计14 汪隽立 2021012957

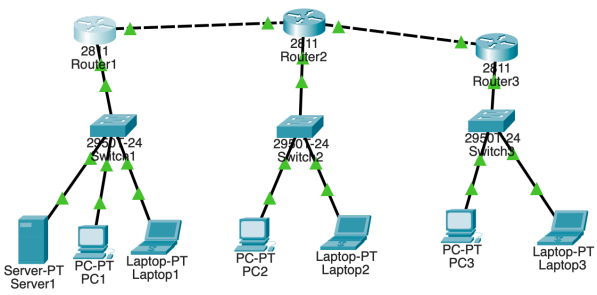
Lab1 实验报告

1. 破旧的莎草纸

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	**1**0.0.2.2	/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

2. “一天建起的罗马城”

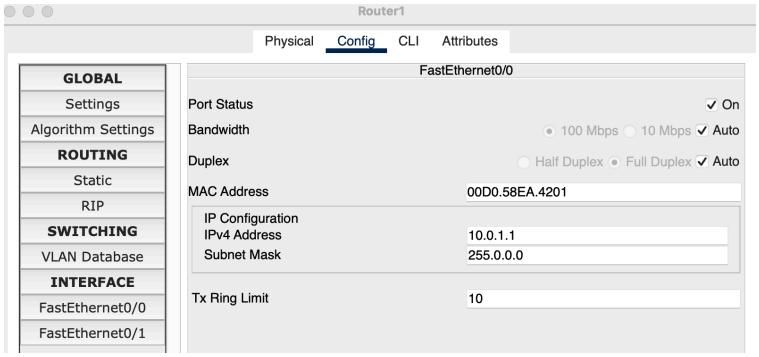
网络拓扑图

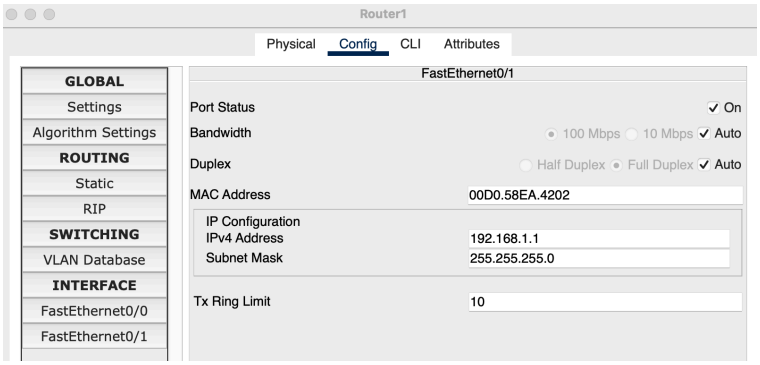


各路由器端口配置

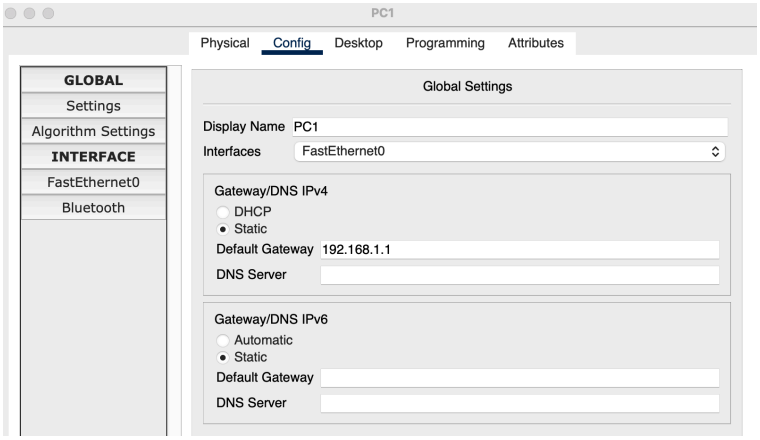
以**元老院子网为例，展示路由器及PC的配置**（为了节省报告的空间，元老院的服务器、Laptop，以及其他子网配置类似）：

