计算机网络LAB3

姓名：姚丁钰

班级：智能2103班

学号：202107030125

实验目的

通过本实验，熟悉PacketTracer的使用，学习在PacketTracer中仿真分析**应用层和传输层**协议，进一步加深对协议工作过程的理解。

实验内容

研究应用层和传输层协议

从 PC 使用 URL 捕获 Web 请求，运行模拟并捕获通信，研究捕获的通信。

Wireshark 可以捕获和显示通过网络接口进出其所在 PC 的所有网络通信。Packet Tracer 的模拟模式可以捕获流经整个网络的所有网络通信，但支持的协议数量有限。我们将使用一台 PC 直接连接到 Web 服务器网络，并捕获使用 URL 的网页请求。

任务1：从 PC 使用 URL 捕获 Web 请求。

步骤1. 运行模拟并捕获通信。 进入 Simulation（模拟）模式。单击 PC。在 Desktop（桌面）上打开 Web Browser（Web 浏览器）。在浏览器中访问服务器的web服务（服务器的IP地址请自己设置）。单击 Go（转到）将会发出 Web 服务器请求。最小化 Web 客户端配置窗口。Event List（事件列表）中将会显

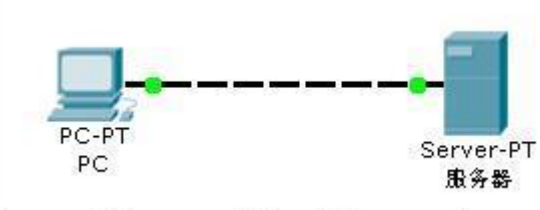
示两个数据包：将 URL 解析为服务器 IP 地址所需的 DNS 请求，以及将服务器 IP 地址解析为其硬件 MAC 地址所需的 ARP 请求。

单击 Auto Capture/Play（自动捕获/播放）按钮以运行模拟和捕获事件。收到 "No More Events"（没有更多事件）消息时单击 OK（确定）。

步骤2. 研究捕获的通信。 在 Event List（事件列表）中找到第一个数据包，然后单击 Info（信息）列中的彩色正方形。单击事件列表中数据包的 Info（信息）正方形时，将会打开 PDU Information（PDU 信息）窗口。此窗口将按 OSI 模型组织。在我们查看的第一个数据包中，注意 DNS 查询（第 7 层）封装在第 4 层的 UDP 数据段中，等等。如果单击这些层，将会显示设备（本例中为 PC）使用的算法。查看每一层发生的事件。

打开 PDU Information（PDU 信息）窗口时，默认显示 OSI Model（OSI 模型）视图。此时单击 Outbound PDU Details（出站 PDU 详细数据）选项卡。向下滚动到此窗口的底部，您将会看到 DNS 查询在 UDP 数据段中封装成数据，并且封装于 IP 数据包中。

