**中国矿业大学计算机科学与技术学院**

**2023-2024(2)《计算机网络实验》课程报告(本科)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 专业班级: | | 计算机科学与技术2022-2班 | | | | 姓名: | 杨晓琦 | | | 学号: | | 08222213 | |
|  | | | 指派的网络号： | | | 172.16.82~172.16.84 | | | | |  | | |
| **序号** | **报告题目** | **基础理论掌握程度** | | **综合知**  **识应用**  **能力** | **实验**  **内容** | **报告**  **格式** | **完成**  **状况** | **工作量** | **学习、**  **工作**  **态度** | **抄袭**  **现象** | | **其它** | **综合**  **成绩** |
|  |  |  | |  |  |  |  |  |  |  | |  |  |
|  |  |  | |  |  |  |  |  |  |  | |  |  |
|  |  |  | |  |  |  |  |  |  |  | |  |  |
|  |  |  | |  |  |  |  |  |  |  | |  |  |
|  |  |  | |  |  |  |  |  |  |  | |  |  |
|  |  |  | |  |  |  |  |  |  |  | |  |  |
|  |  |  | |  |  |  |  |  |  |  | |  |  |
|  |  |  | |  |  |  |  |  |  |  | |  |  |
| 任课教师： | | 杨东平 | | |  |  |  | |  | | |  |  |
| 批阅时间： | |  | | | |  |  | |  | | | | |

**目录**

[8 应用层 1](#_Toc170575460)

[8.1 实验1：常用应用服务器配置 1](#_Toc170575461)

[8.1.1 实验1.1：DHCP服务器配置实例 1](#_Toc170575462)

[8.1.2 实验1.2：FTP服务器配置实例 8](#_Toc170575463)

[8.1.3 实验1.3：DNS服务器配置实例 10](#_Toc170575464)

[8.1.4 实验1.4：TFTP服务器配置实例 10](#_Toc170575465)

[8.1.5 实验1.5：E-Mail服务器配置实例 12](#_Toc170575466)

[8.1.6 实验1.6：Email与VLAN的结合 17](#_Toc170575467)

[8.1.7 实验1.7：HTTP服务器配置实例 20](#_Toc170575468)

[8.2 实验2：常用应用层协议分析 22](#_Toc170575469)

[8.2.1 实验2.1：DNS协议分析 22](#_Toc170575470)

[8.2.2 实验2.2：HTTP协议分析 28](#_Toc170575471)

[8.2.3 实验2.3：电子邮件协议分析 31](#_Toc170575472)

[8.2.4 实验2.4：QQ协议分析 34](#_Toc170575473)

[8.2.5 实验2.5：微信协议分析 35](#_Toc170575474)

[8.2.6 实验2.6：迅雷协议分析 37](#_Toc170575475)

[8.3 实验体会 39](#_Toc170575476)

# 8 应用层

**实验内容：**

1. 使用仿真软件PT完成常用网络应用服务（FTP、Telnet、Mail、DHCP、Web）的访问场景设计、拓扑构建、网络配置和应用测试
2. 使用抓包工具Wireshark获取和分析DNS、HTTP、QQ、微信、邮件服务等协议的工作过程

**实验报告要求(必须认真阅读)：**

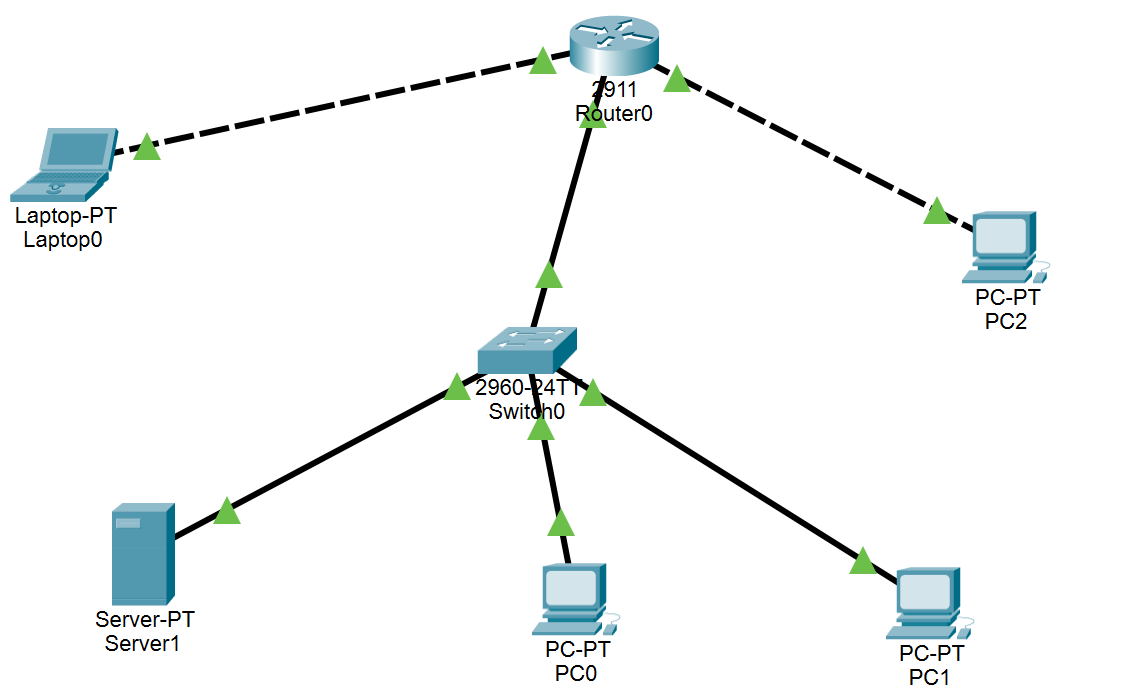
1. 不得使用实验指导书中的图片(截图)及图片(截图)的相关说明，否则所涉及实验内容视作无效， 并按0分计入成绩；
2. 实验中所使用的IP地址必须按照统一分配给个人的IP地址完成，否则所涉及实验内容视作无效，并按0分计入成绩；
3. 实验内容需要使用的网站、数据文件或其它软件必须作明确的说明，并配有相应的截图(或运行截图或文件目录截图)，否则所涉及实验内容视作抄袭，并按0分计入成绩；
4. 使用仿真软件的实验内容必须同时提交仿真软件所形成的工程文件，否则所涉及的实验内容视作未完成，并按0分计入成绩；
5. 编程的实验内容必须在报告中指出编程环境及其版本号，并同时提交编程环境所形成的工作空间文件或工程文件，以及源代码文件，否则所涉及的实验内容视作未完成，并按0分计入成绩；
6. 实验步骤及实验步骤所涉及的参数必须明确，否则酌情扣除一定的分数；
7. 必须在规定的时间内完成每一次的实验任务，并提交相关文件，否则该次实验内容按0分计入成绩。

说明：如果撰写规范不符合《计算机学院考查类课程报告撰写规范》要求的，整体上酌情扣除1-10分。

## 8.1 实验1：常用应用服务器配置

### 8.1.1 实验1.1：DHCP服务器配置实例

第一步：构建DHCP网络拓扑，如图1-1-1所示。

图1-1-1 DNS服务器配置拓扑图

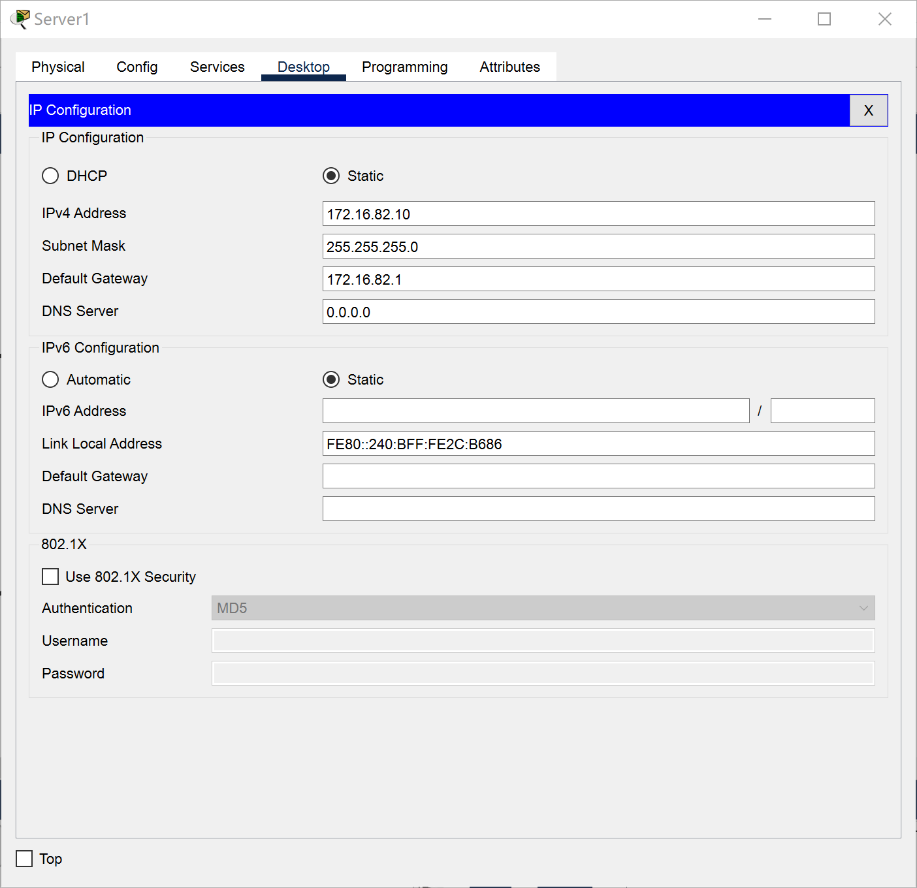
第二步：配置DHCP Server，如图1-1-2所示。

图1-1-2 DHCP Server基本网络参数

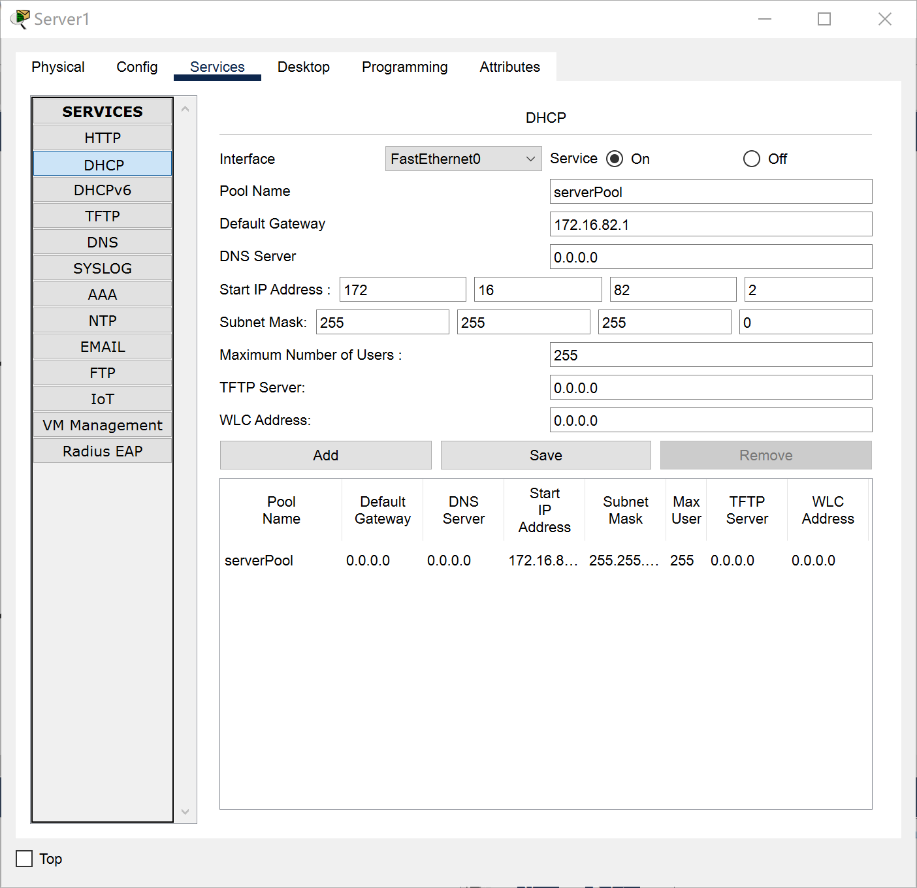
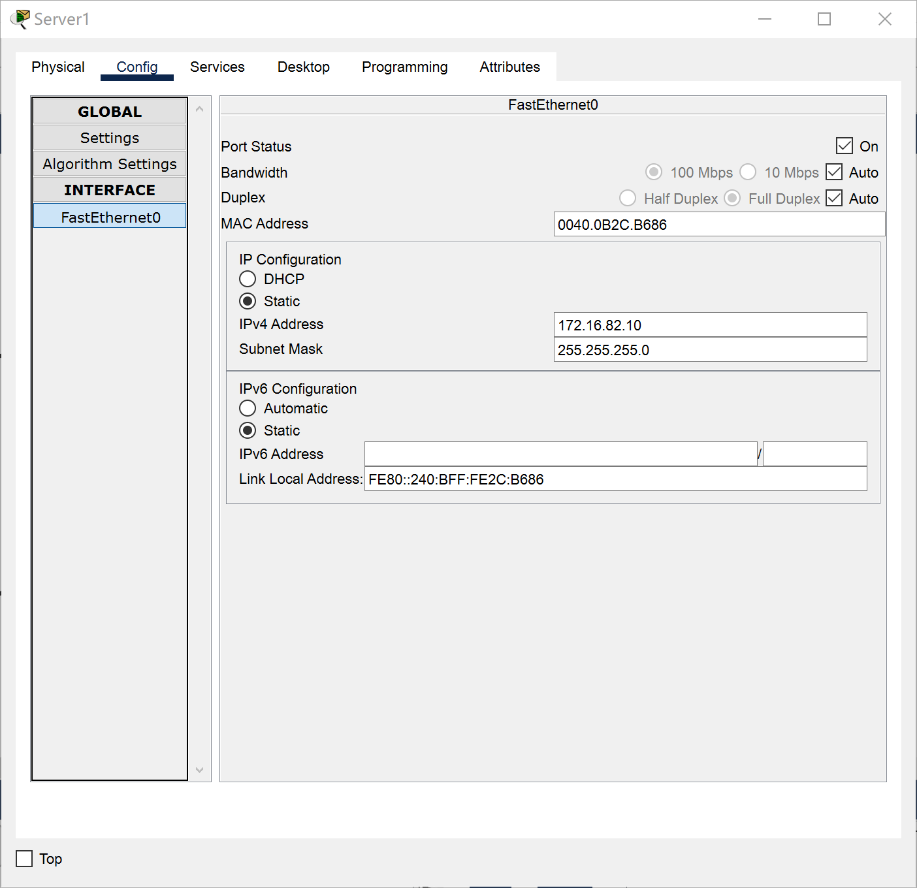
图1-1-3 DNS服务器的接口配置

图1-1-4 DNS服务器的地址池

第三步：配置主机(以PC0为例)，具体过程如下图所示。

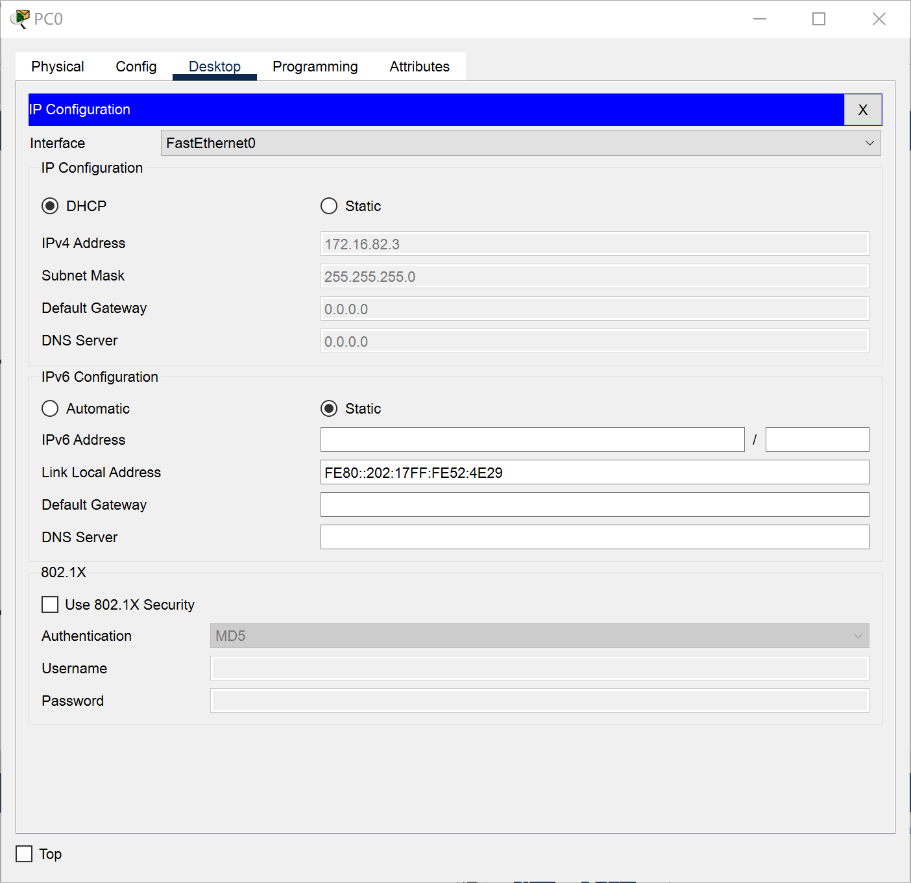
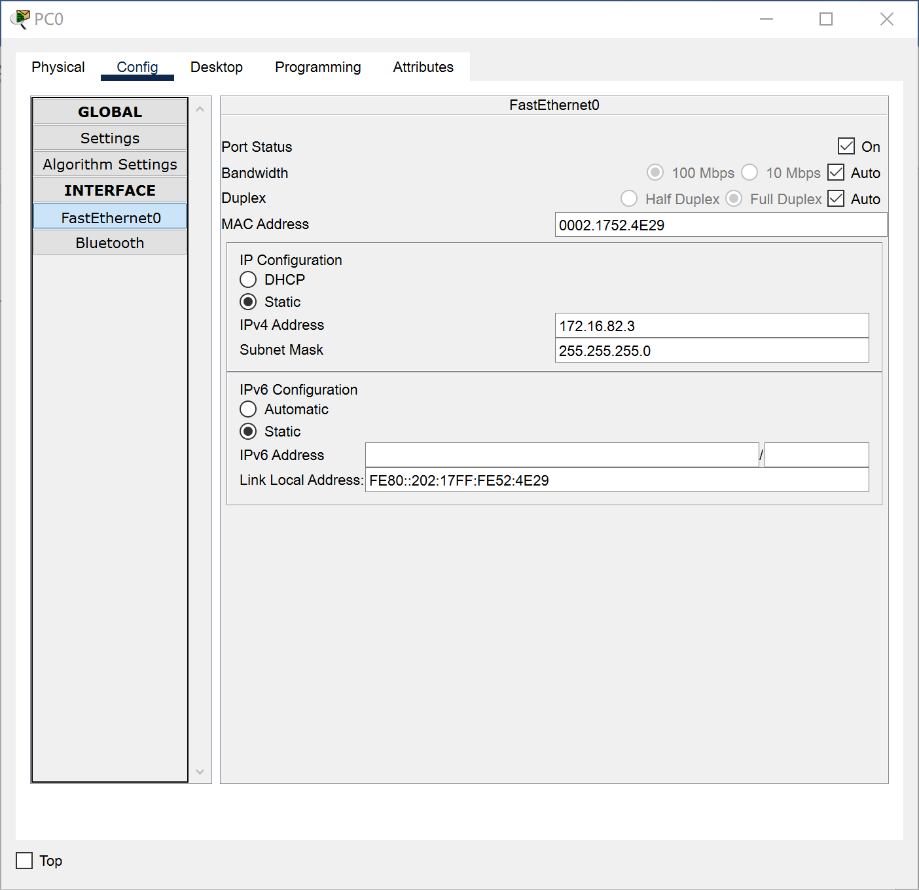
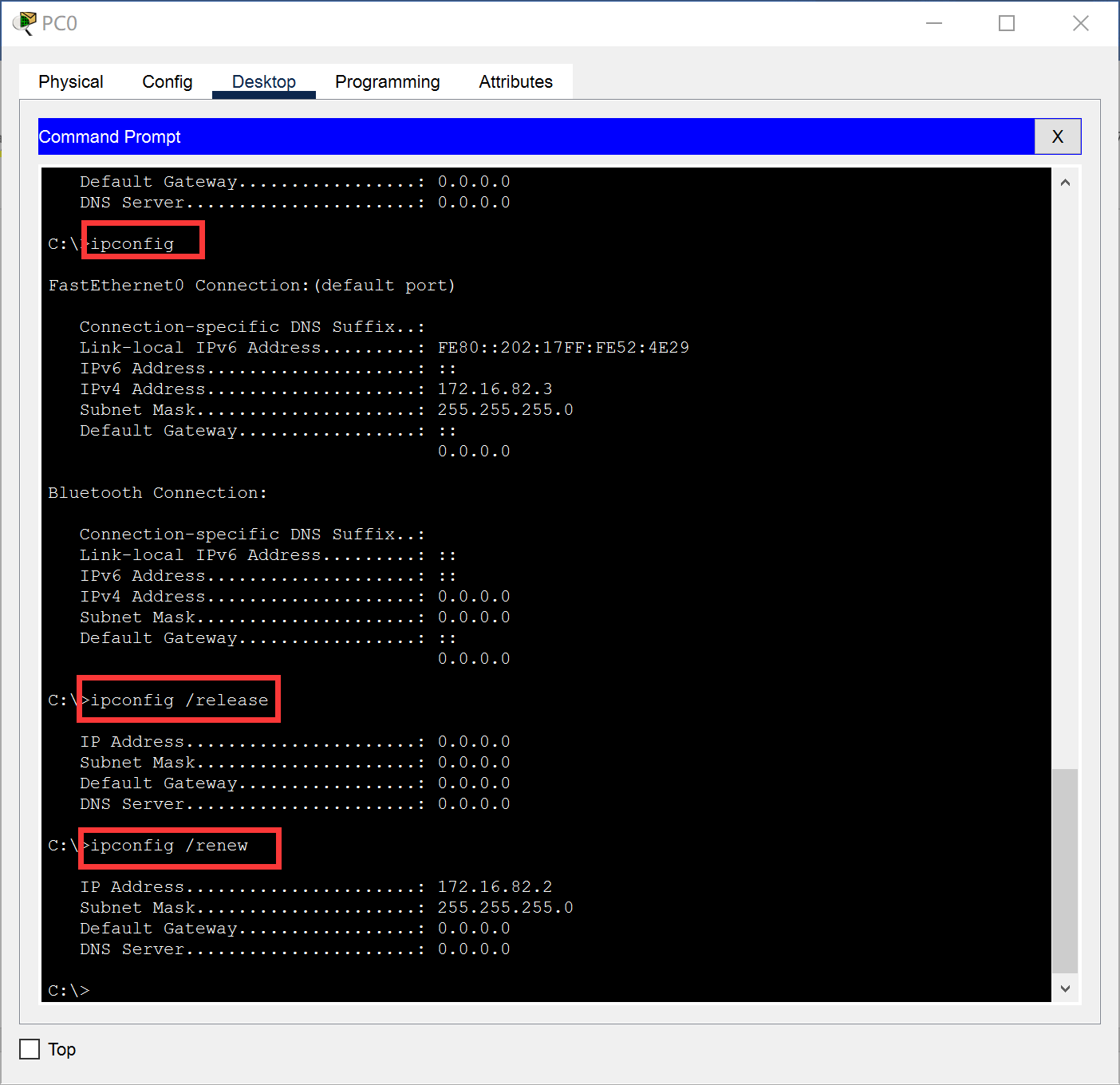
 图1-1-5 配置PC0

