计算机网络安全技术 · 实验1报告

计01　容逸朗　2020010869

实验内容

任务 1：破旧的莎草纸（3'）

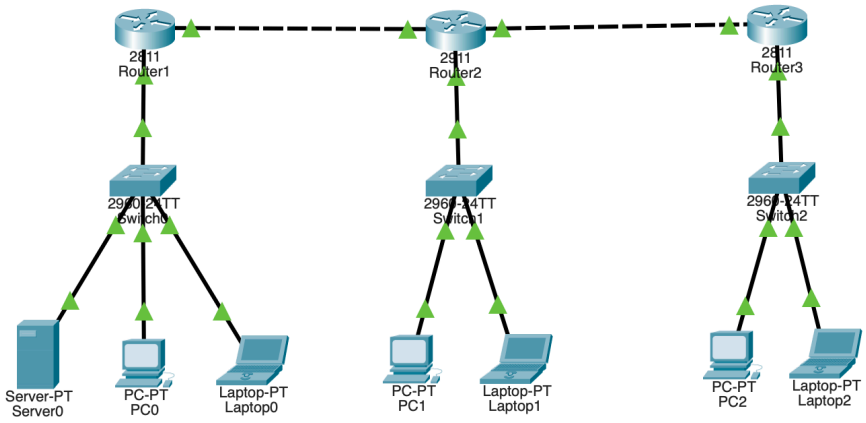
由于保留字段并不包括 `20.0.2.2/24`，因此将对应的 IP 更改为合法的 A 类私有字段 `10.0.2.2/24`。

更正後的 IP 方案如下所示，其中用红色字标记的文字是需要填充或更正的部分：

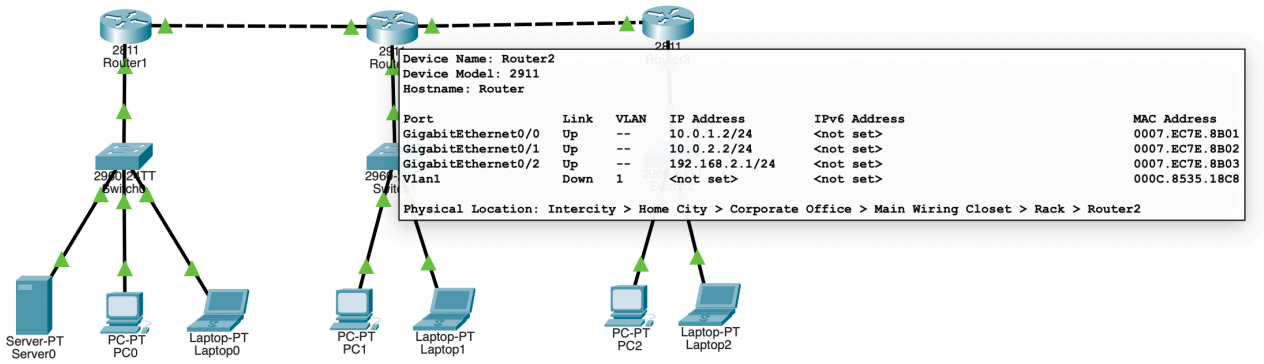
Device	Port	IP	Mask	Gateway
Router1	端口1	192.168.1.1	/24	-
	端口2	10.0.1.1	/24	-
Router2	端口1	10.0.1.2	/24	-
	端口2	10.0.2.2	/24	-
	端口3	192.168.2.1	/24	-
Router3	端口1	10.0.2.1	/24	-
	端口2	192.168.3.1	/24	-
PC1	端口1	192.168.1.2	/24	192.168.1.1
PC2	端口1	192.168.2.2	/24	192.168.2.1
PC3	端口1	192.168.3.2	/24	192.168.3.1
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 2：“一天建起的罗马城”（2'）

