

# Lab 1

*by flrs*

课程：计算机网络安全技术（2023秋）

## Task 1

---

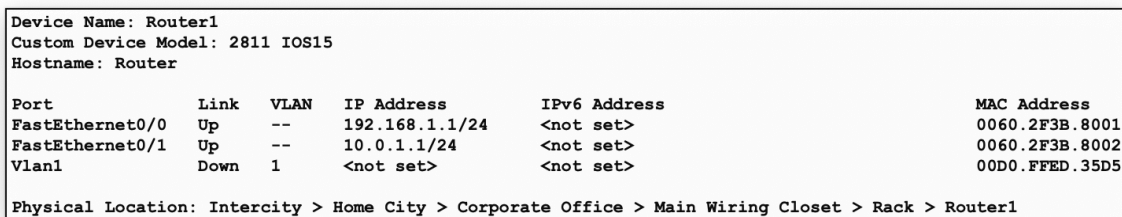
纰漏：Router2的端口2的IP地址使用了公有IP地址，这会容易导致地址冲突，同时将内部设备暴露在互联网上，使得遭受攻击的风险更大。

更正和补全后的结果：

| Device  | Port | IP                 | Mask | Gateway            |
|---------|------|--------------------|------|--------------------|
| Router1 | 端口1  | 192.168.1.1        | /24  | -                  |
|         | 端口2  | 10.0.1.1           | /24  | -                  |
| Router2 | 端口1  | 10.0.1.2           | /24  | -                  |
|         | 端口2  | <b>10.0.2.2</b>    | /24  | -                  |
|         | 端口3  | 192.168.2.1        | /24  | -                  |
| Router3 | 端口1  | <b>10.0.2.1</b>    | /24  | -                  |
|         | 端口2  | 192.168.3.1        | /24  | -                  |
| PC1     | 端口1  | 192.168.1.2        | /24  | 192.168.1.1        |
| PC2     | 端口1  | 192.168.2.2        | /24  | 192.168.2.1        |
| PC3     | 端口1  | <b>192.168.3.2</b> | /24  | 192.168.3.1        |
| Server1 | 端口1  | 192.168.1.3        | /24  | 192.168.1.1        |
| Laptop1 | 端口1  | 192.168.1.4        | /24  | 192.168.1.1        |
| Laptop2 | 端口1  | 192.168.2.3        | /24  | <b>192.168.2.1</b> |
| Laptop3 | 端口1  | 192.168.3.3        | /24  | 192.168.3.1        |

## Task 2

必要截图：



```

Device Name: Router2
Custom Device Model: 2811 IOS15
Hostname: Router

Port      Link    VLAN    IP Address      IPv6 Address      MAC Address
FastEthernet0/0  Up      --      10.0.1.2/24     <not set>         000D.BDC1.2801
FastEthernet0/1  Up      --      10.0.2.2/24     <not set>         000D.BDC1.2802
FastEthernet1/0  Up      --      192.168.2.1/24  <not set>         0001.4345.A214
Vlan1         Down    1        <not set>        <not set>         000A.F323.6DE8

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router2

```

```

Device Name: Router3
Custom Device Model: 2811 IOS15
Hostname: Router

Port      Link   VLAN   IP Address      IPv6 Address      MAC Address
FastEthernet0/0  Up    --    10.0.2.1/24     <not set>         0030.F212.0401
FastEthernet0/1  Up    --    192.168.3.1/24  <not set>         0030.F212.0402
Vlan1        Down  1      <not set>       <not set>         0009.7C38.C030

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router3

```

## Task 3

---

配置文件不会泄露的情况下可采取：

1. 进入全局配置模式：

```
Router> enable
Router# configure terminal
Router(config)#
```

2. 进入console线路配置模式：

```
Router(config)# line console 0
```

3. 配置控制台口的访问密码

```
Router(config-line)# password password1
Router(config-line)# login
Router(config-line)# exit
```

4. 配置特权模式的密码

```
Router(config)# enable password password2
```

5. 进入vty线路配置模式

```
Router(config)# line vty 0 15
```

6. 设置 Telnet 密码：

```
Router(config-line)# password password3
Router(config-line)# login
Router1(config-line)# exit
```

