IPv6组网与配置在虚拟仿真环境下进行，要求如下：

- 1. 能对IPv6地址段进行合理划分。
- 2. 能正确配置路由器的IP地址和路由表。
- 3. 能利用手工或自动获取方式正确配置主机的IPv6地址。
- 4. 通过网络连通性测试。
- 5. 在仿真环境的“模拟”方式中观察IPv6数据报传递过程。

2. 实验准备

2.1 NAT配置

实验拓扑图如图所示：



各设备的IP地址、掩码信息如下表：

设备/接口	IP地址	掩码
内网		

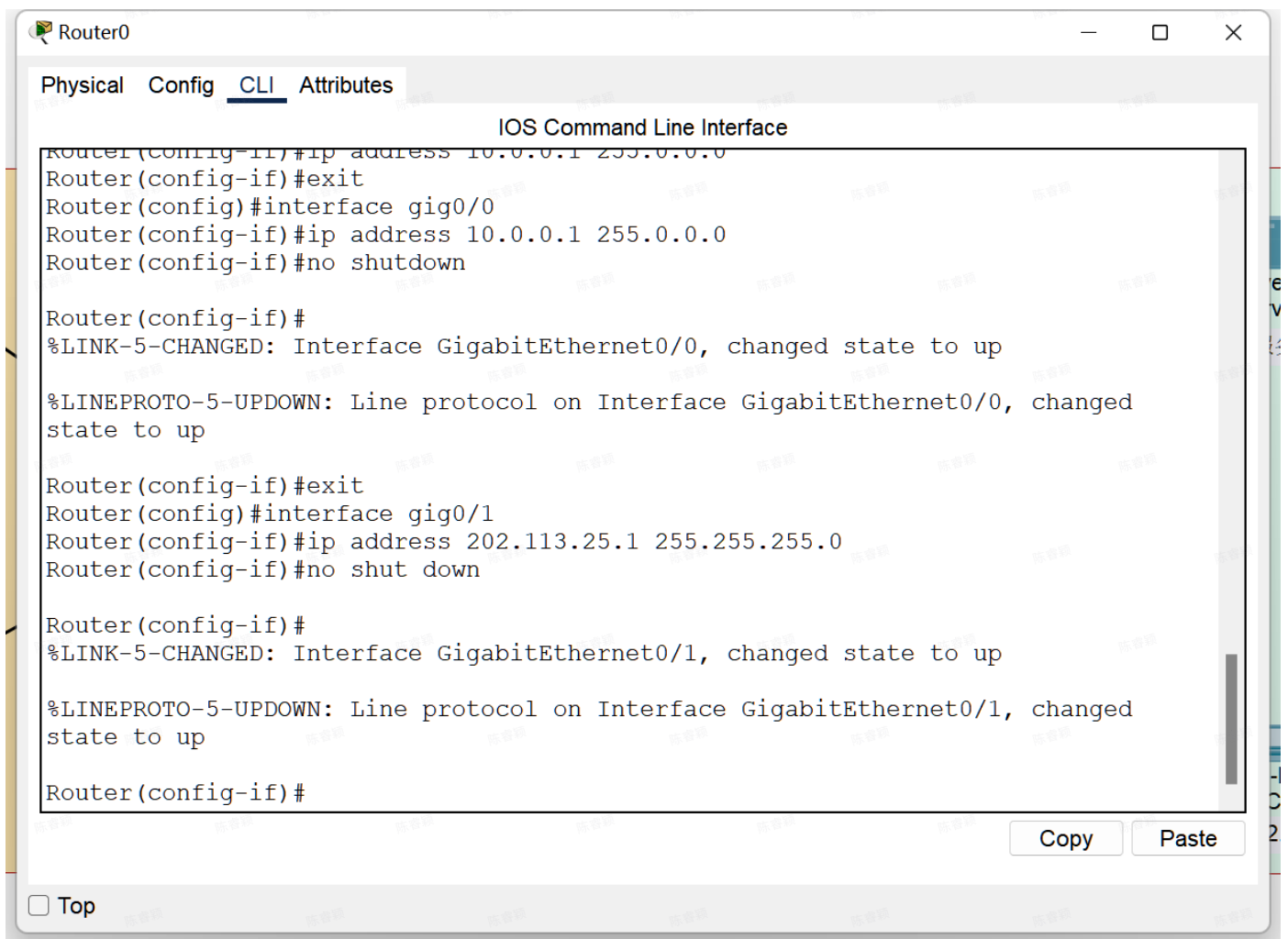
主机A（PC0）	10.0.0.2	255.0.0.0
主机B（PC1）	10.0.0.3	255.0.0.0
默认路由：10.0.0.1		
外网		
Web服务器	202.113.25.100	255.255.255.0
主机C（PC2）	202.113.25.101	
路由器		
Gig0/0	10.0.0.1	255.0.0.0
Gig0/1	202.113.25.1	255.255.255.0

3. 实验过程

3.1 NAT配置实验

3.1.1 路由器Router0配置

- 首先配置路由器的IP地址：



2. 在全局模式下，指定NAT使用的全局IP地址的范围，使用如下命令建立NAT地址池：

```
1 Router(config) #ip nat pool myNATPool 202.113.25.1 202.113.25.10 netmask 255.255.255.0
```

起始地址：202.113.25.1 结束地址：202.113.25.10 掩码：255.255.255.0

3. 设置内部网络使用的IP地址范围，在全局模式下使用如下命令建立标准访问控制列表：

```
1 Router(config)#access-list 6 permit 10.0.0.0 0.255.255.255
```

0.255.255.255为通配符，与掩码正好相反

4. 将使用的地址池与访问控制列表进行关联

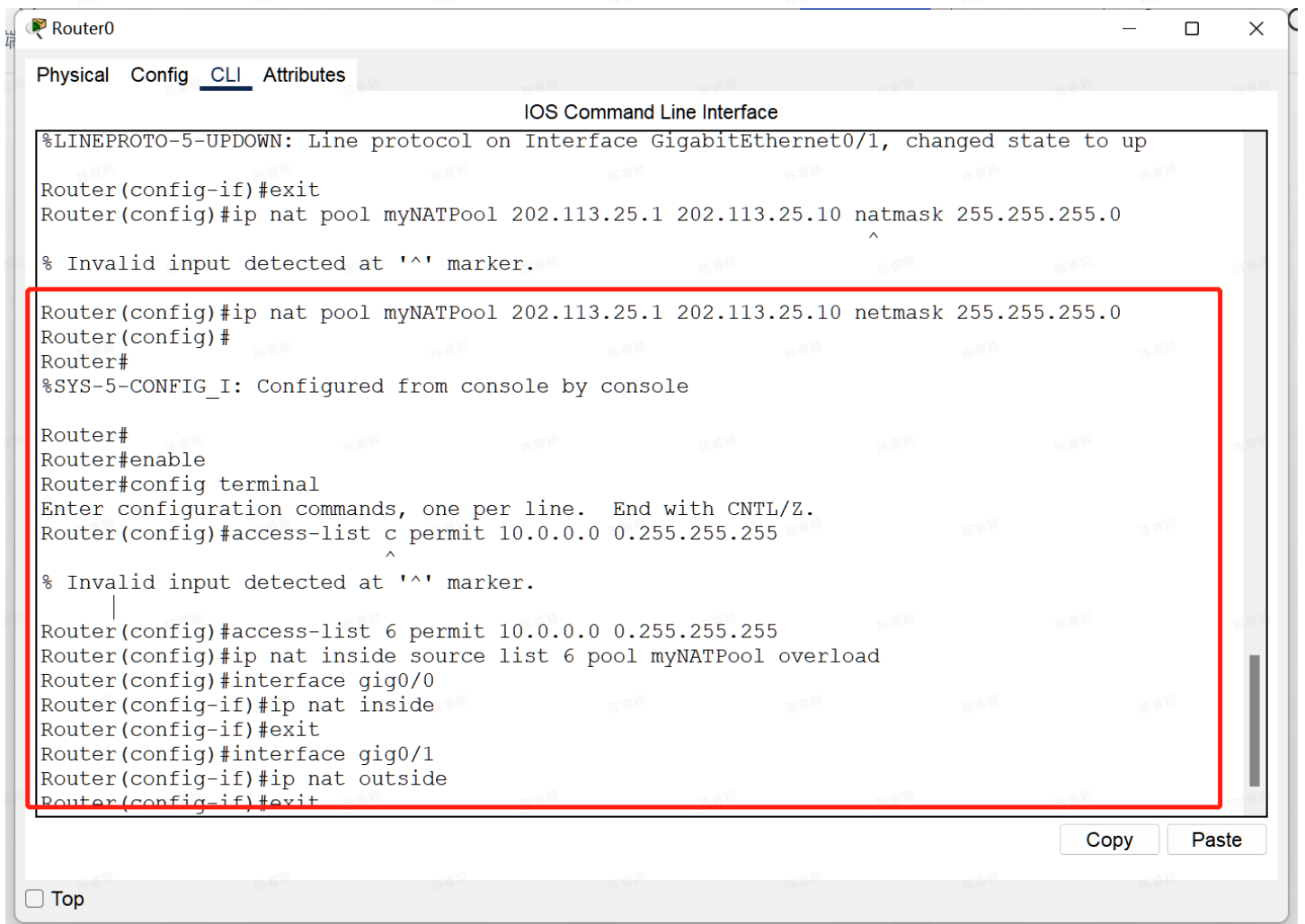
```
1 Router(config)#ip nat inside source list 6 pool myNATPool overload
```

overload意为进行端口转换NAPT

5. 在接口配置模式下，指定连接外部网络和内部网络的接口：

```
1 Router(config)#interface gig0/0
2 Router(config-if)#ip nat inside
3 Router(config-if)#exit
4 Router(config)#interface gig0/1
5 Router(config-if)#ip nat outside
6 Router(config-if)#exit
```