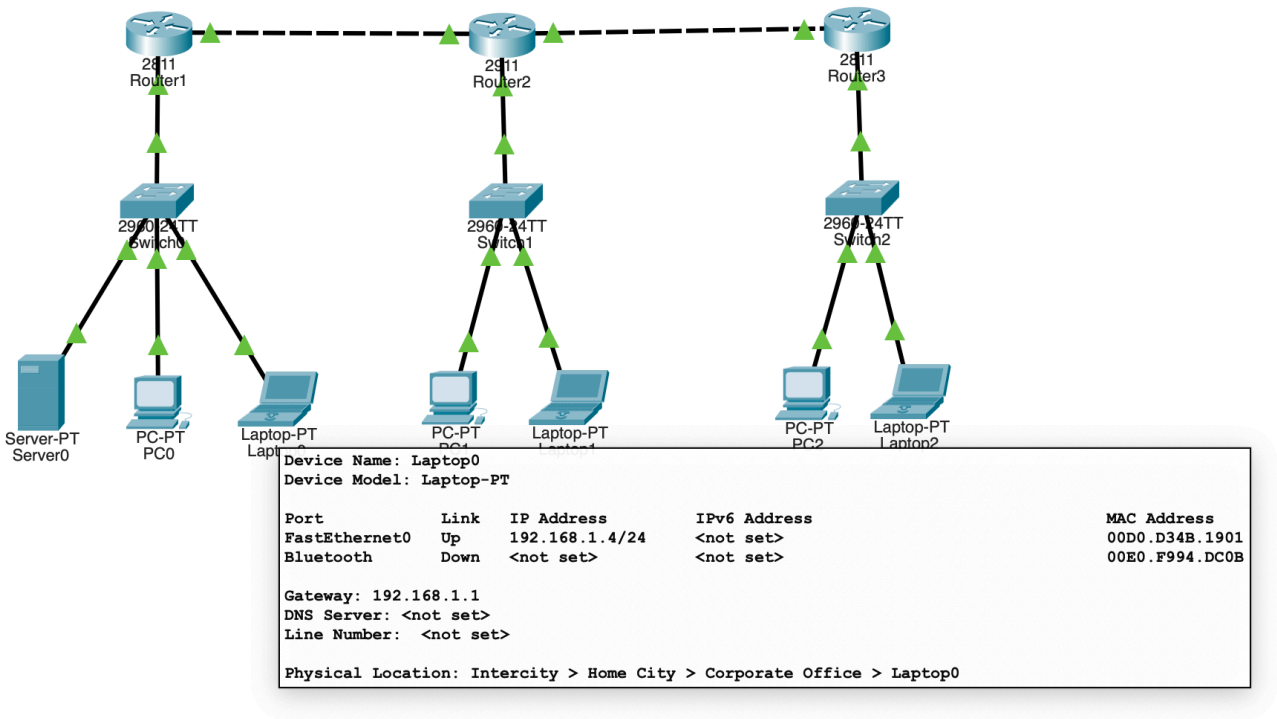
整体拓扑图



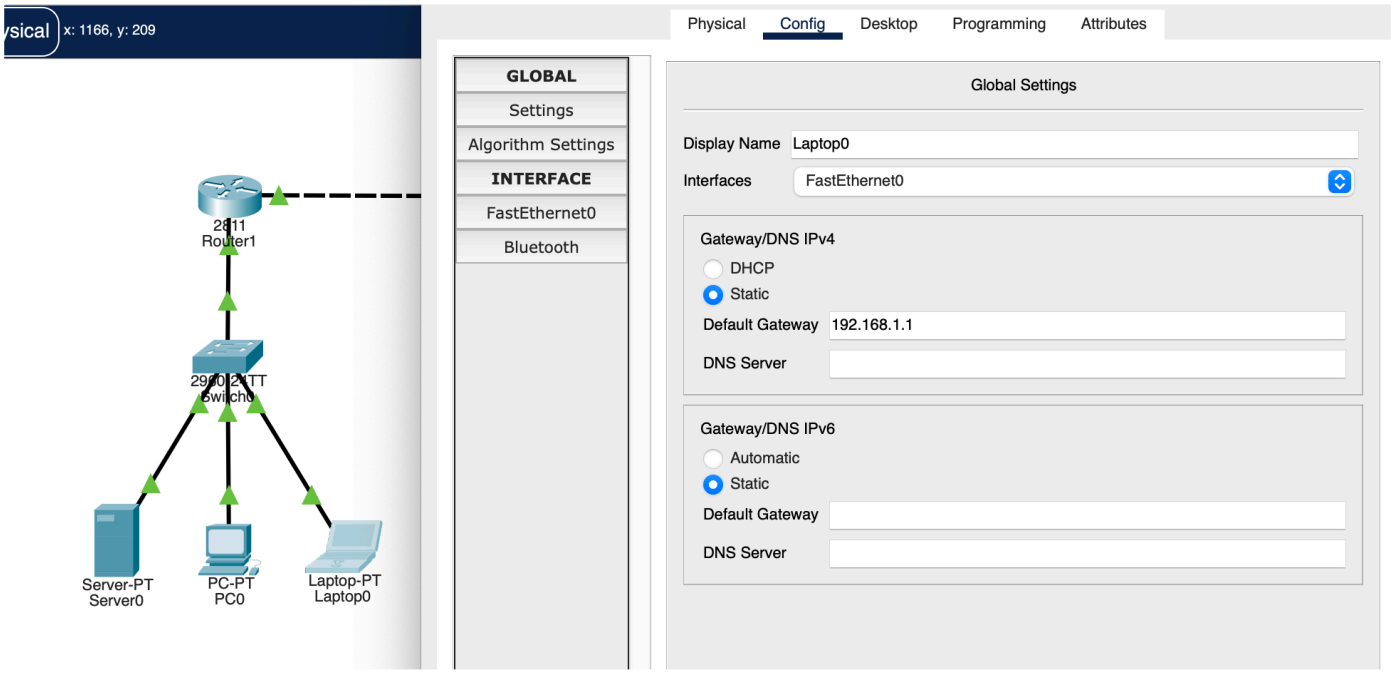
路由器端口配置



终端设备端口配置



终端设备网关配置



任务 3：要点防卫（6'）

密码设计

> 他留下一张莎草纸，上面写着一段奇怪的文字“YHQL, YLGL, YLFL”。同时凯撒也交代给你一句话，“如果无法离开迷雾，就朝着扑克牌里我面庞的方向走三步”。凭借着你在计算机网络安全技术课上学到的知识，你似乎明白了这段文字背后的含义。

