

## 《信息安全及实践》课程实验报告

学院： 信息学院    专业： 计算机科学与技术    年级： 2019

姓名： 李泽昊                      学号： 20191060065

姓名： 白文强                      学号： 20191060064

姓名： 赵浩杰                      学号： 20191060074

实验时间： 2021 年 12 月 2 日

实验名称： OSPF 路由项欺骗攻击和防御实验和 NAT 实验

实验成绩：

---



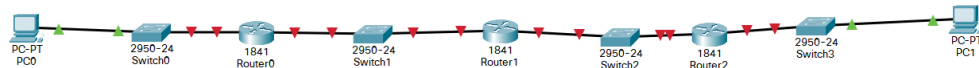
# OSPF 路由项欺骗攻击和防御实验

## 一、实验目的

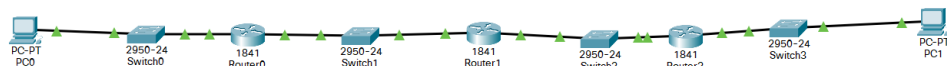
- (1)验证路由器 OSPF 配置过程。
- (2)验证 OSPF 建立动态路由项过程。
- (3)验证 OSPF 路由项欺骗攻击过程。
- (4)验证 OSPF 源端鉴别功能的配置。
- (5)验证 OSPF 防路由项欺骗攻击功能的实现过程。

## 二、实验步骤

- (1)完成去掉入侵路由器的网络结构放置和连接设备。



- (2)完成各设备配置和路由器 OSPF 配置，完成配置后生成路由表。



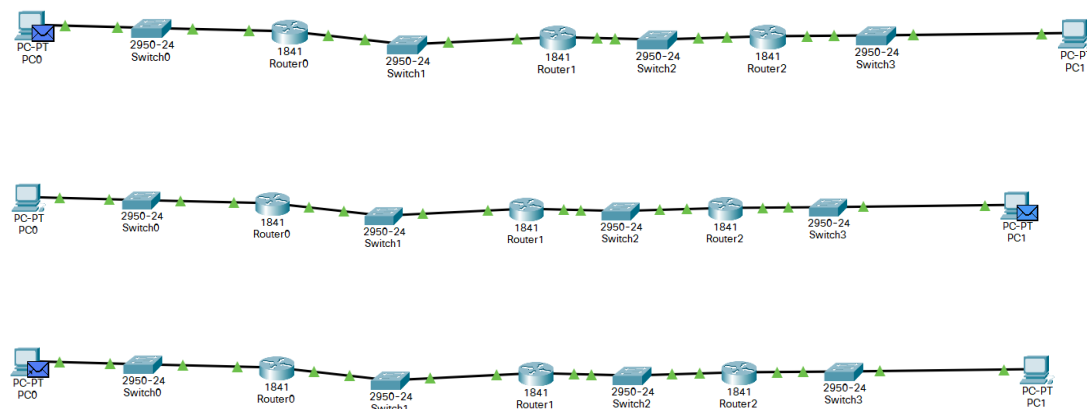
Router0 路由表:

```
Gateway of last resort is not set

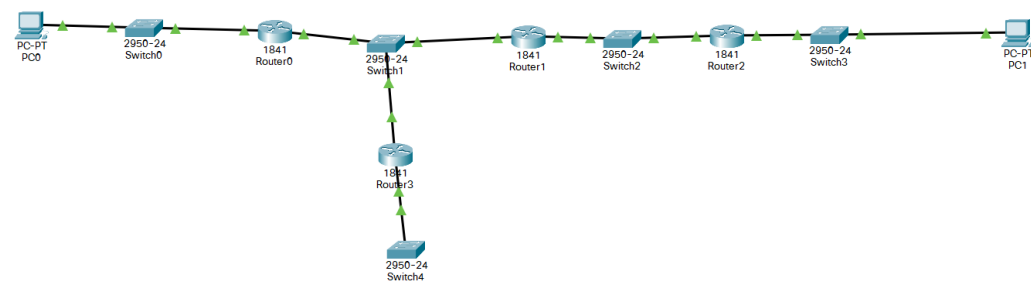
C    192.1.1.0/24 is directly connected, FastEthernet0/0
C    192.1.2.0/24 is directly connected, FastEthernet0/1
O    192.1.3.0/24 [110/2] via 192.1.2.253, 00:03:13, FastEthernet0/1
O    192.1.4.0/24 [110/3] via 192.1.2.253, 00:03:03, FastEthernet0/1

Router#
```