查看 PDU 信息，了解交换中的其余事件。



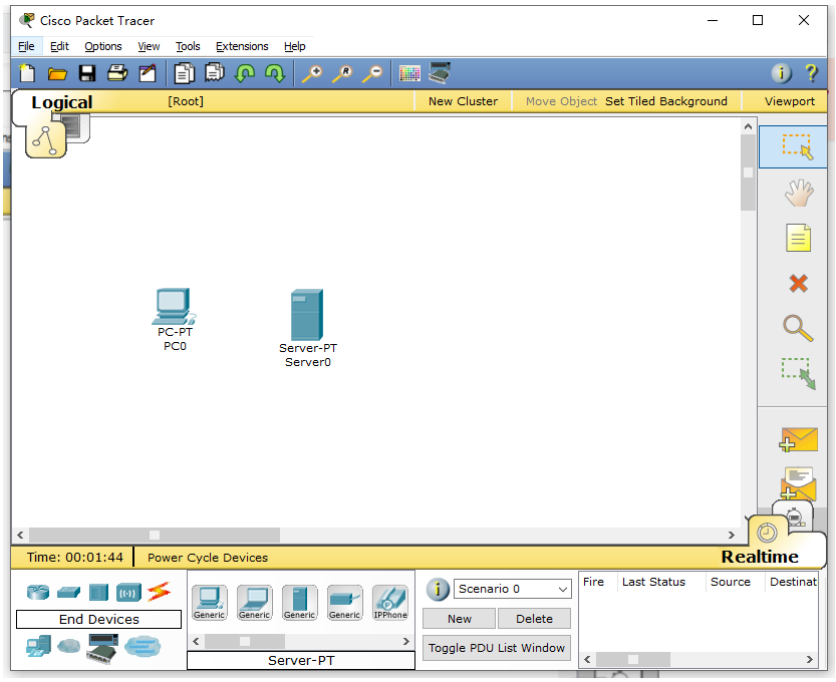
任务2：从 PC 访问服务器的HTTPS服务，捕获数据包并分析。

任务3：从 PC 访问服务器的FTP服务，捕获数据包并分析。

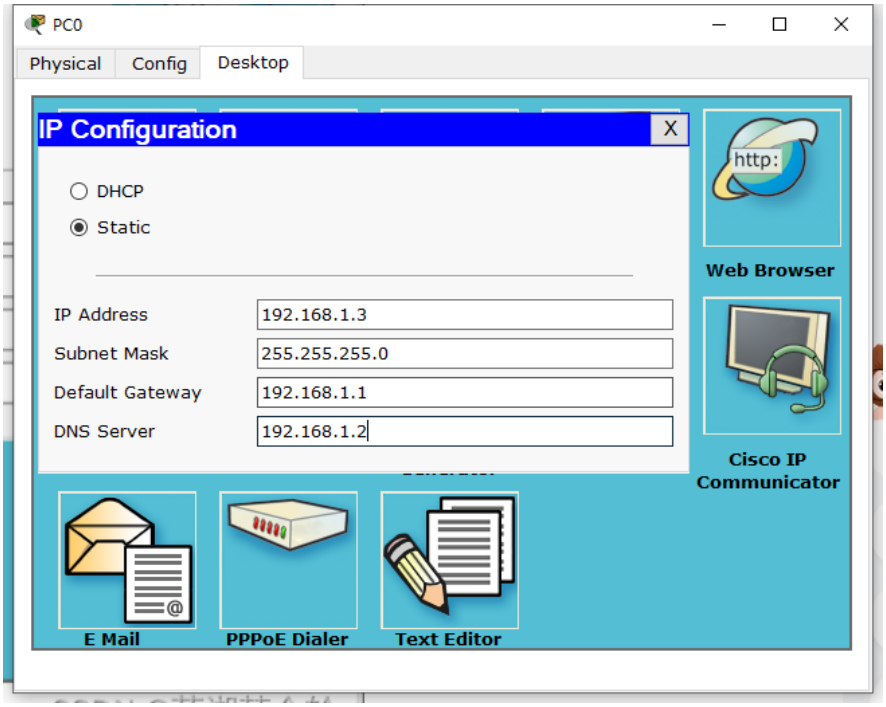
实验过程

任务一：从PC使用URL捕获Web请求

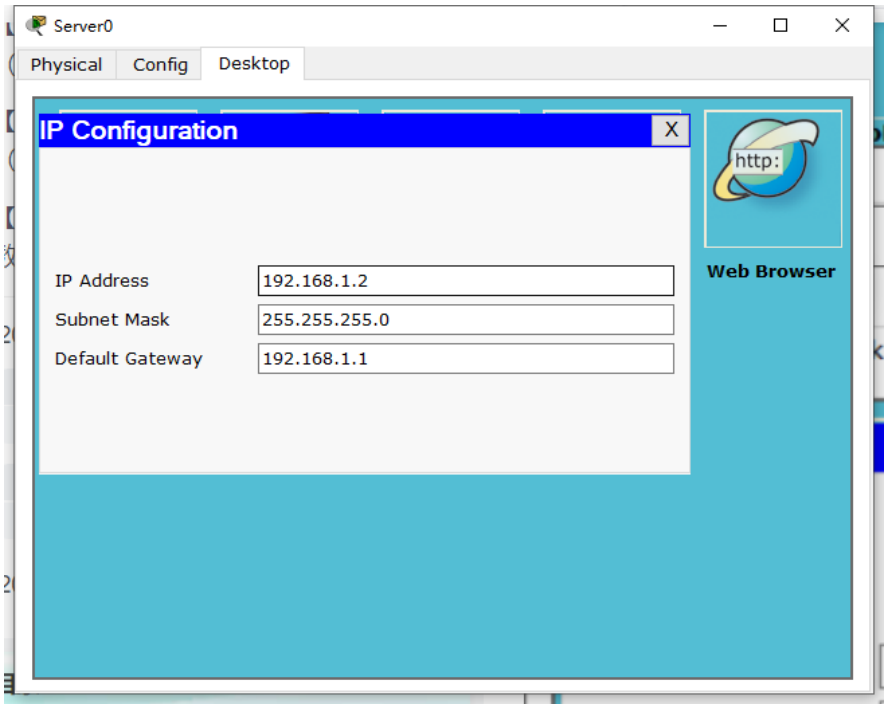
1. 新建拓扑图如下



2. 设置PC的IP配置，使用静态地址

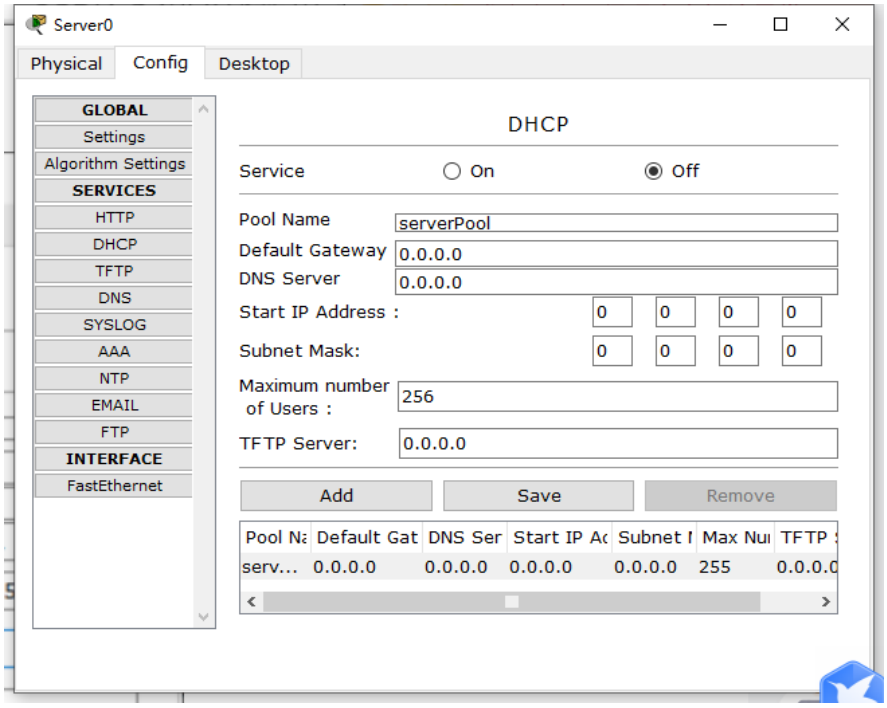


3. 设置Server的IP 配置



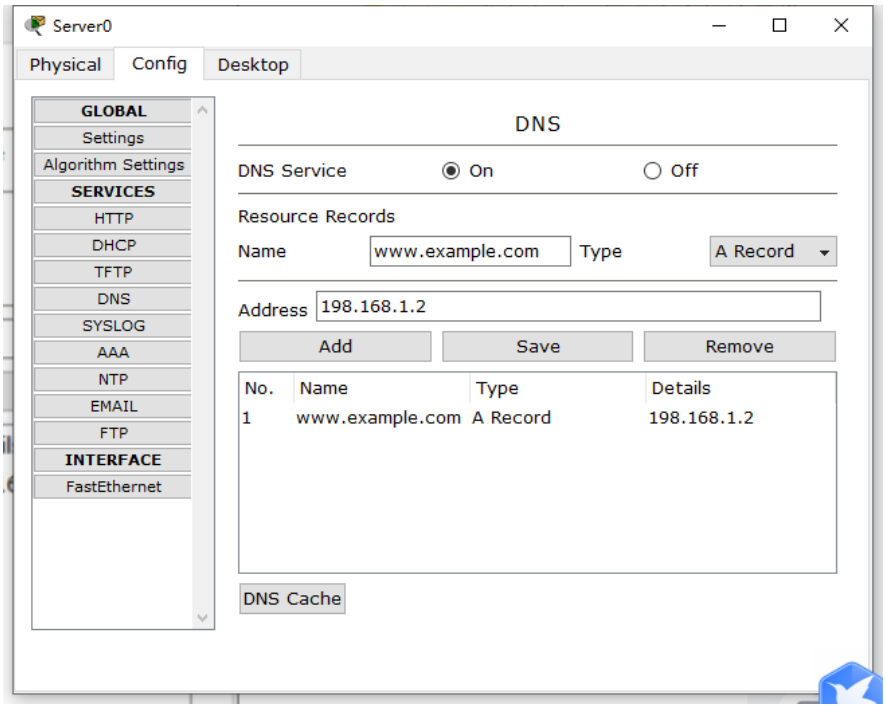
4. 配置DHCP

将Service设置为OFF，使用静态分配IP



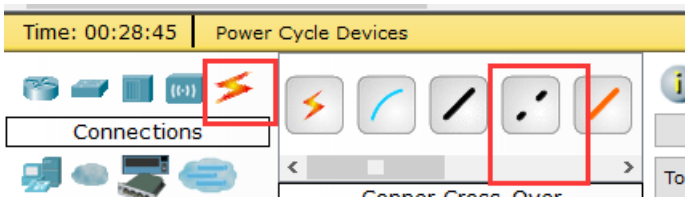
5. 配置DNS

增加解析域名www.example.com，填入Name中，设置IP为192.168.1.2

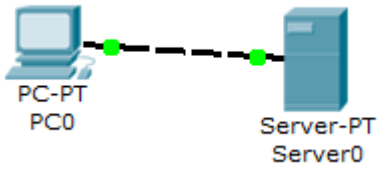


6. 用交叉线连接主机与服务器

在左下角中，点击闪电图标，出现多种连接线，点击虚线：

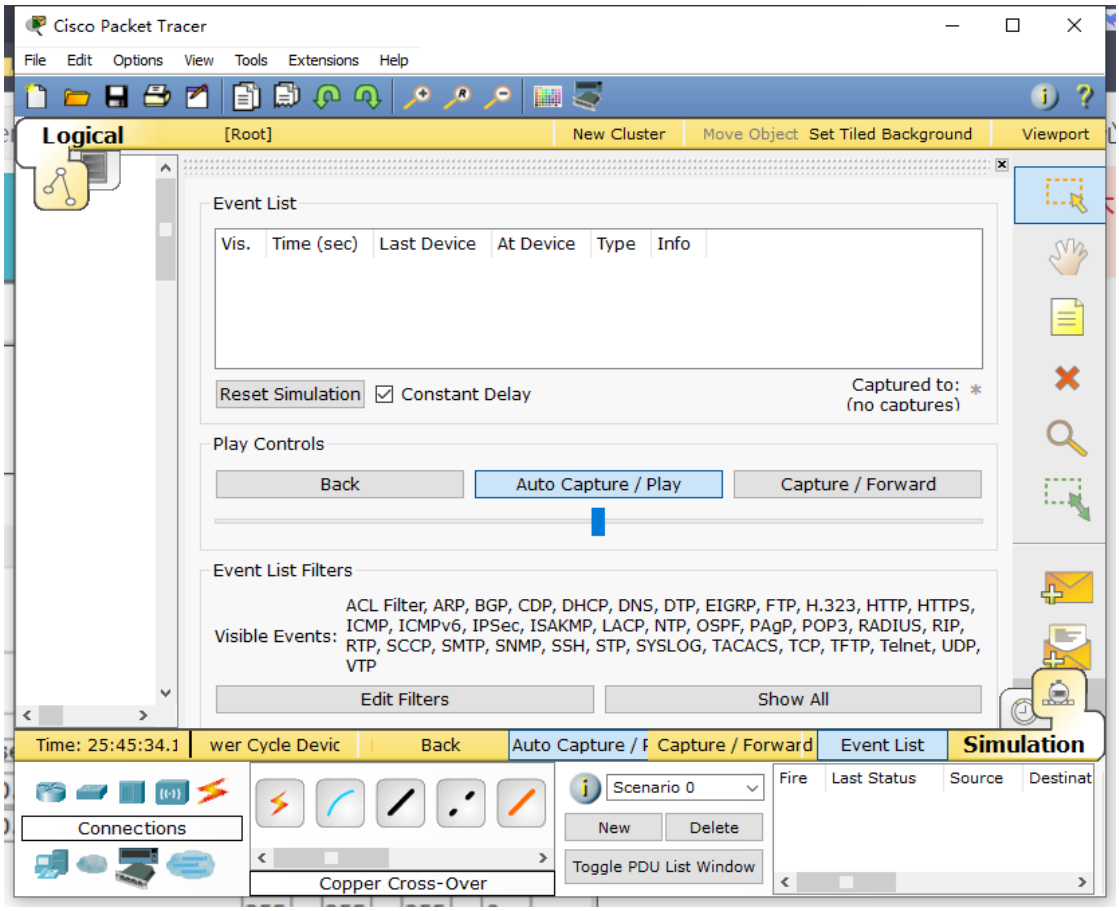