7. 保存配置

```
Router(config)# end
Router# write memory
```

如果路由器配置文件可能泄露添加如下步骤：

1. 进入全局配置模式

```
Router> enable
Router# configure terminal
Router(config)#
```

## 2. 启用密码加密服务

```
Router(config)# service password-encryption
```

（不过这里默认使用的是Type 7加密，这其实是一种隐藏而非真正的加密）

## 3. 保存配置

```
Router(config)# end
Router# write memory
```

暴力破解时时间需求的变化（最大可能攻击次数）：

据助教是算错了

1. 总长六位纯数字： $10^6$ （记为\*）
2. 总长六位的混合有数字及小写字母的密码： $1.87 \times 10^9$ （\*的 $1.87 \times 10^3$ 倍）
3. 总长六位的混合有数字、大写字母、小写字母的密码： $7.91 \times 10^{10}$ （\*的 $7.91 \times 10^4$ 倍）
4. 总长八位的混合有数字、大写字母、小写字母的密码： $2.76 \times 10^{14}$ （\*的 $2.76 \times 10^8$ 倍）

# Task 4

分别执行以下操作：

### ■ Router1:

```
Router(config)# ip route 192.168.0.0 255.255.0.0 10.0.1.2
```

上面是配置最少静态路由的策略，当然，可以更具体地：

```
Router(config)# ip route 192.168.2.0 255.255.255.0 10.0.1.2
Router(config)# ip route 192.168.3.0 255.255.255.0 10.0.1.2
```

### ■ Router2:

```
Router(config)# ip route 192.168.1.0 255.255.255.0 10.0.1.1
Router(config)# ip route 192.168.3.0 255.255.255.0 10.0.2.2
```

■ Router3:

```
Router(config)# ip route 192.168.0.0 255.255.0.0 10.0.2.1
```

上面是配置最少静态路由的策略，当然，可以更具具体地：

```
Router(config)# ip route 192.168.1.0 255.255.255.0 10.0.2.1
Router(config)# ip route 192.168.2.0 255.255.255.0 10.0.2.1
```

并保存配置：

```
Router(config)# end
Router# write memory
```

## Task 5

我决定选用RIP路由协议；凯撒的观点没有问题：在元老院和部族会议所的路由器之间建立新的通信链路后，元老院向部族会议所发送信息时不经过执政官首府跳数总是更少的，因此RIP协议可以满足要求。

首先删除所有的静态路由，并为Router1和Router3的新端口分配IP地址；

接着分别采取如下操作

■ Router1:

```
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# network 192.168.1.0
```

■ Router2:

```
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# network 192.168.2.0
```

## ■ Router3:

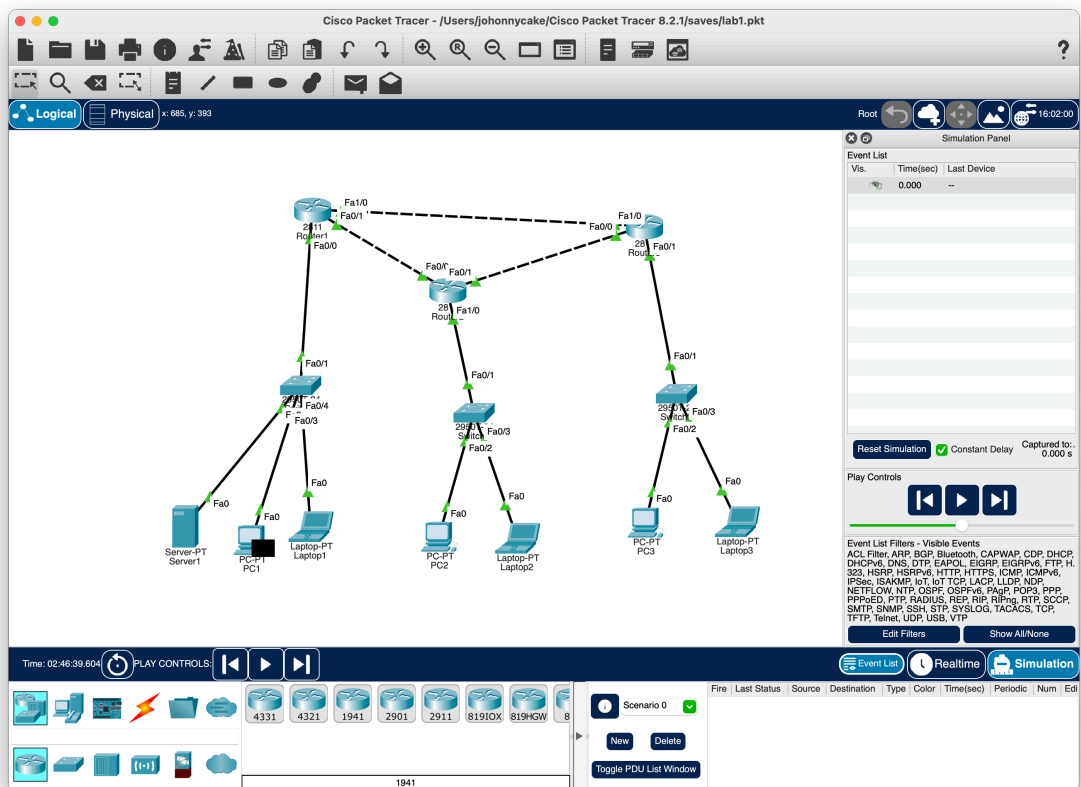
```
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# network 192.168.3.0
```