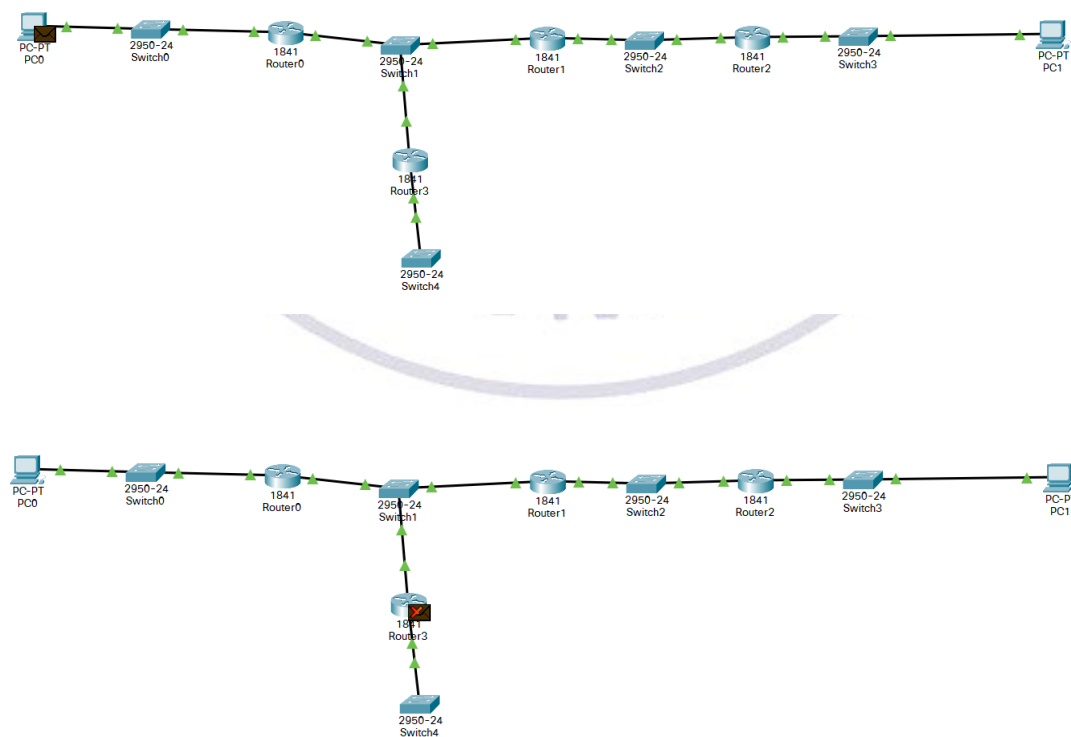
(3) 切换到模拟操作模式，启动 PC0 和 PC1 的 ICMP 报文传输过程。



