编号：

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 实验 | 一 | 二 | 三 | 四 | 五 | 六 | 七 | 八 | 总评 | 教师签名 |
| 成绩 |  |  |  |  |  |  |  |  |  |  |

武汉大学国家网络安全学院

课程实验(设计)报告

题 目： NAT设计实验

专业(班)： 信息安全

学 号： 2021302181156

姓 名： 赵伯俣

课程名称： 计算机网络实践

任课教师： 杜瑞颖

2024年5月13日

**目录**

[1 实验目的 2](#_Toc166527215)

[2 实验内容 2](#_Toc166527216)

[3 实验原理 4](#_Toc166527217)

[3.1 NAT 4](#_Toc166527218)

[3.2 NAPT端口转换技术 6](#_Toc166527219)

[3.3 NAPT端口安全配置 7](#_Toc166527220)

[4 实验环境 9](#_Toc166527221)

[5 实验过程 10](#_Toc166527222)

[5.1 设计拓扑图 10](#_Toc166527223)

[5.2 连线图及逻辑拓扑图 10](#_Toc166527224)

[5.3 配置路由器 14](#_Toc166527225)

[6 实验结果 17](#_Toc166527226)

[6.1 查看路由表及NAT信息 17](#_Toc166527227)

[6.2 查看端口安全配置 18](#_Toc166527228)

[6.3 ping测试及访问服务器网站 20](#_Toc166527229)

[7 实验心得 23](#_Toc166527230)

# 1 实验目的

* 掌握NAT的原理及配置
* 掌握NAT源地址转换和目的地址转换的区别
* 掌握如何向外网发布内网的服务器

# 2 实验内容

（1）A公司的企业网络如下图所示，由三台路由器和两台二层交换机构成。现要求网 络管理员进行如下配置：

1）通过配置 NAT，实现 192.168.2.0 网络中的计算机共享IP地址 202.114.66.2上网；

2）通过配置NAT，192.168.1.0网络中的计算机通过IP池 202.114.65.5-202.114.65.12上网；

3） 配置 NAT，通过 202.114.65.100:80 访问内网中的 WWW2 服务器；

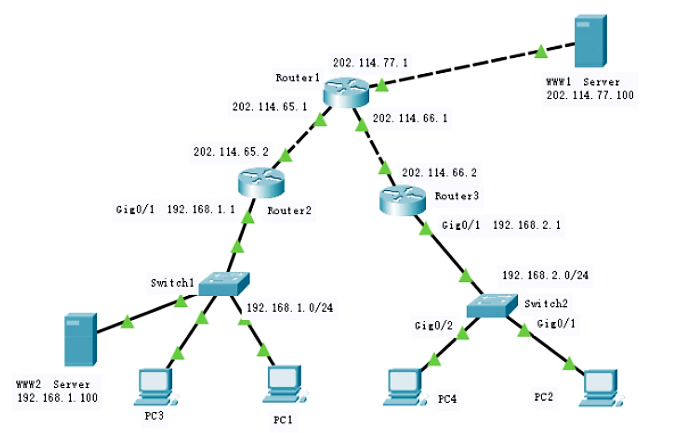
4） 在交换机 Switch2 中配置端口安全，设置Gig0/1端口只允许 PC2 使用192.168.2.100访问；设置 Gig0/2 端口只允许 PC4 等至多4台机器访问；

5） 路由器之间采用静态路由协议。

（2）查看路由器 Router3的路由协议和路由表；查看路由器 Router3的NAT信息

（3）查看路由器 Router2的路由协议和路由表；查看路由器 Router2的NAT信息

（4）实验报告中包含路由器 Router2 和 Router3 中的全部配置信息；Switch2 交换机 中的端口安全配置信息；以及从 PC1->WWW1 服务器、PC2->WWW1 服务器、PC4访问WWW2 服务器的测试截图



# 3 实验原理

## 3.1 NAT

NAT（Network Address Translation，网络地址转换）是一种在网络通信中常用的技术，用于在不同网络之间转换IP地址的过程。它在Internet Protocol（IP）网络中广泛应用，旨在解决IPv4地址不足的问题，并提供网络安全和隔离。

**1. NAT的原理**

NAT的原理比较简单，它通过在网络边界设备（如路由器、防火墙）上维护一张地址转换表，将内部私有网络（如局域网）中的私有IP地址映射到公共IP地址上，以便与外部网络通信。当内部网络中的主机要发送数据到外部网络时，数据包首先发送到NAT设备。NAT设备根据转换表将源IP地址和端口替换为公共IP地址和端口，然后将数据包发送到目标主机。当外部网络的响应数据包返回时，NAT设备将目标IP地址和端口还原为原始的私有IP地址和端口，然后将数据包发送到内部网络中的目标主机。

**2. NAT的类型**

NAT根据转换的方式和功能可以分为多种类型，包括：

* 静态NAT（Static NAT）：一对一映射，将内部私有IP地址固定映射到公共IP地址上，常用于服务器对外提供服务的场景。
* 动态NAT（Dynamic NAT）：多对多映射，将内部私有IP地址动态映射到公共IP地址上，通过动态分配端口号实现。
* PAT（Port Address Translation，端口地址转换）：一对多映射，将多个内部私有IP地址映射到单个公共IP地址上，通过不同的端口号区分不同的内部主机。

**3. NAT的优势**

* 缓解IPv4地址枯竭问题：由于IPv4地址资源有限，NAT技术可以将多个私有IP地址映射到一个公共IP地址上，从而减少对公共IP地址的需求，延长IPv4地址的使用寿命。
* 增强网络安全性：NAT隐藏了内部网络的真实IP地址，使外部网络无法直接访问内部网络中的主机，从而提高了网络的安全性，有效防止了一些网络攻击，如端口扫描、DDoS攻击等。
* 简化网络配置：NAT技术可以在不改变内部网络结构的情况下连接到Internet，减少了对公共IP地址的需求，同时也简化了网络配置和管理。

尽管NAT技术在IPv4网络中有着广泛的应用，但它也带来了一些问题，如难以支持一些应用层协议（如IPSec、SIP等）、增加了网络延迟等。随着IPv6的逐渐普及和应用，NAT技术在未来可能会逐渐被取代，但在当前IPv4网络环境下，NAT仍然是一种非常重要的网络技术。