最后保存配置：

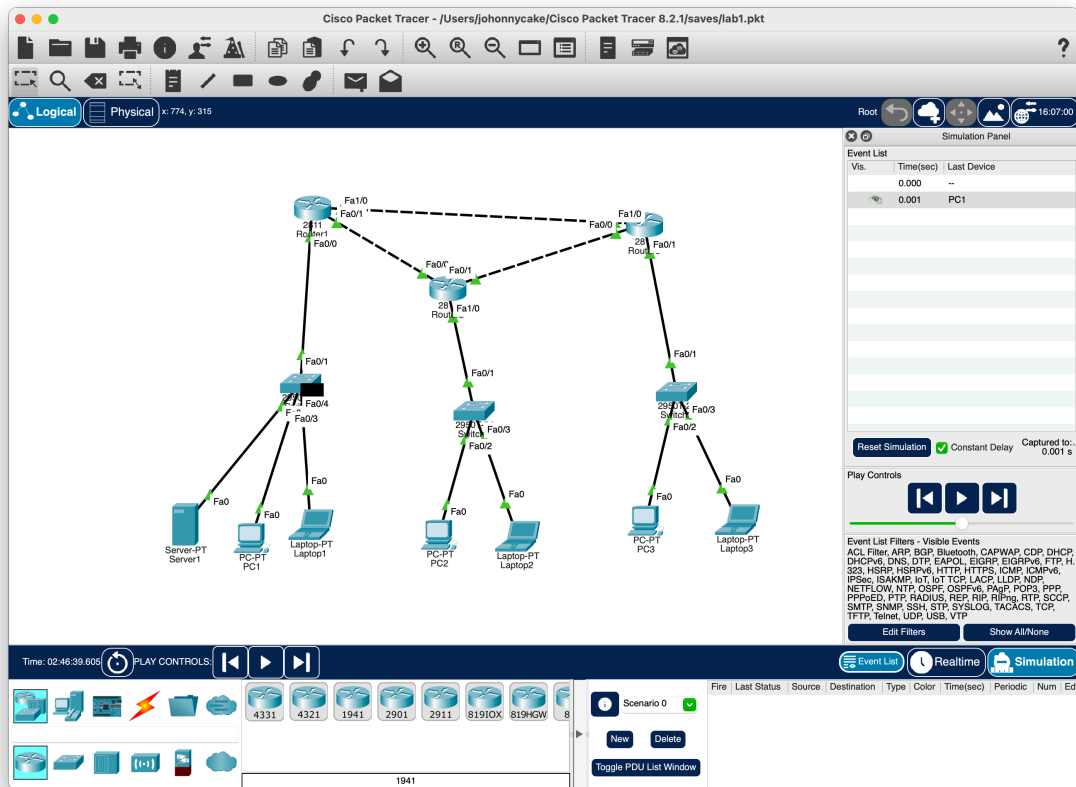
```
Router(config)# end
Router# write memory
```

