南 开 大 学

计算机与网络空间安全学院

网络技术与应用课程报告

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**第六次实验报告**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

学号：2012911

姓名：马永田

年级：2020级

专业：计算机科学与技术

2022年11月26日

1. **实验内容说明**

**（一）  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。

**（二）  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. **实验准备**
2. **学习路由器的NAT配置过程。**

### NAT（Network Address Translation ）技术提供了一种完全将内部网络和Internet网隔离的方法，让内部网络中的计算机通过少数几个甚至一个合法IP地址（已申请的一个公网IP）访问Internet资源，从而节省了IP地址，并得到广泛的应用。

### **NAT常见的三种类型：**

### **静态[地址转换](https://so.csdn.net/so/search?q=%E5%9C%B0%E5%9D%80%E8%BD%AC%E6%8D%A2&spm=1001.2101.3001.7020" \t "https://blog.csdn.net/besti_white/article/details/_blank)：**

### 指将内部网络的私有IP地址转换为公有IP地址，IP地址对是一对一的，是一成不变的，某个私有IP地址只转换为某个公有IP地址。借助于静态转换，可以实现外部网络对内部网络中某些特定设备（如服务器）的访问。

### **动态地址转换：**

### 指将内部网络的私有IP地址转换为公用IP地址时，IP地址是不确定的，是随机的，所有被授权访问上Internet的私有IP地址可随机转换为指定的合法IP地址集。

### **端口多路复用：**

### 指改变外出数据包的源端口并进行端口转换，即端口地址转换（PAT，Port Address Translation).采用端口多路复用方式。内部网络的所有主机均可共享一个合法外部IP地址实现对Internet的访问，从而可以最大限度地节约IP地址资源。

### 注：一条NAT转换条目要占用160字节内存，因此NAT的转换数目受路由器的内存限制。

**在Cisco路由器上配置NAT的方法如下。**

1. 配置路由器的IP地址：按照前面学习的方法配置路由器Router0的IP地址，并

保证接口处于激活状态。

1. 指定NAT使用的全局IP地址范围：在全局配置模式下，使用命令

**ip nat pool PoolName StartIP EndIP netmask Mask** 定义一个 IP 地址池。

其中,PoolName 是一个用户选择的字符串，用于标识该IP地址池；StartIP、EndIP和Mask分别表示该地址池的起始IP地址、终止IP地址和掩码。在NAT配置中，IP地址池定义了内网访问外网时可以使用的全局 IP 地址。例如，ip nat pool MyNATPool 202. 113. 25. 1 202. 113. 25. 10 netmask 255. 255. 255. 0 定义了一个名字为 MyNATPool 的 IP 地址池。该 MyNATPool 地址池中的IP地址从202. 113. 25. 1开始，至202. 113.25. 10结束，共10个IP地址。

1. 设置内部网络使用的IP地址范围：在全局配置模式下，使用命令

**access-list LabellD permit IPAddr WildMask**定义一个允许通过的标准访问列表。

其中，LabellD是一个用户选择的数字编号，标号的范围为1〜99, 标识该访问列表；IPAddr和WildMask分别表示起始IP地址和通配符，用于定义IP地址的范围。在NAT配置中，访问列表用于指定内部网络使用的IP地址范围。例如,access-list 6 permit 10. 0. 0. 0 0. 255.255.255定义了一个标号为6的访问列表，该访问列表允许10. 0. 0. 0到10. 255. 255.25的IP地址通过。

1. 建立全局IP地址与内部私有IP地址之间的关联：在全局模式下，利用

**ip nat inside source list LabellD pool PoolName overload** 建立全局 IP 地址与内部私有 IP 地址之间的关联。

其意义为访问列表LabellD中指定的IP地址可以转换成地址池PoolName中的IP地址访问外部网络。overload关键词表示NAT转换中釆用NAPT方式，PoolName中的IP地址可以重用。如果不加。verload关键词，则说明NAT转换中采用动态 NAT 方式。例如,ip nat inside source list 6 pool MyNATPool overload 通知系统该NAT转换釆用NAPT方式，将访问列表6中指定的IP地址(10. 0. 0. 0到10. 255. 255. 255)转换成地址池MyNATPool中的IP地址(202. 113. 25. 1到202. 113. 25. 10)访问外部互联网。