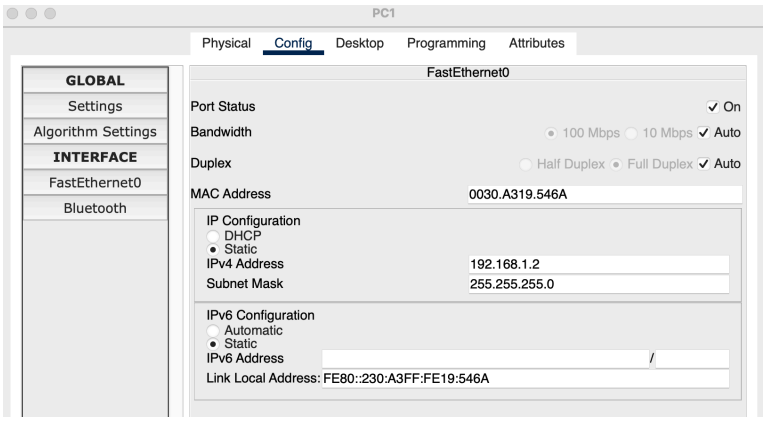
- Router1



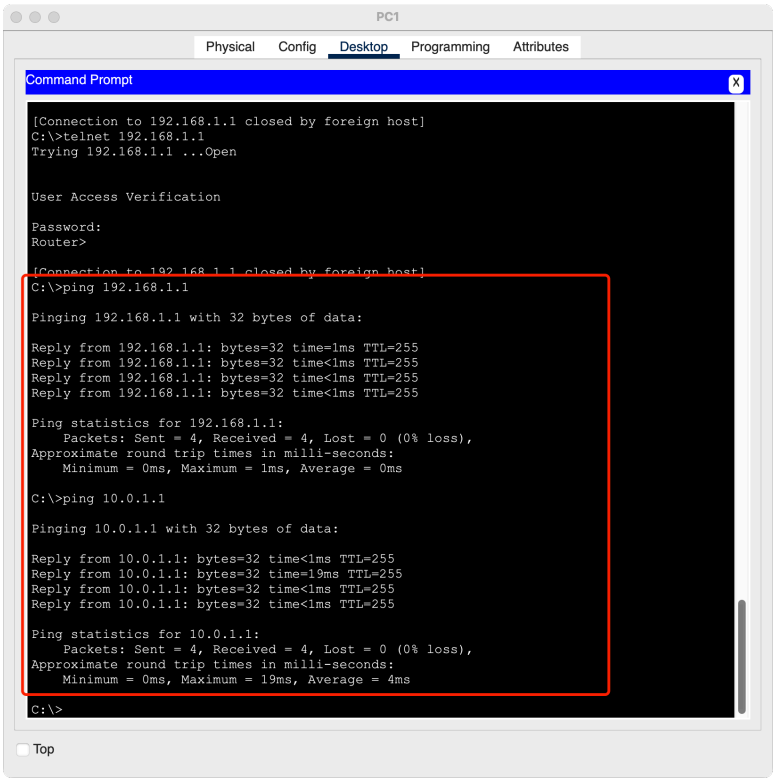


- PC1

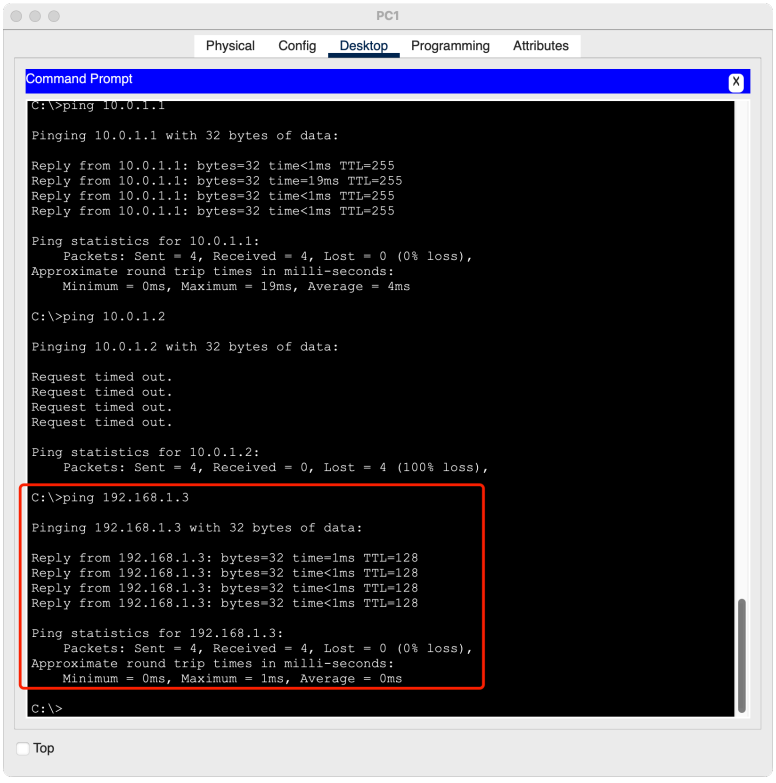




然后，我们便可以在PC1上尝试Ping路由器：



也可以ping通同一子网的其他设备（如Server1）：



3. 要点防卫

`YHQL, YLGL, YLFL`是加密后的`VENI, VIDI, VICI` (I came, I saw, I conquered)，加密方式是Caesar密码的加密方式 ($c = (m + 3) \mod 26$)。