对从PC1到PC3的仿真截图：

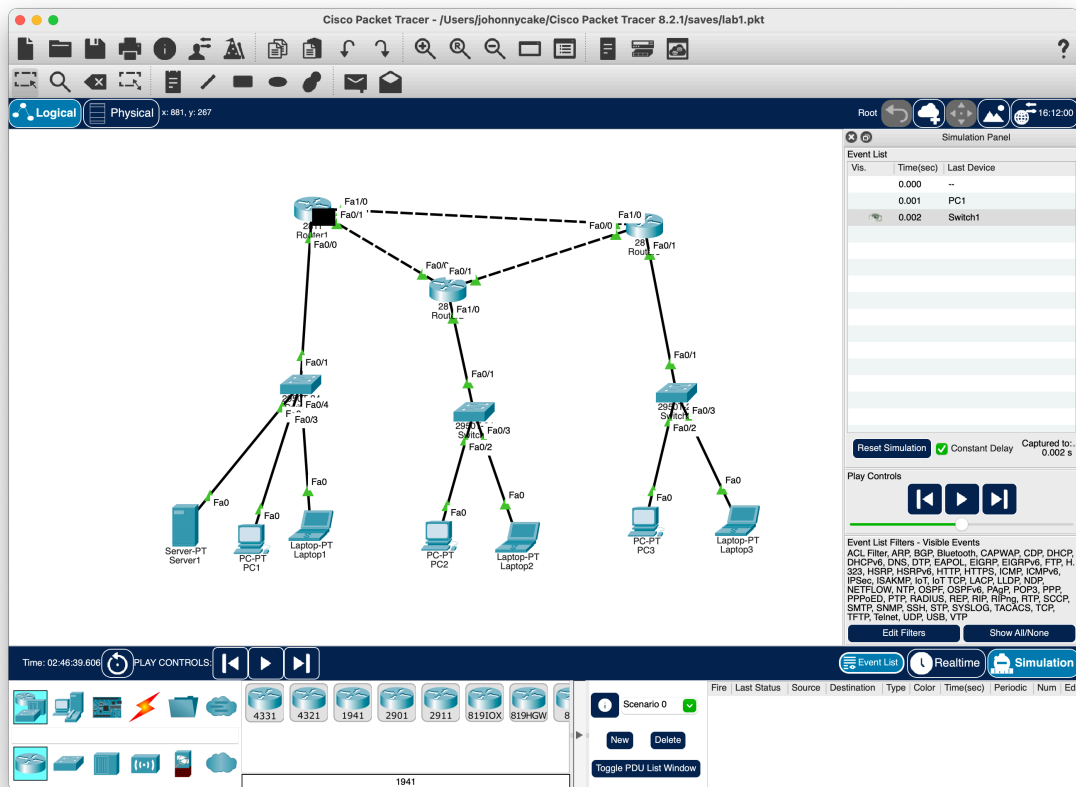
1.



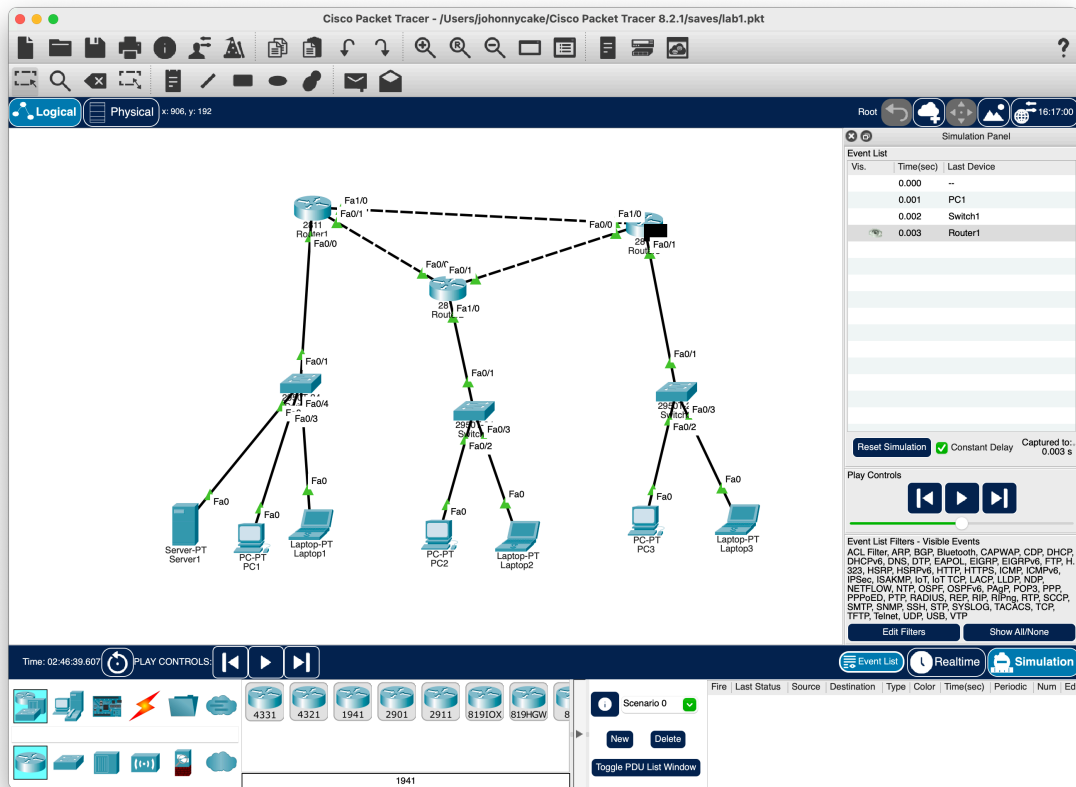
2.