选择虚线（交叉线），然后点PC，出现两个选项，点击FastEthemet，再把线拖到server上，同样选择FastEthemet。连接后效果如下：

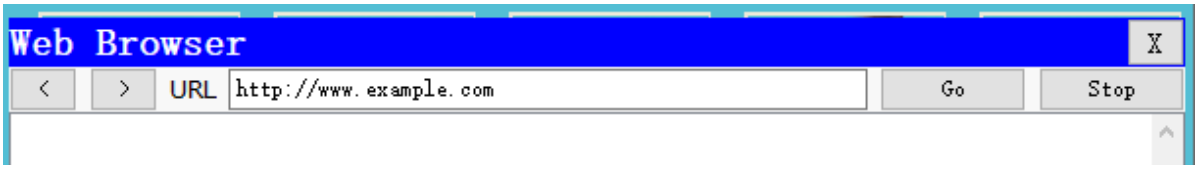


7. 打开模拟模式

点击右下角的simulation，切换模式。



8. 单击主机，进入web browser，输入url，即http://www.example.com，点击go，发出 Web 服务器请求。



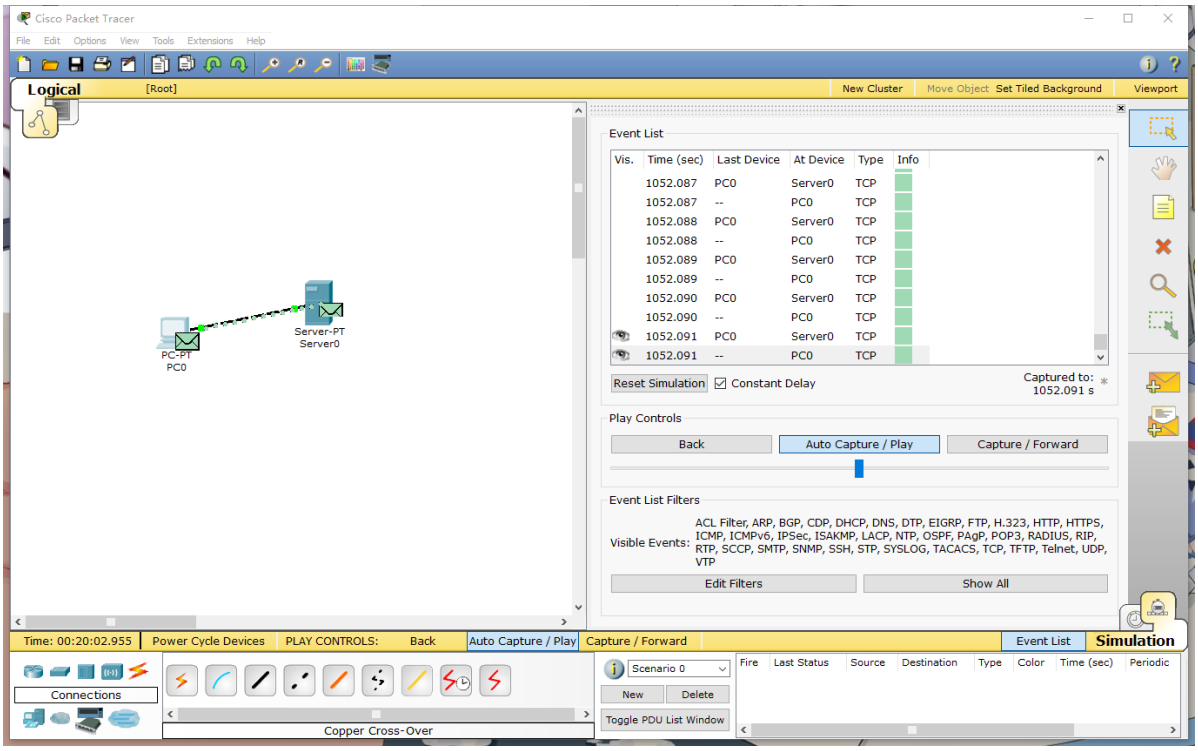
9. Event List 显示出刚抓的DNS包

Event List（事件列表）中将会显示两个数据包：

- 将 URL 解析为服务器 IP 地址所需的 DNS 请求
- 将服务器 IP 地址解析为其硬件 MAC 地址所需的 ARP 请求

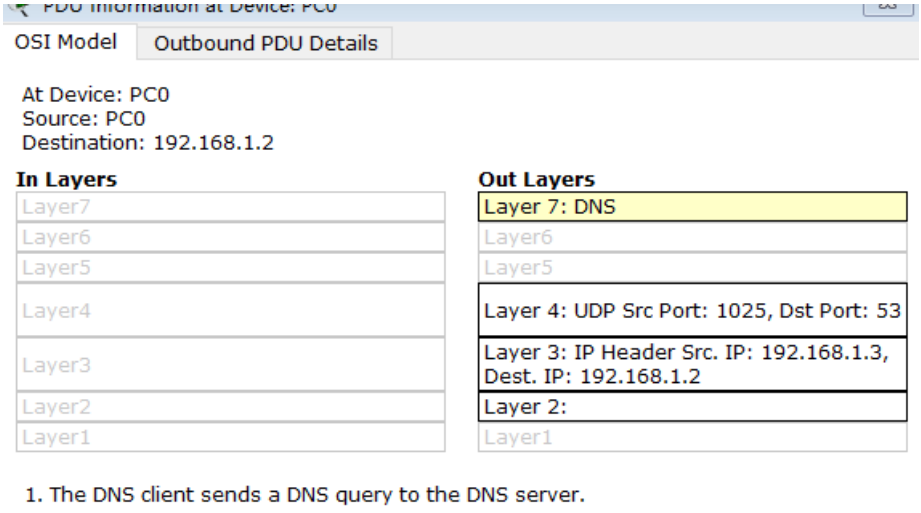
Time (sec)	Last Device	At Device	Type	Info
1052.061	--	PC0	DNS	
1052.061	--	PC0	ARP	

单击 Auto Capture/Play（自动捕获/播放）按钮自动模拟和捕获事件。在拓扑图中可以动态看到web请求的模拟过程（点击show all可以重新展示整个过程）