图1-1-6 PC0的配置信息

图1-1-7 刷新PC0的网络配置

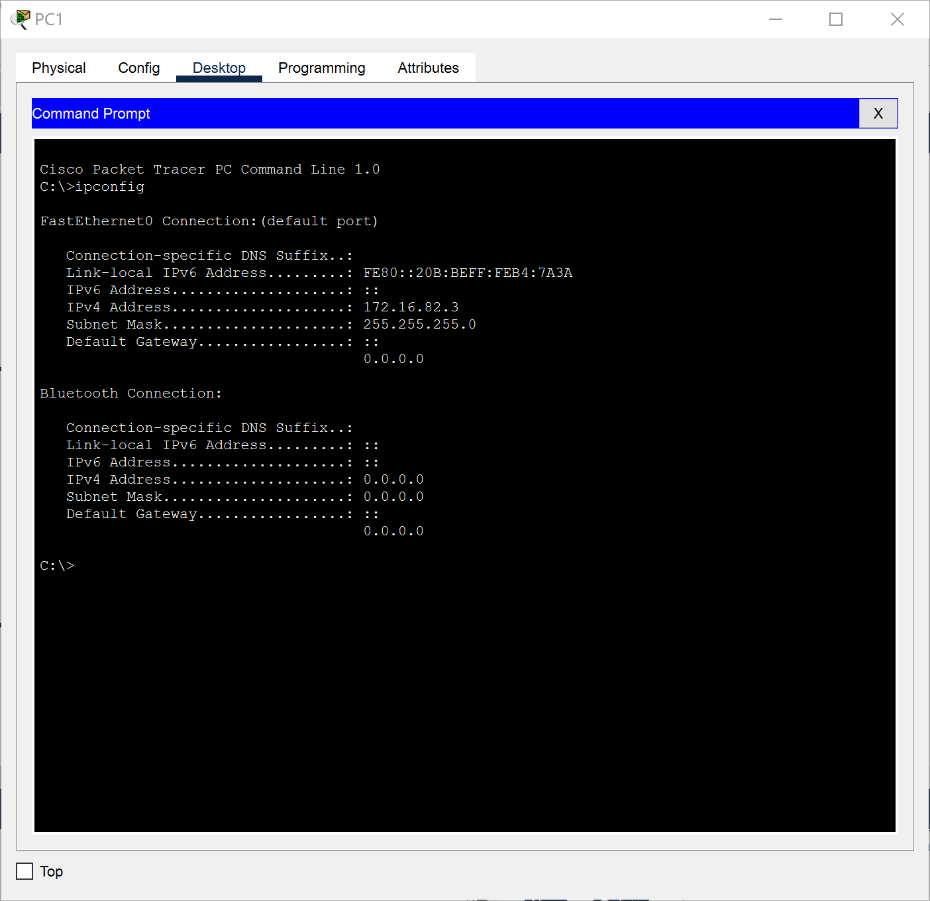
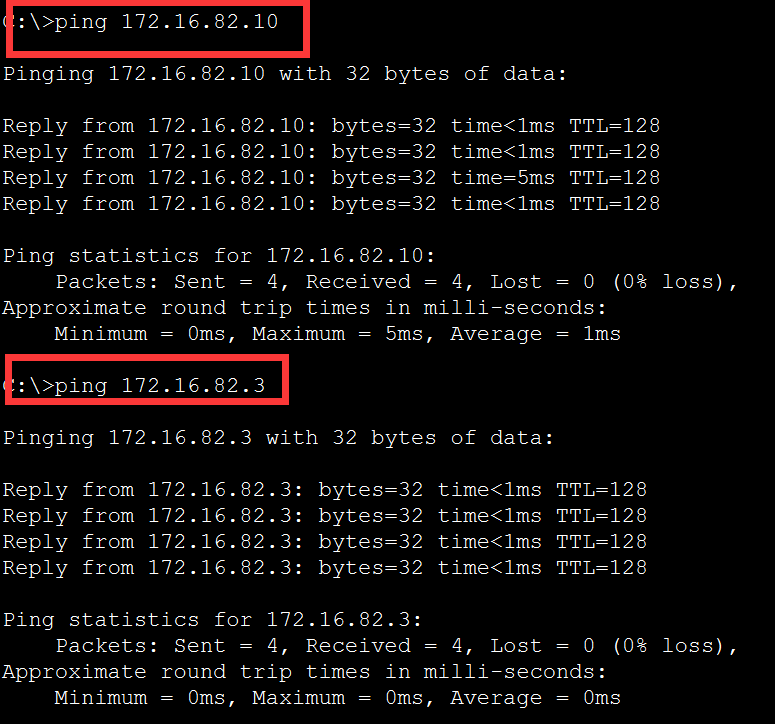
第四步 测试连通性(以PC0和PC1为例)，具体过程如下图所示。

图1-1-8 PC1的网络配置

图1-1-9 PC0 与 DHCP Server、PC1的连通性

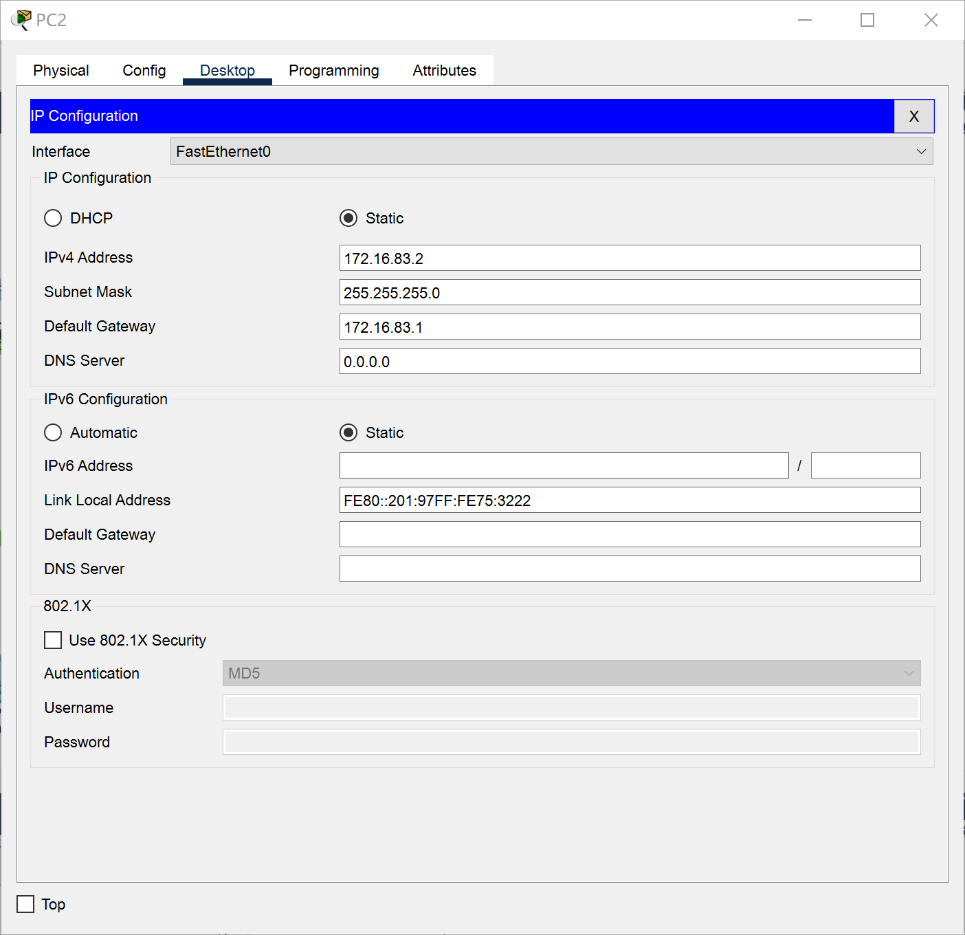
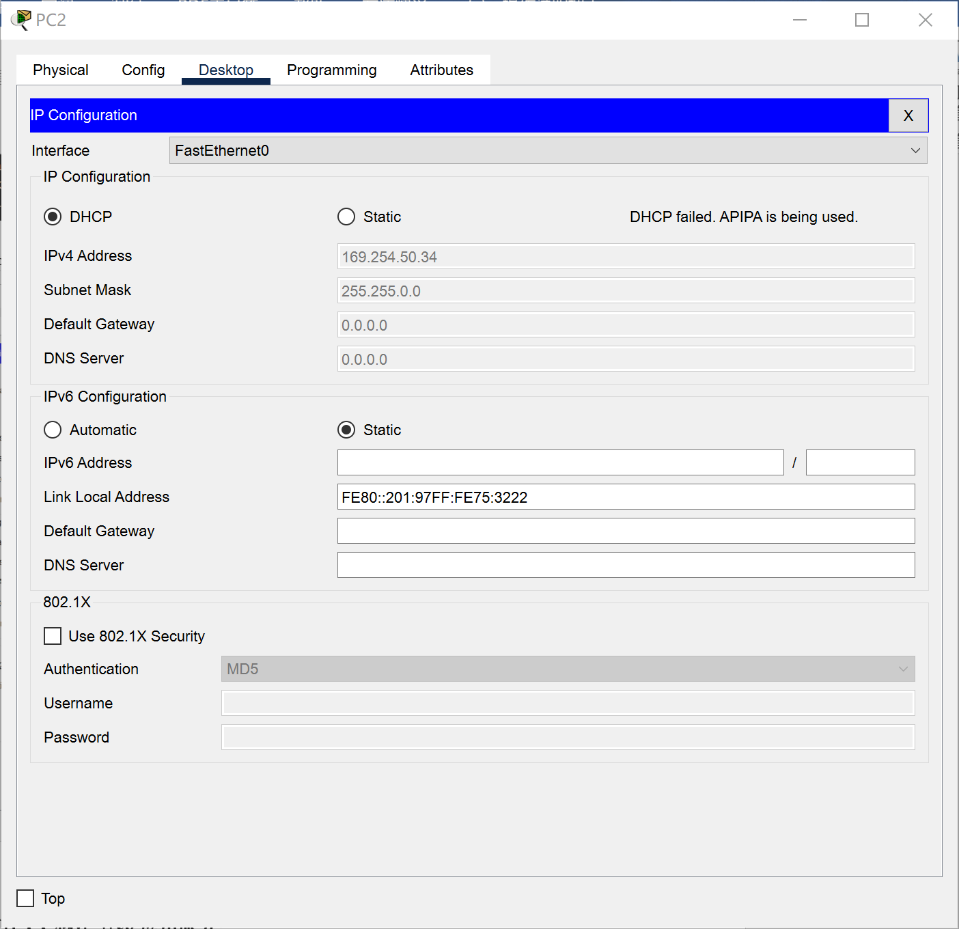
第五步：APIPA机制(以PC2为例)，如下图所示。

图1-1-10 PC2基本配置信息

图1-1-11 修改PC2为DHCP

自动私有IP编址(APIPA)是一个DHCP故障转移机制。当主机失去DHCP服务器的连接时，APIPA在169.254.0.1到169.254.255.254的私有地址空间内分配地址。所有设备使用默认的地址掩码255.255.0.0。APIPA可以为没有DHCP服务器的单网段自动配置TCP/IP协议。此时PC2自动配置IP地址为169.254.50.34。

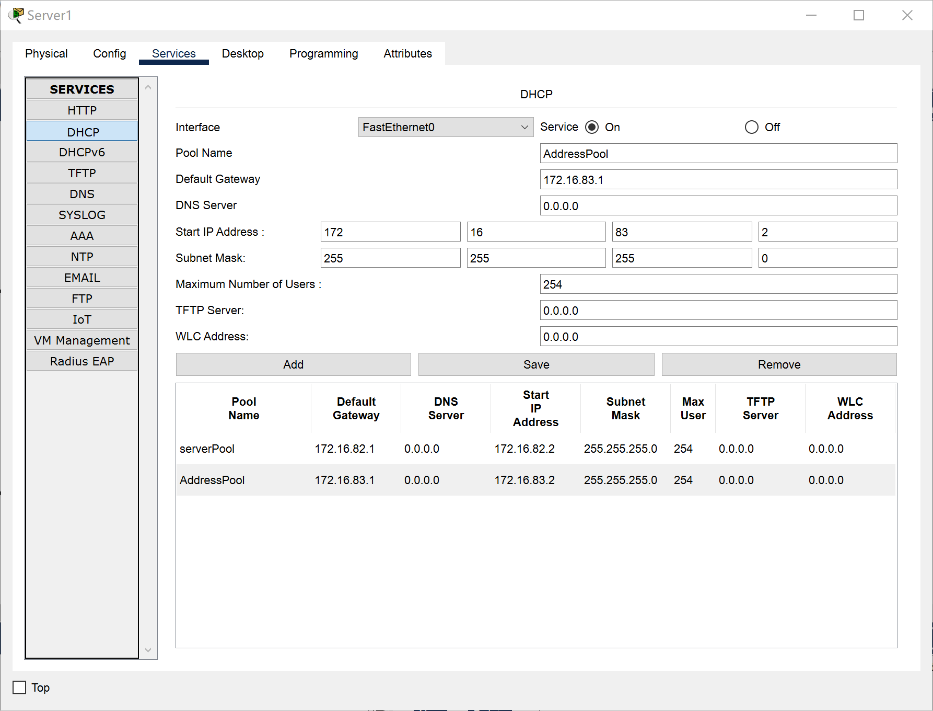
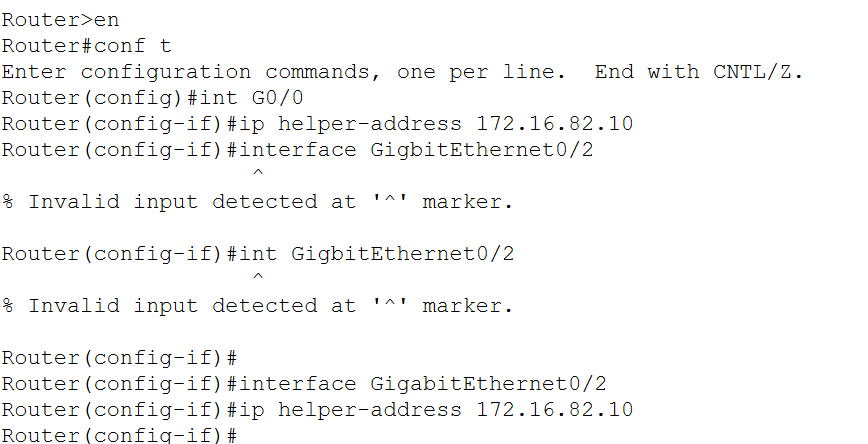
第六步：跨网段分配IP地址。如图1-4-12所示。

图1-1-12 增加DHCP地址池

(1) 对路由器R0完成一下配置命令：

图1-1-13 R0配置命令

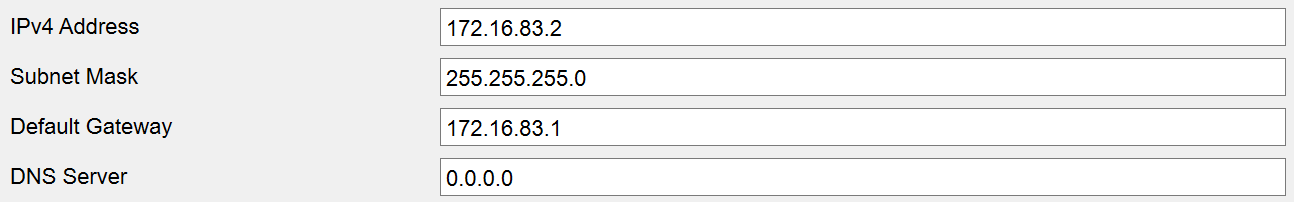
(2) 将PC2的IP地址改为DHCP动态IP地址，可以自动获取到IP地址

图1-1-14 配置路由器以支持跨网段分配IP地址

### 8.1.2 实验1.2：FTP服务器配置实例

第一步：构建FTP网络拓扑，如图1-2-1所示。

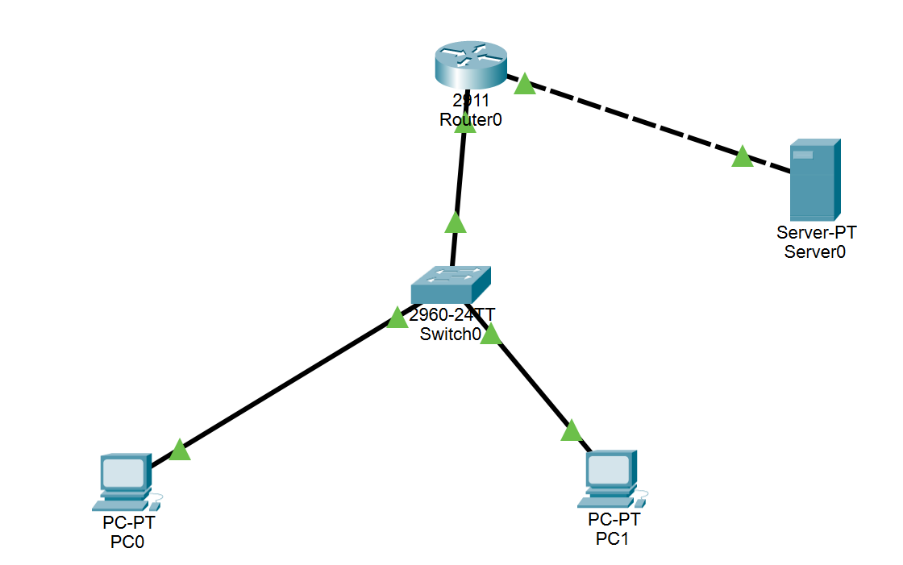
图1-2-1 FTP服务器配置拓扑图

表1-2-1 各设备参数配置

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | IP | Submark | GW | DNS |
| Router 0 | G0/1 | 172.16.84.1 | 255.255.255.0 |  |  |
| G0/0 | 172.16.82.1 | 255.255.255.0 |  |  |
| PC0 | | 172.16.82.2 | 255.255.255.0 | 172.16.82.1 | 172.16.84.10 |
| PC1 | | 172.16.82.3 | 255.255.255.0 | 172.16.82.1 | 172.16.84.10 |
| FTP Server | | 172.16.84.10 | 255.255.255.0 | 172.16.84.1 |  |