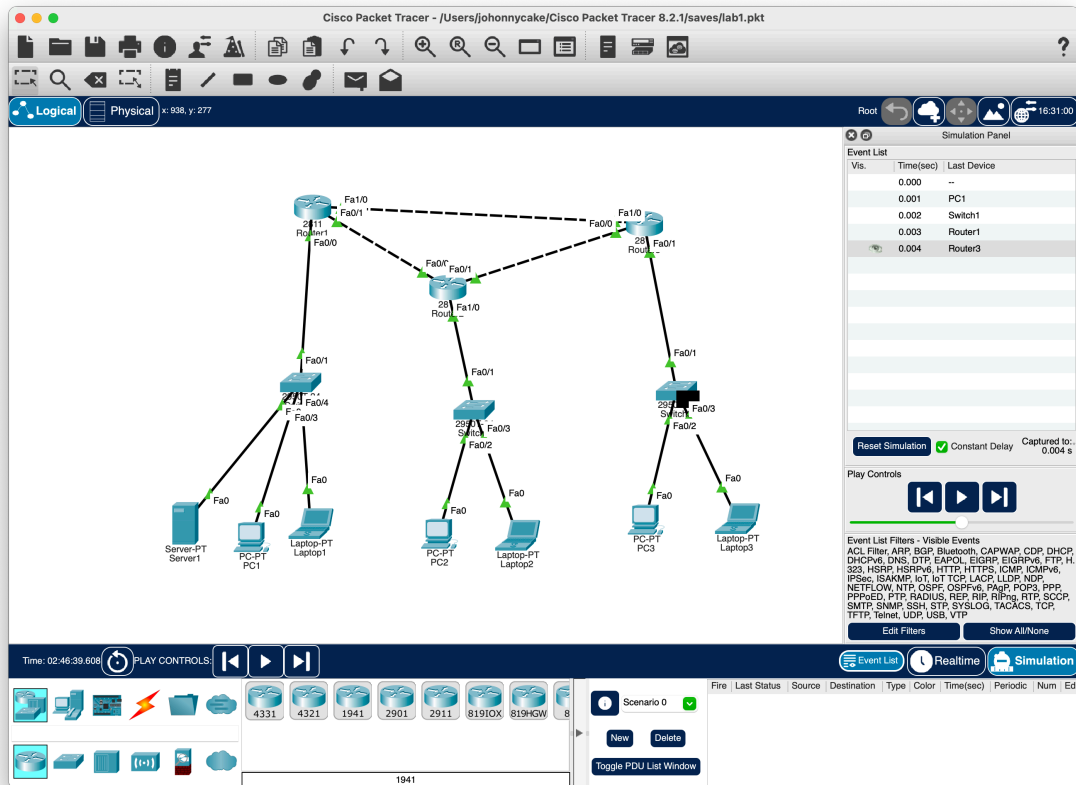
3.