由此段提示可知，这句话是经过凯撒加密，且偏移量为向左 3 位的，故对应的密文如下：

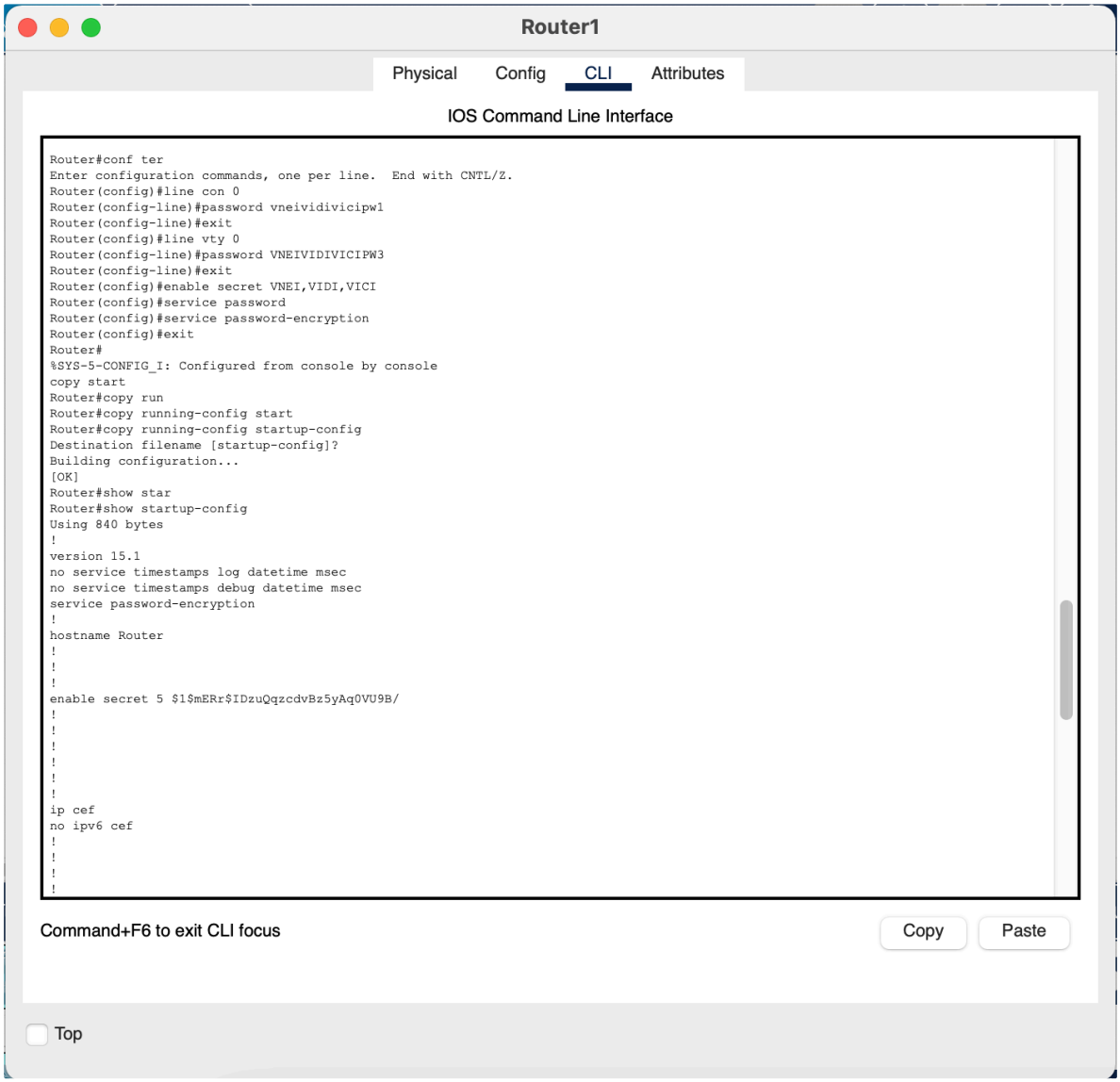
- 明文：YHQL,YLGL,YLFL
- 密文：VENI,VIDI,VICI

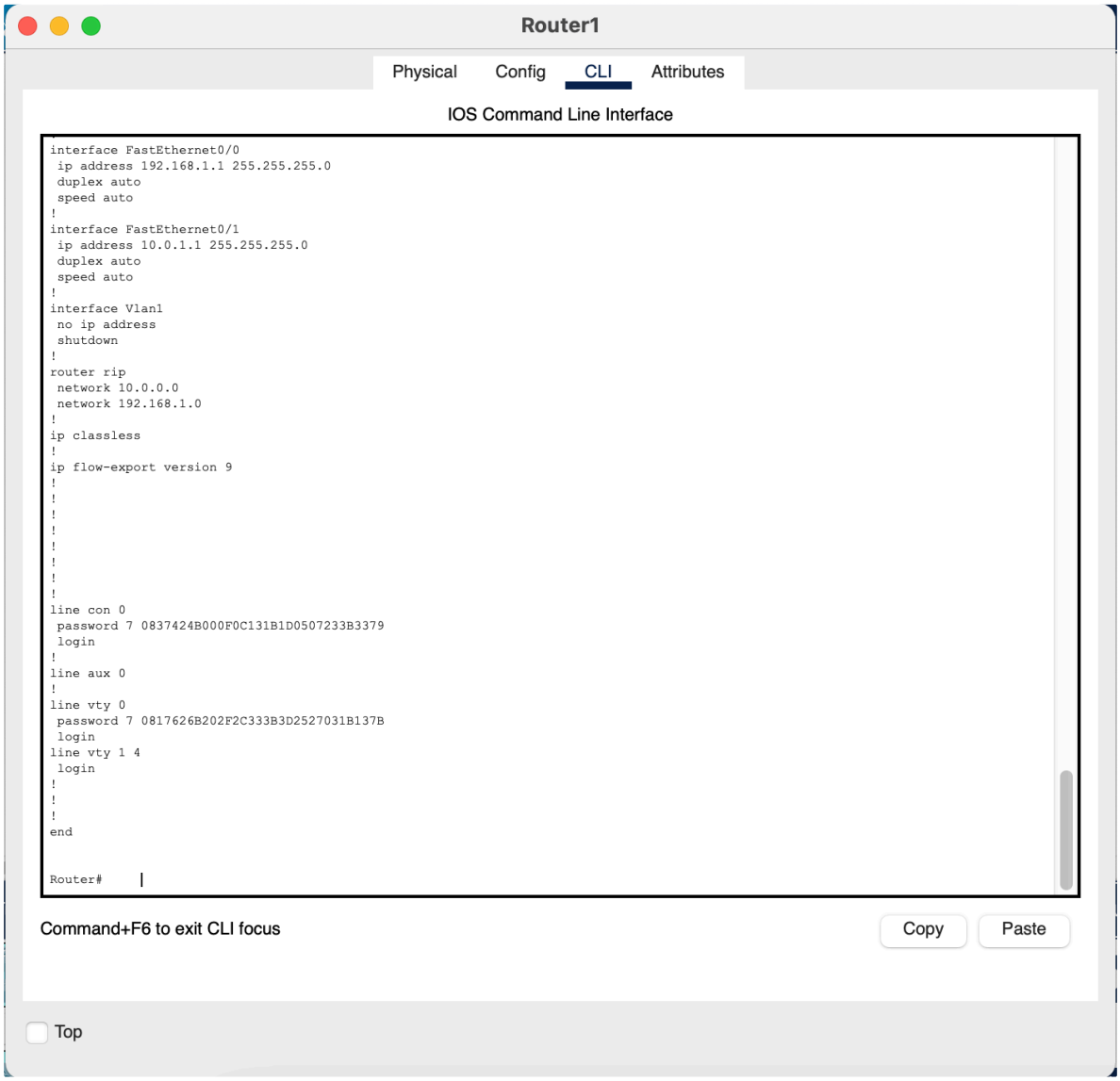
根据上面的文字，设计出的密码如下所示：

- console登录密码：vneividivicipw1
- 进入特权模式密码：VNEI,VIDI,VICI
- telnet登录密码：VNEIVIDIVICIPW3

密码配置

具体配置的截图如下：





由上图可见，我首先配置了上一部分设计的密码，然后使用 `service password-encryption` 加密密码，在这里：

- `console, telnet` 登录密码使用思科加密方式 7（双向密码加密、易破解）
- 进入特权模式的密码采用思科加密方式 5（复杂密文加密）

> 如果路由器配置文件可能泄露，你的设置是否有所变化？

应该将所有密码的加密方式设为加密方式 5（复杂密文加密）

密码分析

> 试分析，当你使用如下四种复杂程度的密码进行配置时，攻击者进行暴力破解时时间需求的变化。(假设暴力尝试一次密码的时间为1)

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：$36^6 = 2.176 \times 10^9$
3. 总长六位的混合有数字、大写字母、小写字母的密码：$62^6 = 5.680 \times 10^{10}$
4. 总长八位的混合有数字、大写字母、小写字母的密码：$62^8 = 2.183 \times 10^{14}$

由此可知，攻击者破解 2 所需的时间是 1 的 2000 倍，破解 3 需要 5×10^4 倍时间，破解 4 则需要花费 2×10^8 倍的时间。

（注：对于 2, 3, 4 而言，这里也计算了只有数字出现或只有字母出现的密码）

任务 4："三权"间的初步通信（4'）

本任务需要配置静态路由表。

路由表设计

在 Router1 加入如下规则：

```
ip route 192.168.2.0 255.255.255.0 10.0.1.2
ip route 192.168.3.0 255.255.255.0 10.0.1.2
```

注 1：由于 192.168.1.0/24 和 10.0.1.0/24 是直连的，所以在此处不再加入相关规则，下面的设置同理。

注 2：由于只要求三个权力部门能够相互通讯，因此没有加入连通另一个路由子网 10.0.2.0 的规则。

在 Router2 加入如下规则：

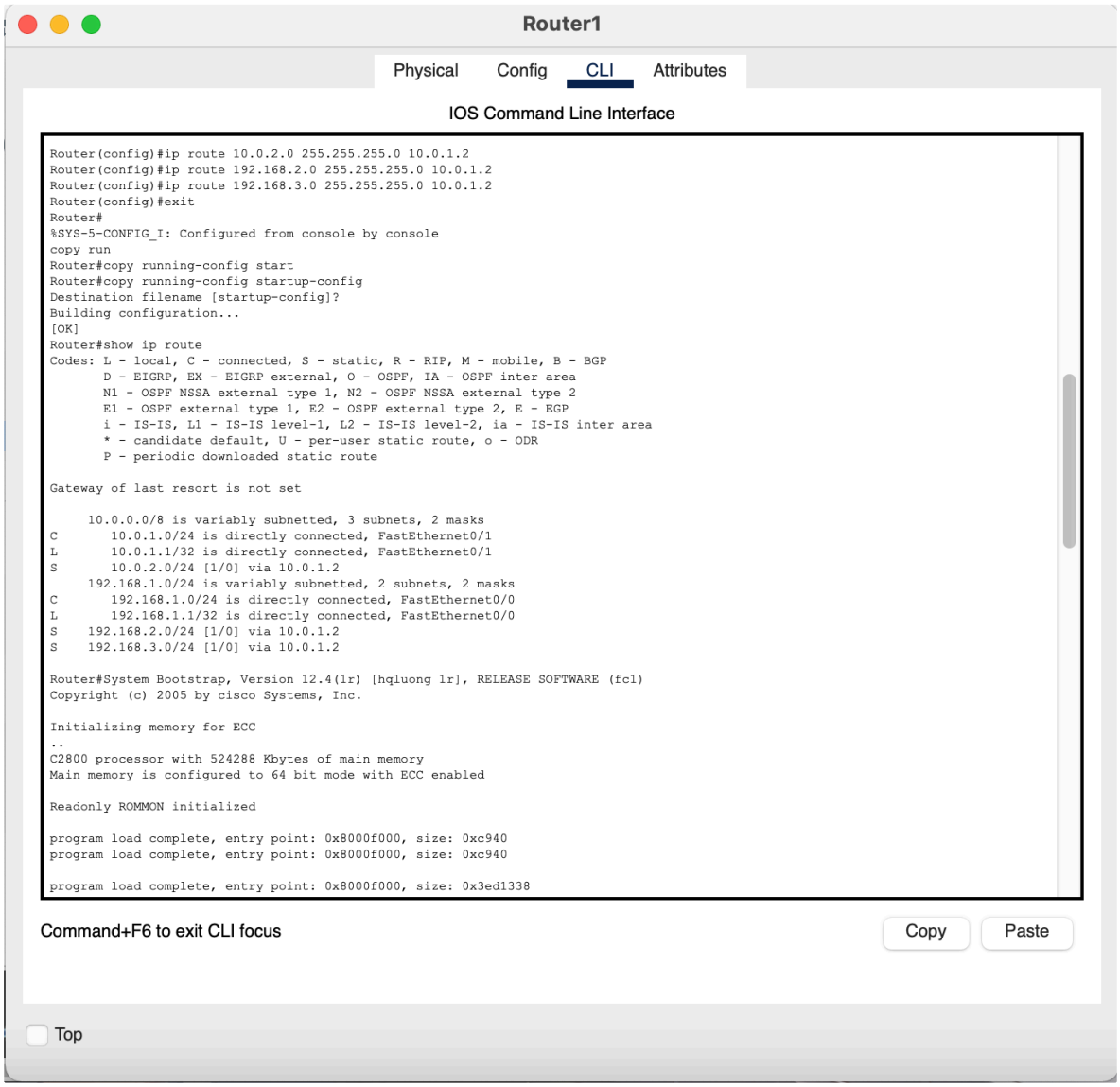
```
ip route 192.168.1.0 255.255.255.0 10.0.1.1
ip route 192.168.3.0 255.255.255.0 10.0.2.1
```

