《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 28 日

实验名称： VPN 应用实验

实验成绩：

VPN 应用实验

一、实验需求

将某个企业网划分为 4 个 VLAN，分别是 VLAN2-VLAN5，其中 VLAN2 属于生产管理部门，VLAN3 属于销售部门，VLAN4 属于财务部门，VLAN5 属于信息服务部门。企业网和 Internet 互连，连接在 Internet 上的终端可以通过 VPN 访问 VLAN5 中的信息资源。为了安全，要求企业网实施以下安全策略。

（1） 属于财务部门的终端不允许访问 Internet。

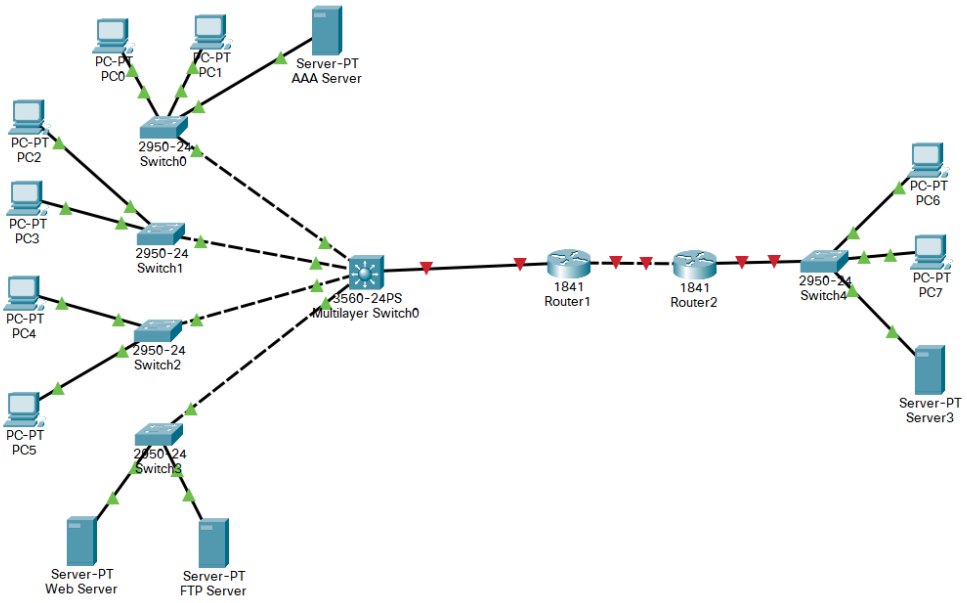
（2） 属于财务部门的 VLAN4 与属于信息部门的 VLAN5 之间不能互相通信。

（3） 允许 VLAN2 和 VLAN3 中的终端发起访问 Internet 的过程。

（4） 连接在 Internet 上的终端如果需要发起访问企业网的过程，必须先通过 VPN 接入企业网，且只能访问 VLAN5 中的信息资源，不能与其他 VLAN 中的终端相互通信。