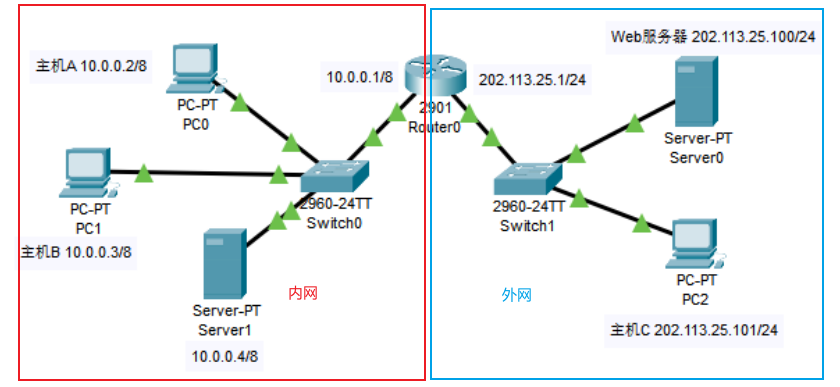
1. 指定连接内部网络和外部网络的接口：指定哪个接口连接内部网络，哪个接口

连接外部网络需要在具体的接口配置模式下设定。使用**ip nat inside**指定该接口连接内

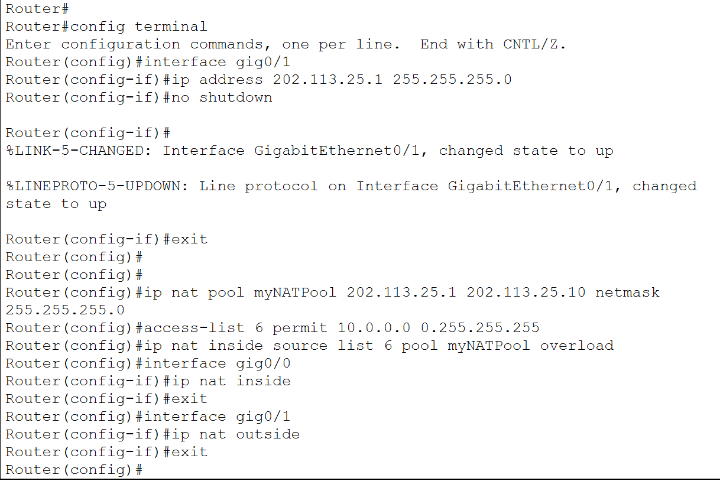
部网络，使用**ip nat outside**指定该接口连接外部网络。

1. 查看NAT的工作状况：为了测试网络的连通性，查看NAT的工作情况，首先需要为PC和服务器配置正确的IP地址和默认网关。其次，单击工作区中的Web服务器图标，可以在Services页面启动Web服务。只有在Web服务启动后，才可以通过单击工作区中的PC图标，在Desktop页面中运行Web Browser,进而访问该Web服务器。为了查看NAT的工作状况,Cisco路由器提供了**show ip nat statistics**和**show ip nat translations**命令。这两个命令需要在特权模式下运行，分别显示NAT转换的统计 信息和NAT地址转换表。
2. **实验过程**