在 Router3 加入如下规则：

```
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
```

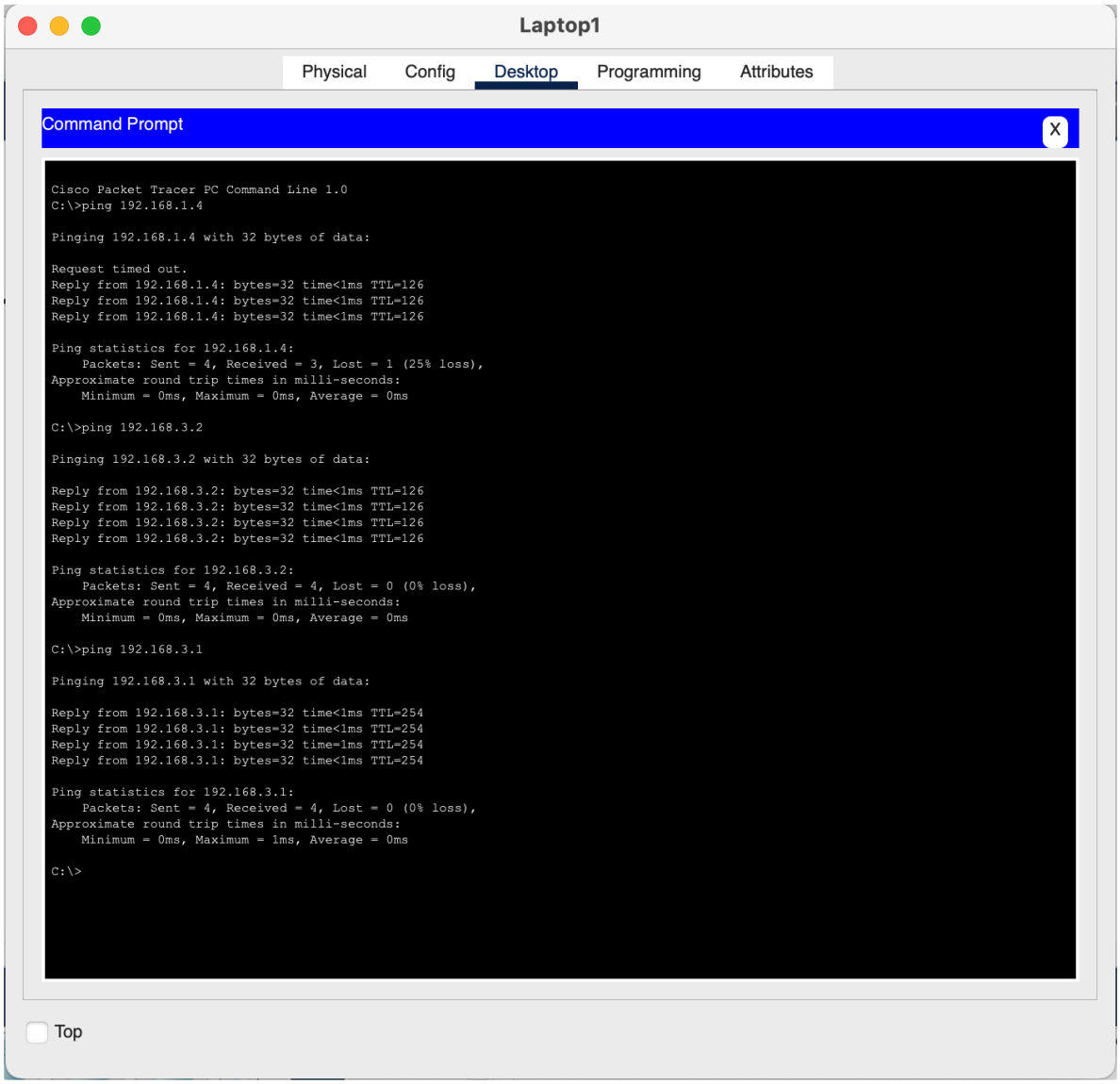
路由表配置

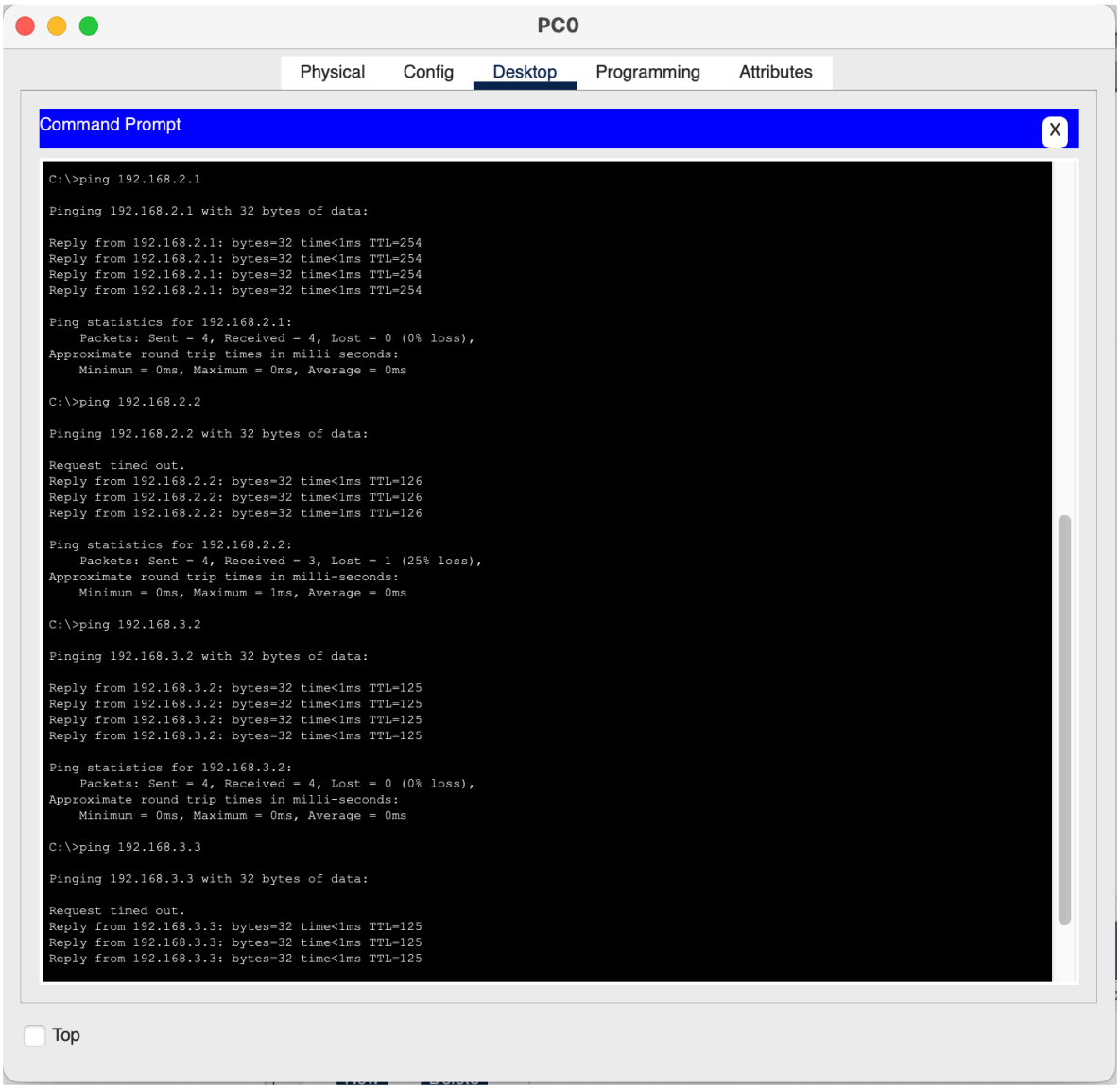
路由器 1 的配置介面及对应路由表如下：



连通性测试

分别从执政官首府的 Laptop（Laptop1）和元老院的 PC（PC0）向另外两个子网 ping

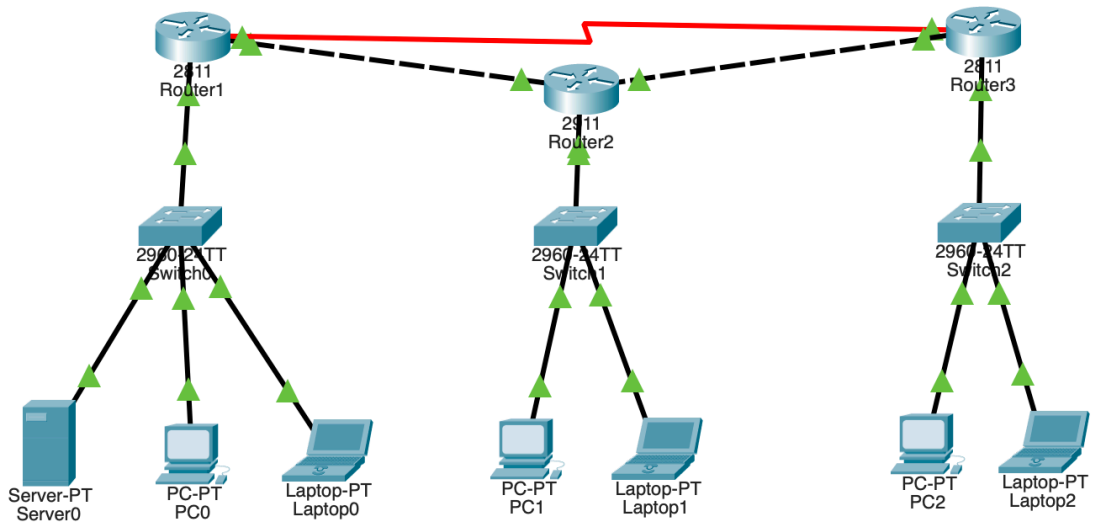

Laptop1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.4
Pinging 192.168.1.4 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.4: bytes=32 time<1ms TTL=126
Reply from 192.168.1.4: bytes=32 time<1ms TTL=126
Reply from 192.168.1.4: bytes=32 time<1ms TTL=126
Ping statistics for 192.168.1.4:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.3.2
Pinging 192.168.3.2 with 32 bytes of data:
Reply from 192.168.3.2: bytes=32 time<1ms TTL=126
Reply from 192.168.3.2: bytes=32 time<1ms TTL=126
Reply from 192.168.3.2: bytes=32 time<1ms TTL=126
Reply from 192.168.3.2: bytes=32 time<1ms TTL=126
Ping statistics for 192.168.3.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.3.1
Pinging 192.168.3.1 with 32 bytes of data:
Reply from 192.168.3.1: bytes=32 time<1ms TTL=254
Reply from 192.168.3.1: bytes=32 time<1ms TTL=254
Reply from 192.168.3.1: bytes=32 time=1ms TTL=254
Reply from 192.168.3.1: bytes=32 time<1ms TTL=254
Ping statistics for 192.168.3.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
Top