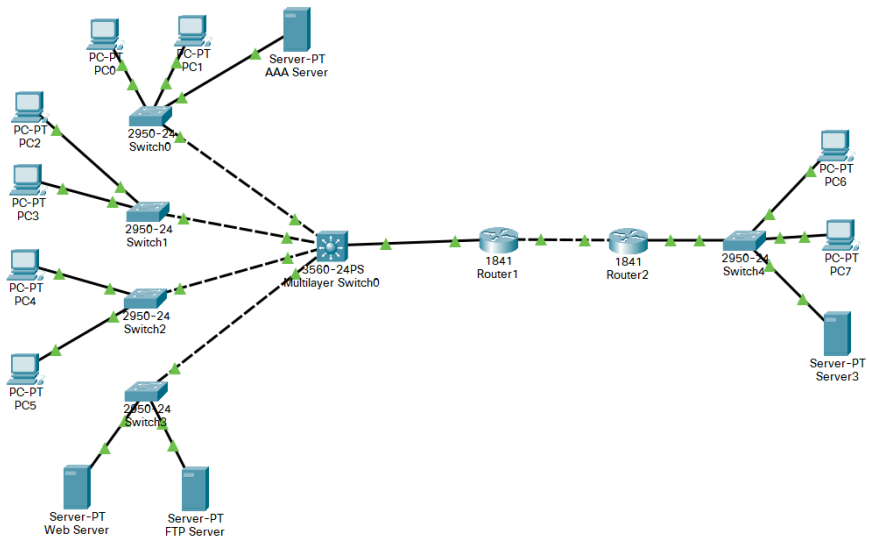
二、实验步骤

(1) 完成网络结构放置和连接设备。



(2) 完成路由器各个接口的 IP 地址和子网掩码配置过程，完成三层交换机 Multilayer Switch0 IP 接口定义和配置过程，完成三层交换机 Multilayer Switch0 和路由器 R1 默认路由配置过程。

配置完成后：



三层交换机路由表：

```
Gateway of last resort is 192.168.5.2 to network 0.0.0.0

C    192.168.1.0/24 is directly connected, Vlan2
C    192.168.2.0/24 is directly connected, Vlan3
C    192.168.3.0/24 is directly connected, Vlan4
C    192.168.4.0/24 is directly connected, Vlan5
C    192.168.5.0/24 is directly connected, Vlan6
S*   0.0.0.0/0 [1/0] via 192.168.5.2