(4) 加入入侵路由器，并配置 OSPF 协议。



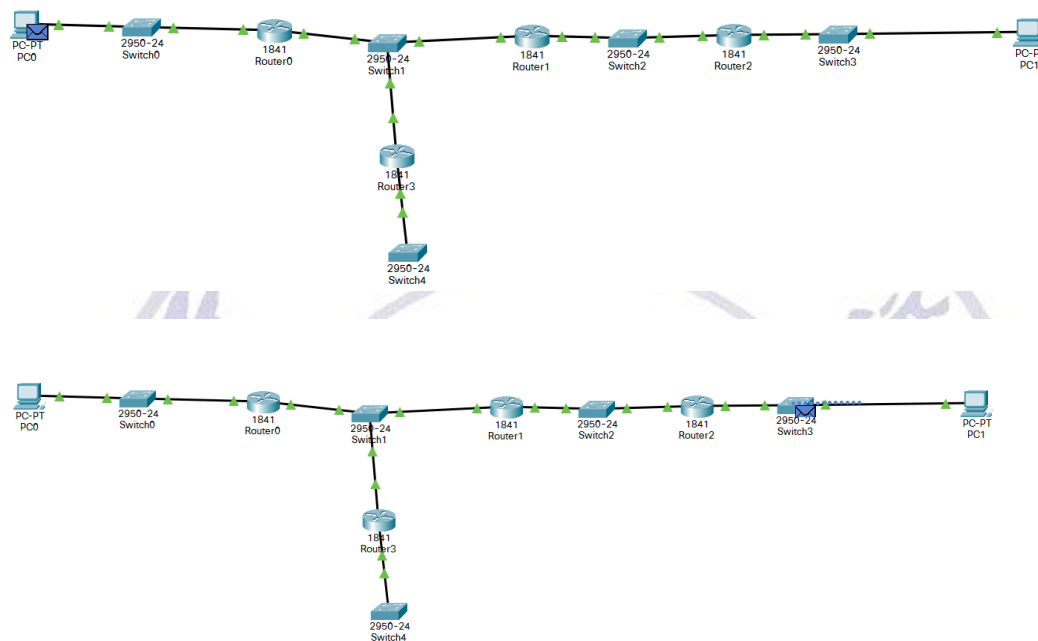
(5) 通过简单报文工具启动 PC0 到 PC1 的 ICMP 报文传输过程。



(6) 在 CLI 命令下配置三个路由器的源鉴别和完整性检测功能的配置，为相邻路由器配置相同的密钥，查看 R0 的路由表。

```
C 192.1.1.0/24 is directly connected, FastEthernet0/0
C 192.1.2.0/24 is directly connected, FastEthernet0/1
O 192.1.3.0/24 [110/2] via 192.1.2.253, 00:00:08, FastEthernet0/1
O 192.1.4.0/24 [110/3] via 192.1.2.253, 00:00:08, FastEthernet0/1
```

(7) 验证 ICMP 报文传输过程。



实验结果验证鉴别成功，成功在入侵路由器干扰下实现 PC0 和 PC1 的通信过程。

### 三、实验结果及分析

在未加入路由器的情况下连接设备并设置完 IP 地址后，配置 OSPF 协议。

随后在模拟操作模式进行 PC0 和 PC1 之间的 ICMP 通信，可以看到，ICMP 报文从 PC0 到 PC1，再由 PC1 到达 PC1，证明本次 ICMP 通信正常。

加入入侵路由器后，将路由器远端配置好和 192.1.4.0 一样的子网，通过路由欺骗进行攻击，发现 PC0 送往 PC1 的报文被截获。

为了防止 OSPF 路由项欺骗，通过设置在路由器上的源端鉴别协议，通过鉴别报文来源和密钥是否匹配进行传输，可以防止路由项欺骗协议，最后发现 PC0 到 PC1 的报文通信正常。

#### 四、实验总结及体会

在实验中并未遇到比较棘手的困难，遇到的最大问题是第一次做实验的时候，设置好 OSPF 协议都不能通信，尝试了各种方法也不行，但是关掉软件，重新配置过一次后，发现可以正常通信，我怀疑是因为在第一次配置 OSPF 的地方某个小地方出现了错误，导致整个区块的 OSPF 不能正常通畅。

防止路由项欺骗的原理其实很简单，通过鉴别双方共同的密钥是否正确，是否一致来判断你是否是消息的真正接收方，但是同样也有缺点，如果密钥被破解，那么这个源端鉴别协议将不再安全。