与作业要求的对应关系一致，将**Router1**的三个密码设置为（且都为密文储存）：

```
password1=venividivici
password2=VENIVIDIVICI
password3=VeniVidiVici
```

利用`show running-config`，可以看到：

```
!
!
enable secret 5 $1$mERr$KFV/oW/sAldSseZvEUESY0
!
!
```

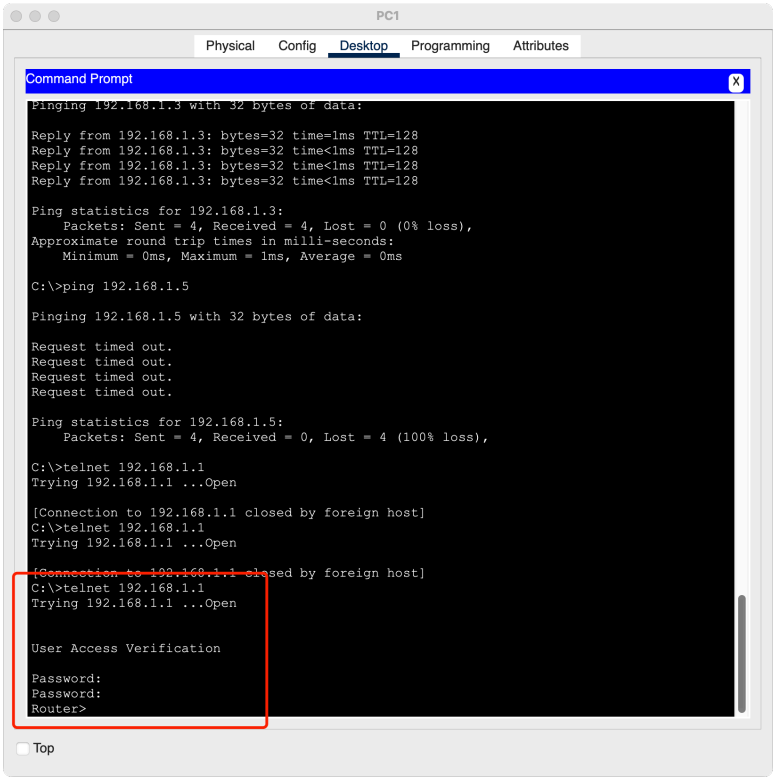
```
!
line con 0
 password 7 08374940000F0C131B1D050723
 login
!
line aux 0
!
line vty 0
 password 7 08174940002F0C131B3D050723
 login
line vty 1 4
 login
!
```

利用Console登陆Router1时，需要输入密码：

```
User Access Verification

Password:
```

利用telnet访问Router1时，需要输入密码：



开启特权模式时，也需要输入密码：

```
Router>enable
Password:
Router#
```

如果路由器配置文件可能泄露，你的设置是否有所变化?

由于配置文件中的密码是以密文存储的，故（在密文不被破译的情况下），我们的设置可以不变。

复杂度分析

首先，字条上的内容经过RSA解密后是：“**注意题目中的混合，考虑容斥原理**”。

- 总长六位的纯数字密码
  - 每个位有10种可能，故总共是10^6个时间单位。
- 总长六位的混合有数字及小写字母的密码
  - 总长六位的只有数字的密码共10^6个可能，总长六位的只有小写字母的密码共26^6个可能，总长六位的由数字和小写字母的密码（即每一位既可以是数字，也可以是小写字母）共36^6个可能。
  - 前两个集合不相交，故总长六位的混合有数字及小写字母的密码共有$36^6-10^6-26^6=1866866550\approx1.87\times10^9$种可能。
- 总长六位的混合有数字、大写字母、小写字母的密码
  - 记$U=$总长为六位的由数字、大写字母、小写字母的密码（每一位有62种可能），$|U|=62^6$。
  - 记$S=$总长六位的混合有数字、大写字母、小写字母的密码，$A=$总长六位的不含数字的密码，$B=$总长六位不含大写字母的密码，$C=$总长六位不含小写字母的密码。$|S|=|U|-|A\cup B\cup C|$。
  - 由容斥原理，

$$\begin{aligned}|A\cup B\cup C|&=|A|+|B|+|C|-|A\cap B|-|A\cap C|-|B\cap C|+|A\cap B\cap C|\\&=52^6+36^6+36^6-26^6-26^6-10^6+0=23505342784\end{aligned}\tag{1}$$