Switch#
```

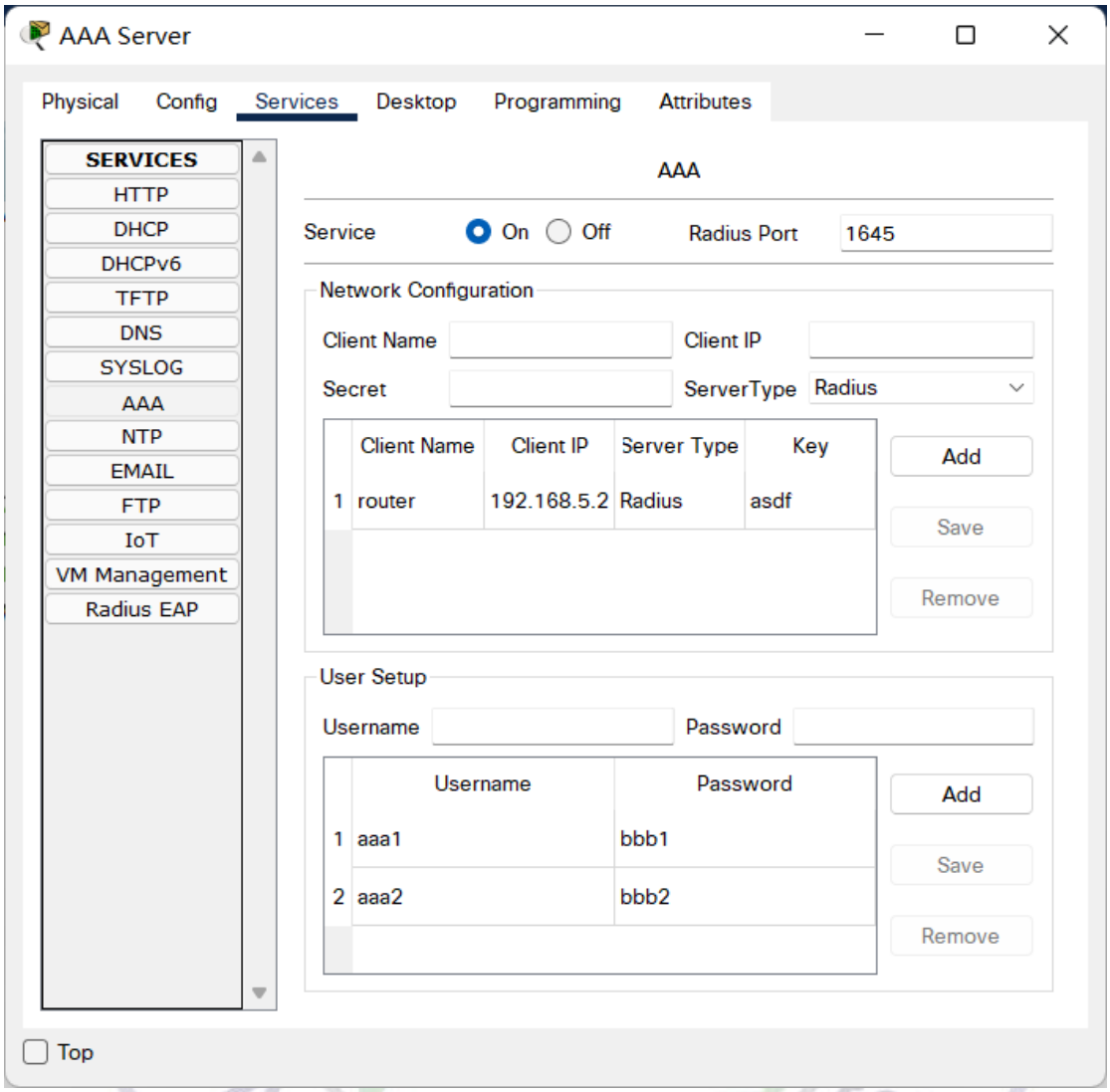
Router1 路由表：

```
Gateway of last resort is 192.1.1.2 to network 0.0.0.0

C    192.1.1.0/24 is directly connected, FastEthernet0/1
R    192.168.1.0/24 [120/1] via 192.168.5.1, 00:00:01, FastEthernet0/0
R    192.168.2.0/24 [120/1] via 192.168.5.1, 00:00:01, FastEthernet0/0
R    192.168.3.0/24 [120/1] via 192.168.5.1, 00:00:01, FastEthernet0/0
R    192.168.4.0/24 [120/1] via 192.168.5.1, 00:00:01, FastEthernet0/0
C    192.168.5.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 192.1.1.2
```