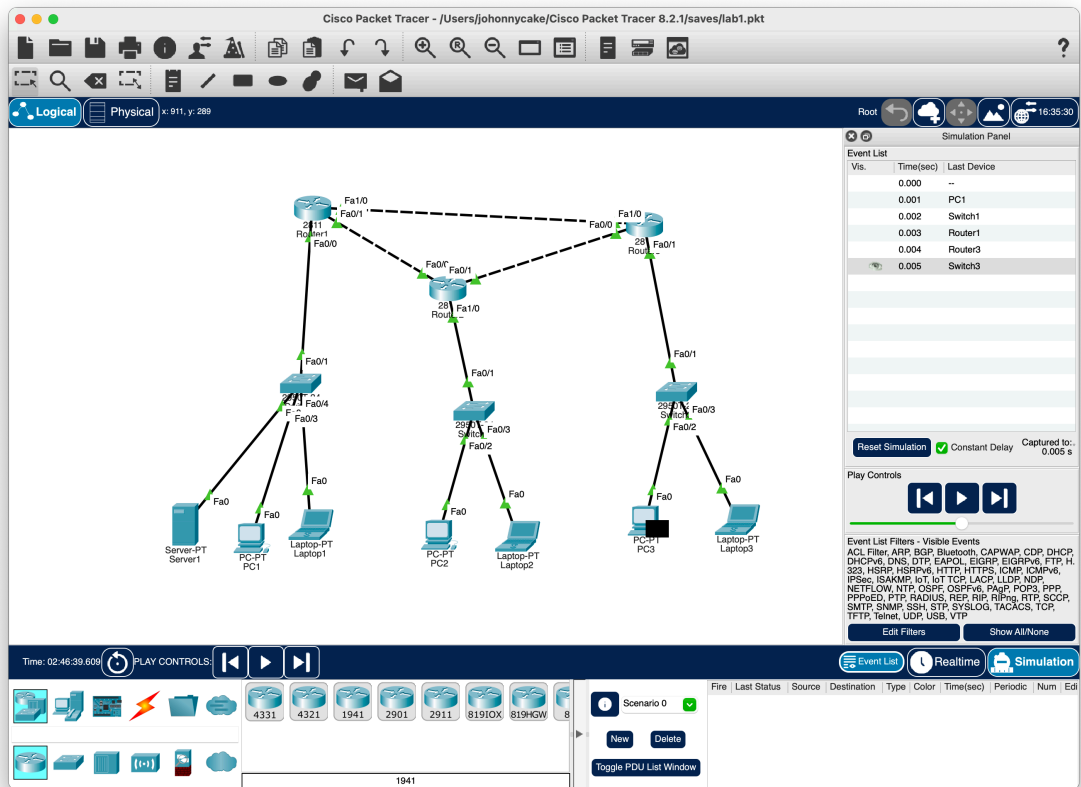
4.



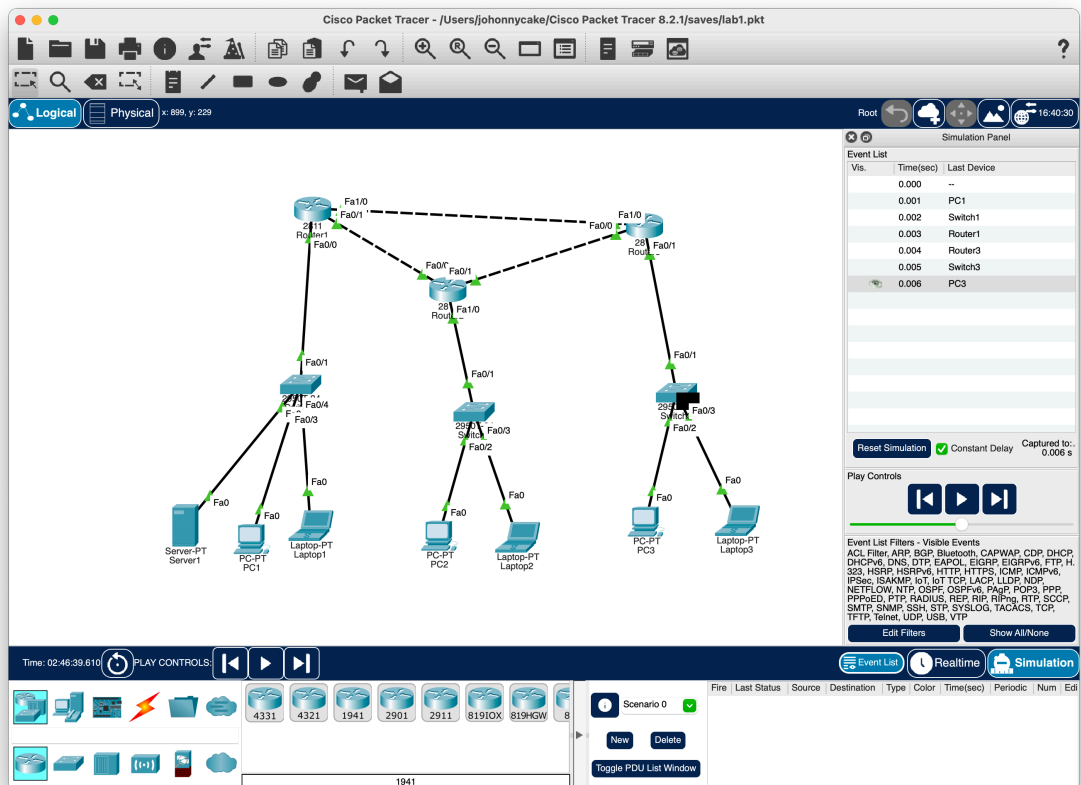
5.



