



**计算机网络课程设计报告**

**学 院 计算机学院**

**专 业 软件工程**

**班 别 20级二班**

**学 号 3120005013**

**学生姓名 冯志文**

**指导教师 许青林**

**2021 年 7 月 4**

**目录**

[1、课程设计任务书 3](#_Toc107823983)

[2、涉及相关技术 3](#_Toc107823984)

[3、分析与设计 3](#_Toc107823985)

[4、系统的实现 4](#_Toc107823986)

[5、系统部署与运行 10](#_Toc107823987)

[6、总结 14](#_Toc107823988)

## 1、课程设计任务书

某公司有财务部（6人）、技术部（30人）和工程部（50人）。每一个部门建一个vlan，同一部门的员工之间可以通信，不同部门之间的员工不能通信，但是部门经理之间可以通信。公司配有多个服务器，包括web、ftp、email、dns等，为公司人员设置相应ftp和email账号和密码。公司通过一个公网地址与外网通信。请设计网络、地址规划并进行相应配置，调通。并完成一篇3000字的课程设计报告。

## 2、涉及相关技术

NAT：网络地址转换,是一种将私有(保留)地址转化为合法IP地址的转换技术,它被广泛应用于各种类型Internet接入方式和各种类型的网络中。原因很简单，NAT不仅完美地解决了lP地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。这里将用来解决公司与外网的通信。

VLAN：又称虚拟局域网，是指在交换局域网的基础上，采用网络管理软件构建的可跨越不同网段、不同网络的端到端的逻辑网络。一个VLAN组成一个逻辑子网，即一个逻辑广播域，它可以覆盖多个网络设备，允许处于不同地理位置的网络用户加入到一个逻辑子网中。而VLAN可以很好将不同VLAN的隔绝通信，刚好符合“同一部门的员工之间可以通信，不同部门之间的员工不能通信”，也是地址规划里的依据之一。

ACL:访问控制列表(ACL)是一种基于包过滤的访问控制技术。它可以根据设定的条件对接口上的数据包进行过滤，允许其通过或丢弃。访问控制列表被广泛地应用于路由器和三层交换机，借助于访问控制列表，可以有效地控制用户对网络的访问，从而最大程度地保障网络安全。

## 3、分析与设计

3.1三层交换机划分子网

需要对不同部门划分不同的VLAN,对于划分不公VLAN可以选择二层交换机或三层交换机进行划分。由于又需要让不同部门的部长可以相互通信，二层交换机工作在二层，没有那么灵活。可以考虑用三层交换机进行VLAN划分。因为三层交换机工作在第三层，我们可以根据不同ip进行子网划。可以用acl技术根据不同ip进行访问控制。