  - 故$|S|=62^6-23505342784=33294892800\approx3.33\times10^{10}$。
- 总长八位的混合有数字、大写字母、小写字母的密码
  - 计算方式与上一样，$|S|=62^8-(52^8+36^8+36^8-26^8-26^8-10^8)=159655911367680\approx1.60\times10^{14}$。

4.“三权”间的初步通信

为Router1增加的静态路由为:

```
1  ip route 192.168.2.0 255.255.255.0 10.0.1.2
2  ip route 192.168.3.0 255.255.255.0 10.0.1.2
```

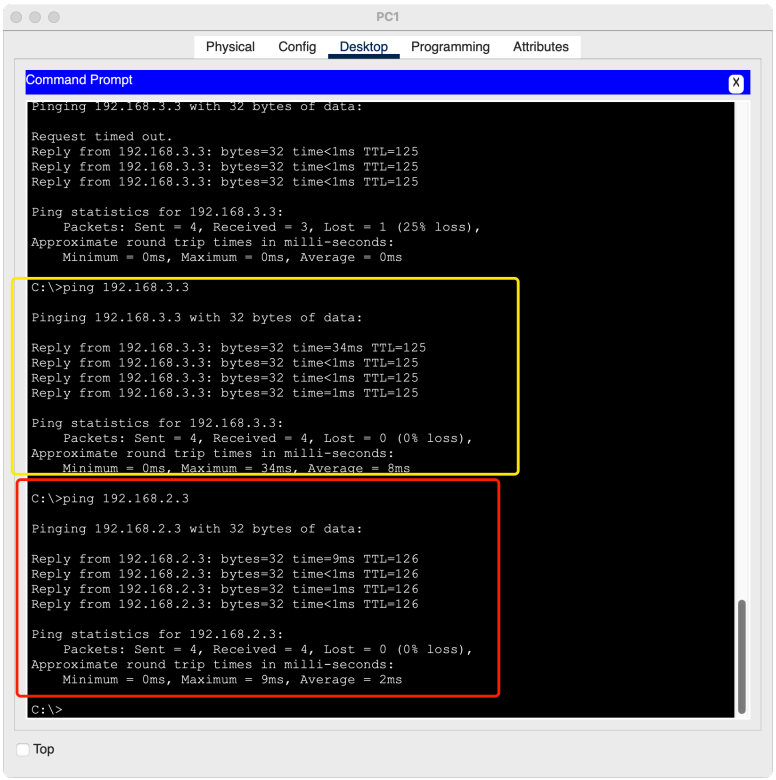
Router2:

```
ip route 192.168.1.0 255.255.255.0 10.0.1.1
ip route 192.168.3.0 255.255.255.0 10.0.2.1
```

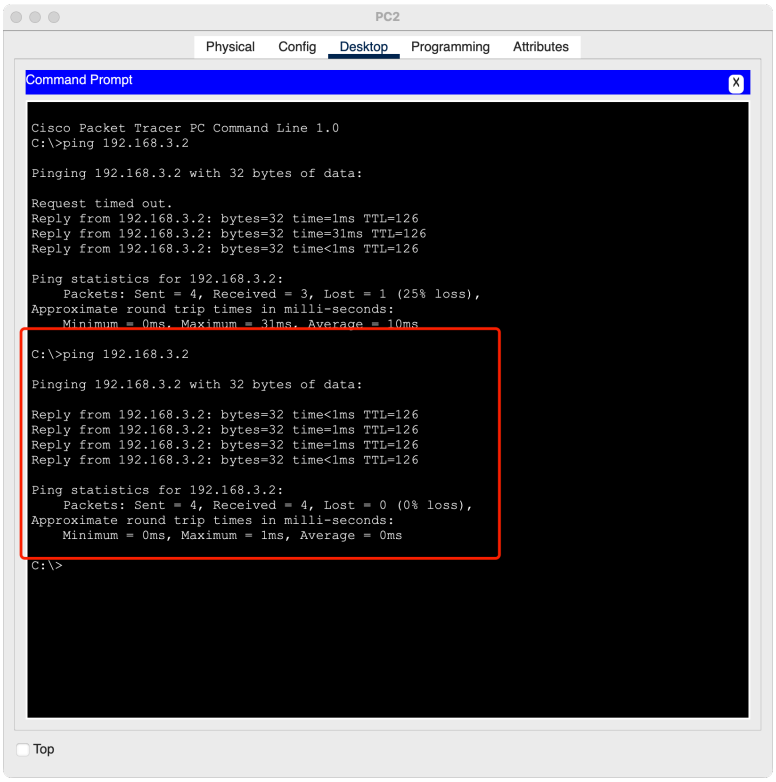
Router3:

```
ip route 192.168.1.0 255.255.255.0 10.0.2.2
ip route 192.168.2.0 255.255.255.0 10.0.2.2
```