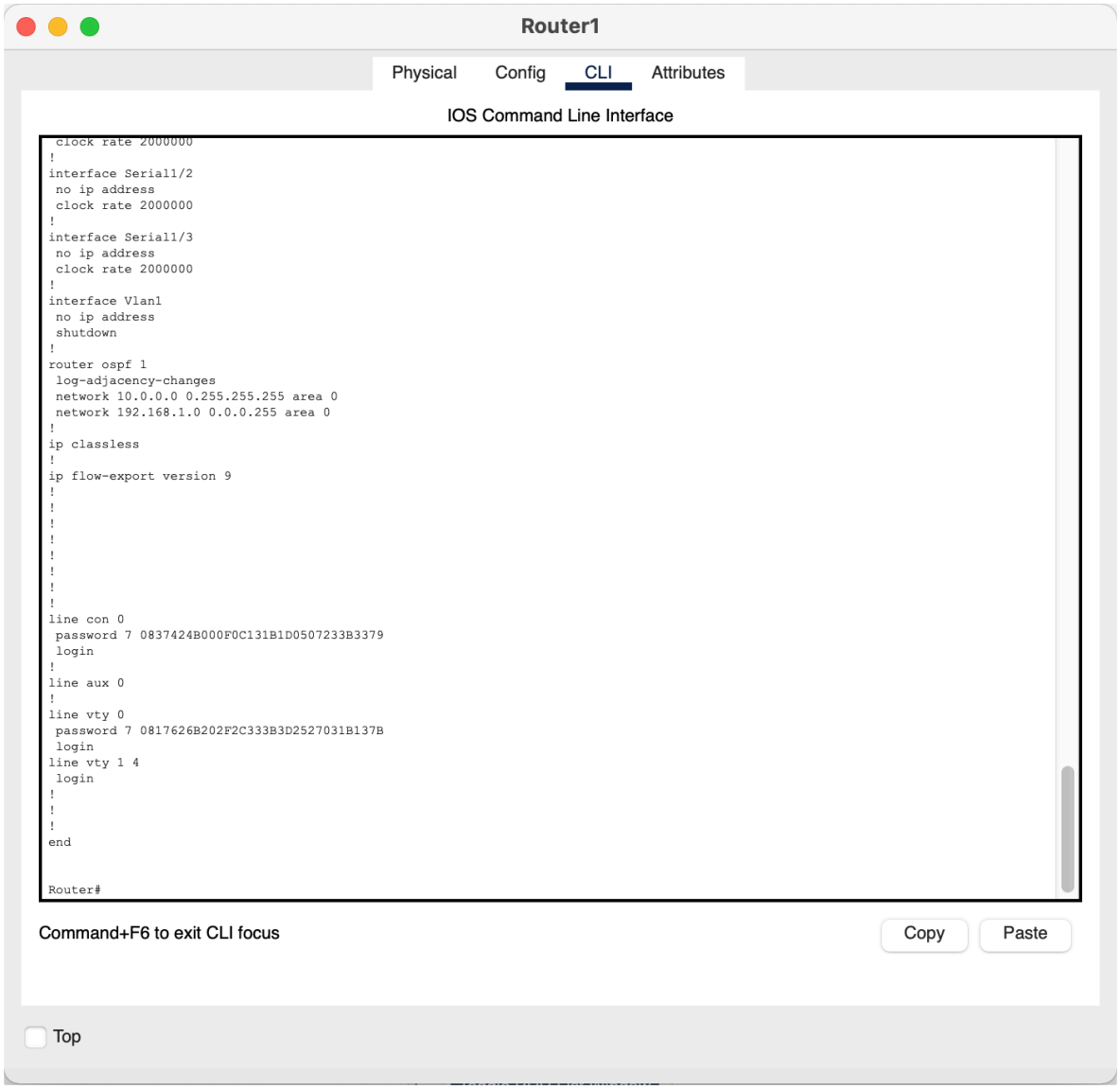
从上图可见，三个子网之间已经连通。

任务 5：“三权”间的高效通信（5'）

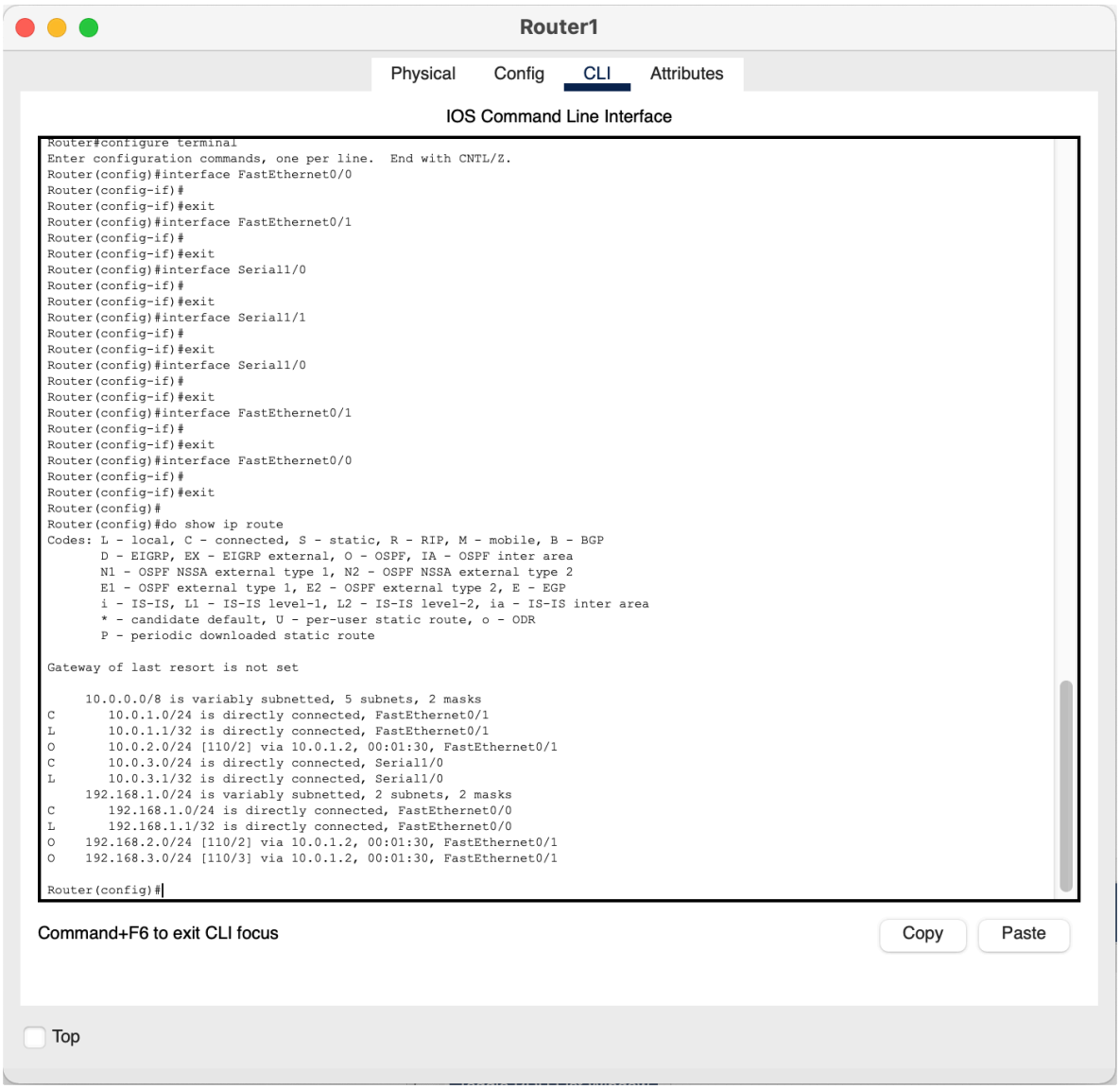
本任务中，我选择按布鲁图的思路配置动态路由，因此采用了 OSPF 路由协议来维护“共和国”目前的局域网。与任务 4 相比，Router1 和 3 之间新增了一条带宽很小的链路，最终的网络拓扑如下所示：



