《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

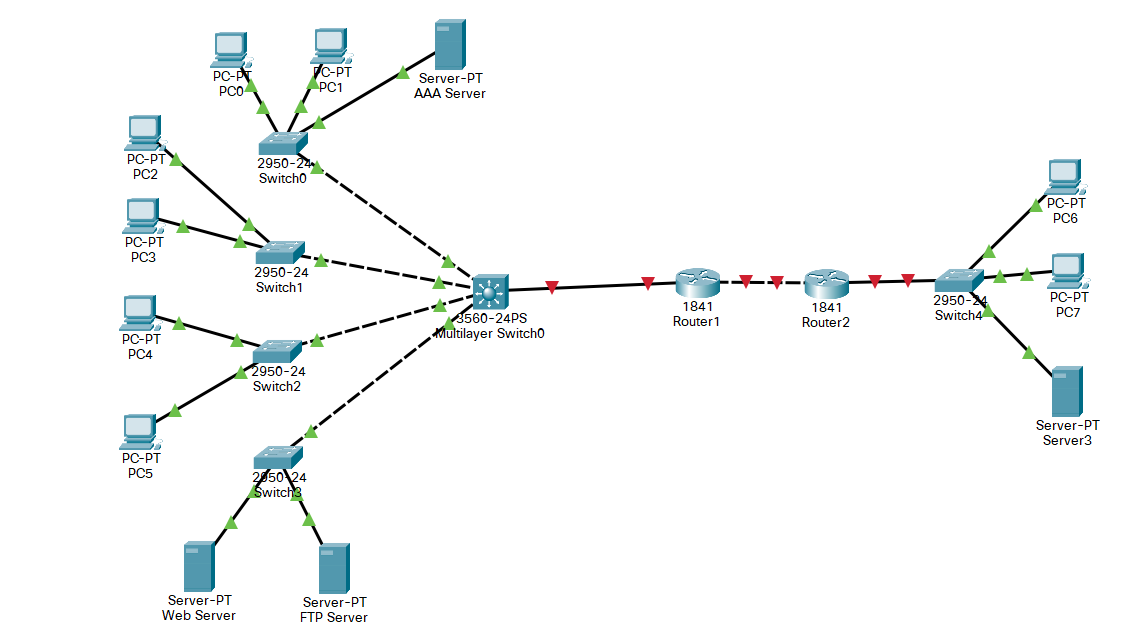
一、实验需求

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。

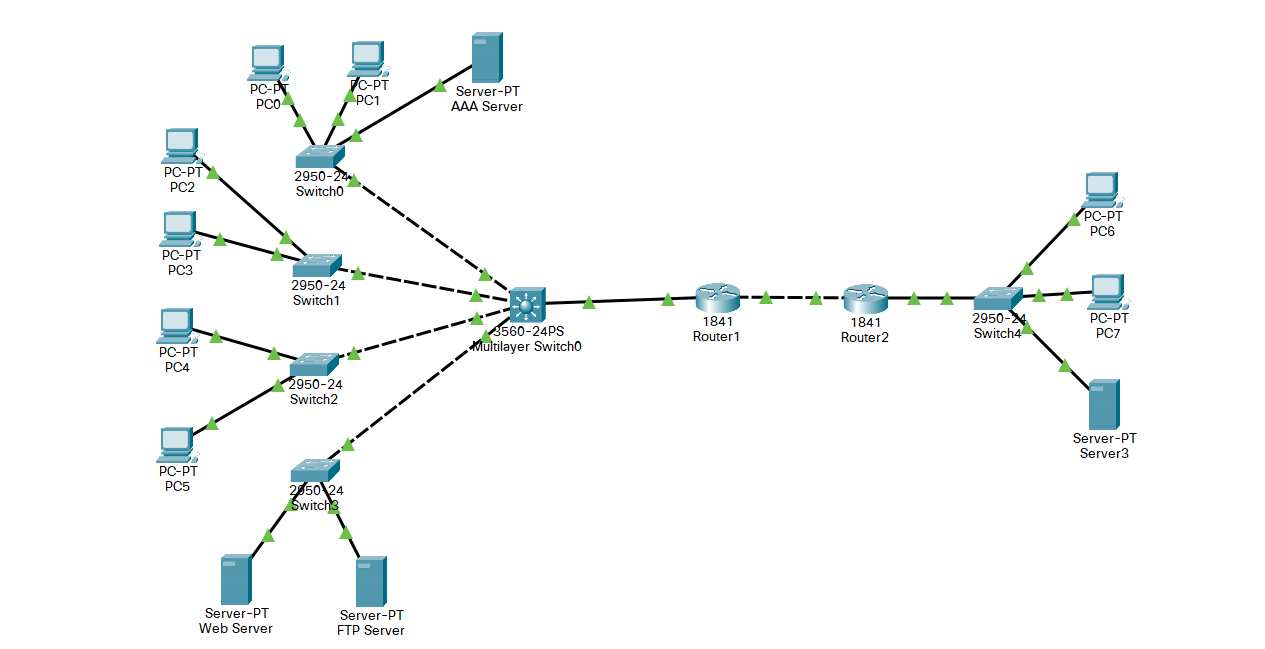
二、实验步骤

(1)完成网络结构放置和连接设备。

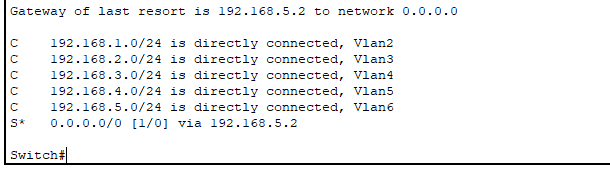


(2) 完成路由器各个接口的IP地址和子网掩码配置过程，完成三层交换机Multilayer Switch0 