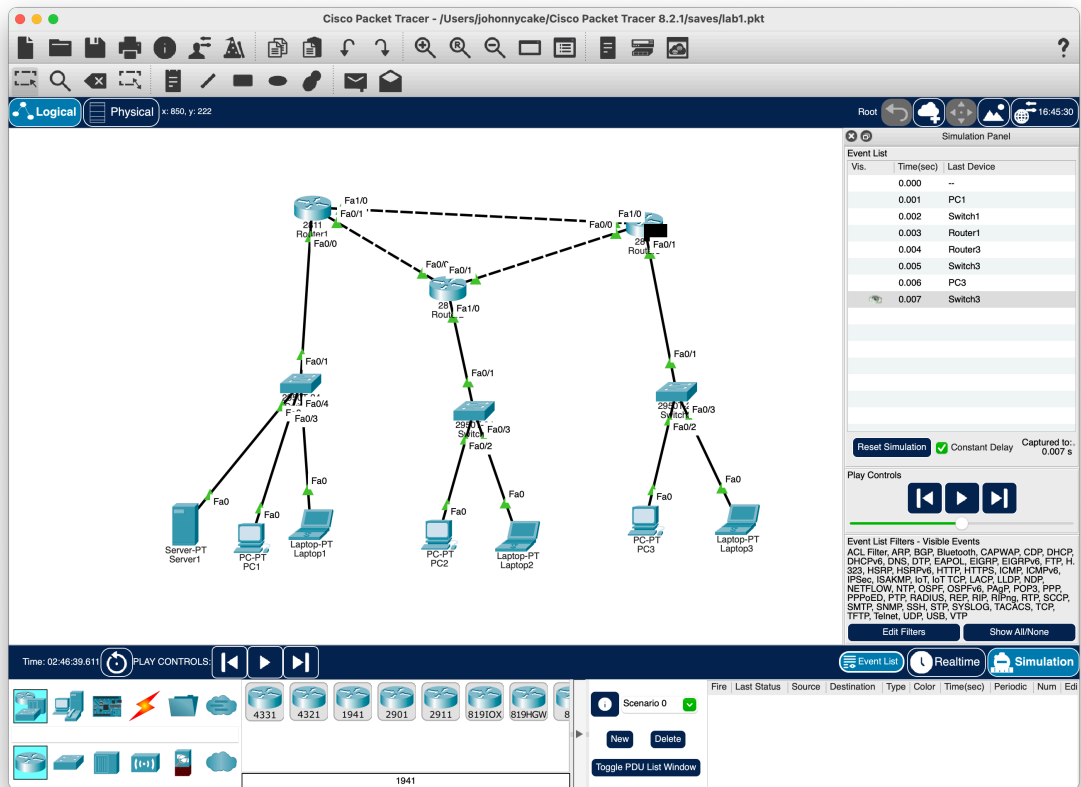
6.



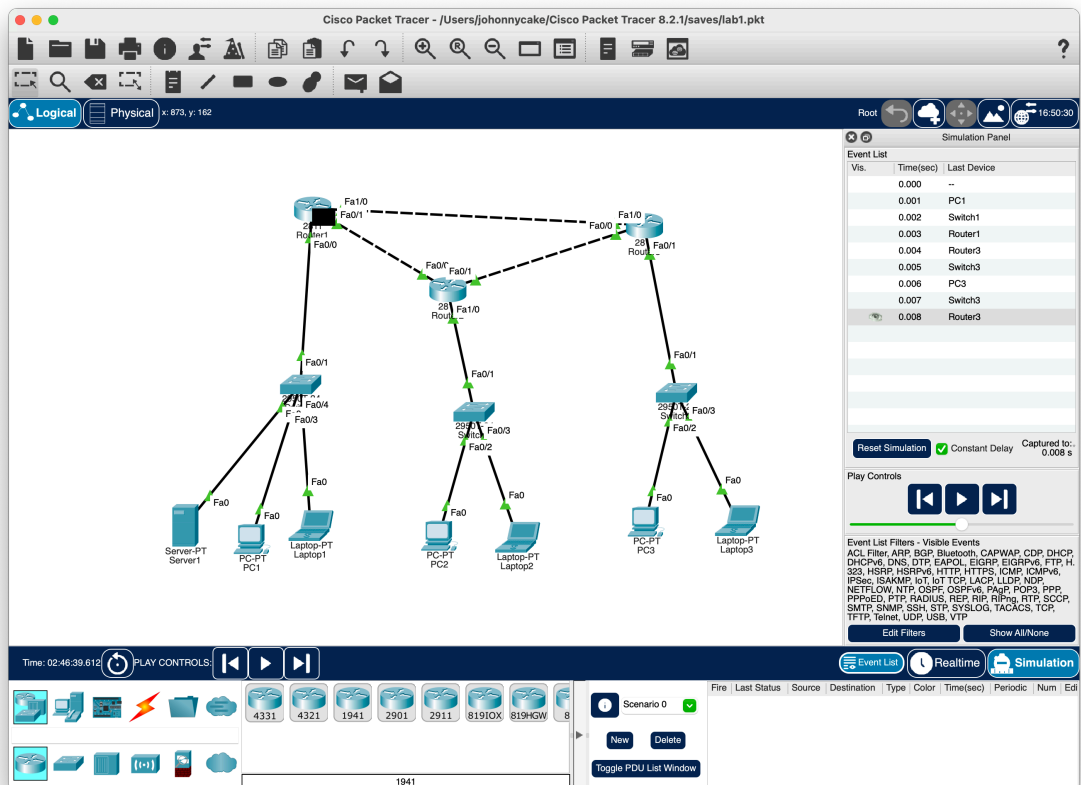
7.