## 3.2 NAPT端口转换技术

NAPT（Network Address and Port Translation，网络地址和端口转换）也称为PAT（Port Address Translation，端口地址转换），是NAT（Network Address Translation，网络地址转换）的一种扩展形式，旨在解决IPv4地址短缺问题，并支持多个内部主机通过单个公共IP地址访问Internet。NAPT通过在地址转换表中同时记录IP地址和端口信息，实现了将多个内部私有IP地址映射到单个公共IP地址上，并通过不同的端口号区分不同的内部主机。

**NAPT的工作原理**：

1. **内部主机发送数据包**：内部网络中的主机发送数据包到外部网络（如Internet）上的目标主机。
2. **NAPT设备转换IP地址和端口**：数据包首先到达NAPT设备，NAPT设备根据转换表将源IP地址和端口号转换为NAPT设备的公共IP地址和一个新的端口号，并在转换表中记录映射关系。这样可以确保在NAPT设备和目标主机之间建立了唯一的映射关系。
3. **数据包发送到目标主机**：NAPT设备将转换后的数据包发送到目标主机，目标主机收到数据包后，会根据目标端口号将数据包交付给相应的目标内部主机。
4. **目标主机的响应数据包返回**：当目标主机的响应数据包返回时，NAPT设备根据转换表中的映射关系，将目标IP地址和端口号还原为原始的内部私有IP地址和端口号，然后将数据包发送到内部网络中的源主机。

**NAPT的优势**：

1. **节约IP地址资源**：NAPT技术可以将多个内部私有IP地址映射到单个公共IP地址上，从而节约了公共IP地址资源，延长了IPv4地址的使用寿命。
2. **提高网络安全性**：NAPT隐藏了内部网络的真实IP地址，使外部网络无法直接访问内部网络中的主机，从而提高了网络的安全性，有效防止了一些网络攻击，如端口扫描、DDoS攻击等。
3. **支持多主机同时访问Internet**：NAPT支持多个内部主机通过单个公共IP地址访问Internet，提高了网络的可用性和效率。
4. **简化网络配置**：NAPT技术可以在不改变内部网络结构的情况下连接到Internet，减少了对公共IP地址的需求，同时也简化了网络配置和管理。

NAPT技术在IPv4网络中有着广泛的应用，是解决IPv4地址短缺问题的重要手段之一，同时也提高了网络的安全性和可用性。

## 3.3 NAPT端口安全配置

**1. 配置访问控制列表（ACL）**：

访问控制列表可以用来限制允许通过NAPT进行转换的数据包。可以配置ACL以允许或拒绝特定的IP地址或地址范围通过NAPT设备。这可以帮助防止未经授权的主机访问Internet，从而提高网络的安全性。

**2. 配置端口范围**：

为了避免NAPT设备上的端口资源被耗尽或被滥用，可以配置一个合适的端口范围，限制NAPT设备在转换数据包时可以使用的端口范围。这可以有效地防止一些恶意主机通过大量的连接占用所有可用的端口资源，从而影响其他合法用户的使用体验。

**3. 实施会话限制**：

NAPT设备可以实施会话限制，限制每个内部主机或IP地址可以同时建立的最大会话数量。这可以防止某些恶意主机通过大量的会话占用所有可用的资源，从而保护网络免受过载和拒绝服务（DoS）攻击。

**4. 日志记录和监控**：

对于NAPT设备上的所有转换操作和安全事件，应该进行日志记录和监控。这样可以及时发现异常行为和安全事件，并采取适当的措施进行应对和处理，以保护网络的安全性和稳定性。

**5. 更新和维护**：

定期更新NAPT设备的固件和软件，以修复已知的漏洞和安全问题。同时，定期进行安全审计和漏洞扫描，及时发现和修复潜在的安全风险，保障网络的安全。

**6. 加密和身份验证**：

对于一些敏感数据和重要应用，可以考虑使用加密和身份验证等安全措施，保护数据的机密性和完整性。这可以防止数据在传输过程中被窃听或篡改，提高数据的安全性。

综上所述，NAPT端口安全配置是保护网络安全的重要措施之一。通过合理配置ACL、端口范围、会话限制等安全策略，加强日志记录和监控，定期更新和维护设备，以及使用加密和身份验证等安全措施，可以有效地提高网络的安全性，保护网络免受各种攻击和滥用。

