



**《计算机网络》课程设计**

**课程名称**  **计算机网络**

**学生学院 计算机学院**

**专业班级 信息安全一班**

**指导教师 许青林**

**学生姓名 郭鹏燕**

**学 号 3216005166**

2018年7 月 5 日

目录

1. [环境配置 3](#_Toc515831519)
2. [引言 3](#_Toc515831519)
3. [相关技术基础 3](#_Toc515831519)
4. [网络结构及地址分配 5](#_Toc515831519)
5. [配置与实施 6](#_Toc515831519)
6. [结果与分析 1](#_Toc515831519)1
7. [总结 1](#_Toc515831519)5

企业网络规划及访问控制

1. **环境配置**

Cisco Packet Track Student

1. **引言**

在企业中，要实现所有的员工都能与互联网进行通信，每个人各使用一个公网地址是很不现实的。一般，企业有1个或几个公网地址，而企业有几十、几百个员工。要想让所有的员工使用这仅有的几个公网地址与互联网通信该怎么做呢？使用NAT技术！

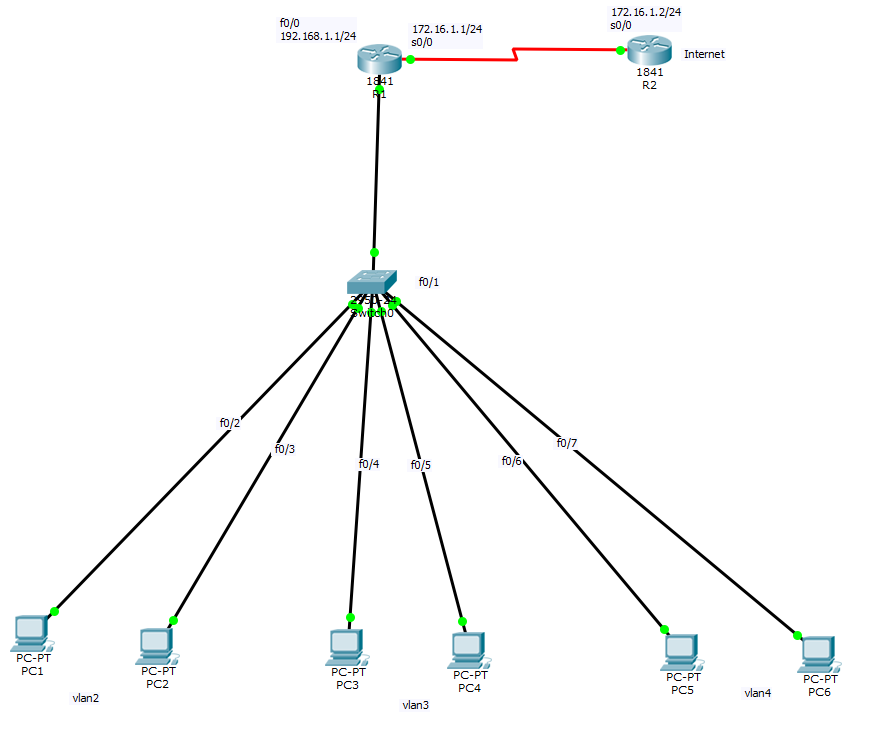
在企业中，一般会有多个部门，像财务部、技术部、工程部等等。每个部门有每个部门的职责。像财务部这种重要的部门有些资料是不允许被其他员工知道的。怎样能清楚的区分不同的部门，以便于管理呢？使用VLAN技术！