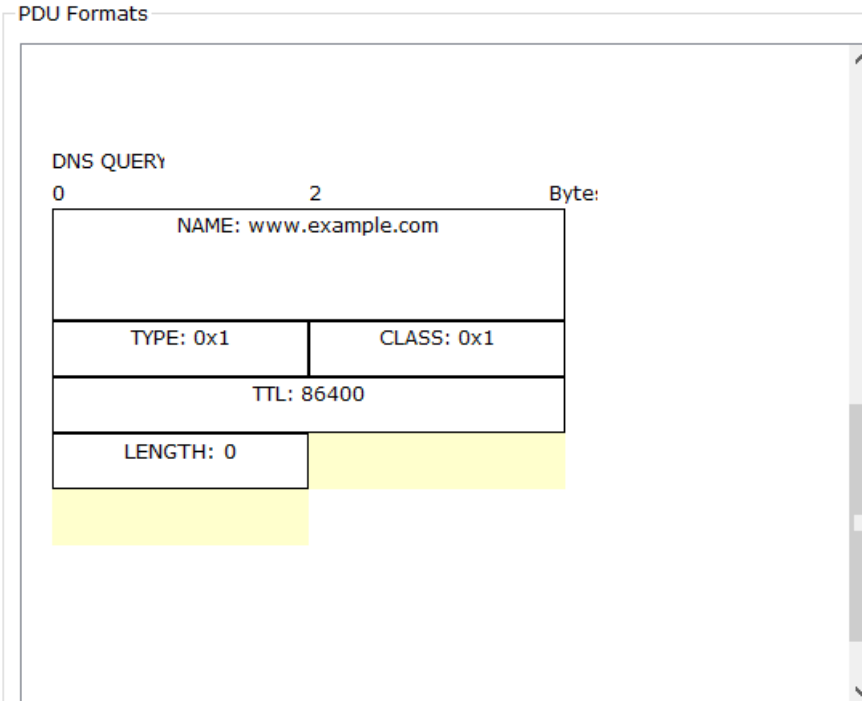
10. 点击第一个DNS数据包的右边正方形，查看PDU信息

打开 PDU Information（PDU 信息）窗口时，默认显示 OSI Model（OSI 模型）视图。此时单击 Outbound PDU Details（出站 PDU 详细数据）选项卡。向下滚动到此窗口的底部，您将会看到 DNS 查询在 UDP 数据段中封装成数据，并且封装于 IP 数据包中。
DNS 查询（第 7 层）封装在第 4 层的 UDP 数据段中。如果单击这些层，将会显示设备（本例中为 PC）使用的算法。

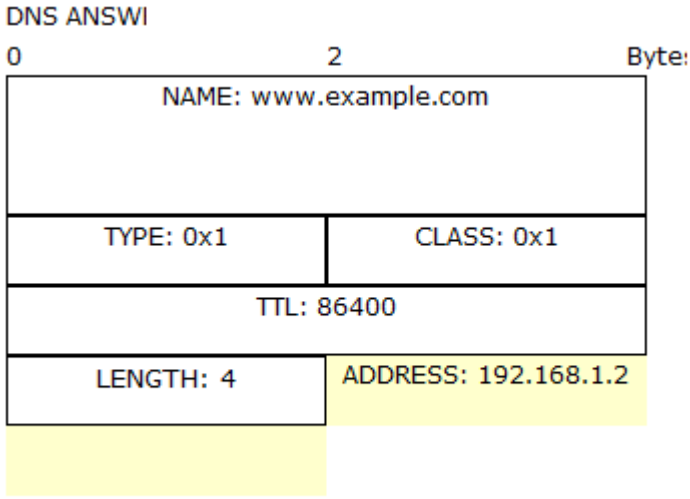


从上图中可以得知，DNS是建立在UDP的基础上的，与书上描述的一致。并且Destination指向的是之前自己设置的static server IP address。

单击 Outbound PDU Details（PDU 详细数据）选项卡。向下滚动到此窗口的底部，将会看到 DNS 查询在 UDP 数据段中封装成数据，并且封装于 IP 数据包中。查看 PDU 信息，了解交换中的其余事件。DNS QUERY可以看到请求的URL。



点击第二个DNS，可以看到返回了IP地址192.168.1.2

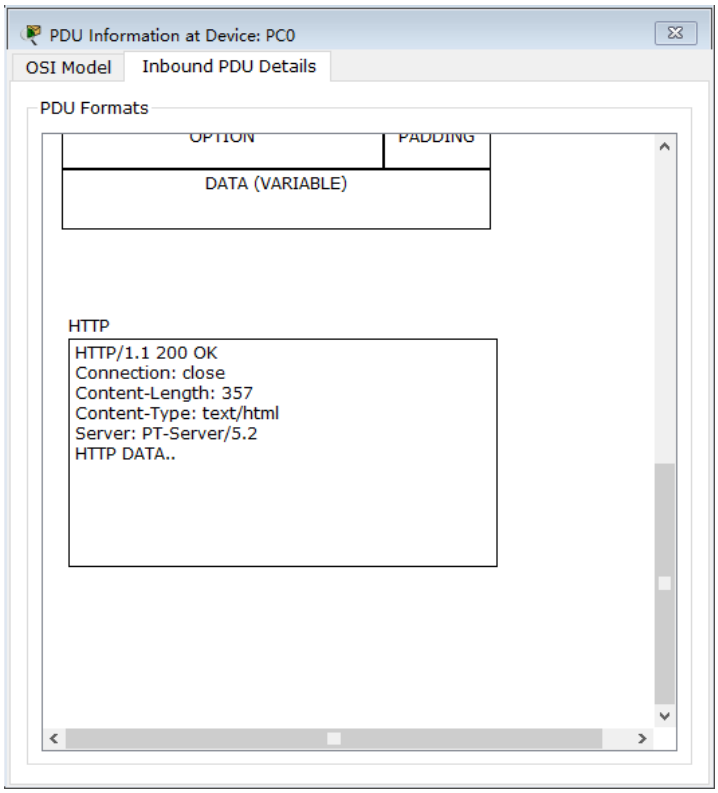


11. 对DNS协议的分析

首先根据www.example.com的URL地址，然后查询到了IP地址为192.168.1.1的目的地址，将 URL 解析为服务器 IP 地址所需的 DNS 请求，以及将服务器 IP 地址解析为其硬件 MAC 地址所需的 ARP 请求。

DNS报文类型	源站点	目的站点	报文信息
DNS请求信息	192.168.1.2	192.168.1.1	请求www.examplec.com的IP地址
DNS应答报文	192.168.1.1	192.168.1.2	对192.168.1.1请求的回复，将IP地址给它

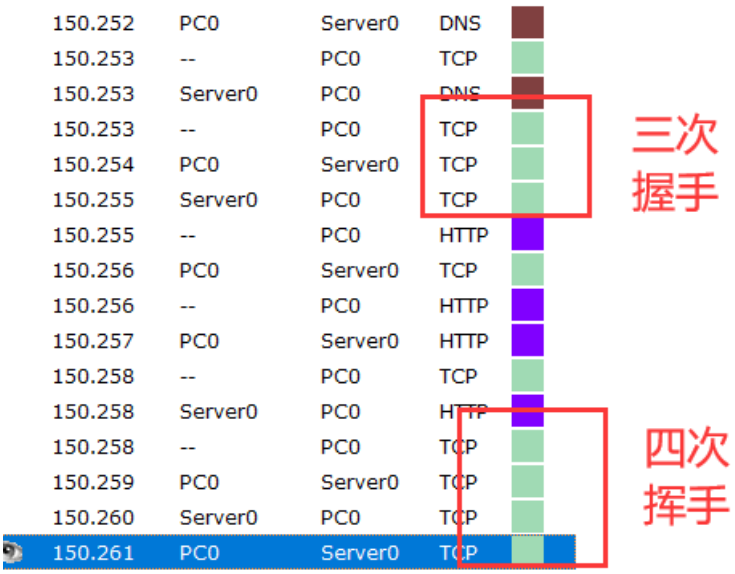
12. 查看http响应报文，分析HTTP协议和TCP协议：



在上图，我们可以清晰看到使用http协议，可以看到http协议的响应报文。

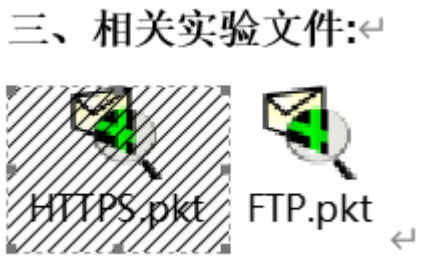
在HTTP响应报文里，可以看到200的状态码表示OK,请求的文件类型html(text/html)。连接的方式是非持续性连接。

