目录

计算机网络实践八

一、 实验目的及内容

1.1 实验内容

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

网络拓扑图如下:

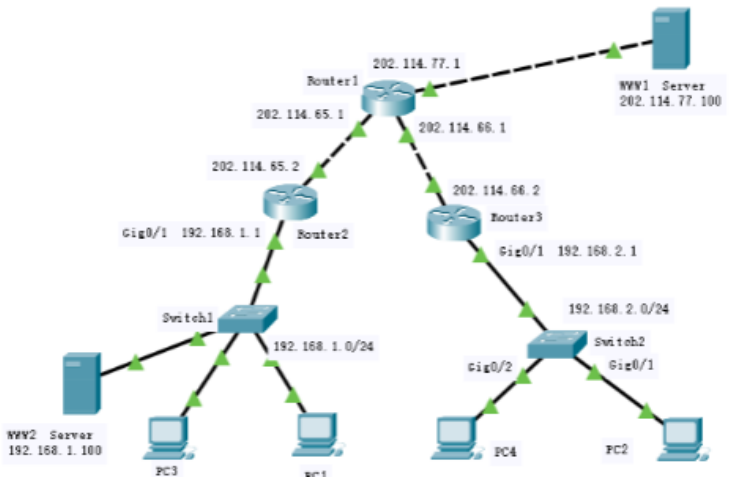

图 1: 网络拓扑图

1.2 实验要求

1. 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
2. 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
3. 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

二、 实验原理

2.1 NAT

2.1.1 定义

NAT（Network Address Translator，网络地址转换）是用于在本地网络中使用私有地址，在连接互联网时转而使用全局 IP 地址的技术。NAT 实际上是为解决 IPv4 地址短缺而开发的技术。

2.1.2 类型

1. 静态 NAT: 内部本地地址一对一转换成内部全局地址，相当内部本地的每一台 PC 都绑定了一个全局地址。一般用于在内网中对外提供服务的服务器
2. 动态 NAT: 在内部本地地址转换的时候，在地址池中选择一个空闲的，没有正在被使用的地址，来进行转换，一般选择的是在地址池定义中排在前面的地址，当数据传输或者访问完成时就会放回地址池中，以供内部本地的其他主机使用，但是，如果这个地址正在被使用的时候，是不能被另外的主机拿来进行地址转换的
3. 端口复用 NAPT：面对私网内部数量庞大的主机，如果 NAT 只进行 IP 地址的简单替换，就会产生一个问题：当有多个内部主机去访问同一个服务器时，从返回的信息不足以区分响应应该转发到哪个内部主机。此时，需要 NAT 设备根据传输层信息或其他上层协议去区分不同的会话，并且可能要对上层协议的标识进行转换，比如 TCP 或 UDP 端口号。这样 NAT 网关就可以将不同的内部连接访问映射到同一公网 IP 的不同传输层端口，通过这种方式实现公网 IP 的复用和解复用。这种方式也被称为端口转换 PAT、NAPT 或 IP 伪装，但更多时候直接被称为 NAT，因为它是最典型的一种应用模式。

2.2 端口安全

端口安全（Port Security），从基本原理上讲，Port Security 特性会通过 MAC 地址表记录连接到交换机端口的以太网 MAC 地址（即网卡号），并只允许某个 MAC 地址通过本端口通信。其他 MAC 地址发送的数据包通过此端口时，端口安全特性会阻止它。使用端口安全特性可以防止未经允许的设备访问网络，并增强安全性。另外，端口安全特性也可用于防止 MAC 地址泛洪造成 MAC 地址表填满。