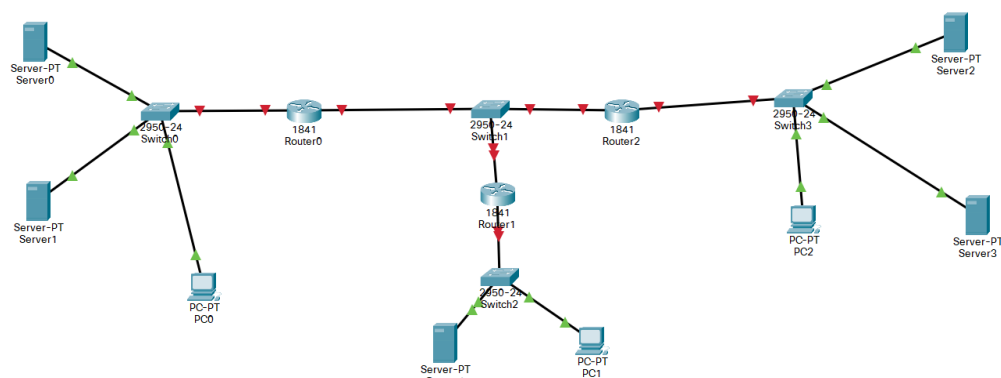
# NAT 实验

## 一、实验目的

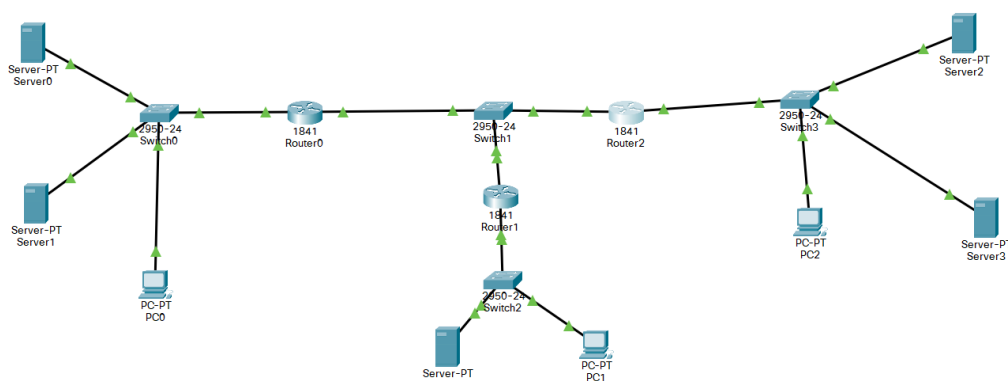
- (1) 理解“内部网络对于外部网络是透明的”的含义。
- (2) 验证动态 NAT 实现过程。
- (3) 验证静态 NAT 实现过程。
- (4) 验证动态 NAT 配置过程
- (5) 验证静态 NAT 配置过程
- (6) 验证 NAT 的安全性。

## 二、实验步骤

- (1) 完成内部网络和外部网络的设备放置和连接。



- (2) 完成各个设备接口 IP、子网掩码配置，RIP 协议配置、静态路由项的配置。



Route0:

## IOS Command Line Interface

```
% Invalid input detected at '^' marker.

Router(config)#access-list 1 deny any
Router(config)#ip nat pool a1 192.1.3.1 192.1.3.12 netmask 255.255.255.240
Router(config)#ip nat inside source list 1 pool a1
Router(config)#
Router(config)#
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.1.1.0/24 is directly connected, FastEthernet0/1
R    192.1.2.0/24 [120/1] via 192.1.1.252, 00:00:27, FastEthernet0/1
     192.1.3.0/28 is subnetted, 1 subnets
S       192.1.3.16 [1/0] via 192.1.1.253
C    192.168.1.0/24 is directly connected, FastEthernet0/0

Router#
```