以上所有配置如图：

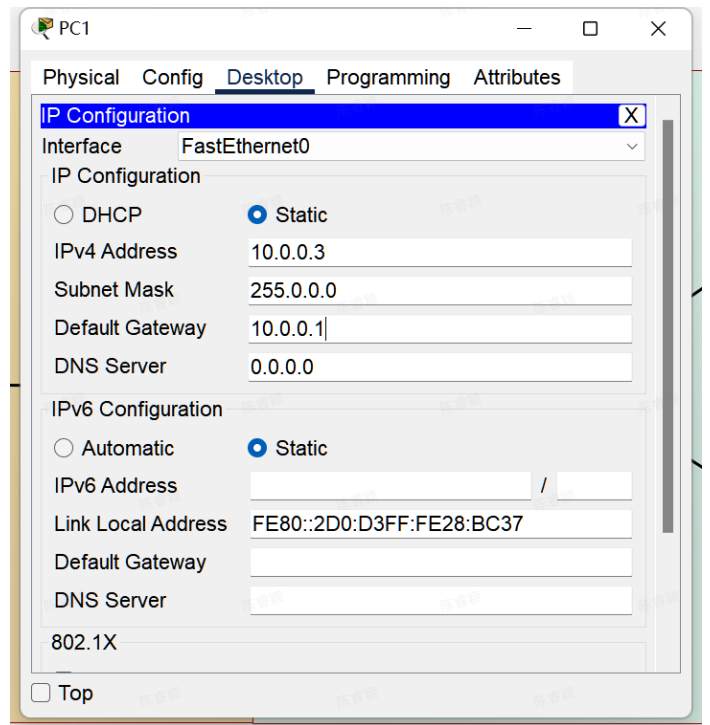
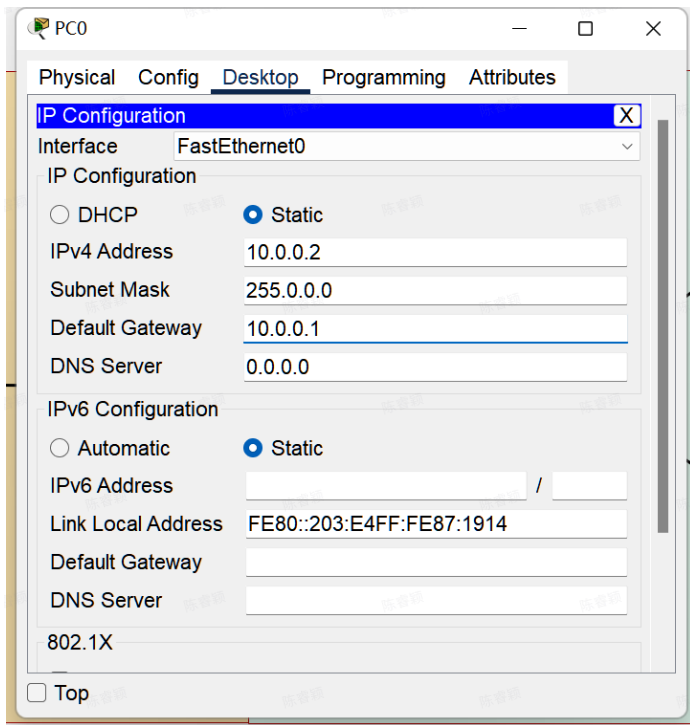


3.1.2 主机IP地址配置

1. 内部网络：

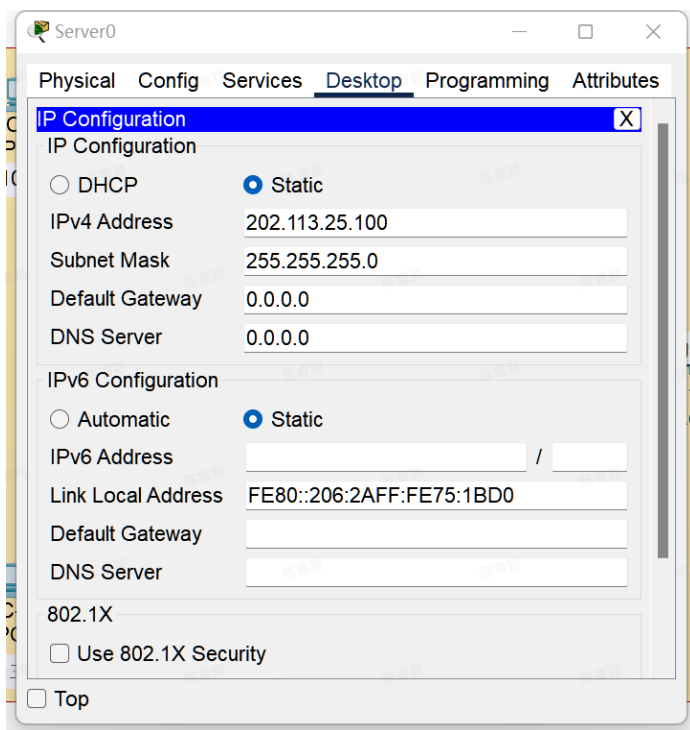
PC0:

PC1:

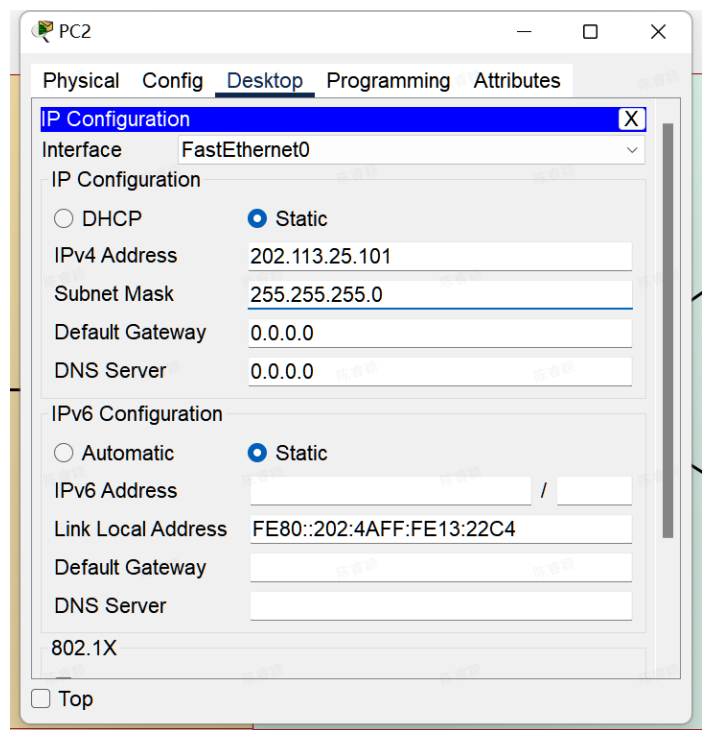


2. 外部网络：

Web服务器：



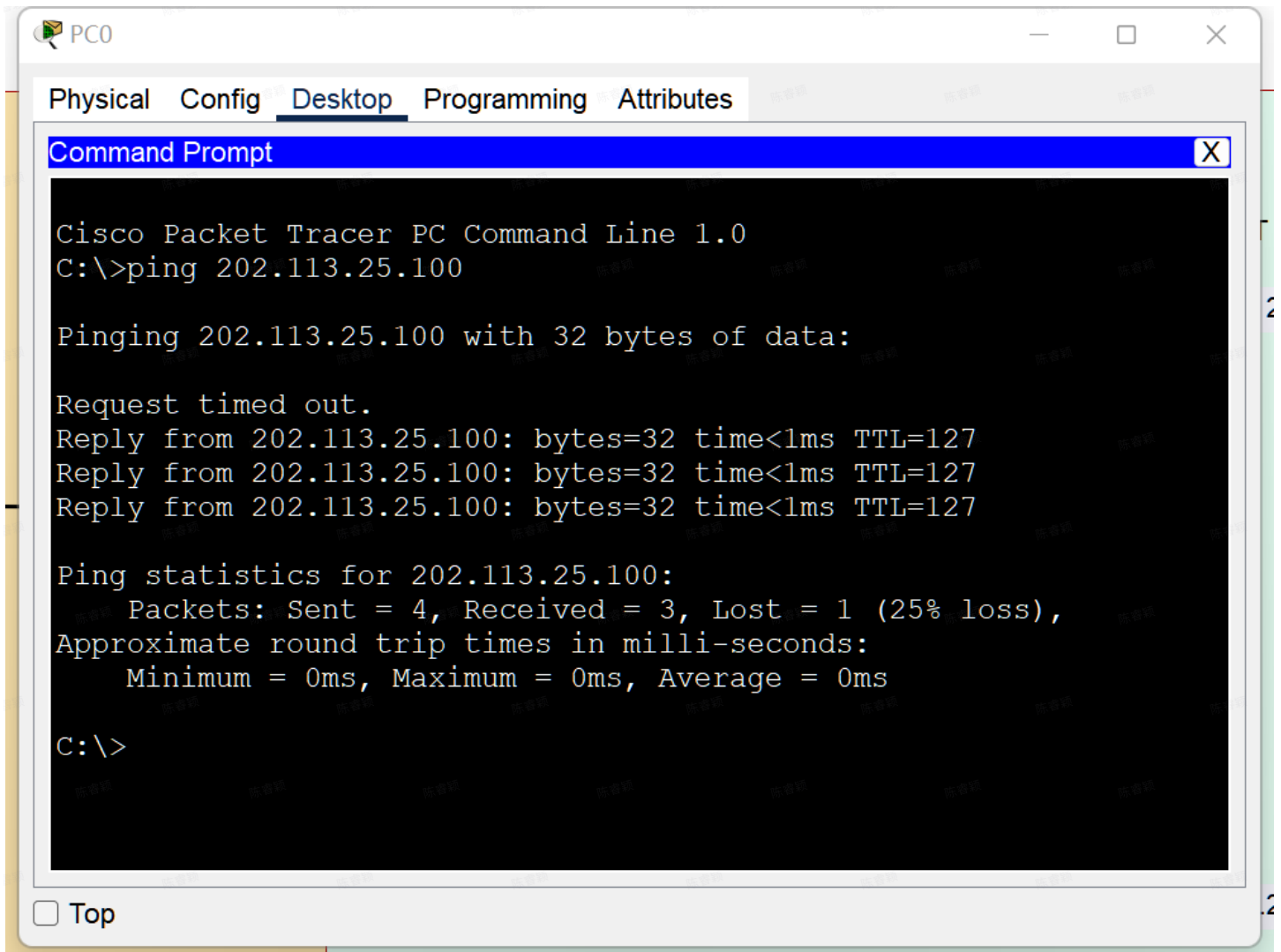
PC2：



3.1.3 测试网络的连通性

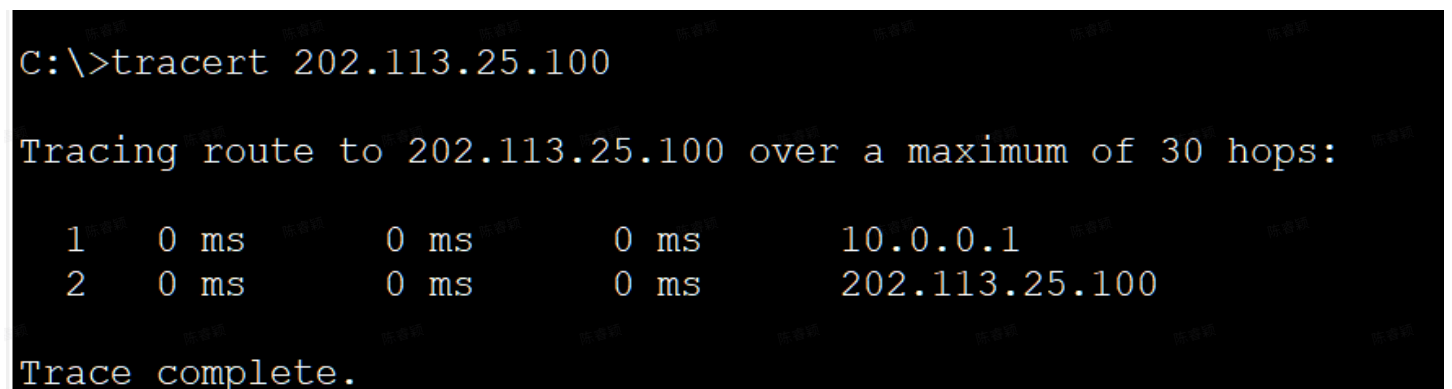
在PC0上使用ping命令：

```
1 ping 202.113.25.100
```