第二步：配置FTP服务器

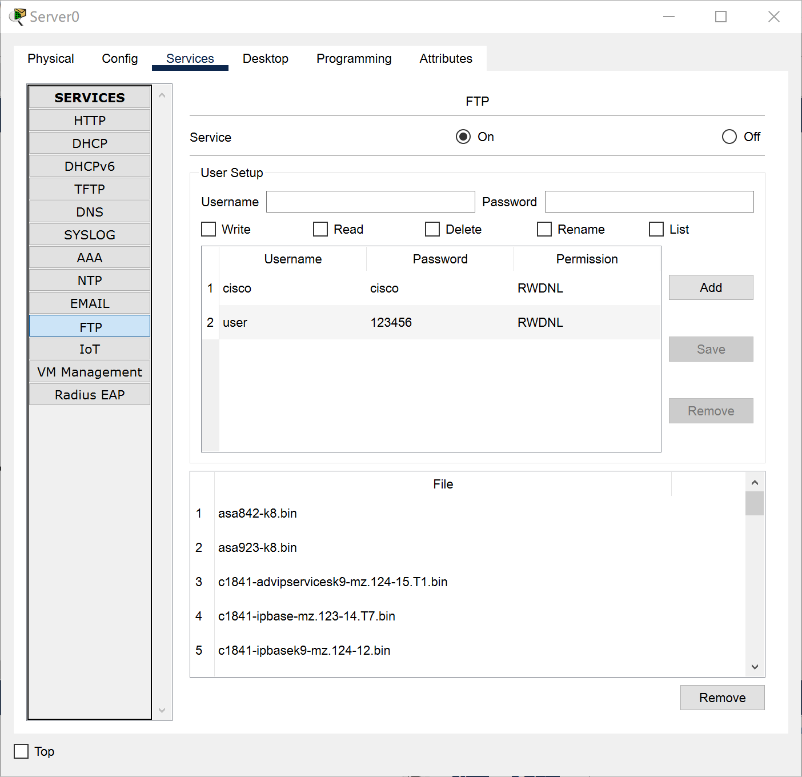
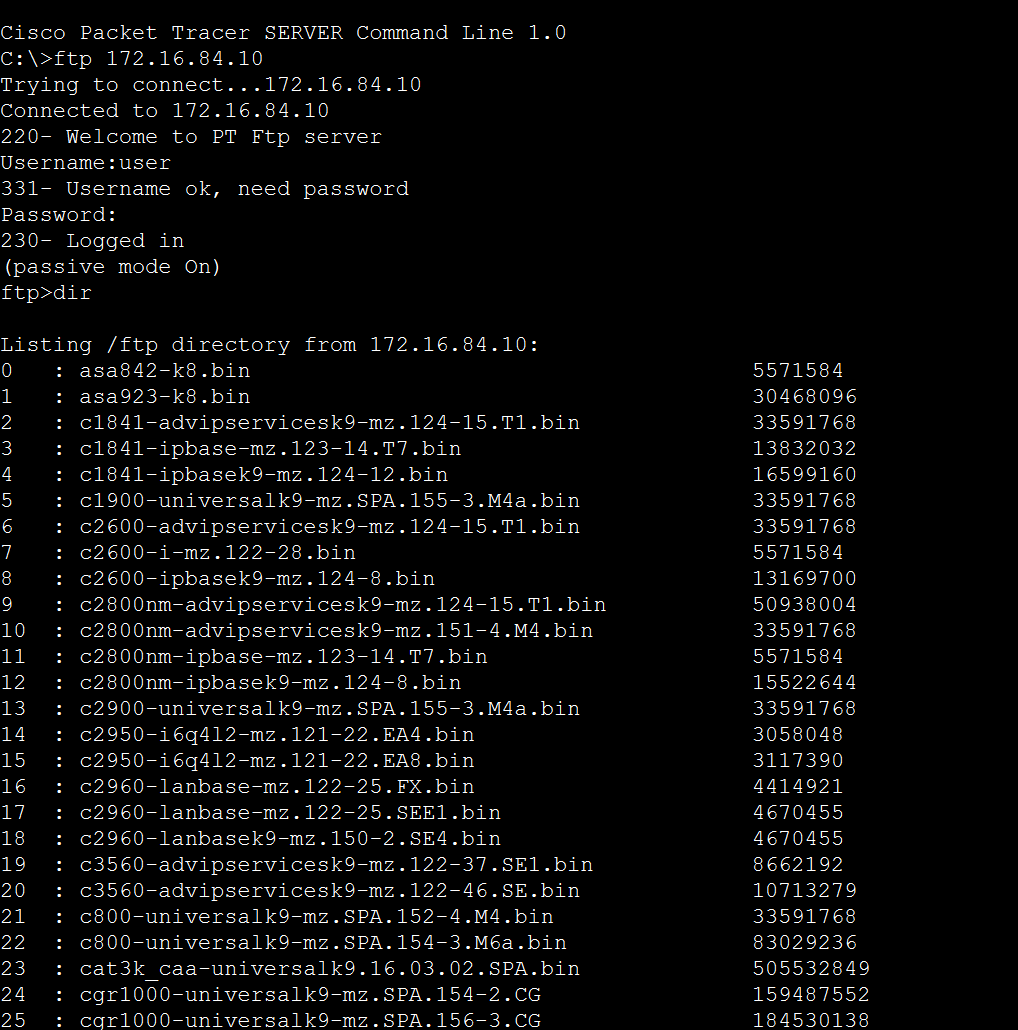
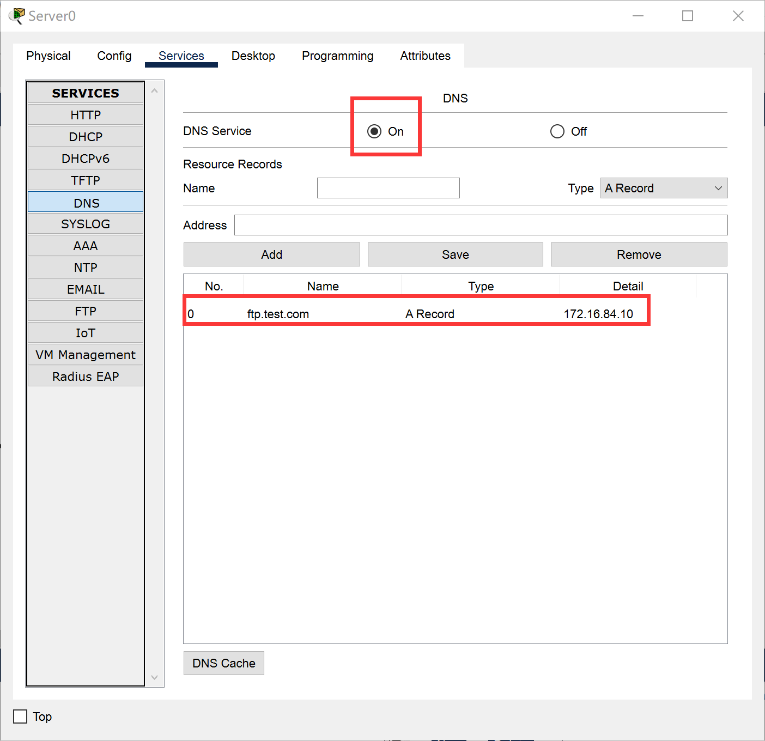
(1)开启FTP服务，添加用户权限

图1-2-2 配置FTP服务器

(2)使用ftp命令访问FTP sever

图1-2-3 访问FTP服务器

### 8.1.3 实验1.3：DNS服务器配置实例

在FTP开启DNS解析服务，将ftp.test解析为172.16.84.10。

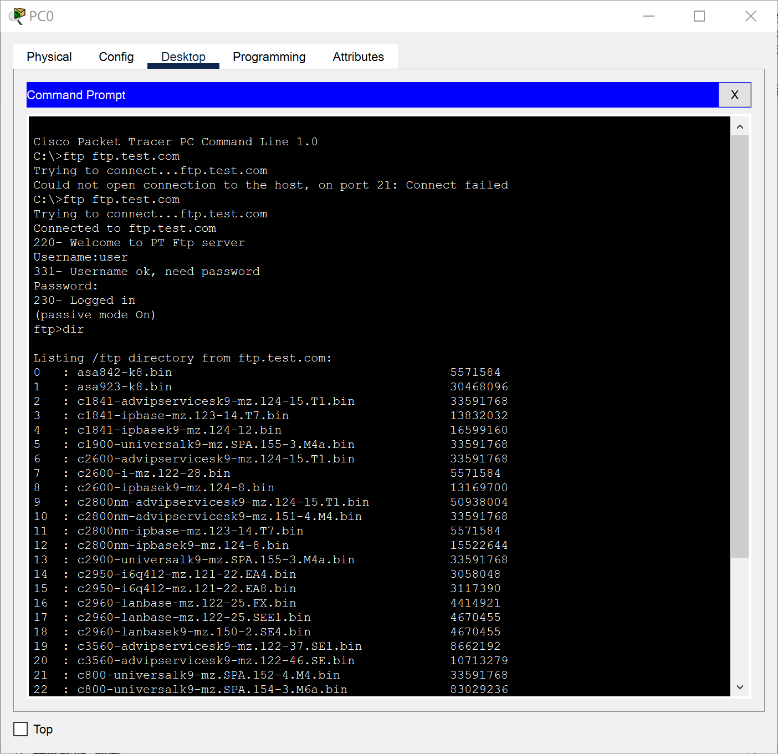
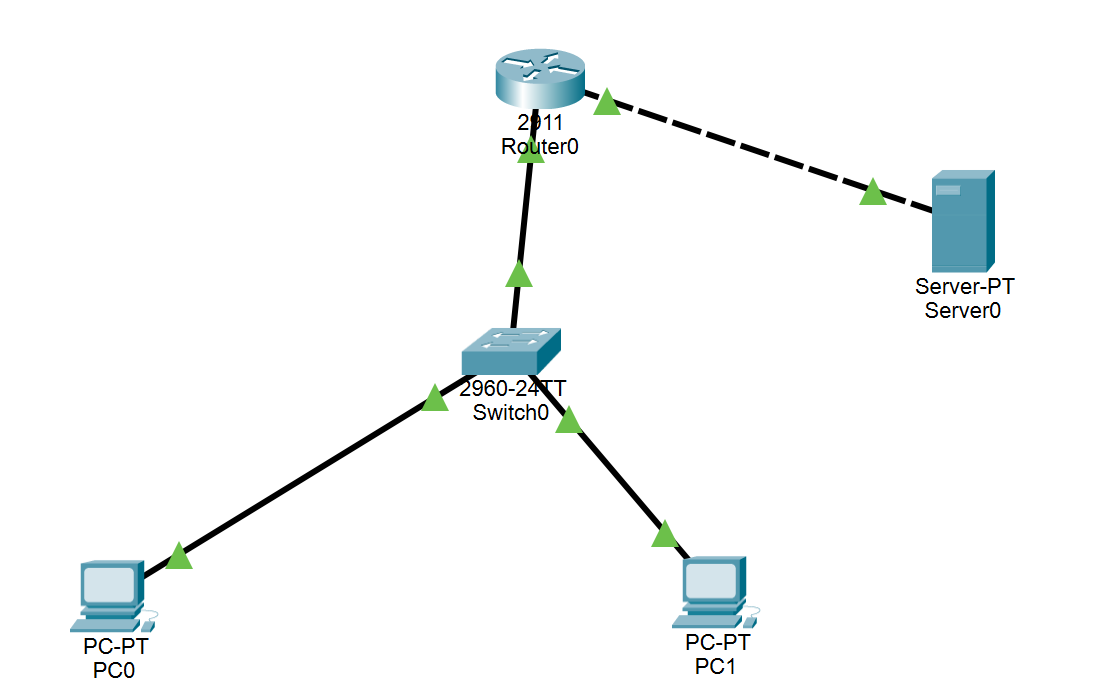
图1-3-1 开通FTP服务器的DNS服务

图1-3-2 域名访问FTP服务器

### 8.1.4 实验1.4：TFTP服务器配置实例

(1)配置TFTP服务器，如图1-4-1所示。

图1-4-1 TFTP服务器配置拓扑图

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | IP | Submark | GW | DNS |
| Router 0 | G0/1 | 172.16.84.1 | 255.255.255.0 |  |  |
| G0/0 | 172.16.82.1 | 255.255.255.0 |  |  |
| PC0 | | 172.16.82.2 | 255.255.255.0 | 172.16.82.1 | 172.16.84.10 |
| PC1 | | 172.16.82.3 | 255.255.255.0 | 172.16.82.1 | 172.16.84.10 |
| FTP Server | | 172.16.84.10 | 255.255.255.0 | 172.16.84.1 |  |

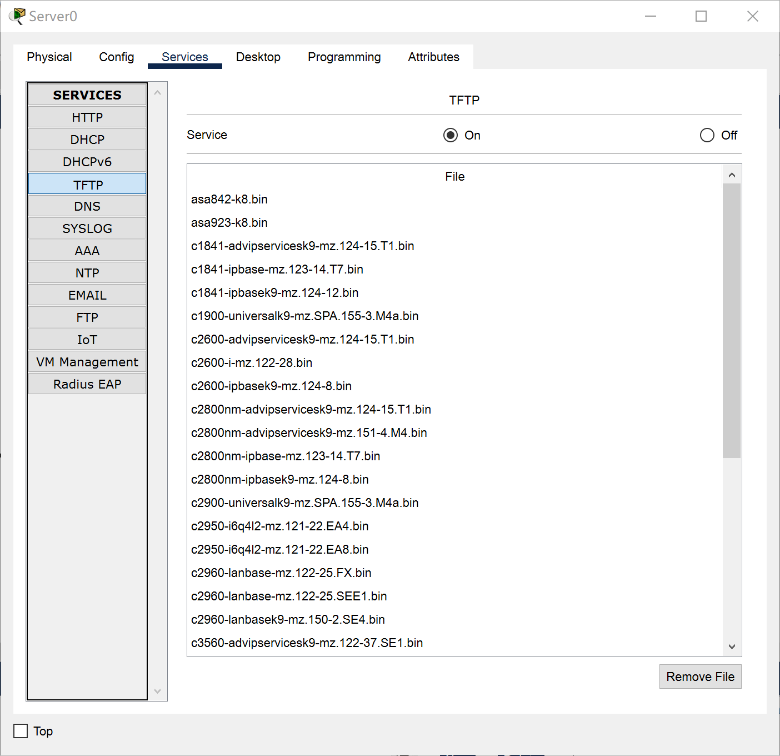
表1-4-1 各设备参数配置

图1-4-2 配置TFTP服务器

(2)利用TFTP升级网络设备

配置命令如下图所示：

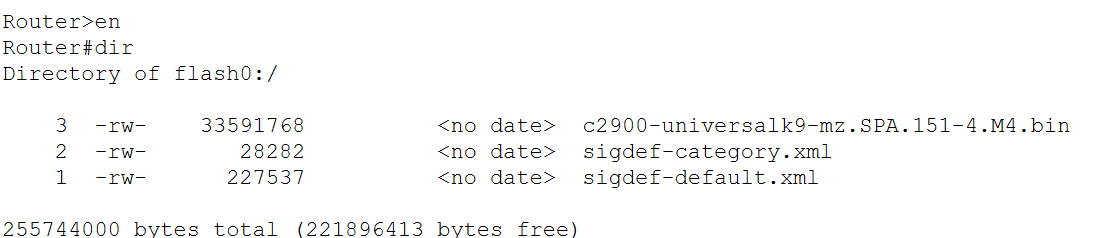
图1-4-3 查看已有路由器的配置文件

图1-4-4 成功下载TFTP文件

### 8.1.5 实验1.5：E-Mail服务器配置实例

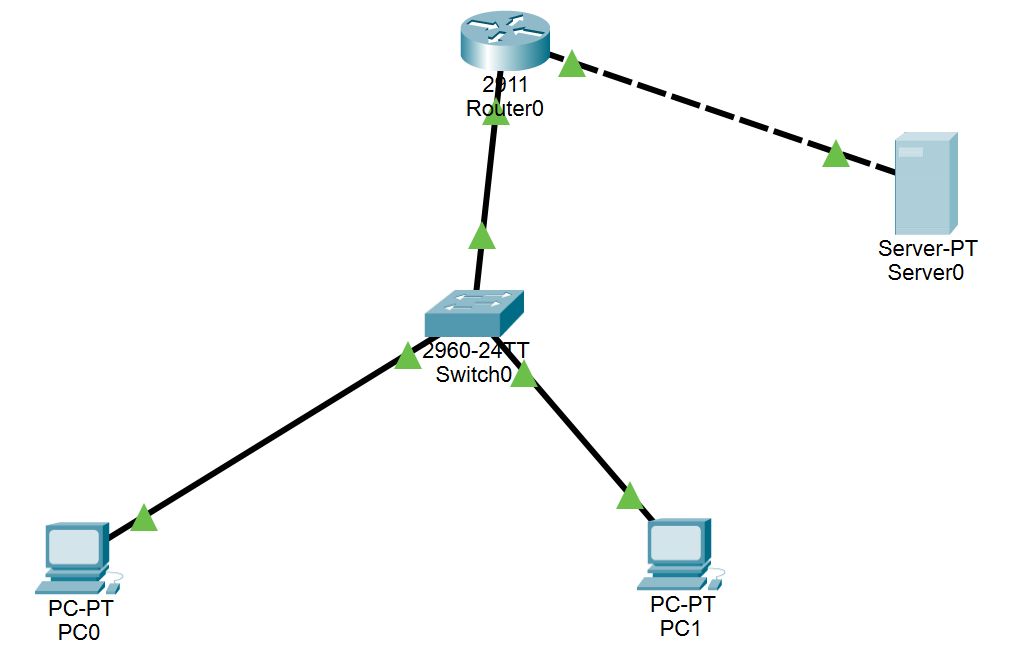
第一步：构建E-Mail网络拓扑，如图1-5-1所示。

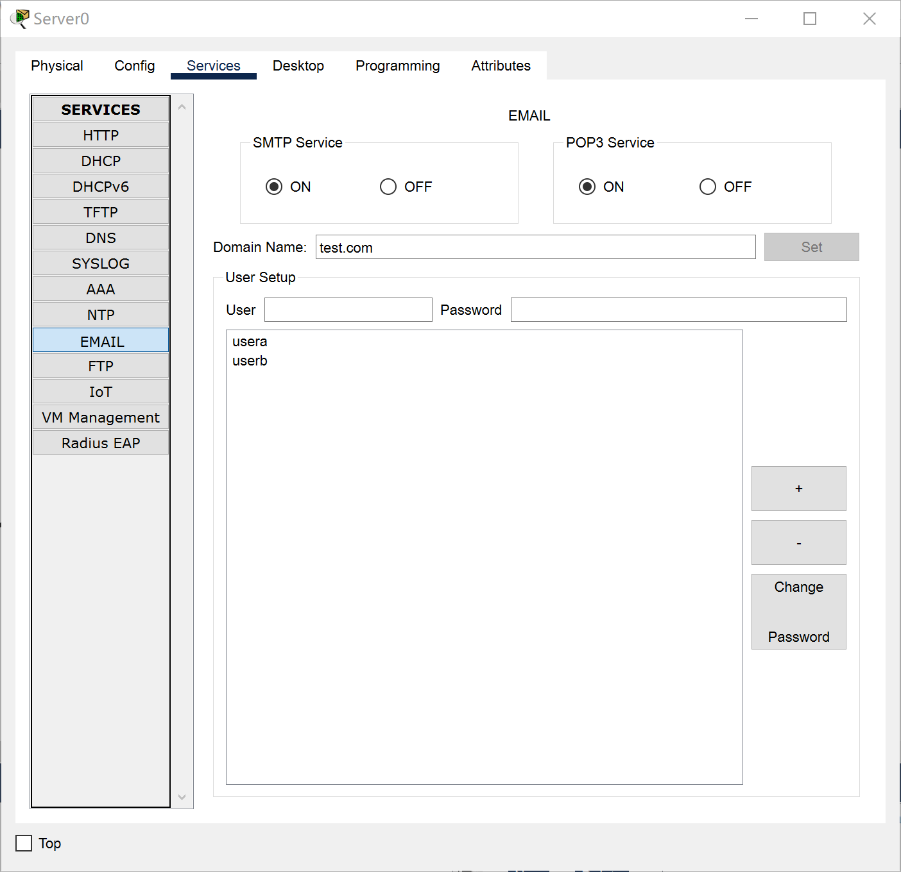
图1-5-1 Email服务器配置拓扑图

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | IP | Submark | GW | DNS |
| Router 0 | G0/1 | 172.16.84.1 | 255.255.255.0 |  |  |
| G0/0 | 172.16.82.1 | 255.255.255.0 |  |  |
| PC0 | | 172.16.82.2 | 255.255.255.0 | 172.16.82.1 | 172.16.84.10 |
| PC1 | | 172.16.82.3 | 255.255.255.0 | 172.16.82.1 | 172.16.84.10 |
| FTP Server | | 172.16.84.10 | 255.255.255.0 | 172.16.84.1 |  |

表1-5-1 各设备参数配置

第二步：配置邮件服务器，如下图所示。

开启邮件服务器，添加两个邮件账户：usera@test.com，userb@test.com。

图1-5-2开启邮件服务器

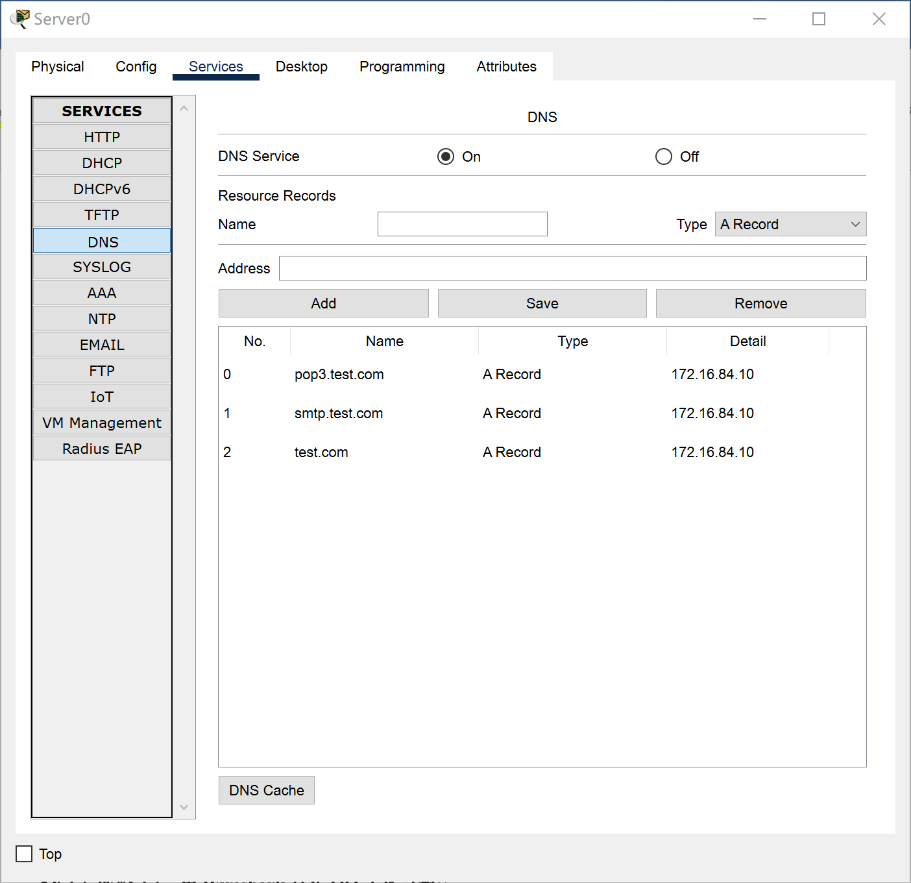
第三步：配置邮件服务器的域名访问功能

图1-5-3 开启邮件服务器的域名访问功能

第四步：配置邮件访问客户端(以PC0为例)，如下图所示。

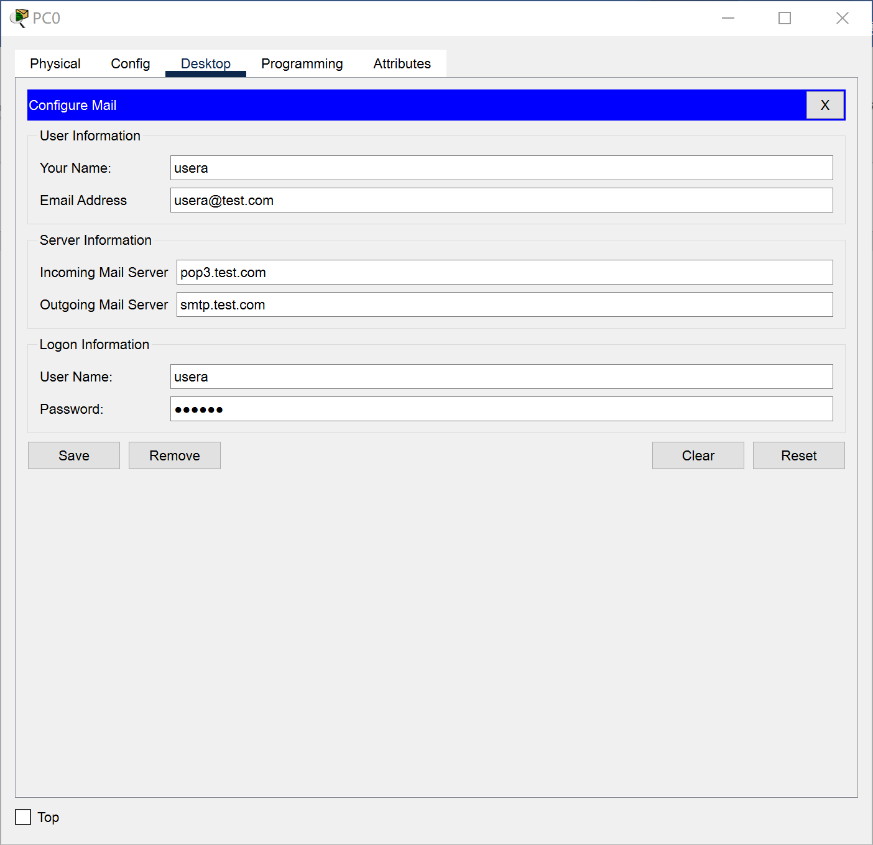
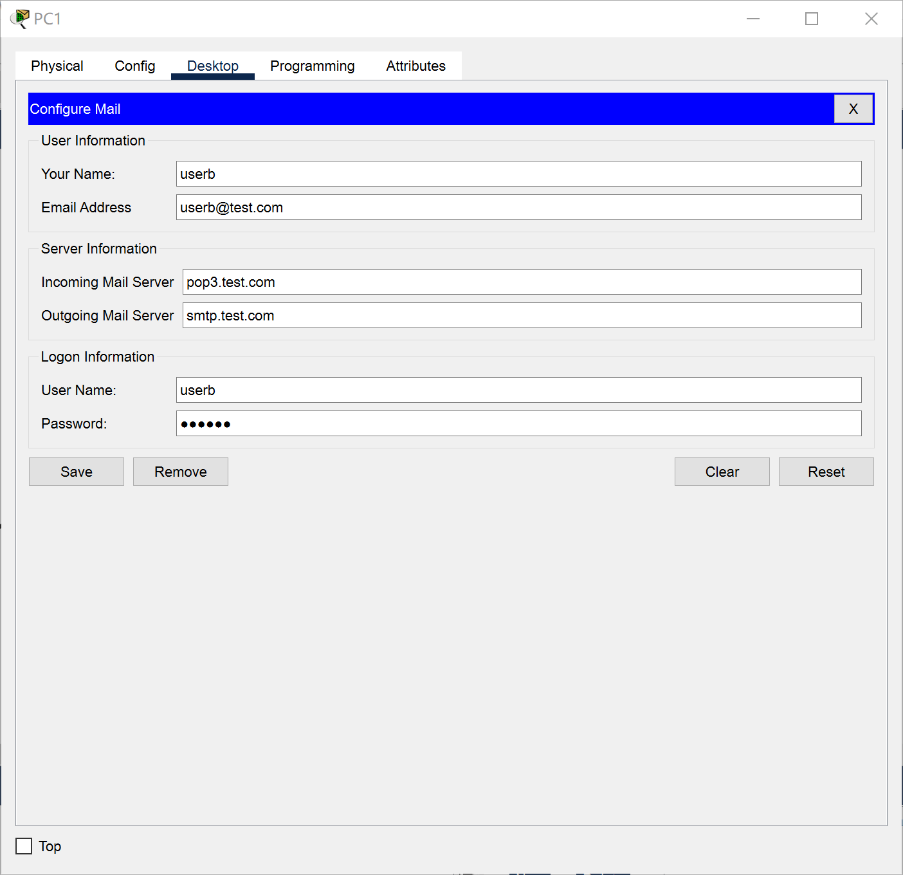
图1-5-4 配置PC0的邮件访问代理