三、 实验步骤

3.1 分配端口并连线

根据设备分配端口信息，新的拓扑图如下：

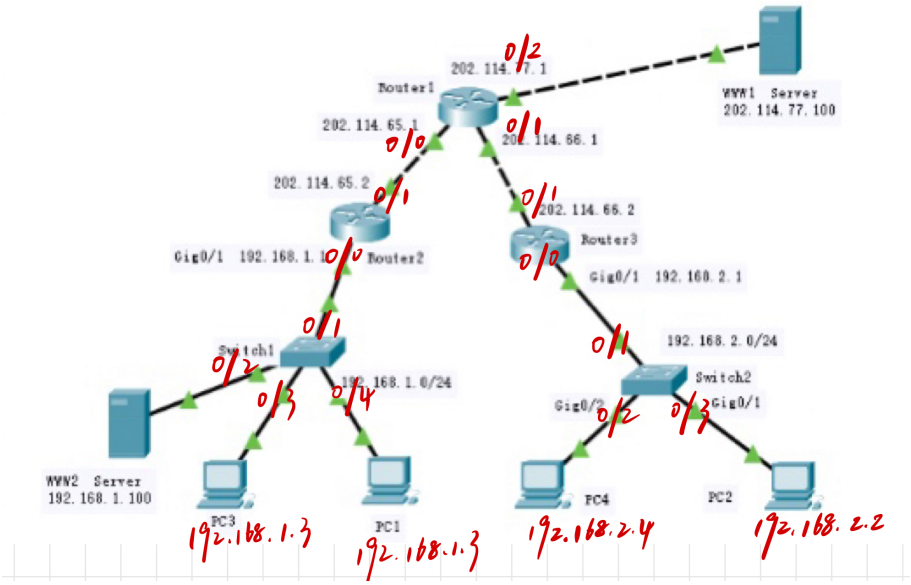

图 2: 网络拓扑图

物理连线如下:

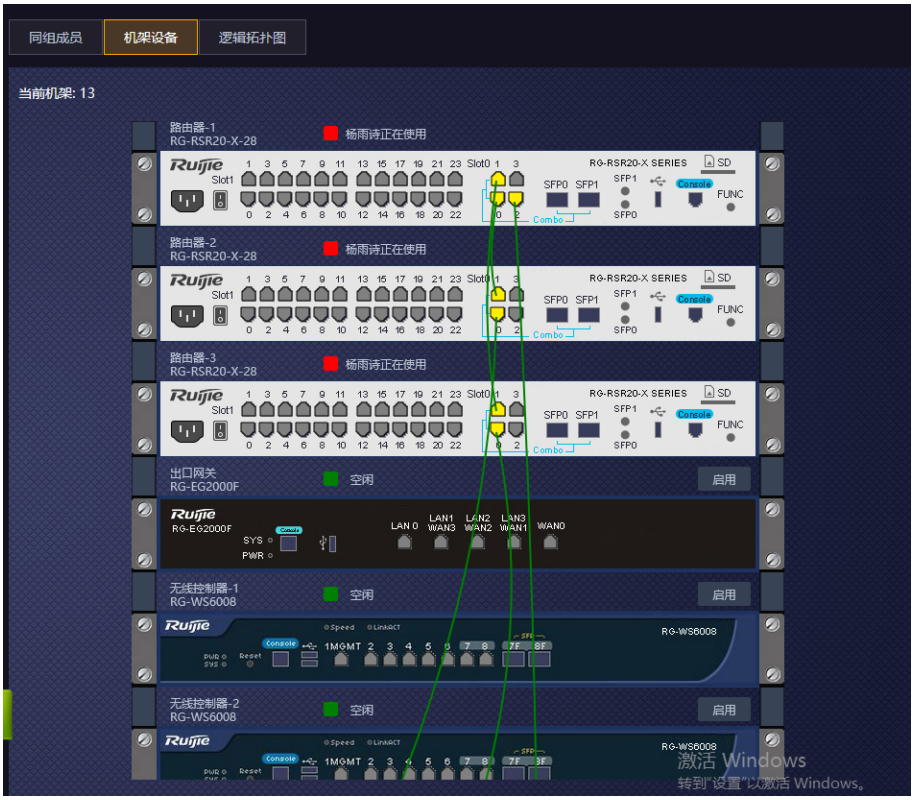

图 3: 物理连线

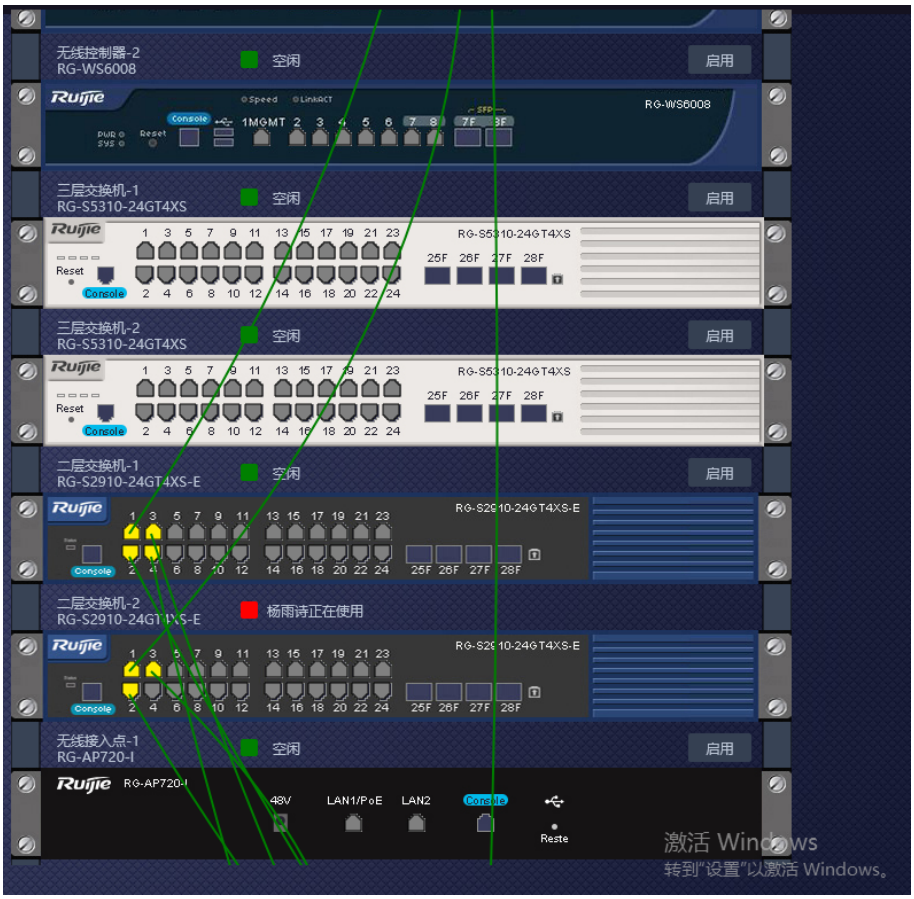

图 4: 物理连线续

3.2 路由器 1

路由器 1 仅仅连接了 2 个路由器，它只需要实现一个简单路由功能，配置命令如下：

```
en
con
int g 0/0
ip addr 202.114.65.1 255.255.255.0
int g 0/1
ip addr 202.114.66.1 255.255.255.0
int g 0/2
ip addr 202.114.77.1 255.255.255.0
```

3.3 路由器 2

对于路由器 2，首先配置路由器 2 的各接口 IP，然后定义 IP 池，并定义 nat 的内网和外网位置。接下来指明只有 192.168.1.0 网段的计算机通过 IP 池上网。通过 ip nat inside source static tcp 命令将 WWW2 服务器的内网地址转换为外网地址，最后设置默认路由即可。

```
Ruijie(config)#int g 0/1
Ruijie(config-if-GigabitEthernet 0/1)#ip nat outside
Ruijie(config-if-GigabitEthernet 0/1)#int g 0/0
Ruijie(config-if-GigabitEthernet 0/0)#ip nat inside
Ruijie(config-if-GigabitEthernet 0/0)#exit
Ruijie(config)#access-list 1 permit 192.168.1.1 0.0.0.255
failed, for the entry is existed or the sequence number has been allocated!
Ruijie(config)#$.114.65.5 202.114.65.12 netmask 255.255.255.0
Ruijie(config)#ip nat inside source list 1 pool mypool
 Translation with list 1 exist,please delete and recreate
Ruijie(config)#ip nat inside source static 192.168.1.100 202.114.65.100
 202.114.65.100 already mapped (192.168.1.100 -> 202.114.65.100)
Ruijie(config)#
```