3.2 在三层交换机上使用acl技术

由于需要限制不同部门的通信，但是不同部长之间可以相互通信。可以使用ACL技术进行访问控制。限制不同部门网络的通信。但是放行部长和部长间的数据传输。

3.2各种服务放在不同的服务器

各种ftp，web,email,dns服务放在不同的服务器，防止服务器过载而宕机。各种服务器间组成一个小的网络和不同部门的网络区分开来，方便管理。

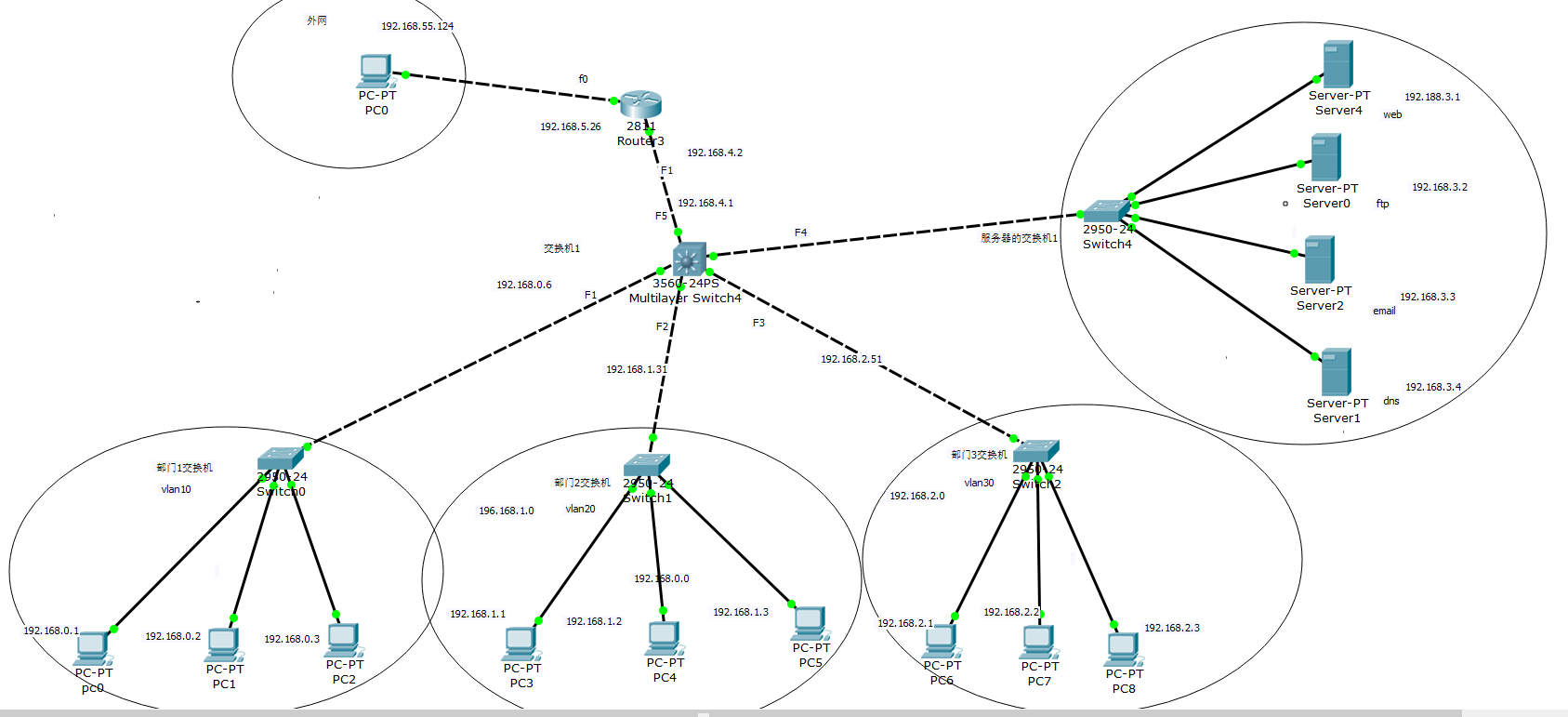
3.3使用NAT技术进行网络地址转换

公司内部主机多，不可能给每一个员工都分配一个外部可访问的ip地址。毕竟ip地址不可能够。而且外部可以直接访问内部的网络，安全性无法保障。我们可以使用nat技术做地址转换。只需要给路由器配置一个外部可以访问的ip。在公司内部使用内部ip， nat技术进行网络地址的转换。把内部地址转换掉，访问外网。同时由于外网无法访问内网，这样公司内部网络的安全性也可以得到保障。