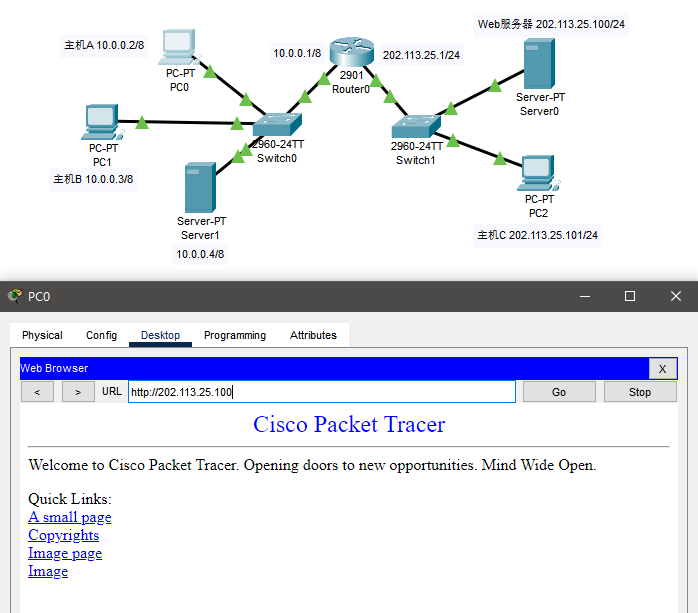
**（一）组建由NAT连接的内网和外网。**



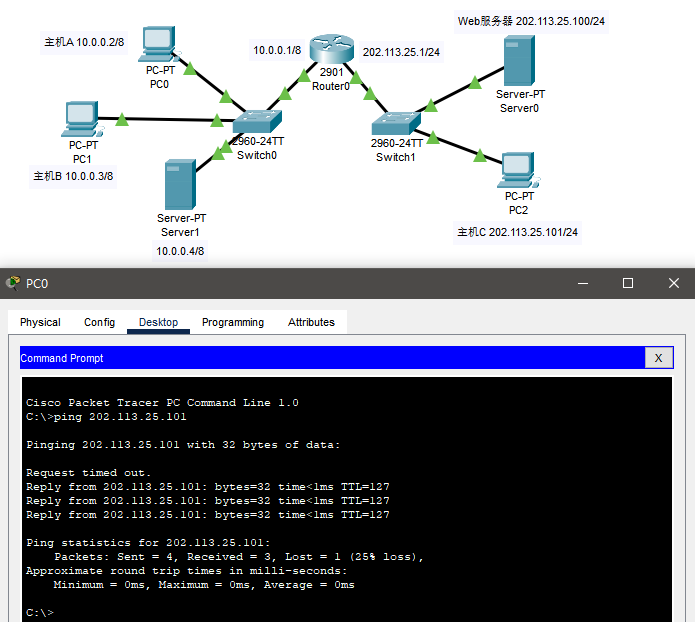
如上图标签所示，为路由器、主机和服务器设置相应的IP地址，全局配置模式下，使用如下命令进行NAT的配置：



1. **测试网络的连通性，观察网络地址映射表。**

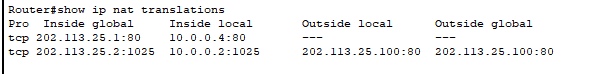


使用内网的主机PC0通过浏览器访问外网的Web服务器Server0，如上图可见访问成功，



在内部网络的主机PC0上对外部网络的主机PC2上使用ping命令测试网络连通性，如上图可见网络正常连通。

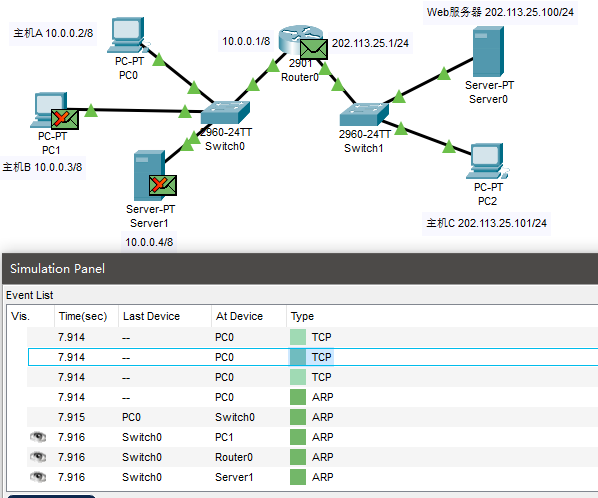
路由器R0全局配置模式下输入命令show ip nat translations 观察网络地址映射表：



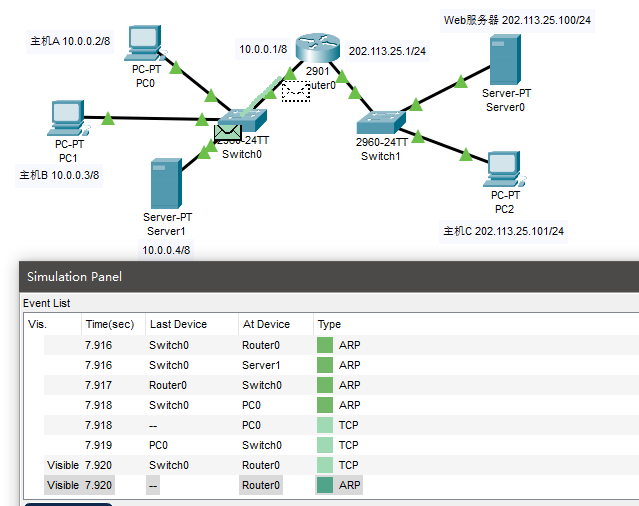
可以看到主机PC0的私有IP地址10.0.0.2:1025会被转换为外网IP地址202.113.25.2:1025