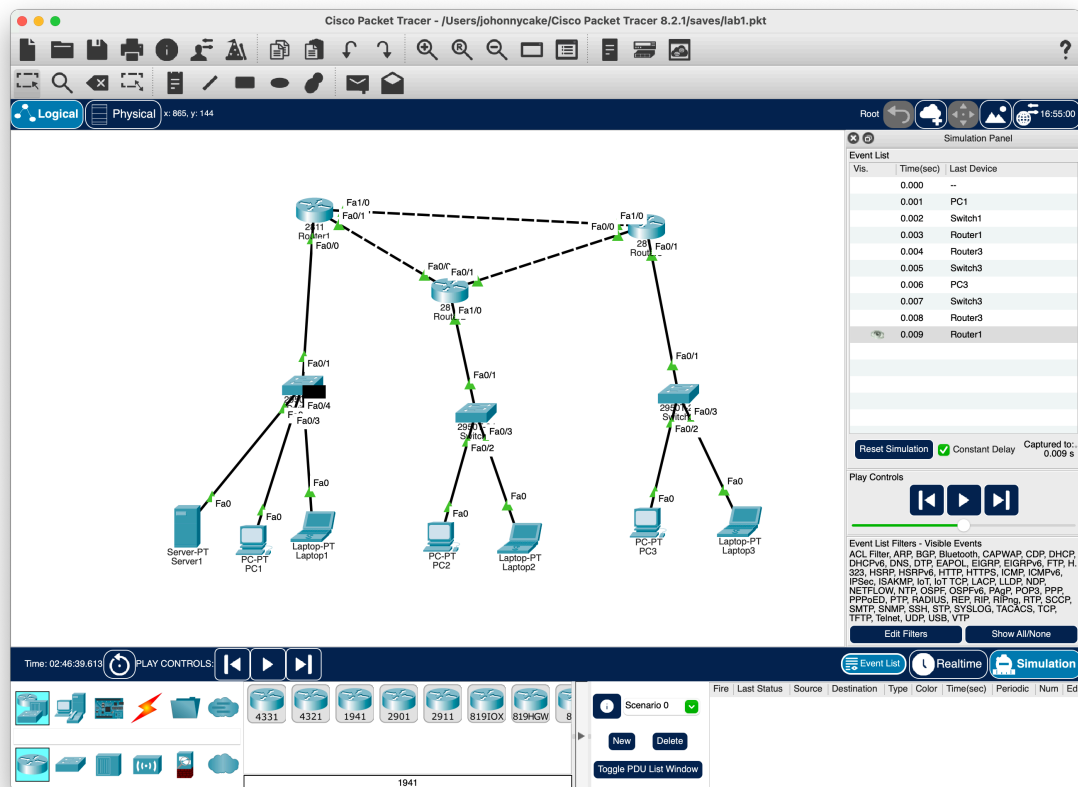
8.



9.



0.



## Bonus Task

选择任务1:

加密方式有Type 5(MD5), Type 7, Type 9(SCRIPT), 其中Type 7其实是一种隐藏而非真正的加密, 当安全性要求高时应使用Type 9进行加密。