元老院和执政官首府 & 部族议会所：



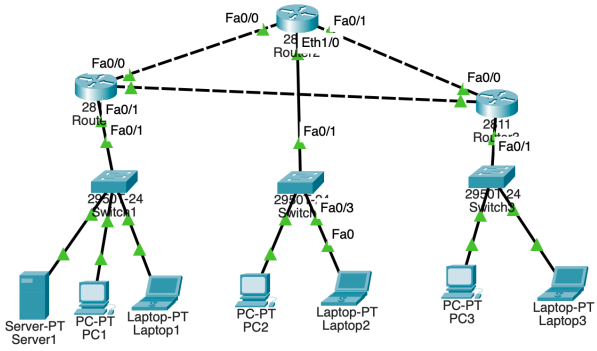
执政官首府和部族议会所：



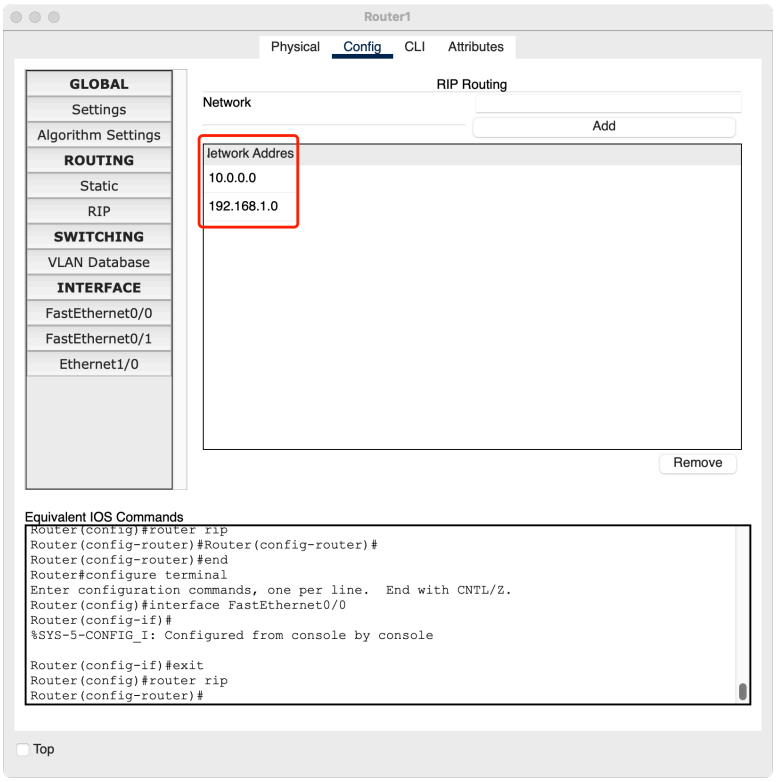
5. 三权间的高效通信

我最终决定选择**动态**路由协议维护“共和国”目前的局域网。

拓扑结构



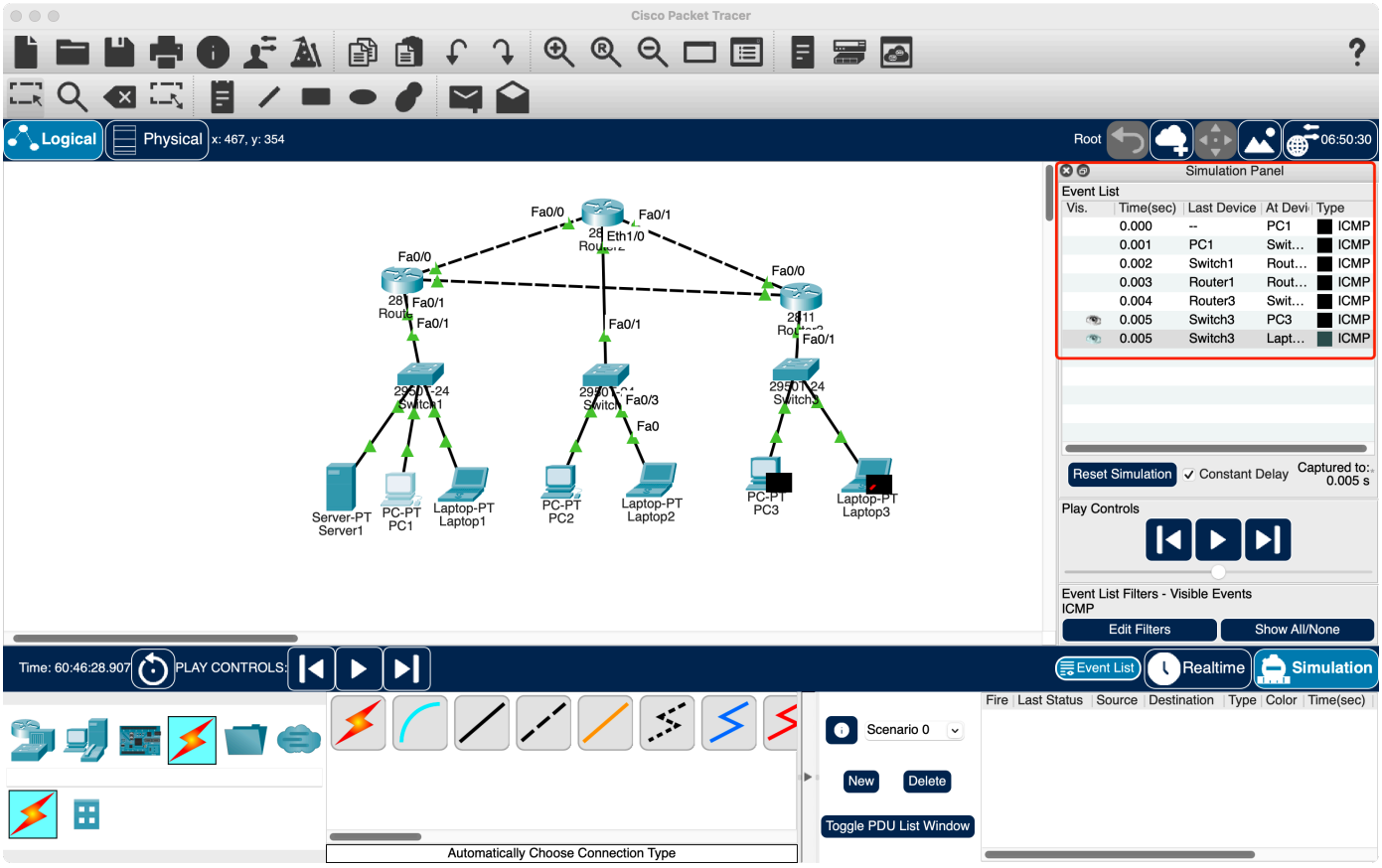
增加的动态路由设置如下（删去了先前的静态路由设置）：