为了工作方便、增强工作效率，各部门经理必须能相互通信。但不允许员工之间相互通信。我们又该怎样做呢？使用ACL技术！

1. **相关技术基础**

(1)**网络地址转换**（Network Address Translation，缩写为**NAT**），也叫做**网络掩蔽**或者IP**掩蔽**（IP masquerading），是一种在IP数据包通过[路由器](https://zh.wikipedia.org/wiki/%E8%B7%AF%E7%94%B1%E5%99%A8" \o "路由器)或[防火墙](https://zh.wikipedia.org/wiki/%E9%98%B2%E7%81%AB%E5%A2%99" \o "防火墙)时重写来源IP地址或目的[IP地址](https://zh.wikipedia.org/wiki/IP%E5%9C%B0%E5%9D%80" \o "IP地址)的技术。这种技术被普遍使用在有多台主机但只通过一个公有IP地址访问[因特网](https://zh.wikipedia.org/wiki/%E5%9B%A0%E7%89%B9%E7%BD%91" \o "因特网)的私有网络中。一个本地网络使用一个专有网络的指定子网（比如192.168.x.x或10.x.x.x）和连在这个网络上的一个路由器。这个路由器占有这个网络地址空间的一个专有地址（比如192.168.0.1），同时它还通过一个或多个因特网服务提供商提供的公有的IP地址（叫做“过载”NAT）连接到因特网上。当信息由本地网络向因特网传递时，源地址从专有地址转换为公用地址。由路由器跟踪每个连接上的基本数据，主要是目的地址和端口。当有回复返回路由器时，它通过输出阶段记录的连接跟踪数据来决定该转发给内部网的哪个主机；如果有多个公用地址可用，当数据包返回时，TCP或UDP客户机的端口号可以用来分解数据包。对于因特网上的通信，路由器本身充源和目的。

1. **拟局域网**（**VLAN**）是一组逻辑上的设备和用户，这些设备和用户并不受物理位置的限制，可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在[同一个网段](https://baike.baidu.com/item/%E5%90%8C%E4%B8%80%E4%B8%AA%E7%BD%91%E6%AE%B5/10612240" \t "https://baike.baidu.com/item/%E8%99%9A%E6%8B%9F%E5%B1%80%E5%9F%9F%E7%BD%91/_blank)中一样，由此得名虚拟局域网。VLAN是一种比较新的技术，工作在[OSI参考模型](https://baike.baidu.com/item/OSI%E5%8F%82%E8%80%83%E6%A8%A1%E5%9E%8B" \t "https://baike.baidu.com/item/%E8%99%9A%E6%8B%9F%E5%B1%80%E5%9F%9F%E7%BD%91/_blank)的第2层和第3层，一个VLAN就是一个**[广播域](https://baike.baidu.com/item/%E5%B9%BF%E6%92%AD%E5%9F%9F/5293530" \t "https://baike.baidu.com/item/%E8%99%9A%E6%8B%9F%E5%B1%80%E5%9F%9F%E7%BD%91/_blank)**，VLAN之间的通信是通过第3层的[路由器](https://baike.baidu.com/item/%E8%B7%AF%E7%94%B1%E5%99%A8/108294" \t "https://baike.baidu.com/item/%E8%99%9A%E6%8B%9F%E5%B1%80%E5%9F%9F%E7%BD%91/_blank)来完成的。与传统的[局域网技术](https://baike.baidu.com/item/%E5%B1%80%E5%9F%9F%E7%BD%91%E6%8A%80%E6%9C%AF/2597024" \t "https://baike.baidu.com/item/%E8%99%9A%E6%8B%9F%E5%B1%80%E5%9F%9F%E7%BD%91/_blank)相比较，VLAN技术更加灵活，它具有以下优点： 网络设备的移动、添加和修改的管理开销减少；可以控制[广播](https://baike.baidu.com/item/%E5%B9%BF%E6%92%AD/656406" \t "https://baike.baidu.com/item/%E8%99%9A%E6%8B%9F%E5%B1%80%E5%9F%9F%E7%BD%91/_blank)活动；可提高[网络](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C/143243" \t "https://baike.baidu.com/item/%E8%99%9A%E6%8B%9F%E5%B1%80%E5%9F%9F%E7%BD%91/_blank)的安全性。在计算机网络中，一个二层网络可以被划分为多个不同的广播域，一个广播域对应了一个特定的用户组，默认情况下这些不同的广播域是相互隔离的。不同的广播域之间想要通信，需要通过一个或多个路由器。这样的一个广播域就称为VLAN。
2. **[访问控制列表](https://baike.baidu.com/item/%E8%AE%BF%E9%97%AE%E6%8E%A7%E5%88%B6%E5%88%97%E8%A1%A8/1844390" \t "https://baike.baidu.com/item/_blank)**（Access Control List，**ACL**） 是[路由器](https://baike.baidu.com/item/%E8%B7%AF%E7%94%B1%E5%99%A8/108294" \t "https://baike.baidu.com/item/_blank)和[交换机](https://baike.baidu.com/item/%E4%BA%A4%E6%8D%A2%E6%9C%BA/103532" \t "https://baike.baidu.com/item/_blank)接口的指令列表，用来[控制端口](https://baike.baidu.com/item/%E6%8E%A7%E5%88%B6%E7%AB%AF%E5%8F%A3/1688757" \t "https://baike.baidu.com/item/_blank)进出的**数据包**。ACL适用于所有的[被路由协议](https://baike.baidu.com/item/%E8%A2%AB%E8%B7%AF%E7%94%B1%E5%8D%8F%E8%AE%AE/9765626" \t "https://baike.baidu.com/item/_blank)，如IP、IPX、AppleTalk等。信息点间通信和内外网络的通信都是企业网络中必不可少的业务需求，为了保证内网的安全性，需要通过[安全策略](https://baike.baidu.com/item/%E5%AE%89%E5%85%A8%E7%AD%96%E7%95%A5/2890163" \t "https://baike.baidu.com/item/_blank)来保障非授权用户只能访问特定的网络资源，从而达到对访问进行控制的目的。简而言之，ACL可以过滤网络中的流量，是控制访问的一种网络技术手段。配置ACL后，可以限制网络流量，允许特定设备访问，指定转发特定端口数据包等。如可以配置ACL，禁止局域网内的设备访问外部公共网络，或者只能使用FTP服务。ACL既可以在路由器上配置，也可以在具有ACL功能的业务软件上进行配置。
3. **网络结构及地址分配**