# 4 实验环境

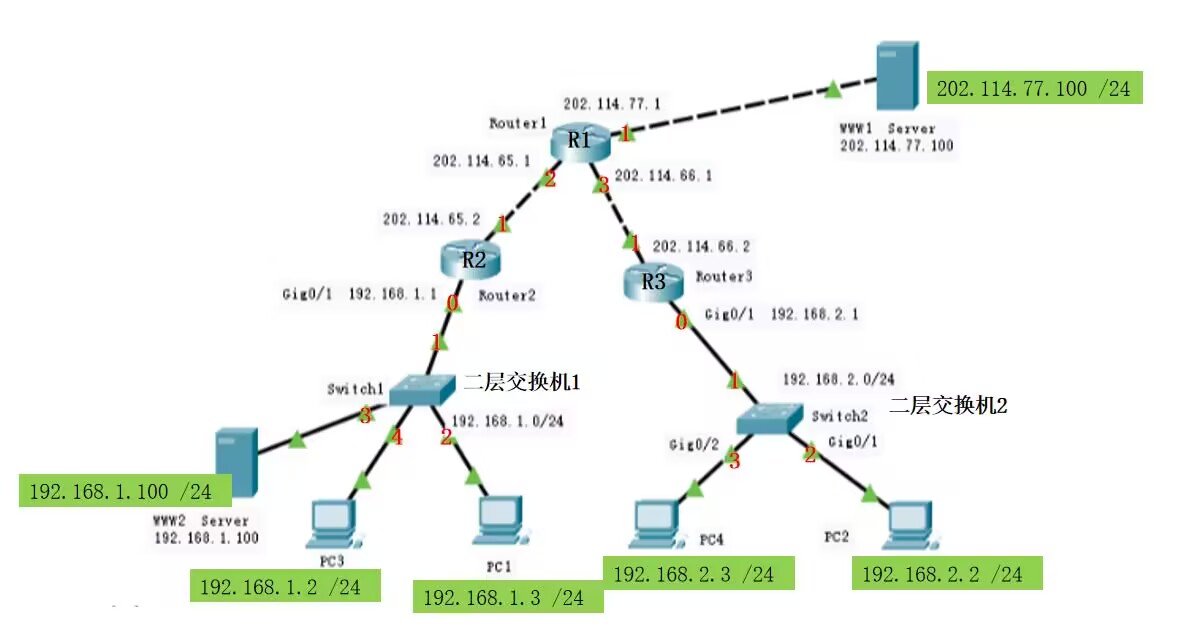
本次实验使用CII云教学领航中心配套设备和实验平台。

在本次实验中，使用三台路由器、两台二层交换机和六台PC机。

# 5 实验过程

## 5.1 设计拓扑图

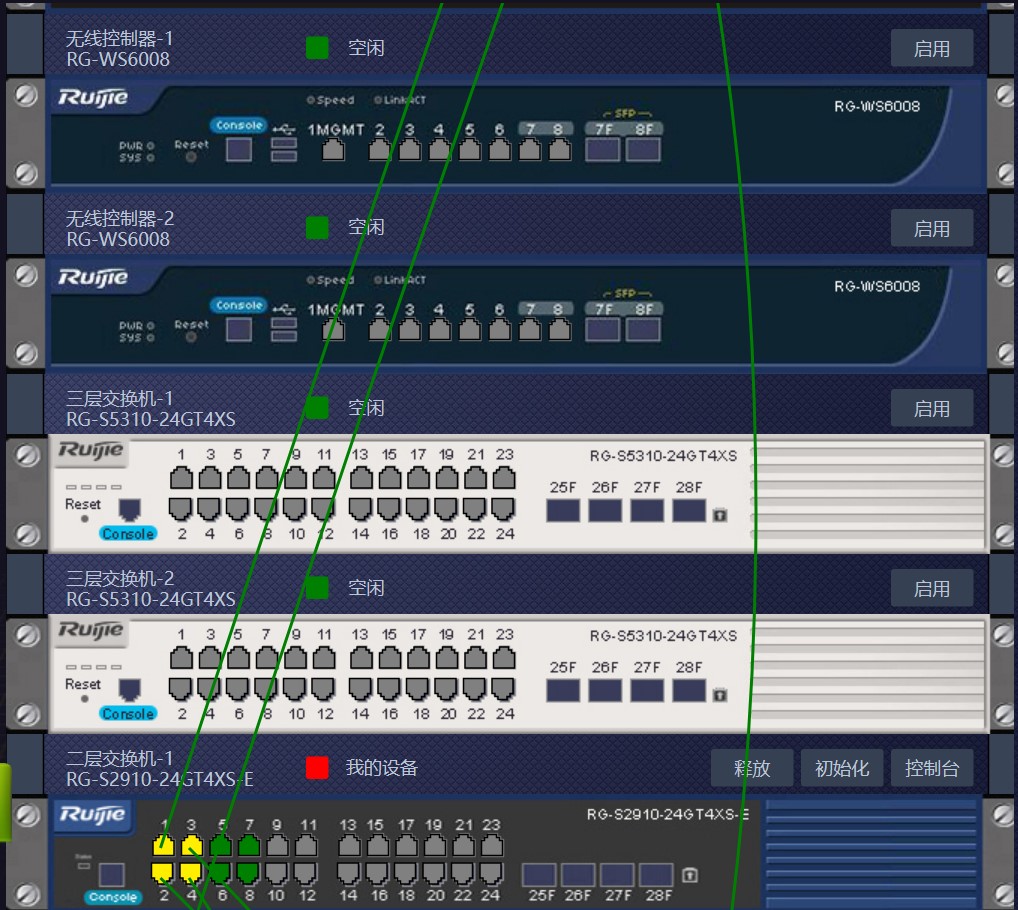
实验拓扑图如下：

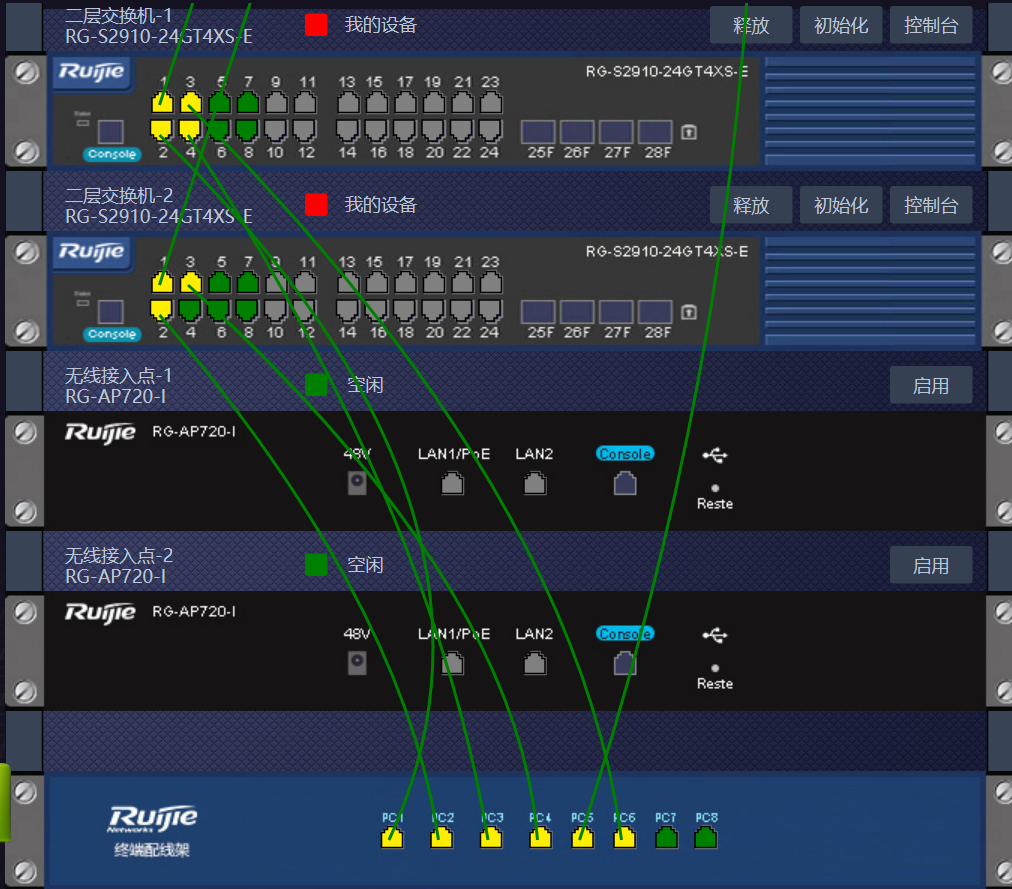


## 5.2 连线图及逻辑拓扑图

连线图如下



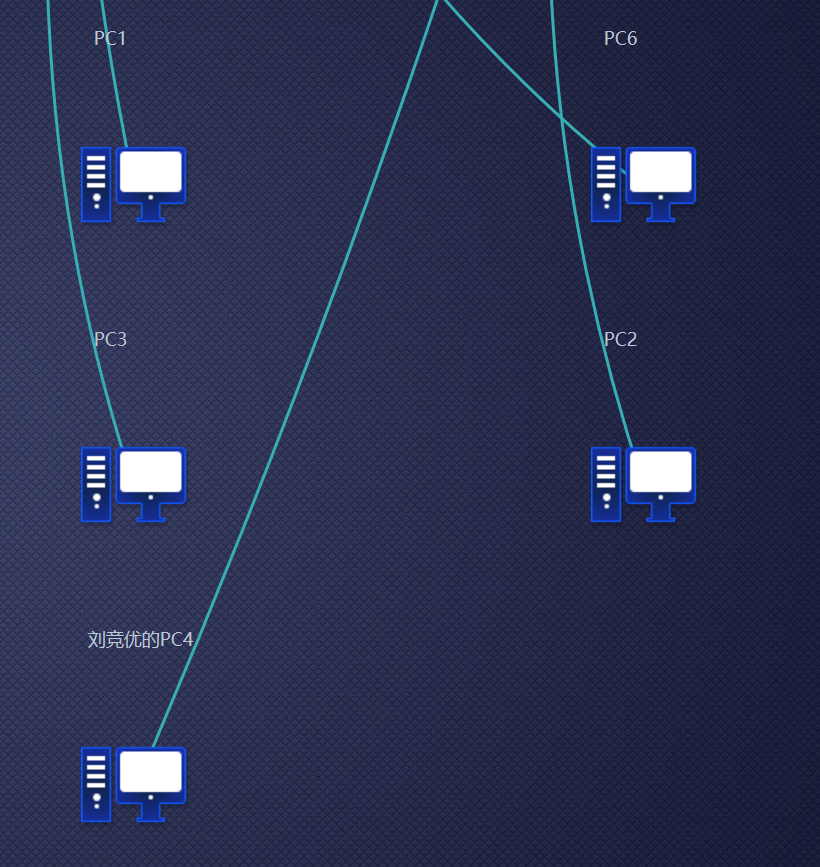




逻辑拓扑图







## 5.3 配置路由器与交换机

### 5.3.1 配置路由器1

对于路由器1来说我们只需要配置其3个端口的IP地址即可，在终端中执行如下命令

en

conf t

int gi 0/1

ip add 202.114.77.1 255.255.255.0

no shutdown

exit

int gi 0/2

ip add 202.114.65.1 255.255.255.0

no shutdown

exit

int gig 0/3

ip add 202.114.66.1 255.255.255.0

exit

路由器R1配置信息如下所示



### 5.3.2 配置路由器R2

在配置路由器2时需要将与路由器1相连的1端口设置ip

en

conf t

int gi 0/1

ip add 202.114.65.2 255.255.255.0

exit