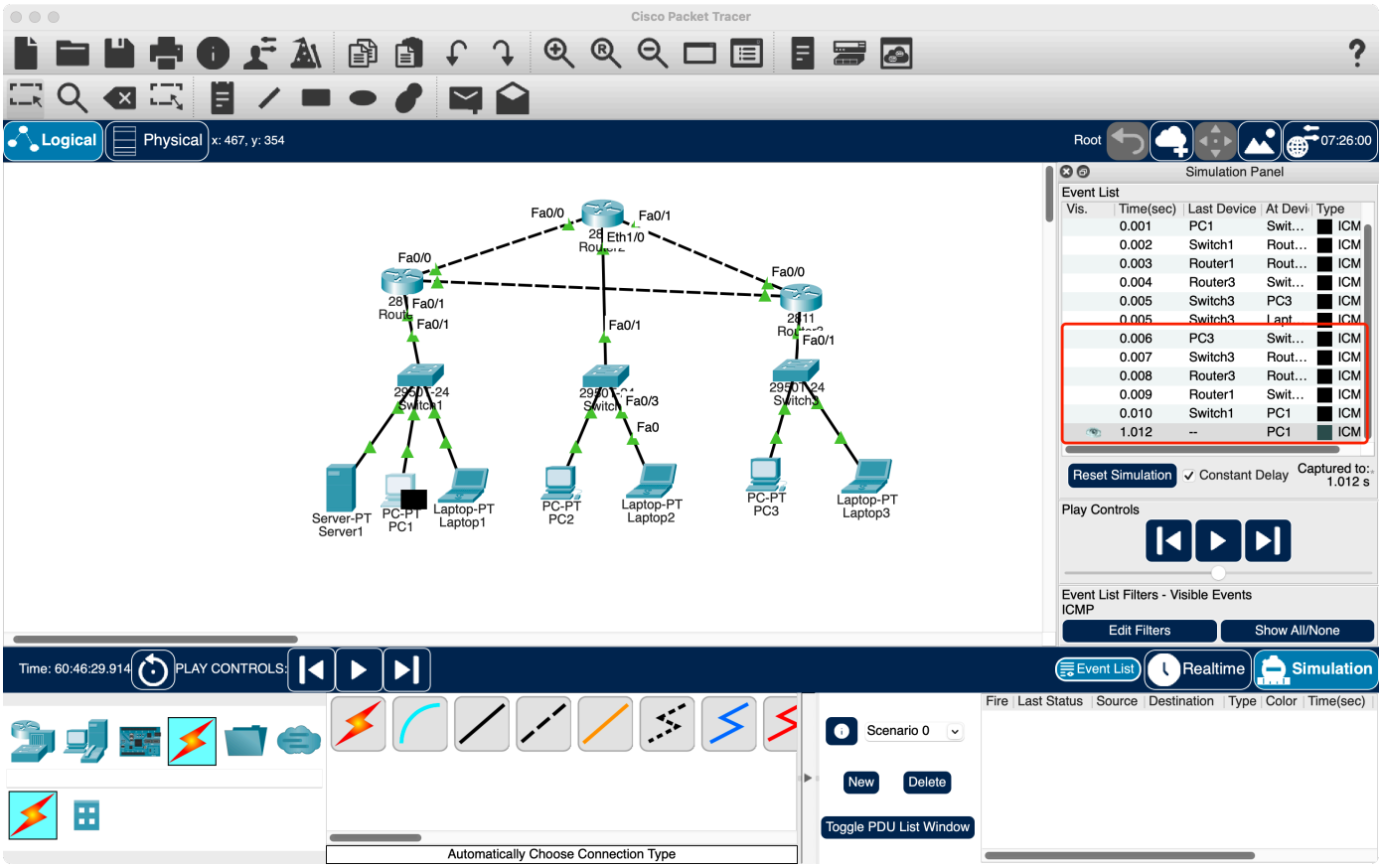
Router2, Router3类似。

实际路径

打开simulation mode之后，从192.168.1.2 ping 192.168.3.2，如下图：



可以看到，路径是PC1 -> Router1 -> Router3 -> PC3。从PC3发回来的包也是如此：



包的路径为PC3 -> Router3 -> Router1 -> PC1。