## 4、系统的实现

3.1总体设计

这里给出网络拓扑图

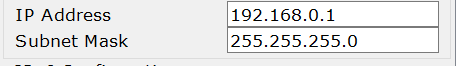


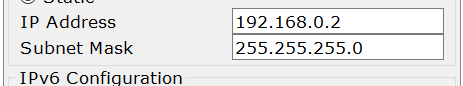
3.2 详细设计

3.2.1分配ip

部门1配置内网ip为192.168.0.0/24，足够6台电脑

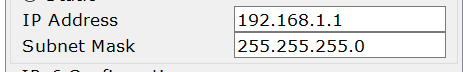
设置192.168.0.1为部长的ip

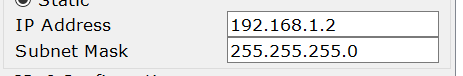




部门2配置内网ip为192.168.1.0/24，足够30台电脑

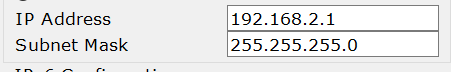
设置192.168.1.1为部长的ip





部门3配置内网ip为192.168.2.0/24，足够50台电脑

设置192.168.2.1为部长的ip





3.2.3三层交换机1配置vlan

|  |
| --- |
| 在交换机Switch3上创建Vlan 10  Switch3 # enable  Switch3 # configure terminal ！进入全局配置模式。  Switch3(config)# vlan 10 ！创建Vlan 10。  Switch3(config-vlan)# name department1 ！将Vlan 10命名为department1。  Switch3(config-vlan)#exit  Switch3(config)#interface fastethernet 0/1 ！进入接口配置模式。  Switch3(config-if)#switchport mode access  Switch3(config-if)#switchport access vlan 10  Switch3(config)#int vlan10  Switch3(config-if)# ip add 192.168.0.6 255.255.255.0 ！给vlan10配置ip  Switch3(config-if)#no shutdown  **第二步：**在交换机SwitchA上创建Vlan 20  Switch3(config)# vlan 20 ！创建Vlan 20。  Switch3(config-vlan)# name department2 ！将Vlan 20命名为department2。  Switch3(config-vlan)#exit  Switch3(config)#interface fastethernet 0/2 ！进入接口配置模式。  Switch3(config-if)#switchport mode acces  Switch3(config-if)#switchport access vlan 20 ！将0/8端口划分到Vlan 20。  Switch3(config)#int vlan20  Switch3(config-if)# ip add 192.168.1.31 255.255.255.0 ！给vlan20配置ip  Switch3(config-if)#no shutdown  **第三步：**在交换机SwitchA上创建Vlan 30  Switch3(config)# vlan 30 ！创建Vlan 30。  Switch3(config-vlan)# name department3 ！将Vlan 30命名为department3。  Switch3(config-vlan)#exit  Switch3(config)#interface fastethernet 0/3 ！进入接口配置模式。  Switch3(config-if)#switchport mode access  Switch3(config-if)#switchport access vlan 30 ！将0/3端口划分到Vlan 30。  Switch3(config-if)# int vlan30  Switch3(config-if)# ip add 192.168.2.51 255.255.255.0 ！给vlan30配置ip  Switch3(config-if)#no shutdown  **第四步：**在交换机SwitchA上创建Vlan 40  Switch3(config)# vlan 40 ！创建Vlan 40。  Switch3(config-vlan)# name server ！将Vlan 40命名为server。  Switch3(config-vlan)#exit  Switch3(config)#interface fastethernet 0/4 ！进入接口配置模式。  Switch3(config-if)#switchport mode access  Switch3(config-if)#switchport access vlan 40 ！将0/4端口划分到Vlan 40。  Switch3(config-if)# int vlan40  Switch3(config-if)# ip add 192.168.3.10 255.255.255.0 ！给vlan40配置ip  Switch3(config-if)#no shutdown  第五步,给接口F5配ip  Switch3(config)#interface fastethernet 0/5  Switch3(config-if)#no switchport  Switch3(config-if)#ip add 192.168.4.1 255.255.255.0  Switch3(config-if)#no shutdown  第六步：配置路由 Switch3(config-if)# ip routing  第七步：配置ospf  Router3(config)#router ospf 100  Router3(config-router)#net  Router3(config-router)#network 192.168.0.0 0.0.0.255 area 0  Router3(config-router)#network 192.168.1.0 0.0.0.255 area 0  Router3(config-router)#network 192.168.2.0 0.0.0.255 area 0  Router3(config-router)#network 192.168.3.0 0.0.0.255 area 0  Router3(config-router)#network 192.168.4.0 0.0.0.255 area 0 |