然后需要清楚vlan虚拟接口配置

no int vlan 1

然后为路由器2的0号端口设置ip地址

int g 0/0

ip add 192.168.1.1 255.255.255.0

exit

然后我们需要配置路由器2的静态路由

ip route 202.114.66.0 255.255.255.0 202.114.65.1

ip route 202.114.77.0 255.255.255.0 202.114.65.1

接下来需要为路由器2配置NAT转换，首先需要执行ip nat inside/outside将端口状态设置为内部端口还是外部端口

int g 0/1

ip nat outside

int g 0/0

ip nat inside

exit

然后执行命令ip nat pool <pool-id> <start-ip> <end-ip> netmask <子网掩码>创建NAT转换可用的IP池

ip nat pool mypool 202.114.65.5 202.114.65.12 netmask 255.255.255.0

然后执行命令ip nat inside source static <内部IP> <外部IP>静态配置NAT

ip nat inside source static 192.168.1.100 202.114.65.100

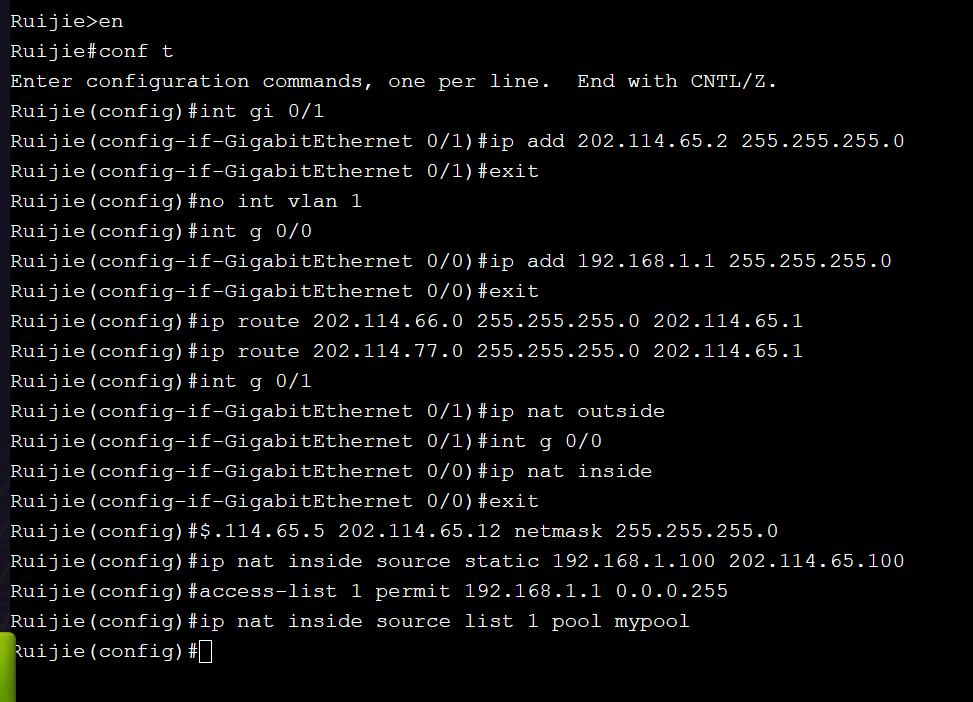
之后执行命令access-list <list-id> permit <网络地址> <子网掩码>来创建一个允许访问的IP列表