图 5: 配置 nat

```
Ruijie(config)#int g 0/1
Ruijie(config-if-GigabitEthernet 0/1)#ip add 202.114.65.2 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)#int g 0/0
Ruijie(config-if-GigabitEthernet 0/0)#ip add 192.168.1.1 255.255.255.0
Primary IP address conflict with "VLAN 1".
Ruijie(config-if-GigabitEthernet 0/0)#ip add 192.168.3.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#int vlan1
Ruijie(config-if-VLAN 1)#no ip addr
%notice: all IPv4 addresses on this interface are removed.

Ruijie(config-if-VLAN 1)#exit
Ruijie(config)#int g 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no ip add 192.168.3.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#int g 0/0
Ruijie(config-if-GigabitEthernet 0/0)#ip add 192.168.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#no shutdown
Ruijie(config-if-GigabitEthernet 0/0)#exit
```

图 6: 配置 ip 池

然后显示 ip 路由和转换的统计信息:

```
Gateway of last resort is no set
C    192.168.1.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.1.1/32 is local host.
C    202.114.65.0/24 is directly connected, GigabitEthernet 0/1
C    202.114.65.2/32 is local host.
S    202.114.66.0/24 [1/0] via 202.114.65.1
S    202.114.77.0/24 [1/0] via 202.114.65.1
```

图 7: 路由器 2ip 路由

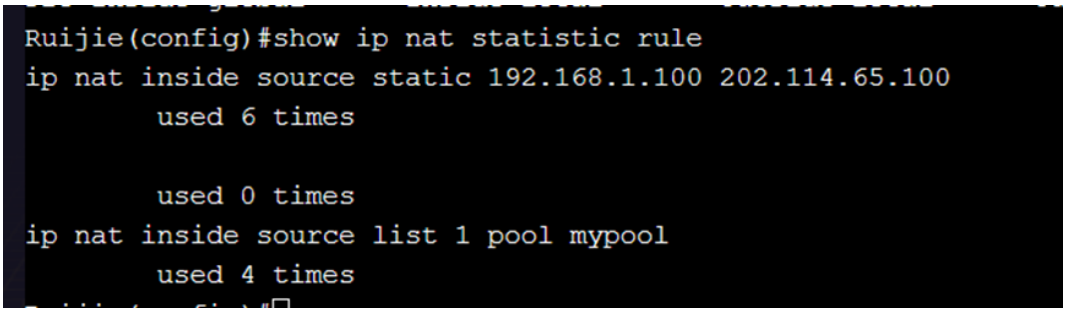

图 8: 转换的统计结果

3.4 路由器 3

路由器 3 的 0/1 端口连接的是公网路由，0/0 部分连接的是 NAT 路由（需要进行 NAT）配置。

0/1 端口配置:

```
en
con
int g 0/1
ip addr 202.114.66.2 255.255.255.0
```

0/0 端口需要 PC 机通过共享的 IP 地址进行公网访问，我们选择的方法是构建一个只包含 IP 202.114.66.2 的 IP 池，然后通过将该 IP 池连接到相应的 access list 中实现共享 IP 地址。

在 ip nat inside 配置中，list 的名称和 pool 的名称需要和前面设置相对应。

```
int g 0/1
ip nat outside
int g 0/0
ip nat inside
access-list 10 permit 192.168.2.0 0.0.0.255
ip nat pool router3 202.114.66.2 202.114.66.2 netmask 255.255.255.0
ip nat inside source list 10 pool router3
```

最后为路由器 3 添加静态路由信息。

```
ip route 202.114.65.0 202.114.66.1
ip route 202.114.77.0 202.114.66.1
```

3.5 交换机 1

本实验交换机 1 没有特殊要求，仅做交换功能使用，因此无需配置。

3.6 交换机 2

实验要求在交换机 Switch2 中配置端口安全：
设置 0/3 端口只允许 PC2 使用 192.168.2.100 访问，我们首先查看一下 PC2 的 MAC 地址：