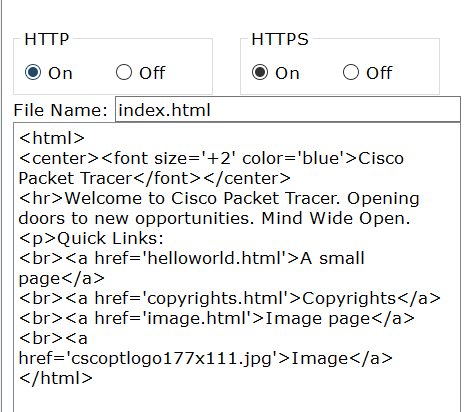
3.2.4各个服务器配置

web服务器配置

1. 配置IP为192.168.3.1

2. 开启服务

3. 添加可以访问的文件

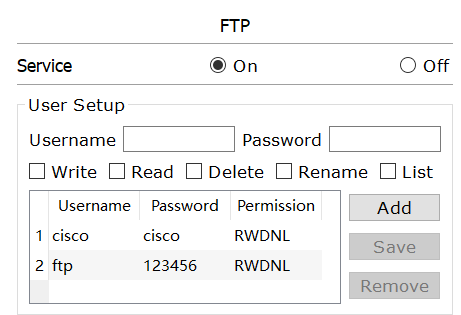


ftp服务器

1. 配置ip为192.168.3.2

2. 开启ftp服务

3. 设置账号密码为：ftp 123456



email服务器

1. 配置ip为192.168.3.3

2. 开启email服务

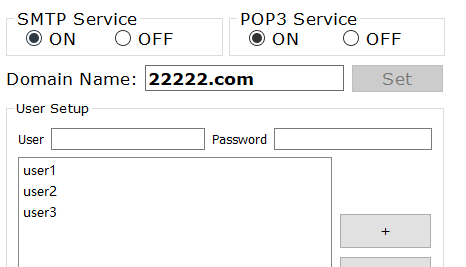
3. 设置账号密码为：

user1 123456

user2 123456

…

4. 配置服务器域名为2222.com

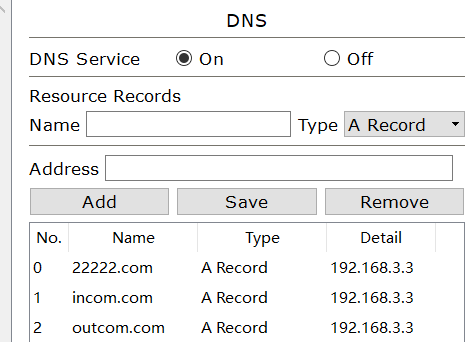


dns服务器

1. 配置ip为192.168.3.4

2. 开启dns服务

3. 给各个主机配置dns服务器ip



对于刚才的邮件，也需要添加域名解析，对于需要使用到DNS的主机也需要配置DNS的ip

3.2.4 设置访问控制ACL

在三层交换机中继续配置

|  |
| --- |
| 第一步，设置部门1拒绝访问部门2和3，但是部长可以访问  Switch3(config)#ip access-list extended deny1  ！设置允许访问部长2  Switch3(config-ext-nacl)# permit ip 192.168.0.1 0.0.0.0 192.168.1.1 0.0.0.0  ！设置允许访问部长3  Switch3(config-ext-nacl)# permit ip 192.168.0.1 0.0.0.0 192.168.2.1 0.0.0.0  Switch3(config-ext-nacl)# deny ip 192.168.0.1 0.0.0.255 192.168.1.0 0.0.0.255！拒绝部门2访问  Switch3(config-ext-nacl)# deny ip 192.168.0.1 0.0.0.255 192.168.2.0 0.0.0.255 !拒绝部门3访问  Switch3(config-ext-nacl)# permit ip any any  ！添加到网络vlan 10  Switch3(config)#int vlan 10  Switch3(config)#ip access-group deny1 in  第二步，设置部门2拒绝访问部门1和3，但是部长可以访问  Switch3(config)#ip access-list extended deny2  ！设置允许访问部长1  Switch3(config-ext-nacl)# permit ip 192.168.1.1 0.0.0.0 192.168.0.1 0.0.0.0  ！设置允许访问部长3  Switch3(config-ext-nacl)# permit ip 192.168.1.1 0.0.0.0 192.168.2.1 0.0.0.0  Switch3(config-ext-nacl)# deny ip 192.168.1.1 0.0.0.255 192.168.0.0 0.0.0.255！拒绝部门1访问  Switch3(config-ext-nacl)# deny ip 192.168.1.1 0.0.0.255 192.168.2.0 0.0.0.255 !拒绝部门3访问  Switch3(config-ext-nacl)# permit ip any any  ！添加到网络vlan 20  Switch3(config)#int vlan 20  Switch3(config)#ip access-group deny2 in  第三步，设置部门3拒绝访问部门1和2，但是部长可以访问  Switch3(config)#ip access-list extended deny3  ！设置允许访问部长1  Switch3(config-ext-nacl)# permit ip 192.168.2.1 0.0.0.0 192.168.0.1 0.0.0.0  ！设置允许访问部长2  Switch3(config-ext-nacl)# permit ip 192.168.2.1 0.0.0.0 192.168.1.1 0.0.0.0  Switch3(config-ext-nacl)# deny ip 192.168.2.1 0.0.0.255 192.168.0.0 0.0.0.255！拒绝访问部门1  Switch3(config-ext-nacl)# deny ip 192.168.2.1 0.0.0.255 192.168.1.0 0.0.0.255 !拒绝访问部门2  Switch3(config-ext-nacl)# permit ip any any  ！添加到网络vlan 30  Switch3(config)#int vlan 30  Switch3(config)#ip access-group deny3 in  Switch3(config)#access-list 1 permit any |

