

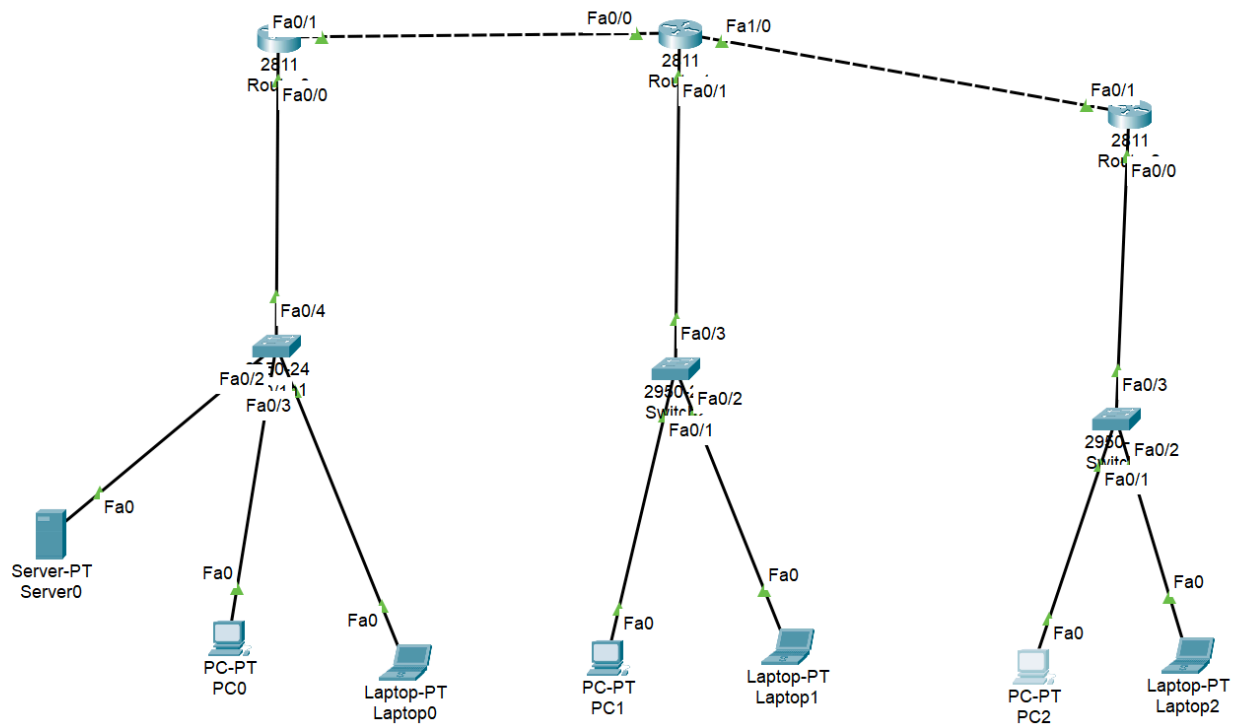
《计算机网络安全技术》第一次作业

任务一

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	10.0.2.2	/24	-
	端口 3	192.168.2.1	/24	-
Router3	端口 1	10.0.2.1	/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	192.168.3.2	/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	192.168.2.1
Laptop3	端口 1	192.168.3.3	/24	192.168.3.1