图1-5-5 配置PC1的邮件访问代理

图1-5-6 主机的邮件代理管理

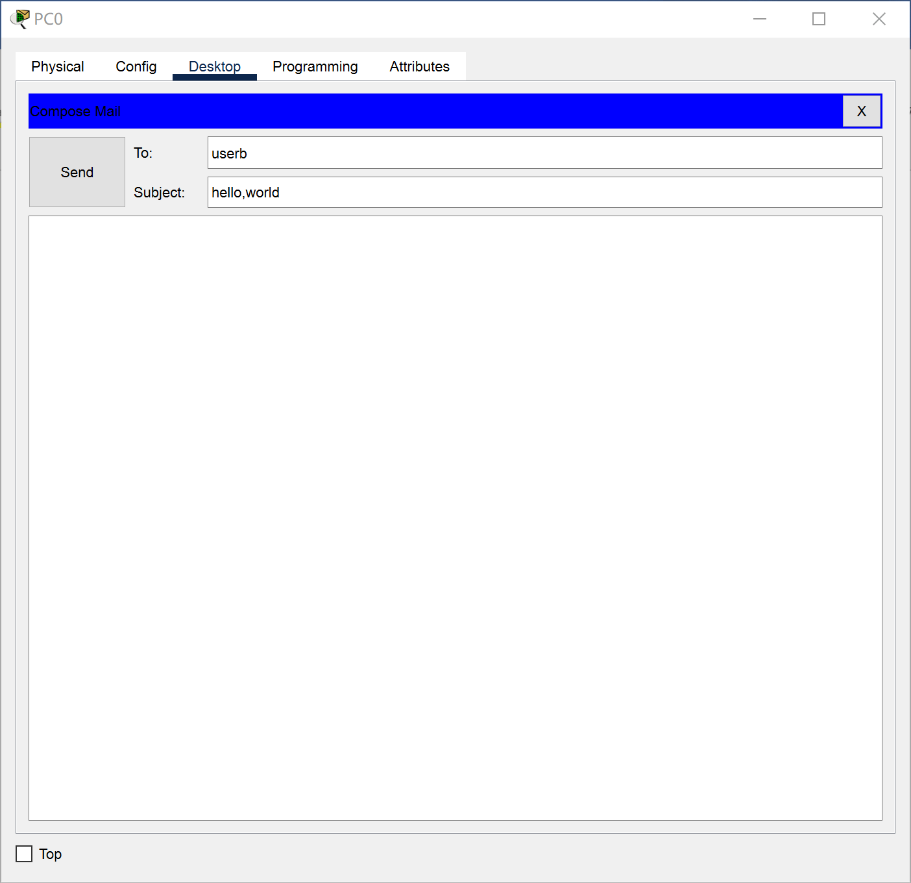
第五步：邮件的发送和接收(以PC0和PC1为例)

图1-5-7 从PC0向PC1发送邮件

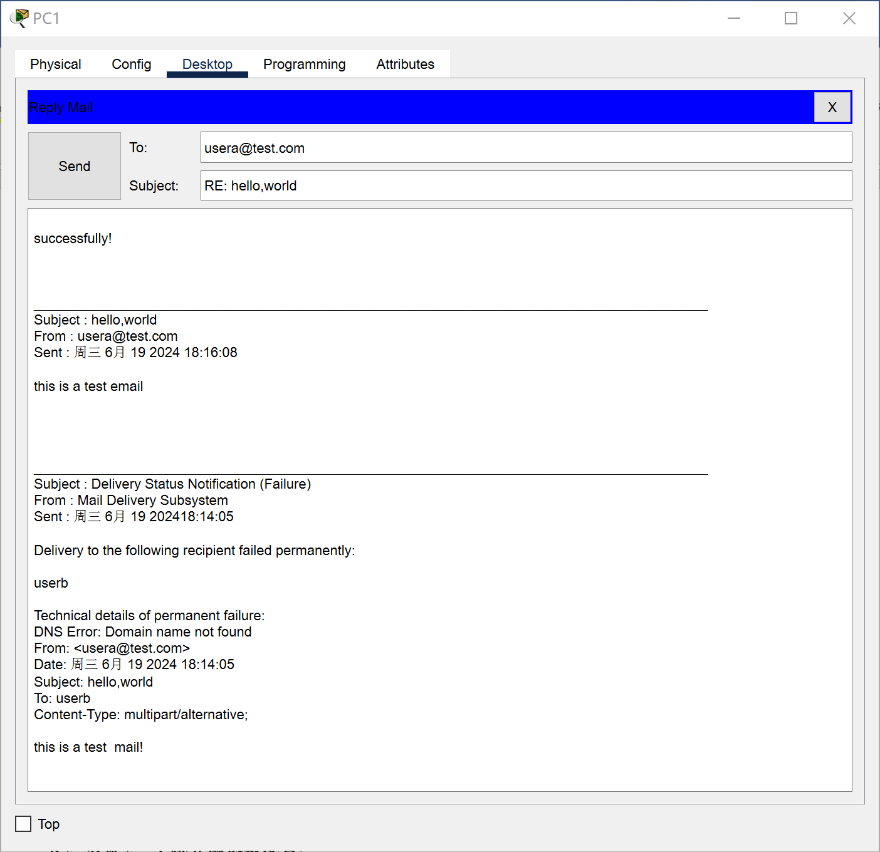
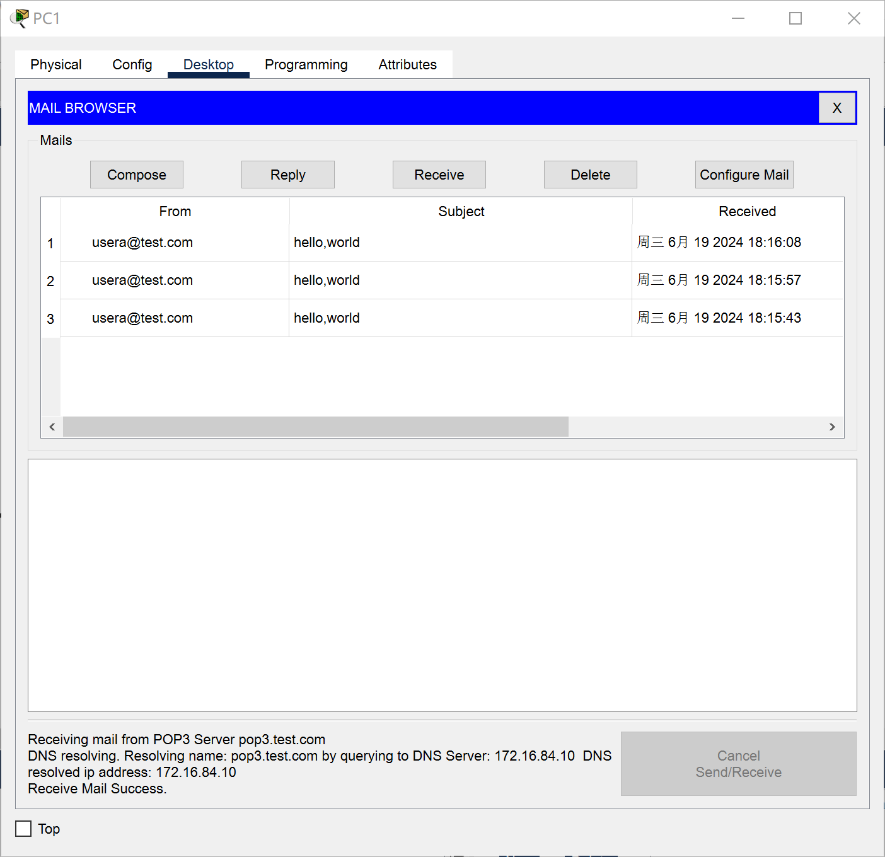
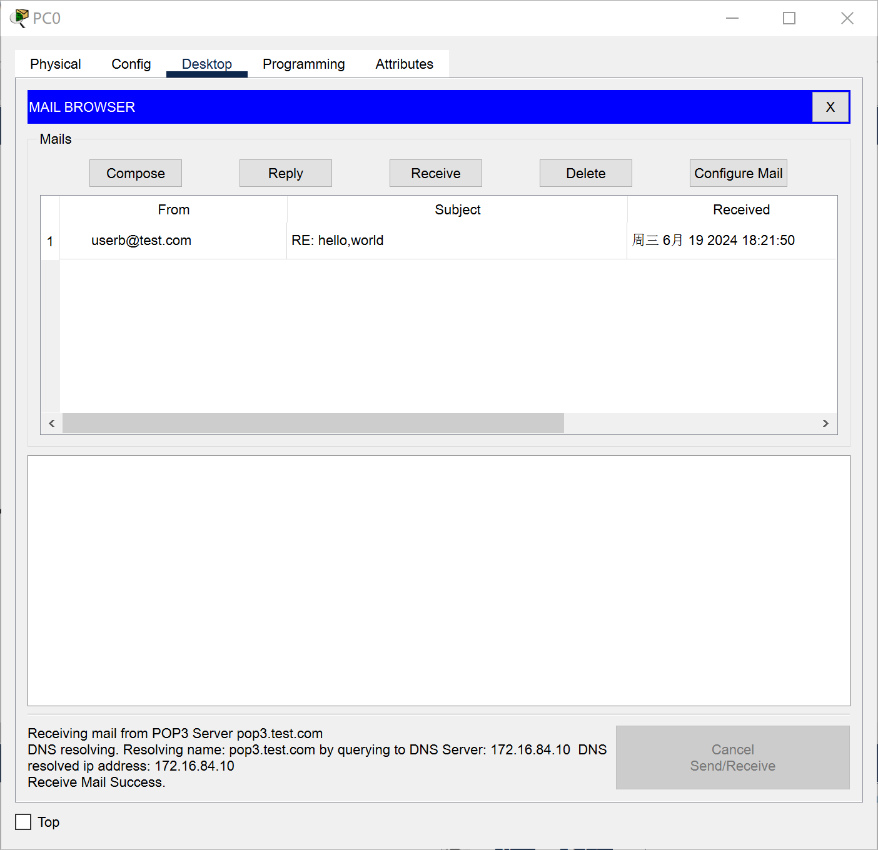
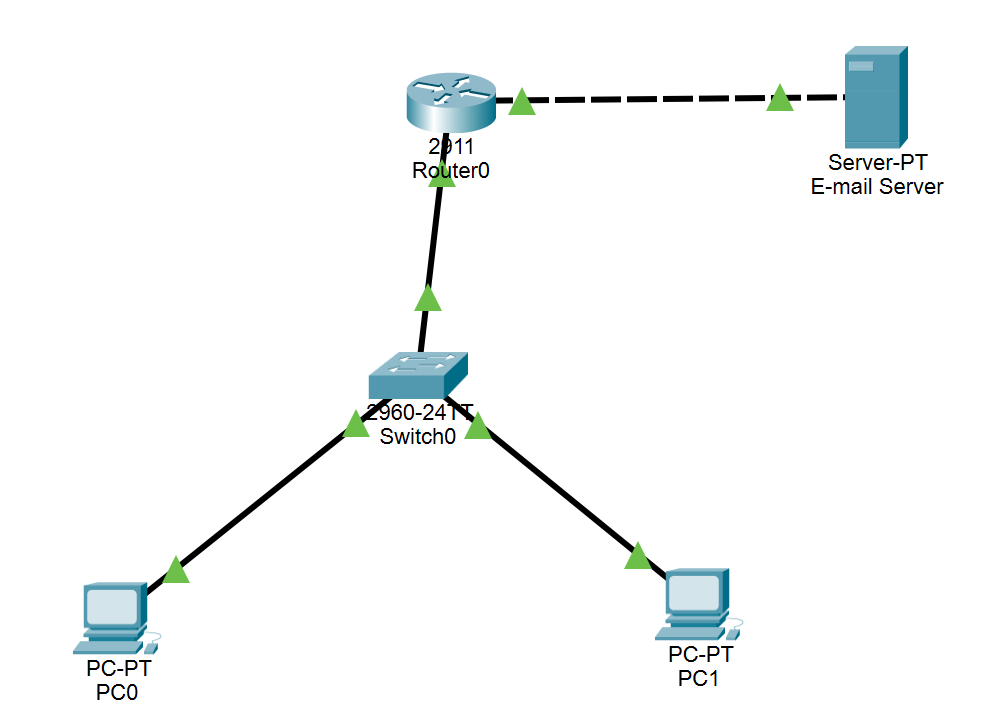
图1-5-8 在PC1上接收邮件

图1-5-9 从PC1向PC0回复邮件

图1-5-10 在PC0上收到PC1的回复



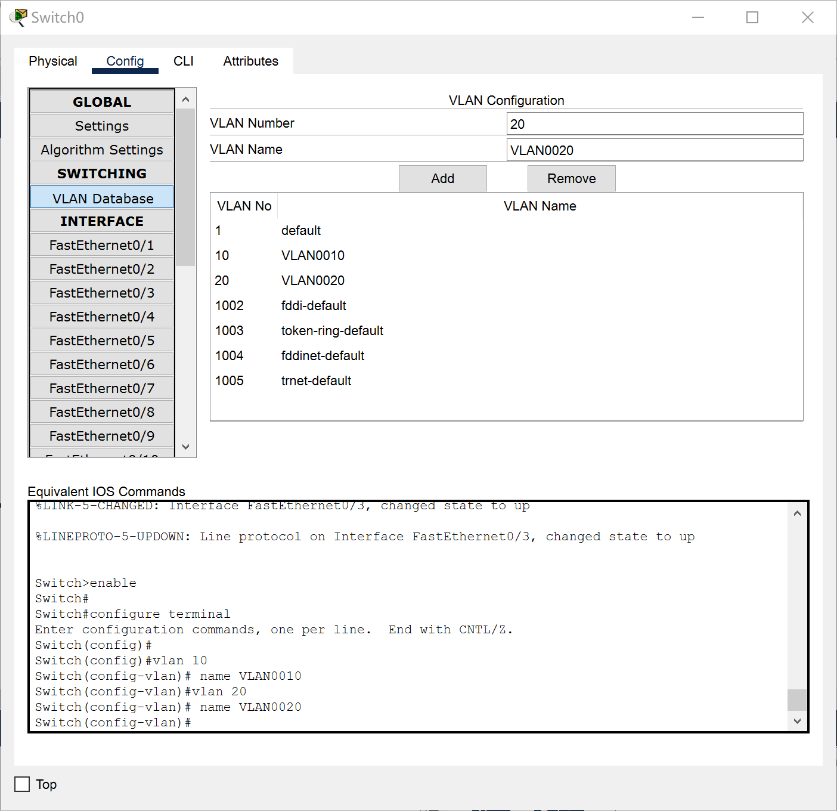
### 8.1.6 实验1.6：Email与VLAN的结合

图1-6-1 VLAN与邮件服务器拓扑图

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | IP | Submark | GW | DNS |
| Router 0 | G0/1 | 172.16.84.1 | 255.255.255.0 |  |  |
| G0/0 | 172.16.82.1 | 255.255.255.0 |  |  |
| PC0 | | 172.16.82.2 | 255.255.255.0 | 172.16.82.1 | 172.16.84.10 |
| PC1 | | 172.16.82.3 | 255.255.255.0 | 172.16.82.1 | 172.16.84.10 |
| FTP Server | | 172.16.84.10 | 255.255.255.0 | 172.16.84.1 |  |

表1-6-1各设备参数配置

第一步：配置交换机的VLAN

图1-6-2 交换机的VLAN配置

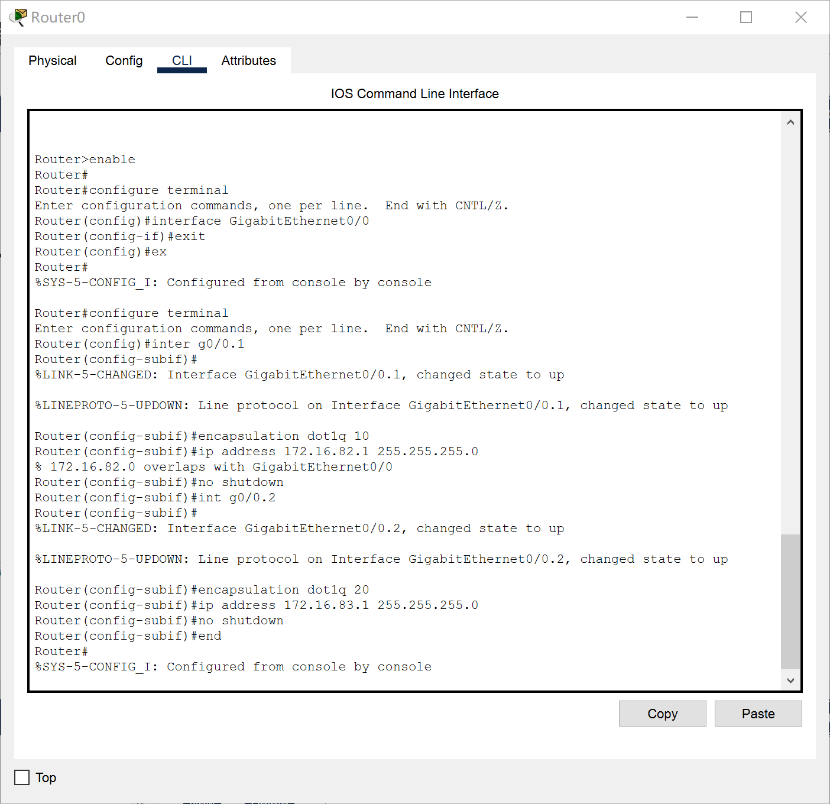
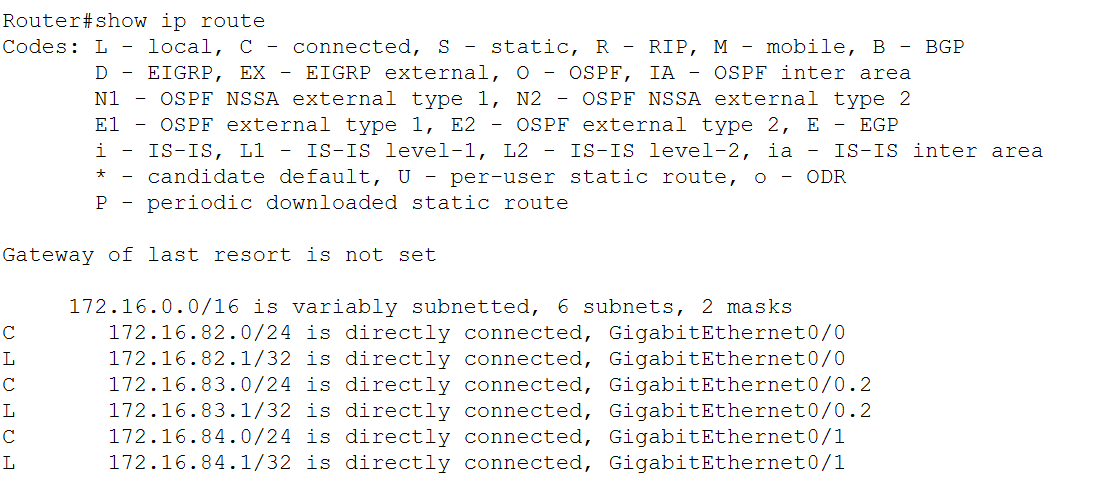
第二步：配置路由器的单臂路由

