同济大学
TONGJI UNIVERSITY

《计算机网络实验》

期末项目课程设计

基于Packet Tracer的医院局域网的仿真设计

小组成员

1950849 李乐天

1951477 孟　宇

1951821 刘睿萌

2052522 杨嘉仪

目 录

1. 项目需求分析

1.1 项目要求

某医院有若干部门，如门诊部，急诊部，住院部，检验科，财务部，后勤，人事部，行政管理部门等，每个部门有自己的独立局域网， 且有自己的文件服务器和web服务器（部门内部用）。几个部门连接成一个大的局域网，并通过医院提供接入到互联网的接口（假如医院有两个公网IP 地址（IPV4））接入到互联网。 医院统一提供一个外网访问的邮件服务器和web服务器，以及一个内部各部门公用的文件服务器。

- 网络提供WIFI接入功能。
- 每个部门有若干内部独立的局域网。
- 医院局域网提供VoIP服务。
- 随机抓取（在Packet Tracer内）某些类型的数据包并解读，如TCP, IP, MAC等（需现场演示）。

1.2 需求分析

以医院中只有门诊部，急诊部，行政管理部门，人事部这四个部门为例，网络需要分成四个网络，每个网络属于一个VLAN。

- 各层网络要求互相访问。
- 需要访问外网，配置NAT协议。
- 为用户配置DHCP使其可以自动获取IP地址。
- 需要配置ACL访问控制实现各部门专用的文件服务器和Web服务器。
- 配置动态路由协议EIGRP，实现全网可达。(这里我们最开始尝试RIP了，但最终选择EIGRP，这个原因我们将在原理部分讲解）
- 配置服务器，使用户可以访问 www 服务器，ftp 服务器和邮件服务器。
- 提供WiFi接入。
- 配置IP电话。

除此之外，在查阅一些博客资料中，我们发现：有时搭建局域网时，为了保证可靠性，会配置热备份协议，它确保了当网络边缘设备或接入链路出现故障时，用户通信能迅速并透明的恢复， 以此为IP网络提供冗余性。为了较为真实的还原医院局域网，我们也尝试配置了热备份协议，具体来讲，当一个三层交换机出现故障时，可以由另一台交换机暂时顶替该交换机的工作，从而保障网络的可靠性。

2. 原理说明

2.1 VLAN

VLAN（Virtual Local Area Network）的中文名为"虚拟局域网"。

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参考模型的第2层和第3层，一个VLAN就是一个广播域，VLAN之间的通信是通过第3层的路由器来完成的。与传统的局域网技术相比较，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；可以控制广播活动；可提高网络的安全性。

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。

在我们的各个部门的小局域网络中，采用了VLAN技术。将门诊部，急诊部，行政管理部门，人事部四个部分划分为四个小的局域网。

2.2 DHCP

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）通常被应用在大型的局域 网络环境中，主要作用是集中的管理、分配IP地址，使网络环境中的主机动态的获得IP地址、 Gateway地址、DNS服务器地址等信息，并能够提升地址的使用率。

DHCP协议采用客户端/服务器模型，主机地址的动态分配任务由网络主机驱动。当DHCP服务器接收到来自网络主机申请地址的信息时，才会向网络主机发送相关的地址配置等信息，以实现网络主机地址信息的动态配置。

2.3 ACL

访问控制列表ACL（Access Control List）是由一条或多条规则组成的集合。所谓规则，是指描述报文匹配条件的判断语句，这些条件可以是报文的源地址、目的地址、端口号等。

ACL本质上是一种报文过滤器，规则是过滤器的滤芯。设备基于这些规则进行报文匹配，可以过滤出特定的报文，并根据应用ACL的业务模块的处理策略来允许或阻止该报文通过。

借助ACL，可以实现以下功能：

(1) 提供安全访问：若医院重要服务器资源被随意访问，医院的机密信息容易泄露，造成安全隐患。使 用ACL可以指定用户访问特定的服务器、网络与服务，从而避免随意访问的情况。

(2) 防止网络攻击：Internet病毒肆意侵略企医院内网，内网环境的安全性堪忧。使用ACL可以封堵高危端口，从而达成为外网流量的阻塞。

(3) 提高网络带宽利用率：网络带宽被各类业务随意挤占，服务质量要求最高的语音、视频业务的带宽得不到保障，造成用户体验差。使用ACL实现对网络流量的精确识别和控制，限制部分网 络流量从而保障主要业务的质量。

在项目中要求各个部门内部的文件服务器和Web服务器时是独立的，也就是说，各个部门内部 的服

务器不应该被其他部门访问到。因此，我们采用ACL对访问进行控制。

2.4 NAT

NAT（Network Address Translation，网络地址转换）是1994年提出的。当在专用网内部的一些主机本来已经分配到了本地IP地址（即仅在本专用网内使用的专用地址），但现在又想和因特网上 的主机通信（并不需要加密）时，可使用NAT方法。

这种方法需要在专用网（私网IP）连接到因特网（公网IP）的路由器上安装NAT软件。装有NAT 软件的路由器叫做NAT路由器，它至少有一个有效的外部全球IP地址（公网IP地址）。这样，所有使 用本地地址（私网IP地址）的主机在和外界通信时，都要在NAT路由器上将其本地地址转换成全球IP 地址，才能和因特网连接。

在我们的配置过程中，我们使用到了NAT转换对从而为提供一个外网访问的邮件服务器和web服务器。

2.5 EIGRP协议

在我们最初配置时，是采用RIP协议的。但是后来发现外网是无法访问内网的Web服务器，在验证中也发现外网传来的包虽然已经进入了Router0，但是包在Router0所处的局域网下四处分发，迟迟也无法分配到Web服务器中。经过查阅资料，我们发现，我们的拓扑结构实际上是一个负载不均衡的结构。但是RIP只适用于负载均衡的网络。因此我们最终采用EIGRP协议用于替代RIP协议。

EIGRP（Enhanced Interior Gateway Routing Protocol）即增强内部网关路由协议。EIGRP是 Cisco公司的私有协议（2013年已经公有化）。 EIGRP结合了链路状态和距离矢量型路由选择协议的 Cisco专用协议，采用弥散修正算法（DUAL）来实现快速收敛，可以不发送定期的路由更新信息以 减少带宽的占用，支持Appletalk、IP、Novell和NetWare等多种网络层协议。

它综合了距离矢量和链路状态二者的优点，它的特点包括：

(1) 快速收敛

EIGRP采用DUAL来实现快速收敛。运行EIGRP的路由器存储了邻居的路由表，因此能够快速 适应网络中的变化。如果本地路由表中没有合适的路由且拓扑表中没有合适的备用路由， EIGRP将查询邻居以发现替代路由。查询将不断传播，直到找到替代路由或确定不存在替代路由.

(2) 部分更新

EIGRP发送部分更新而不是定期更新，且仅在路由路径或者度量值发生变化时才发送。更新中 只包含已变化的链路的信息，而不是整个路由表，可以减少带宽的占用。此外，还自动限制这 些部分更新的传播，只将其传递给需要的路由器，因此EIGRP消耗的带宽比IGRP少很多。这种行为也不同于链路状态路由协议，后者将更新发送给区域内的所有路由器。

(3) 支持多种网络层协议

EIGRP使用协议相关模块来支持IPv4、IPv6、Apple Talk和IPX，以满足特定网络层需求。

(4) 使用组播和单播

EIGRP在路由器之间通信时使用组播和单播而不是广播，因此终端站不受路由更新和查询的影响。

EIGRP使用的组播地址是224.0.0.10 。

(5) 支持变长子网掩码（VLSM)

EIGRP是一种无类路由协议，它将通告每个目标网络的子网掩码，支持不连续子网和VLSM 。

(6) 无缝连接数据链路层协议和拓扑结构

EIGRP不要求对OSI参考模型的2层协议做特别的配置，不像OSPF。OSPF对不同的2层协议要 做不同配置，比如以太网和帧中继，EIGRP能够有效的工作在LAN和WAN中，而且EIGRP保证 网络及不会产生环路（loop-free）；而且配置起来很简单；支持VLSM；它使用组播和单播， 不使用广播，这样做节约了带宽；它使用和IGRP一样的度量值算法，但是EIGRP度量值是32 位的；它可以做非等价的路径的负载平衡。

(7) 配置简单

使用EIGRP协议组建网络，路由器配置非常简单，它没有复杂的区域设置，也无需针对不同网 络接口类型实施不同的配置方法。使用EIGRP协议只需使用router eigrp命令在路由器上启动 EIGRP路由进程，然后再使用network命令使能网络范围内的接口即可。

2.6 热备份协议

HSRP（Hot Standby Routing Protocol），即热备份路由选择协议。它是Cisco私有的一种技术，它确保了当网络边缘设备或接入链路出现故障时，用户通信能迅速并透明的恢复，以此为IP网络提供冗余性。通过应用HSRP，可使网络的正常运行时间接近100%，从而满足用户对网络可靠性的要求。为了保证网络的可靠性，我们为网络额外配置了一台多层交换机，从而保证了网络能够更加稳定的运行。

3. 拓扑结构

3.1 总拓扑图

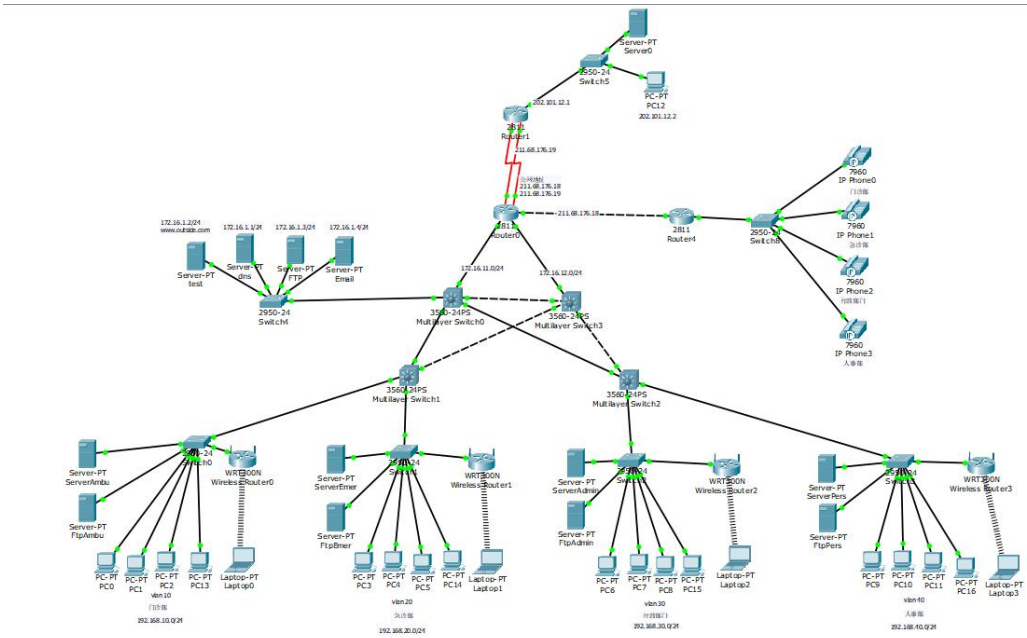
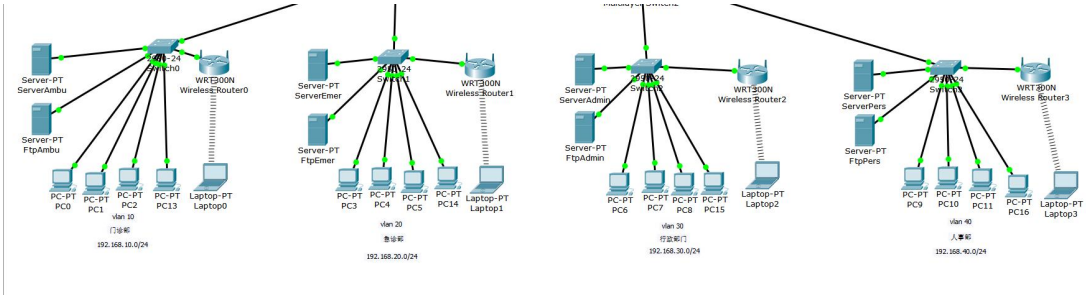