任务二

搭建的网络如下



对PC0的配置如下，对于pc，需要配置ip地址和gateway

PC0

Physical

Config

Desktop

Programming

Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

FastEthernet0

Bluetooth

Global Settings

Display Name

PC0

Interfaces

FastEthernet0

Gateway/DNS IPv4

DHCP

Static

Default Gateway

192.168.1.1

DNS Server

Gateway/DNS IPv6

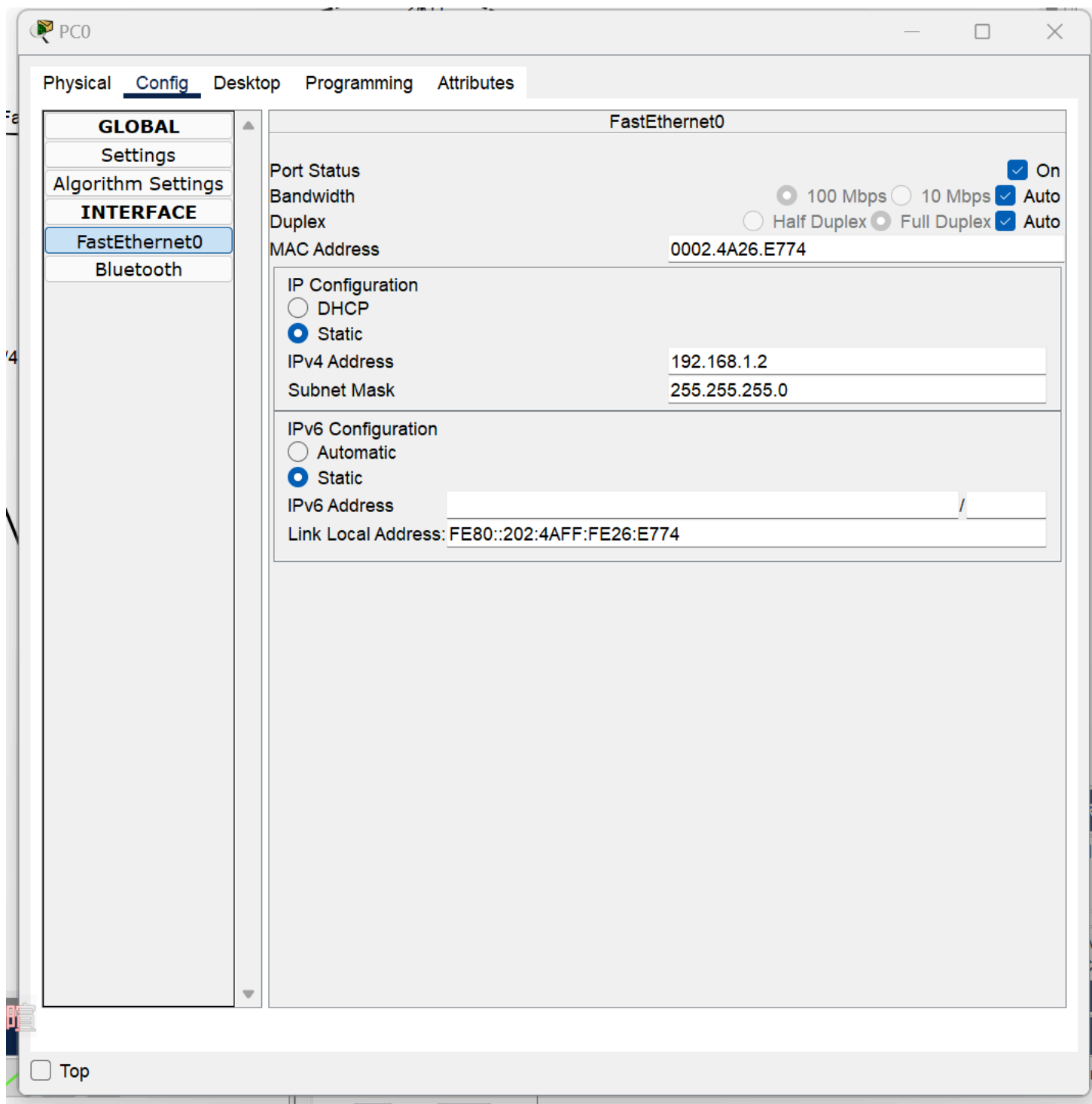
Automatic

Static

Default Gateway

DNS Server

Top



其余ip配置类似

任务三

凯撒希望包含的文字为

venividivici

将三种密码均设置为venividivici

通过console口进入用户模式的口令

```
Router>enable
Router#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line con 0
Router(config-line)#password venividivici
Router(config-line)#login
Router(config-line)#exit
```

用户模式进入特权模式的口令

```
Router(config)#enable password venividivici
Router(config)#exit
- - - - -
```