1. **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。**

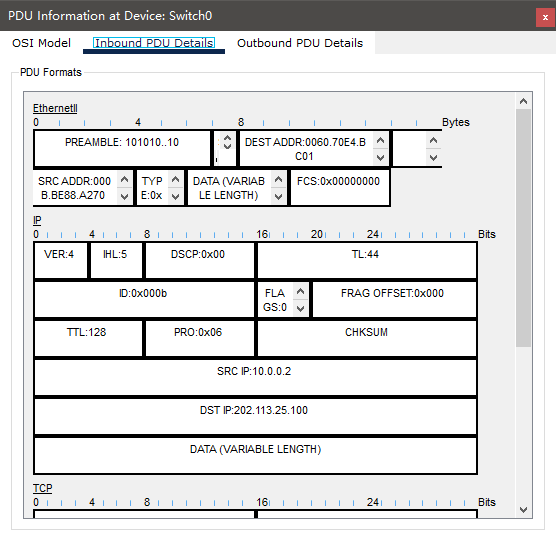
在仿真环境的“模拟”方式中使用内网中的主机PC0通过浏览器访问外网中的服务器Server0,如下图可见，首先PC0产生一个TCP报文和一个ARP报文，其中TCP报文一开始不会发送，而是会先发送ARP报文，之后即同之前实验中的流程：PC0通过ARP广播获取到路由器的IP与MAC地址映射关系，如此PC0即可与路由器进行通信。



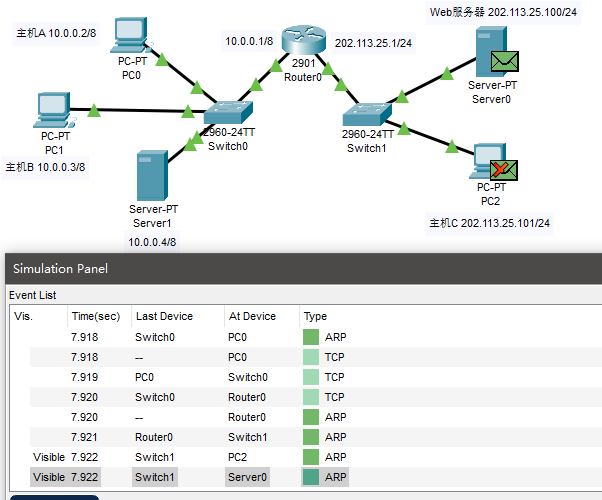
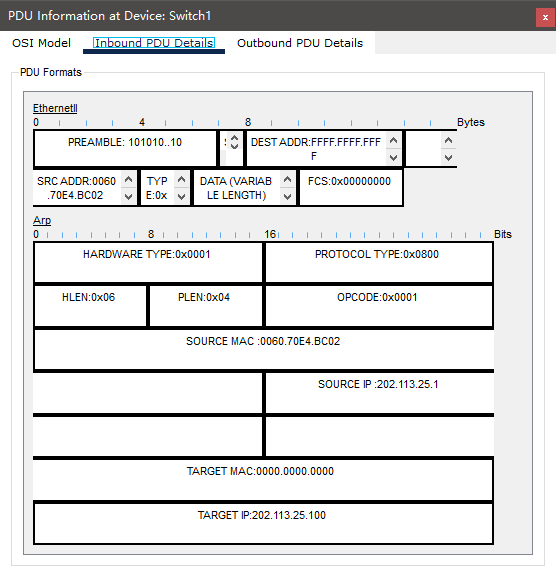
由于该TCP报文的目的地址与PC0并非同一个网段，因此PC0会将TCP报文发送给路由器，如下图路由器收到了主机PC0发来的TCP报文，此时路由器收到的TCP报文会显示红叉错误，同时Router0也会产生一个ARP报文：