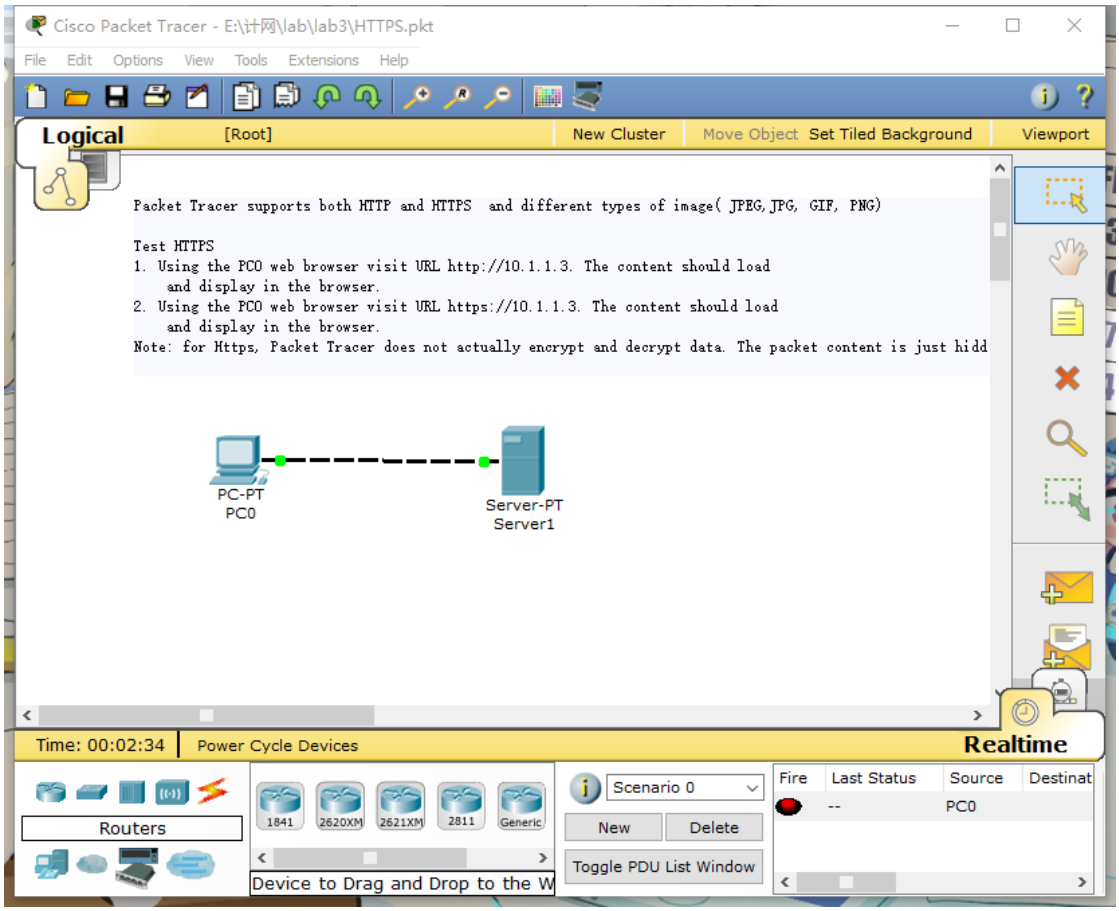
13. 其中在TCP协议中，在开始建立连接阶段，经历了3次握手；在断开连接阶段，经历了四次挥手。



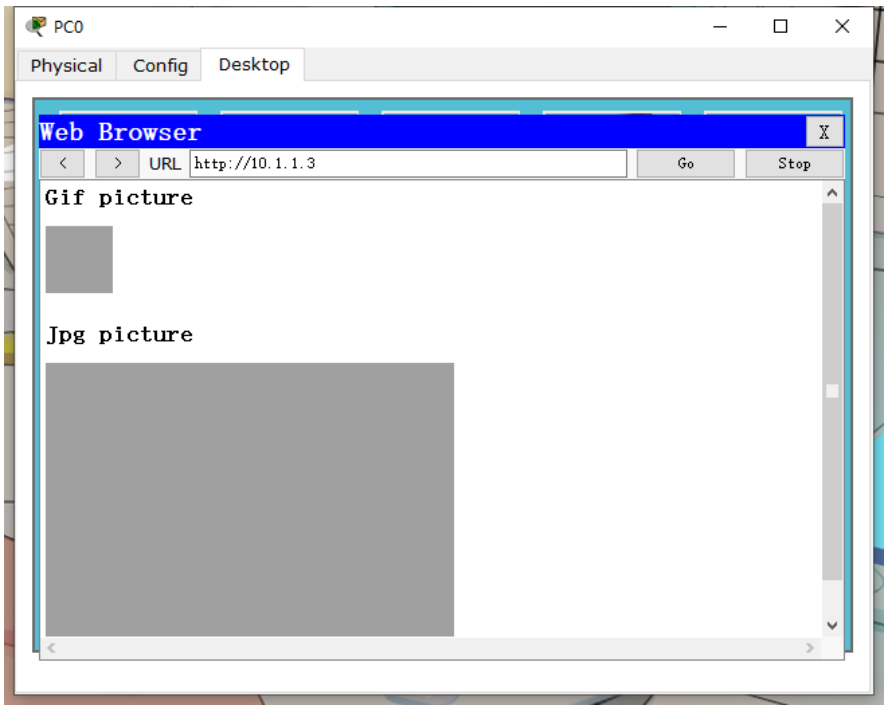
任务二：从 PC 访问服务器的HTTPS服务，捕获数据包并分析。

1. 打开实验pkt文件

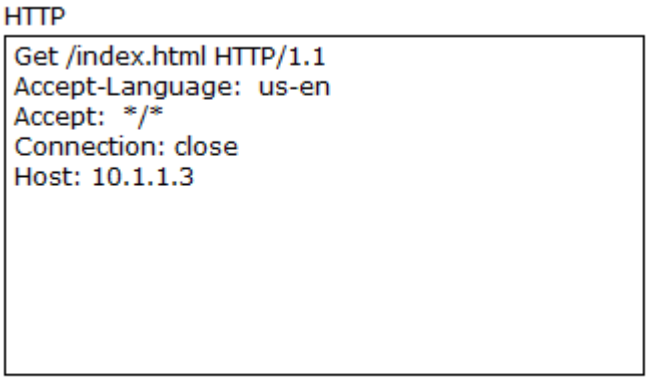




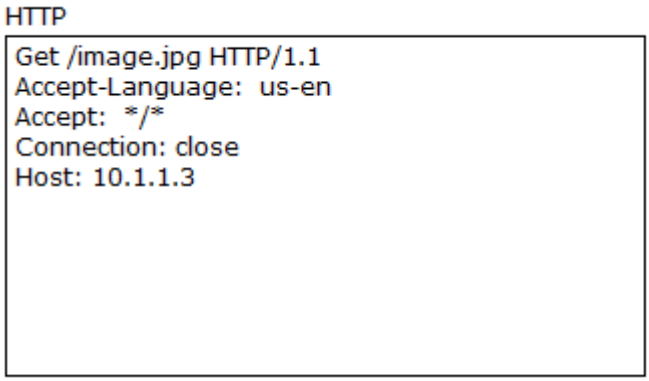
2. 进入simulation模式，使用auto capture捕获数据包，在PC访问http://10.1.1.3



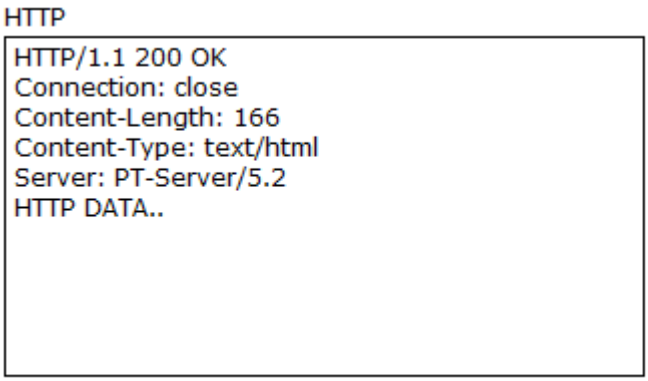
3. 在Event List中找到HTTP请求，查看PDU信息：可以看到第一个HTTP请求，请求的是默认的索引页。



