湖南大學

HUNAN UNIVERSITY

课程实验报告

课　程 名 称：计算机网络

实验项目名称：

专　业 班 级：计科 1902

姓　　名：樊一鸣

学　　号：2019028010212

指　导 教 师：罗辉章

信息科学与工程学院

一、实验题目

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。

二、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。

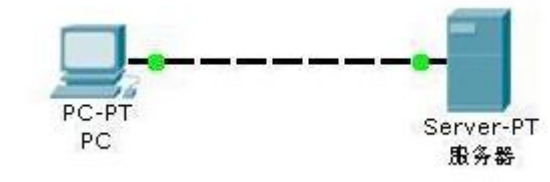
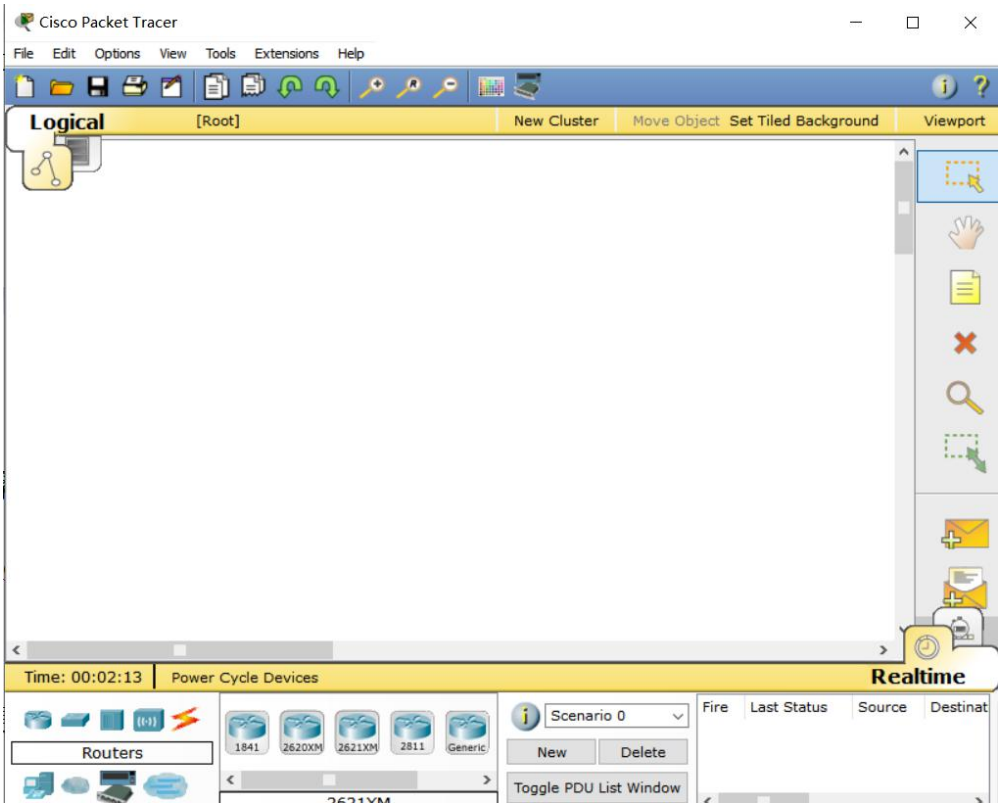