IP接口定义和配置过程，完成三层交换机Multilayer Switch0和路由器R1默认路由配置过程。

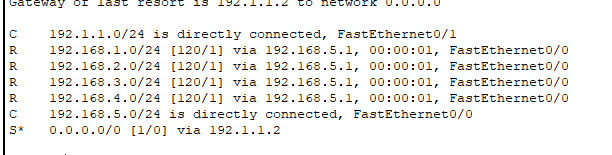
配置完成后：



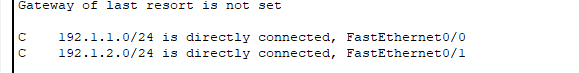
**三层交换机路由表：**



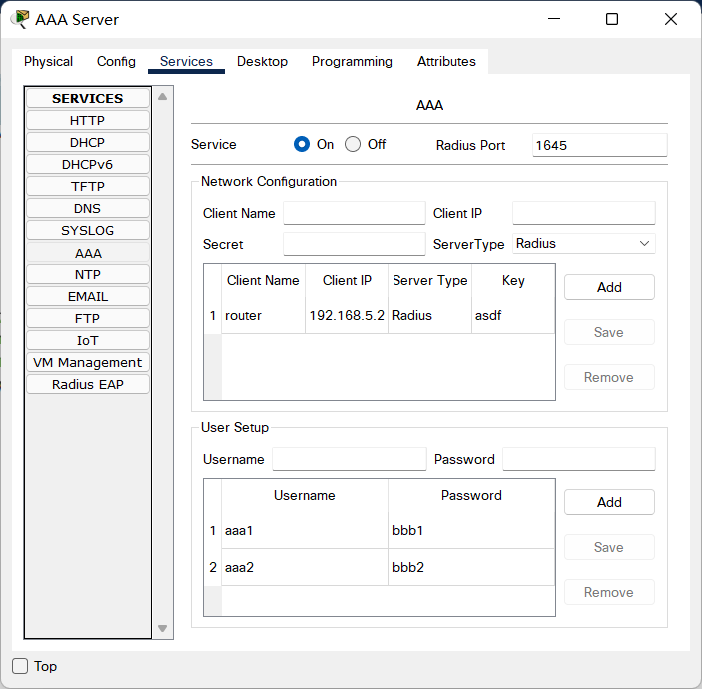
**Router1路由表：**



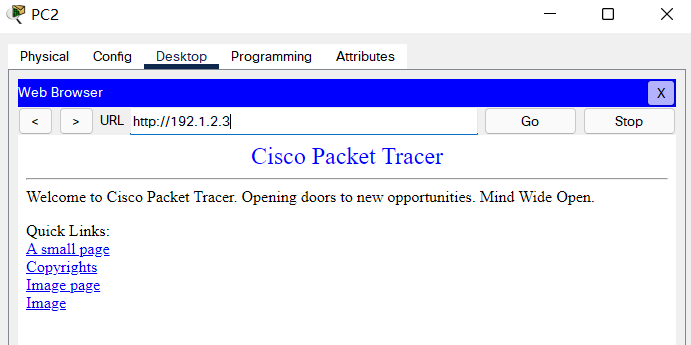
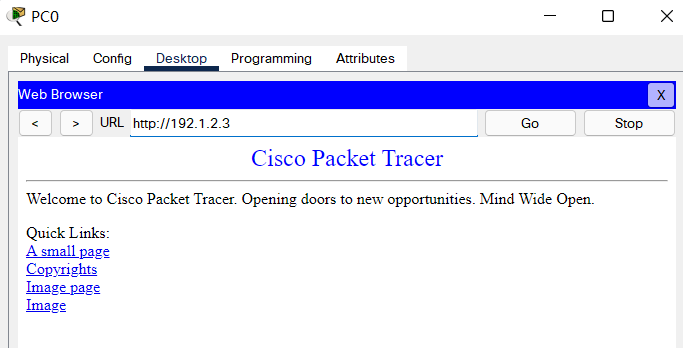
**Router2路由表**