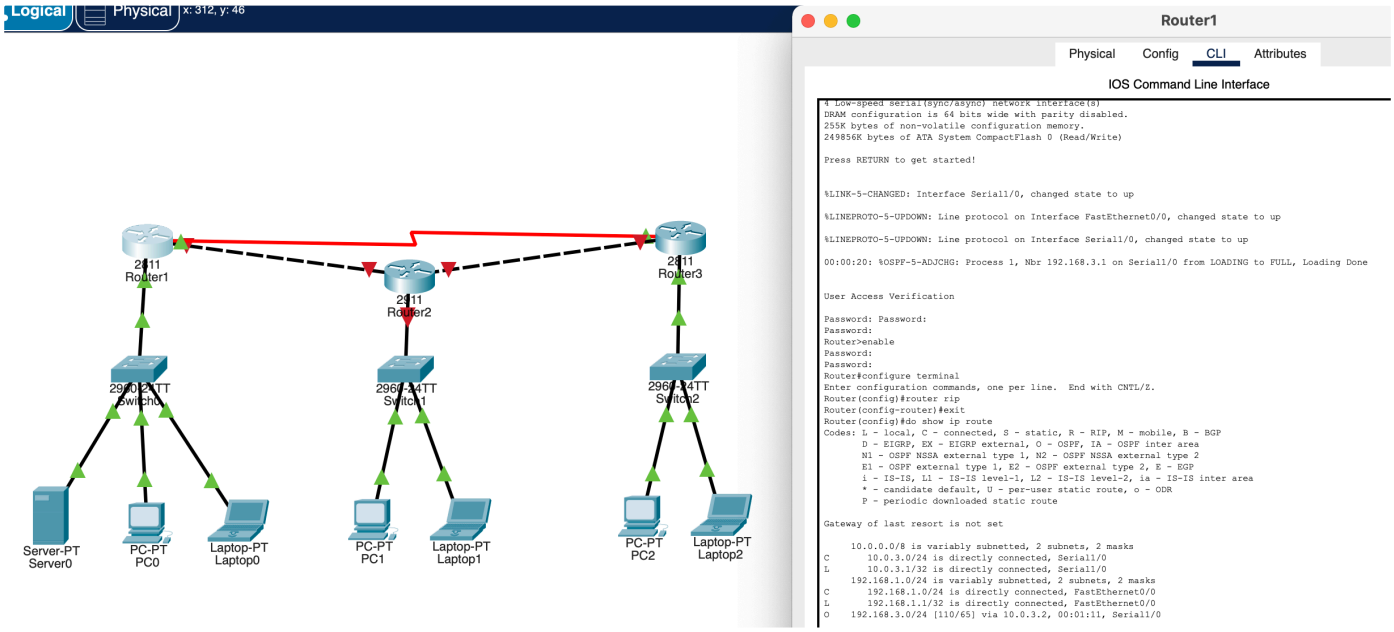
接下来为 Router1, 2, 3 配置 OSPF 协议，可以看到路由表已经成功创建：



此时检查 Router1 的路由表，可以看到所有流量都不会直接传输到 Router3，而是只会转发到 Router2：

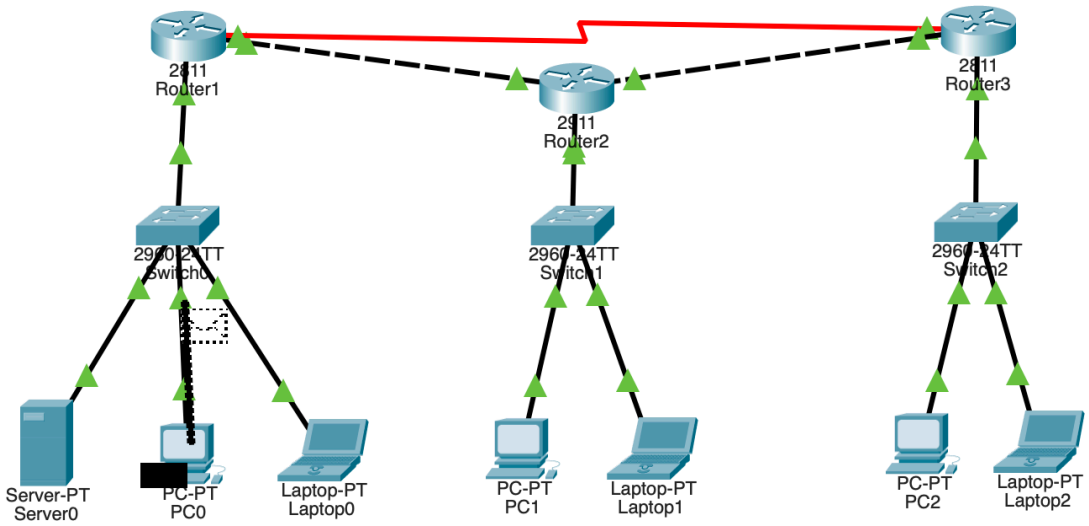


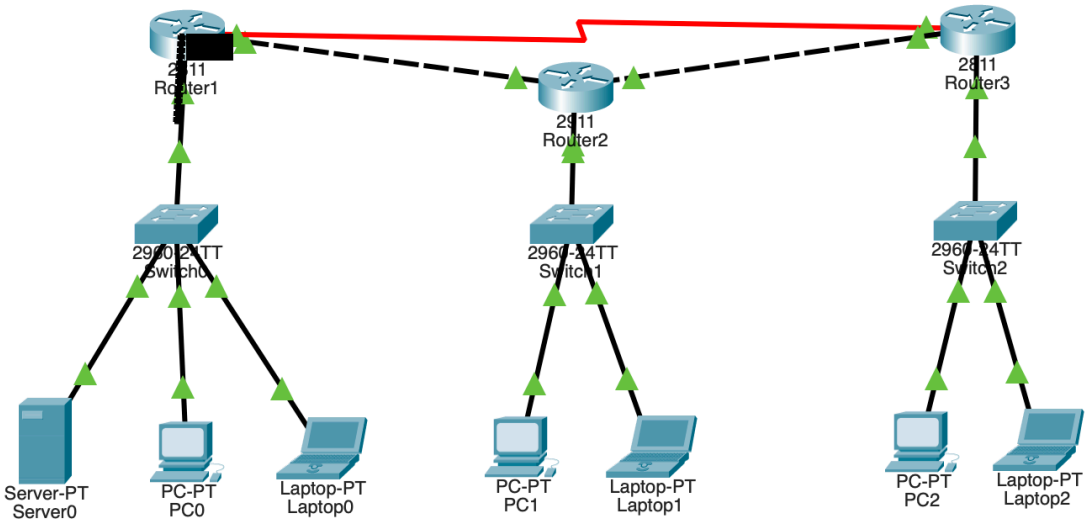
关闭 Router2，可以看到 Router1 改用新的线路前往 Router3，说明红线功能正常：