access-list 1 permit 192.168.1.1 0.0.0.255

 然后执行命令ip nat inside source <list-id> pool <pool-id>指定访问列表转换的目标IP池

ip nat inside source list 1 pool mypool

路由器2的完整配置指令如下图所示



### 5.3.3 配置路由器3

首先给路由器3的0号和1号端口配置ip地址

en

conf t

int g 0/0

ip add 192.168.2.1 255.255.255.0

no shutdown

exit

int g 0/1

ip add 202.114.66.2 255.255.255.0

no shutdown

exit

 然后为路由器3的两个端口配置静态路由

ip route 202.114.65.0 255.255.255.0 202.114.66.1

ip route 202.114.77.0 255.255.255.0 202.114.66.1

 然后创建命名访问控制列表

ip access-list standard 10

之后创建一个允许访问的IP列表

access-list 10 permit 192.168.2.0 0.0.0.255

exit

然后指令访问列表转换的目标ip池

ip nat inside source list 10 int g 0/1 overload

之后设置端口状态

int g 0/1

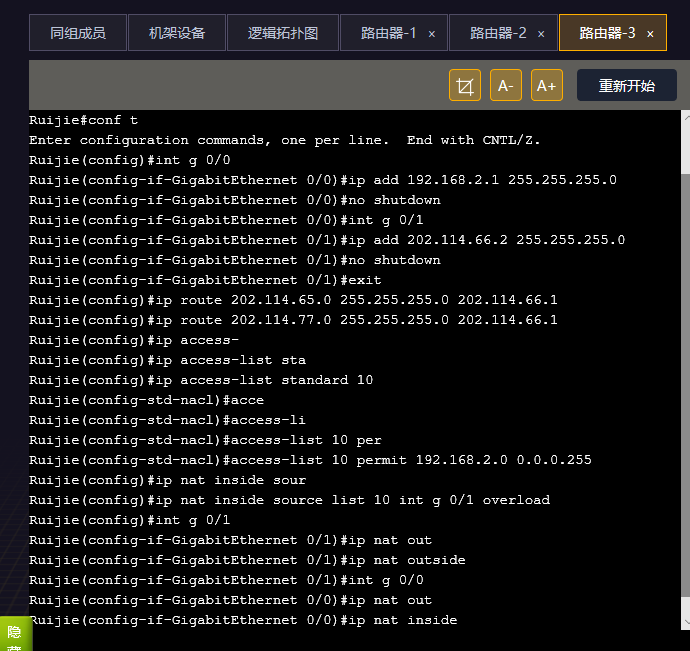
ip nat outside

int g 0/0

ip nat inside

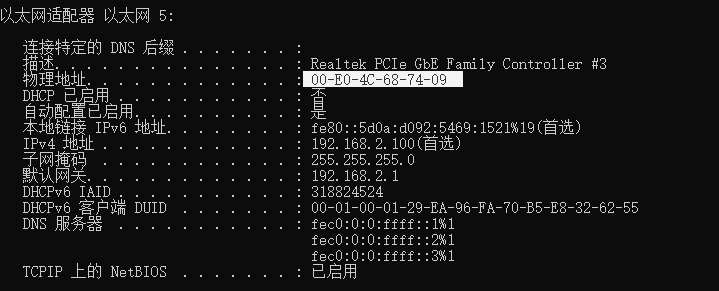
exit

路由器R3全部配置信息如下所示



### 5.3.4 二层交换机2配置

首先查看PC2以太网5的MAC地址如下



查看PC4以太网5的MAC地址如下



然后首先进入二层交换机2的3端口，执行指令switchport port-security激活端口安全；之后执行指令switchport port-security max <max-num>设置端口最大连接数为4；之后执行switchport port-security mac-address <PC4 MAC地址>设置端口允许的MAC地址

en

conf t

int g 0/3

switchport port-security

sw port-security maximum 4

switchport port-security mac-address 00E0.4C68.95E5

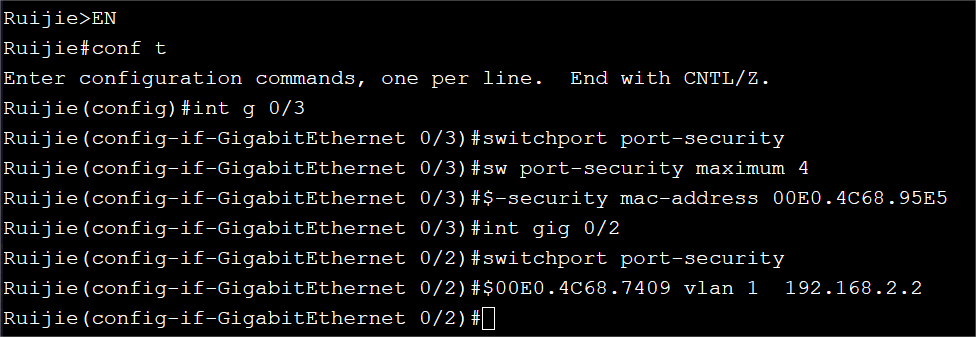
然后进入端口2，激活端口安全后执行指令switchport port-security binding <PC2 MAC地址> valn <vlan-id> <IP地址>设置端口安全的IP和MAC绑定