图 3.1 捕获 Web 请求

任务 2：从 PC 访问服务器的 HTTPS 服务，捕获数据包并分析。

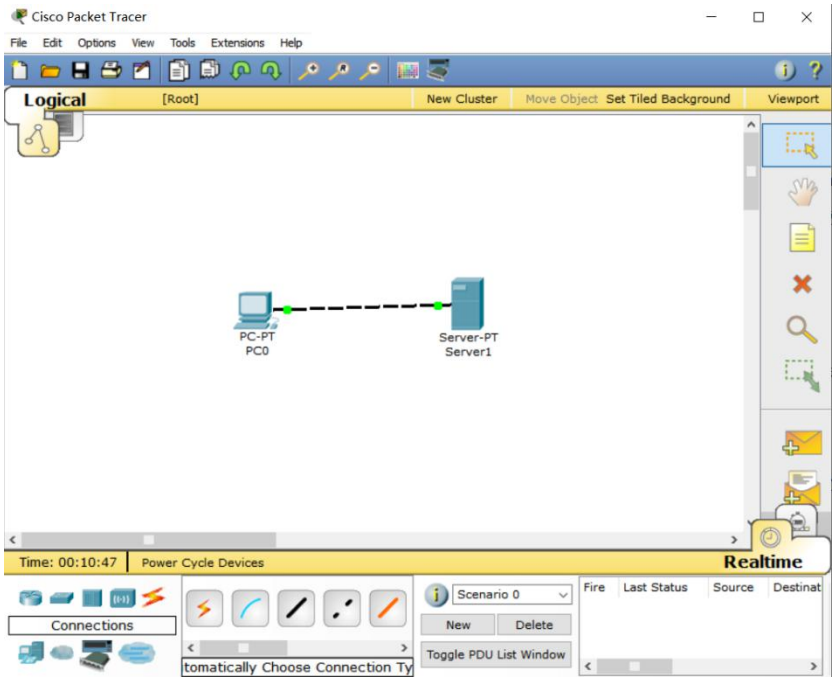
三、实验步骤

（一）下载 PacketTracer，我使用的是 5.3 的版本

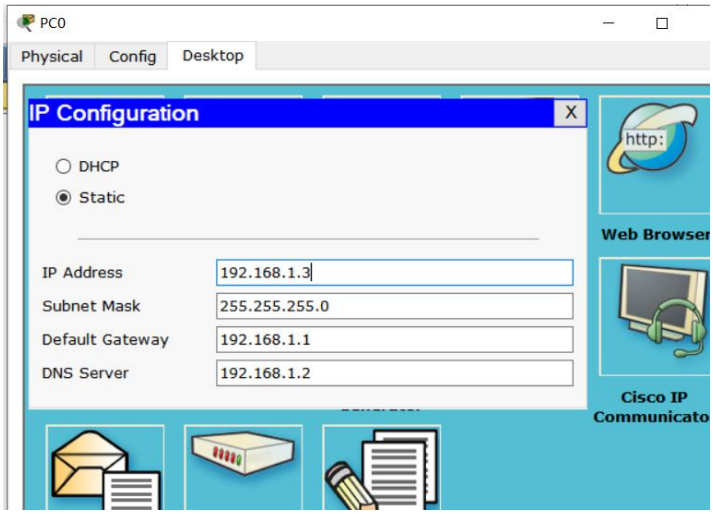


（二）任务 1：从 PC 使用 URL 捕获 Web 请求。

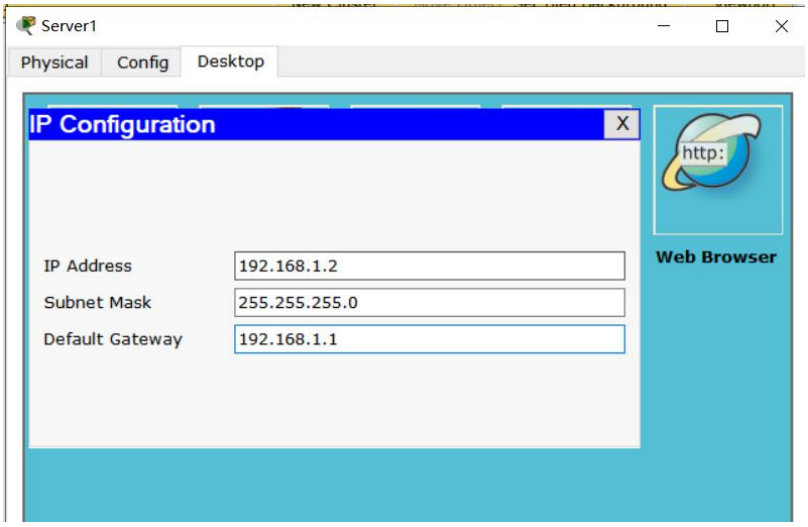
首先建立如下拓扑结构，添加一个主机和一个服务器



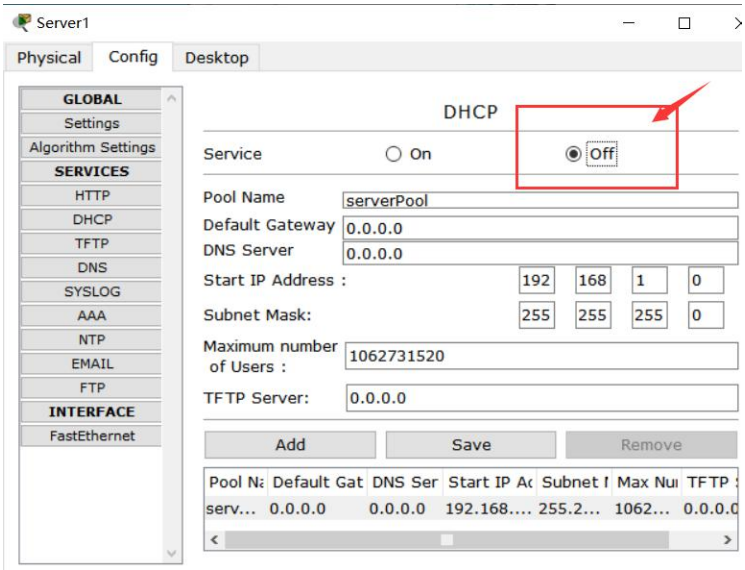
然后设置相关的参数，主机的 IP 设置如下



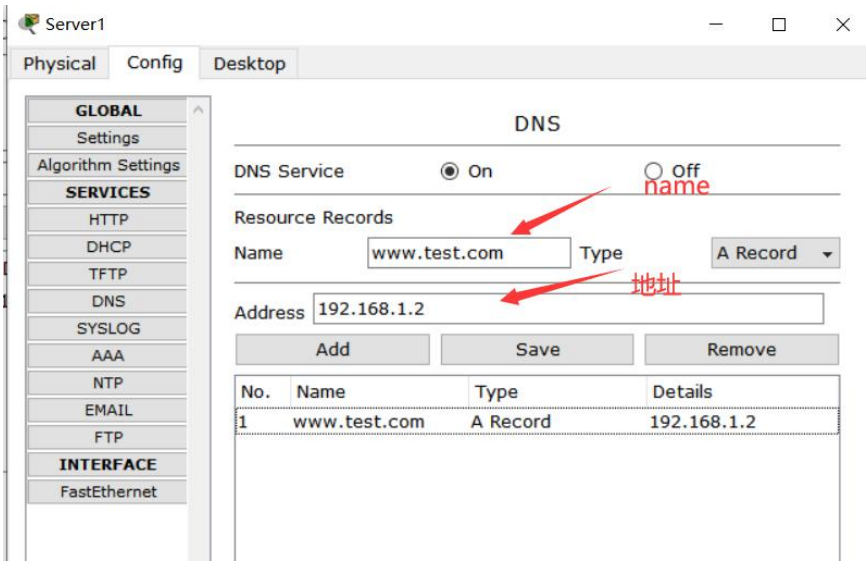
服务器 IP 设置如下



配置 DHCP,将 Service 设置为 OFF，使用静态分配 IP:

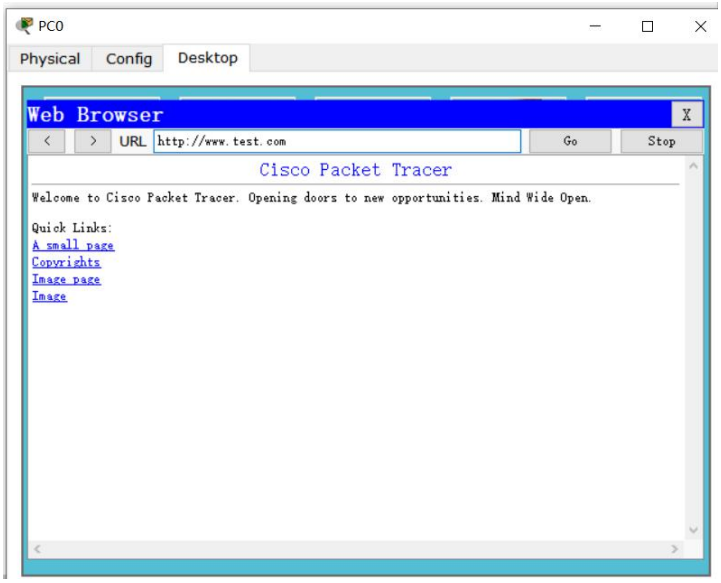


配置 DNS，增加解析域名 www.example.com:

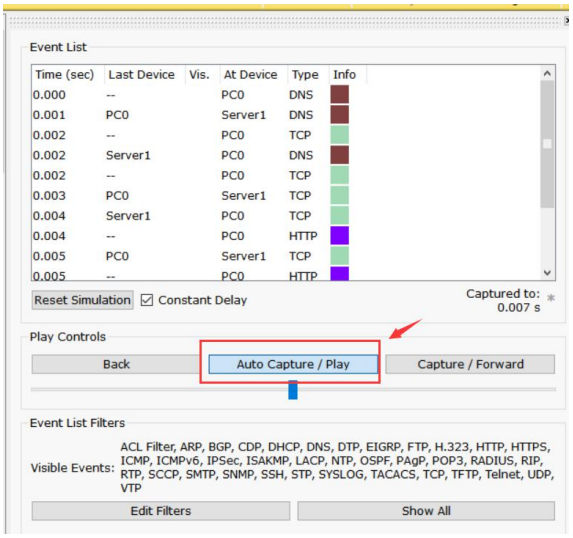


打开模拟模式：点击右下角，进入模拟模式

然后打开 PC 的 Web Browser 并访问 www.test.com

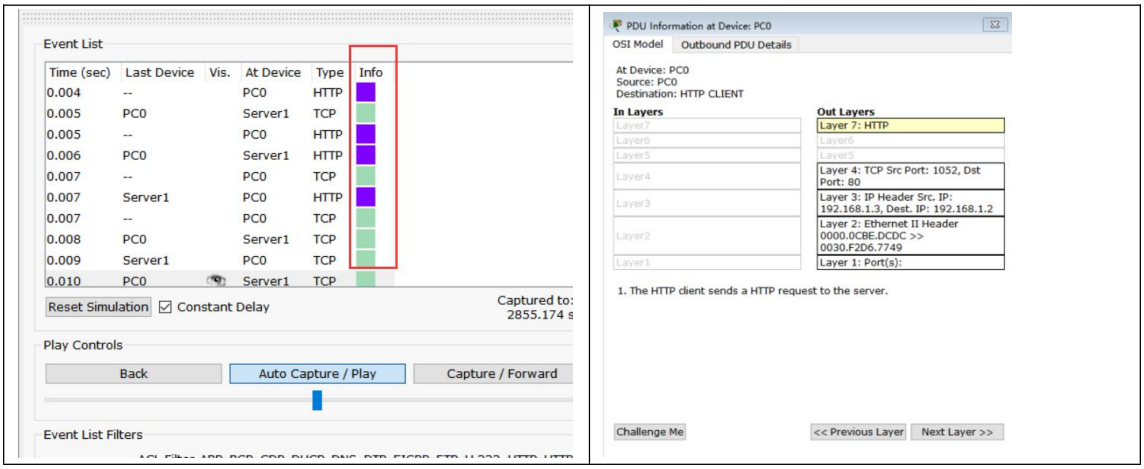


然后在仿真界面点击自动捕获

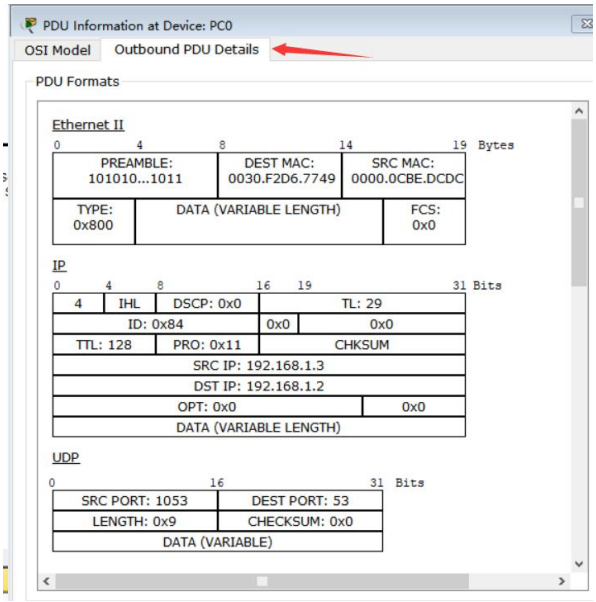


DNS 服务分析

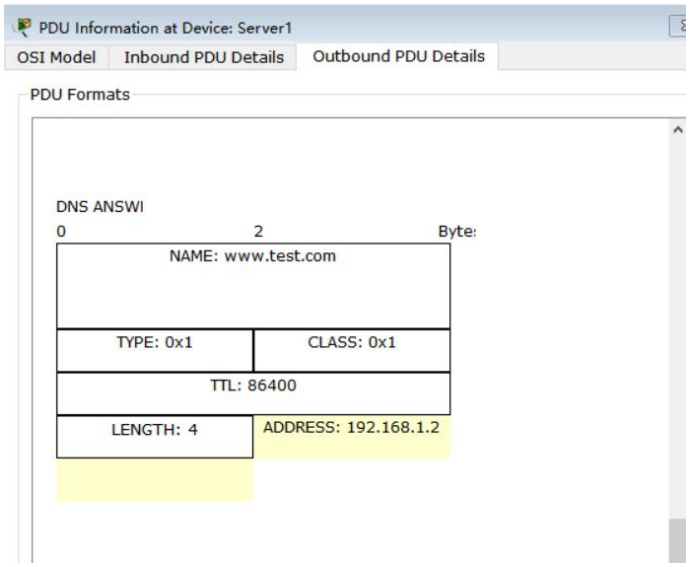
点击 info 下面的方块可以查看数据包信息，在具体信息中，单机对应层，可以看到在对应层中使用的算法，例如第七层的 HTTP 表示应用层使用的是 HTTP 协议



点击 Details，我们可以看到各个层的数据封装详细信息。



查看第二个 DNS 报文，看到返回了一个地址 192.168.1.2



对 DNS 报文的分析:

（1）首先从 PC 向 DNS 服务器发送报文（从 192.168.1.3 发送到 192.168.1.2）.

（2）DNS 服务器查询了 www.test.com 的 IP 并返回给 PC。

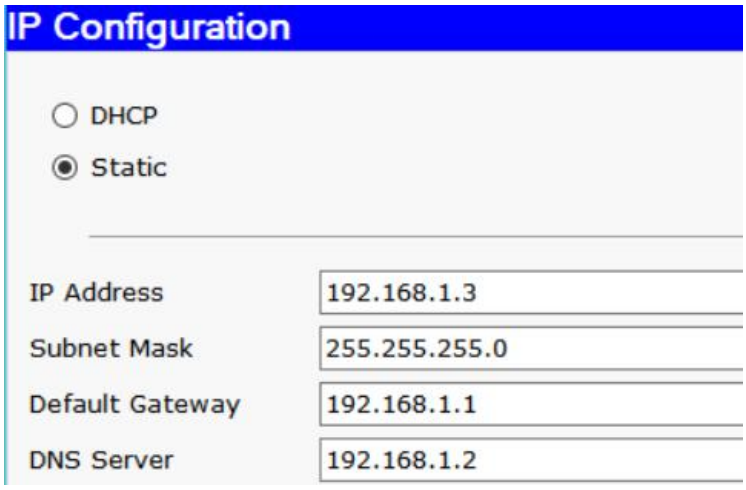
（3）之后就变成了 PC 向 www.test.com 对应的 IP 发送信息。

ARP 分析

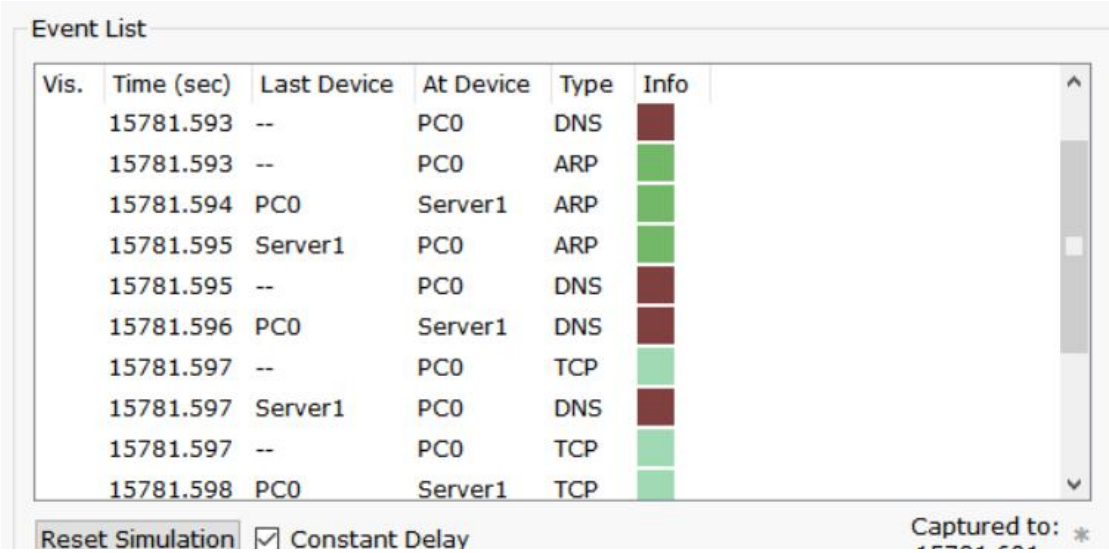
清空 arp 后点击自动抓包,

```
Packet Tracer PC Command Line 1.0
PC>arp -a
  Internet Address      Physical Address      Type
  192.168.1.2           0030.f2d6.7749        dynamic

PC>arp -d
PC>arp -a
  Internet Address      Physical Address      Type
```