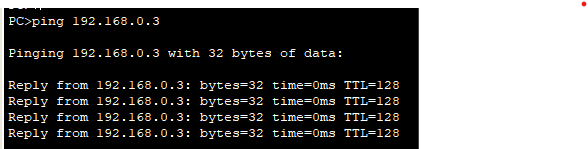
3.2.5 设置NAT路由器

|  |
| --- |
| Switch3 # enable  Switch3 # configure terminal ！进入全局配置模式  第一步，先设置与内网相连端口的ip  Router(config)# interface fastethernet0/1  Router (config-if)#ip add 192.168.4.2 255.255.255.0  Router (config-if)#no shutdown  第二步，配置与外网相连端口ip，该ip是外网ip  Router(config)# interface fastethernet0/0  Router (config-if)#ip add 192.168.5.26 255.255.255.0  Router (config-if)#no shutdown  Router (config-if)#exit  第三步，配置静态路由  Router (config-if)#ip route 0.0.0.0 0.0.0.0 f0/0  第三步，配置acl  Router(config)#access-list 1 permit any !允许内网的所有  第四步，配置可转换的公网IP地址池  ！地址池是向ISP（Internet服务提供商，如电信、联通）申请得到的，内网主机（上一步ACL中所包含的IP地址）到外网的访问，内网地址将被动态的、随机的转换为这些合法地址。  Router(config)#ip nat pool webtest 172.16.1.20 172.16.1.30 netmask 255.255.255.0 //设置内部全局地址，也就是转化成的地址池，为172.16.1.20 到172.16.1.30  Router(config)#ip nat inside source list 1 pool webtest //将访问控制的列表和池进行匹配  Router(config)#int fa0/1  Router(config-if)#ip nat inside //部署在端口中  Router(config-if)#int fa0/0  Router(config-if)#ip nat outside //部署在端口中  第五步，配置ospf  Router3(config)#router ospf 100  Router3(config-router)#net  Router3(config-router)#network 192.168.5.0 0.0.0.255 area 0  Router3(config-router)#network 192.168.4.0 0.0.0.255 area 0 |