int gig 0/2

switchport port-security

switch port-security binding 00E0.4C68.7409 vlan 1 192.168.2.2

交换机配置信息如下所示



# 6 实验结果

## 6.1 查看路由表及NAT信息

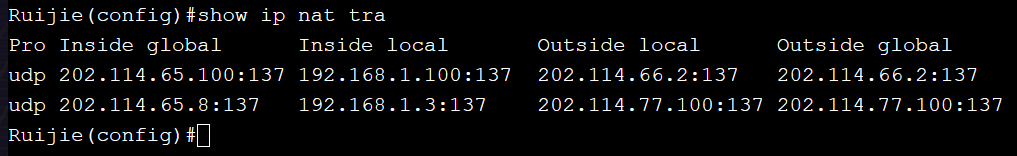
查看路由器1的路由协议和路由表如下所示，可以发现均为直连路由



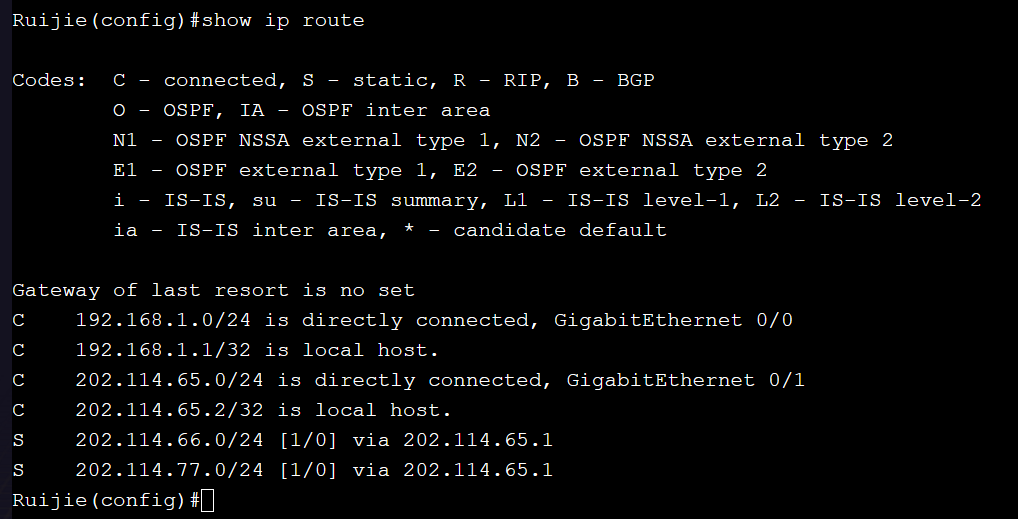
查看路由器1的NAT信息如下，因为在路由器1中并没有使用NAT协议，所以查看NAT信息应该不会有输出



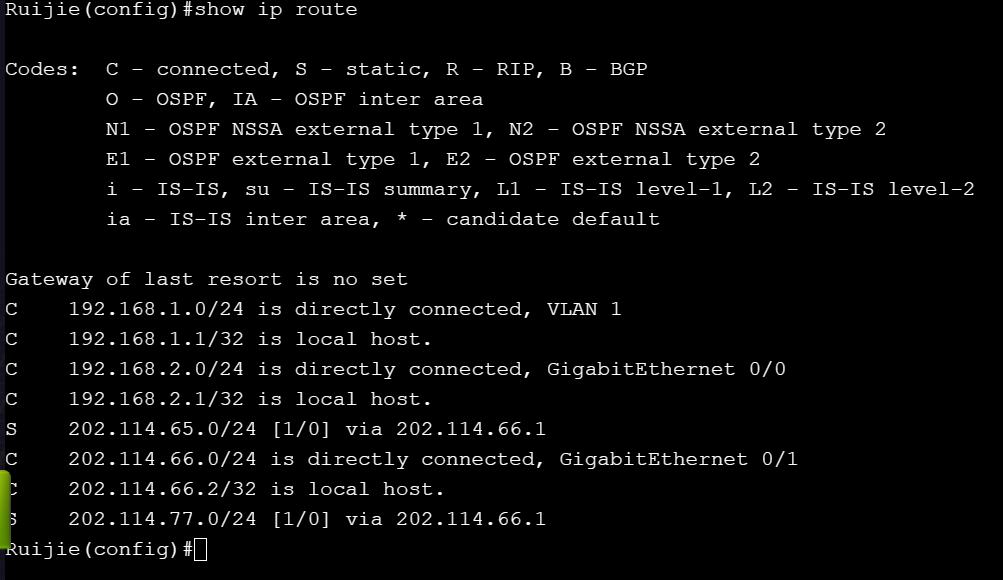
查看路由器Router2的NAT信息如下，可以看到内网主机192.168.1.3经过NAT转换之后，获取到IP池中的202.114.65.8地址，内网服务器2经过NAT转换之后获取到IP池中的202.114.65.100地址