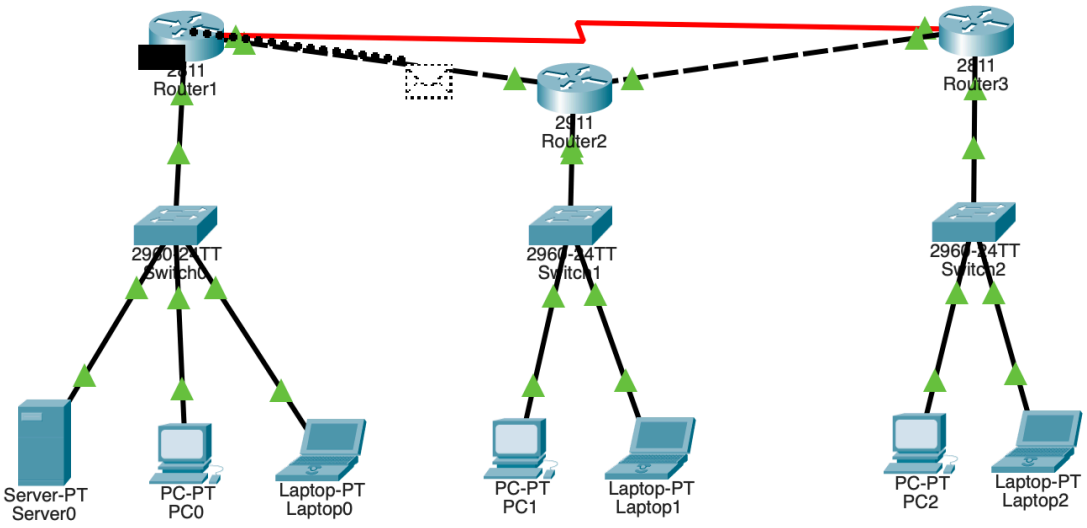


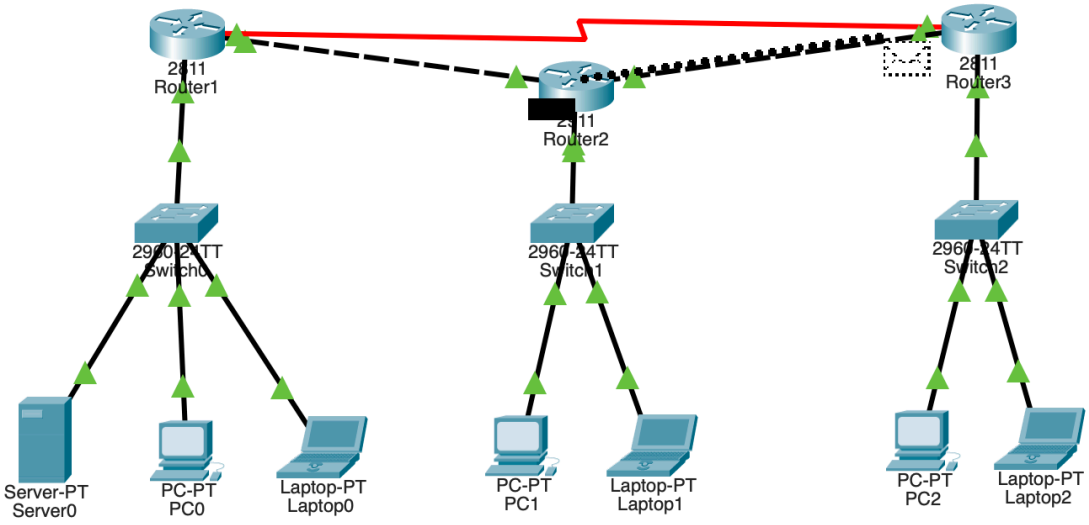
实际传输路径

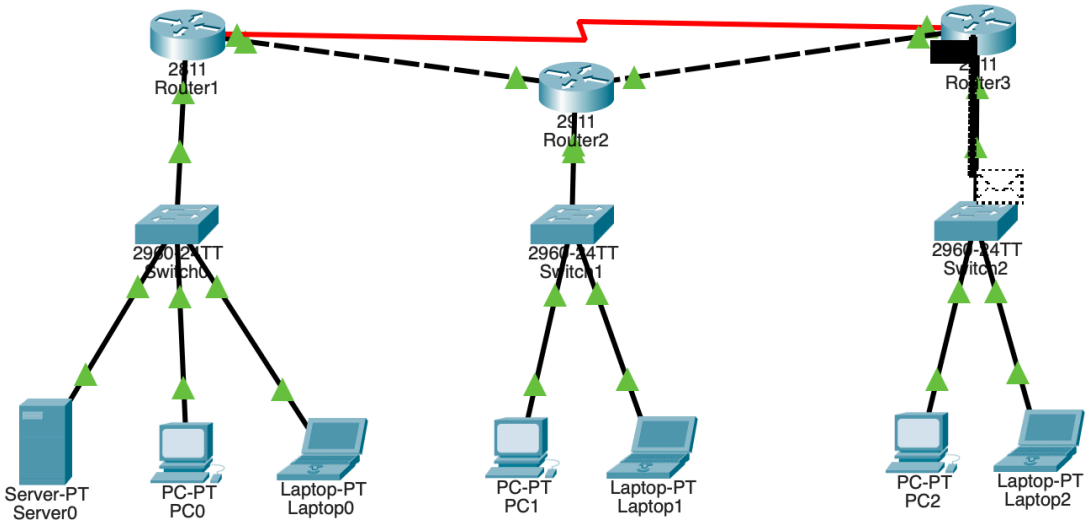
以元老院的 PC（PC0）向部族会议所的 Laptop（Laptop2）ping 为例：