通过telnet方式登录路由器的口令

```
Router>enable
Password:
Router#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#password venividivici
Router(config-line)#login
Router(config-line)#exit
Router(config)#
```

如果路由器配置文件可能泄露，则需要加密储存密码，需要将 enable password 改为 enable secret

1. 总长六位的纯数字密码： 10^6
2. 总长六位的混合有数字及小写字母的密码： 36^6
3. 总长六位的混合有数字、大写字母、小写字母的密码： 62^6
4. 总长八位的混合有数字、大写字母、小写字母的密码： 62^8

任务四

以router2的配置为例，需要配置向另外两个router的下一跳地址

Router1

PhysicalConfigCLIAttributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

FastEthernet0/0

FastEthernet0/1

FastEthernet1/0

FastEthernet1/1

Static Routes

Network

Mask

Next Hop

Add

Network Address

192.168.1.0/24 via 10.0.1.1

192.168.3.0/24 via 10.0.2.1

Remove

Equivalent IOS Commands

Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#

☐ Top

配置完成后，可以相互ping通

```
C:\>ping 192.168.2.2
```

```
Pinging 192.168.2.2 with 32 bytes of data:
```

```
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
```

```
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
```

```
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
```

```
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
```

```
Ping statistics for 192.168.2.2:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

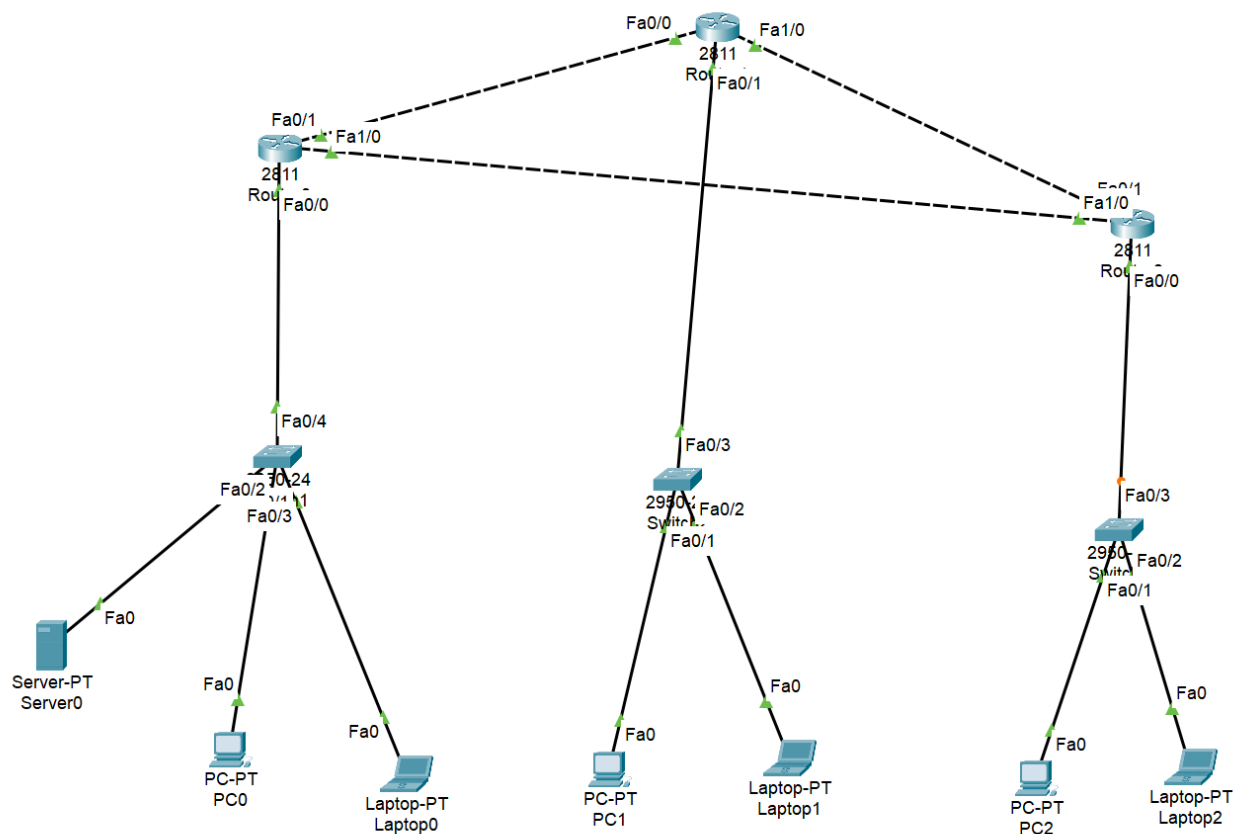
```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>
```

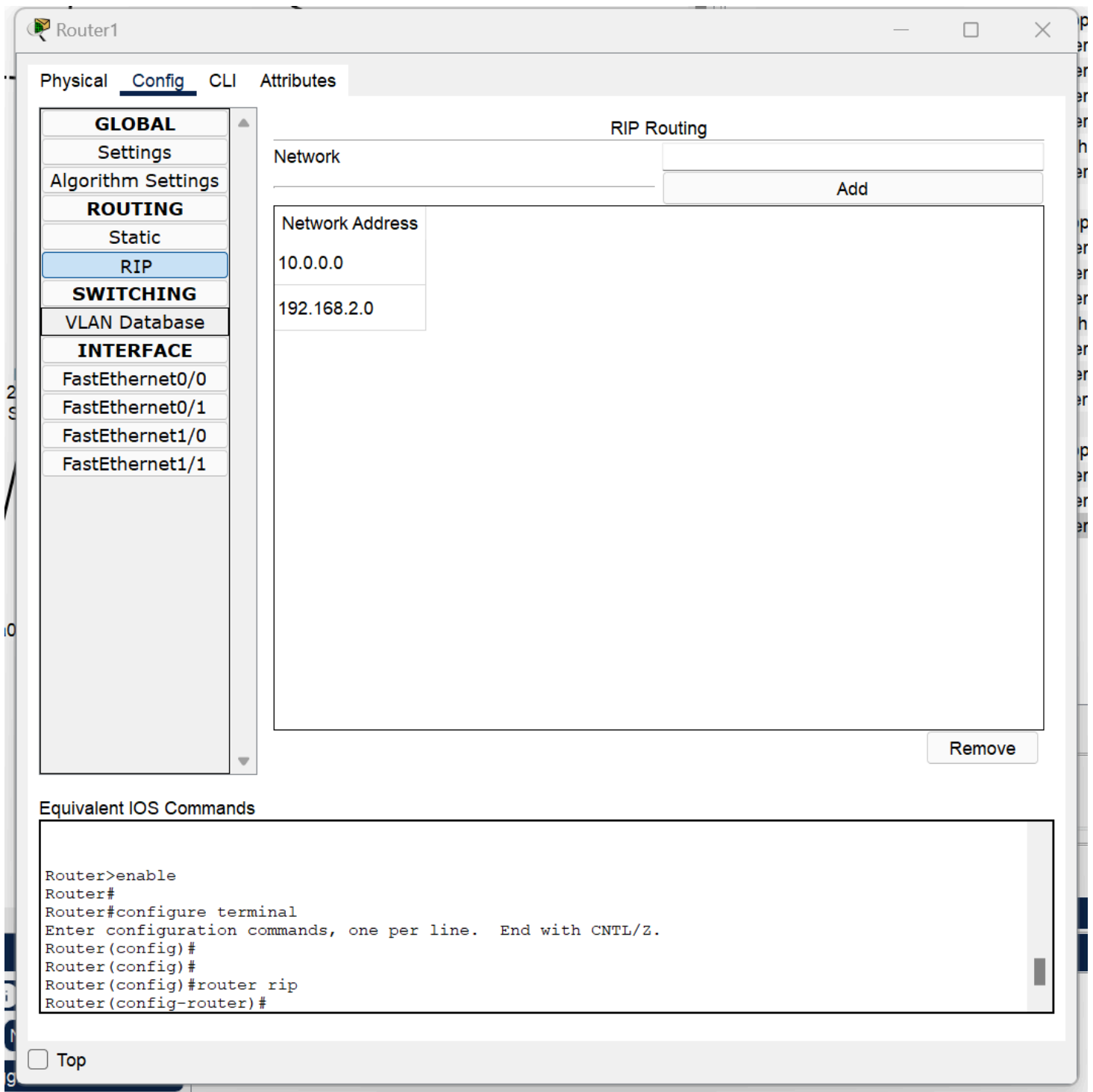
任务五

使用RIP路由协议

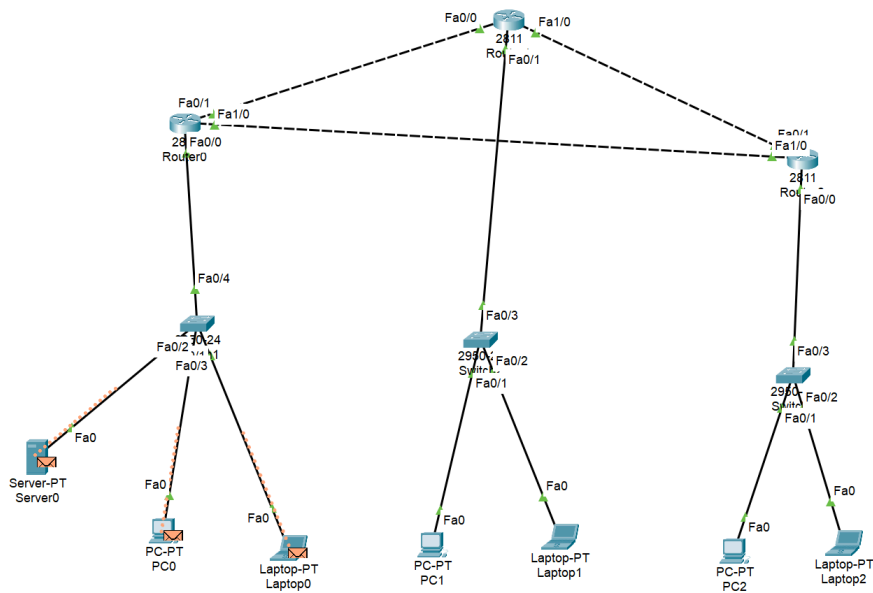
修改后的拓扑如下



以router2的配置为例，需要配置RIP协议



进行仿真，可见router0的数据包可以不经过router1直接到达router2（图中的router0为题目中的router1）



Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	1.302	--	Router2	RIPv1
	1.302	--	Router2	RIPv1
	1.302	--	Router2	RIPv1