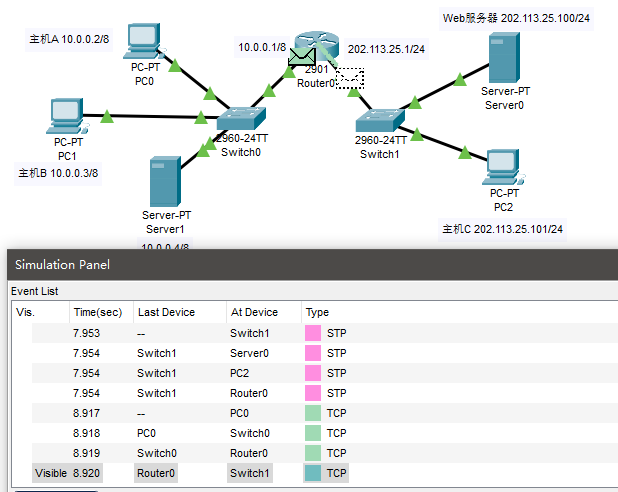
查看从PC0发出的TCP报文可以看到如下图，其中源IP为10.0.0.2，即内网地址，而目的IP为202.113.25.100，即要访问的网服务器的IP地址。



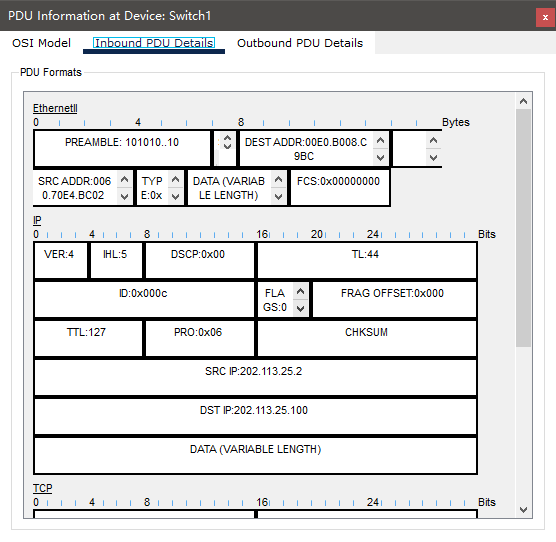
之后Router0会在目的外网IP所在的网段中广播ARP报文，如下图可见，该ARP报文中的目的地址为我们要访问的服务器IP地址，即为之前Router0收到的TCP报文中的目的IP。



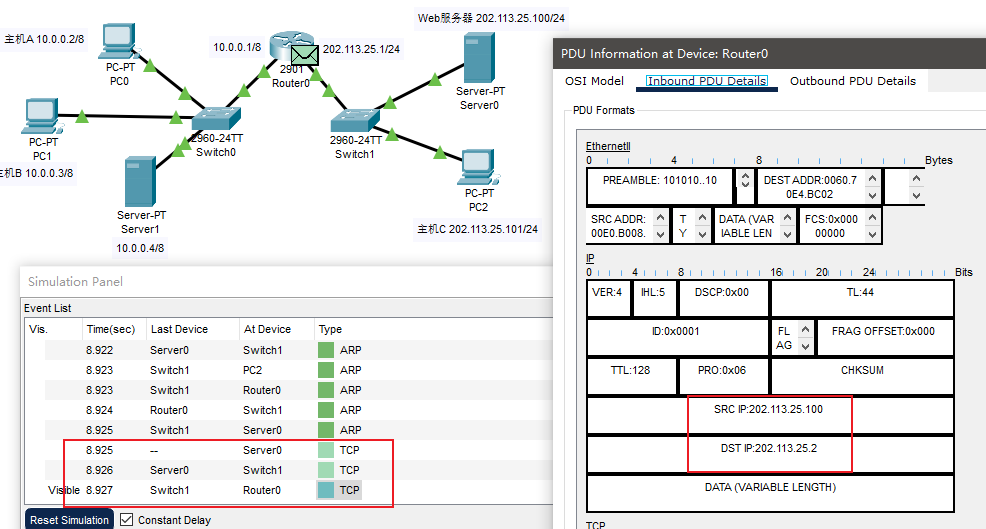
在经过ARP广播与响应获取到服务器的MAC地址后，Router0可以与Server0进行通信，之后由于之前的TCP报文未成功到达目的IP，已经失效，此时PC0会重新发送一个TCP报文，其内容与之前的相同，源IP地址为内网10.0.0.2，目的IP地址为外网服务器的IP地址。