图1-6-3 配置路由器

图1-6-4 路由表项信息

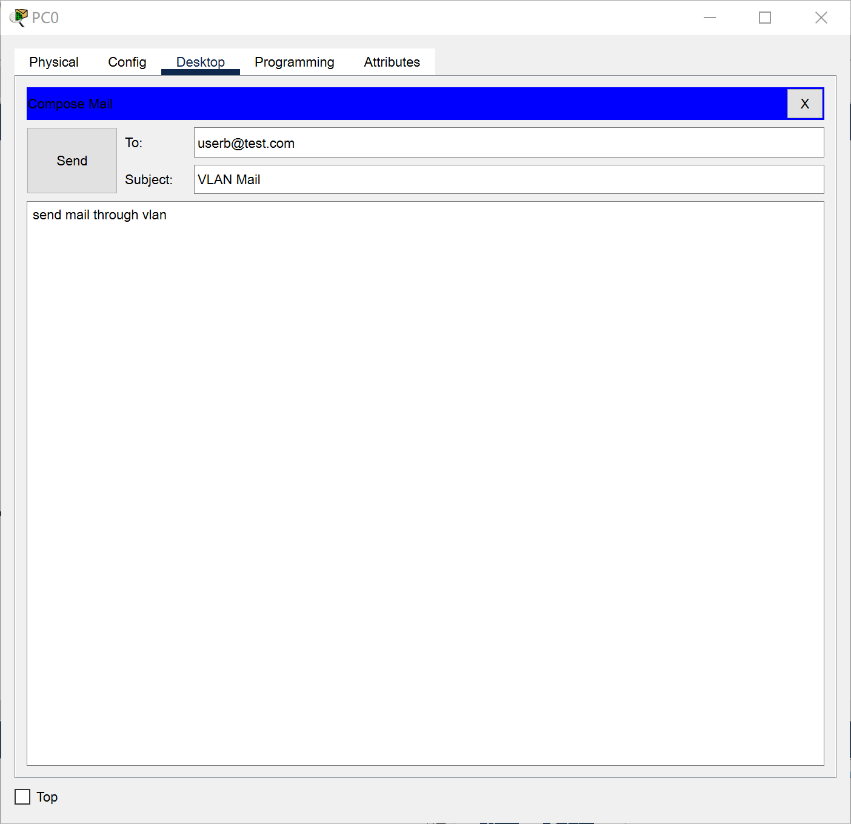
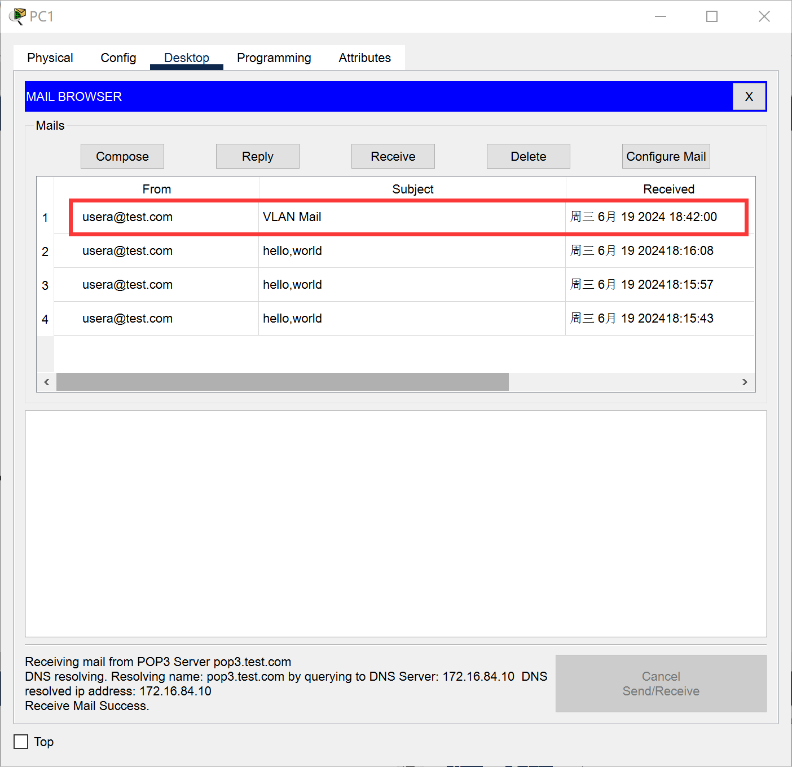
第三步：连通性测试

图1-6-5 发送邮件

图1-6-6 接收邮件

### 8.1.7 实验1.7：HTTP服务器配置实例

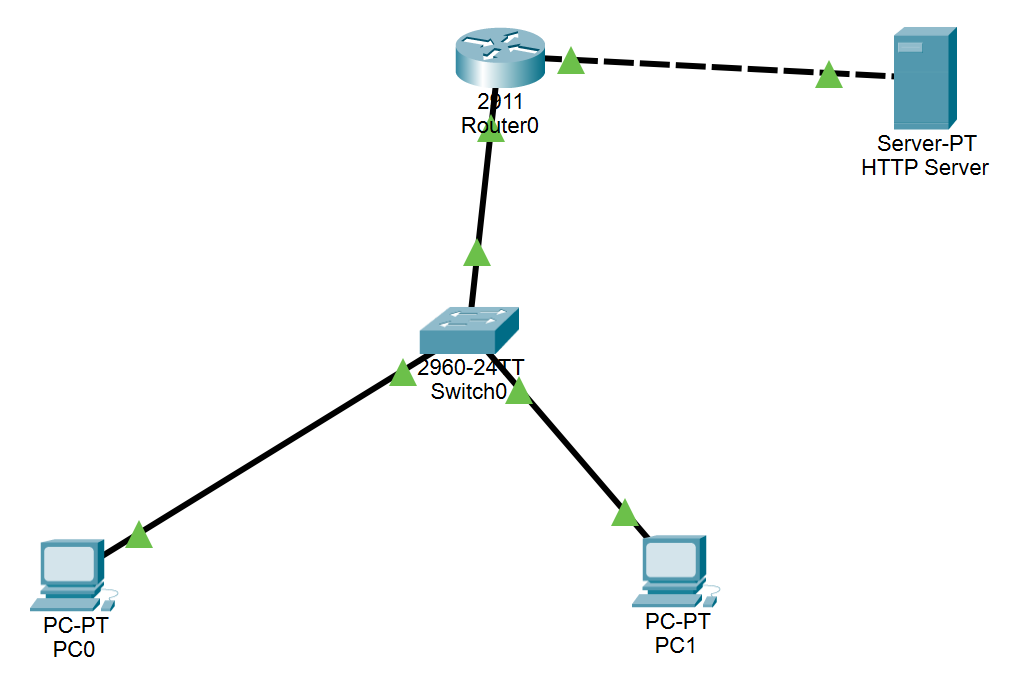
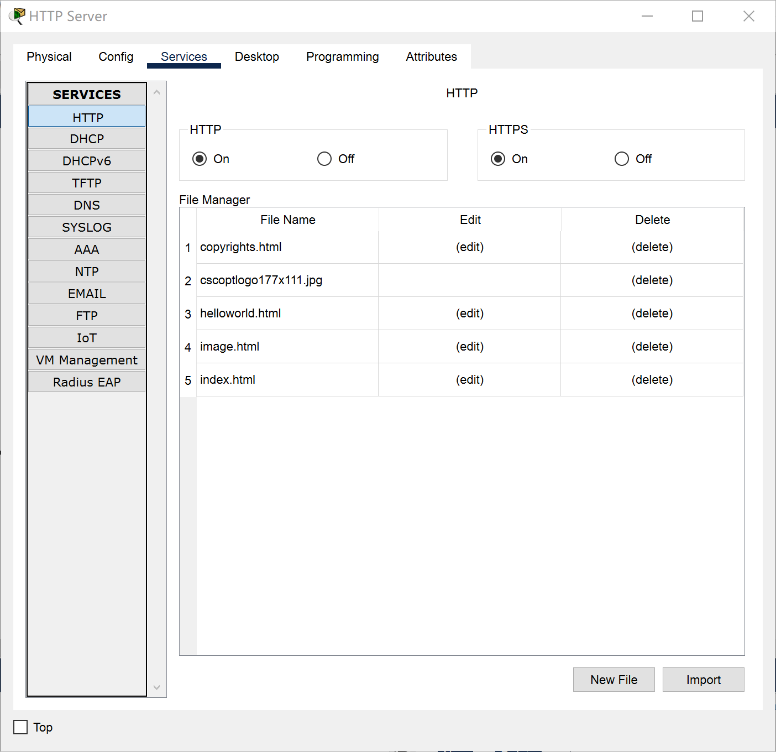
第一步：构建HTTP网络拓扑，如图1-7-1所示。

图1-7-1 HTTP服务器配置拓扑图

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | IP | Submark | GW | DNS |
| Router 0 | G0/1 | 172.16.84.1 | 255.255.255.0 |  |  |
| G0/0 | 172.16.82.1 | 255.255.255.0 |  |  |
| PC0 | | 172.16.82.2 | 255.255.255.0 | 172.16.82.1 | 172.16.84.10 |
| PC1 | | 172.16.82.3 | 255.255.255.0 | 172.16.82.1 | 172.16.84.10 |
| FTP Server | | 172.16.84.10 | 255.255.255.0 | 172.16.84.1 |  |

表1-7-1 各设备参数配置

第二步：配置HTTP server

图1-7-2 配置HTTP服务器

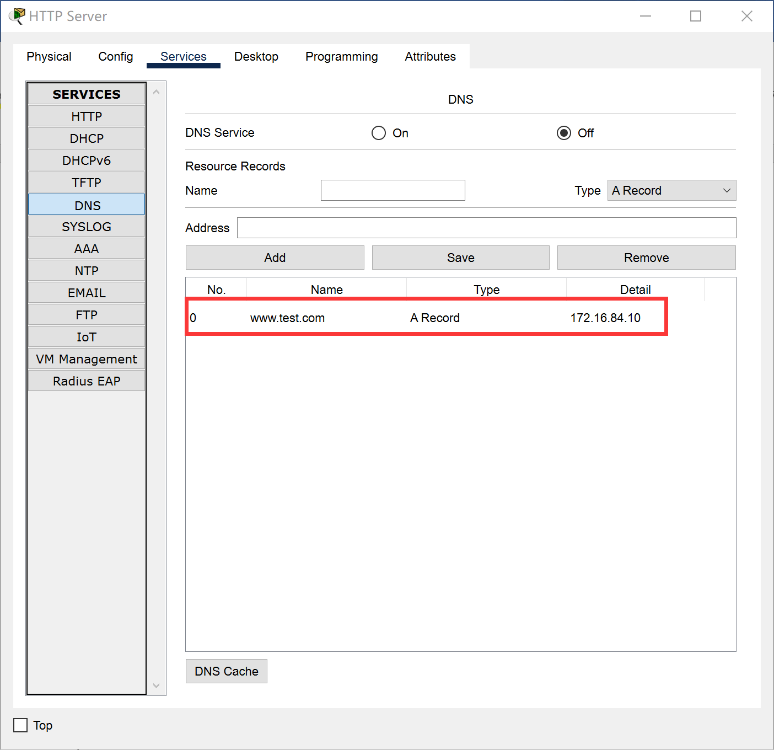
第三步：开启DNS解析服务

图1-7-3 DNS域名服务配置

第四步：Web网页访问(以PC0为例)

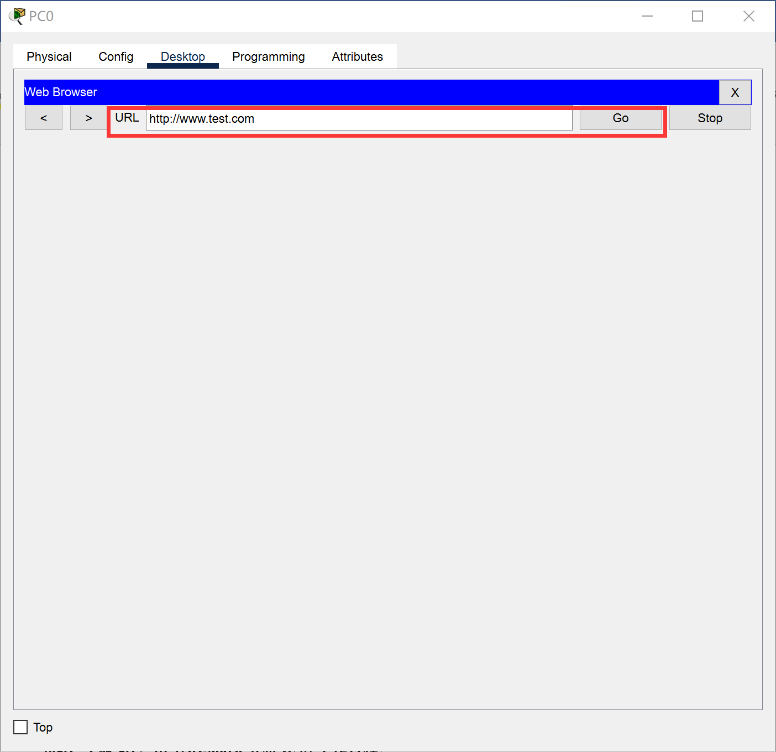
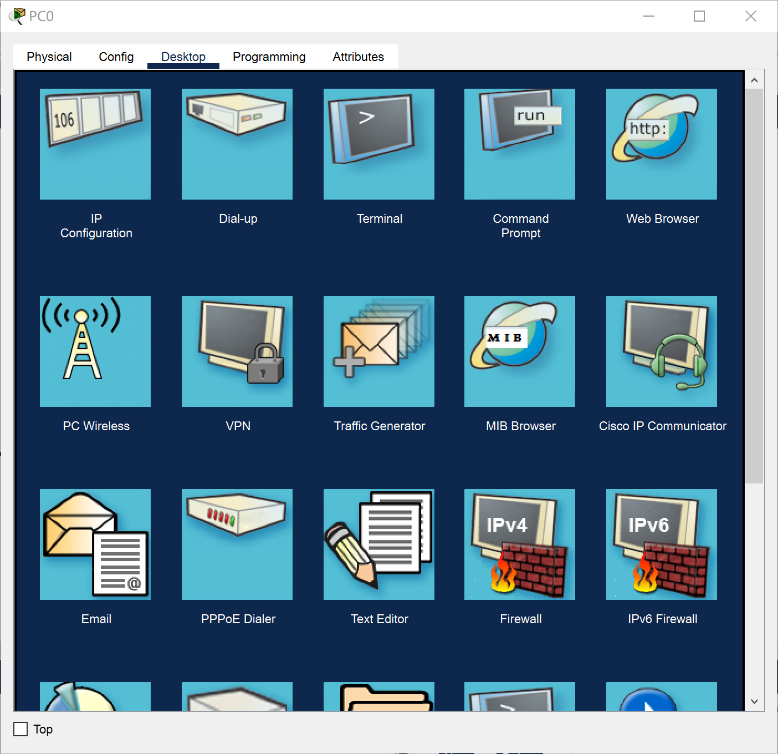
图1-7-4 PC0上的Web浏览器

图1-7-5 PC0上的Web服务器

## 8.2 实验2：常用应用层协议分析

### 8.2.1 实验2.1：DNS协议分析

8.2.1.1 域名查询分析

nslookup命令作用是用于查询dns解析域名记录，查看域名解析是否正常，在网络故障的时候用来诊断网络问题。

(1)在cmd中输入 nslookup -qt www.baidu.com

图2-1-1 nslookup命令

(2) 用wireshark抓包

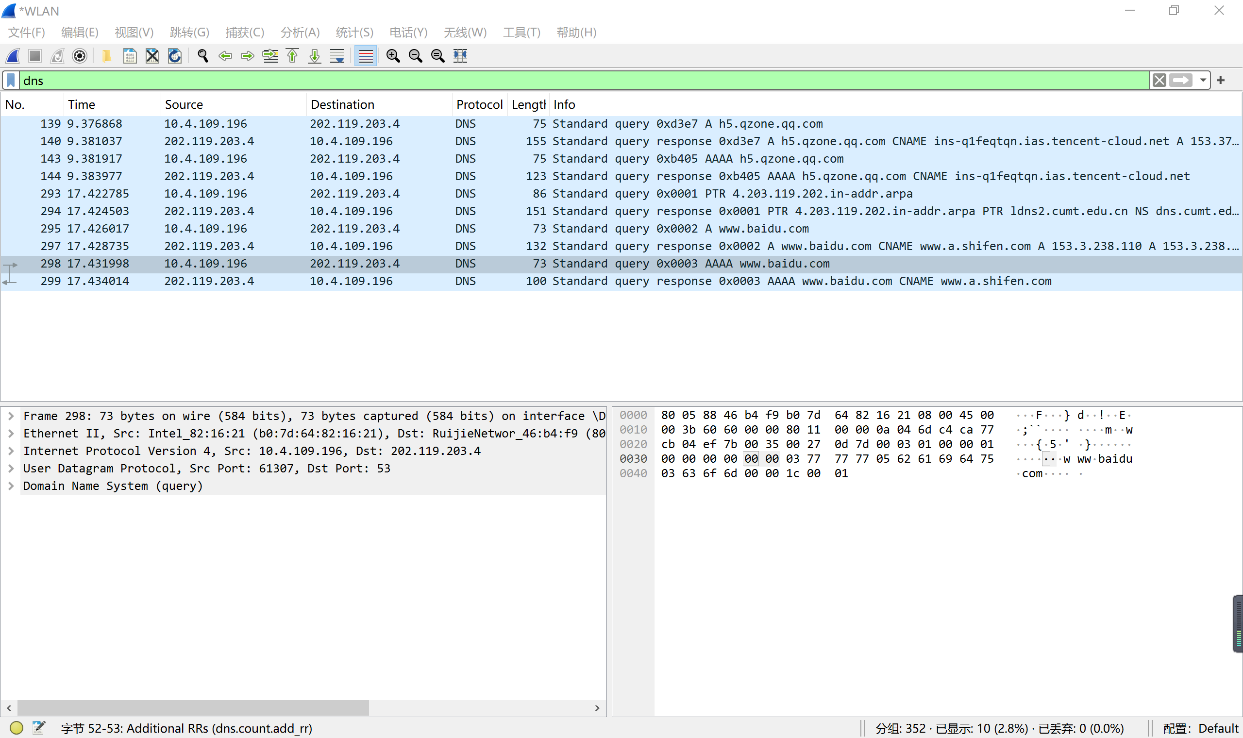
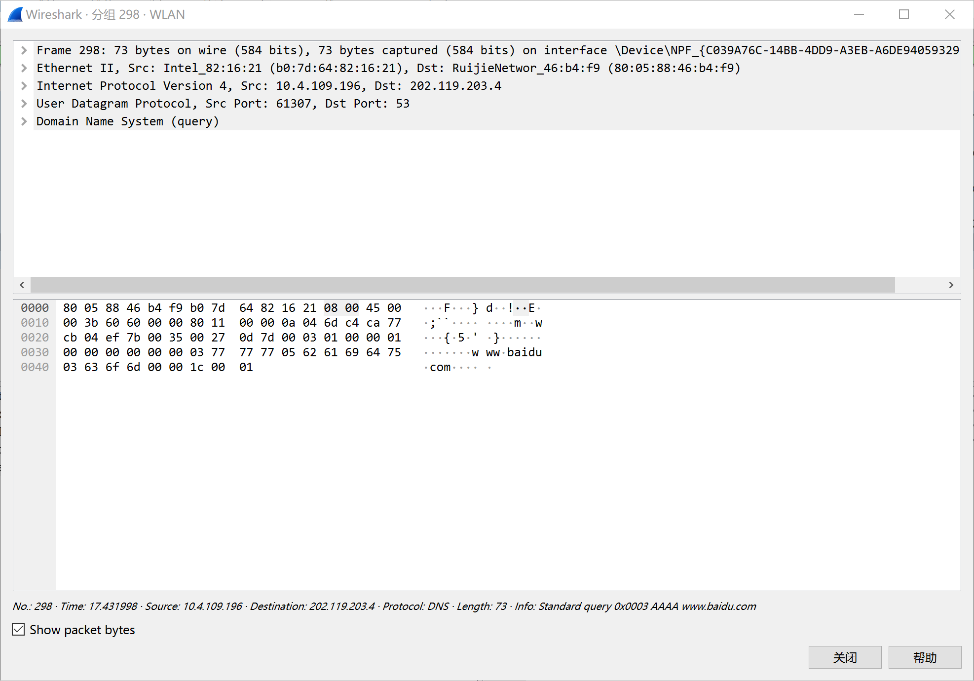
在wireshark中设置过滤条件为DNS：

图2-1-2 wireshark抓取DNS报文

(3)DNS协议的封装结构

DNS为应用层协议，传输采用UDP，网络层是IP协议，数据链路层是以太网帧。

图2-1-3 DNS报文的封装结构

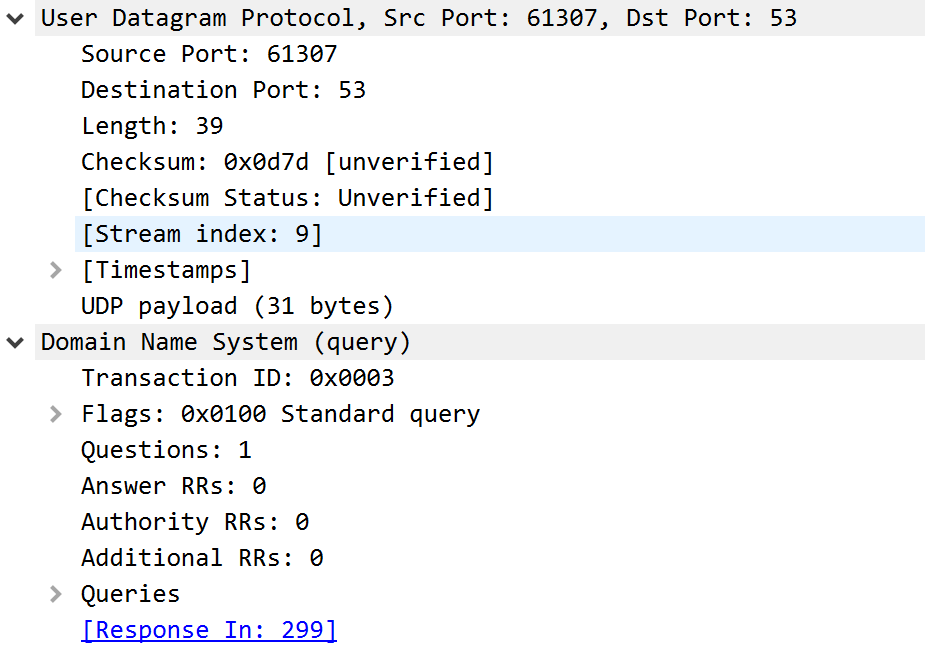
(4)UDP数据报分析

图2-1-4 DNS报文的UDP数据

表2-1-1 UDP各字段分析

|  |  |  |
| --- | --- | --- |
| 名称 | 字节数 | 表示 |
| Source Port | 2 | 源端口号为61307 |
| Destination Port | 2 | 目的端口号为53 |
| Length | 2 | 长度为39字节 |
| Checksum | 2 | 校验和为0x0d7d |

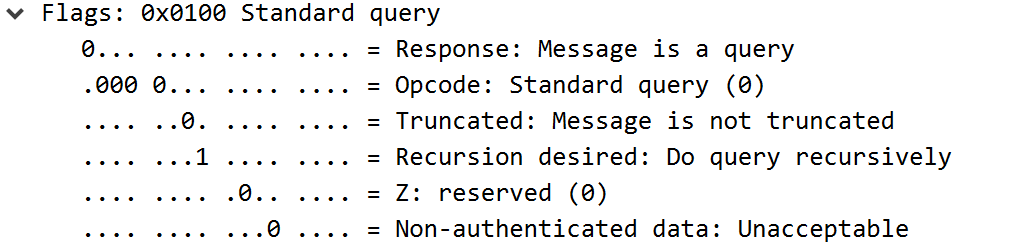
(5)DNS报文分析

图2-1-5 DNS报文分析

由图2-1-4和2-1-5分析，如下所示：

①Transaction ID(2字节)：0x0003。会话标识ID字段，用于辨识DNS应答报文是哪个请求报文的响应，用于划分DNS流(一个请求对应一个响应)。图中报文标识数为：0x08e5.