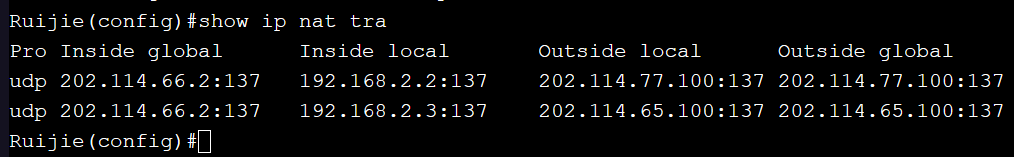
查看路由器2的路由协议即路由表如下，可以发现有静态路由和直连地址



查看路由器Router3的路由协议和路由表及NAT信息，与路由器2相同，都包含静态路由和之直连地址

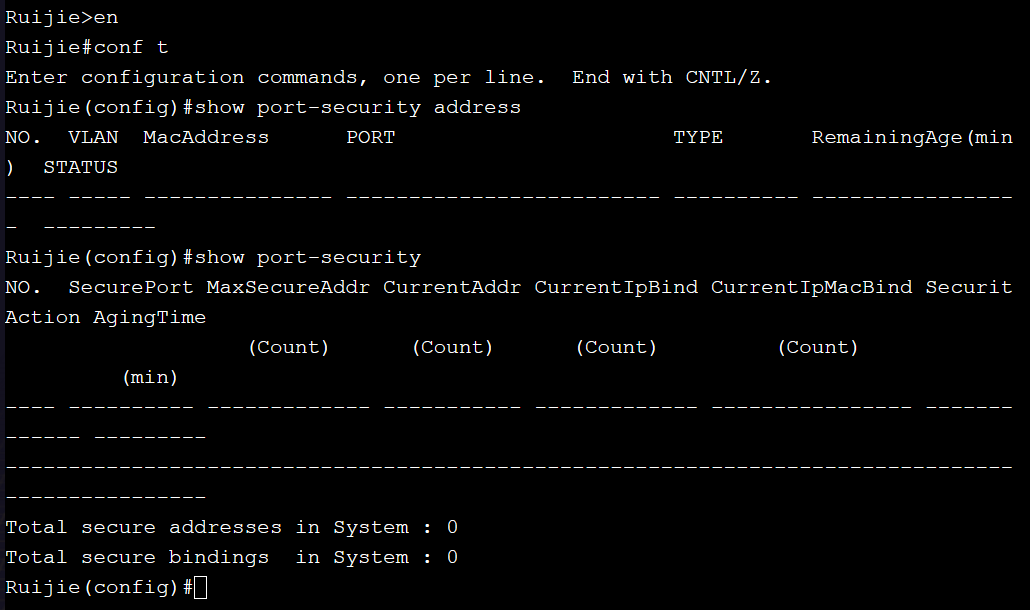


查看路由器3的NAT协议如下，内网主机192.168.2.2经过NAT协议之后获取到202.114.66.2地址；192.168.2.3经过NAT协议之后获取到202.114.66.2地址