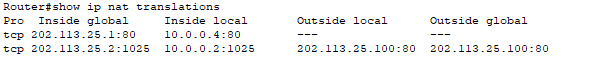
此次路由器收到后不再显示错误，而是继续向后转发，且观察重新发送出去的TCP报文，如下图可以看到，其中的目的IP地址仍为外网服务器地址，但源IP地址不再是内网的IP地址，而是被修改为一个公网IP地址，成功实现内部网络的私有IP地址转换为公有IP地址。

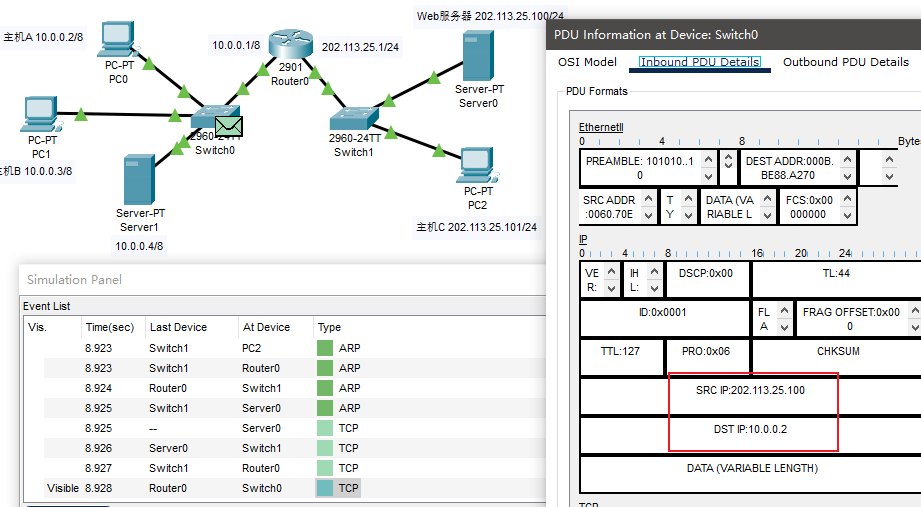


服务器收到该TCP报文后会先通过ARP广播获取路由器的MAC地址，之后回复一个TCP报文，如下图可见，该TCP报文的源IP地址为Server0的地址，而目的地址为内网主机PC0在路由器Router0处通过NAT转换得到的公网地址，即实际上该报文发向了路由器Router0:

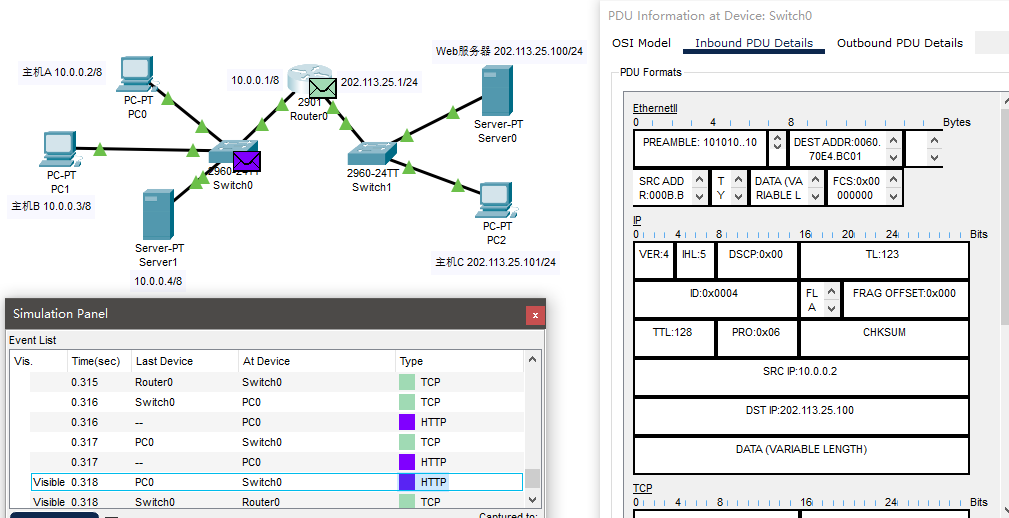


而路由器Router0在收到该TCP报文后，如下图，会根据网络地址映射表，将其中的目的IP(即之前将私有IP 10.0.0.2转换后得到的公网IP 202.113.25.100)重新转换为内网中PC0的私有IP 10.0.0.2。