②Flags(2字节)：0x0100 Standard query

QR(1 bit):查询/响应的标志位,1为响应，0为查询。此处为查询，值为零。

opcode(4 bit):定义查询或响应的类型(0标准查询(QUERY)、1反向查询(IQUERY)、2服务器状态查询(STATUS)、3无、4为通知(Notify)、5为更新(Update)、6-15保留值，暂时未使用)。此处为0，表示标准查询。

Truncated (1 bit)︰截断标志位。用来指出报文比允许的长度还要长，导致被截断。1表示响应已超过512字节并已被截断，此处为0，表示没有被截断。

Recursion desired (1 bit)︰期望递归，该位为1表示期望进行递归查询(从域名服务器进行递归查询)，此处为1。

Zero (3 bit):保留字段，在所有的请求和应答报文中必须置为0。

rcode (4 bit):返回码，在响应报文中，各取值的含义: 0-无差错,1-格式错误，2-域名服务器出现错误，3-域参照问题，4-查询类型不支持，5-被禁止，6~15保留。此处为0，表示无差错。

Non-authenticated data:意思为未经认证的数据。0为服务器已经进行了相关DNSSEC 数字签名的验证， 1为服务器并未进行相关DNSSEC 数字签名的验证。

数字字段，都为⒉字节:

Questions: 1表示表示查询问题区域的数量，此处为1

Answer RRs: 0表示回答区域的数量，此处为0

Authority RRs: 0表示授权区域的数量，此处为0

Additional RRs: 0表示附加区域的数量,此处为0。

8.2.1.2 域名解析分析

访问www.sina.com.cn

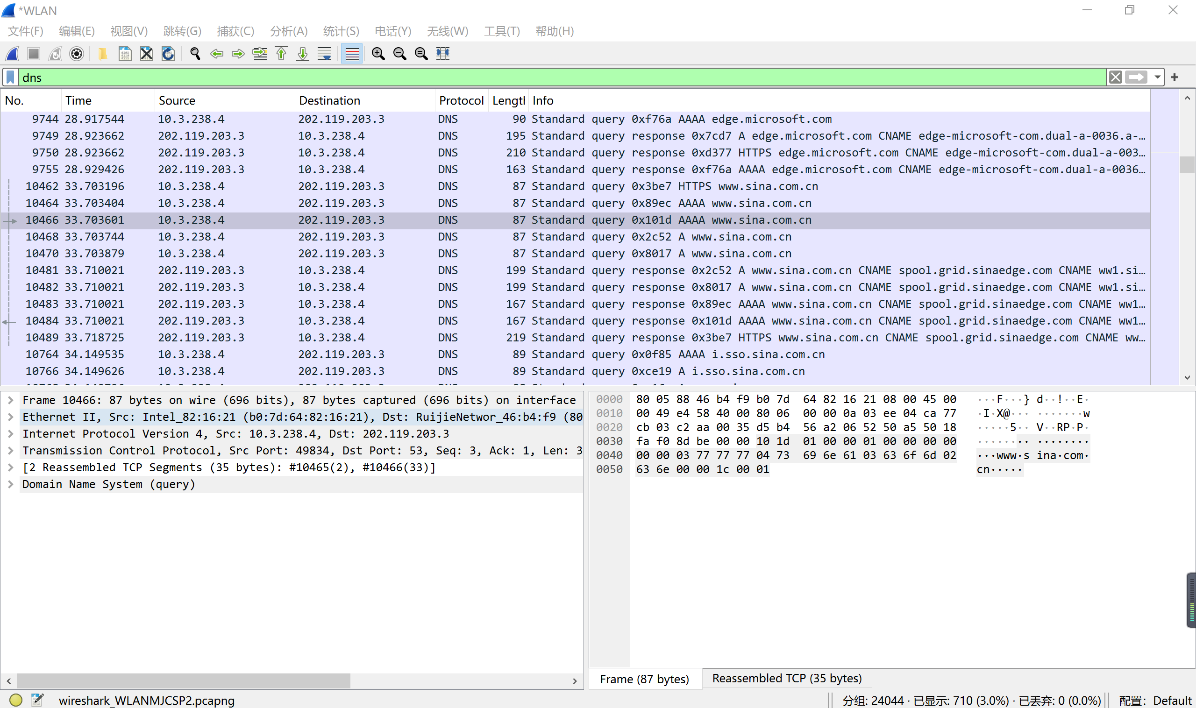
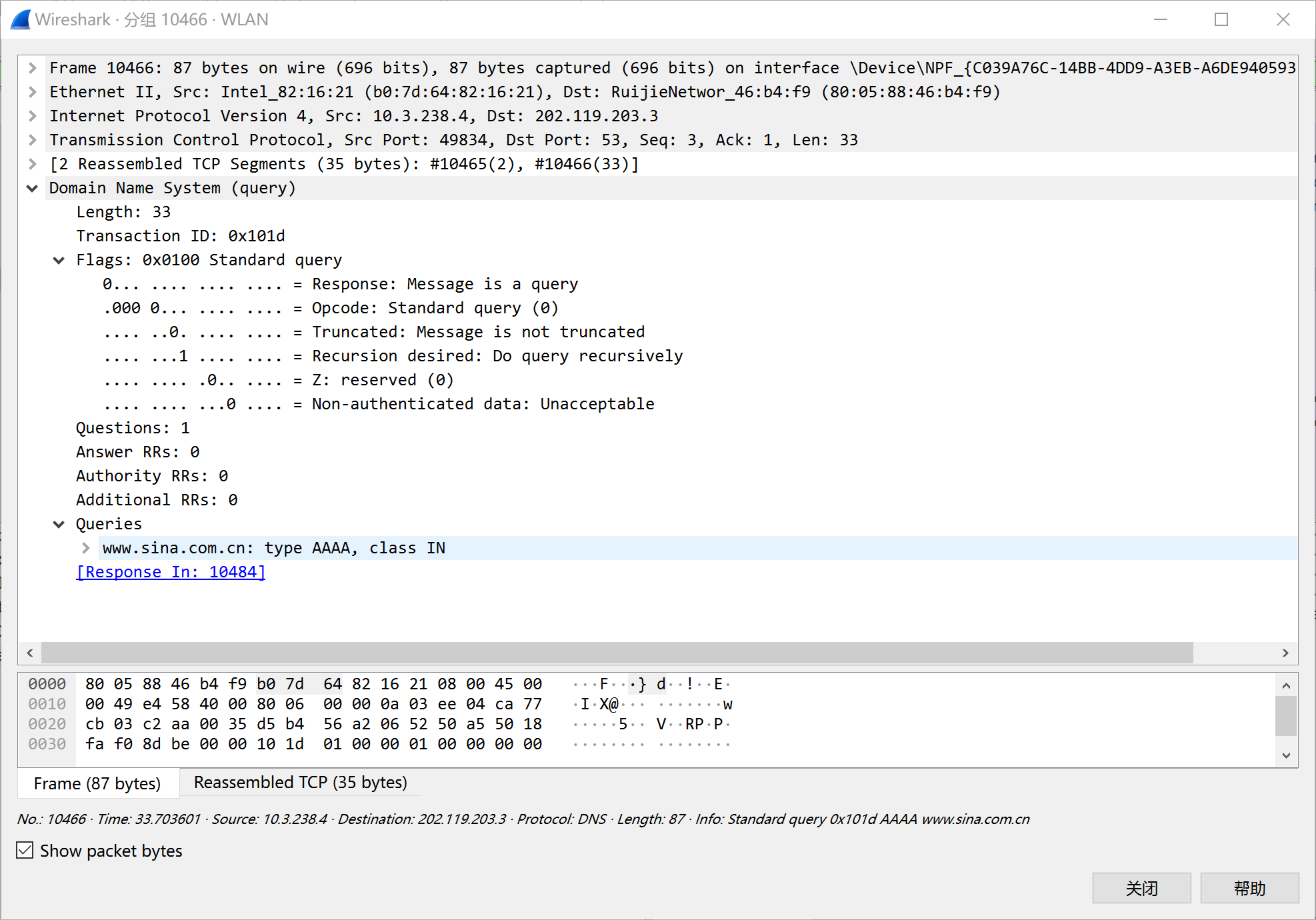
图2-1-6 DNS报文抓取

图2-1-7 DNS查询报文分析

数据帧：长度 72 字节

WLAN帧：IPv4类型数据

源MAC地址：b0:7d:64:82:16:21

目的MAC地址：80：05：88：46：b4:f9

IP数据报：

源IP地址：10.3.238.4

目的IP地址：202.119.203.3

UDP数据报：

源端口：49834

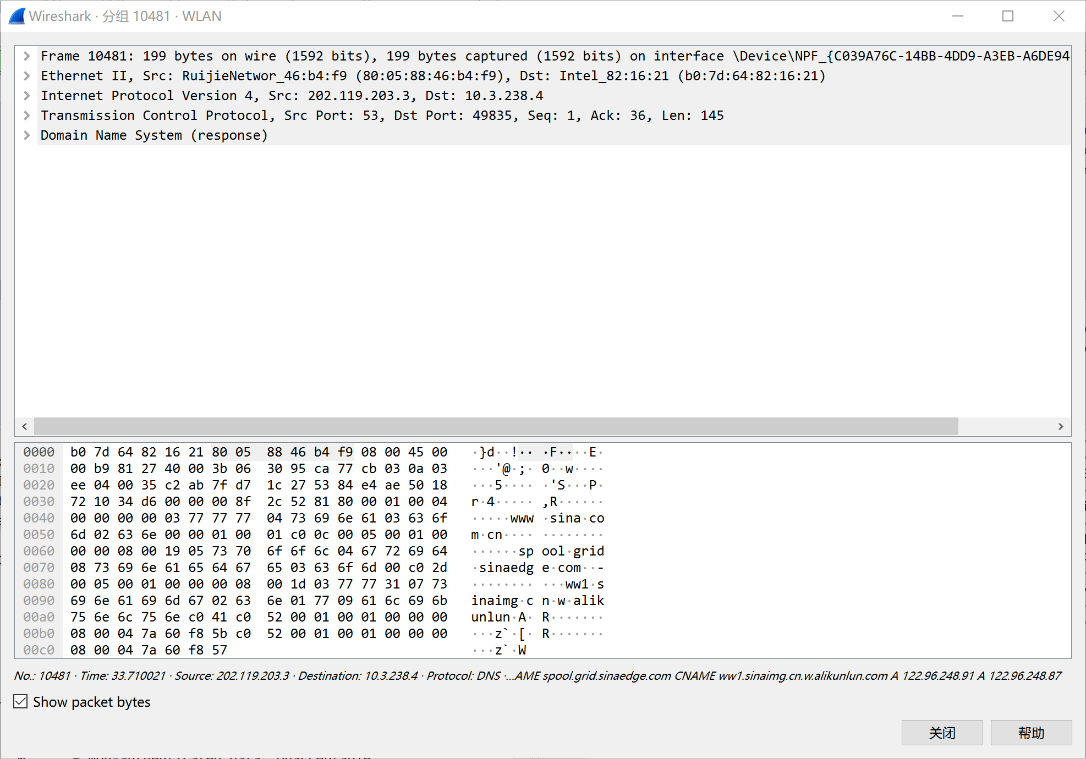
目的端口：53

图2-1-8 DNS响应报文

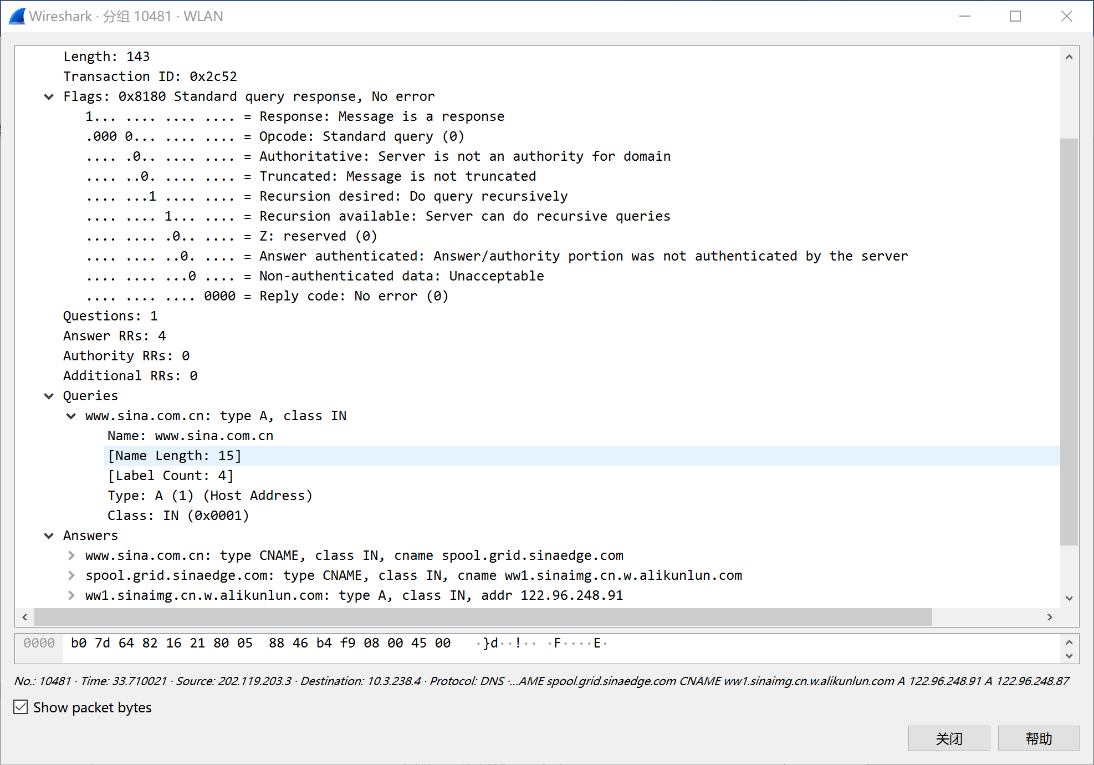


图2-1-9 DNS响应报文分析

Transaction ID：0x2c52

Flags标志字段：2字节

Questions(2字节)：1

Answer RRs(资源记录数)：4 说明Answer中会出现4个解析结果。

Authority RRs(授权资源记录数)：0

Additional RRs(额外资源记录数)：0

字段Queries为查询或者响应的正文部分，分为Name、Type和Class

Name(查询名字)：www.sina.com.cn

Type(查询类型)：2字节，这里是主机A记录

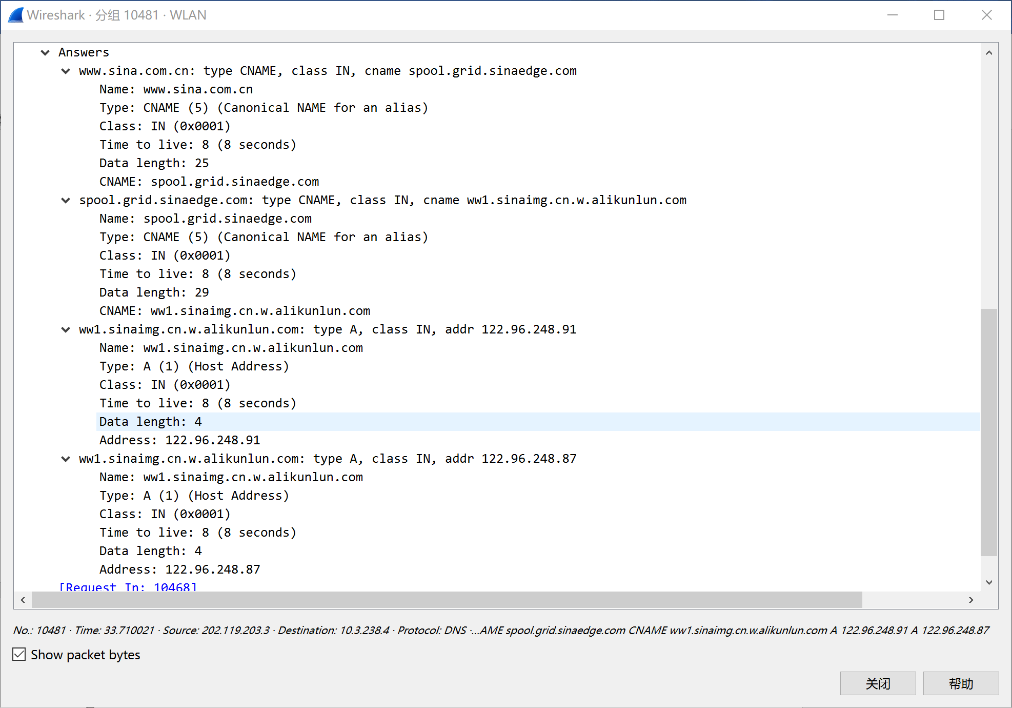
Class(2字节)：IN表示Internet数据，为1

图2-1-10 DNS响应报文的Answers字段

Answers字段可以看成一个List，集合中每项为一个资源记录，除了上面提到过的Name、Type和Class之外，还有Time to Live、Data length和Addr。

Type:值为CNAME，意思是规范名称定义主机的正式名字的别名

Time to Live(生存时间TTL):表示该资源记录的生命周期，从取出记录到抹掉记录缓存的时间，以秒为单位。这里是8s

Data length(资源数据长度):以字节为单位，这里是25

可以发现有2条资源记录，4个不同的CNAME，说明域名www.sina.com.cn对应有4个CNAME，分别是:

spool.grid.sinaedge.com

ww1.sinaimg.cn.w.alikunlun.com

### 8.2.2 实验2.2：HTTP协议分析

(1) Wireshark抓取HTTP报文

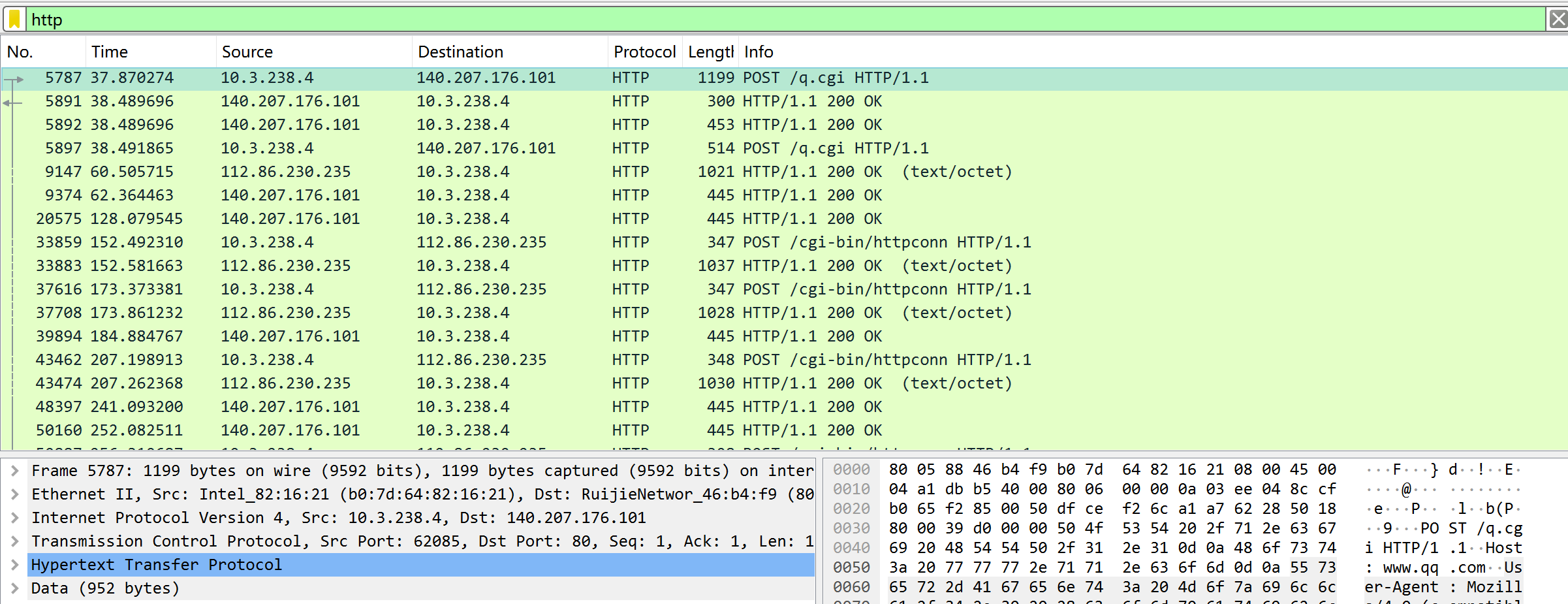


图2-2-1 HTTP报文抓取

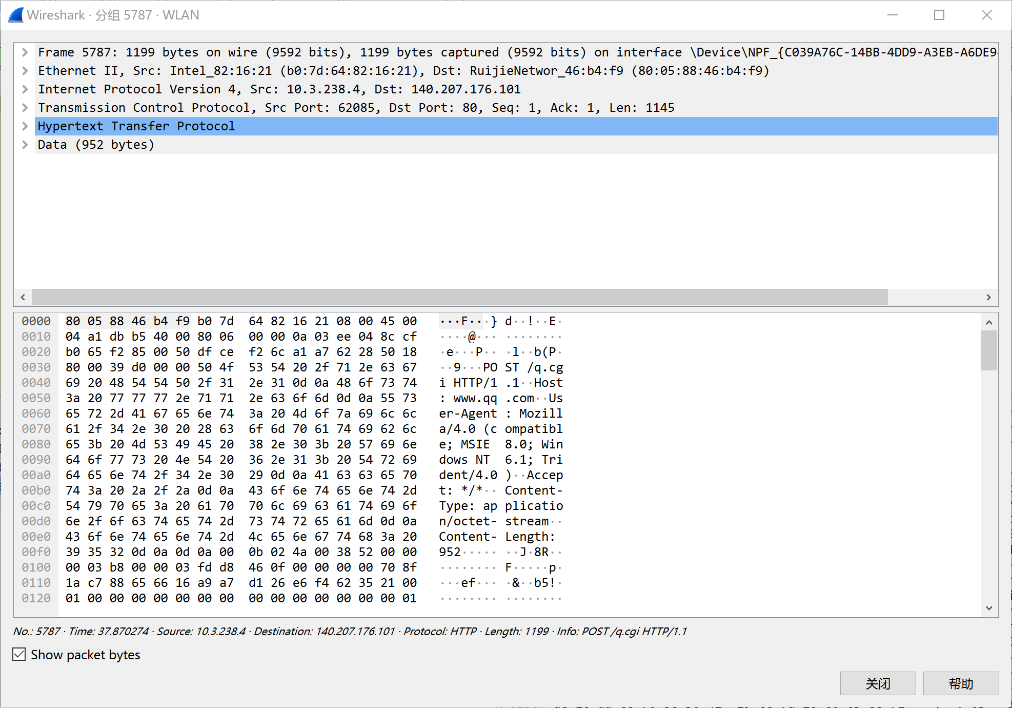
(2)HTTP报文的封装层次

图2-2-2 HTTP报文的层次结构

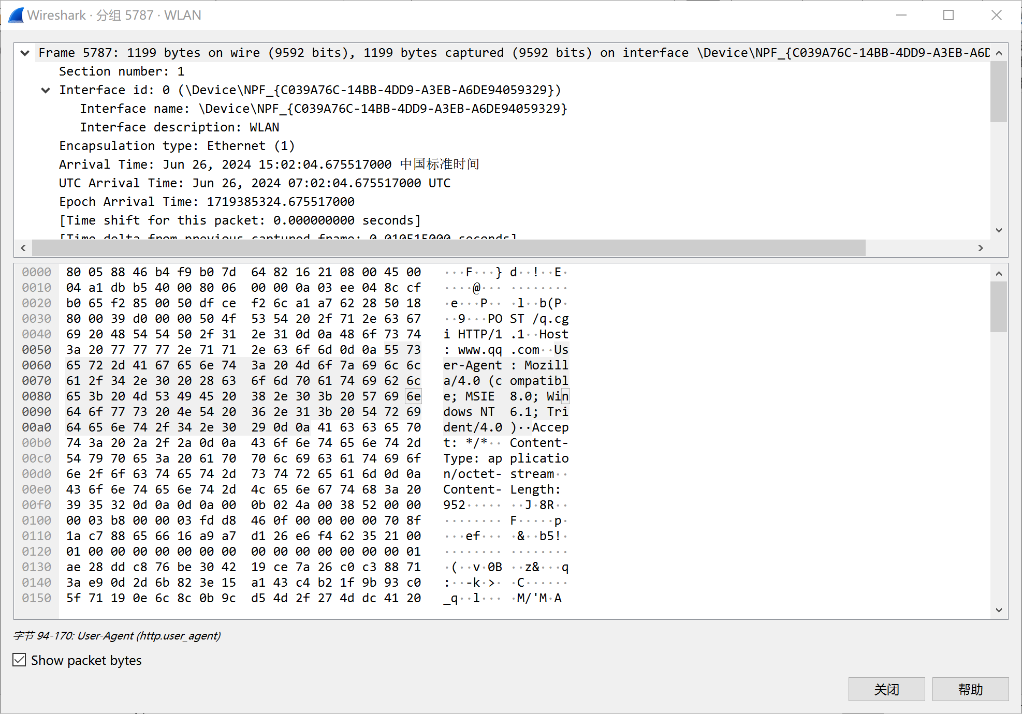
(3)抓取包的总体信息

图2-2-3 数据帧的总体信息

抓取的数据报帧为5787号，长度为1199字节，由接口0获取，封装方式是WLAN

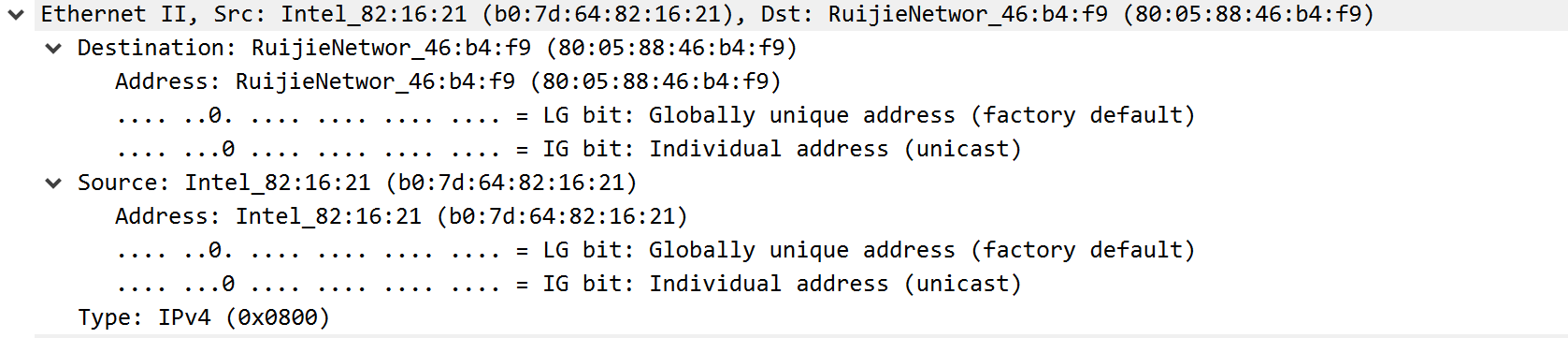
(4)WLAN帧分析

图2-2-4 WLAN帧

WLAN帧的type类型为IPV4，是一个IP包，版本是v4

还给出了源MAC地址：b0:7d:64:82:16:21和目的MAC地址：80:05:88:46:b4:f9

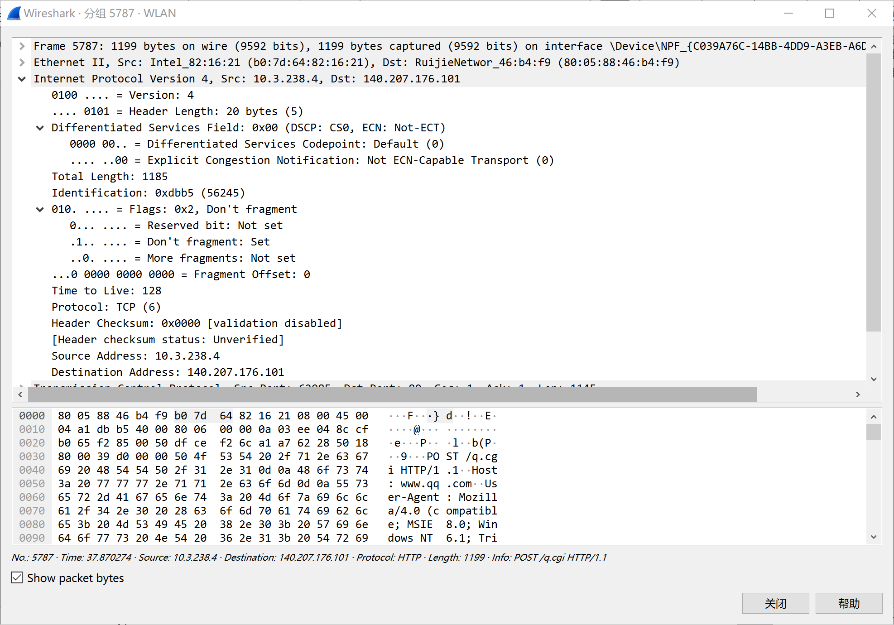
(5)IP数据报分析

图2-2-5 IP数据报

版本(4 bit): IPv4

首部长度(4 bit):值为5，以4 bit为单位表示20 byte区分服务(4 bit):值为0，在区分服务时才有用总长度(16 bit):值为1185，表示数据报总长度11185

标识(16 bit):值为56245，标识数据报计数器，当重组时起作用

标识(3 bit):此处为010，一般前两位有用，MF表示还有没有分片，0表示这是最后一个，DF表示不能分片，为1表示可以分片。

片偏移(13 bit):值为0，以8字节为偏移单位,此处表示在开头。

生存时间(4 bit):值为128，表示数据报在网络中的寿命，现在多用于表示跳数协议(8 bit):值为6，表示上交给TCP协议

首部检验和(16 bit):只检验首部，由于系统原因无法显示

源地址(32 bit):值为10.3.238.4

目的地址(32 bit):值为140.207.176.101

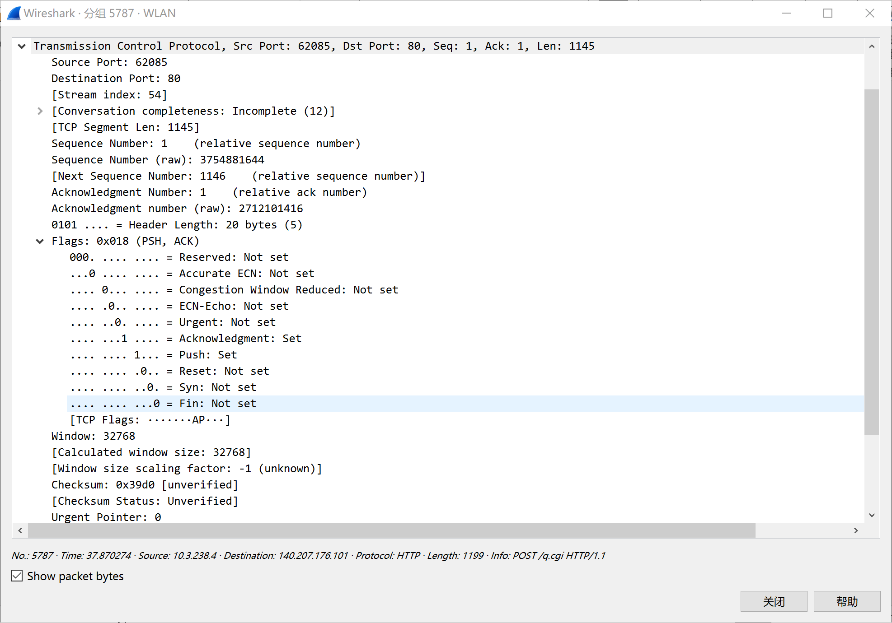
(6)TCP分组分析

图2-2-6 TCP分组第1部分

源端口(16 bit): 62085端口

目的端口(16 bit): 80端口

序号(32 bit):值为1，表示序列号，因为每个字节都要按顺序编号，本段第一个字节的序号

确认序号(32 bit):值为1期望下一个收到的报文段的第一个数据字节的序号

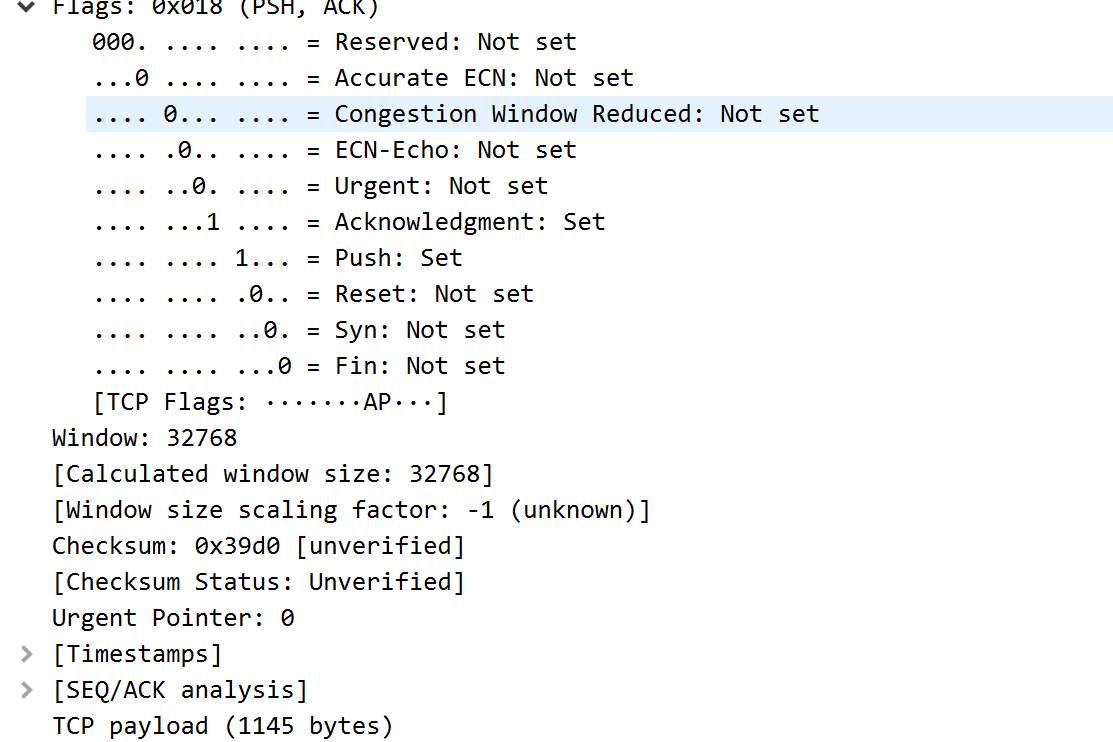
数据偏移(4 bit): 以字节为单位，值为5表示离报文首部20字节

图2-2-7 TCP分组第2部分

Flags:确认为1表示确认号字段有用，推送为1表示在一端命令进程键入一个命令后立即能够收到对方响应。

窗口(2 byte):值为32768，用于提醒现在允许对方的发送量。

检验和(2 byte):检验首部和字段两部分，此处为39d0

紧急指针(2 byte): 0时没有意义

(7)HTTP报文分析

图2-2-8 HTTP报文

HTTP请求报文由四部分组成，分别是请求行、请求头、空行、消息体，每部分内容占一行。

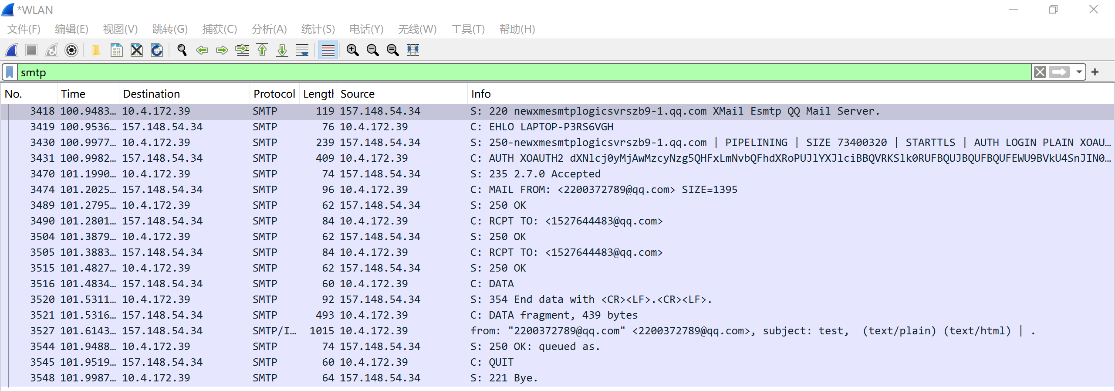
请求行:由三部分组成:分别是请求方法(GET/POST/DELETE/PUT/HEAD)、URI路径、HTTP版本号。此处请求方法为POST，版本号为HTTP/1.1，希望优先接受中文版本文档，主机域名为www.qq.com，还未发送完需要保持链接

请求头:缓存相关信息(Cache-Control，If-Modified-Since)、客户端身份信息(User-Agent)等键值对信息。

主体:客户端发给服务端的请求数据，这部分数据并不是每个请求必须的。

### 8.2.3 实验2.3：电子邮件协议分析

下载Foxmail客户端，设置端口并相应设置wireshark 的过滤器，发送邮件并对SMTP协议进行抓包。

图2-3-1 SMTP协议报文抓取

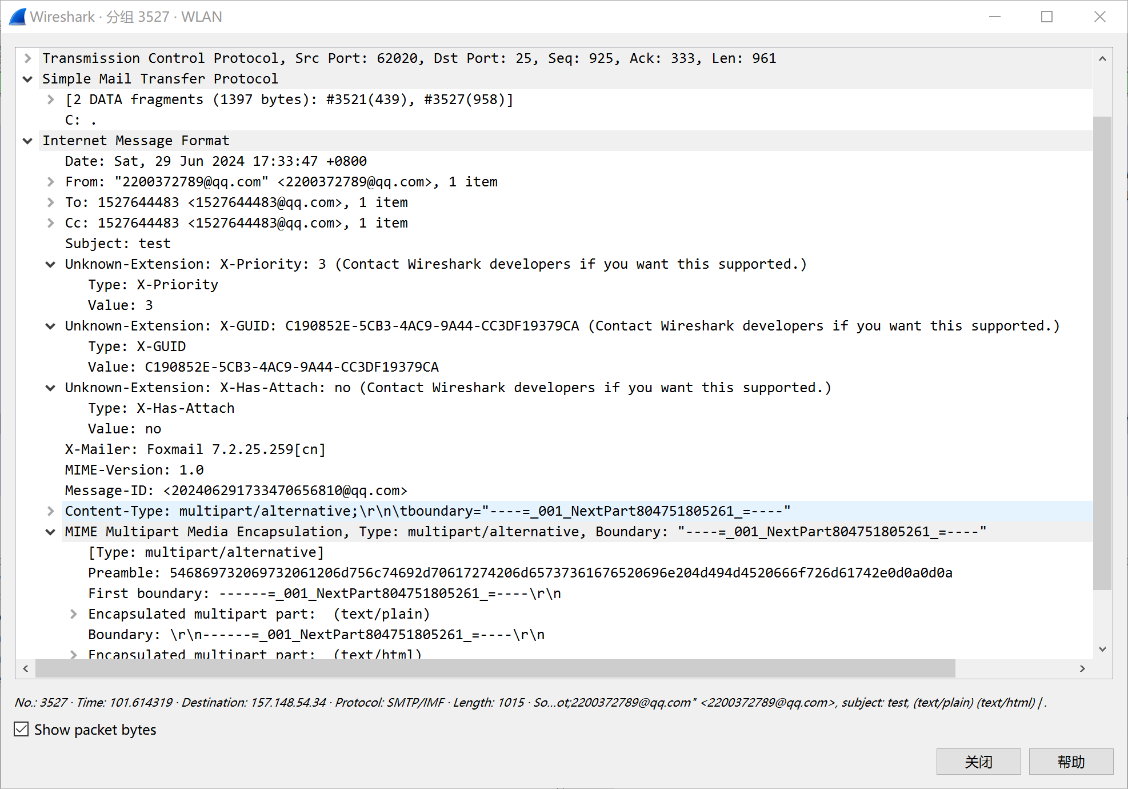
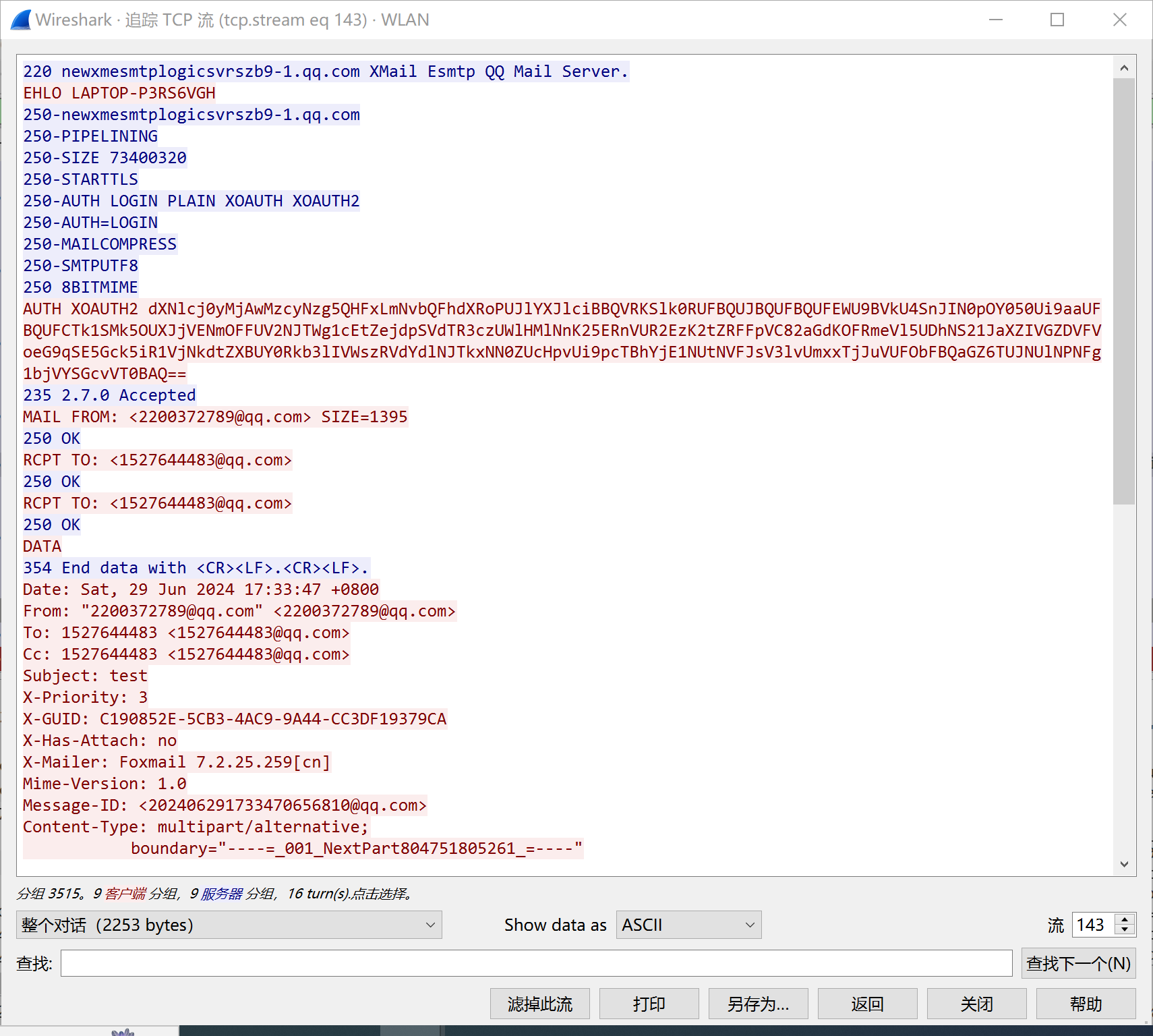
分析其中一帧，可以看到SMTP中的各种信息。