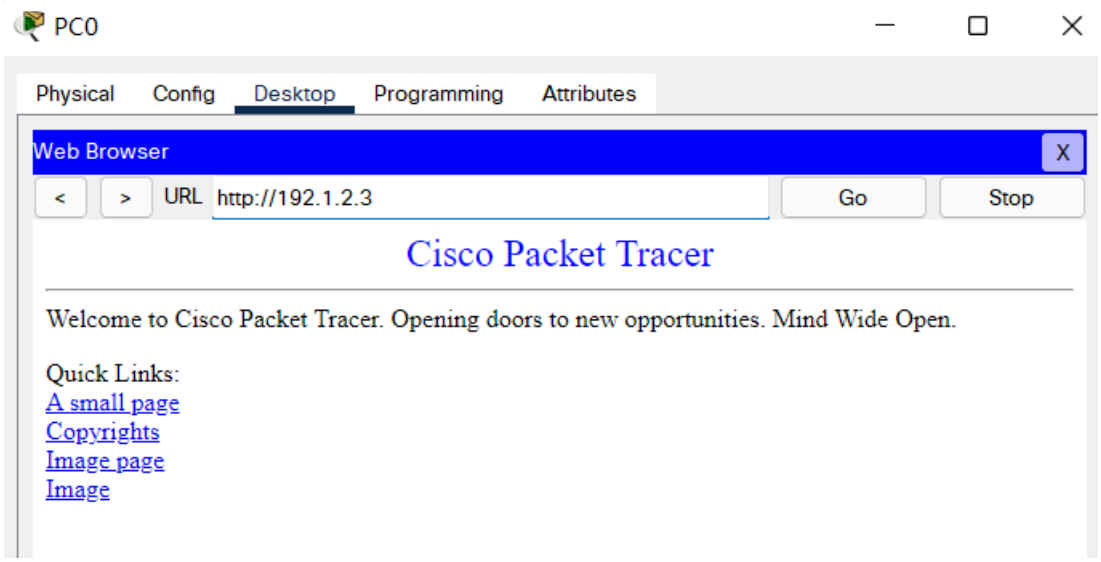
Router2 路由表

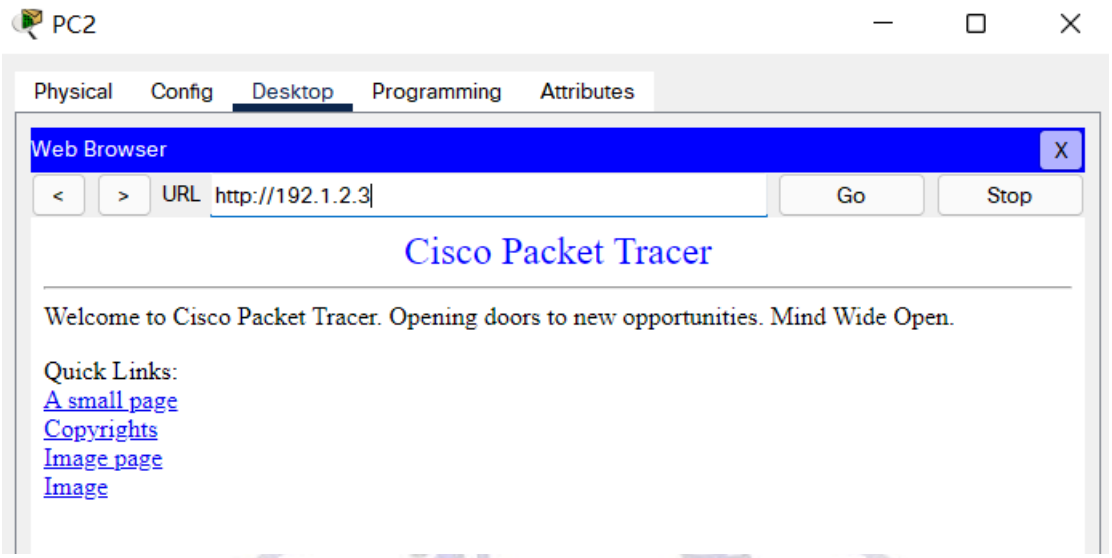
```
Gateway of last resort is not set

C    192.1.1.0/24 is directly connected, FastEthernet0/0
C    192.1.2.0/24 is directly connected, FastEthernet0/1
```

(3)完成 AAA Server 的配置



(4)PC0 和 PC2 访问 Internet 中 Web Server2.