PC 配置如下

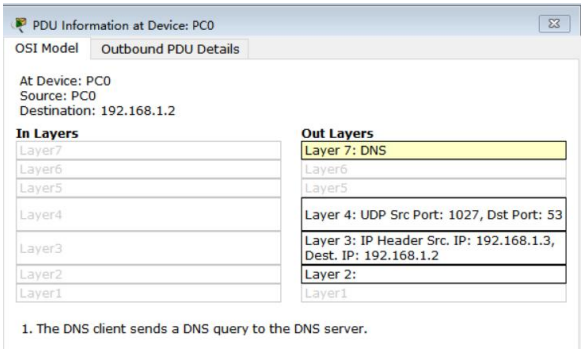


用 PC 的浏览器发送 www.test.com 去寻找网站地址，可以看到有如下报文

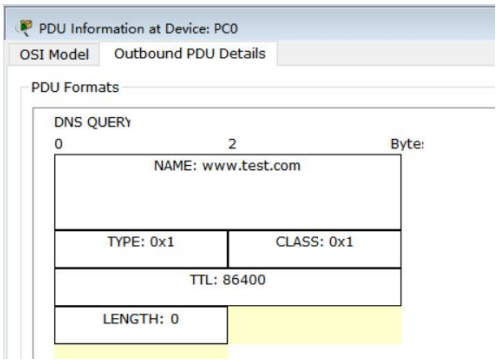


这些报文的作用：

（1）DNS 报文：可以看到这个 DNS 报文没有物理层的信息，他的含义是向 DNS 服务器地址信息，请求查询 www.test.com

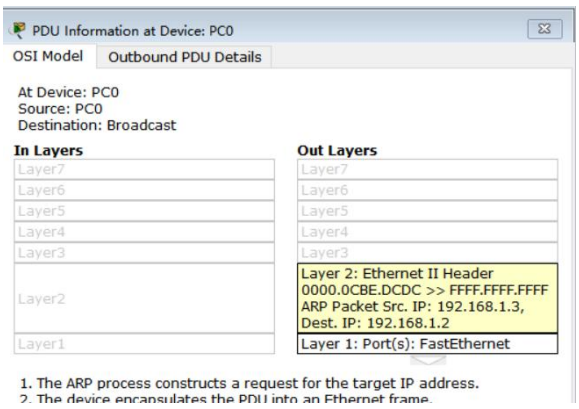


协议信息

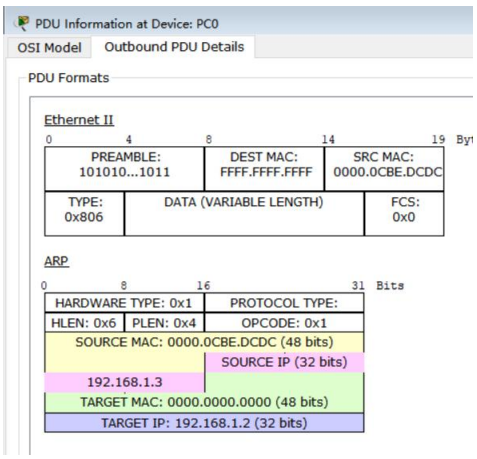


DNS 服务报文

（2）第二条是 ARP 协议：从 ARP 协议中的目标 MAC 地址是广播地址，会发向同网段的所有主机。这条 ARP 的含义是 PC 寻找 DNS 服务地址：你们知道 192.168.1.2 的地址吗，知道请告诉我（192.168.1.3）

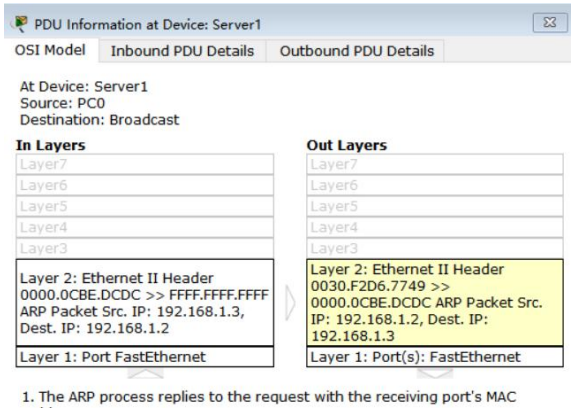


协议信息

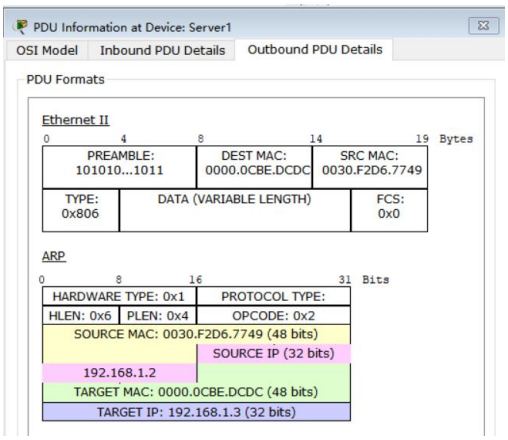


ARP 报文段

（2）第三条报文也是 ARP 报文：因为服务器收到了来自 PC 的报文请求（寻找 192.168.1.2），他核对自己的地址与要找的地址相同，因此发送了 ARP 报文，告诉 PC 的他的 MAC 地址。

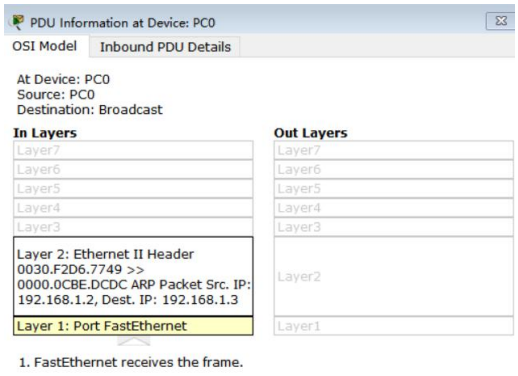


协议信息



ARP 报文段

（4）第四条报文是 PC 收到服务器的 ARP 报文：表明 PC 知道了 192.168.1.2 的地址。之后的报文就是正常的 DNS 报文了。

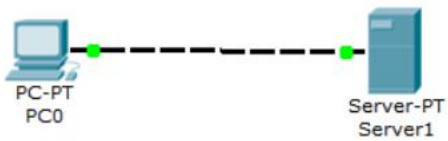


ARP 报文分析：（1）PC 发送广播报文，寻找 192.168.1.2　　（2）server 收到报文，核对自己的地址是 PC 寻找的地址，因此发送给 PC 一个报文，告诉他自己的地址。