再使用tracert命令：

```
1 tracert 202.113.25.100
```

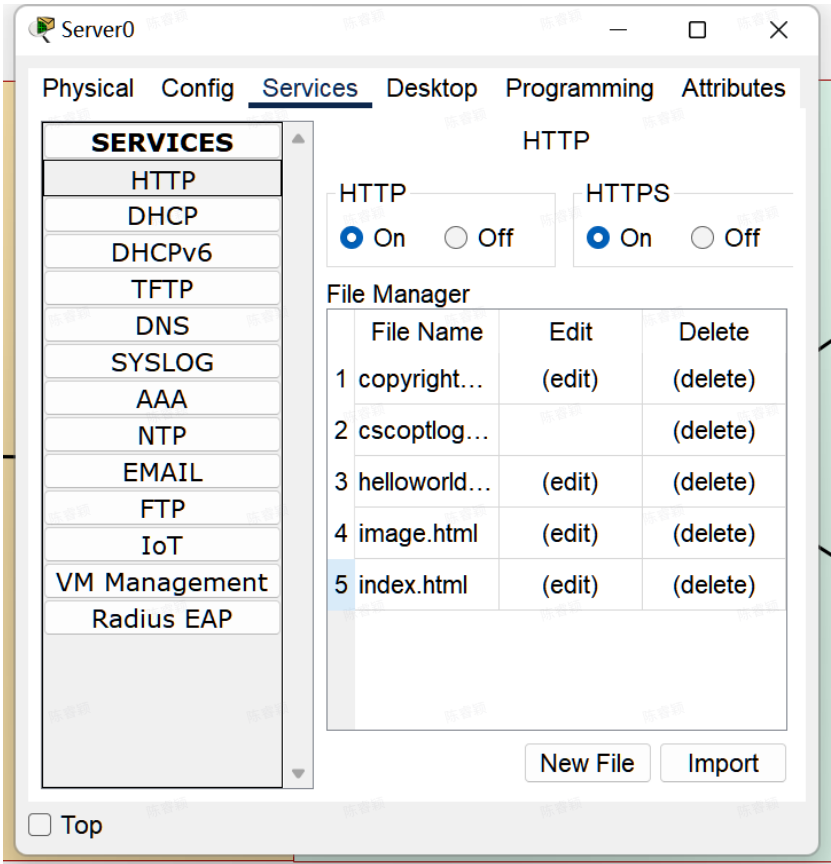


可以看到主机A向Web服务器发送数据报时，先经过了10.0.0.1接口，最终到达Web服务器。

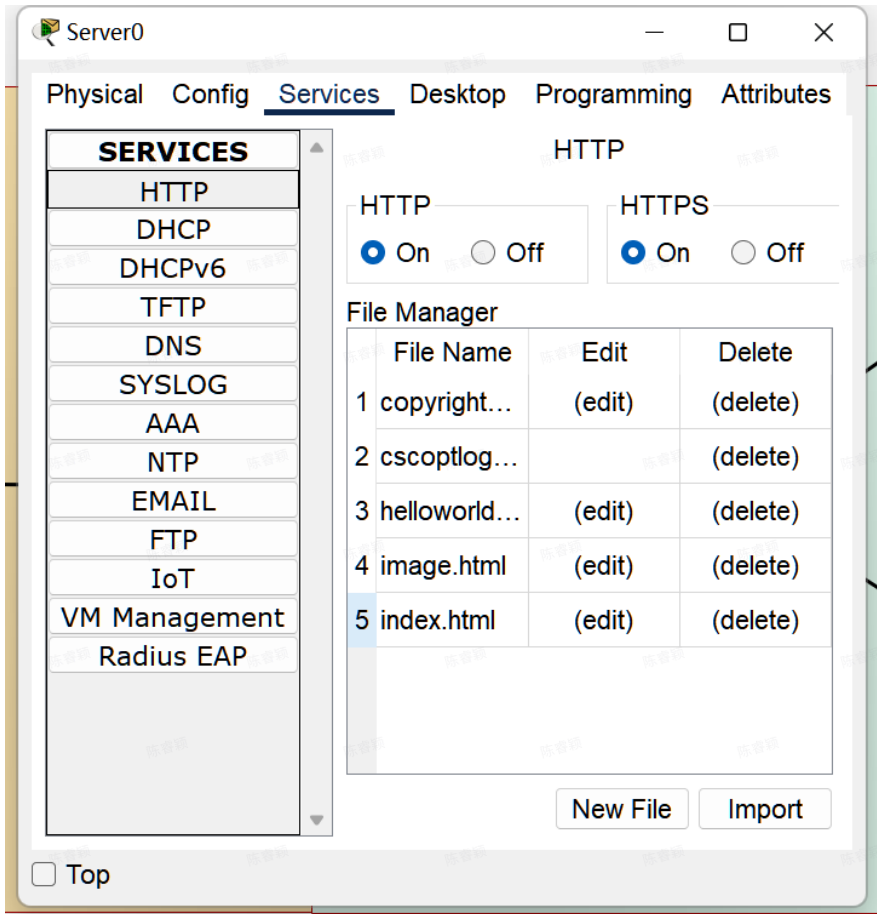
3.1.4 使用Web服务

为了更清晰地查看到NAT的工作情况，启用Web服务器上的Web服务：

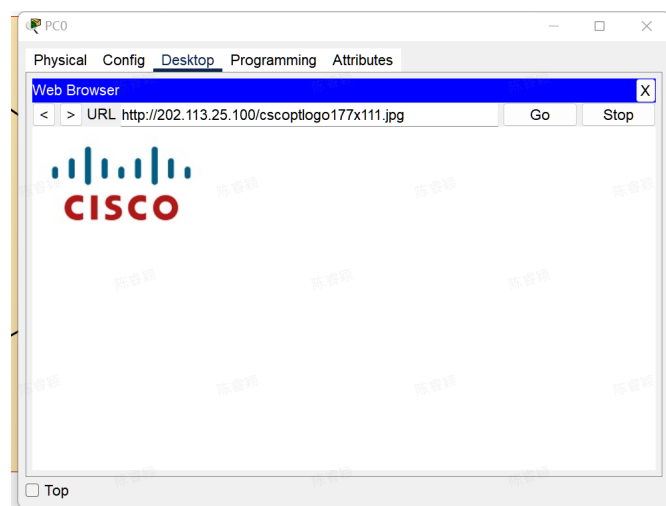
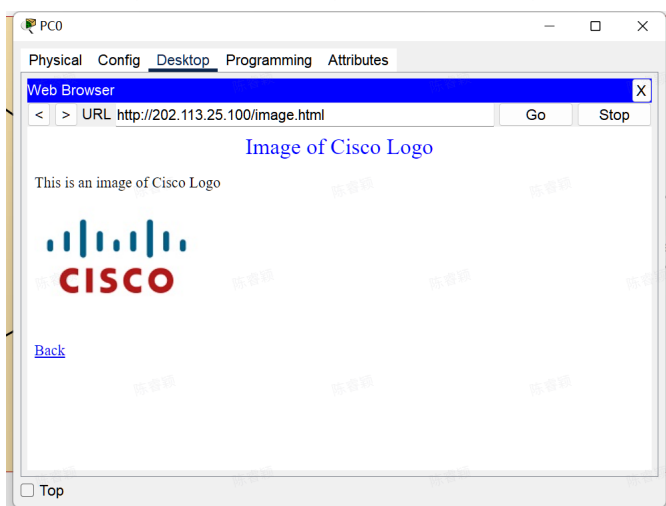
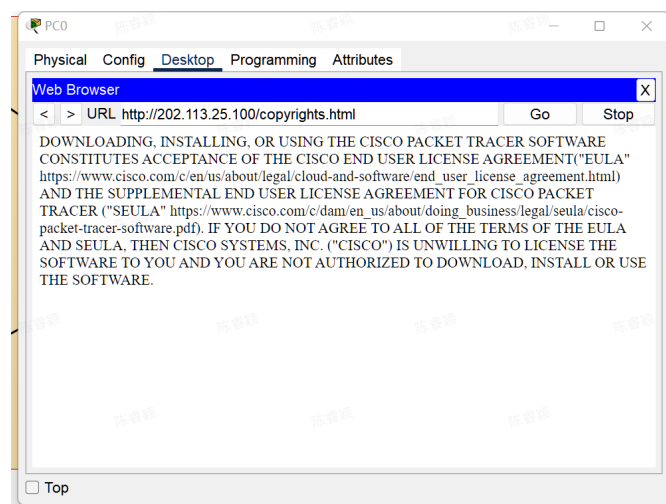
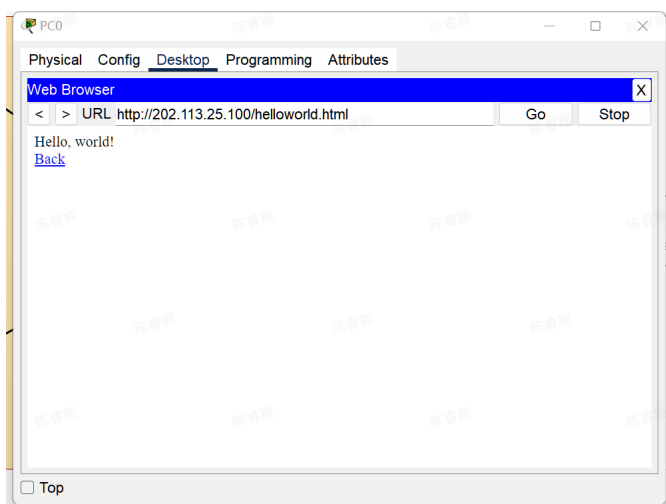
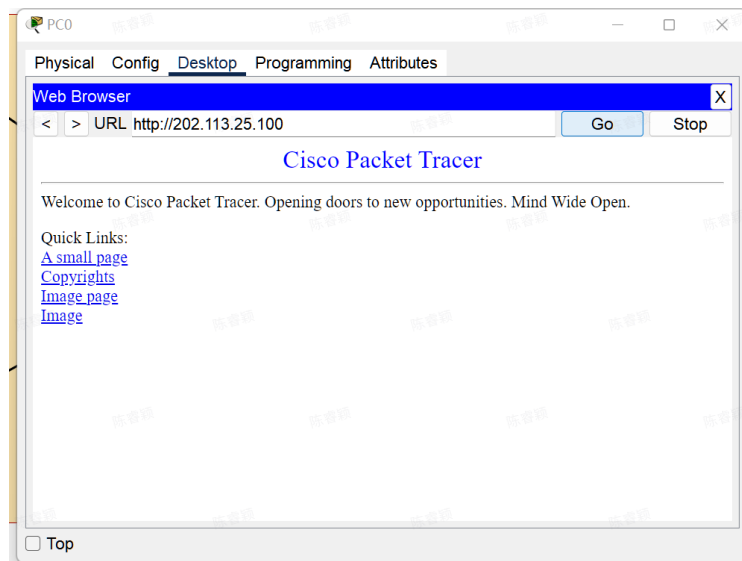
a. 打开web服务器上的web服务：