图 3-1 总拓扑图

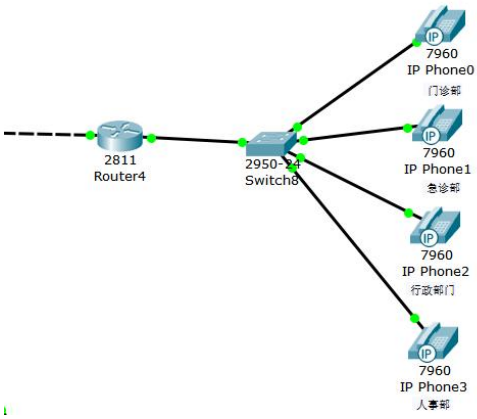
3.2 各个部门

下图部分为我们医院的四个部门，分别为门诊部，急诊部，行政部门与人事部。



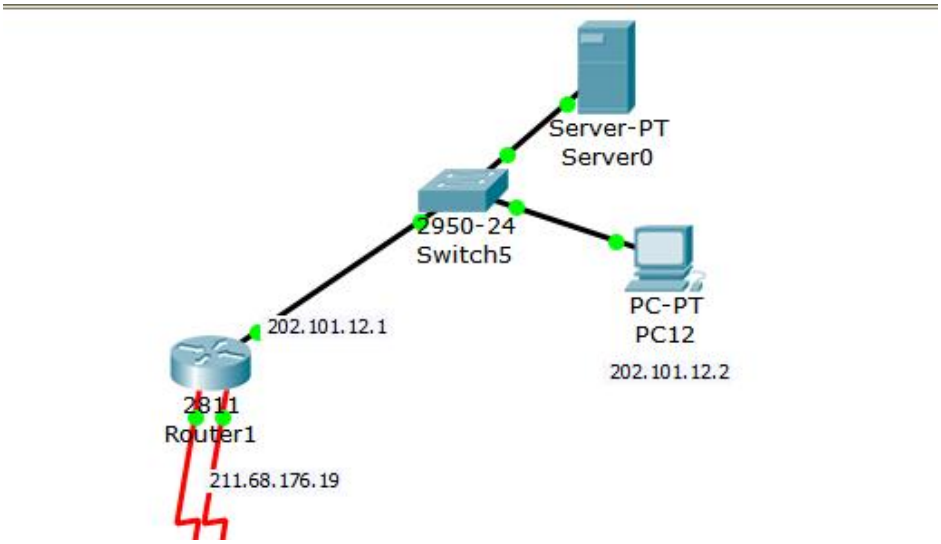
3.3 VOIP 服务

下图部分为我们提供的VOIP服务。



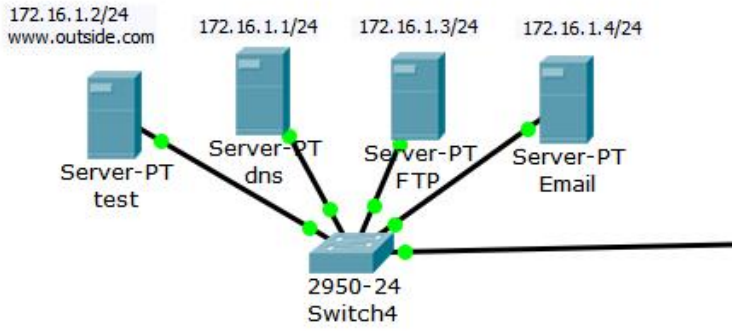
3.4 外网配置

下图为一个简单的外网配置。



3.5 供外网访问的各个服务器

下图为我们所提供的外网访问的Web服务器和邮件服务器，以及内部公用的文件服务器。



4. 实验过程

4.1 VLAN 配置

（1）二层交换机配置：

```
Shell
SW1#config terminal
SW1(config)#vlan 10                                    // 创建VLAN
```

```
SW1(config-vlan)#inter range f0/1-4                    // 给端口分别划分VLAN
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#no shutdown
SW1(config-if-range)#exit
SW1(config)#inter f0/24                                // 设置f0/24端口为trunk模式
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allowed vlan 10
SW1(config-if)#no shutdown
SW1(config-if)#exit

SW2#config terminal
SW2(config)#vlan 20                                    // 创建VLAN
SW2(config-vlan)#inter range f0/1-4                    // 给端口分别划分VLAN
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 20
SW2(config-if-range)#no shutdown
SW2(config-if-range)#exit
SW2(config)#inter f0/24                                // 设置f0/24端口为trunk模式
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport trunk allowed vlan 20
SW2(config-if)#no shutdown
SW2(config-if)#exit

SW3#config terminal
SW3(config)#vlan 30                                    // 创建VLAN
SW3(config-vlan)#inter range f0/1-4                    // 给端口分别划分VLAN
SW3(config-if-range)#switchport mode access
SW3(config-if-range)#switchport access vlan 30
SW3(config-if-range)#no shutdown
SW3(config-if)#exit
SW3(config)#inter f0/24                                // 设置f0/24端口为trunk模式
SW3(config-if)#switchport mode trunk
SW3(config-if)#switchport trunk allowed vlan 30
SW3(config-if)#no shutdown
SW3(config-if)#exit
```

```
SW4#config terminal
SW4(config)#vlan 40                                    // 创建VLAN
SW4(config-vlan)#inter range f0/1-4                    // 给端口分别划分VLAN
SW4(config-if-range)#switchport mode access
SW4(config-if-range)#switchport access vlan 40
SW4(config-if-range)#no shutdown
SW4(config-if-range)#exit
SW4(config)#inter f0/24                                // 设置f0/24端口为trunk模式
SW4(config-if)#switchport mode trunk
SW4(config-if)#switchport trunk allowed vlan 40
SW4(config-if)#no shutdown
SW4(config-if)#exit
```

(2)三层交换机配置：

```
Shell
Multilayer Switch配置
SW#conf ter
SW(config)#vlan 10                                     // 创建VLAN
SW(config-vlan)#vlan 20
SW(config-vlan)#vlan 30
SW(config-vlan)#vlan 40
SW(config-vlan)#inter range f0/1-4
SW(config-if-range)#switchport trunk encapsulation dot1q
SW(config-if-range)#switchport mode trunk              // 设置接口为trunk 模式
SW(config-if-range)#switchport trunk allowed vlan 10,20,30,40
                                                       //允许 VLAN10,20,30,40的流量通过
SW(config-if-range)#no shutdown
SW(config-if-range)#exit
```

4.2 DHCP 配置

```
Shell
配置Multilayer Switch
SW(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
                                                       // 对DHCP地址池地址做排除
SW(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.10
```

```
SW(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.10
SW(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.10
// 设置VLAN10的IP地址。三层交换机不能用单臂路由，划分子端口，所以用此方法分别设置VLAN的地址作为每个DHCP地址池的网关地址
SW(config)#inter vlan 10
SW(config-if)#ip address 192.168.10.252 255.255.255.0
SW(config-if)#ip routing                                    // 开启VLAN间路由的功能
SW(config-if)#exit
SW(config)#ip dhcp pool 10                                  //创建DHCP地址池10
SW(config-dhcp)#network 192.168.10.0 255.255.255.0     // 设置DHCP地址池网段
// 设置默认网关地址。这里设置为VLAN10的IP地址，所有VLAN10的主机通过这个网关地址获取IP
SW(config-dhcp)#default-router 192.168.10.252
SW(config-dhcp)#exit
SW(config)#inter vlan 20
SW(config-if)#ip address 192.168.20.252 255.255.255.0
SW(config-if)#ip routing
SW(config-if)#exit
SW(config)#ip dhcp pool 20
SW(config-dhcp)#network 192.168.20.0 255.255.255.0
SW(config-dhcp)#default-router 192.168.20.252
SW(config-dhcp)#exit
SW(config)#inter vlan 30
SW(config-if)#ip address 192.168.30.252 255.255.255.0
SW(config-if)#ip routing
SW(config-if)#exit
SW(config)#ip dhcp pool 30
SW(config-dhcp)#network 192.168.30.0 255.255.255.0
SW(config-dhcp)#default-router 192.168.30.252
SW(config-dhcp)#exit
SW(config)#inter vlan 40
SW(config-if)#ip address 192.168.40.252 255.255.255.0
SW(config-if)#ip routing
SW(config-if)#exit
SW(config)#ip dhcp pool 40
SW(config-dhcp)#network 192.168.40.0 255.255.255.0
SW(config-dhcp)#default-router 192.168.40.252
```

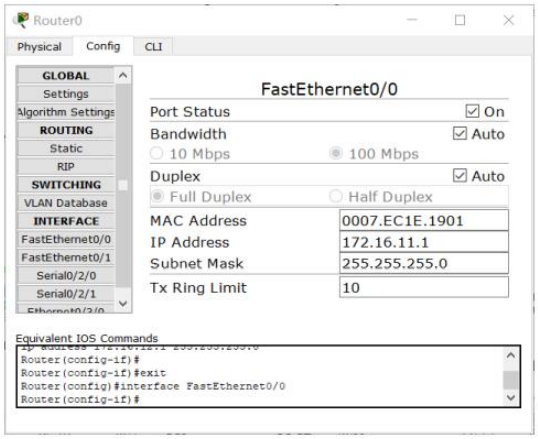
```
SW(config-dhcp)#exit
```

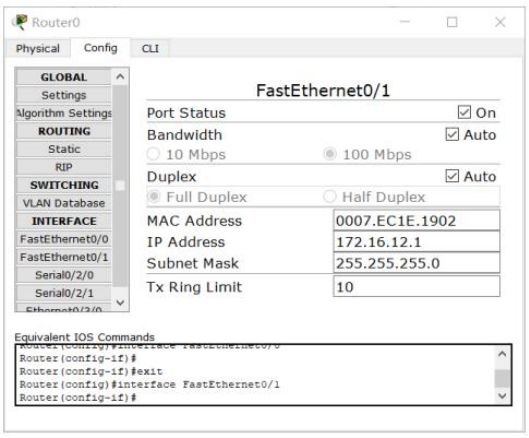
4.3 ACL 访问控制

```
Shell
配置Multilayer Switch
SW(config-if)#inter vlan 10
SW(config-if)#ip access-group 101 in                    //将访问控制列表添加到相应的接口
SW(config-if)#inter vlan 20
SW(config-if)#ip access-group 102 in
SW(config-if)#inter vlan 30
SW(config-if)#ip access-group 103 in
SW(config-if)#inter vlan 40
SW(config-if)#ip access-group 104 in
SW(config)#access-list 101 deny tcp any 192.168.20.0 0.0.0.255 //配置访问控制列表
SW(config)#access-list 101 deny tcp any 192.168.30.0 0.0.0.255
SW(config)#access-list 101 deny tcp any 192.168.40.0 0.0.0.255
SW(config)#access-list 102 deny tcp any 192.168.10.0 0.0.0.255
SW(config)#access-list 102 deny tcp any 192.168.30.0 0.0.0.255
SW(config)#access-list 102 deny tcp any 192.168.40.0 0.0.0.255
SW(config)#access-list 103 deny tcp any 192.168.10.0 0.0.0.255
SW(config)#access-list 103 deny tcp any 192.168.20.0 0.0.0.255
SW(config)#access-list 103 deny tcp any 192.168.40.0 0.0.0.255
SW(config)#access-list 104 deny tcp any 192.168.10.0 0.0.0.255
SW(config)#access-list 104 deny tcp any 192.168.20.0 0.0.0.255
SW(config)#access-list 104 deny tcp any 192.168.30.0 0.0.0.255
SW(config)#access-list 101 permit ip any any                    //解决ACL默认禁止
SW(config)#access-list 102 permit ip any any
SW(config)#access-list 103 permit ip any any
SW(config)#access-list 104 permit ip any any
```

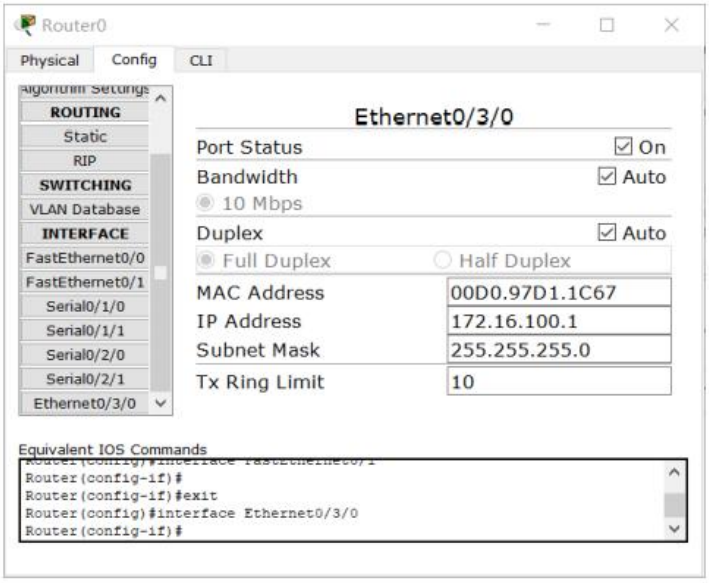
4.4 路由器接口配置

Router0各端口ip配置:



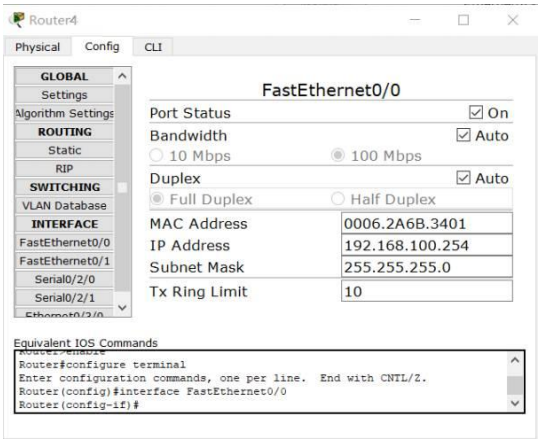


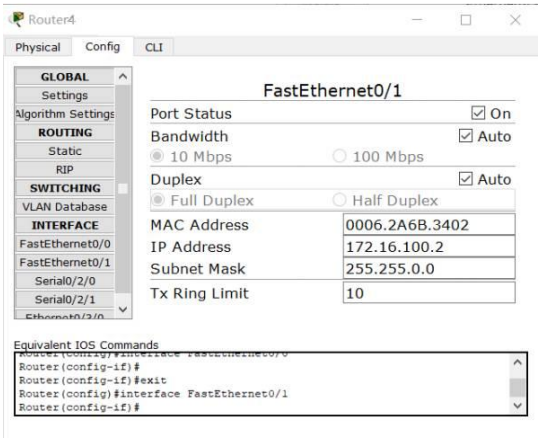
Ethernet0/3/0用于连接医院大局域网IP电话:



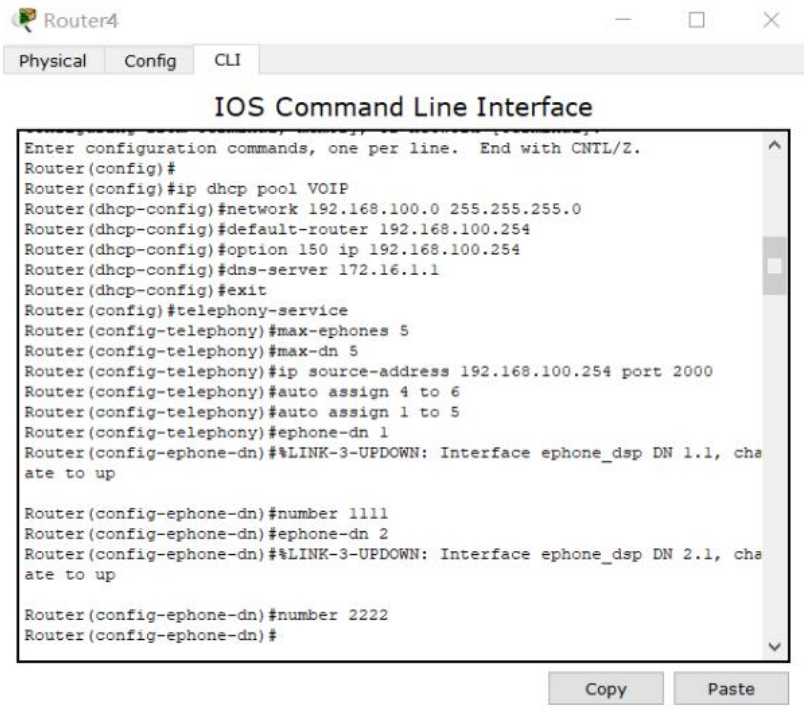
4.5 IP 电话配置

Router4各个端口ip配置:

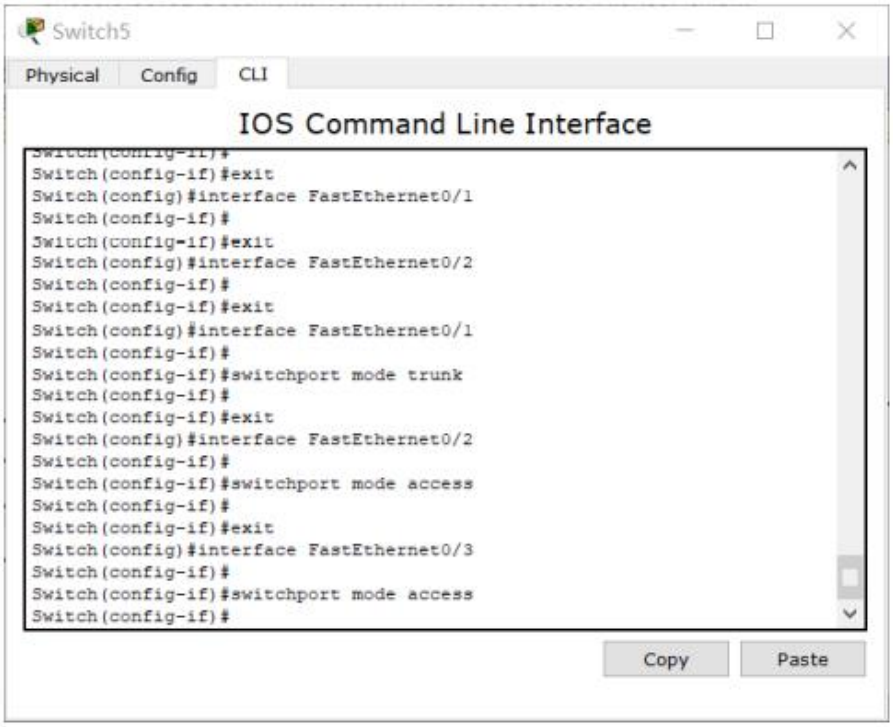




IP电话配置:

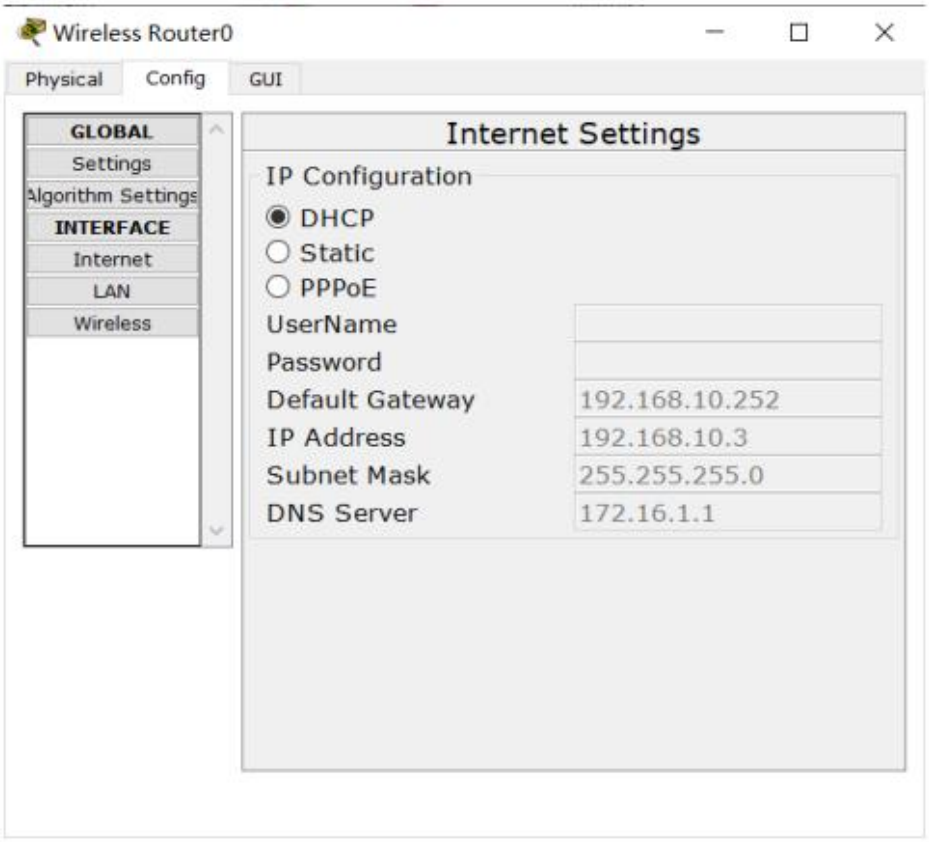


switch配置：

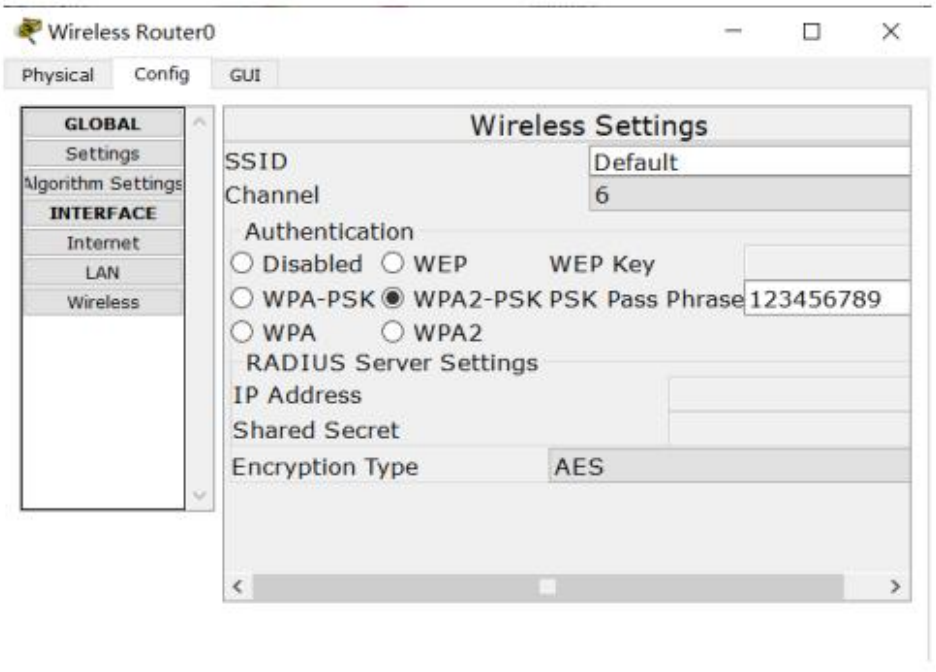


4.6 IP 电话配置

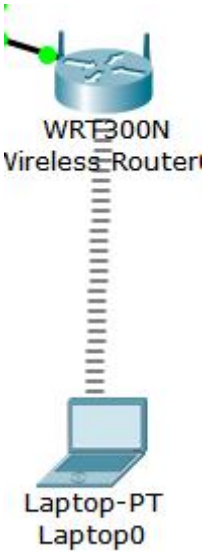
无线路由配置：



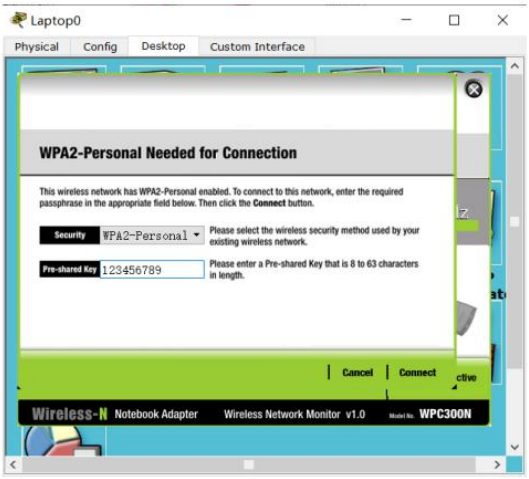
设置WiFi的密码为123456789：

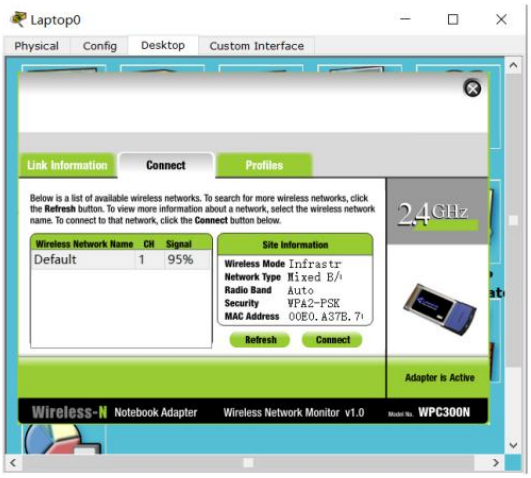


加入笔记本电脑：



输入密码123456789，连接成功：





4.7 IP 电话配置

在项目要求中，涉及到了公网访问问题。对此，我们使用的是NAT方式进行公网配置。按照要求，我们提供了两个公网接口，分别为 211.68.176.18 和 211.68.176.19。

以公网接口 211.68.176.18 为例，首先，我们router的NAT的出入口进行配置。对于 Serial0/2/0，配置其出口的指令为：

```
Shell
Router(config)#interface Serial0/2/0
Router(config-if)#ip address
211.68.176.18 255.255.255.0 Router(config-if)#ip nat outside
```

配置NAT的入口，其指令为：

```
Shell
Router(config)#interface FastEthernet0/0
```

```
Router(config-if)#ip address 172.16.11.1 255.255.255.0
Router(config-if)#ip nat inside source static 172.16.1.2 211.68.176.100
```

此时，即完成了我们内外网的转换。内网 172.16.1.2 ，通过NAT转换至外网接口 211.68.176.100 。而外网用户通过 211.68.176.100 这个网址即可访问到服务器。

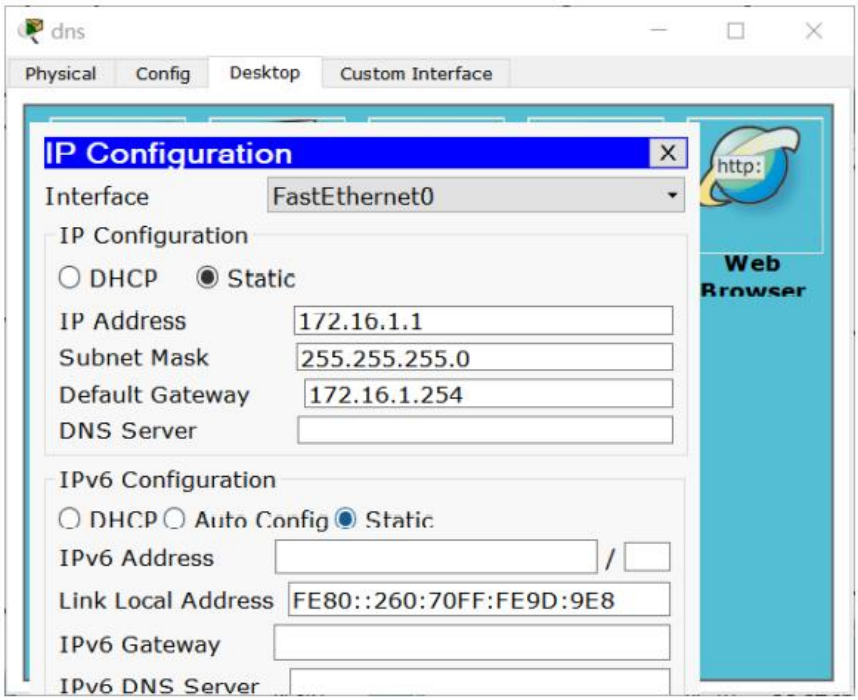
4.8 EIGRP 配置

根据已学知识，这里我们设想使用RIP基于距离向量的路由选择协议，但在实际测试过程中，发现外 部网络无法访问到内部的web网址，查阅资料后发现是我们搭建的拓扑网络不满足RIP的基于距离向 量的负载均衡条件，因此我们选择了CISCO的私有协议EIGRP。

```
Shell
Router(config)#router eigrp 90
Router(config-if)#redistribute static
Router(config-if)#network 172.16.0.0
Router(config-if)#no auto-summary
```

4.9 DNS 服务配置

DNS服务器配置：



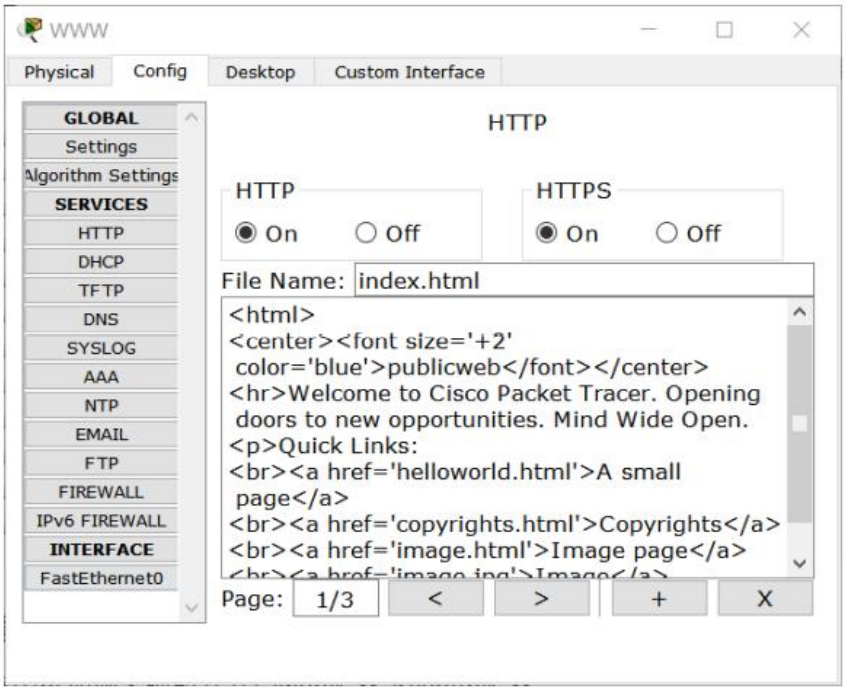
DNS服务配置：

```
Shell
SW(config)#ip dhcp pool 10
```