（三）任务 2：从 PC 访问服务器的 HTTPS 服务，捕获数据包并分析

双击下面的实验文件打开 HTTPS，此工程的结构如右图，一台 PC0 连接一台 server1

三、相关实验文件：



有注释信息如下：他提示我们访问 10.1.1.3 网站。

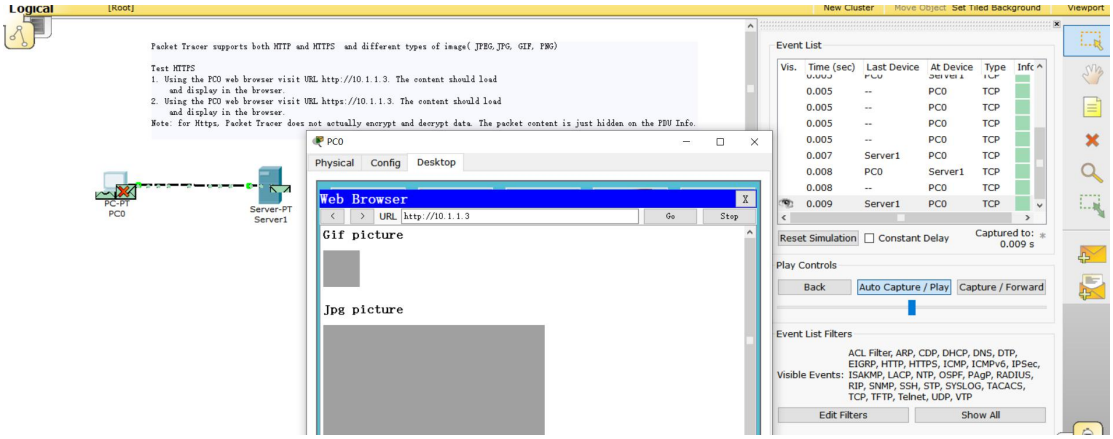
Packet Tracer supports both HTTP and HTTPS　and different types of image(JPEG,JPG, GIF, PNG)

Test HTTPS

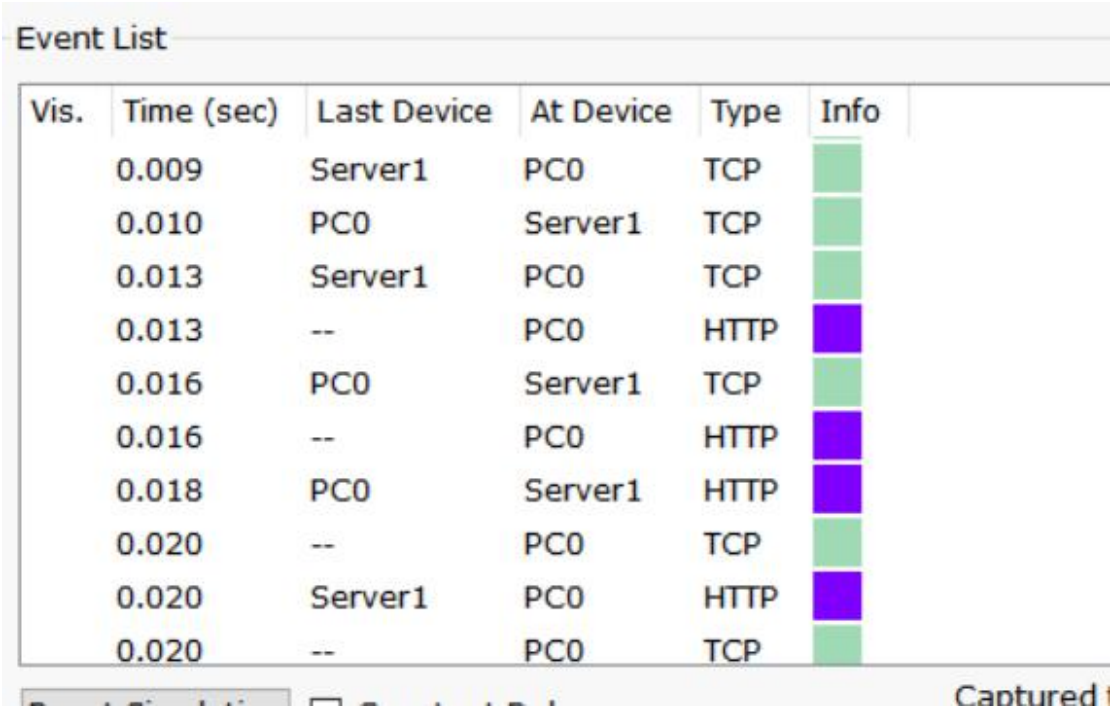
1. Using the PC0 web browser visit URL http://10.1.1.3. The content should load and display in the browser.
2. Using the PC0 web browser visit URL https://10.1.1.3. The content should load and display in the browser.

Note: for Https, Packet Tracer does not actually encrypt and decrypt data. The packet content is just hidden on the PDU Info.

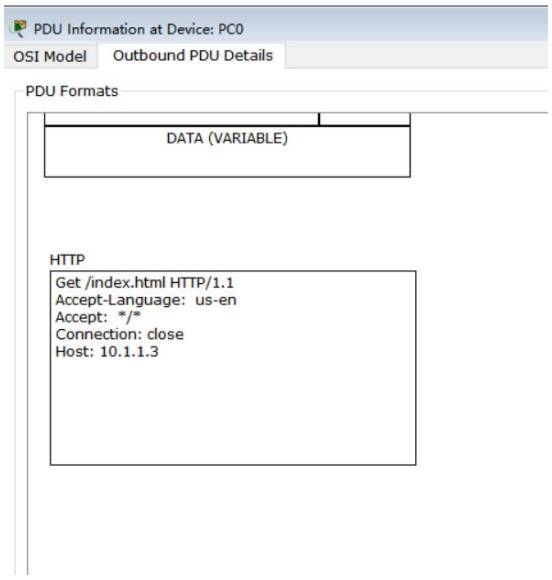
1. 进入 simulation 模式，访问上述地址并自动抓包.