再打开一个HTTP请求：可以看到请求的对象是一个图片。



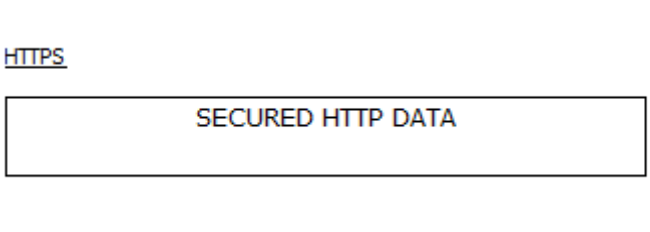
查看应答报文



以上两个HTTP请求，请求的方式都是GET，请求的对象不一样，但结果都是请求成功。

4. 重新访问URL为https://10.1.1.3 的IP地址

点击第一个HTTPS请求，查看其PDU信息：



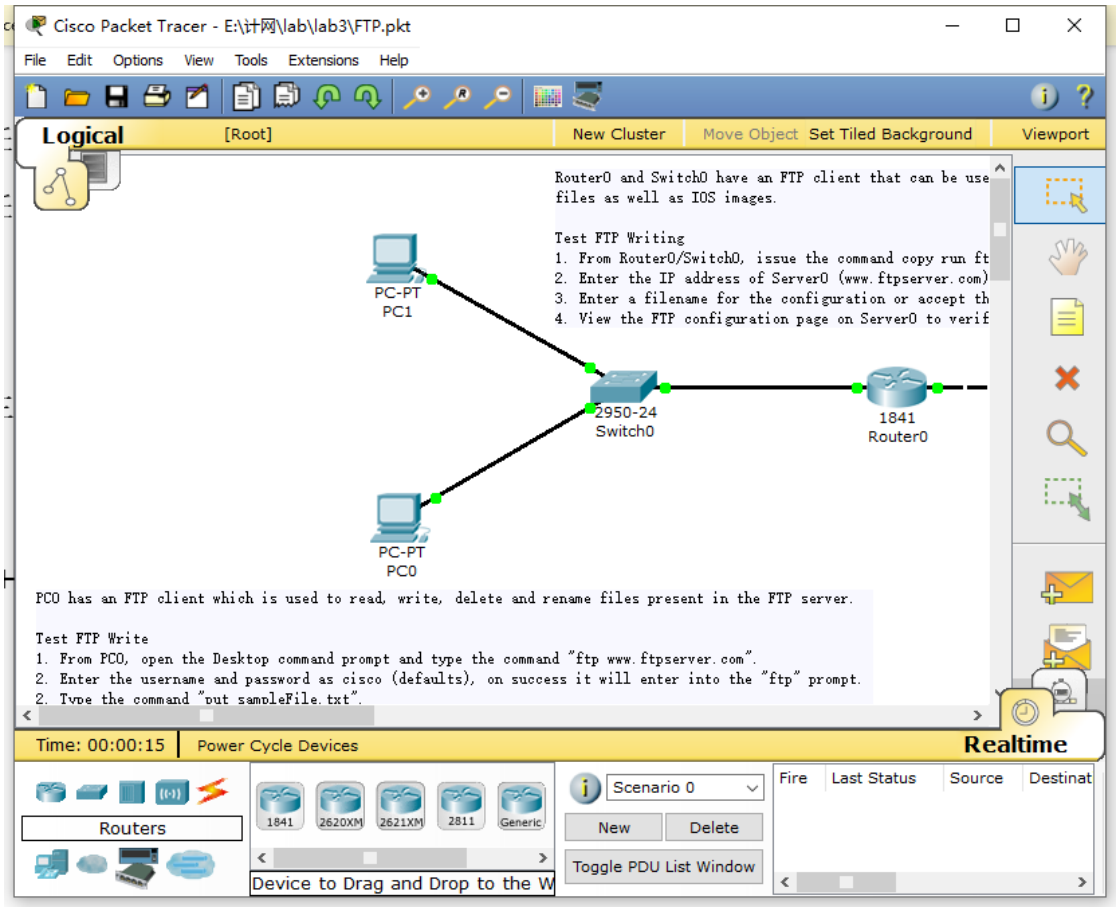
可以看到HTTPS的内容是不可看的。原因是HTTPS有如下特点：

1. 内容加密：采用混合加密技术，中间者无法直接查看明文内容
2. 验证身份：通过证书认证客户端访问的是自己的服务器
3. 保护数据完整性：防止传输的内容被中间人冒充或者篡改

总结：HTTP是超文本传输协议，信息通过明文传输，HTTPS则是具有安全性的ssl加密传输协议。因此总体来说，HTTPS更加安全

任务三：从 PC 访问服务器的FTP服务，捕获数据包并分析。

1. 打开实验pkt文件



2. 查看注释的实验要求

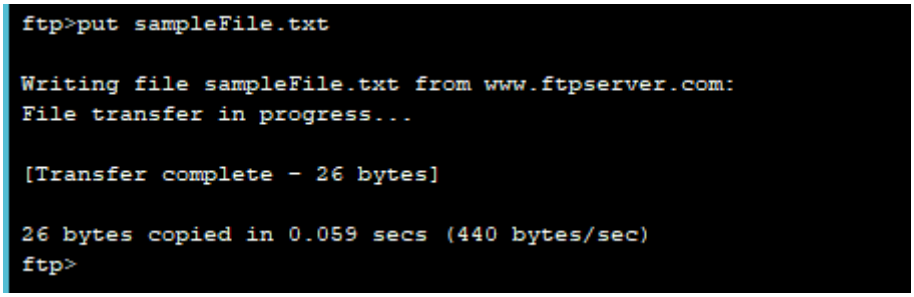
通过PC0测试FTP的写、读、查看删除文件列表、重命名、删除、退出。

```
PC0 has an FTP client which is used to read, write, delete and rename files present in the FTP server.

Test FTP Write
1. From PC0, open the Desktop command prompt and type the command "ftp www.ftpserver.com".
2. Enter the username and password as cisco (defaults), on success it will enter into the "ftp" prompt.
2. Type the command "put sampleFile.txt".
3. From Server0, open the FTP configuration page and view the file "sampleFile.txt" uploaded.

Test FTP Read and Directory listing
1. In the ftp prompt, type "get <remote filename>", make sure <remote filename> exists on the FTP server
2. Type "quit" command to exit from from the ftp prompt.
3. Type "dir" to view the file <remote filename> that was downloaded.

Test FTP Remote Directory listing
    In the ftp prompt, type "dir" to view the files in remote FTP server directory.

Test FTP Rename
1. In the ftp prompt, type "rename <old remote filename> <new remote filename>".
2. If renamed succesfully then type "dir" to view the change.

Test FTP Delete
1. In the ftp prompt, type "delete <filename>" to delete a file from the remote FTP server.
2. If deleted succesfully then type "dir" to view the change.

Test FTP Quit
    In the ftp prompt, type "quit" to exit from the ftp prompt and return to the previous prompt.
```

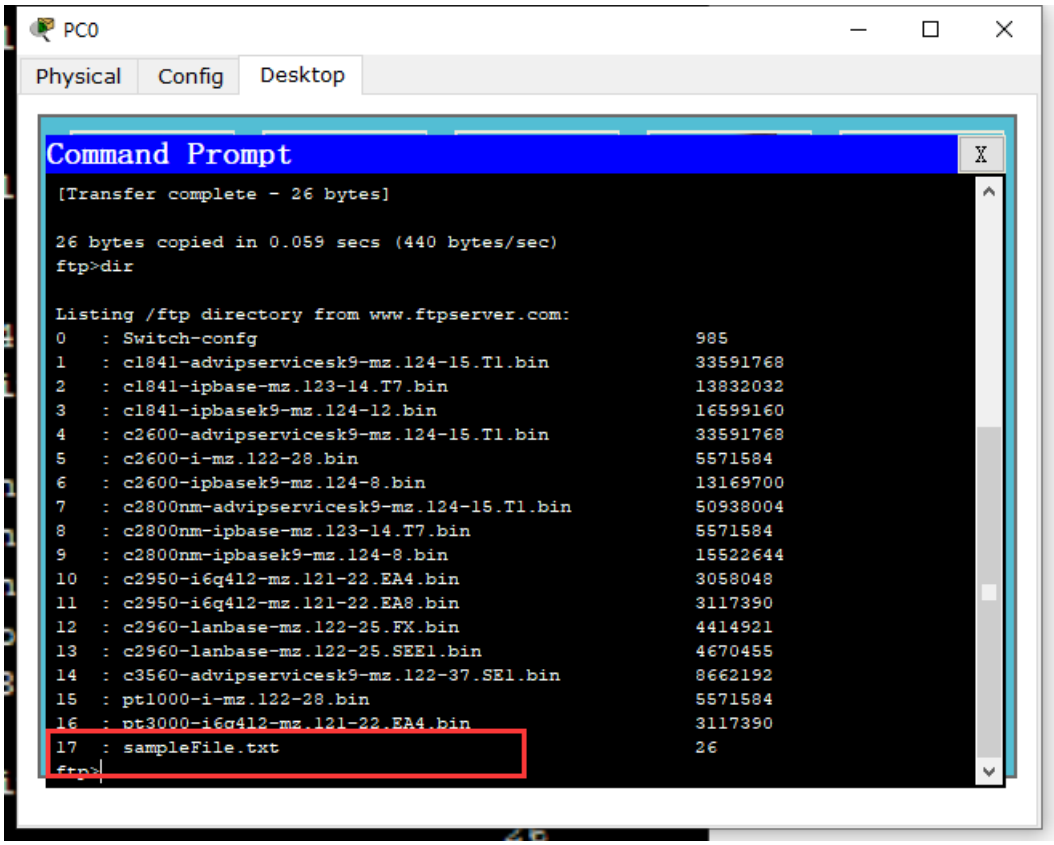
3. 写操作

- 按照指导，点击PC0，打开command prompt。
- 首先连接FTP服务器，输入：ftp www.ftpserver.com。
- 然后输入用户名：cisco，密码：cisco，进入FTP prompt界面 。