(3)完成AAA Server的配置

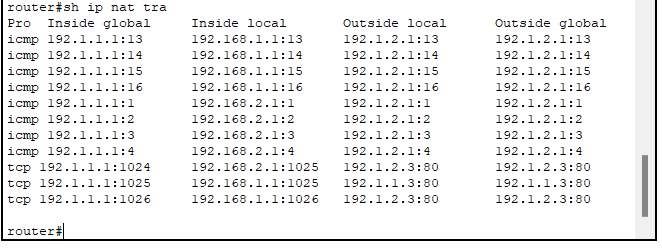


(4)PC0和PC2访问Internet中Web Server2.

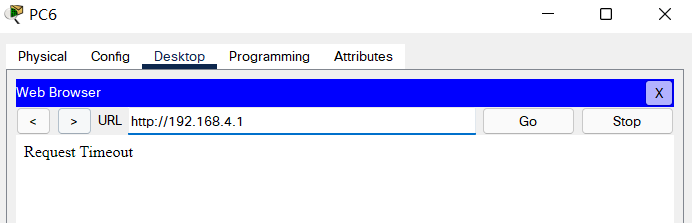


(5)属于VLAN2和VLAN3的终端访问Internet后，路由器R1的NAT转换表如图所示。

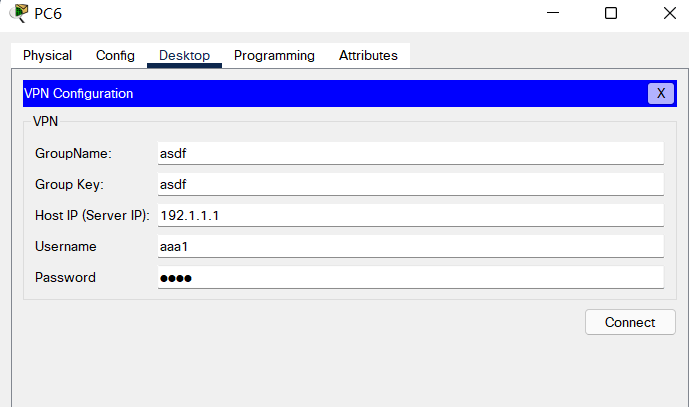
地址转换表：



(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。

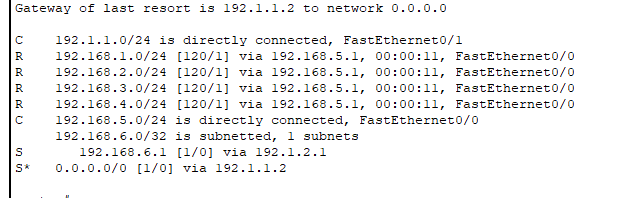


接入企业网：

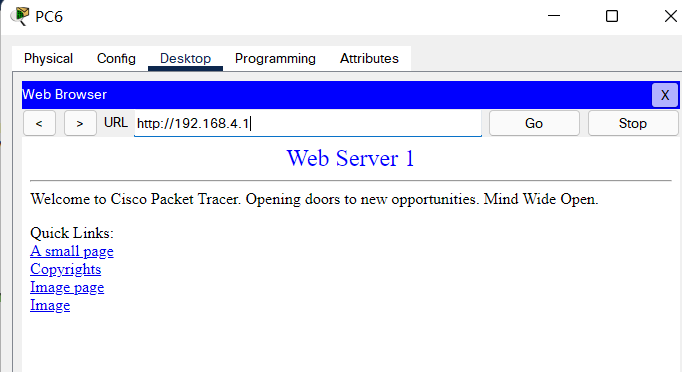


（7）接入企业网后，分配私有IP地址，路由器将建立对应路由项。

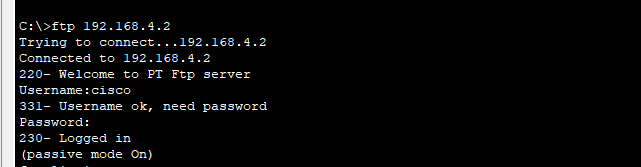
R1路由表：



（8）PC6可以访问Web Server1的资源。



PC6访问FTP资源：



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。