## Router1

## IOS Command Line Interface

```
% Invalid input detected at '^' marker.

Router(config-router)#exit
Router(config)#ip route 192.1.3.0 255.255.255.240 192.1.1.254
Router(config)#ip route 192.1.3.16 255.255.255.240 192.1.1.253
Router(config)#
Router(config)#
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

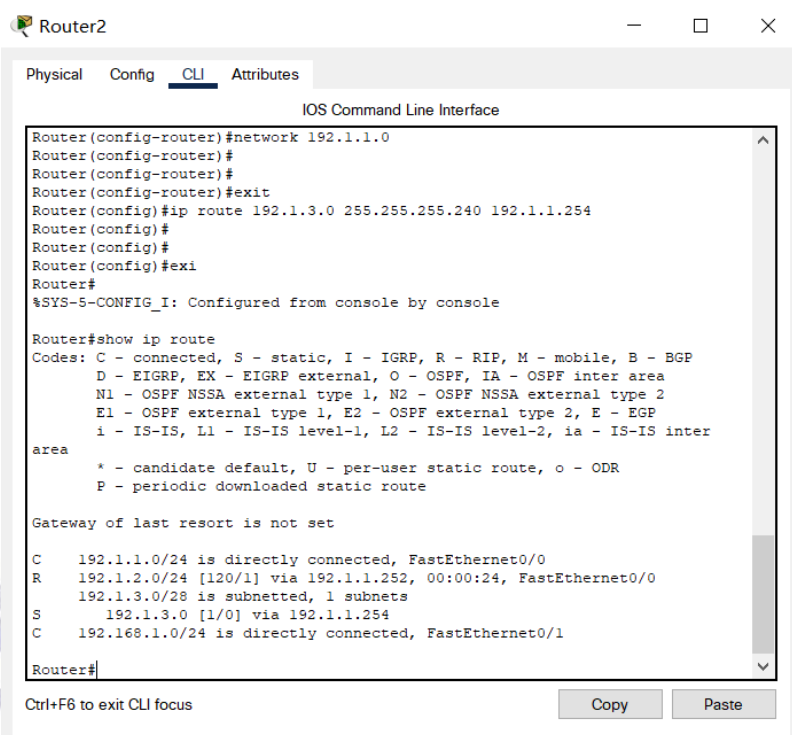
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.1.1.0/24 is directly connected, FastEthernet0/0
C    192.1.2.0/24 is directly connected, FastEthernet0/1
     192.1.3.0/28 is subnetted, 2 subnets
S       192.1.3.0 [1/0] via 192.1.1.254
S       192.1.3.16 [1/0] via 192.1.1.253

Router#
```

## Router2:



The screenshot shows the Router2 CLI interface with the following content:

```
Router2
Physical Config CLI Attributes
IOS Command Line Interface

Router(config-router)#network 192.1.1.0
Router(config-router)#
Router(config-router)#
Router(config-router)#exit
Router(config)#ip route 192.1.3.0 255.255.255.240 192.1.1.254
Router(config)#
Router(config)#
Router(config)#exi
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

C    192.1.1.0/24 is directly connected, FastEthernet0/0
R    192.1.2.0/24 [120/1] via 192.1.1.252, 00:00:24, FastEthernet0/0
    192.1.3.0/28 is subnetted, 1 subnets
S        192.1.3.0 [1/0] via 192.1.1.254
C    192.168.1.0/24 is directly connected, FastEthernet0/1

Router#
```