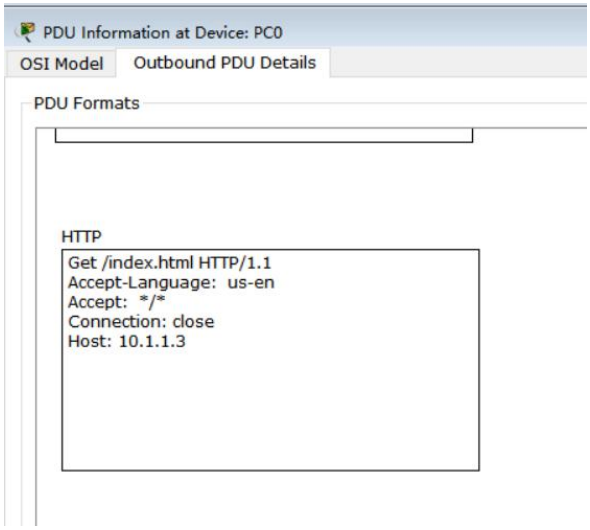
2. 查看数据包信息：HTTP 内容如下



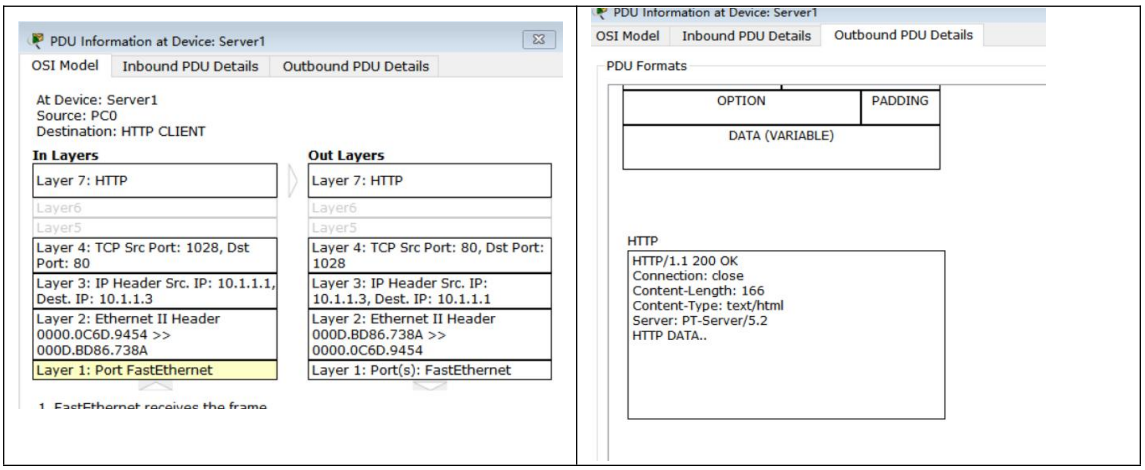
（1）第一条 http 报文如下图:请求的是默认的页。



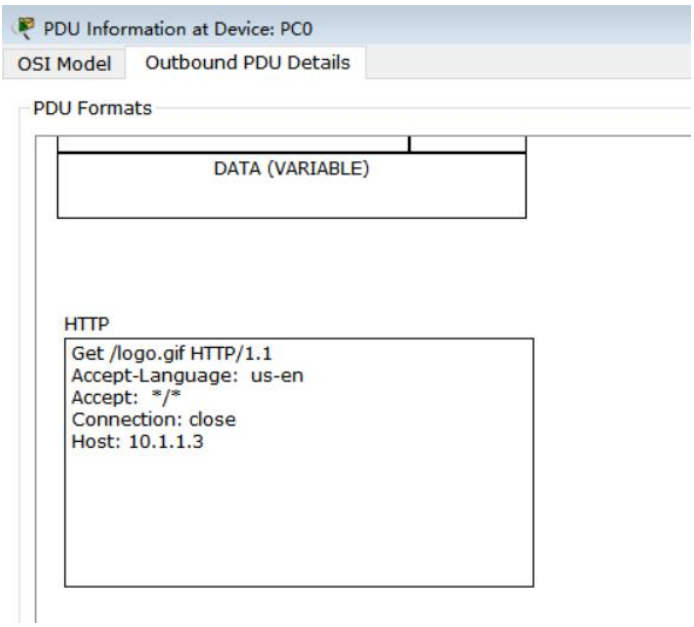
（2）第二条 HTTP 请求：仍然是默认页面



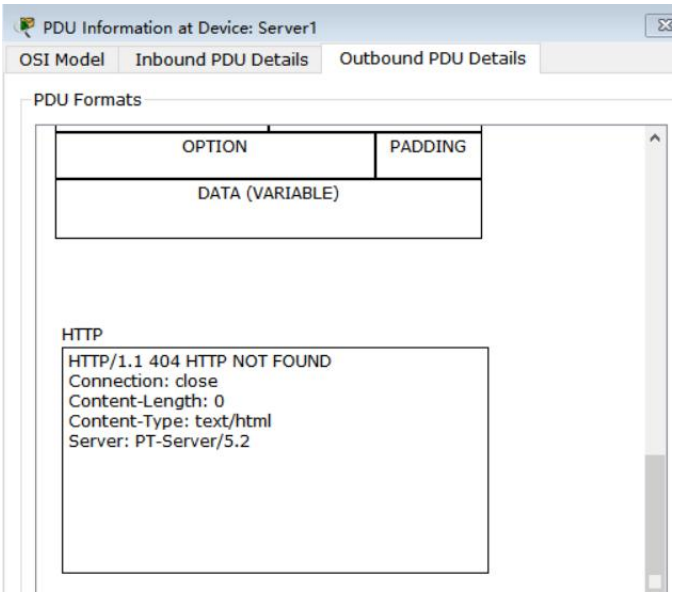
（2）第三条 HTTP 消息：是服务 server 收到 PC 的信息，右图是 server 发送给 PC 的信息，他发送了 index.html 文件报文给 PC1。



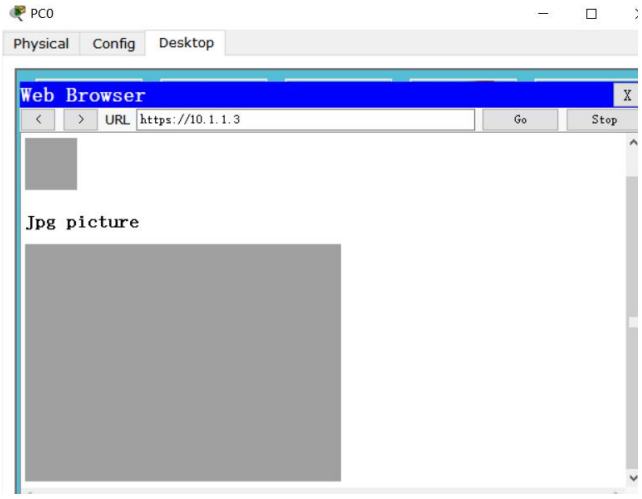
（3）收到网页文件后，PC 发现网页中有图片，因此向服务器请求这些图片，现请求 log.gif



(4）服务器收到 gif 的请求后，发现他没有这个图片，发送了 404NOTFIND。



HTTPS 协议分析：访问 HTTPS 网址

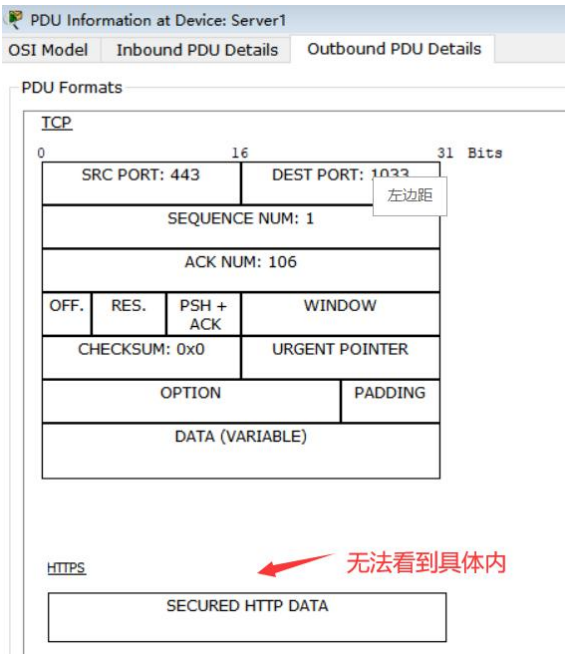


得到的数据包与 HTTP 类似

Event List

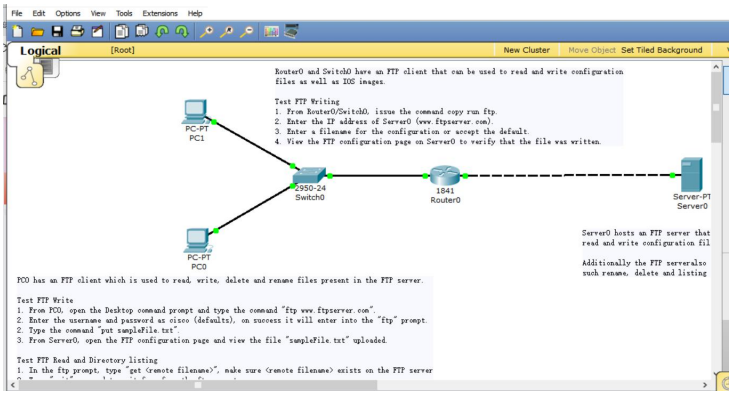
Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.032	PC0	Server1	TCP	
	0.032	--	PC0	HTTPS	
	0.033	PC0	Server1	HTTPS	
	0.035	--	PC0	TCP	
	0.035	Server1	PC0	HTTPS	
	0.035	--	PC0	TCP	
	0.038	PC0	Server1	TCP	
	0.039	Server1	PC0	TCP	
	0.042	PC0	Server1	TCP	
	2.002	--	PC0	ICMP	