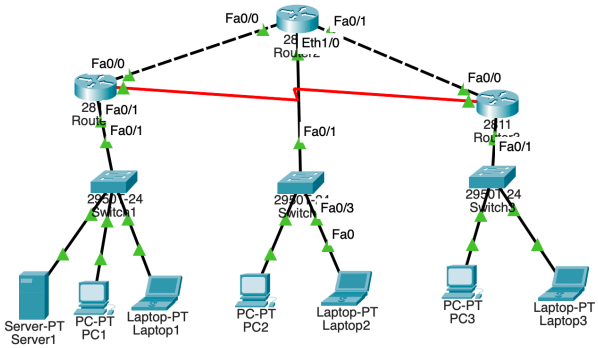
凯撒的观点

凯撒的观点存在问题：只要路径跳数小于16条，那么就可以使用RIP协议。这与总的设备数无关，只和经过的路由器数目有关。

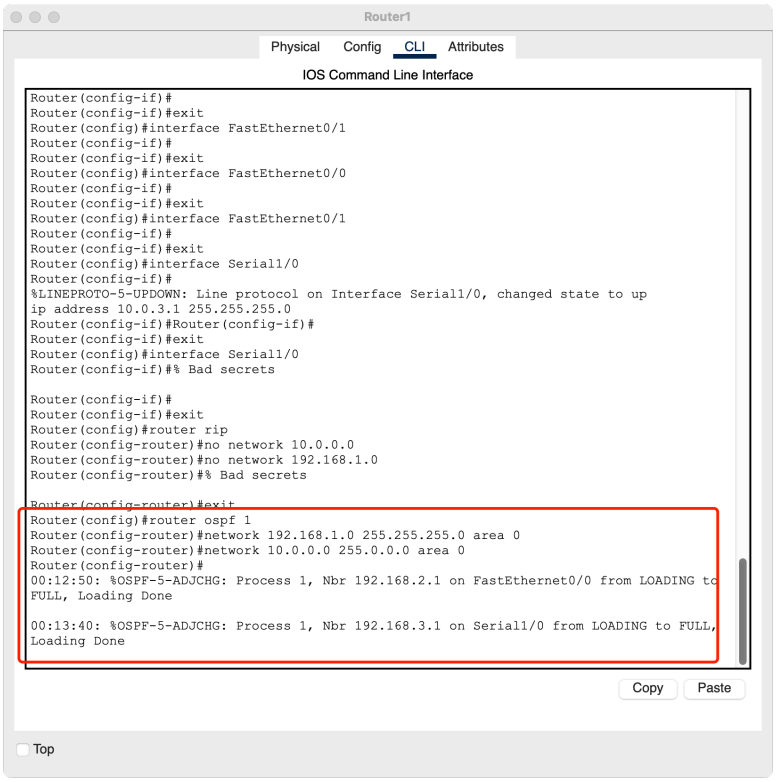
当前可以使用RIP作为路由协议，因为路由器数目为3，最长跳数不可能超过16。

Bonus：布鲁托的要求

我们利用OSPF技术实现这里的要求。首先，我们将连接Router1和Router3改为使用串口连接。