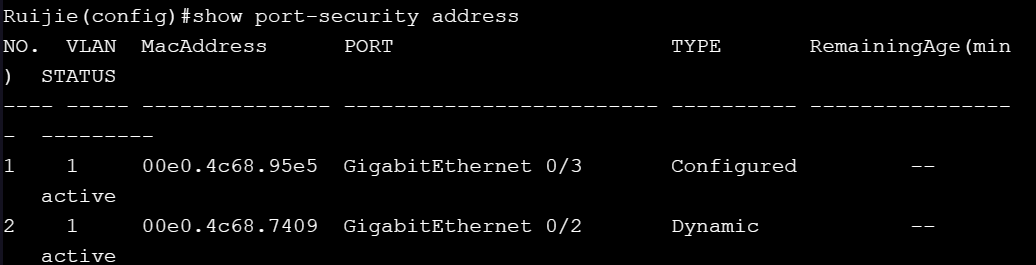


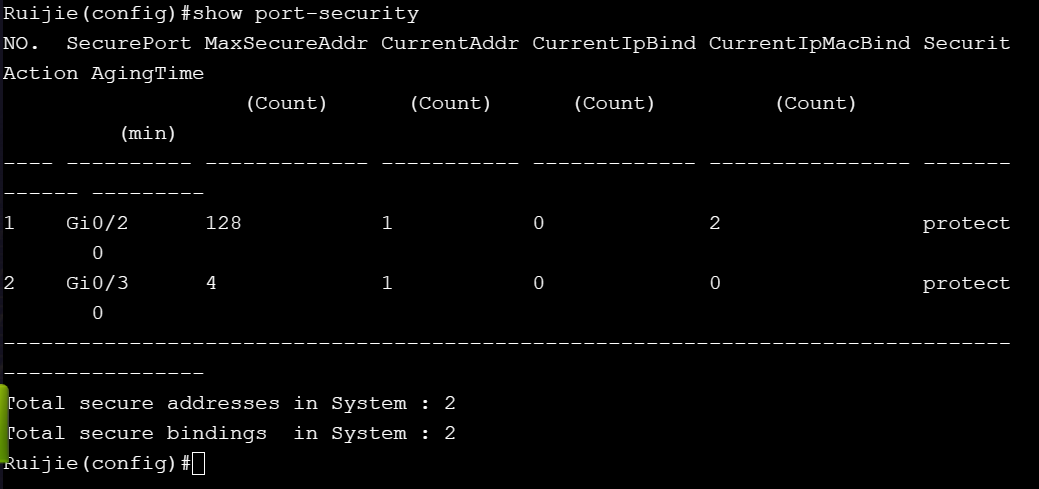
## 6.2 查看端口安全配置

查看二层交换机1开启端口安全配置



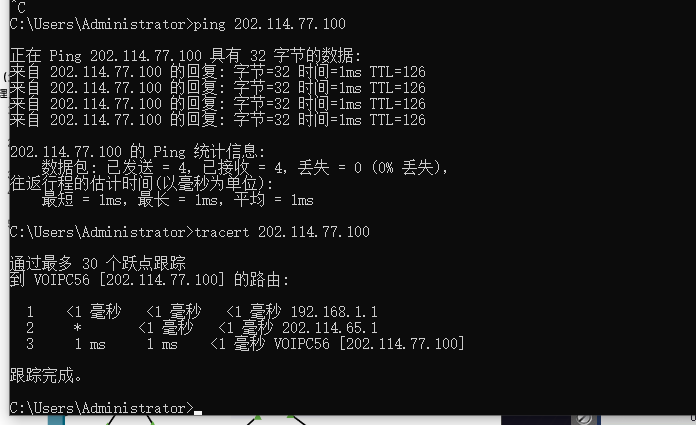
查看二层交换机2开启端口安全配置如下



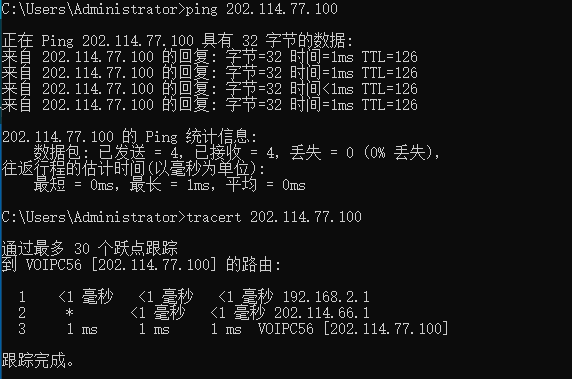


## 6.3 ping测试及访问服务器网站

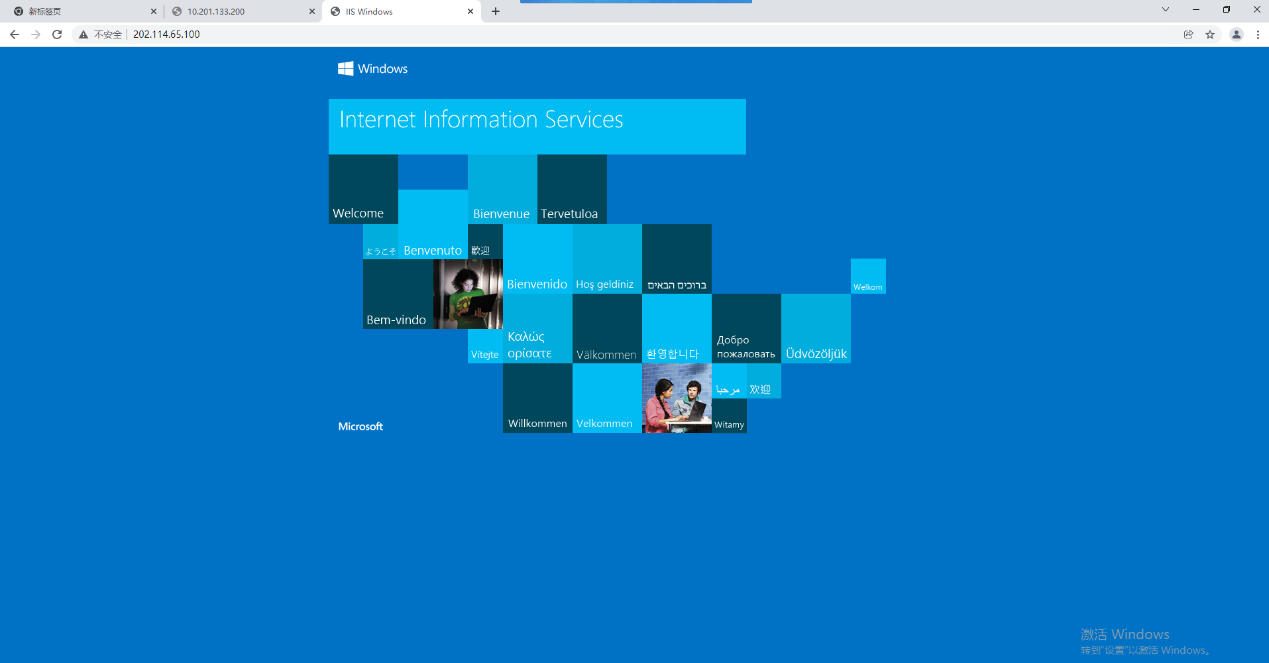
PC1->www1服务器



PC2->www1服务器



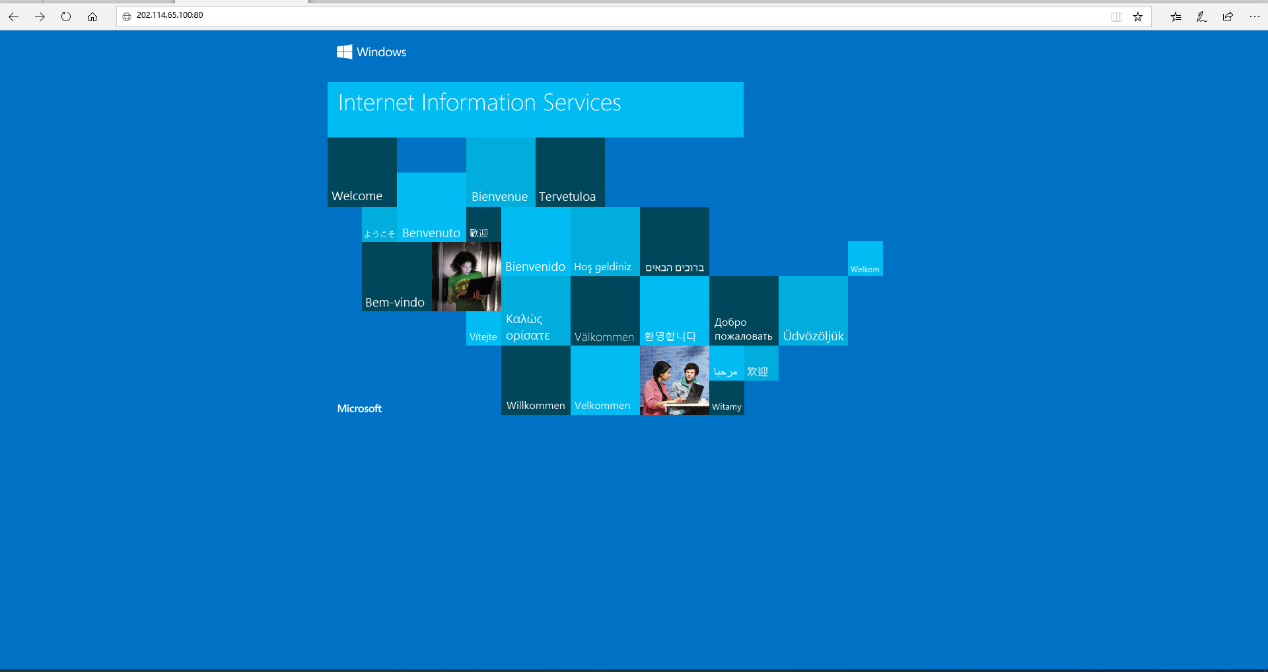
PC2访问www2服务器网站



PC4->www2服务器



PC4访问www2服务器



# 7 实验心得

在进行这次实验后，我对NAT（Network Address Translation，网络地址转换）有了更深入的理解。通过实践，我掌握了NAT的原理及配置方法，特别是对NAT源地址转换和目的地址转换的区别有了更清晰的认识。在实验中，我学会了如何配置NAT，使内部网络中的计算机能够与外部网络通信，并且实现了不同的转换需求，如通过IP地址池和端口映射的方式实现不同级别的访问权限控制。

此外，通过配置NAT，我还学会了如何向外网发布内网的服务器，这对于企业网络中的服务提供商来说是非常重要的。我了解到NAT技术能够有效地解决IPv4地址不足的问题，同时提高了网络的安全性和隔离性。

在实验过程中，我还学习了静态路由的配置方法，以及如何查看路由表和NAT信息，这对于理解网络通信的流程和排错非常有帮助。通过实验，我进一步认识到网络安全的重要性，特别是在配置NAT端口安全时，需要注意访问控制列表、端口范围、会话限制等安全策略的配置和管理，以保护网络免受各种攻击和滥用。