b. 用内网的主机A访问外网的web服务器，使其发送TCP报文：



访问各页面均正常显示：

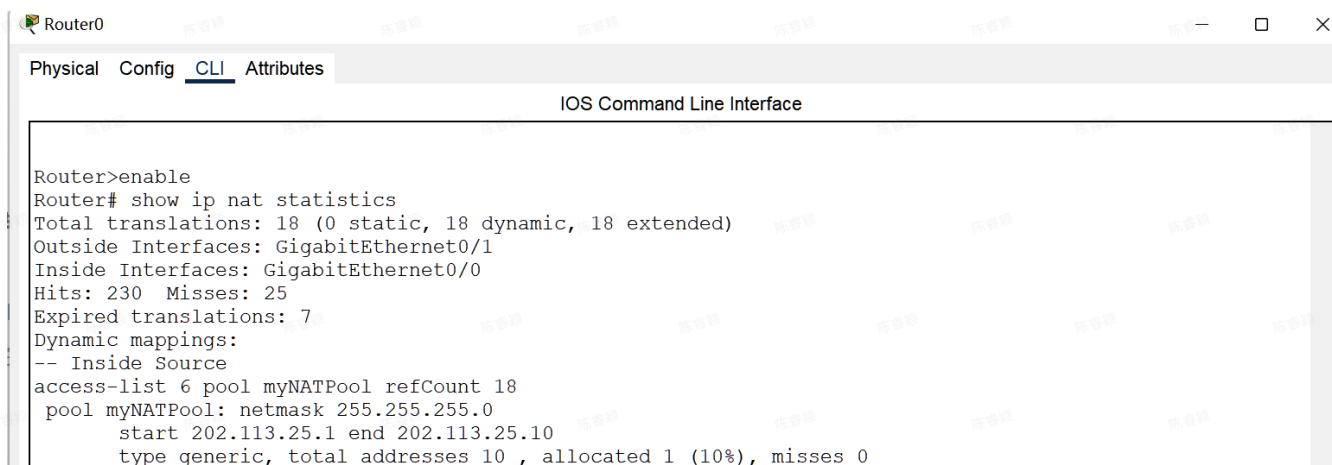


c. 查看NAT对TCP报文的转换情况：

i. 在Router0的CLI中使用命令：

```
1 Router# show ip nat statistics
```

显示NAT统计信息：

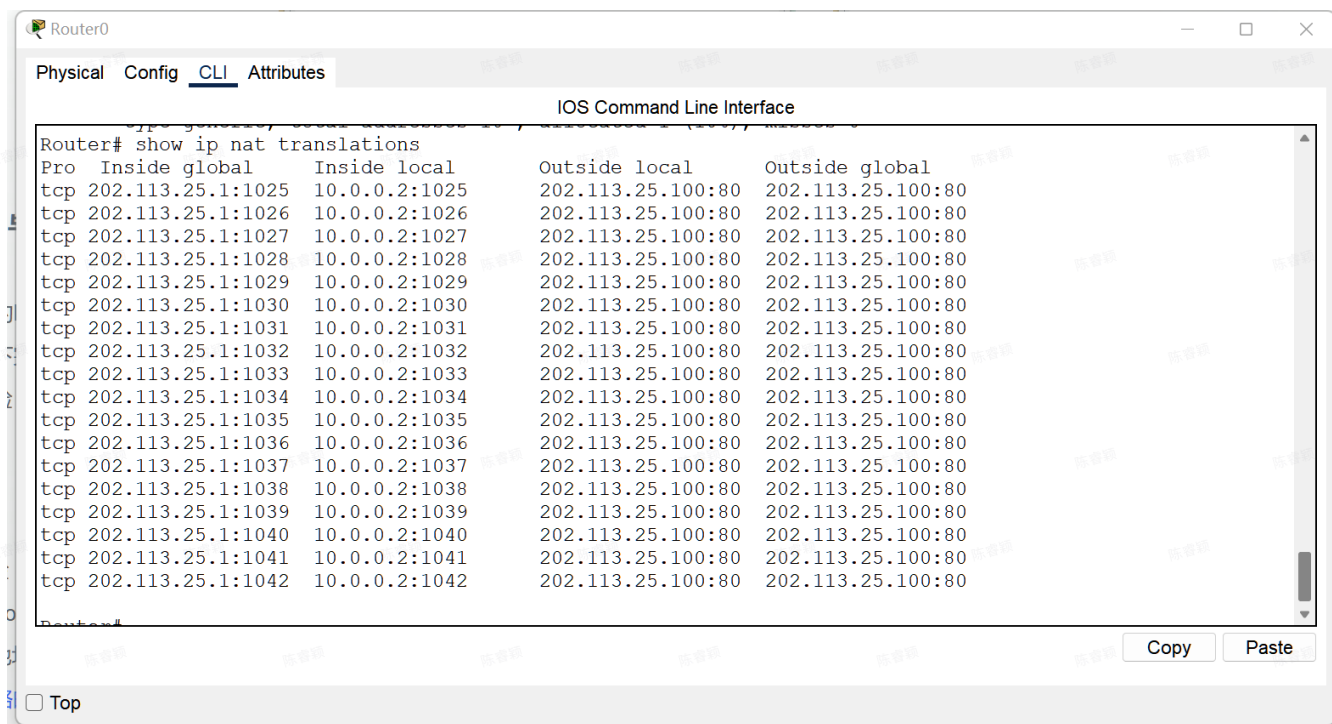


```
Router0>enable
Router# show ip nat statistics
Total translations: 18 (0 static, 18 dynamic, 18 extended)
Outside Interfaces: GigabitEthernet0/1
Inside Interfaces: GigabitEthernet0/0
Hits: 230 Misses: 25
Expired translations: 7
Dynamic mappings:
-- Inside Source
access-list 6 pool myNATPool refCount 18
pool myNATPool: netmask 255.255.255.0
start 202.113.25.1 end 202.113.25.10
type generic, total addresses 10 , allocated 1 (10%), misses 0
```