但是 HTTPS 是加密协议，看不到 HTTPS 的内容



（四）任务 3：从 PC 访问服务器的 FTP 服务，捕获数据包并分析。

打开 FTP.pkt,得到的拓扑结构如下，有两台 PC，一个交换一，一个路由机，一个服务器。



其中一个提示信息如下，他要求我们测试 FTP 的一些列功能

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

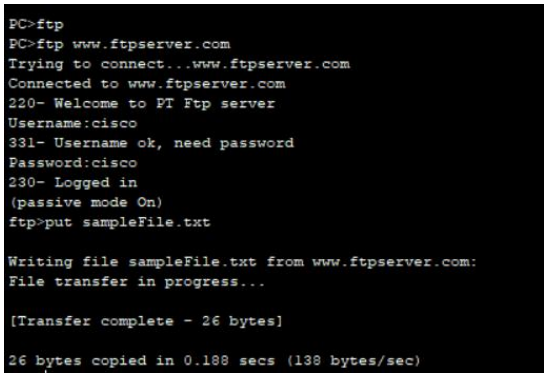
1. In the ftp prompt, type "rename <old remote filename> <new remote filename>".
2. If renamed succesfully then type "dir" to view the change.

Test FTP Delete

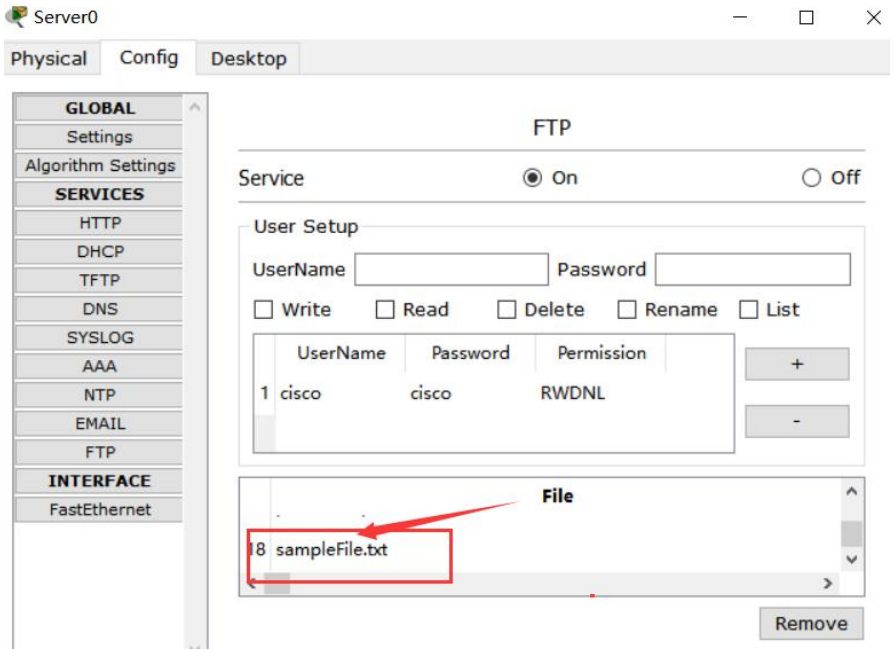
1. In the ftp prompt, type "delete <filename>" to delete a file from the remote FTP server.
2. If deleted succesfully then type "dir" to view the change.

1. Test FTP Write 功能测试

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 。并且把文件上传到服务器：put sampleFile.txt。　　如下图显示上传成功。

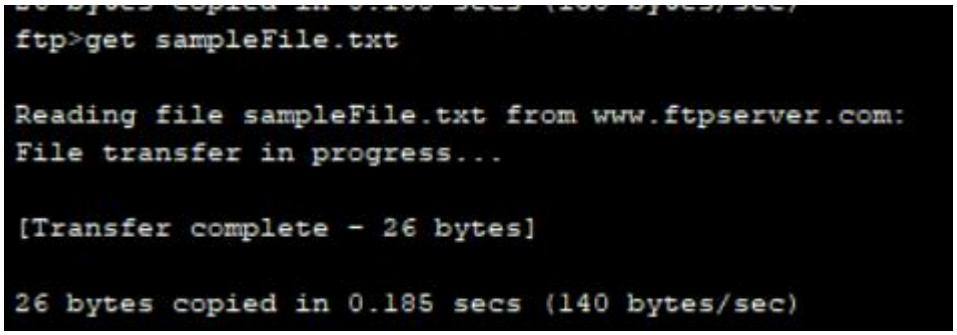


查看 server 的文件列表,可以看到我们上传的文件。

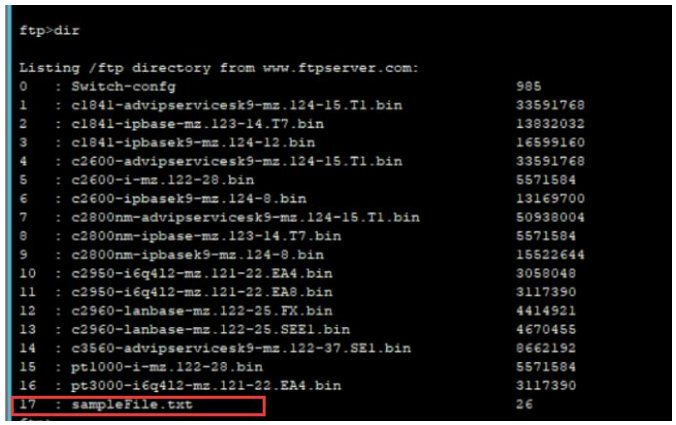


2. Test FTP Read 功能测试

获取 sampleFile



输入 dir，可以看到我们下载的 sample.txt 信息



3. Test FTP Rname 功能测试

重命名文件，将 sampleFile.txt 更名为 newname.txt,可以看到更名成功

```
ftp>rename sampleFile.txt newname.txt

Renaming sampleFile.txt

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

4. Test FTP Delete 功能测试

首先看文件如下：有 newname.txt