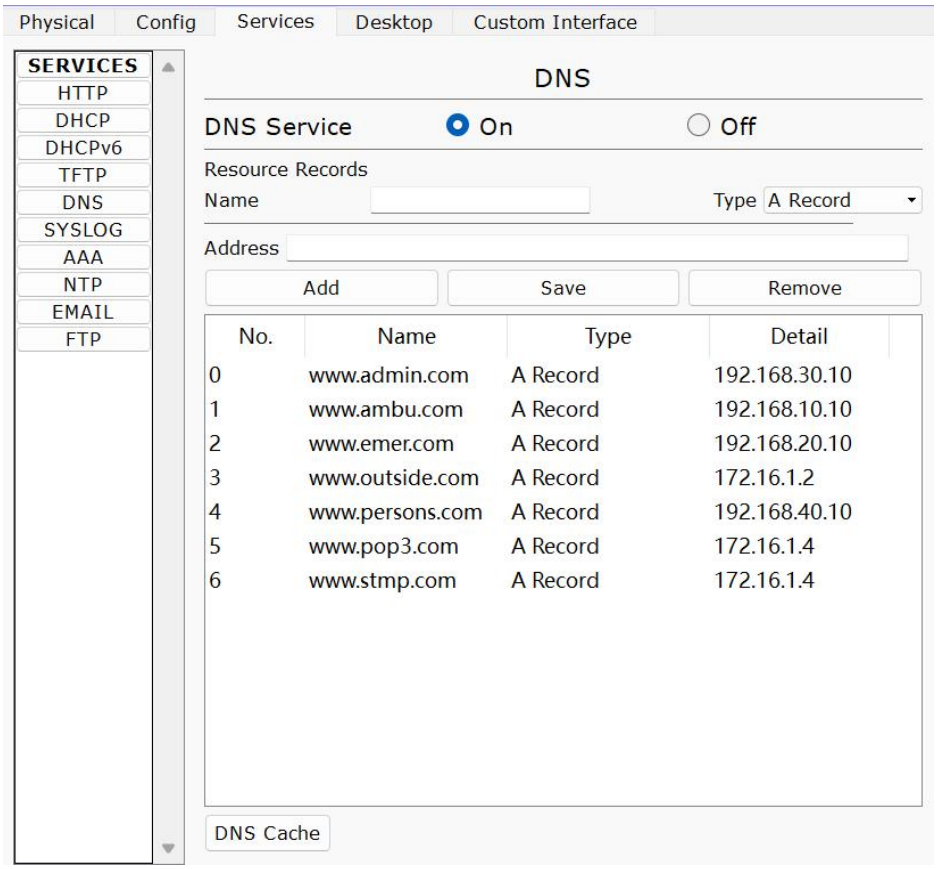
```
SW(config-dhcp)#dns-server 172.16.1.1
SW(config-dhcp)#exit
SW(config)#ip dhcp pool 20
SW(config-dhcp)#dns-server 172.16.1.1
SW(config-dhcp)#exit
SW(config)#ip dhcp pool 30
SW(config-dhcp)#dns-server 172.16.1.1
SW(config-dhcp)#exit
SW(config)#ip dhcp pool 40
SW(config-dhcp)#dns-server 172.16.1.1
SW(config-dhcp)#exit
```

4.10 Web 服务器

开启Web服务器的HTTP服务：

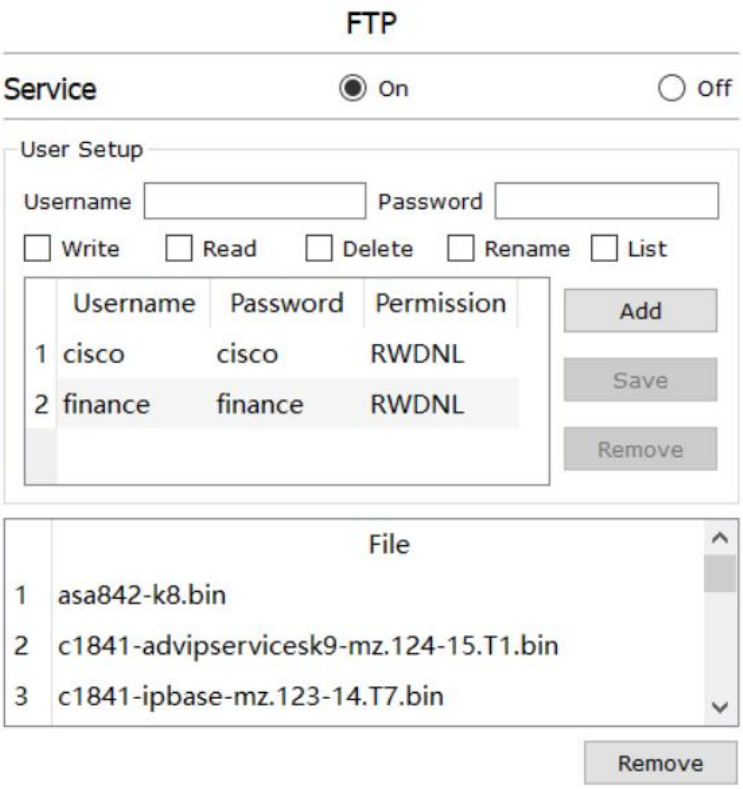


在DNS服务器中添加域名映射：



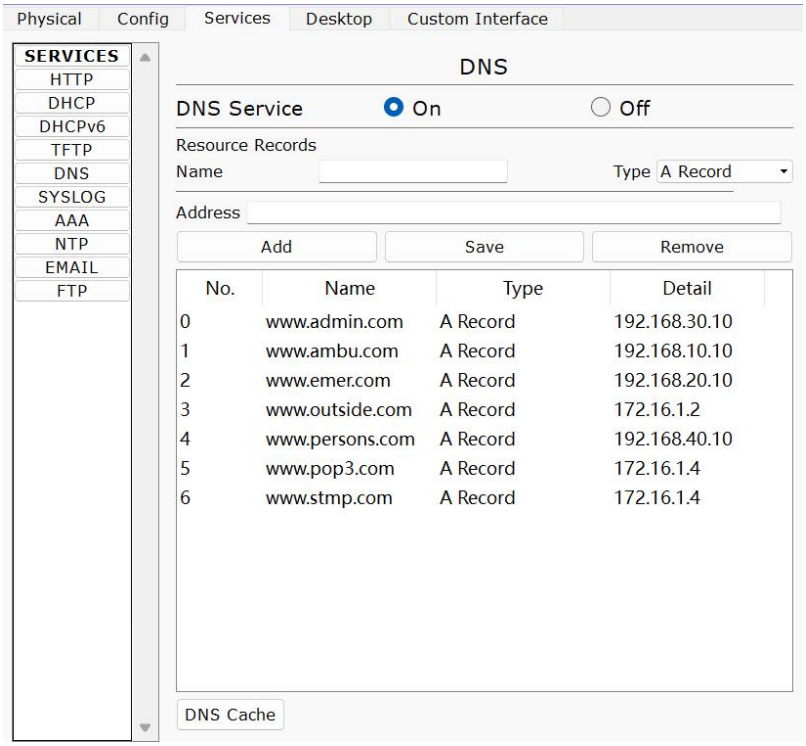
4.11 FTP 服务器

在FTP服务器中开启FTP服务，并添加用户名和密码：

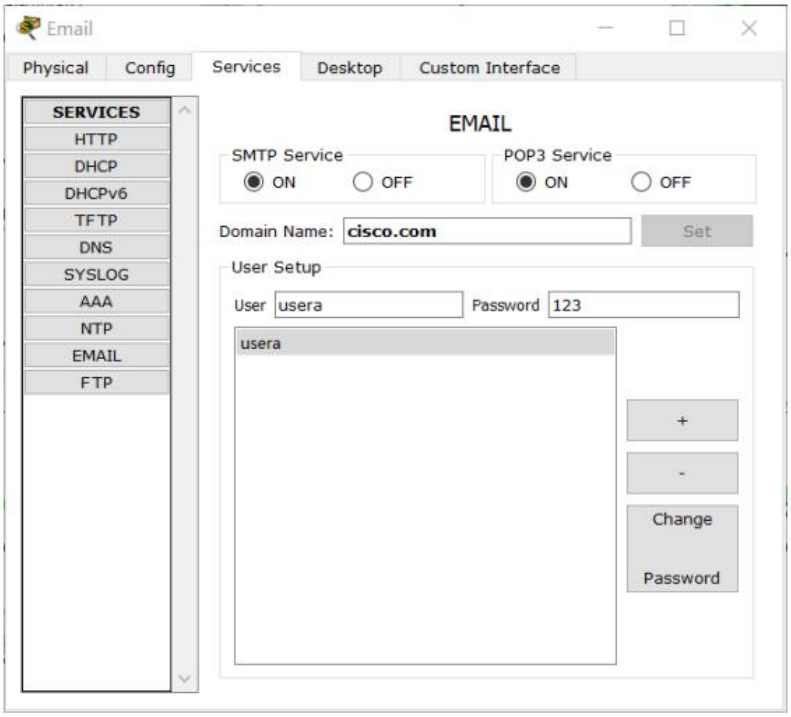


4.12 邮件服务器

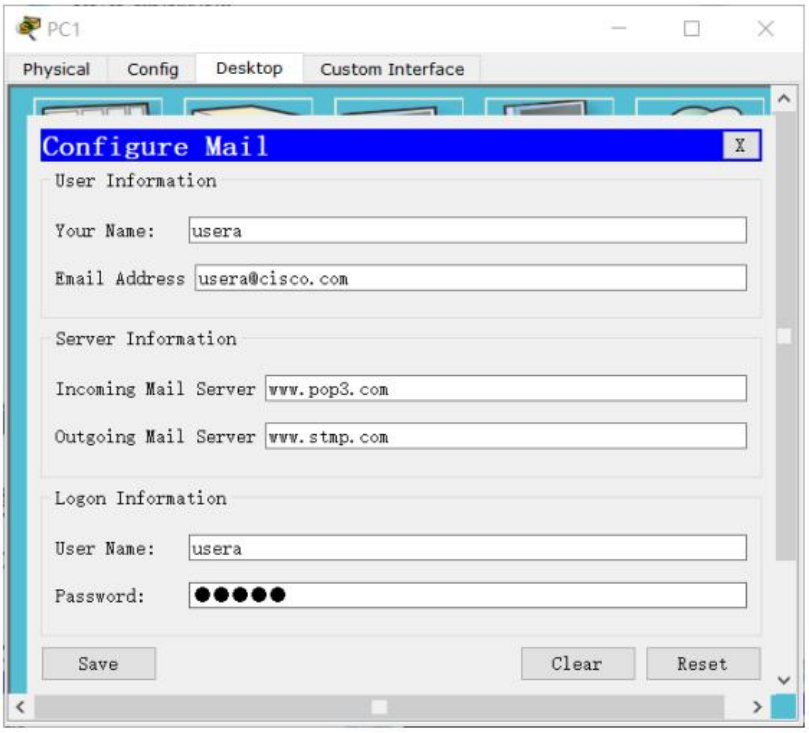
在dns服务器中添加域名映射：



在邮件服务器中打开Email服务，并添加一个用户：



PC机上实现用户登录：



4.13 热备份协议配置

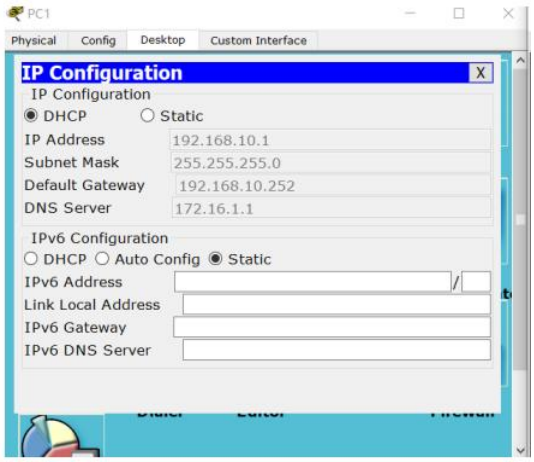
在Multilayer Switch3中输入如下指令:

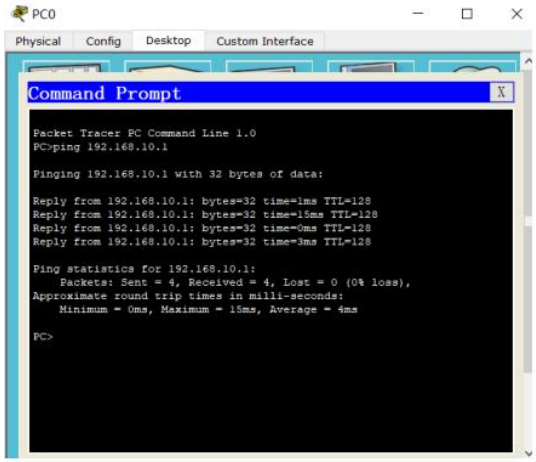
```
Shell
Router(config)#interface Vlan10
Router(config-if)#ip address 192.168.10.253 255.255.255.0
Router(config-if)#standby version 2
Router(config-if)#standby 1 ip 192.168.10.254
Router(config)#interface Vlan20
Router(config-if)#ip address 192.168.20.253 255.255.255.0
Router(config-if)#standby version 2
Router(config-if)#standby 2 ip 192.168.20.254
Router(config)#interface Vlan30
Router(config-if)#ip address 192.168.30.253 255.255.255.0
Router(config-if)#standby version 2
Router(config-if)#standby 3 ip 192.168.30.254
Router(config)#interface Vlan40
Router(config-if)#ip address 192.168.40.253 255.255.255.0
Router(config-if)#standby version 2
Router(config-if)#standby 4 ip 192.168.40.254
```