	1.303	Router2	Switch3	RIPv1
	1.303	Router2	Router1	RIPv1
	1.303	Router2	Router0	RIPv1
	1.304	Switch3	PC2	RIPv1
	1.304	Switch3	Laptop2	RIPv1
	5.538	--	Router1	RIPv1
	5.538	--	Router1	RIPv1
	5.538	--	Router1	RIPv1
	5.539	Router1	Router0	RIPv1
	5.539	Router1	Switch2	RIPv1
	5.539	Router1	Router2	RIPv1
	5.540	Switch2	PC1	RIPv1
	5.540	Switch2	Laptop1	RIPv1
	22.744	--	Router0	RIPv1
	22.744	--	Router0	RIPv1
	22.744	--	Router0	RIPv1
	22.745	Router0	Switch1	RIPv1
	22.745	Router0	Router1	RIPv1
	22.745	Router0	Router2	RIPv1
Visible	22.746	Switch1	Server0	RIPv1
Visible	22.746	Switch1	PC0	RIPv1
Visible	22.746	Switch1	Laptop0	RIPv1

Reset Simulation
☒ Constant Delay

Play Controls

⏮ ⏪ ⏩ ⏭

凯撒的观点存在问题，当前可以将RIP作为路由协议，但是RIP协议的限制是最大跳数为15，与终端的数目无关。

Bonus

enable secret存储的密码是通过MD5加密的，可以通过 `show running-config` 查看加密后的密码。在更高的版本，还可以指定用加密程度更高的SHA-256加密算法