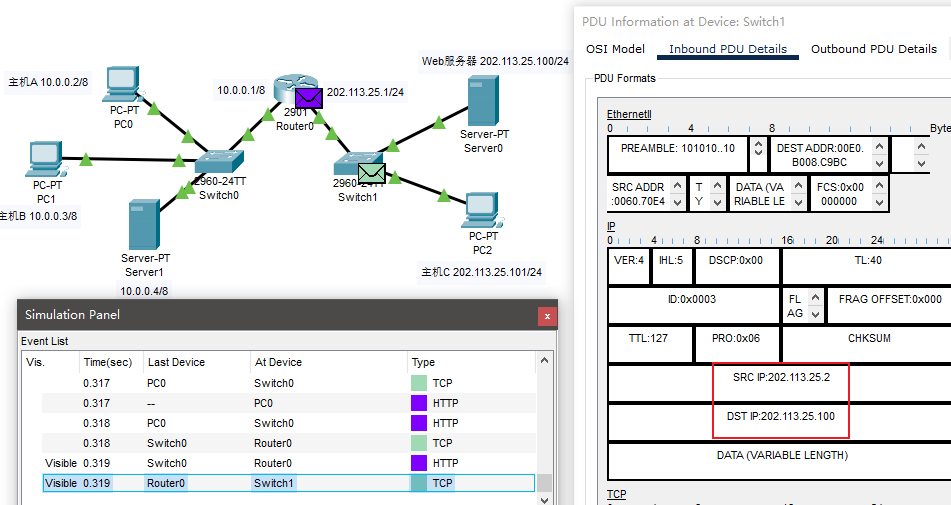


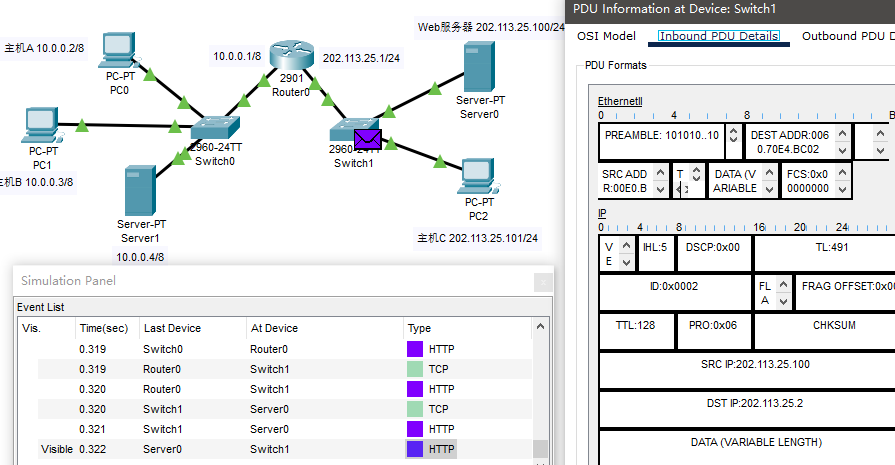


之后路由器将其发送给内网中的主机PC0，当主机PC0收到之后，TCP连接已实现两次握手，请求方处于ESTABLISHED状态，因此PC0发送一个TCP报文完成三次握手之后，又立即发送了下一个HTTP报文进行HTTP资源的请求，且该HTTP报文与TCP报文在到达路由器之前源IP地址均为内网IP地址：



经路由器转发之后，源IP地址均根据网络地址映射表转换为一个公网IP地址：



服务器收到最后一个TCP报文后完成三次握手，进入ESTABLISHED状态，接收HTTP报文并进行回复，之后流程与之前相同，报文在经过Router0后，都会根据网络地址映射表进行一个内网与外网的转换，最终实现了内网主机与外网服务器的通信。

**（四）在内网中设置NAT服务器，使外部主机能够顺利使用该Web服务。**

可以通过在路由器中添加静态NAT来实现外部主机访问内网的服务器，输入如下命令：

ip nat inside source static tcp 10.0.0.4:80 202.113.25.1:80进行配置

如图可见使用PC2成功访问到内网中的NAT服务器。