5. 实验现象

5.1 部门内互通

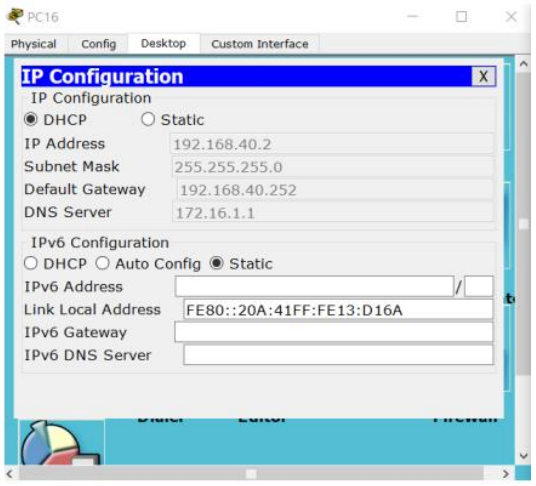
使用PC0与PC1进行ping操作，发现可以ping通：

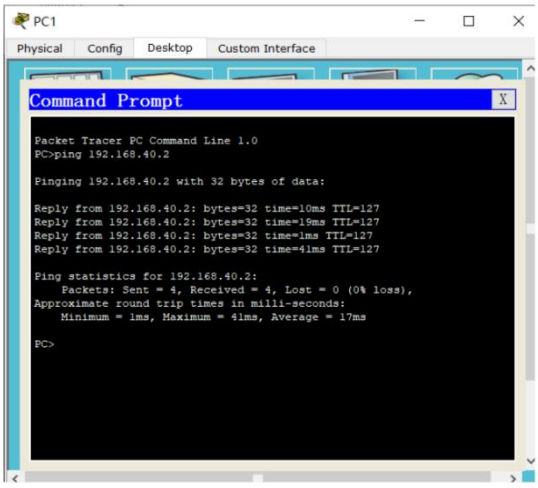




5.2 部门内之间互通

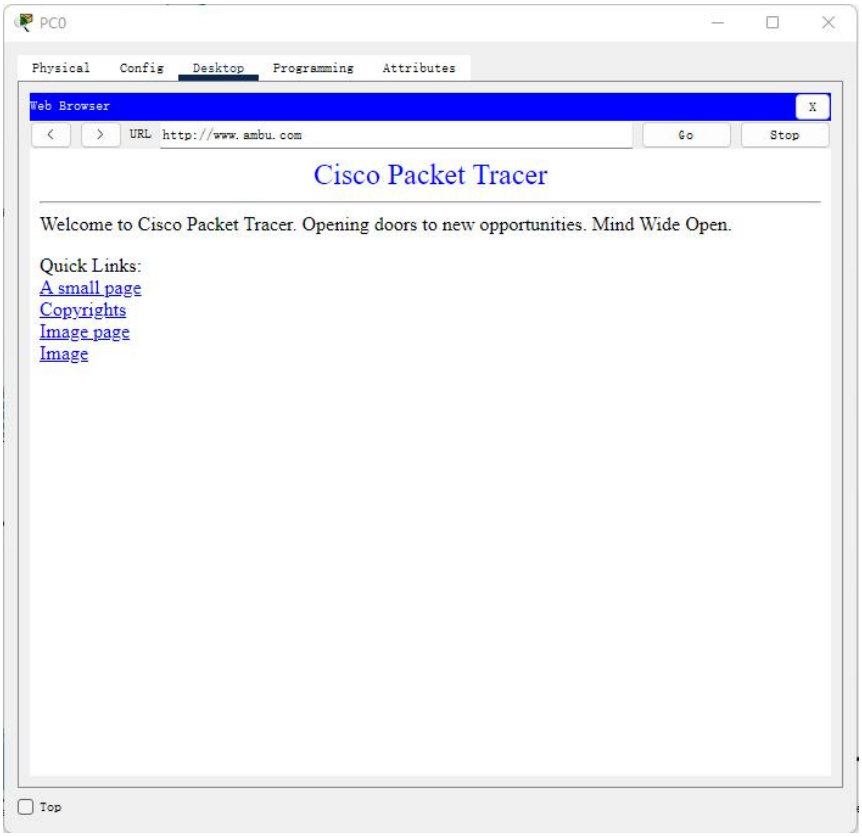
使用PC1和PC16进行ping操作，发现可以ping通：



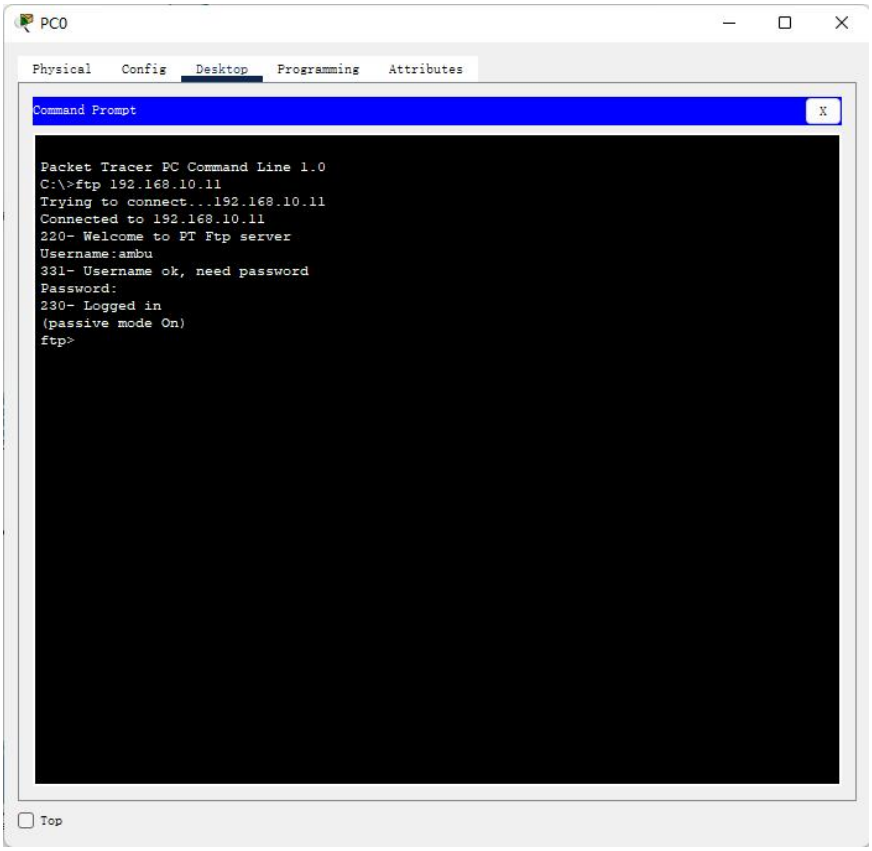


5.3 部门内访问部门内的 Web 服务器和文件服务器

PC0 访问Web服务器 Ambu，www.ambu.com 是其DNS所配置的域名：

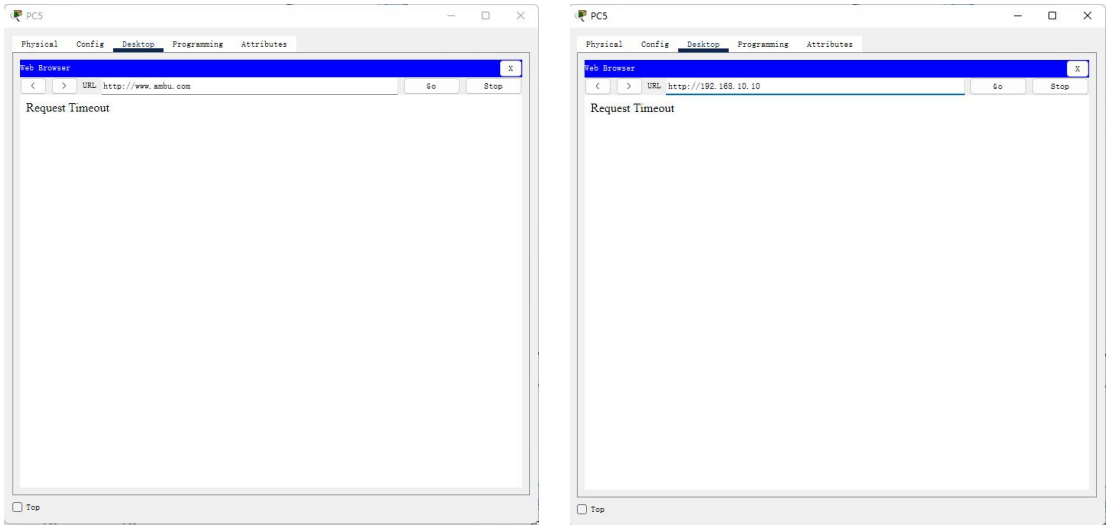


PC0访问文件服务器 Ambu，输入用户名 ambu 和密码 ambu，即可进入文件服务器：

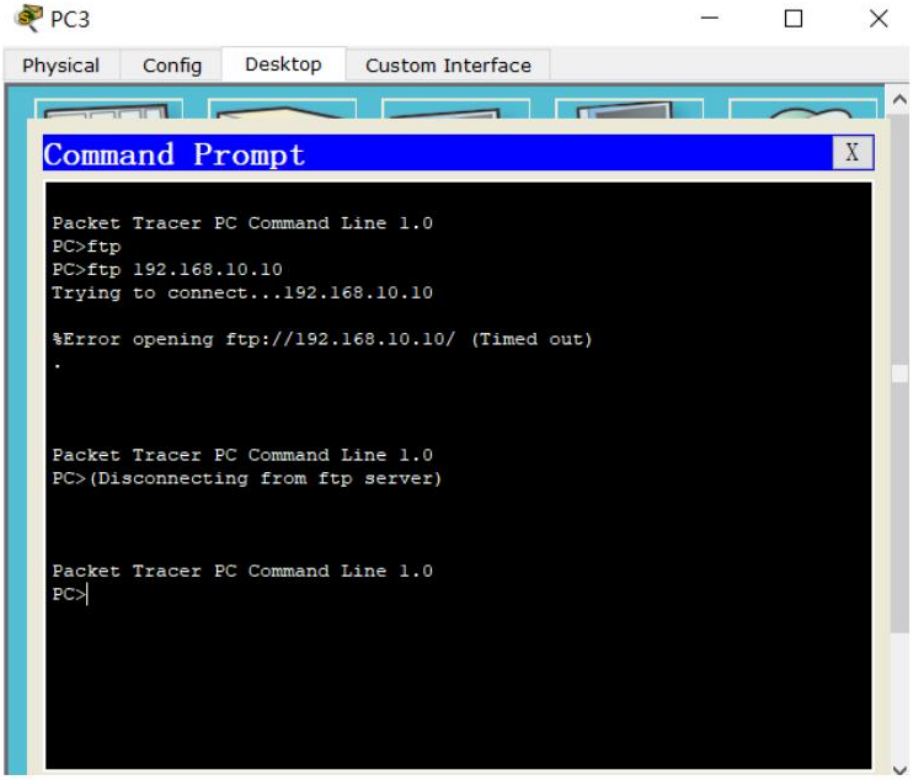


5.4 外部门访问部门内的 Web 服务器和文件服务器

以急诊部 PC3 访问Web服务器 Ambu 为例，可以发现，配置完 ACL 后无论是通过域名还是IP地址都 是无法访问的。



同样，我们对文件服务器进行访问，发现 ACL 阻止了连接：

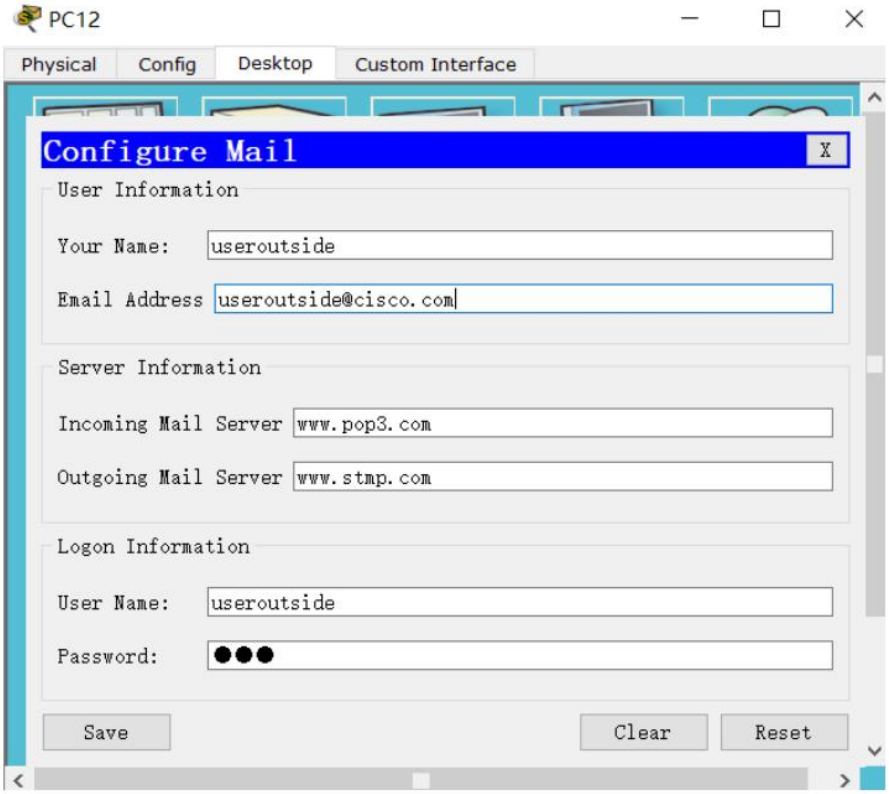


5.5 外网访问 Web 服务器

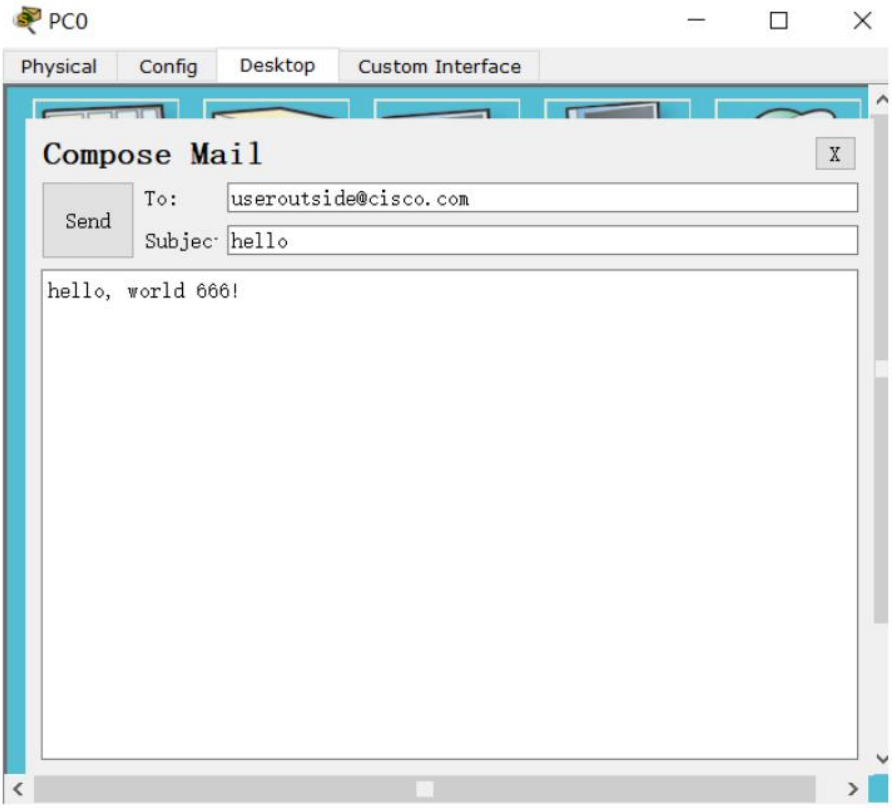
我们在外部配置了一台 PC12，使用其对医院提供的外网访问的 Web 服务器进行访问。在 DNS中 我们配置了其域名为www.outside.com，使用该域名的访问结果如下：