图 9: PC2 的网络配置信息

然后我们使用 switchport port-security 将 PC2 的 mac 地址与 192.168.2.100 绑定，具体的指令实现如下所示：

```
switchport port-security binding 00e0.4c68.8f4d vlan 10 192
    .168.2.100
```

配置的过程如下图所示：

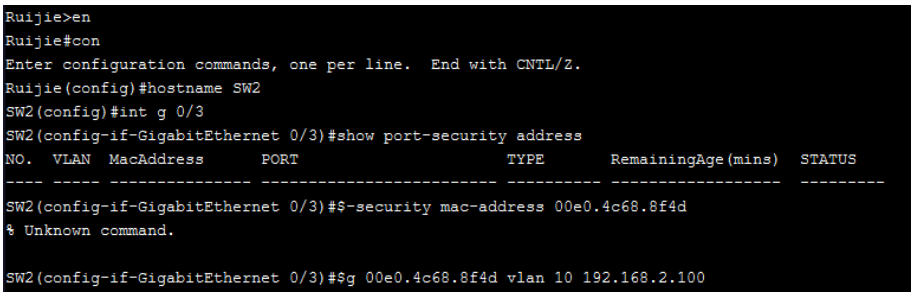

图 10: 设置 0/3 端口仅允许 PC2 使用 192.168.2.100 访问

设置 0/2 端口只允许 PC4 等至多 4 台机器访问

```
sw port-security binding 192.168.2.4
sw port-security maximum 4
```

先将 0/2 端口与 PC2 的 IP 绑定，然后设置最大数量为 4，具体的配置过程如下图所示：

```
SW2(config-if-GigabitEthernet 0/3)#int g 0/2
SW2(config-if-GigabitEthernet 0/2)#sw port-security binding 192.168.2.2
SW2(config-if-GigabitEthernet 0/2)#sw port-security maxinum 4
                                                  ^
% Invalid input detected at '^' marker.

SW2(config-if-GigabitEthernet 0/2)#sw port-security maximum 4
SW2(config-if-GigabitEthernet 0/2)#sw port-security
SW2(config-if-GigabitEthernet 0/2)#exit
SW2(config)#show port-security address
```

图 11: 设置 0/2 端口只允许 PC4 等至多 4 台机器访问

查看交换机绑定的安全表项

```
SW2(config)#show port-security address
NO.  VLAN  MacAddress      PORT                    TYPE       RemainingAge(mins)  STATUS
---- ----- --------------- ----------------------- ---------- ------------------  ---------
1    1     00e0.4c68.6ec6  GigabitEthernet 0/2     Dynamic            --          active
2    1     00e0.4c68.8f4d  GigabitEthernet 0/3     Dynamic            --          active
```

图 12: 交换机绑定的安全表项

可以看到 2 号端口绑定了 PC4 的 mac，3 号端口绑定了 PC2 的 mac。
我们再查看各个端口的安全设置。

```
SW2(config-if-GigabitEthernet 0/3)#show port-security
NO.  SecurePort MaxSecureAddr CurrentAddr CurrentIpBind CurrentIpMacBind SecurityAction AgingTime
                  (Count)       (Count)      (Count)         (Count)                        (min)
---- ---------- ------------ ----------- ------------ --------------- -------------- ---------
1    Gi0/2      4            1           1            0               protect        0
2    Gi0/3      128          1           0            0               protect        0
-------------------------------------------------------------------------------------------------
Total secure addresses in System : 2
Total secure bindings  in System : 1
```

图 13: 交换机各端口的安全设置

可以看到 2 号端口的最大数量被设置为 4，并且已经有两个 ip 地址被绑定（PC2 和 PC4 的 IP）。

四、 出现的问题及解决方法

1. 在配置 NAT 时，主要需要搞清楚 ip nat 配置命令中每个参数的含义，前期实验中由于没有分清楚数值和名称的差异，导致 access list 建立过程中无法正确对应我们设置的 IP 池。从中我们了解到对应配置命令的解析十分重要。

2. 在设置端口安全时,要注意绑定的信息与实际的信息匹配,本题中要求 PC2 只能使用 192.168.2.100 访问，我绑定之后，由于设置 PC2 的 IP 信息的同学，没有看到此要求，设置成另外一个 IP，导致 PC2 一直无法访问网关，我们设置了绑定信息，一定要严格按照信息进行配置!