## 5、系统部署与运行

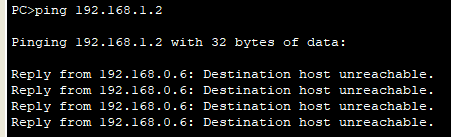
1. 各部门之间进行隔离

192.168.0.2 ping 192.168.0.3



属于同一个部门，可以ping通

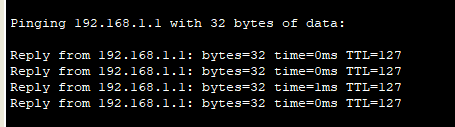
192.168.0.2 ping 192.168.1.2



不输于一个部门，无法ping通

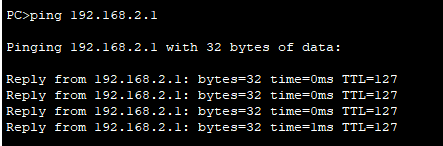
2. 部长可以相互通信

192.168.0.1 ping 192.168.1.1



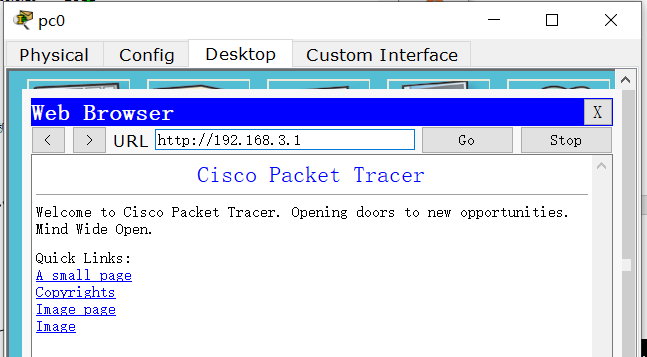
可以ping通

192.168.1.1 ping 192.168.2.1



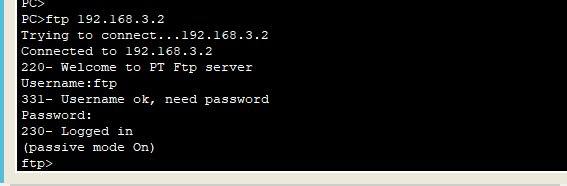
可以ping通

3. 访问http



可以访问

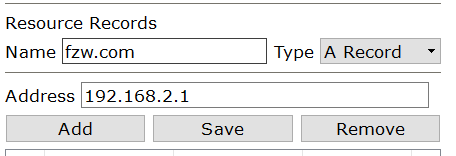
4. 访问ftp

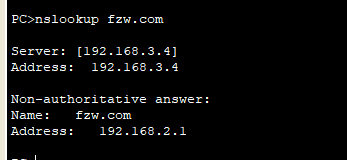


可以成功登录ftp

5.dns解析

添加一条记录

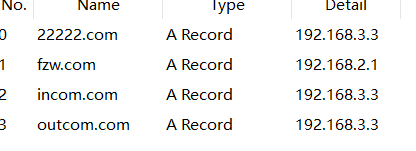




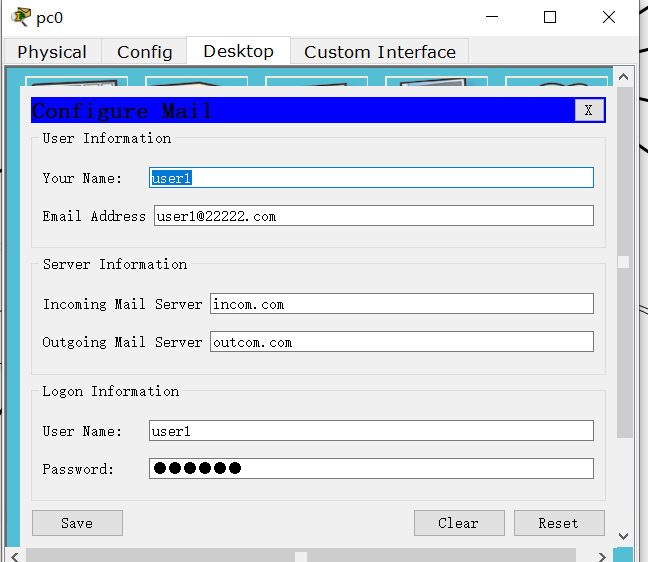
解析成功

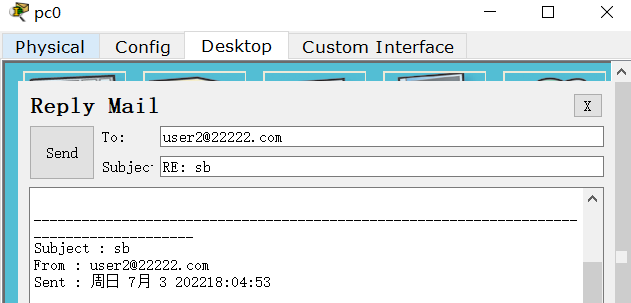