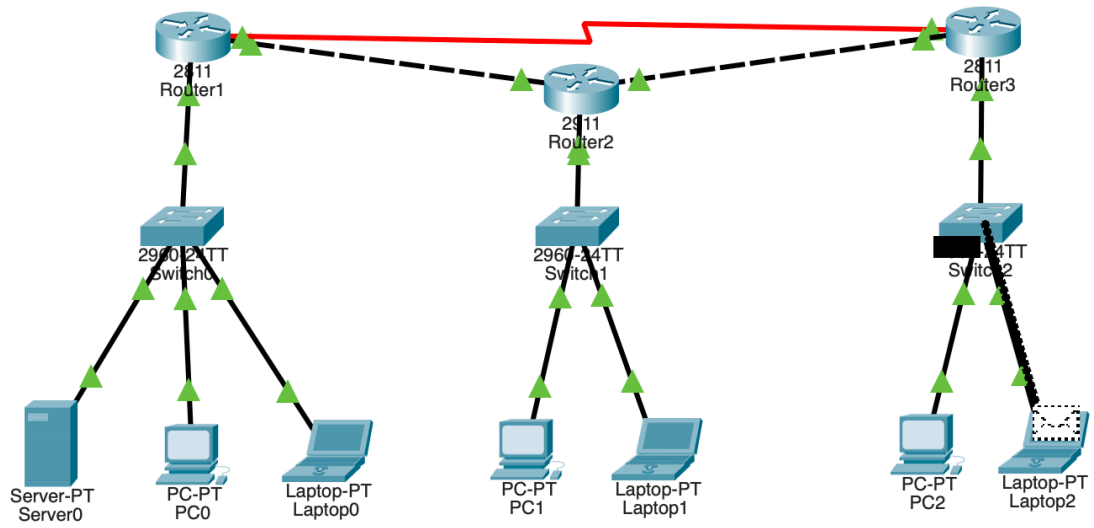


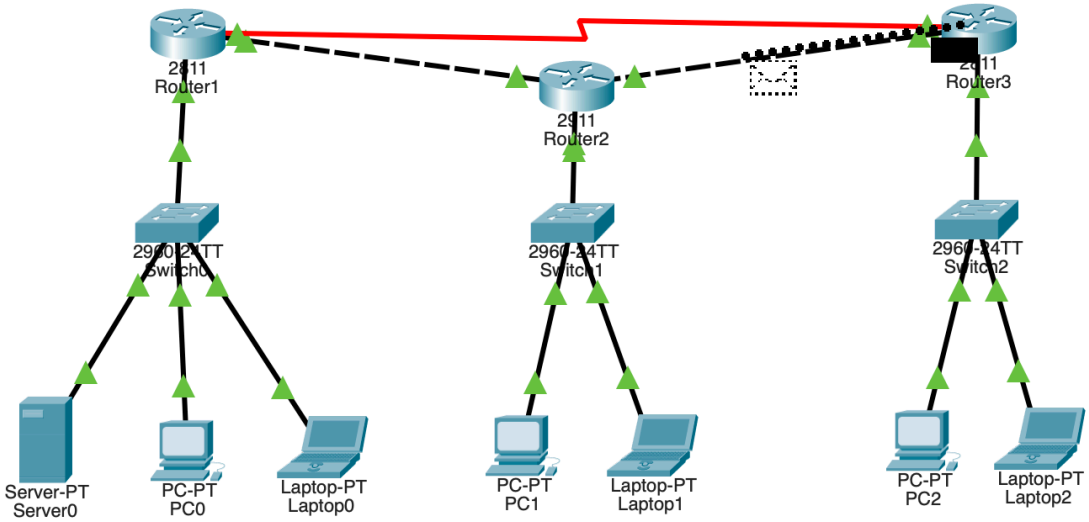


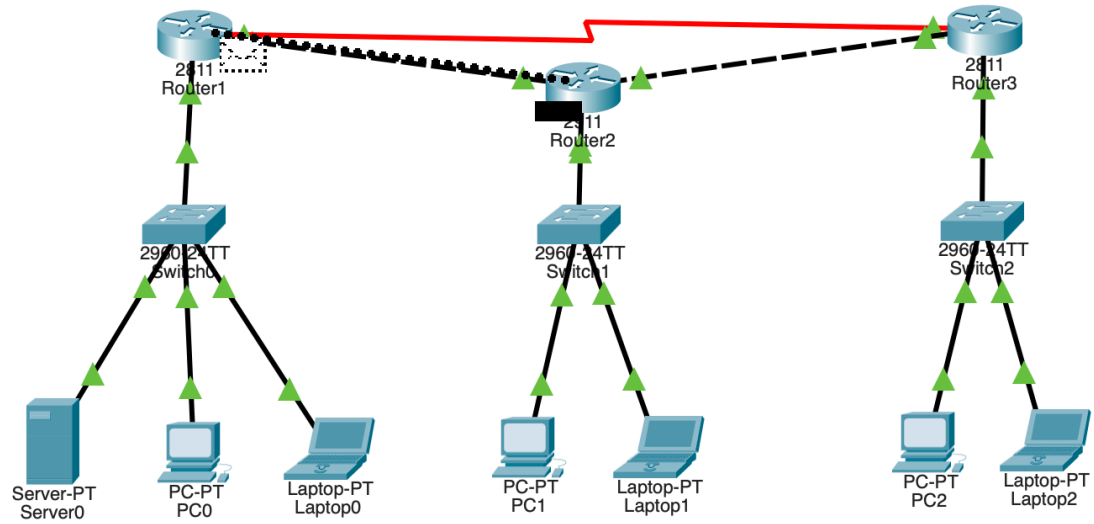

2911
Router1
2911
Router2
2911
Router3
2960-24TT
Switch0
2960-24TT
Switch1
2960-24TT
Switch2
Server-PT
Server0
PC-PT
PC0
Laptop-PT
Laptop0
PC-PT
PC1
Laptop-PT
Laptop1
PC-PT
PC2
Laptop-PT
Laptop2

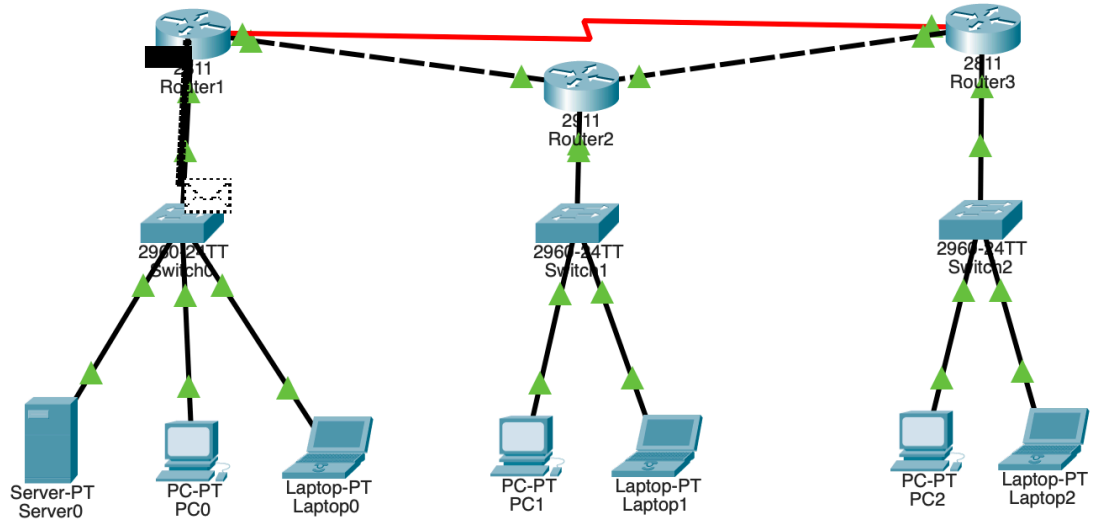

2911
Router1
2911
Router2
2911
Router3
2960-24TT
Switch0
2960-24TT
Switch1
2960-24TT
Switch2
Server-PT
Server0
PC-PT
PC0
Laptop-PT
Laptop0
PC-PT
PC1
Laptop-PT
Laptop1
PC-PT
PC2
Laptop-PT
Laptop2

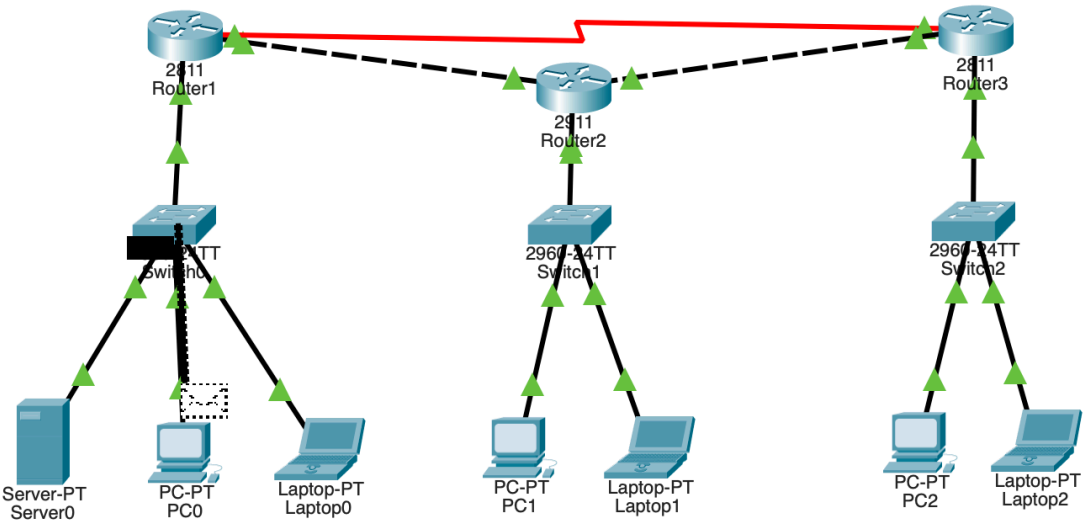

2911
Router1
2911
Router2
2911
Router3
2960-24TT
Switch0
2960-24TT
Switch1
2960-24TT
Switch2
Server-PT
Server0
PC-PT
PC0
Laptop-PT
Laptop0
PC-PT
PC1
Laptop-PT
Laptop1
PC-PT
PC2
Laptop-PT
Laptop2


2911
Router1
2911
Router2
2911
Router3
2960-24TT
Switch0
2960-24TT
Switch1
Server-PT
Server0
PC-PT
PC0
Laptop-PT
Laptop0
PC-PT
PC1
Laptop-PT
Laptop1
PC-PT
PC2
Laptop-PT
Laptop2


2911
Router1
2911
Router2
2911
Router3
2960-24TT
Switch0
2960-24TT
Switch1
2960-24TT
Switch2
Server-PT
Server0
PC-PT
PC0
Laptop-PT
Laptop0
PC-PT
PC1
Laptop-PT
Laptop1
PC-PT
PC2
Laptop-PT
Laptop2


2911
Router1
2911
Router2
2911
Router3
2960-24TT
Switch0
2960-24TT
Switch1
2960-24TT
Switch2
Server-PT
Server0
PC-PT
PC0
Laptop-PT
Laptop0
PC-PT
PC1
Laptop-PT
Laptop1
PC-PT
PC2
Laptop-PT
Laptop2





可以看见传输路线必定会经过执政官首府，此时完成了布鲁图的要求。

> 思考凯撒的观点是否存在问题？为什么？当前能否使用RIP作为路由协议？

凯撒的观点存在问题，原因在于 RIP 协议的限制不是 16 台设备，而是网络中最长路径所经过的路由器数目不超过 15 台 (hop limit = 15)。因此按照凯撒的思路配置网络的话是可以使用 RIP 协议的。若按照布鲁图的要求，则不能使用 RIP 作为路由协议，原因在于 packer tracer 不能更改某个网段的 Metric，导致传输时仍会使用 hop 较少的路线，即 Router1-Router3 的红线，此路径不符合布鲁图的要求。

Bonus: 谁的馈赠 (2')

`enable secret` 指令对应 cisco password type 5，使用了 MD5 散列算法。具体来说，加密时会使用 32 位的 salt 进行 1000 次 MD5 迭代，最终的结果即为加密结果。