5.6 外网访问邮件服务器

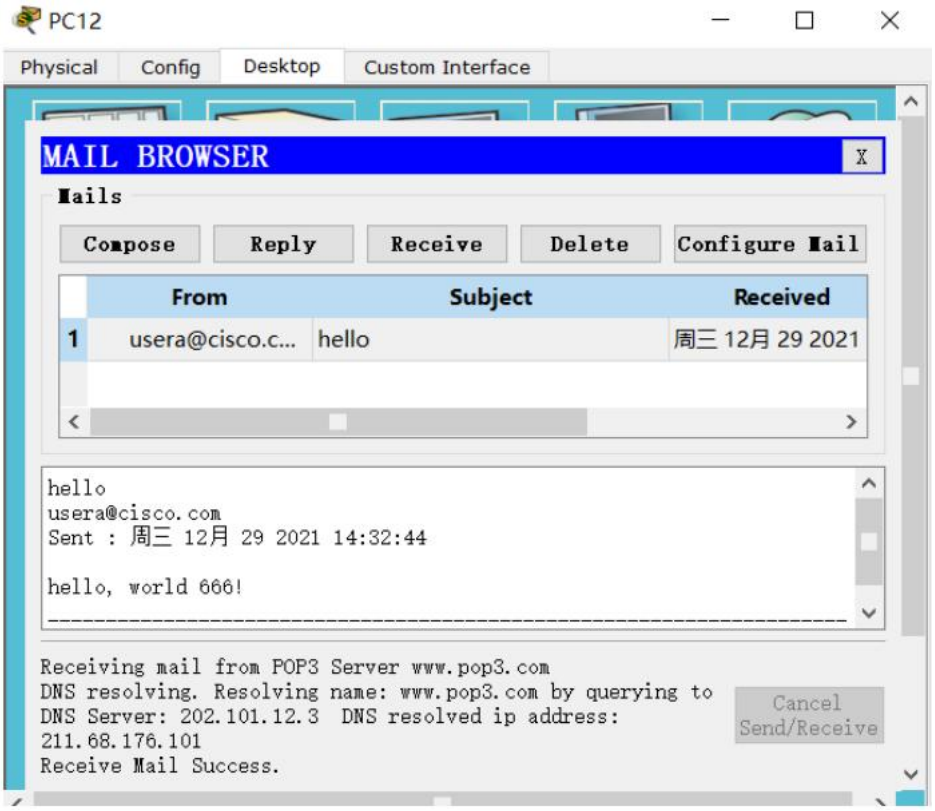
在 PC12 上登录邮箱用户 useroutside：



医院内部的PC1登录邮箱用户 usera，并向 useroutside 发送消息：



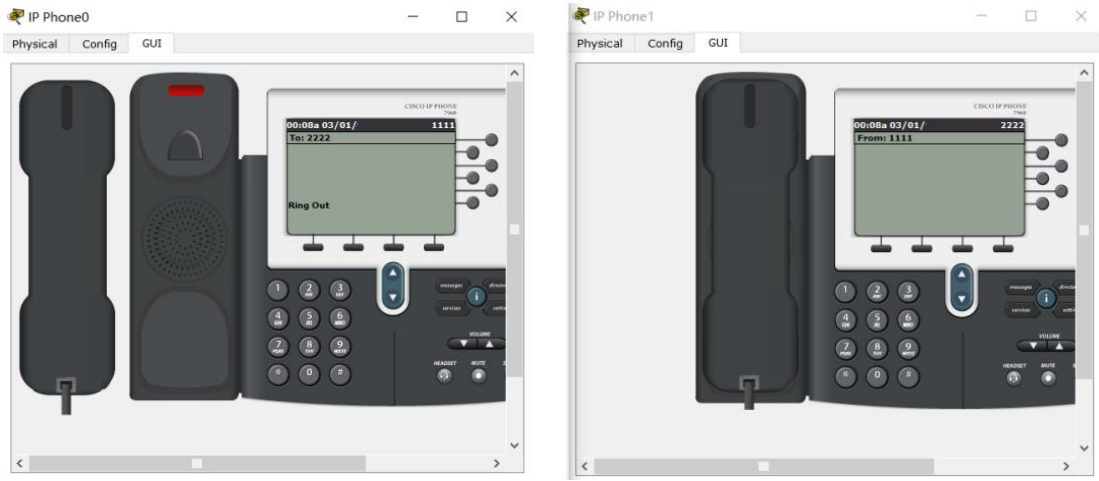
PC12成功接收邮件：



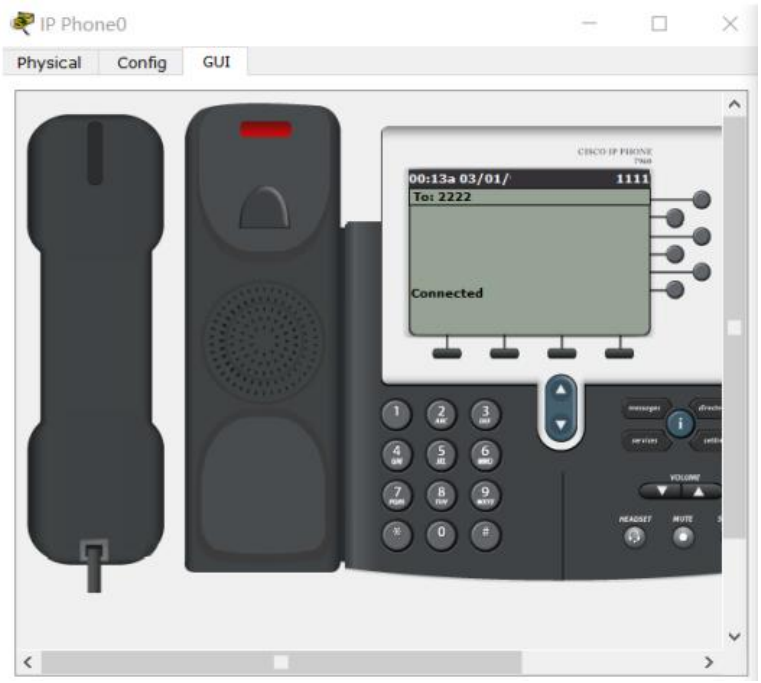
5.7 IP 电话

我们以门诊部 IP Phone0 电话和急诊部 IP Phone1 为例，其中门诊部的电话为 1111 ，急诊部电话为

2222 。我们将电话从 1111 拨打向 2222 ，发现可以 IP Phone1 接收到了来自 IP Phone0 的拨打请求。

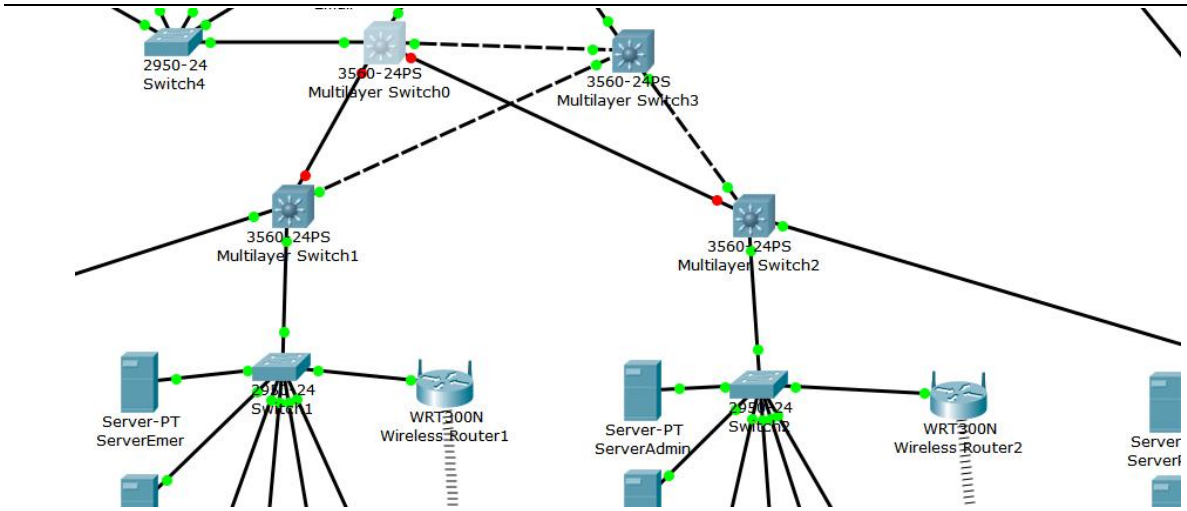


打开 IP Phone1 的话筒，二者可以建立连接：

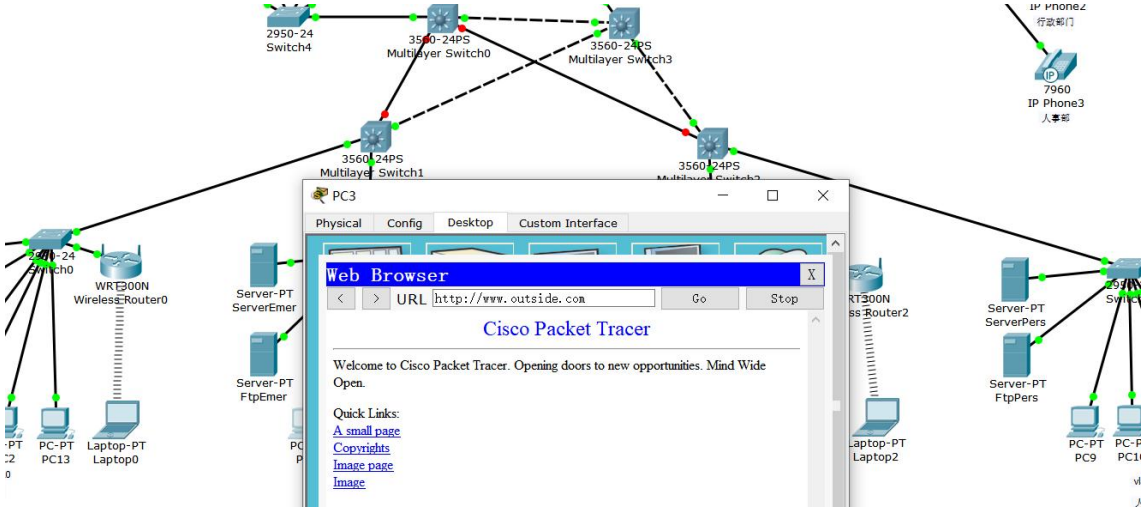


5.8 热备份协议

我们将 Multilayer Switch0 与下面两个路由的连接断开，此时通过 Multilayer Switch0 是无法进 行通信的。但是由于我们配置了热备份协议，因此，PC 机仍可以通过Multilayer Switch3进行通信连接。如图所示，我们断开f0/1，f0/2端口。