6. email 邮件发送

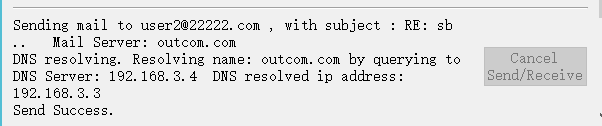
Dns中加上email服务器域名的解析



配置发送端并发送邮件

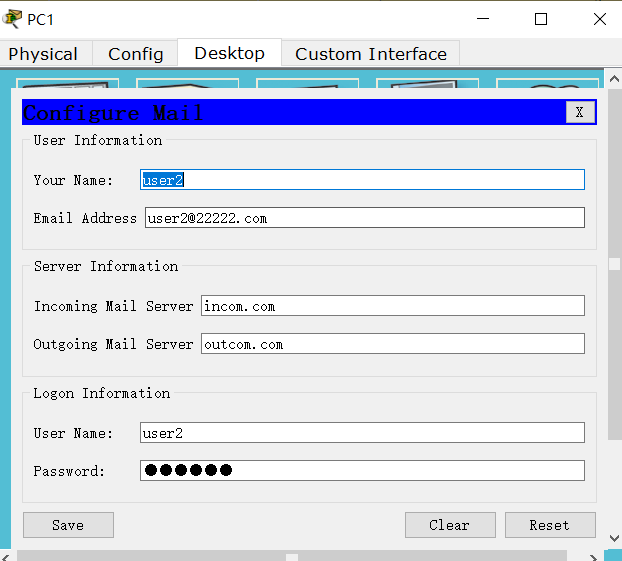


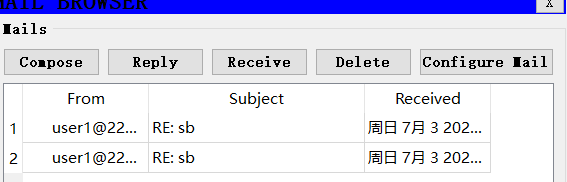




发送成功

配置接收端并接收邮件

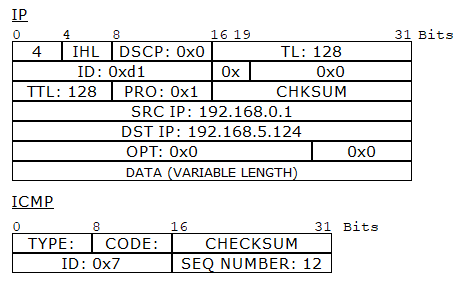




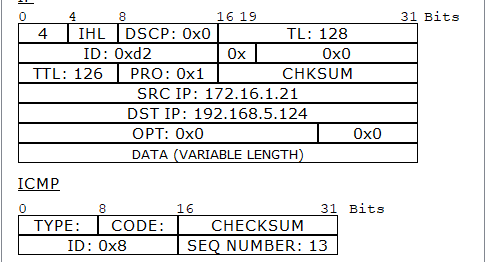
接收成功

7.NAT地址转换测试

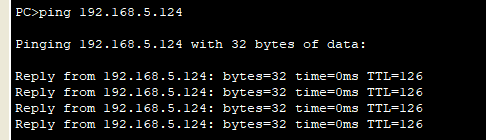
发送的ip包源地址是192.168.0.1



Ip包经过路由器时源地址发生了改变



Ping外网成功



## 6、总结

通过该课程设计可以使之前做过的实验得到很好的实践。通过nat技术做地址转换，那么在公司内部就不需要考虑ip地址不够的问题。还是非常方便。

通过vlan和acl技术，可以划分不同的网络，还可以根据不同的ip进行精准的访问控制，非常灵活。

不过有一些东西并没有做好。比如一个公司对网络的健壮性要求比较高。而且一个三层交换机和一个路由器也不一定可以处理公司那么多的流量。所以可以进一步的扩展。设置两个路由器，两个三层交换机等。可以做一些负载均衡。有一个主路由器，主三层交换机。单主交换机无法工作时，另一个交换机还可以工作，那么出现一些问题不至于网络直接就断掉。