企业中只有一个公网地址，172.16.1.1/24  
企业中共有三个部门工程部、财务部、技术部[。](http://www.pcjx.com)  
PC1 PC3 PC5 分别为三个部门的部门经理使用[。](http://www.pcjx.com)  
 PC1 的ip地址为192.168.1.2/24  
 PC2 的ip地址为192.168.1.3/24  
 PC3 的ip地址为192.168.2.2/24  
 PC4 的ip地址为192.168.2.3/24  
 PC5 的ip地址为192.168.3.2/24  
 PC6 的ip地址为192.168.3.3/24

1. **配置与实施**

通过配置NAT使企业中所有的计算机都能通过唯一的公网地址与互联网通信。

通过配置VLAN划分各个部门，并配置ACL实现每个部门经理之间能够通讯，普通员工之间不能相互通讯。

首先在R1 和 R2上做基本配置，（由于试验过程中要使用VLAN间路由，所以需要使用dot1Q 进行封装来配置子接口）

R1

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#host r1

r1(config)#int s0/0/0

r1(config-if)#ip addr 172.16.1.1 255.255.255.0

r1(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0, changed state to up

r1(config-if)#clock rate 64000

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to u

r1(config-if)#exit

r1(config)#int f0/0

r1(config-if)#no ip addr

r1(config-if)#no shut

r1(config-if)#exit

r1(config)#int f0/0.1 配置子接口，

r1(config-subif)#encapsulation dot1Q 2 配置子接口必须使用dot1Q进行封装

r1(config-subif)#ip addr 192.168.1.1 255.255.255.0

r1(config-subif)#no shut

r1(config-subif)#exit

r1(config)#int f0/0.2 配置子接口

r1(config-subif)#encapsulation dot1Q 3 配置子接口必须使用dot1Q进行封装

r1(config-subif)#ip addr 192.168.2.1 255.255.255.0

r1(config-subif)#no shut

r1(config-subif)#exit

r1(config)#int f0/0.3 配置子接口

r1(config-subif)#encapsulation dot1Q 4 配置子接口必须使用dot1Q进行封装

r1(config-subif)#ip addr 192.168.3.1 255.255.255.0

R2当作公网使用，所以只需要在R2的S0/0口上配置ip就可以啦

R2

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#host r2

r2(config)#int s0/0/0

r2(config-if)#ip addr 172.16.1.2 255.255.255.0

r2(config-if)#no shut

基本配置完成了，接下来第一步，我们要让企业中的所有员工都能通过唯一的公网ip 172.16.1.1/24 与互联网相互通信。

R1

r1(config)#ip nat pool internet 172.16.1.1 172.16.1.1 netmask 255.255.255.0 定义全局地址池