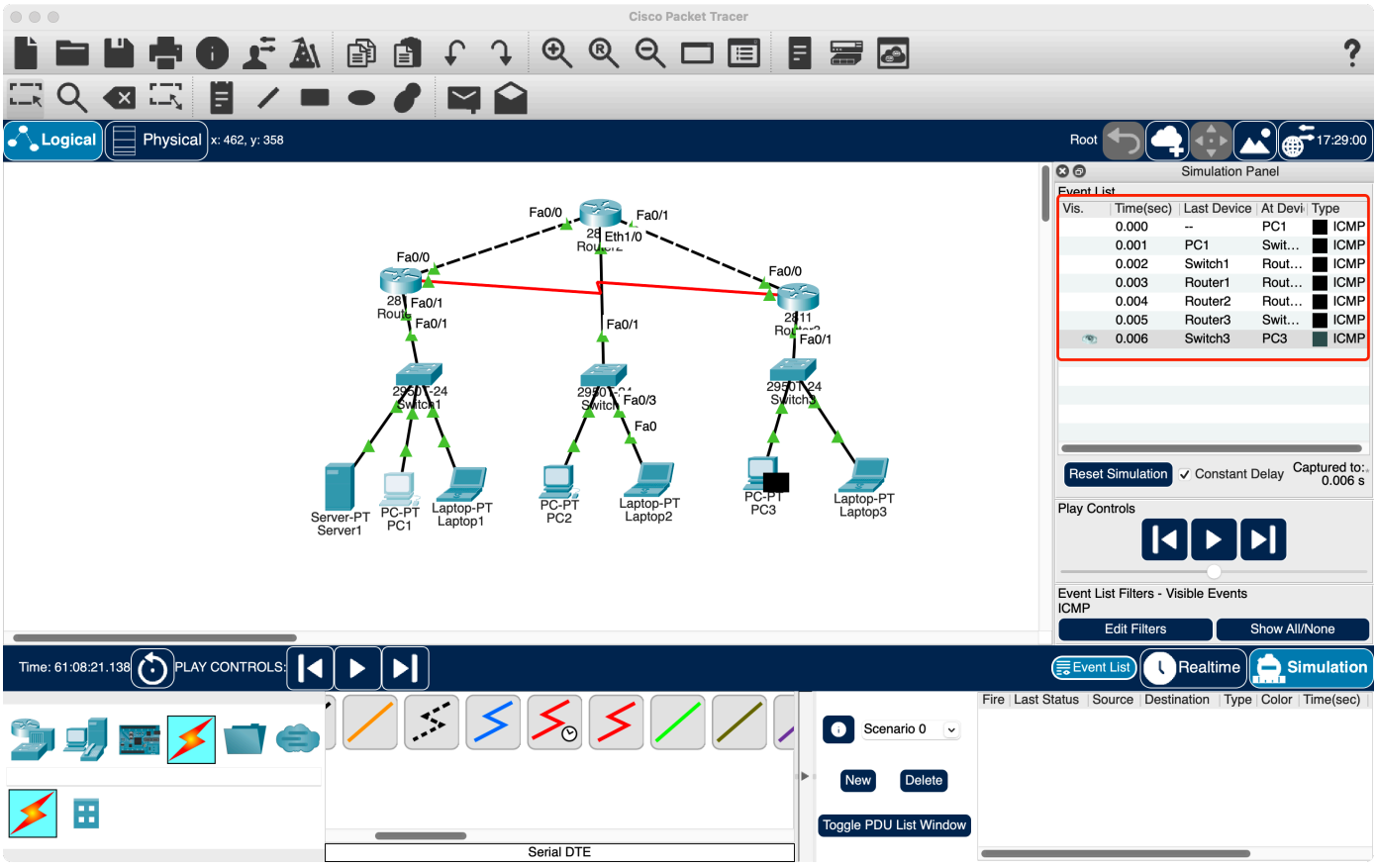


然后，我们对三个路由器都设置OSPF协议（RIP协议已删除）：



这里以Router1为例，其他两个路由器类似。

最后，我们观察从PC1 ping PC3的过程：



可以看到，这时包的路线是PC1 -> Router1 -> Router2 -> Router3（而不是直接从Router1到Router3），执政官首府可以获取元老院和部族会议所之间的消息。