```
ftp>
[OK Renamed file successfully from sampleFile.txt to newname.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-i6q412-mz.121-22.EA4.bin              3058048
11   : c2950-i6q412-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   : newname.txt                                 26
16   : pt1000-i-mz.122-28.bin                      5571584
17   : pt3000-i6q412-mz.121-22.EA4.bin             3117390
ftp>
```

Delete newname.txt

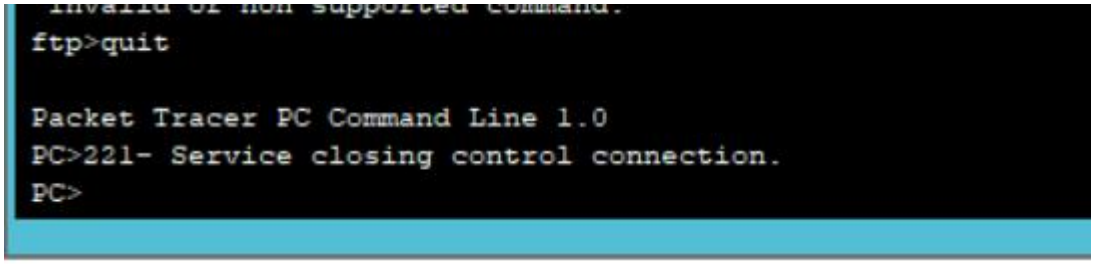
```
ftp>delete newname.txt

Deleting file newname.txt from www.ftpserver.com: ftp>
[Deleted file newname.txt successfully ]
```

可以看到删除后已经没有 newname.txt 文件了。

```
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-i6q412-mz.121-22.EA4.bin              3058048
11   : c2950-i6q412-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-i6q412-mz.121-22.EA4.bin             3117390
```

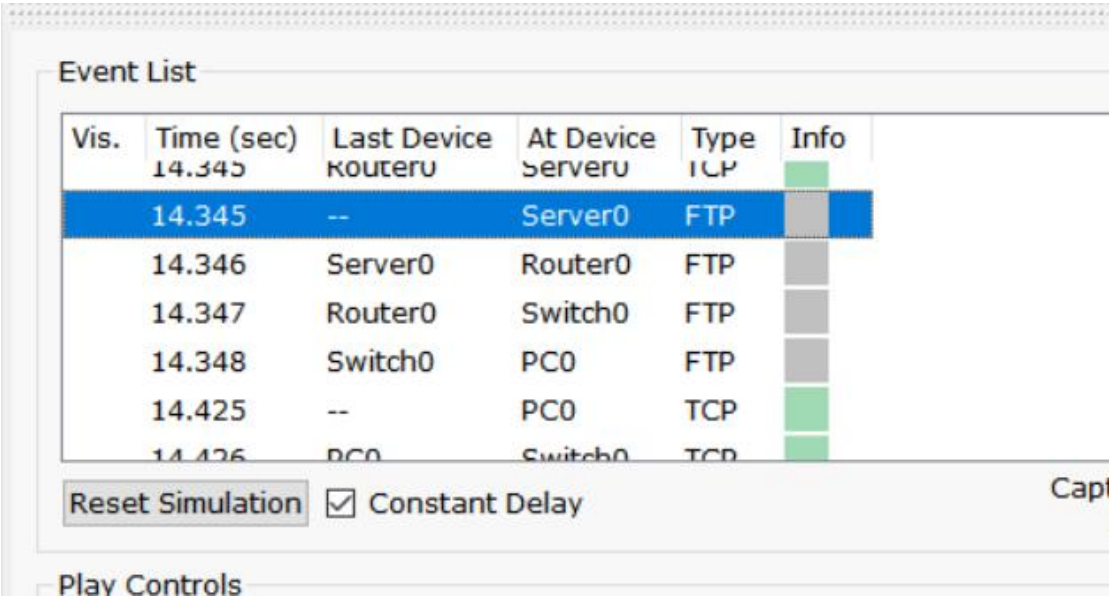
5. Test FTP qiut 功能测试

输入 quit，退出成功

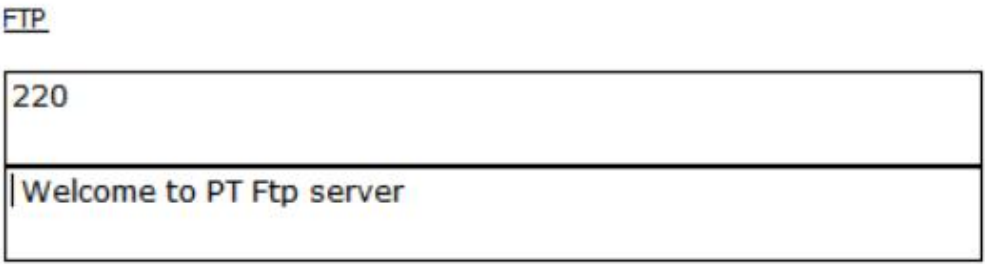


6. 查看具体的 FTP 协议

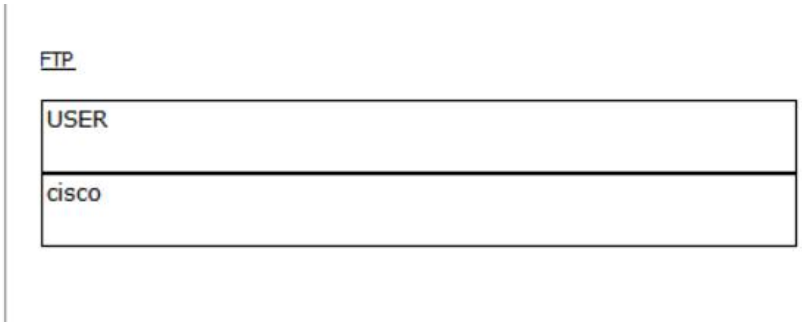
输入 ftp www.ftpserver.com，捕获的包如下：



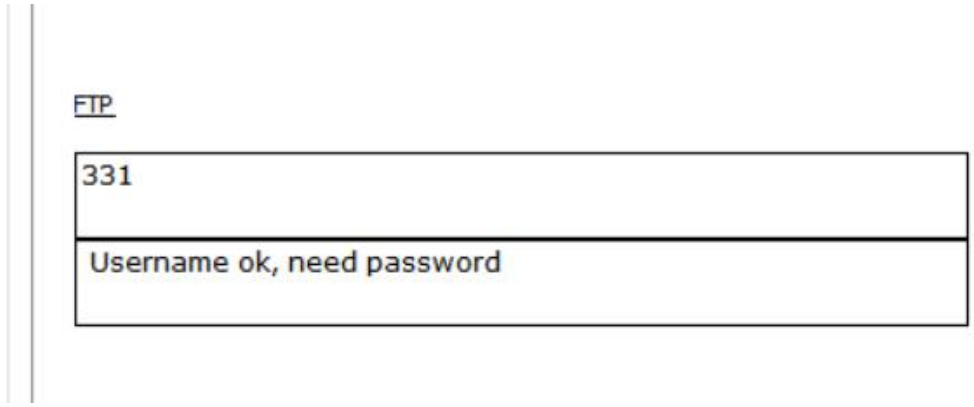
从上面可以看出，FTP 报文从 server0 出发，发送路径是 server0->Router0->swith0->PC0.
第一次响应 FTP：server 到 PC0 完成 FTP 连接。



第二次，PC0 到 server0，发送用户名信息



第三次：server 收到用户名，发送 OK 信息。



之后就是确认 FTP 的密码。与上面的类似。
总结：每次 FTP 都要路由和交换机，因此每发送一条 ftp 信息都会捕获到多条 FTP 报文

四、实验心得与不足

1.学到了 Cisco Packet 的使用，能够自己建立简单的网络。

2.除了上面的实验信息外，在实验过中，还发现了 TCP 的三次握手包，对 HTTP，TCP，ARP，FTP 的功能有了更多的认识。