r1(config)#access-list 10 permit 192.168.0.0 0.0.255.255通过标准访问控制列表定义内部网络的上网条件

r1(config)#ip nat inside source list 10 pool internet overload 建立全局地址池与标准访问控制列表之间的映射关系

r1(config)#int s0/0/0

r1(config-if)#ip nat outside 外网接口绑定（要想配置能实现应用必须在内外网接口上绑定）

r1(config-if)#exit

r1(config)#int f0/0

r1(config-if)#ip nat inside 内网接口绑定

通过配置VLAN划分各个部门，并配置ACL以实现每个部门经理之间能够通讯，普通员工之间不能相互通讯。

Sw

Switch>en

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#int f0/1

Switch(config-if)#switchport mode trunk 配置Trunk链路

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch(config-if)#exit

Switch(config)#vlan 2 创建VLAN 2

Switch(config-vlan)#name gongchengbu vlan2为工程部

Switch(config-vlan)#exit

Switch(config)#vlan 3 创建VLAN 3

Switch(config-vlan)#name caiwubu VLAN3为财务部

Switch(config-vlan)#exit

Switch(config-vlan)#vlan 4 创建VLAN 4

Switch(config-vlan)#name jishubu VLAN4为技术部

Switch(config-vlan)#exit

Switch(config)#int f0/2

Switch(config-if)#switchport access vlan 2 给VLAN 2手工添加成员

Switch(config-if)#exit

Switch(config)#int f0/3

Switch(config-if)#switchport access vlan 2

Switch(config-if)#exit

Switch(config)#int f0/4