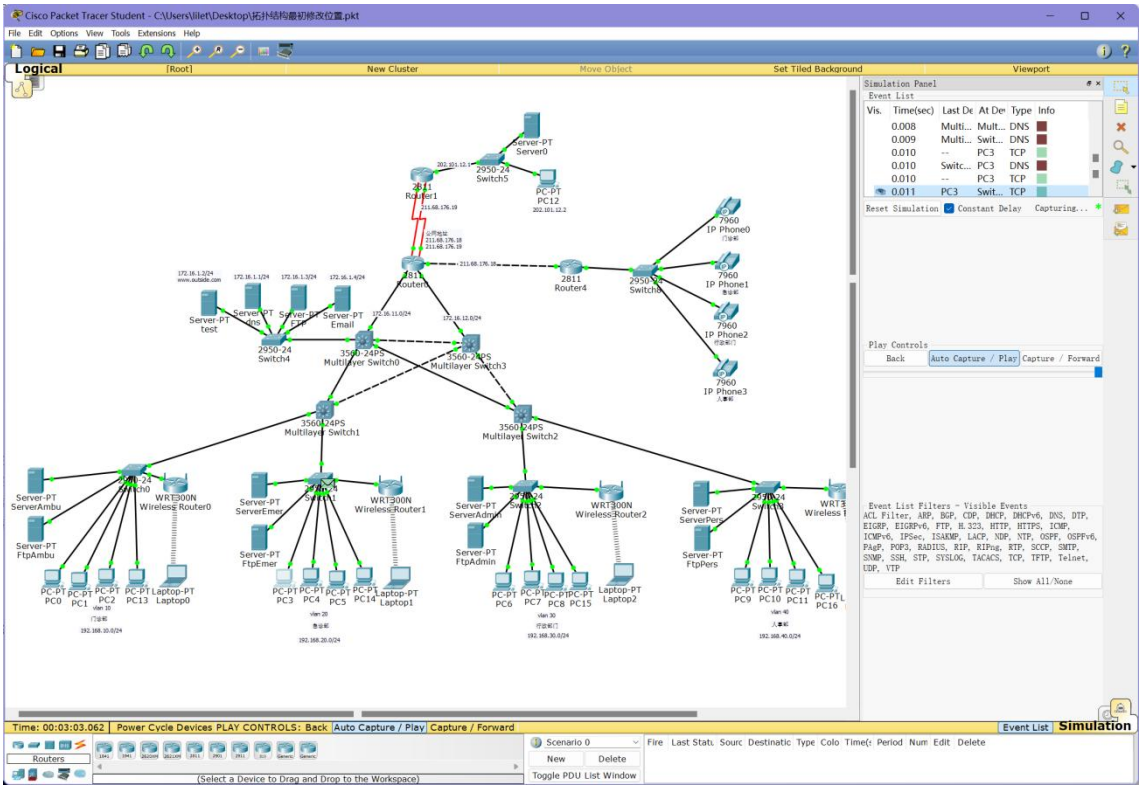


仍然以访问www.outside.com为例，我们使用 PC3 进行访问，发现此时依旧是可以访问的，这说明我们的热备份工作正常。

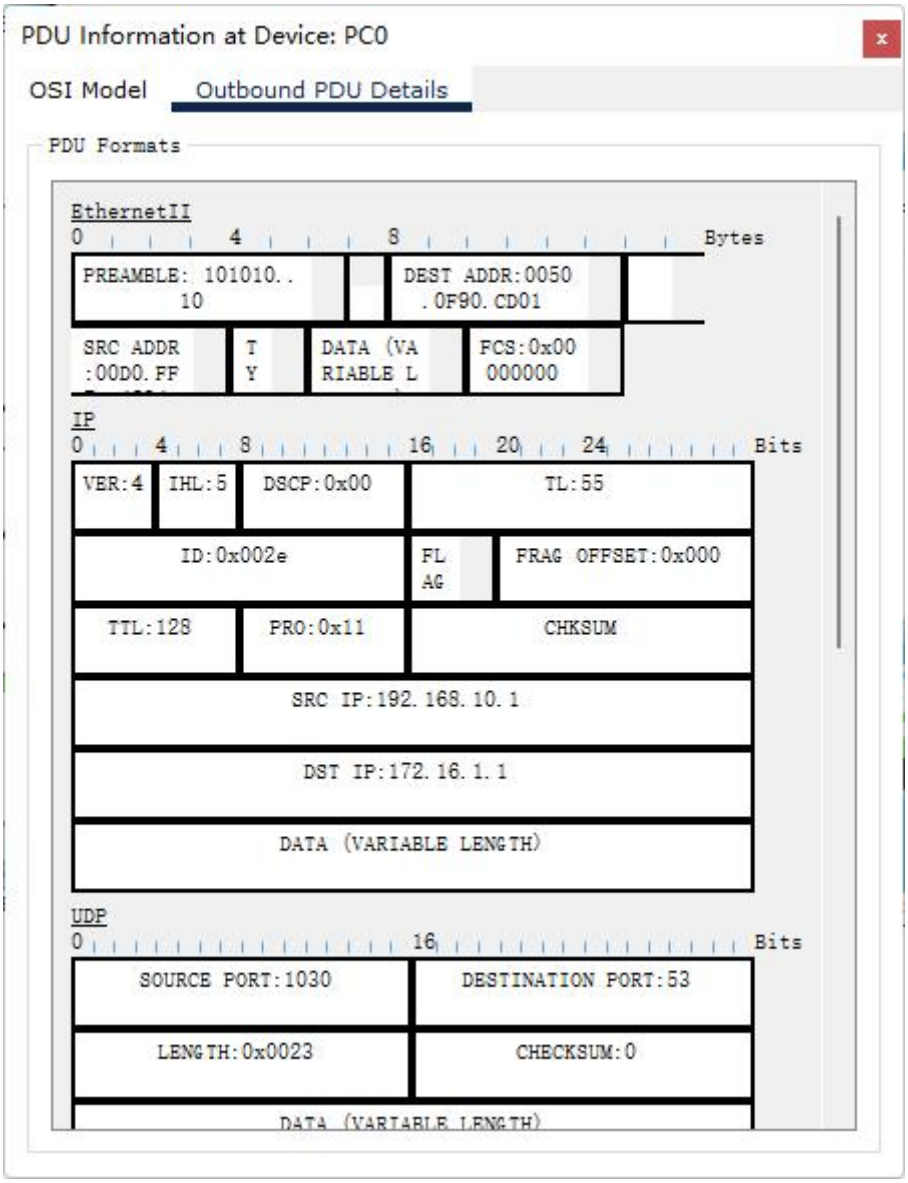


5.9 数据包分析

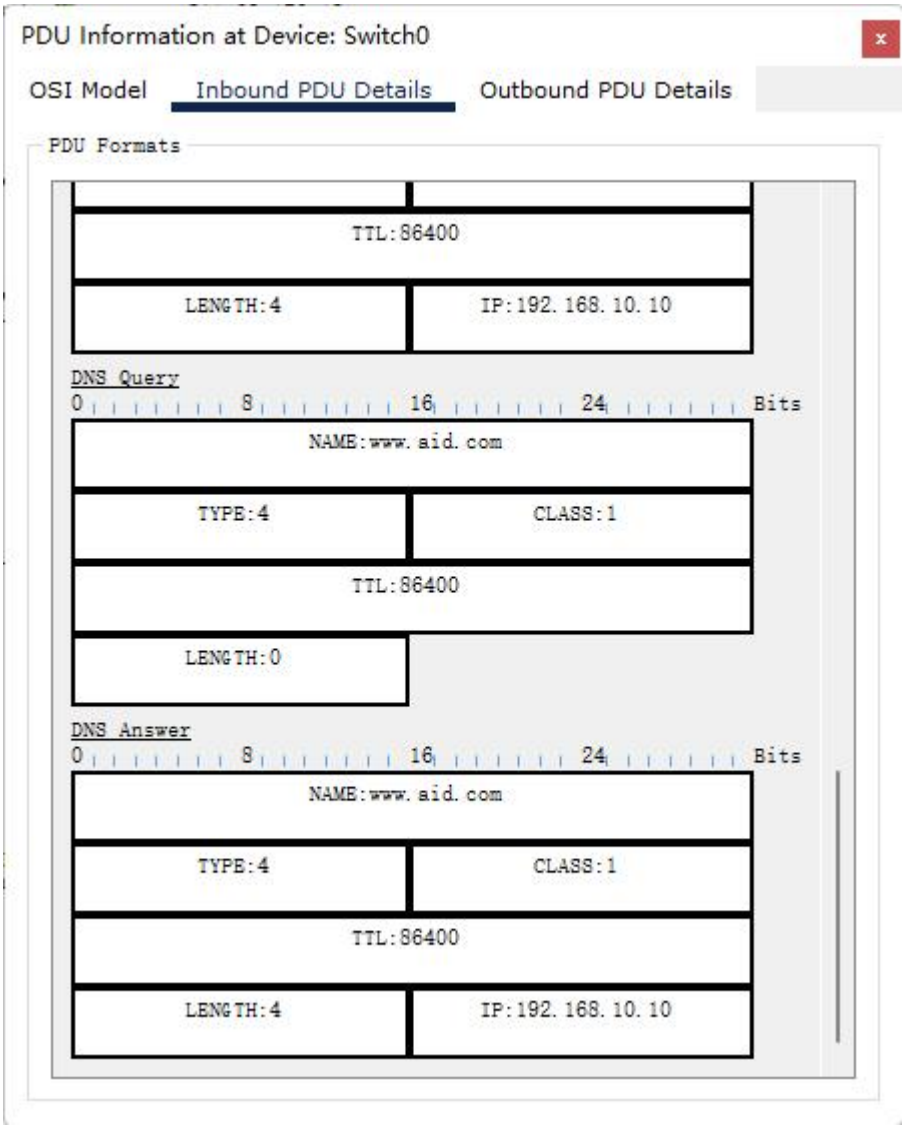
本次实验要求我们随机抓取某类型的数据包并解读，我们可以以急诊部主机访问急诊部的 Web 服务器时发出 http 请求来作为示例：



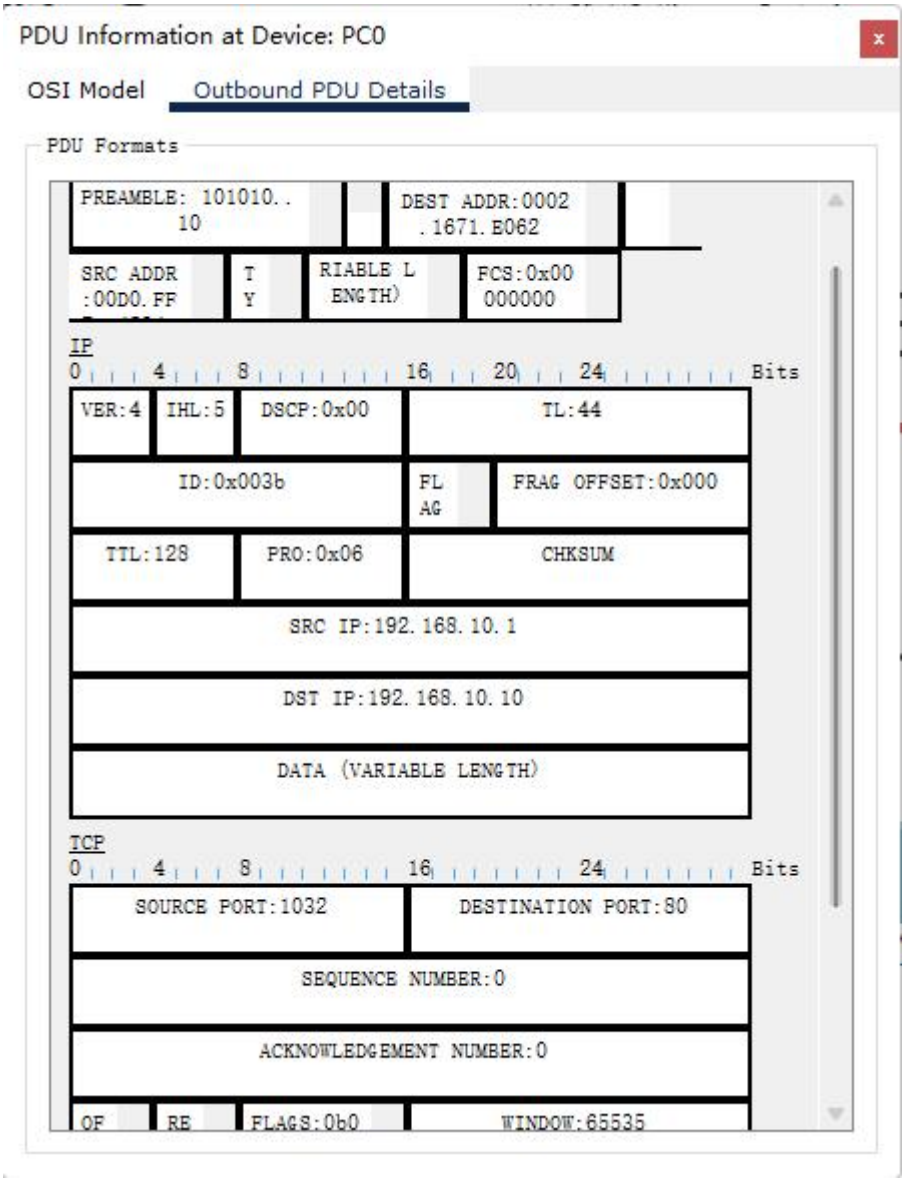
主机首先向 DNS 服务器发出请求，解析域名 www.emer.com 所对应的地址，DNS 协议在传输层是基于 UDP 的，因此可见这是一个 UDP 报文。



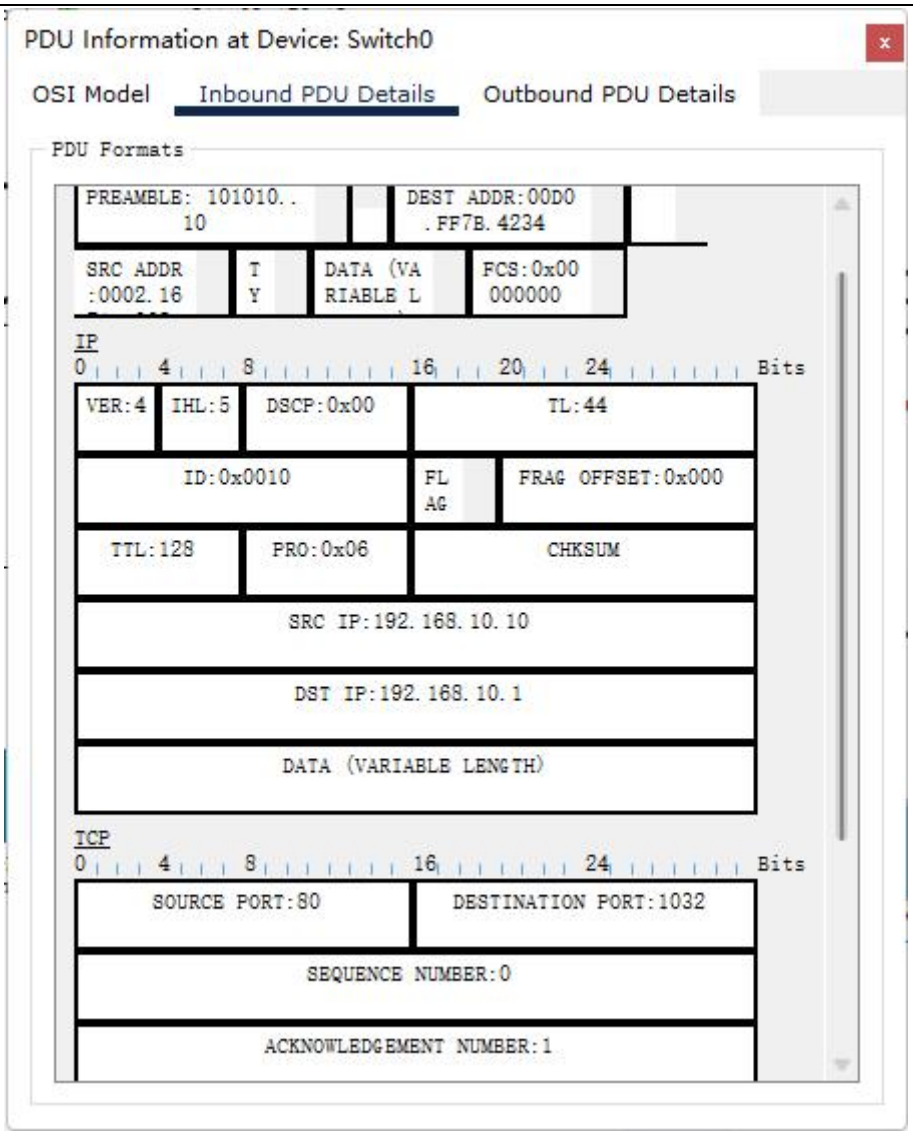
DNS 服务器服务器查询并返回该域名对应的 IP 地址，从报文中可见该地址值为 192.168.10.10。



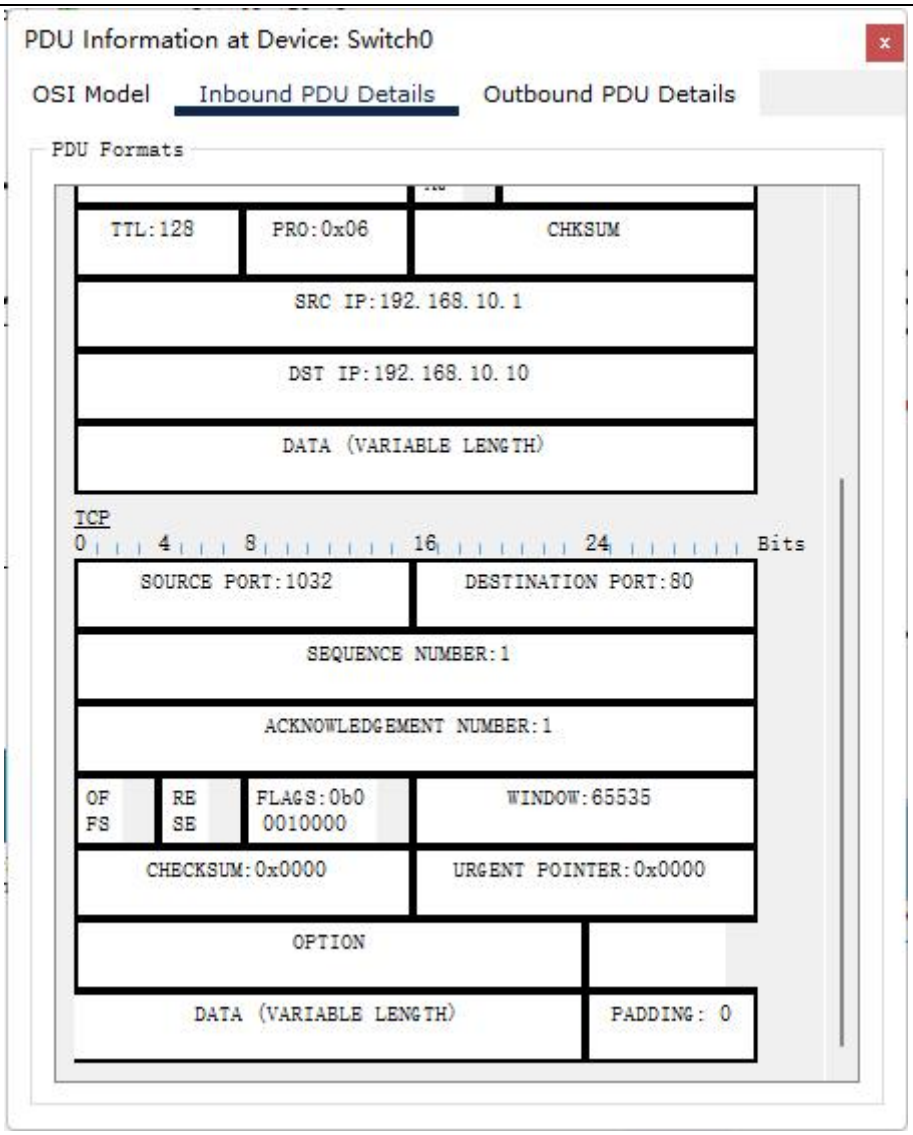
主机得知 Web 服务器的 IP 地址后，开始向其发起 TCP 连接请求，首先是第一次握手，报文如图，分析报文可知服务器 IP 地址为 192.168.10.10，MAC 地址为 0002.1671.E062。