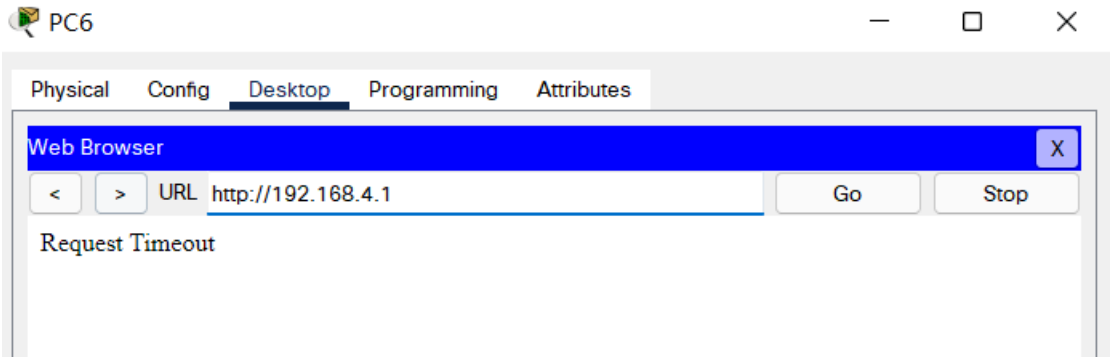


(5)属于 VLAN2 和 VLAN3 的终端访问 Internet 后，路由器 R1 的 NAT 转换表如图所示。

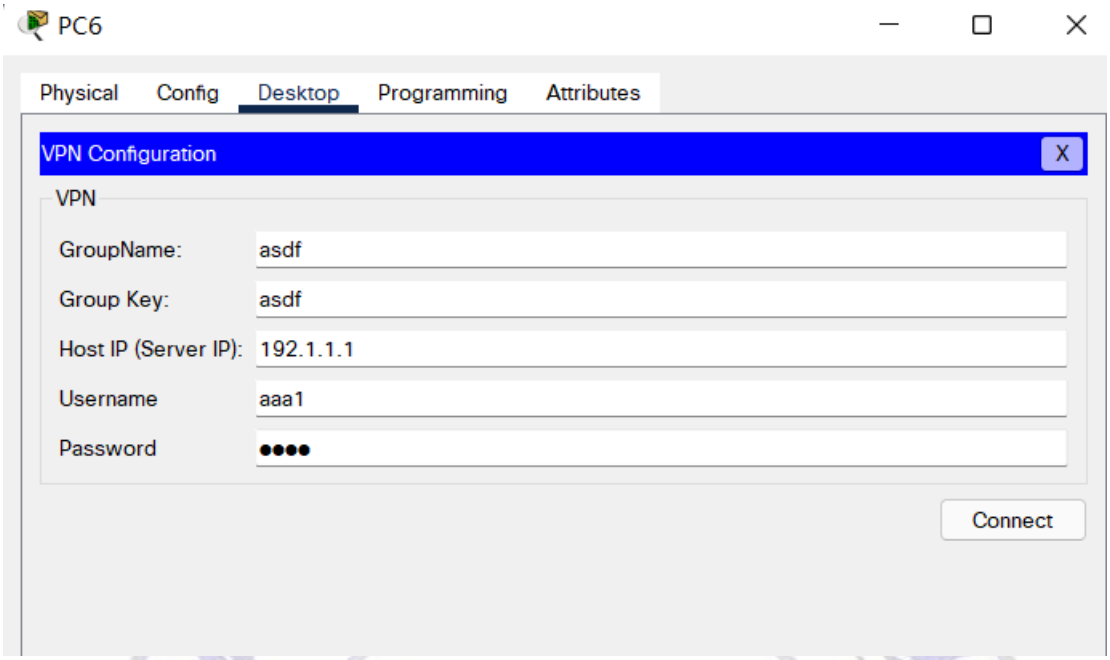
地址转换表：

```
router#sh ip nat tra
Pro  Inside global     Inside local       Outside local      Outside global
icmp 192.1.1.1:13      192.168.1.1:13     192.1.2.1:13       192.1.2.1:13
icmp 192.1.1.1:14      192.168.1.1:14     192.1.2.1:14       192.1.2.1:14
icmp 192.1.1.1:15      192.168.1.1:15     192.1.2.1:15       192.1.2.1:15
icmp 192.1.1.1:16      192.168.1.1:16     192.1.2.1:16       192.1.2.1:16
icmp 192.1.1.1:1       192.168.2.1:1      192.1.2.1:1        192.1.2.1:1
icmp 192.1.1.1:2       192.168.2.1:2      192.1.2.1:2        192.1.2.1:2
icmp 192.1.1.1:3       192.168.2.1:3      192.1.2.1:3        192.1.2.1:3
icmp 192.1.1.1:4       192.168.2.1:4      192.1.2.1:4        192.1.2.1:4
tcp 192.1.1.1:1024     192.168.2.1:1025   192.1.2.3:80       192.1.2.3:80
tcp 192.1.1.1:1025     192.168.1.1:1025   192.1.1.3:80       192.1.1.3:80
tcp 192.1.1.1:1026     192.168.1.1:1026   192.1.2.3:80       192.1.2.3:80

router#
```