- 把文件上传到服务器：put sampleFile.txt

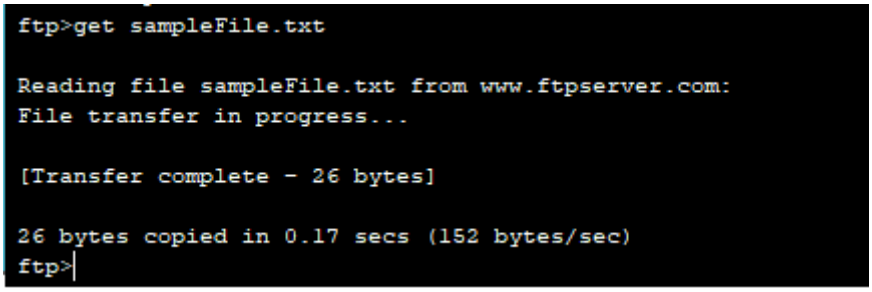


- 通过dir命令可以列出目前server的文件列表，可以看到此时已经上传。



4. 读操作

读取一个文件内容：ftp> get sampleFile.txt



5. 获取文件列表

在command prompt里面输入 dir,可以看到服务器中所有文件的文件列表，包括刚刚上传的sampleFile.txt

```
ftp>dir

Listing /ftp directory from www.ftpserver.com:
0    : Switch-confg                                985
1    : c1841-advipservicesk9-mz.124-15.T1.bin      33591768
2    : c1841-ipbase-mz.123-14.T7.bin               13832032
3    : c1841-ipbasek9-mz.124-12.bin                16599160
4    : c2600-advipservicesk9-mz.124-15.T1.bin      33591768
5    : c2600-i-mz.122-28.bin                       5571584
6    : c2600-ipbasek9-mz.124-8.bin                 13169700
7    : c2800nm-advipservicesk9-mz.124-15.T1.bin    50938004
8    : c2800nm-ipbase-mz.123-14.T7.bin             5571584
9    : c2800nm-ipbasek9-mz.124-8.bin               15522644
10   : c2950-i6q4l2-mz.121-22.EA4.bin              3058048
11   : c2950-i6q4l2-mz.121-22.EA8.bin              3117390
12   : c2960-lanbase-mz.122-25.FX.bin              4414921
13   : c2960-lanbase-mz.122-25.SEE1.bin            4670455
14   : c3560-advipservicesk9-mz.122-37.SE1.bin     8662192
15   : pt1000-i-mz.122-28.bin                      5571584
16   : pt3000-i6q4l2-mz.121-22.EA4.bin             3117390
17   : sampleFile.txt                              26
ftp>
```

6. 重命名

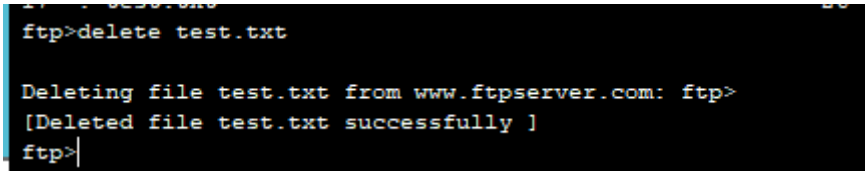
在FTP prompt输入：rename sampleFile.txt test.txt，将sampleFile.txt文件重命名为：test.txt。此时，再输入dir查看文件目录，可以发现更改后的文件。

```
ftp>rename sampleFile.txt test.txt

Renaming sampleFile.txt
ftp>
[OK Renamed file successfully from sampleFile.txt to test.txt]
ftp>
```

```
ftp>dir

Listing /ftp directory from www.ftpserver.com:
0    : Switch-confg                                985
1    : c1841-advipservicesk9-mz.124-15.T1.bin      33591768
2    : c1841-ipbase-mz.123-14.T7.bin               13832032
3    : c1841-ipbasek9-mz.124-12.bin                16599160
4    : c2600-advipservicesk9-mz.124-15.T1.bin      33591768
5    : c2600-i-mz.122-28.bin                       5571584
6    : c2600-ipbasek9-mz.124-8.bin                 13169700
7    : c2800nm-advipservicesk9-mz.124-15.T1.bin    50938004
8    : c2800nm-ipbase-mz.123-14.T7.bin             5571584
9    : c2800nm-ipbasek9-mz.124-8.bin               15522644
10   : c2950-i6q4l2-mz.121-22.EA4.bin              3058048
11   : c2950-i6q4l2-mz.121-22.EA8.bin              3117390
12   : c2960-lanbase-mz.122-25.FX.bin              4414921
13   : c2960-lanbase-mz.122-25.SEE1.bin            4670455
14   : c3560-advipservicesk9-mz.122-37.SE1.bin     8662192
15   : pt1000-i-mz.122-28.bin                      5571584
16   : pt3000-i6q4l2-mz.121-22.EA4.bin             3117390
17   : test.txt                                    26
ftp>
```

7. 删除

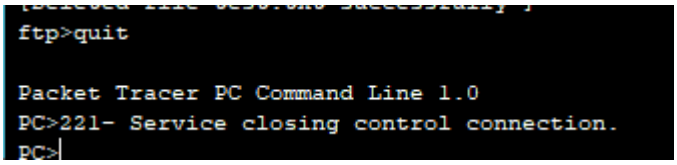
测试删除功能，在FTP prompt输入：delete test.txt



显示删除成功。

8. 退出FTP

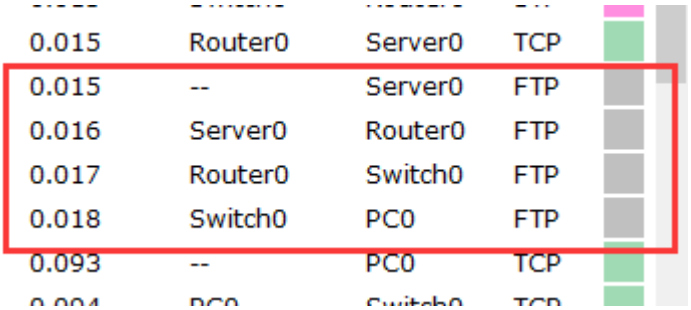
输入quit退出ftp



成功退出FTP，回到PC界面。

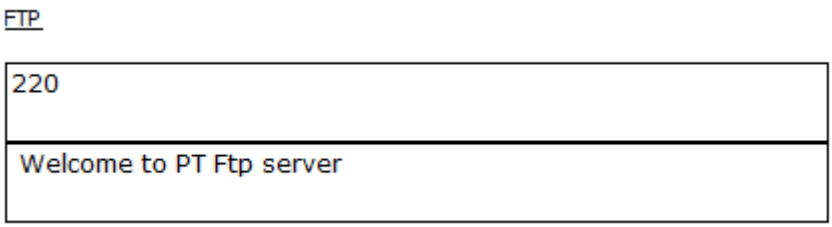
9. 分析FTP数据包

在我们输入“FTP www.ftpserver.com”之后，服务器会提示需要输入用户名，此时会返回一个欢迎用户的信息，如图，是四个连续的FTP，路径为：Server0—>Router0—>Switch0—>PC0。