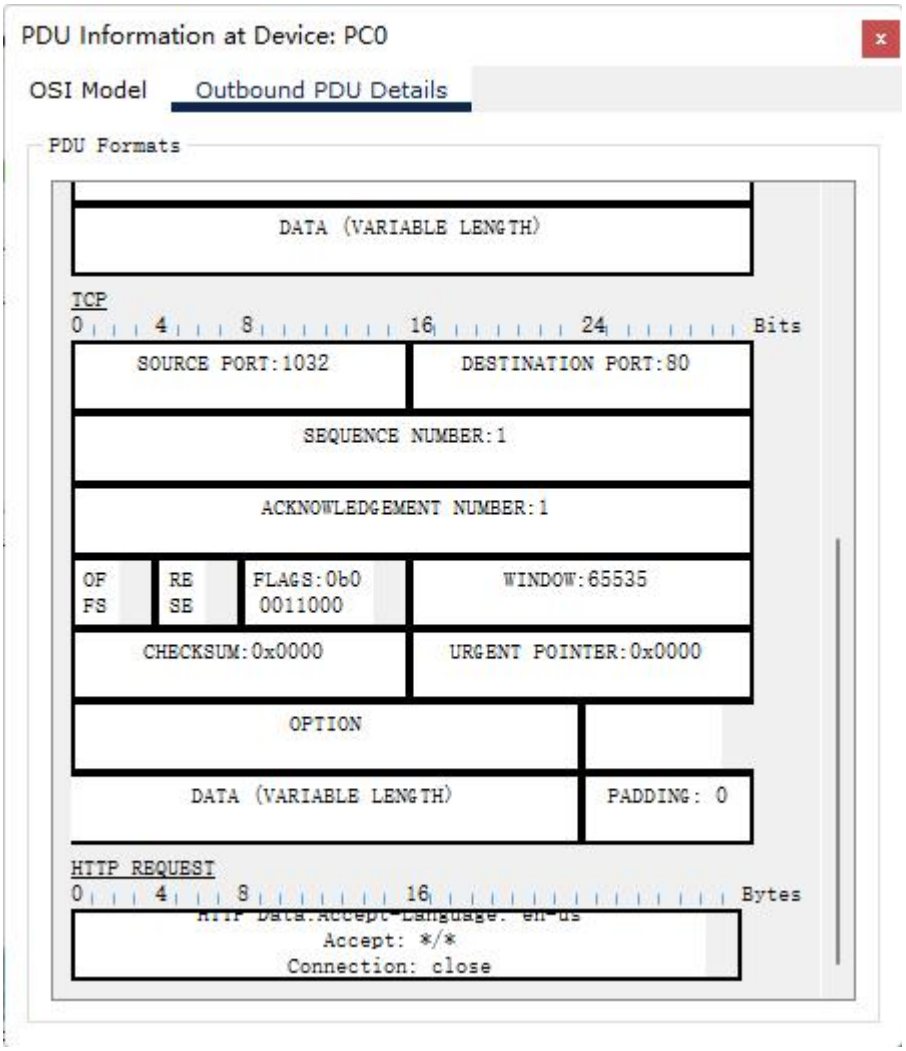
服务器接收到第一次握手的请求后，进行 TCP 第二次握手，返回 ACK 报文，如图 SN = 0，ACK = 1.



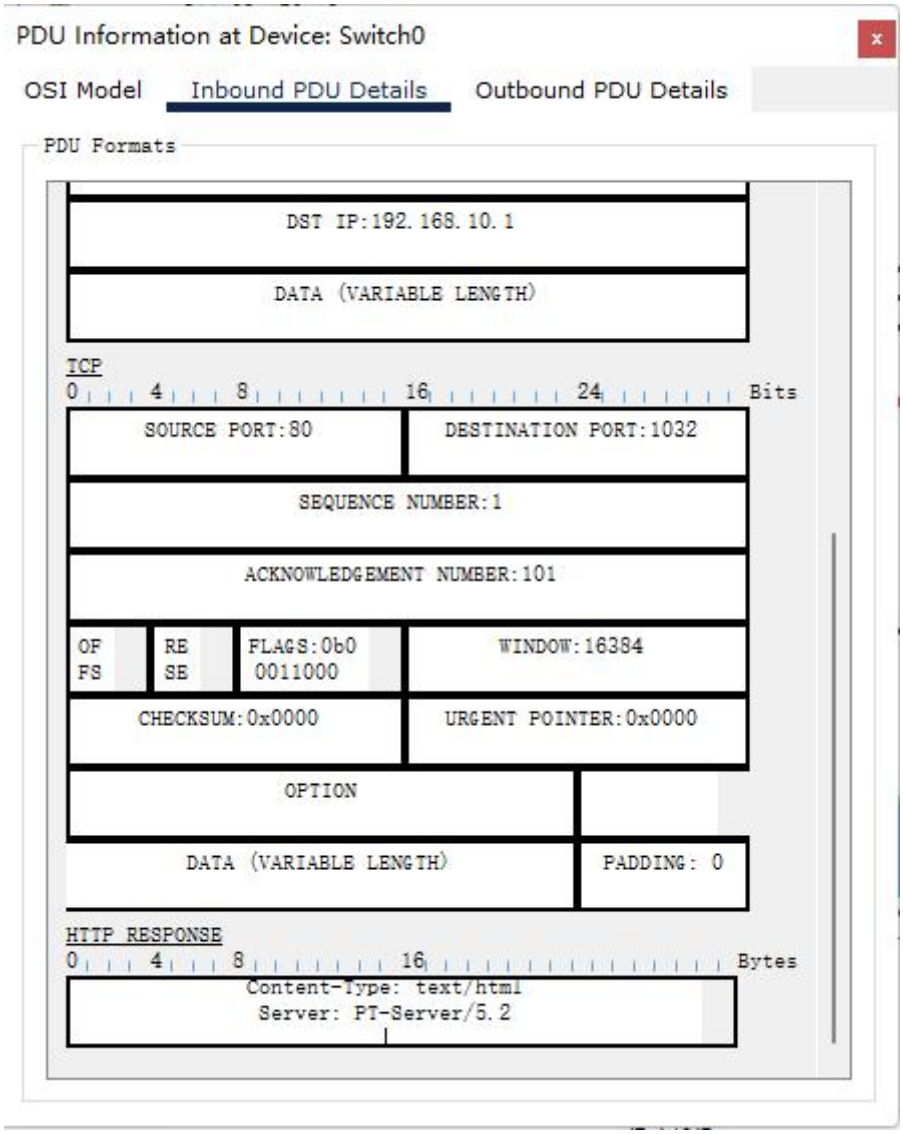
之后主机进行第三次握手，SN=0，ACK=1，之后认为 TCP 连接已经成功建立，接下来主机开始发送 http 请求。



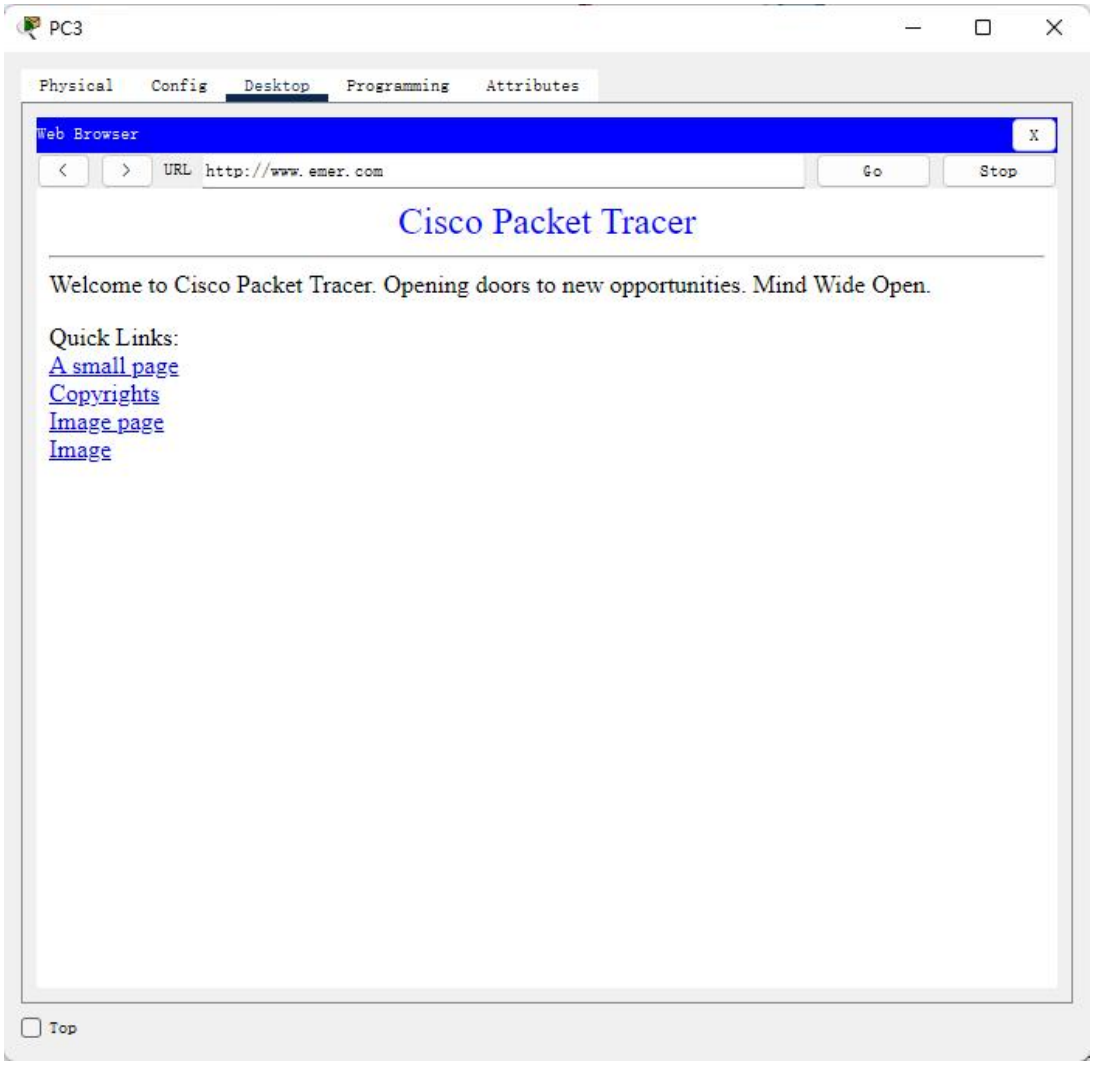
这是主机发送的 http 数据包，分析数据包的最内部一层 http 协议内容可知，这是一个访问服务器根目录的请求头，可以预见服务器将返回 index.html 的内容。



主机返回了如下的 http 数据，可见内部内容的类型为 html 的 text 数据。



主机接收到该 html 文件的数据后，浏览器渲染出了对应的网页。



6. 实验小结

这次实验是本期学习的汇总，在这个实验中，我们通过搭建医院网的过程，首先我们从需求分析开始，对整个医院的局域网进行了初步规划，不过这个规划的过程是循序渐进的，需要明确要使用到 哪些设备、通过配置哪些协议来到达我们的目的，在这个过程中我们发现了初步规划中的很多漏洞，并对其进行了二次迭代，才产生最终的需求分析建模，确认了要使用的协议。这个过程让我们受益良多，为成为一个优秀的拓扑网路设计者和需求分析者提供了一次良好的经验。

其次在我们搭建拓扑网络后，进行各种接口以及协议的配置时，我们再一次将本学期学到的全部知识，OSPF，DHCP，NAT等协议的配置原理及命令融会贯通，更加深刻的理解了其中的内涵。

在搭建过程中我们也遇到了不少的困难，如在外网想要访问医院局域网提供的web时，我们起初配置我们上课学到的RIP协议，但最终却无法成功，通过仔细的分析以及查找大量的资料后我们才明白是我们的拓扑网络不满足RIP的负载均衡条件，因此我们使用了EIGRP协议，成功解决了问题。这也使得我们对计算机网络知识的掌握不再局限于课堂，从而获得更多的知识。

在最终的成功搭建完整个网络后，我们尝试抓取不同网络请求过程中的各种数据包，这也让我们对TCP、

ARP、DNS等各种数据包以及各种报文的知识得以巩固。

7. 附录 网络拓扑规划的设计

7.1 pkt 版本

我们采用的pkt版本是6.2。

7.2 IP 分配

大部分的网络的IP地址均已标注在pkt文件中，我们对一些未标注的信息进行说明。

- 动态IP分配

Switch0下的PC IP为：192.168.10.

Switch1下的PC IP为：192.168.20.

Switch3下的PC IP为：192.168.30.

Switch4下的PC IP为：192.168.40.

- 静态IP分配

门诊部Web服务器：192.168.10.10

门诊部文件服务器：192.168.10.11

急诊部Web服务器：192.168.20.10

急诊部文件服务器：192.168.20.11

行政部Web服务器：192.168.30.10

行政部文件服务器：192.168.30.11

人事部Web服务器：192.168.40.10

人事部文件服务器：192.168.40.11

- 外部局域网IP分配

◦ PC12：202.101.12.2

◦ DNS服务器：202.101.12.3

- IP电话号码分配：

◦ 门诊部：1111

◦ 急诊部：2222

◦ 行政部：3333

◦ 人事部：4444

7.3 域名配置

- web服务器 www.outside.com

7.4 邮箱设置

账户：user*，*是一个字母，依次由a~p代替。

密码均为123

7.5 WIFI 设置

- 门诊部：

WIFI名：ambu

密码：123456789

- 急诊部：

WIFI名：emer

密码：123456789

- 行政部： WIFI名：admin

密码：123456789

- 人事部：

WIFI名：pers 密码：123456789