图2-3-2 SMTP邮件内容

图2-3-3 SMTP邮件发送过程追踪

在“追踪流”页面中可以清楚地看到发送方、接收方、发送时间等信息。

因为暂时关闭了SSL加密，因此邮件内容仅采用了简单的base64加密，如图2-3-4所示：

图2-3-4 加密的邮件内容

解码后可得邮件的原始内容，如图2-3-5所示：

图2-3-5 邮件内容解密

### 8.2.4 实验2.4：QQ协议分析

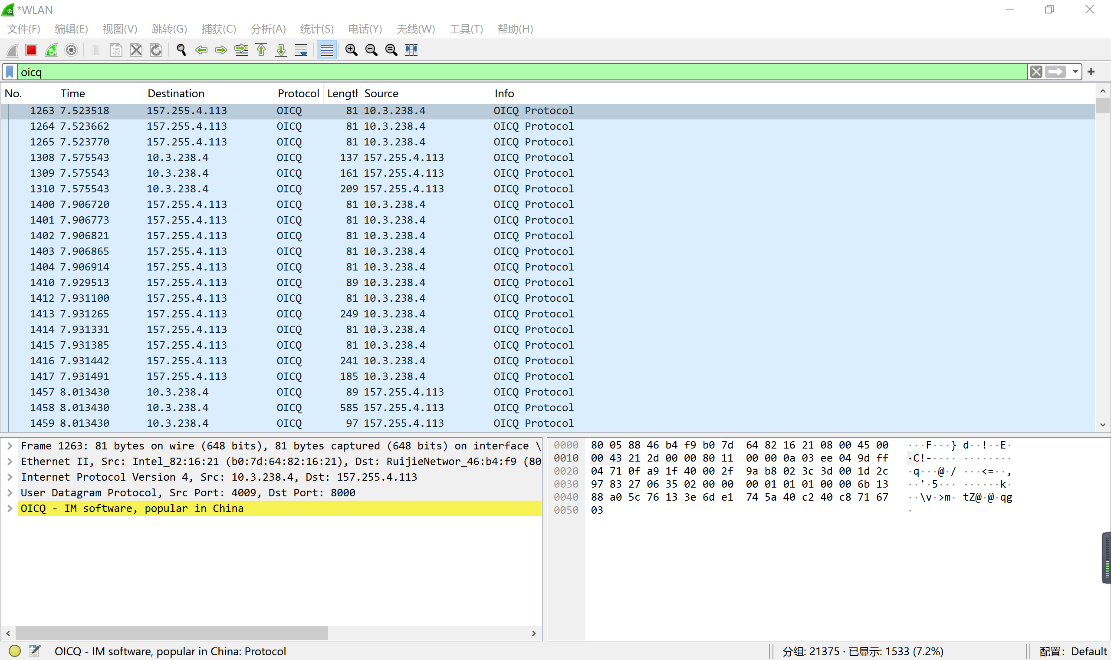
登录QQ，在Wireshark中对QICQ协议进行过滤。

图2-4-1 QICQ协议报文抓取

分析其中一帧：

图2-4-2 QICQ协议报文分析

源地址是10.3.238.4，目的地址为157.255.4.113，源端口是4009，在国内主要是QQ使用的端口号，目的端口是8000。

OICQ协议被描述为"IM software, popular in China"，包含了flag信息(Ox02),版本信息(0x3c3d)，命令信息(29)，序列号(11415)以及发送方QQ号(2200372789)，但data信息已经加密，无法使用Wireshark查看。

### 8.2.5 实验2.5：微信协议分析

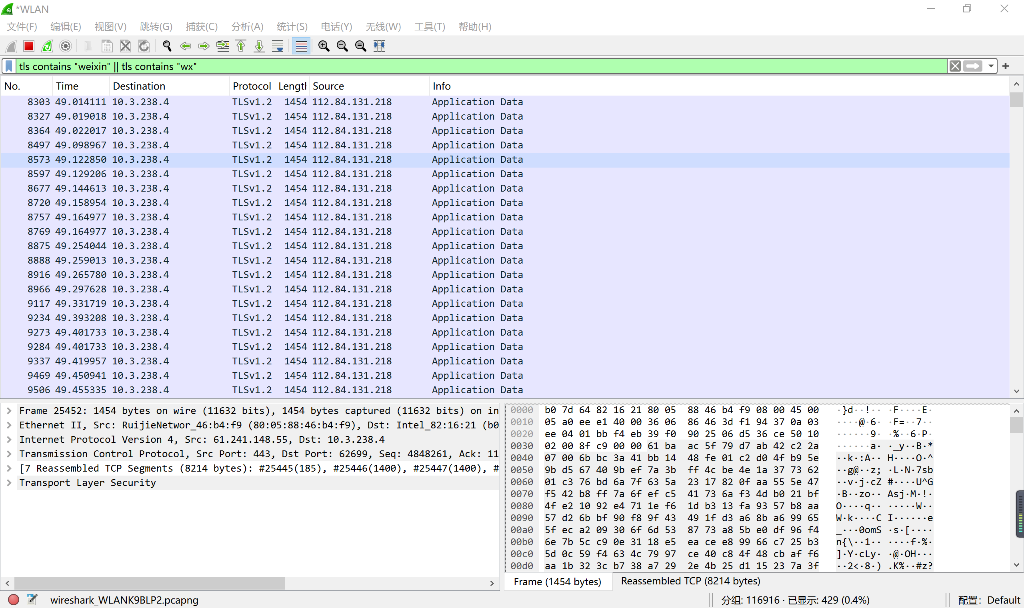
登录微信，找到有wx或者weixin字段的地址并跟踪，可以发现目的地址均为minorshort.weixin.qq.com。

图2-5-1 微信协议报文抓取

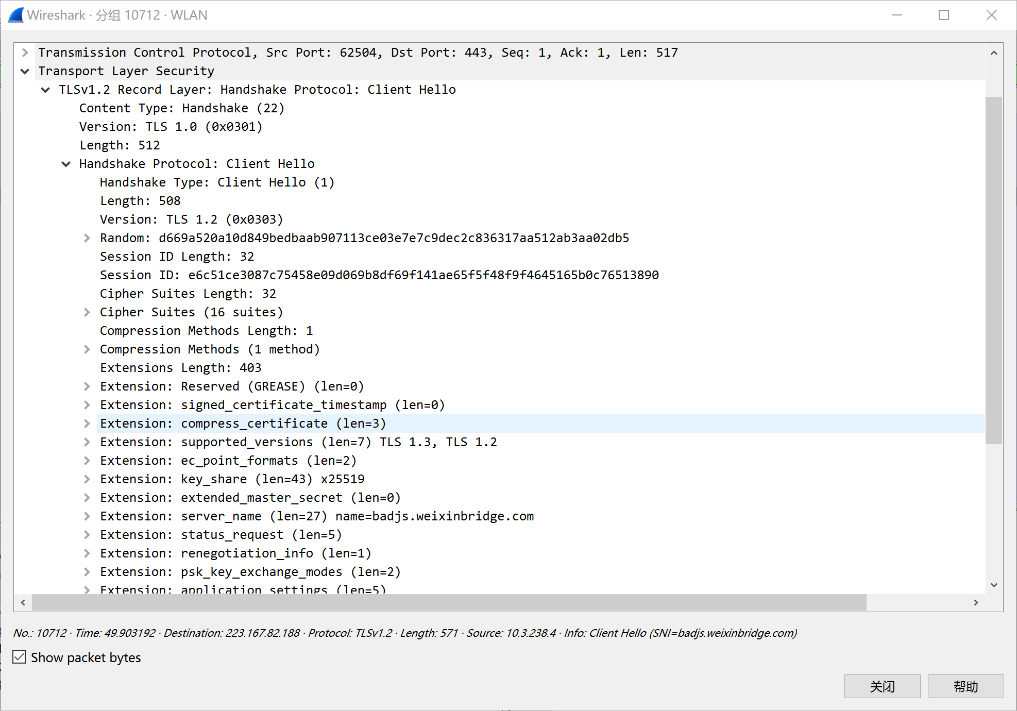
分析其中一帧：

图2-5-2 微信协议报文分析

客户端(浏览器)发送一个hello消息给服务端，发起建立SSL会话的请求。并告诉服务端，自己支持的协议版本和哪些加密算法(Cipher Suite List)。除此之外，还需要产生一个随机数random(第一个随机数，用于以后生成对称密钥)，发送给服务端。

TLSv1.2 Record Layer: Handshake Protocol: Client Hello，表明此包为TLS的第一个包。

Content Type: Handshake (22)，显示了本包的类型为Handshake (22)。

Version: TLS 1.0 (0x0301)，协议版本（客户端期望支持的握手协议版本)

Random: d669a520a10d849bedbaab907113ce03e7e7c9dec2c836317aa512ab3aa02db5，安全随机数

Session ID Length:32，这个值是被服务端设置的，如果这个值为空，表示客户端与服务端没有存活的https会话，需要与服务端进行完整的握手。如果这个值存在，则表明客户端期望恢复上一次的https 会话，这时候客户端与服务端只需要进行快速的握手过程。

Cipher Suites Length: 32

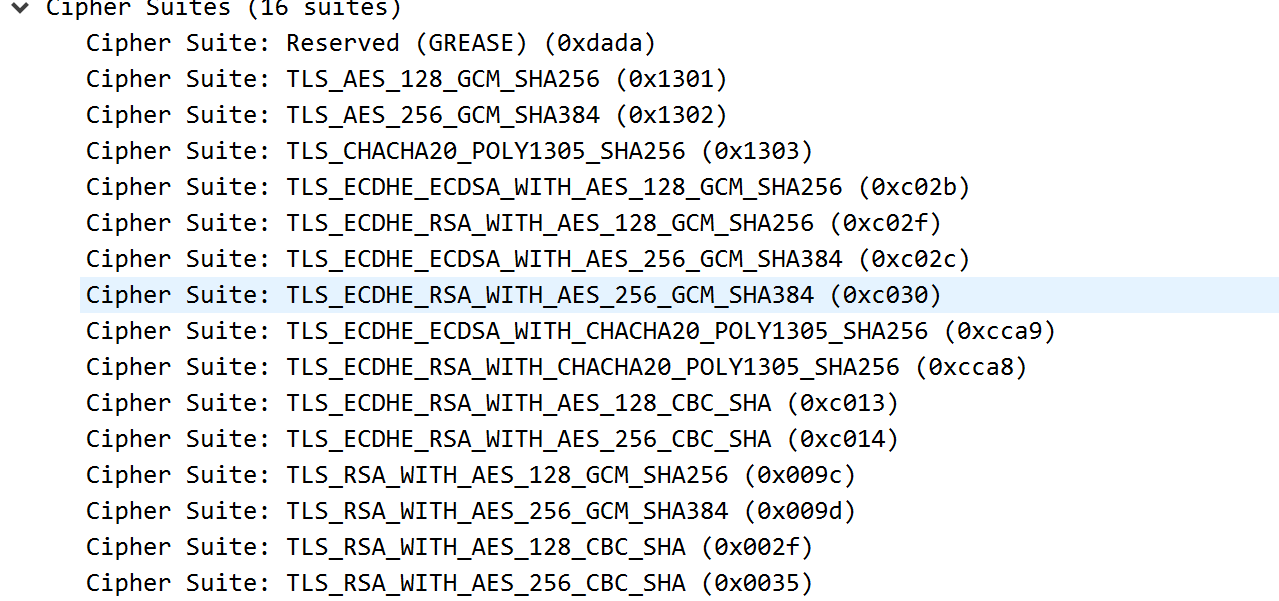
Cipher Suites (16 suites)，加密套件（客户端支持的加密套件列表)

图2-5-3 Cipher Suites详细信息

如果前面的Session ld 不为空，可以不传这个值，服务端可以从上一次会话中恢复这个值。

可以看到，客户端发送了16种可用密码套件给服务端，然后由服务端挑选自己支持的套件。

每个加密组件(Cipher Suite)都包括了下面5类算法:

(1) authentication (认证算法):RSA

(2) encryption(加密算法): AEAD\_AES\_256\_GCM

(3) message authentication code(消息认证码算法简称MAC): SHA384

(4) key exchange (密钥交换算法): ECDHE

(5) key derivation function(密钥衍生算法)

Compression Methods Length: 1

Compression Methods ( 1 method)

Compression Method: null (O)，加密前进行数据压缩

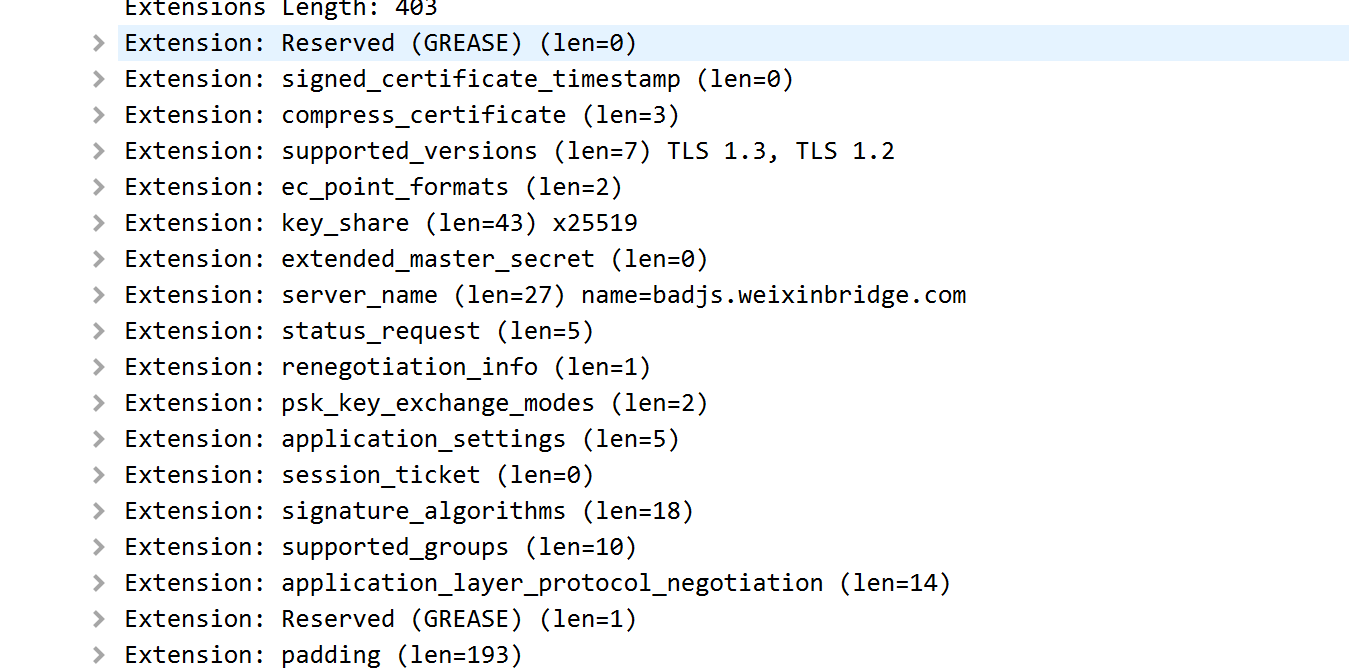
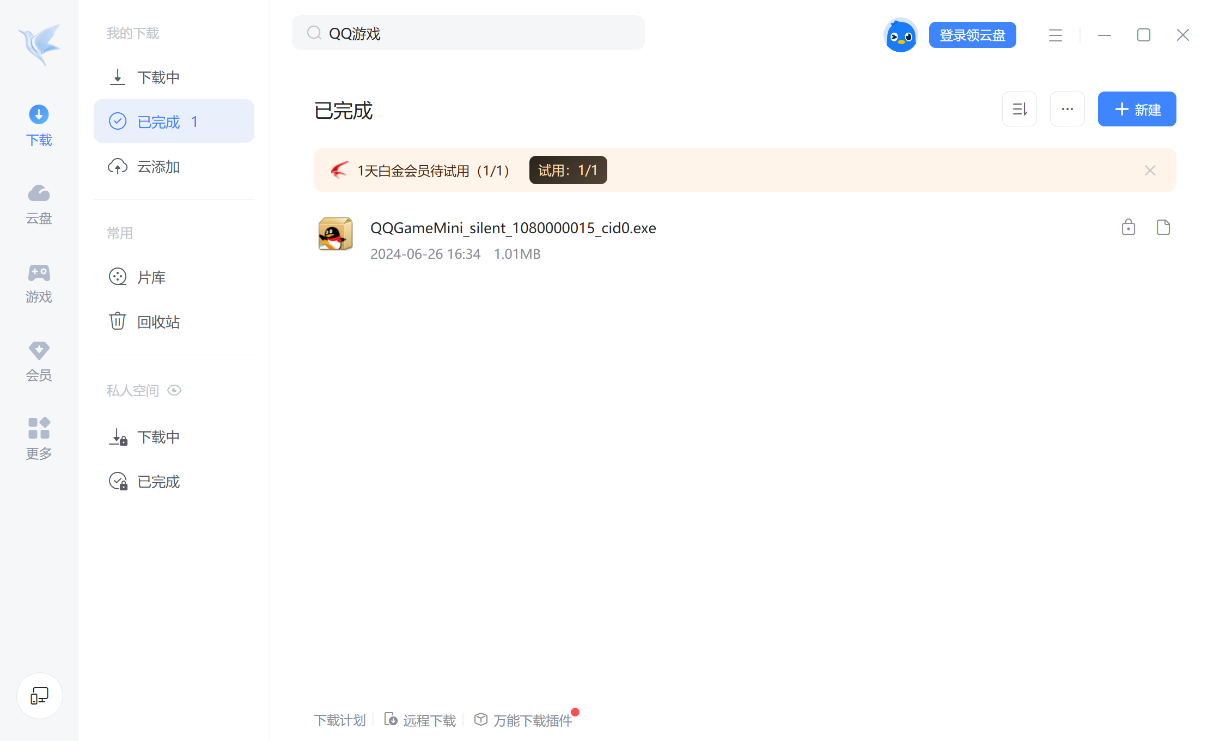
最后即为扩展，包括长度、服务器名称(support.weixin.qq.com)签名算法等信息。

图2-5-4 扩展信息

### 8.2.6 实验2.6：迅雷协议分析

下载迅雷软件，并用迅雷下载一个文件，本例使用QQGameMini\_silent\_1080000015\_cid0.exe

图2-6-1 迅雷下载文件

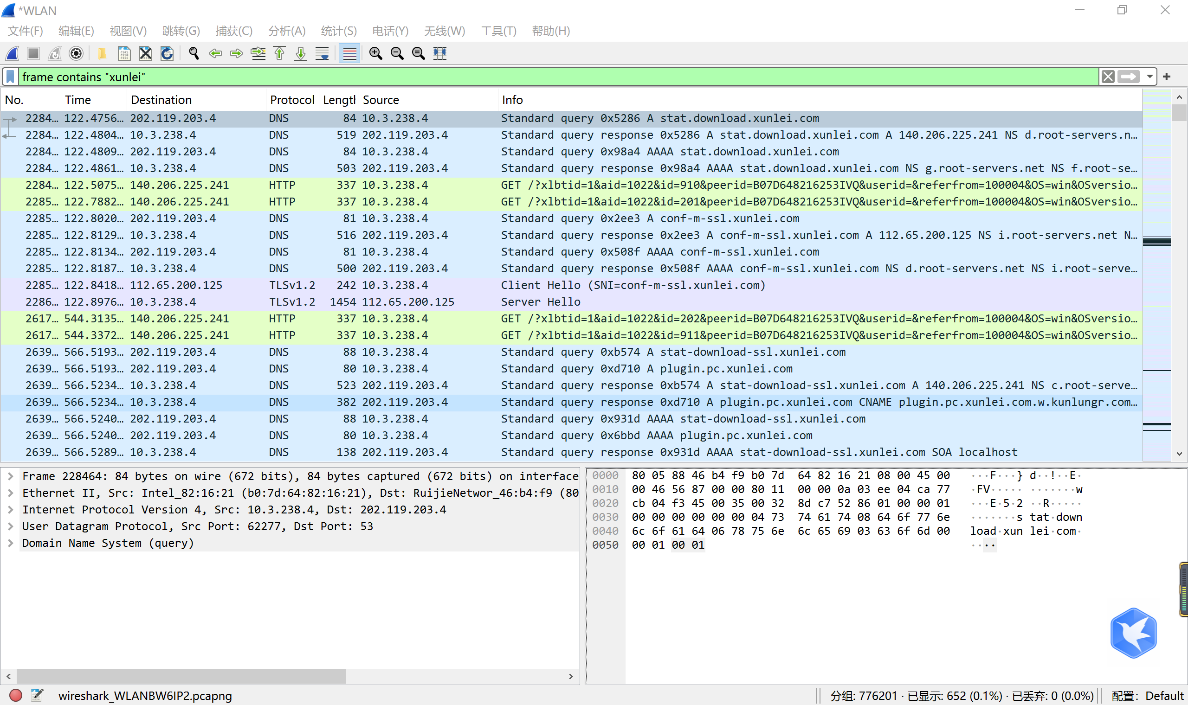
设置Wireshark的过滤器

图2-6-2 迅雷协议报文抓取

分析其中一帧，可以看到应用层为超文本传输协议。



图2-6-3 迅雷的应用层协议为HTTP

其中，

[Expert Info (Chat/Sequence): GET /VipDownloadConfig.json HTTP/1.1\r\n]

[GET /VipDownloadConfig.json HTTP/1.1\r\n]

[Severity level: Chat]

[Group: Sequence]

为前面已经分析过的GET方法,其中包括了下载文件名，HTTP版本(HTTP/1.1)，加密等级等信息。

Host: media.info.client.xunlei.com，指接受请求的服务器地址为media.info.client.xunlei.com。

具体内容在www 服务中已经分析过。

可以看出，迅雷下载时虽然使用简单的HTTP协议，但内容已经加密，只有少量信息可以通过Wireshark得到。

## 8.3 实验体会

经过本次应用层实验，我深刻体会到了网络应用中服务器配置和协议分析的重要性。实验过程中，我首先通过仿真软件PT成功搭建了包括DHCP、FTP、DNS、TFTP等常用网络应用服务的访问场景，并完成了相应的服务器配置。这不仅加深了我对C/S通信模式和常用应用层协议工作原理的理解，也让我掌握了典型应用服务器的配置方法。

在实验中，我使用Wireshark抓包工具对DNS、HTTP等应用层协议报文进行了捕获和分析。通过逐层分析报文的组成结构和字段含义，我更加清晰地理解了这些协议在网络通信中的实际作用和工作机制。特别是在分析FTP和TFTP服务器配置实例时，我感受到了这些协议在文件传输中的高效性和实用性。

此外，实验中的跨网段分配IP地址和APIPA机制等内容，也让我对网络地址分配和故障转移机制有了更深入的了解。这些知识点在实际网络应用中具有重要的应用价值，能够帮助我更好地解决网络问题。

总的来说，本次实验不仅让我掌握了应用层协议和网络服务配置的理论知识，还通过实际操作提高了我的实践能力。我深刻认识到，只有不断学习和实践，才能更好地掌握网络技术的精髓，为未来的学习和工作打下坚实的基础。

----------------------------------以下表格用于评阅，不得擅自修改、删除--------------------------------------------

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **报告内容** | **基础理论掌握程度** | **综合知**  **识应用**  **能力** | **报告**  **内容** | **报告**  **格式** | **完成**  **状况** | **工作量** | **学习、**  **工作**  **态度** | **抄袭**  **现象** | **其它** | **综合**  **成绩** |
| **8** | **应用层** | 请选择 | 请选择 | 请选择 | 请选择 | 请选择 | 请选择 | 请选择 | 学号:  姓名: | 目录、章节编目、错别字、乱码、截图、程序功能、程序源代码、源代码注释、体会、文献 |  |
| 批阅时间 | | 2024年5月22日 | | | | | | | | | |

----------------------------------以上表格用于评阅，不得擅自修改、删除--------------------------------------------