Switch(config-if)#switchport access vlan 3 给VLAN 3手工添加成员

Switch(config-if)#exit

Switch(config)#int f0/5

Switch(config-if)#switchport access vlan 3

Switch(config-if)#exit

Switch(config)#int f0/6

Switch(config-if)#switchport access vlan 4 给VLAN 3手工添加成员

Switch(config-if)#exit

Switch(config)#int f0/7

Switch(config-if)#switchport access vlan 4

Switch(config-if)#exit

 定义访问控制列表

定义访问控制列表时要细心，要把最特殊的访问控制列表放在最上面。（在此例中，允许一台特定主机而拒绝一个网段，所以要把拒绝主机放在上面）。

注意：要想一个访问列表能够得到应用，必须在接口绑定。

R1

r1(config)#access-list 11 permit 192.168.2.2 0.0.0.0

r1(config)#access-list 11 deny 192.168.2.0 0.0.0.255

r1(config)#access-list 11 permit 192.168.3.2 0.0.0.0

r1(config)#access-list 11 deny 192.168.3.0 0.0.0.255

r1(config)#access-list 11 permit any

r1(config)#int f0/0.1

r1(config-subif)#ip access-group 10 out

r1(config-subif)#exit

r1(config)#access-list 12 permit 192.168.1.2 0.0.0.0

r1(config)#access-list 12 deny 192.168.1.0 0.0.0.255

r1(config)#access-list 12 permit 192.168.3.2 0.0.0.0

r1(config)#access-list 12 deny 192.168.3.0 0.0.0.255

r1(config)#access-list 12 permit any

r1(config)#int f0/0.2

r1(config-subif)#ip access-group 11 out