(6) Internet 终端 PC6 和 PC7 不能直接访问 VLAN5. PC6 VPN 接入企业网的界面如图所示。



接入企业网：

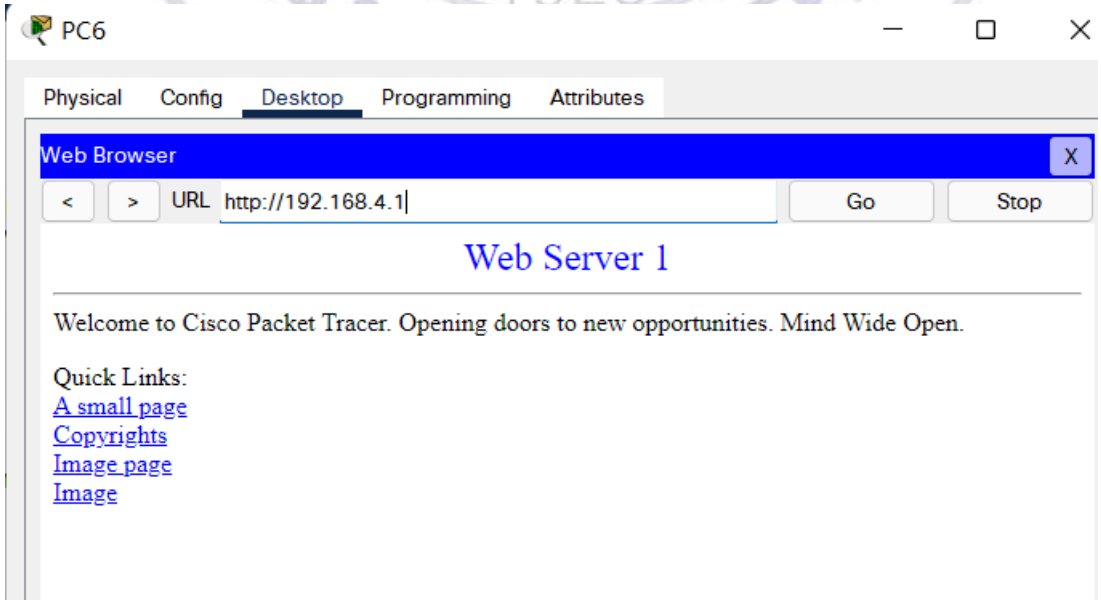


（7）接入企业网后，分配私有 IP 地址，路由器将建立对应路由项。

R1 路由表：

```
Gateway of last resort is 192.1.1.2 to network 0.0.0.0

C    192.1.1.0/24 is directly connected, FastEthernet0/1
R    192.168.1.0/24 [120/1] via 192.168.5.1, 00:00:11, FastEthernet0/0
R    192.168.2.0/24 [120/1] via 192.168.5.1, 00:00:11, FastEthernet0/0
R    192.168.3.0/24 [120/1] via 192.168.5.1, 00:00:11, FastEthernet0/0
R    192.168.4.0/24 [120/1] via 192.168.5.1, 00:00:11, FastEthernet0/0
C    192.168.5.0/24 is directly connected, FastEthernet0/0
     192.168.6.0/32 is subnetted, 1 subnets
S       192.168.6.1 [1/0] via 192.1.2.1
S*   0.0.0.0/0 [1/0] via 192.1.1.2
```

（8）PC6 可以访问 Web Server1 的资源。



PC6 访问 FTP 资源：

```
C:\>ftp 192.168.4.2
Trying to connect...192.168.4.2
Connected to 192.168.4.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
```

三、实验结果及分析

通过 VPN 和 VLAN 的应用将企业网划分成了 4 个 VLAN，每个 VLAN 各司其职，实现各自部分的功能，通过设置安全策略，实现不同 VLAN 之间的不同功能的实施，当外部 Internet 需要访问内部网络时，需要采用 VPN 的方式接入网络，才能访问内部终端。

四、实验总结及体会

在实验中我们可以发现，当不设置安全策略时，不同区的终端与终端之间，终端与服务器之间，服务器与服务器之间都是可以联通的，当我们设置安全策略之后，只允许实现我们预先设置好的通信策略。该种方法适合于局域网内部的管理，当我们有一个庞大的局域网时，我们可以采用安全策略以及 VLAN 划分的方式进行管理。

有了局域网，我们就有与外部 Internet 进行通信的需求，外部网络就可以通过 IP 隧道实现内部私有 IP 地址和外部公有 IP 地址的连接，保证了我们外部网络和内部网络之间的通信。