Ctrl+F6 to exit CLI focus

Copy Paste

(3)完成各个服务器和终端的网络信息配置。

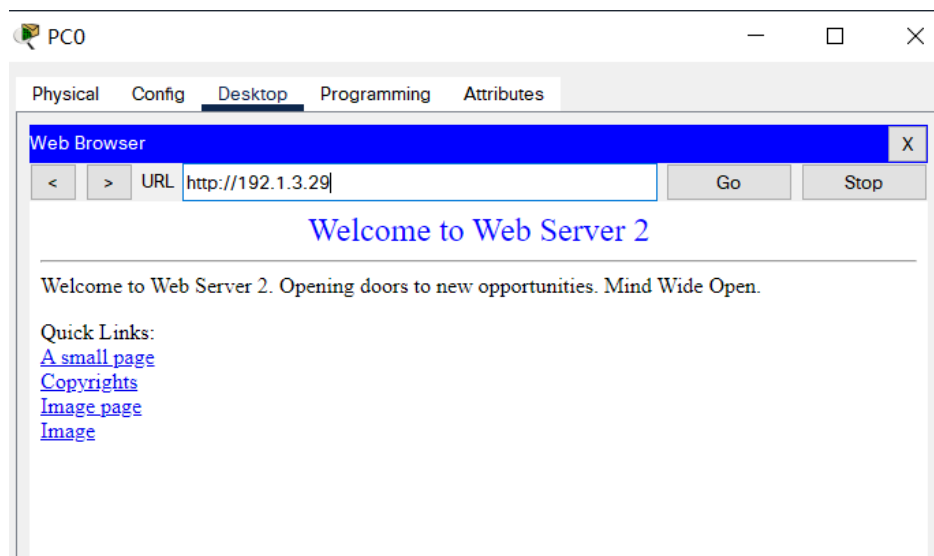
(4)完成两个路由器的地址池的建立，建立全球 IP 地址和服务器私有地址的静态映射。

```
Enter Configuration Commands, one per line. End with Ctrl+Z.
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#access-list 1 deny any
Router(config)#ip nat pool a1 192.1.3.1 192.1.3.12 netmask 255.255.255.240
Router(config)#ip nat inside source list 1 pool a1
Router(config)#ip nat inside source static 192.168.1.3 192.1.3.13
Router(config)#ip nat inside source static 192.168.1.7 192.1.3.14
Router(config)#int f0/0
Router(config-if)#ip nat inside
Router(config-if)#int f0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#
```

```
Enter Configuration Commands, one per line. End with Ctrl+Z.
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#access-list 1 deny any
Router(config)#ip nat pool b1 192.1.3.17 192.1.3.28 netmask 255.255.255.240
Router(config)#ip nat inside source list 1 pool b1
Router(config)#ip nat inside source static 192.168.1.3 192.1.3.29
Router(config)#ip nat inside source static 192.168.1.7 192.1.3.30
Router(config)#int f0/1
Router(config-if)#ip nat inside
Router(config-if)#int f0/0
Router(config-if)#ip nat outside
Router(config-if)#
```