五、 实验结果

路由器 3 的路由表:

```
Ruijie(config)#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        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
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    192.168.2.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.2.1/32 is local host.
S    202.114.65.0/24 [1/0] via 202.114.66.1
C    202.114.66.0/24 is directly connected, GigabitEthernet 0/1
C    202.114.66.2/32 is local host.
S    202.114.77.0/24 [1/0] via 202.114.66.1
```

图 14: 路由器 3 的路由表

路由器 3 的 NAT 信息:

```
Ruijie(config)#show ip nat tra
Pro Inside global      Inside local       Outside local      Outside global
tcp 202.114.66.2:60984 192.168.2.2:60984  202.114.65.100:80  202.114.65.100:80
tcp 202.114.66.2:61039 192.168.2.2:61039  202.114.77.100:80  202.114.77.100:80
```

图 15: 路由器 3 的 NAT 信息

路由器 2 的路由表:

```
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#show ip route*May 13 12:21:51: %ARP-4-ZERO_ADDR: Zero MAC address for 192.168.1.2 in ARP cache.


Codes:  C - connected, S - static, R - RIP, B - BGP
        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
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    192.168.1.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.1.1/32 is local host.
C    202.114.65.0/24 is directly connected, GigabitEthernet 0/1
C    202.114.65.2/32 is local host.
S    202.114.66.0/24 [1/0] via 202.114.65.1
S    202.114.77.0/24 [1/0] via 202.114.65.1
```

图 16: 路由器 2 的路由表

路由器 2 的 NAT 信息:

```
Ruijie(config)#show ip nat trans
Pro Inside global      Inside local       Outside local      Outside global
icmp202.114.65.8:1     192.168.1.3:1      202.114.77.100     202.114.77.100
Ruijie(config)#
```

图 17: 路由器 2 的 NAT 信息

交换机 2 的端口安全信息:

```
SW2(config-if-GigabitEthernet 0/3)#show port-security
NO.  SecurePort MaxSecureAddr CurrentAddr CurrentIpBind CurrentIpMacBind SecurityAction AgingTime
                  (Count)      (Count)      (Count)         (Count)                      (min)
---- ---------- ------------ ----------- ------------- --------------- -------------- ---------
1    Gi0/2      4            1           1             0               protect        0
2    Gi0/3      128          1           0             0               protect        0
-------------------------------------------------------------------------------------------------
Total secure addresses in System : 2
Total secure bindings  in System : 1
```

图 18: 交换机 2 的端口安全信息

PC1 Ping WWW1:

```
C:\Users\Administrator>ping 202.114.77.100

正在 Ping 202.114.77.100 具有 32 字节的数据:
来自 202.114.77.100 的回复: 字节=32 时间<1ms TTL=126
来自 202.114.77.100 的回复: 字节=32 时间=1ms TTL=126
来自 202.114.77.100 的回复: 字节=32 时间<1ms TTL=126
来自 202.114.77.100 的回复: 字节=32 时间<1ms TTL=126

202.114.77.100 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 1ms, 平均 = 0ms
```

图 19: PC1 Ping WWW1

PC2 Ping WWW2:

```
C:\Users\Administrator>ping 202.114.65.100

正在 Ping 202.114.65.100 具有 32 字节的数据:
来自 202.114.65.100 的回复: 字节=32 时间=2ms TTL=123
来自 202.114.65.100 的回复: 字节=32 时间=3ms TTL=123
来自 202.114.65.100 的回复: 字节=32 时间=3ms TTL=123
来自 202.114.65.100 的回复: 字节=32 时间=3ms TTL=123

202.114.65.100 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 2ms, 最长 = 3ms, 平均 = 2ms

C:\Users\Administrator>
```

图 20: PC2 Ping WWW2

PC4 访问 WWW2:

七、 指导教师评语及成绩

【评语】

成　　绩：　　指导老师签名：

批阅日期：