ii. 或者使用命令：

```
1 Router# show ip nat translations
```

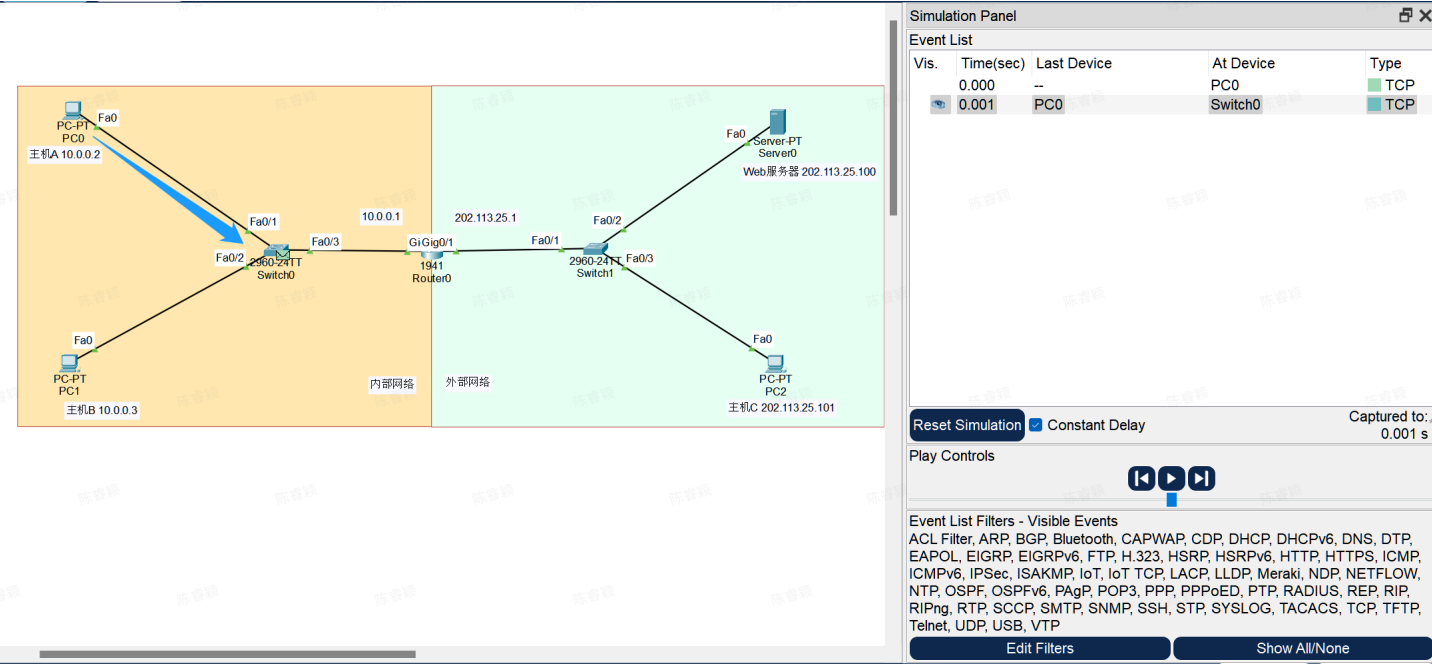
显示地址转换列表：



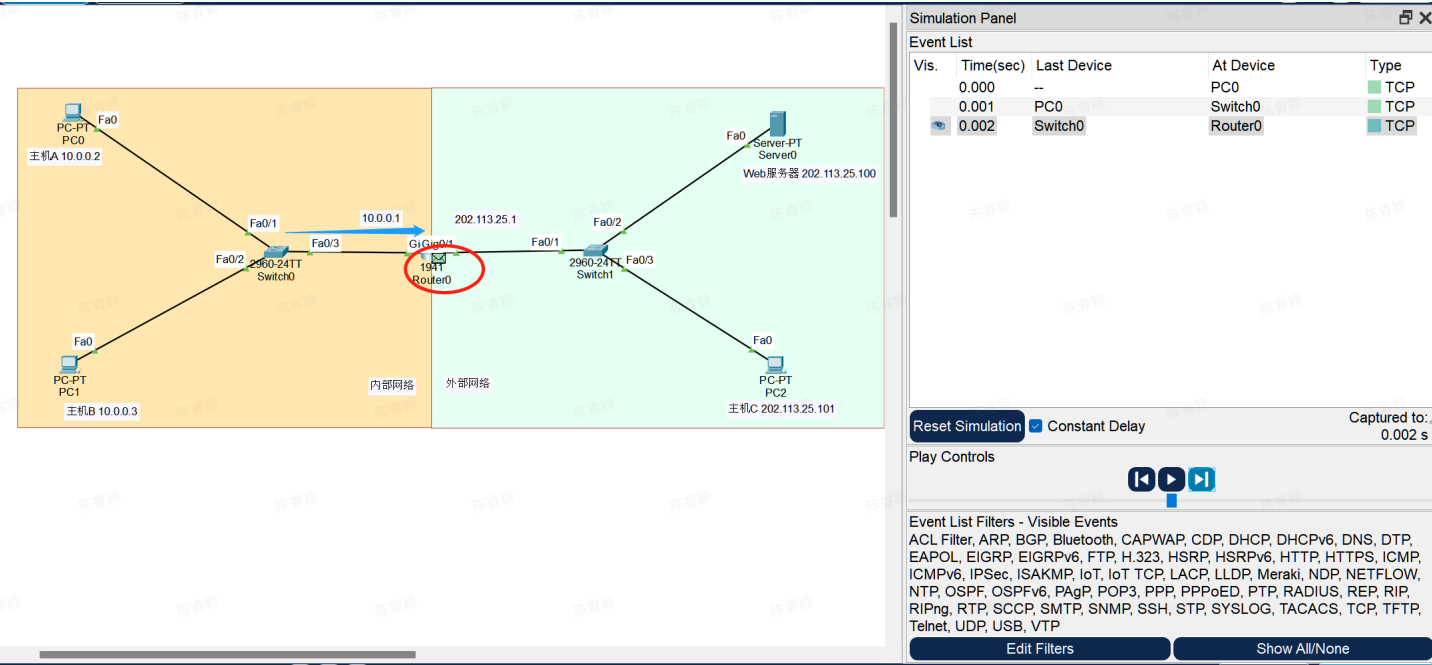
```
Router# show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
tcp  202.113.25.1:1025    10.0.0.2:1025     202.113.25.100:80 202.113.25.100:80
tcp  202.113.25.1:1026    10.0.0.2:1026     202.113.25.100:80 202.113.25.100:80
tcp  202.113.25.1:1027    10.0.0.2:1027     202.113.25.100:80 202.113.25.100:80
tcp  202.113.25.1:1028    10.0.0.2:1028     202.113.25.100:80 202.113.25.100:80
tcp  202.113.25.1:1029    10.0.0.2:1029     202.113.25.100:80 202.113.25.100:80
tcp  202.113.25.1:1030    10.0.0.2:1030     202.113.25.100:80 202.113.25.100:80
tcp  202.113.25.1:1031    10.0.0.2:1031     202.113.25.100:80 202.113.25.100:80
tcp  202.113.25.1:1032    10.0.0.2:1032     202.113.25.100:80 202.113.25.100:80
tcp  202.113.25.1:1033    10.0.0.2:1033     202.113.25.100:80 202.113.25.100:80
tcp  202.113.25.1:1034    10.0.0.2:1034     202.113.25.100:80 202.113.25.100:80
tcp  202.113.25.1:1035    10.0.0.2:1035     202.113.25.100:80 202.113.25.100:80
tcp  202.113.25.1:1036    10.0.0.2:1036     202.113.25.100:80 202.113.25.100:80
tcp  202.113.25.1:1037    10.0.0.2:1037     202.113.25.100:80 202.113.25.100:80
tcp  202.113.25.1:1038    10.0.0.2:1038     202.113.25.100:80 202.113.25.100:80
tcp  202.113.25.1:1039    10.0.0.2:1039     202.113.25.100:80 202.113.25.100:80
tcp  202.113.25.1:1040    10.0.0.2:1040     202.113.25.100:80 202.113.25.100:80
tcp  202.113.25.1:1041    10.0.0.2:1041     202.113.25.100:80 202.113.25.100:80
tcp  202.113.25.1:1042    10.0.0.2:1042     202.113.25.100:80 202.113.25.100:80
```

3.1.5 “模拟” 方式中观察IP数据报在互联网中的传递过程

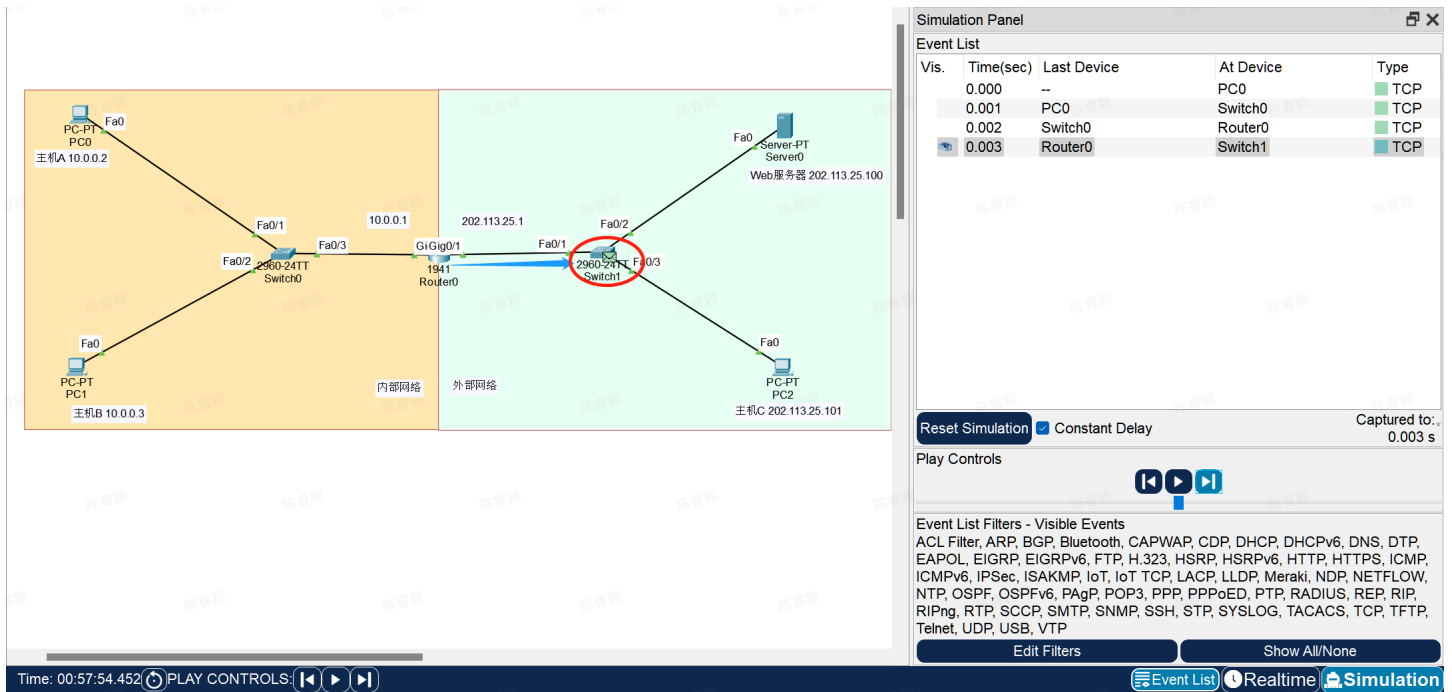
首先在主机A的浏览器中访问web服务器的IP地址，这就需要向服务器发送TCP报文。由于web不在当前的局域网中，所以将报文发送给交换机Switch0：