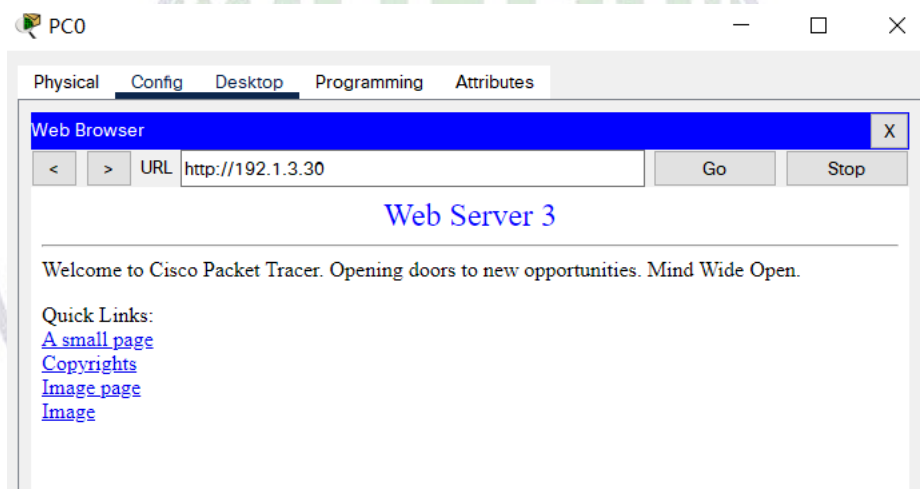


(5)PC0 用全球 IP 地址 192.1.3.29 访问私有 IP 地址 192.168.1.3 的 web2 界面。



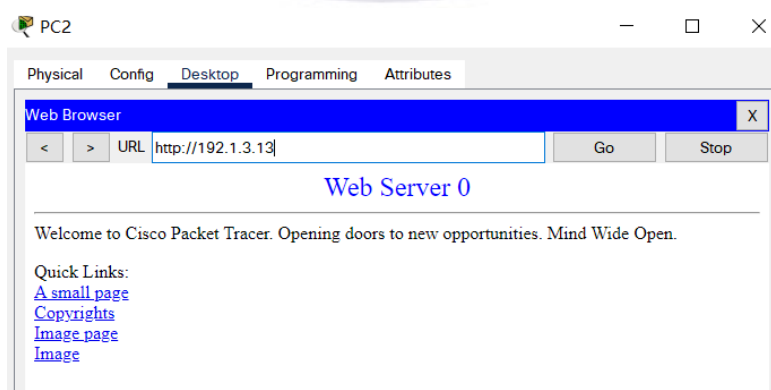
Web2 界面

PC0 用全球 IP 地址 192.1.3.30 访问私有 IP 地址为 192.168.1.7 的 Web3 界面

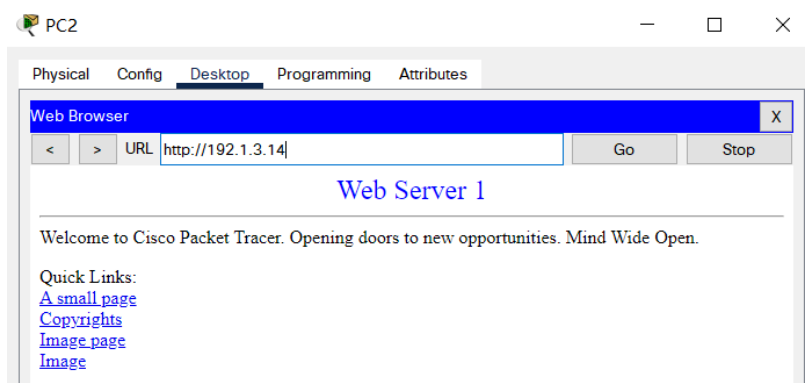


Web3 界面

PC2 用全球 IP 地址 192.1.3.13 访问私有 IP 地址为 192.168.1.3 的 Web1 界面



PC2 用全球 IP 地址 192.1.3.14 访问私有 IP 地址为 192.168.1.7 的 Web2 界面



(6)PC0 用全球 IP 地址 192.1.3.29 和 192.1.30 分别访问私有 IP 地址为 192.168.1.3 和 192.168.1.7 的两个 web 后，路由器 0 的 NAT 表如下图所示

```
Router#sh ip nat tra
```

Pro	Inside global	Inside local	Outside local	Outside global
---	192.1.3.13	192.168.1.3	---	---
---	192.1.3.14	192.168.1.7	---	---
tcp	192.1.3.1:1025	192.168.1.1:1025	192.1.3.29:80	192.1.3.29:80
tcp	192.1.3.1:1026	192.168.1.1:1026	192.1.3.29:80	192.1.3.29:80
tcp	192.1.3.1:1027	192.168.1.1:1027	192.1.3.29:80	192.1.3.29:80
tcp	192.1.3.1:1028	192.168.1.1:1028	192.1.3.29:80	192.1.3.29:80
tcp	192.1.3.1:1030	192.168.1.1:1030	192.1.3.30:80	192.1.3.30:80
tcp	192.1.3.13:80	192.168.1.3:80	192.1.3.17:1025	192.1.3.17:1025
tcp	192.1.3.14:80	192.168.1.7:80	192.1.3.17:1026	192.1.3.17:1026

路由器 2 的转换表如下图所示

```
Router#show ip nat tra
```

Pro	Inside global	Inside local	Outside local	Outside global
---	192.1.3.29	192.168.1.3	---	---
---	192.1.3.30	192.168.1.7	---	---
tcp	192.1.3.17:1025	192.168.1.2:1025	192.1.3.13:80	192.1.3.13:80
tcp	192.1.3.17:1026	192.168.1.2:1026	192.1.3.14:80	192.1.3.14:80
tcp	192.1.3.29:80	192.168.1.3:80	192.1.3.1:1025	192.1.3.1:1025
tcp	192.1.3.29:80	192.168.1.3:80	192.1.3.1:1026	192.1.3.1:1026
tcp	192.1.3.29:80	192.168.1.3:80	192.1.3.1:1027	192.1.3.1:1027
tcp	192.1.3.29:80	192.168.1.3:80	192.1.3.1:1028	192.1.3.1:1028
tcp	192.1.3.30:80	192.168.1.7:80	192.1.3.1:1030	192.1.3.1:1030