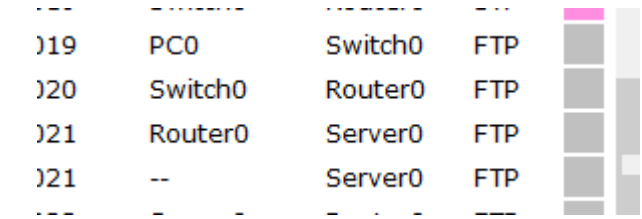


所以完整一次传输过程包含四个FTP。

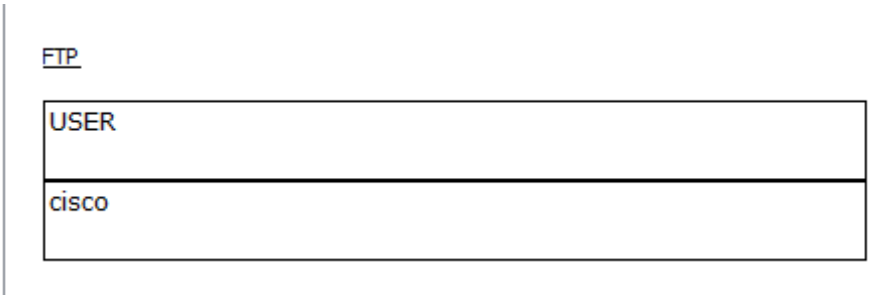
查看里面的内容，发现四个FTP内容是一样的，均为这一条欢迎用户的信息：



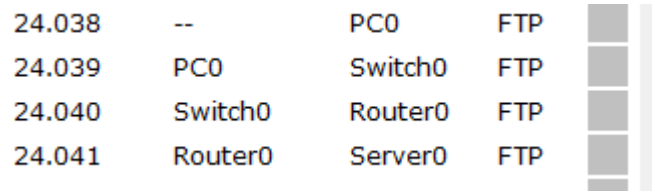
在这之后，命令提示符里面提示要输入用户名，输入“cisco”，又可以观察到连续的四个FTP，路径为PC0—>Switch0—>Router0—>Server0。

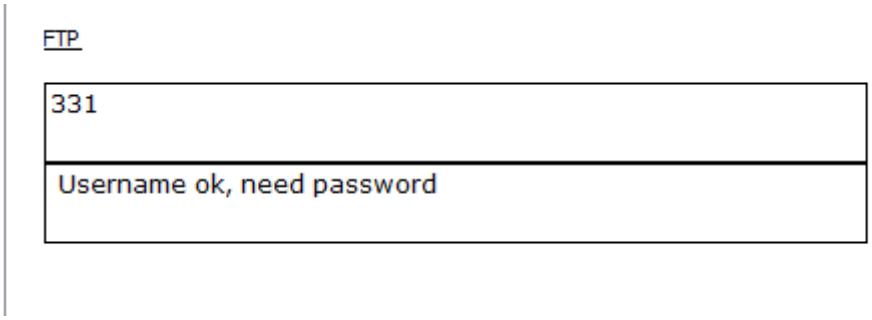


查看里面的内容，发现也是一样的，均为这一条信息，将用户输入的用户名传送给服务器



之后服务器则会继续传回给PC，提示用户需要输入密码

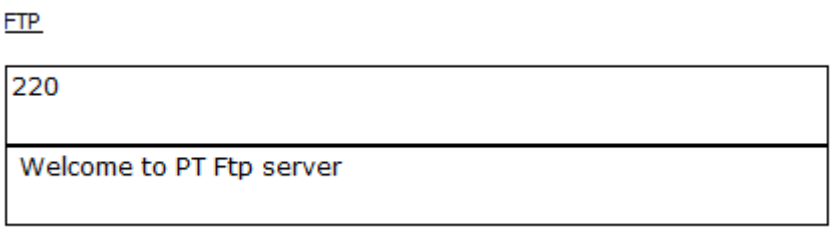




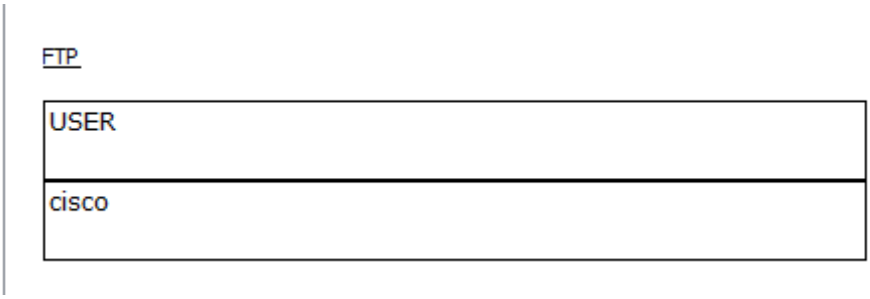
连接并登陆FTP服务器的整个过程如下：

1. 首先PC0输入ftp www.ftpserver.com发起连接；收到服务器回复后；
2. 紧接着输入账号:PC0发出一个包含账号的FTP数据包
3. 然后服务器收到后，发出一个账号已收到，需要密码的ftp包
4. 收到后，PC0再发出包含密码的FTP数据包
5. 服务器回复包含登陆成功的FTP数据包

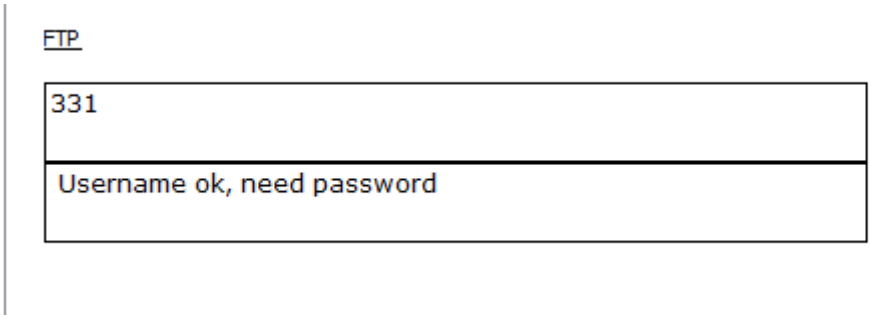
第一次FTP响应：



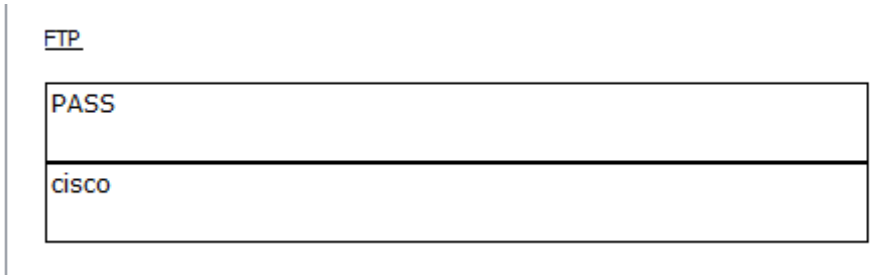
第二次FTP请求：



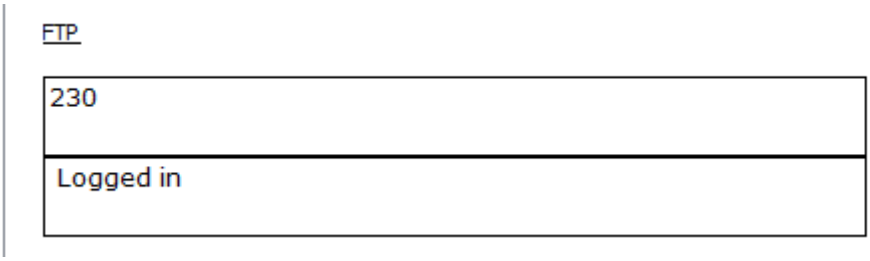
第二次FTP响应：



第三次FTP请求：



第三次FTP响应：



得到了FTP传输的路径情况。在该实验的拓扑图下，从客户机到服务器传输为PC——Switch——Router——Server；从服务器到客户机应答为Server——Router——Switch——PC，且均为连续的四个FTP包。其余过程包括FTP文件传输等等过程类似。

实验总结

通过本次实验学习与熟悉了Packet Tracer的使用，以及使用Packet Tracer进行协议分析的基本方法和过程。通过对HTTP以及FTP请求过程的数据包分析，更加深入了解了这两个应用层协议的工作过程，以及底层的协议的数据包如何传输并支持应用层的协议。