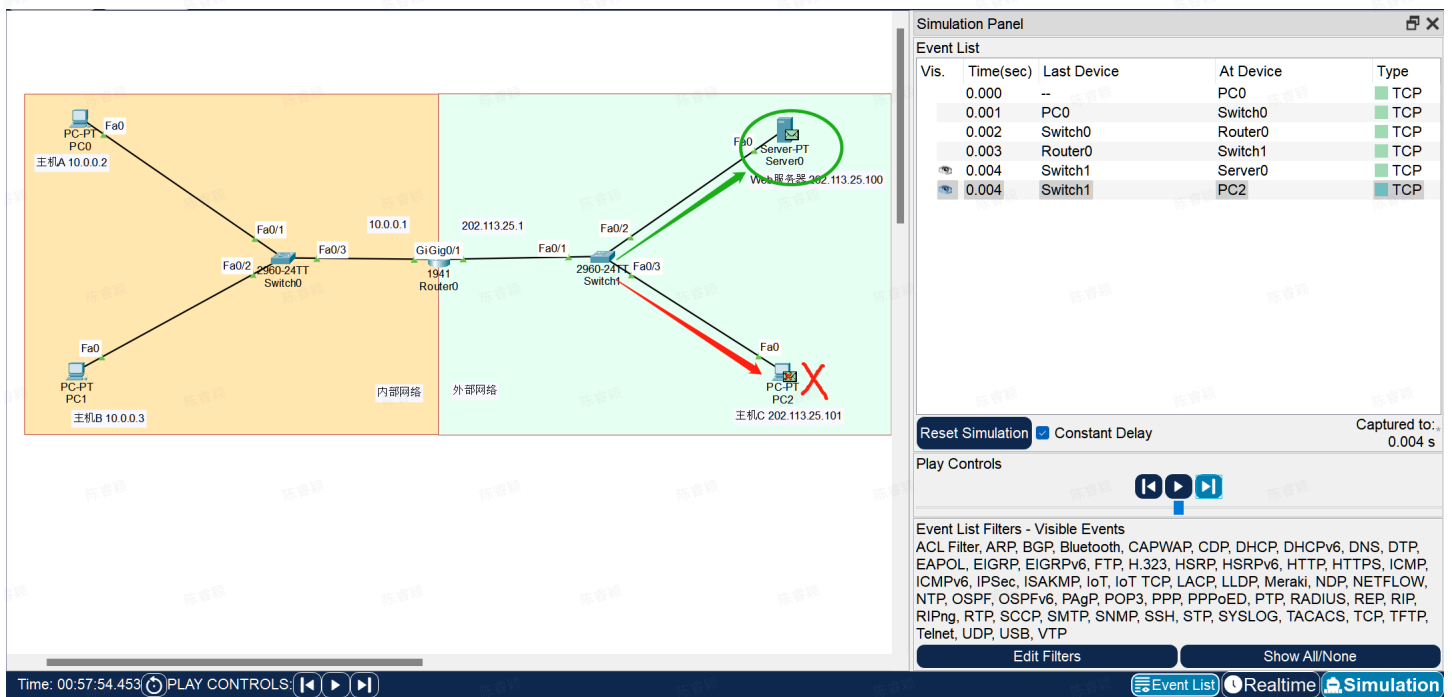
交换机Switch0再发送给路由器Router0：



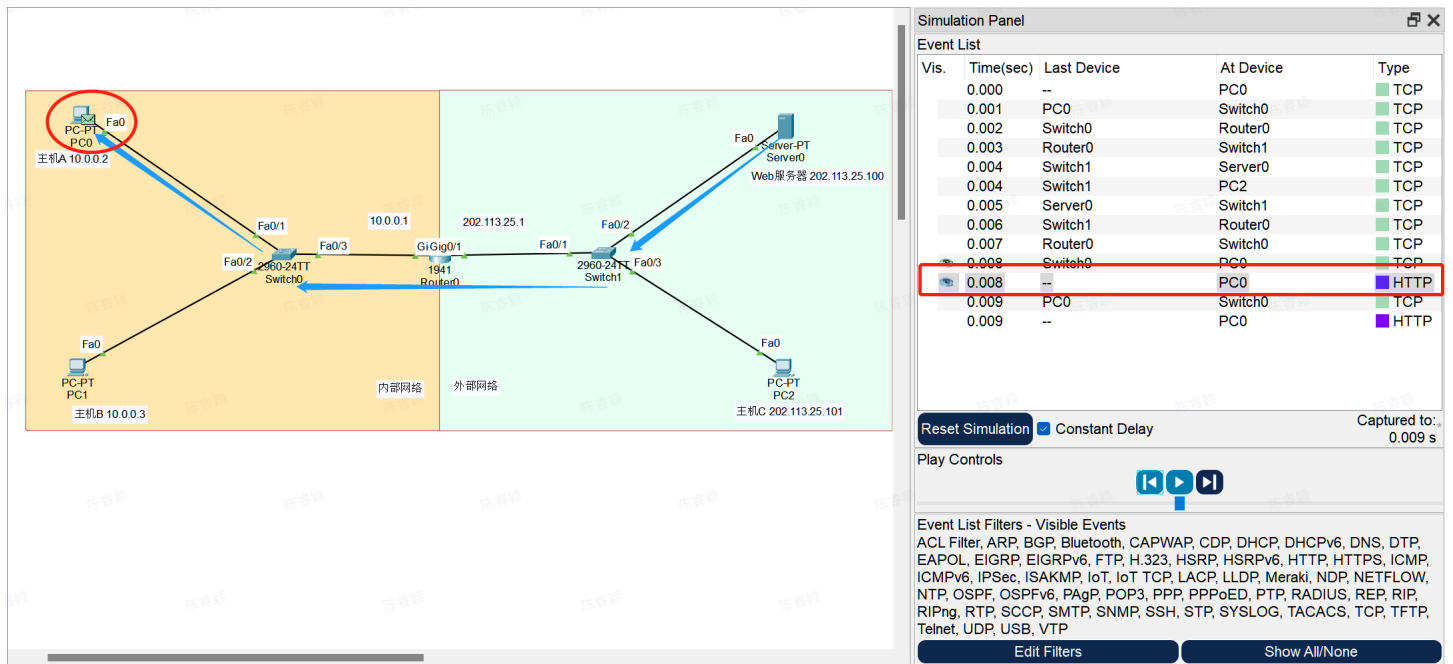
路由器发送给交换机Switch1：



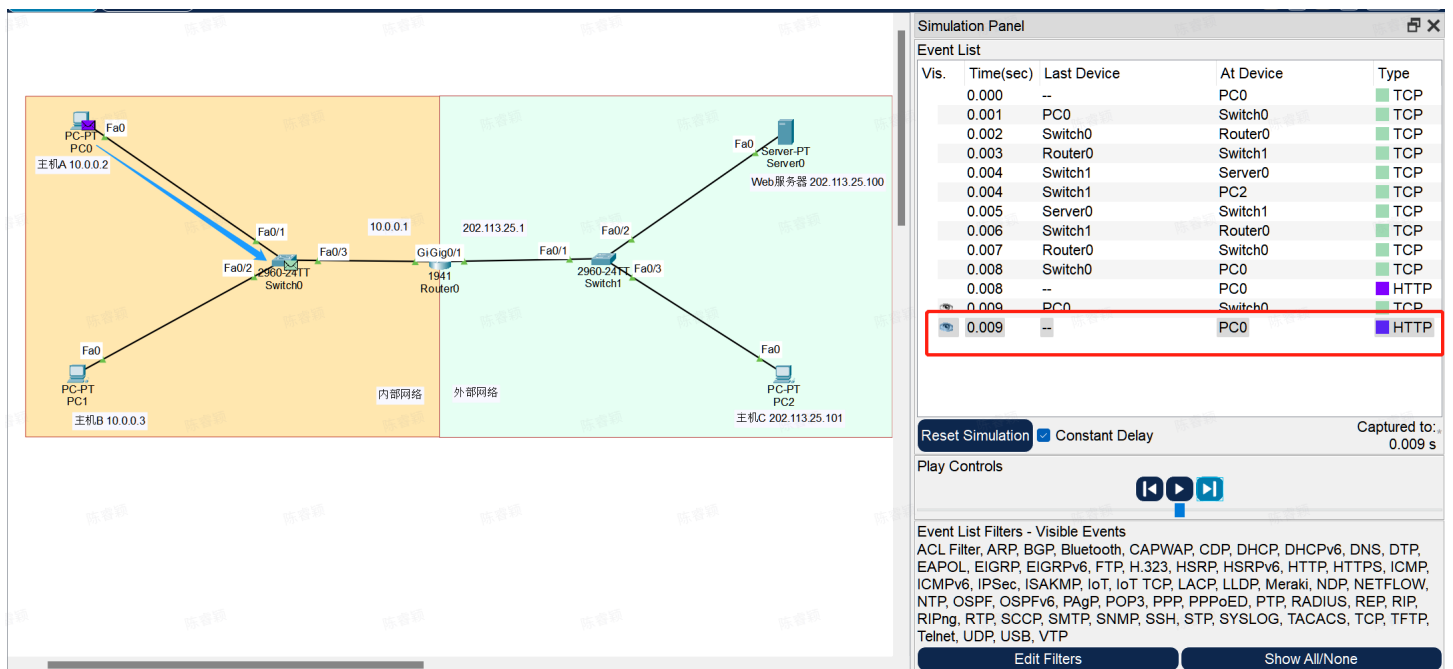
Switch1进行广播转发，web服务器成功收到：

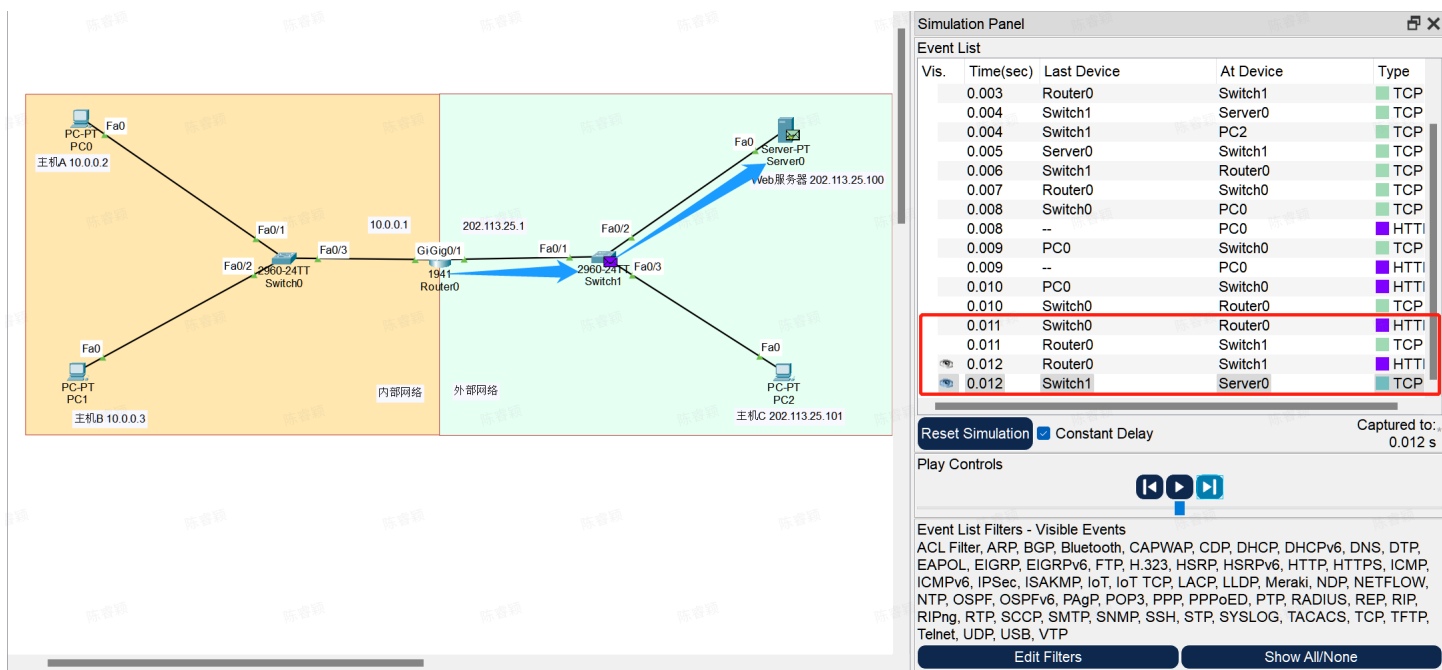
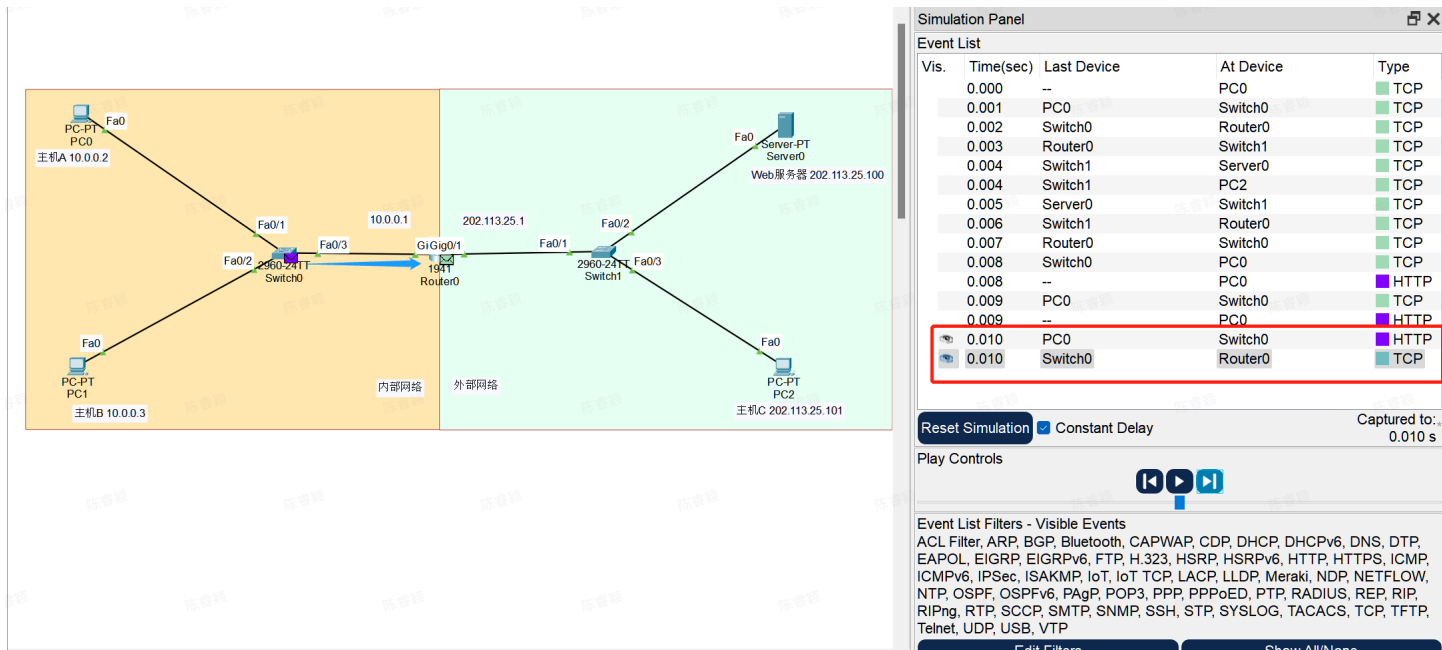


接下来web返回TCP报文给PC0，PC0收到后确认建立连接，即发送TCP和http请求：



TCP和http数据包同建立连接时TCP报文传输路径一样传输给web服务器：





web收到http请求后返回http报文给PC0，此时网页访问成功！

PC-PT
PC0
主机A 10.0.0.2

Fa0

PC-PT
PC1
主机B 10.0.0.3

Fa0

2960-24TT
Switch0

Fa0/1Fa0/3

Router0

GiGig0/1

2960-24TT
Switch1

Fa0/1Fa0/3

Server-PT
Server0
Web服务器 202.113.25.100

Fa0

PC-PT
PC2
主机C 202.113.25.101

Fa0

内部网络外部网络

10.0.0.1202.113.25.1

PC0

Physical Config Desktop Programming Attributes

Web Browser

<> URL http://202.113.25.100 Go Stop

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities.
Mind Wide Open.

Quick Links:
[A small page](#)
[Copyrights](#)
[Image page](#)
[Image](#)

Time: 00:57:54.466 PLAY C

Automatically Choose Connection Type

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.008	Switch0	PC0	TCP
	0.008	--	PC0	HTT
	0.009	PC0	Switch0	TCP
	0.009	--	PC0	HTT
	0.010	PC0	Switch0	HTT
	0.010	Switch0	Router0	TCP
	0.011	Router0	Switch1	HTT
	0.011	Router0	Switch1	TCP
	0.012	Router0	Switch1	HTT
	0.012	Switch1	Server0	TCP
	0.013	Switch1	Server0	HTT
	0.014	Server0	Switch1	HTT
	0.015	Switch1	Router0	HTT
	0.016	Router0	Switch0	HTT
	0.017	Switch0	PC0	HTT
	0.017	--	PC0	TCP

Reset Simulation Constant Delay Captured to: 0.017 s

Play Controls

Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPsec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoE, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters Show All/None

Scenario 0 Fire Last Status Source Destination Type Color Time(sec) Pe

New Delete Toggle PDU List Window