(7)PC0 通过浏览器访问 Web Server2 产生的 IP 分组分别由路由器 R0 和 R2 完成 NAT 过程，查看各路由器中的分组格式。

# PDU Information at Device: Switch0

OSI Model   Inbound PDU Details   **Outbound PDU Details**

## PDU Formats

EthernetII																Bytes							
PREAMBLE: 101010...10										SF D		DEST ADDR:0006.2A38.CD01											
SRC ADDR:0002.161D.8						TY PE		DATA (VARIABLE LENGTH)						FCS:0x00000000									
IP																Bits							
VER:4		IHL:5				DSCP:0x00						TL:29											
ID:0x0039										FLAGS:0x0				FRAG OFFSET:0x000									
TTL:32						PRO:0x01						CHKSUM											
SRC IP:192.168.1.1																							
DST IP:192.1.3.29																							
DATA (VARIABLE LENGTH)																							

PC0 至 R0

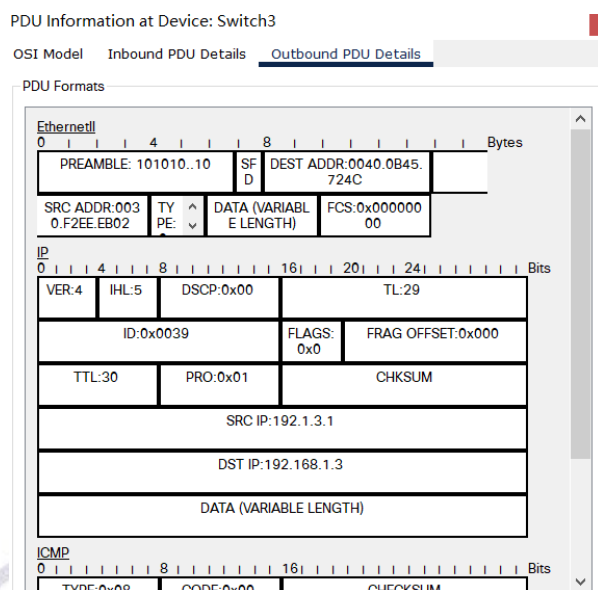
# PDU Information at Device: Switch1

OSI Model   Inbound PDU Details   **Outbound PDU Details**

## PDU Formats

EthernetII																Bytes									
PREAMBLE: 101010...10								SF D		DEST ADDR:0030.F2EE.EB01															
SRC ADDR:0006.2A38.C				TY PE		DATA (VARIABLE LENGTH)								FCS:0x00000000											
IP																Bits									
VER:4				IHL:5				DSCP:0x00								TL:29									
ID:0x0039								FLAGS:0x0				FRAG OFFSET:0x000													
TTL:31				PRO:0x01				CHKSUM																	
SRC IP:192.1.3.1																									
DST IP:192.1.3.29																									
DATA (VARIABLE LENGTH)																									
ICMP																Bits									
TYPE:8				CODE:0				CHECKSUM																	

R0 至 R2



## R2 至服务器

### 三、实验结果及分析

首先通过建立两个内部网路和一个外部网，建立三个路由器，分别设置好各自路由的 RIP 协议，保证外部网络的通畅。

其次通过设置全球地址池，给内部网络映射到全球地址的空间。

最后通过设置动态 NAT 和静态 NAT，实现内部网络终端访问外部网络的过程，实现外部网络的终端和其他内部网络的终端访问某个内部网络的 Web 服务器的过程。

### 四、实验总结及体会

本次实验的易错点在于静态路由项的设置，由于外部网络采用的 RIP 协议无法连接到内部网络，因此当内部网路的地址想要访问外部网络并进行通信时，需要进行静态路由项的设置，当有任意一个静态路由项未设置成功，都有可能导致实验失败。

学会如何更好地利用动态 NAT 协议和静态 NAT 协议，才能更好地搭建一个映射的网络环境，才能保证内部网路与外部网络的正常通信。