r1(config-subif)#exit

r1(config)#access-list 13 permit 192.168.1.2 0.0.0.0

r1(config)#access-list 13 deny 192.168.1.0 0.0.0.255

r1(config)#access-list 13 permit 192.168.2.2 0.0.0.0

r1(config)#access-list 13 deny 192.168.2.0 0.0.0.255

r1(config)#access-list 12 permit any

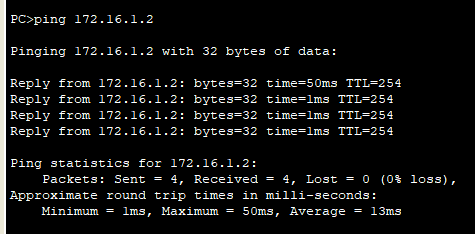
r1(config)#int f0/0.3

r1(config-subif)#ip access-group 12 out

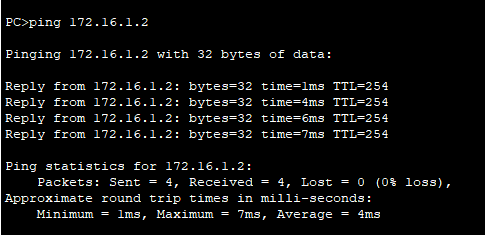
r1(config-subif)#exit

1. **结果及分析**

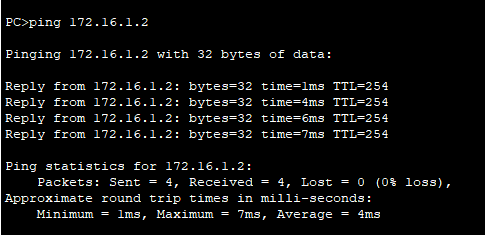
PC1



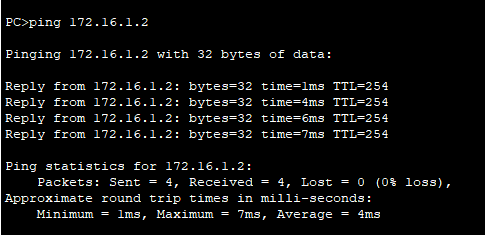
PC2



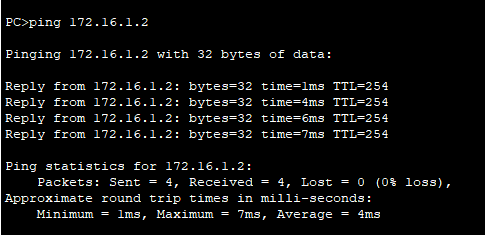
PC3



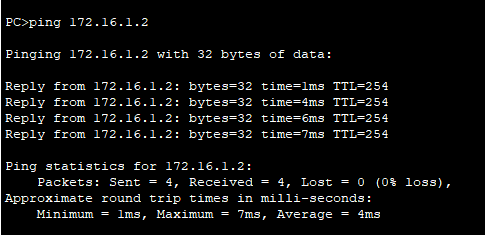
PC4



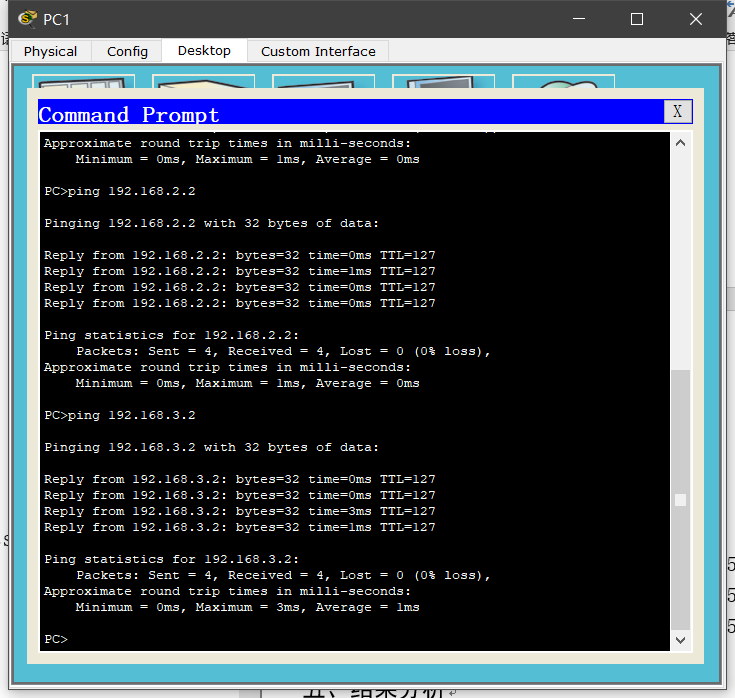
PC5

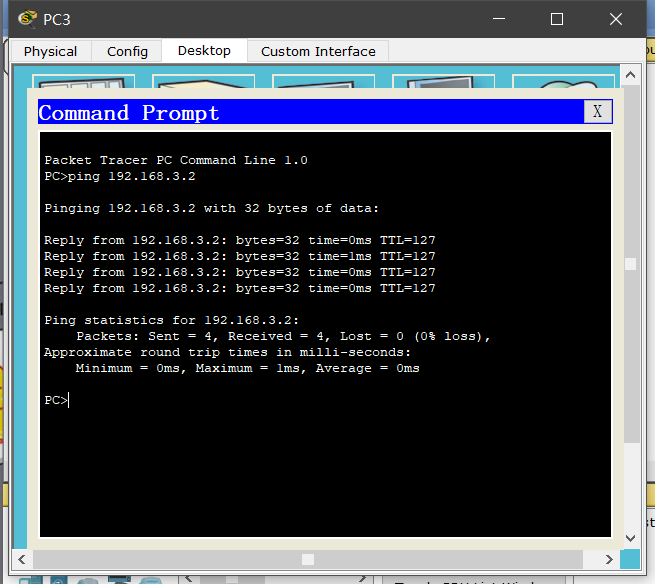


PC6

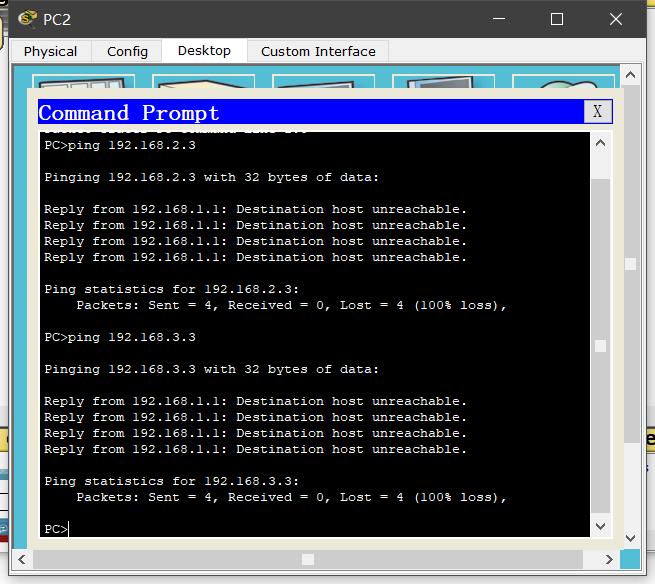


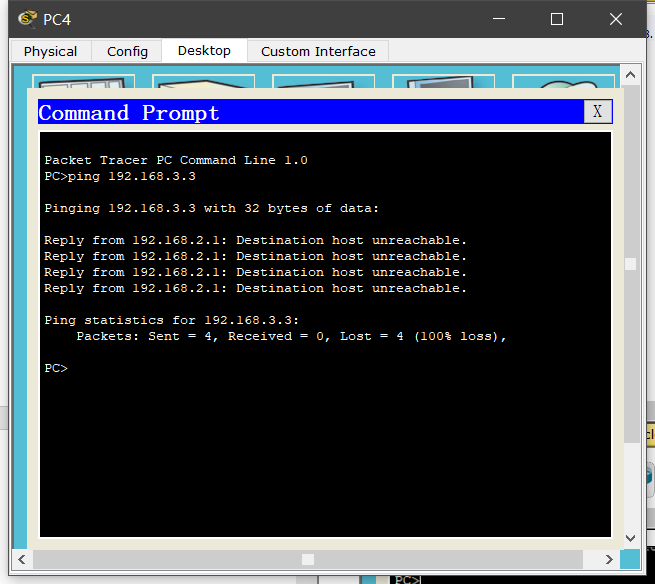
PC1、PC3、PC5之间可以相互通信





**PC2、PC4、PC6之间不能相互通信**





1. **总结**

通过NAT+VLAN+ACL技术实现了对企业网络管理，企业可以通过使用一个公网或者几个公网与互联网通讯，每一台PC机都可以连接到互联网，但是不同部门员工之间不能通讯，只有部门经理之间可以互相通讯，同一部门之间员工之间可以互相通讯。这样不仅使工作方便了很多，也增强了工作效率。通过对这个课设我也增强了自己的动手操作能力，虽然实现的过程遇到很多的坑，但是通过上网查阅资料和在同学的指点下，还是基本完成了功能。由于时间比较紧，还没来得及做VPN，可以等课后自己再去尝试一下！