Lab1-report

计11班 周韧平 2021010699

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	20.0.2.2	/24	-
	端口 3	192.168.2.1	/24	-
Router3	端口 1	[redacted]	/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	[redacted]	/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	[redacted]
Laptop3	端口 1	192.168.3.3	/24	192.168.3.1

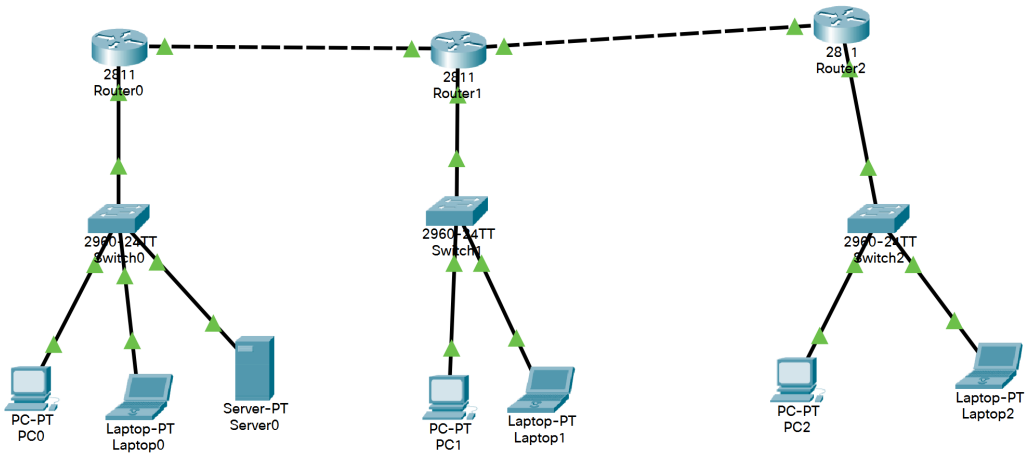
三处污损地方分别为：

- Router3：10.0.2.1
- PC3：192.168.3.2
- Laptop2: 192.168.2.1

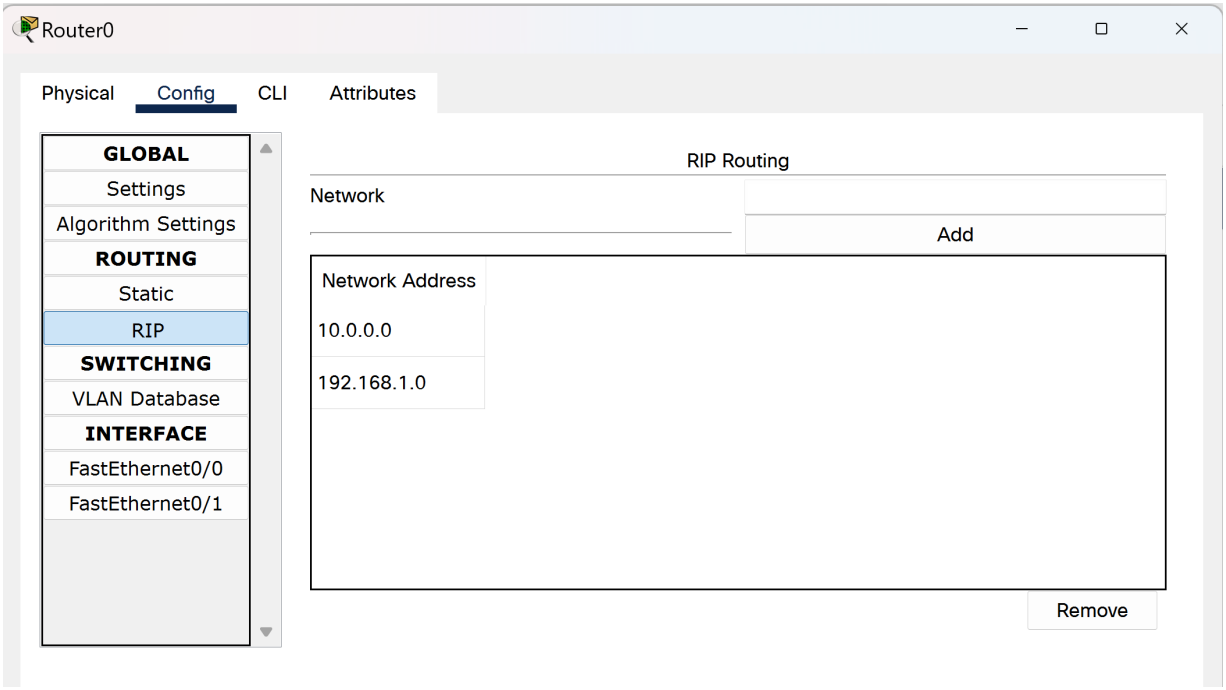
Router2的端口2有错误，20开头属于公网ip地址，不应该用于私人子网搭建，因此应该改为10.0.2.2

任务二

使用2811型号路由器搭配 NM-1E 模块，其它设备均按照拓扑图给出的搭建

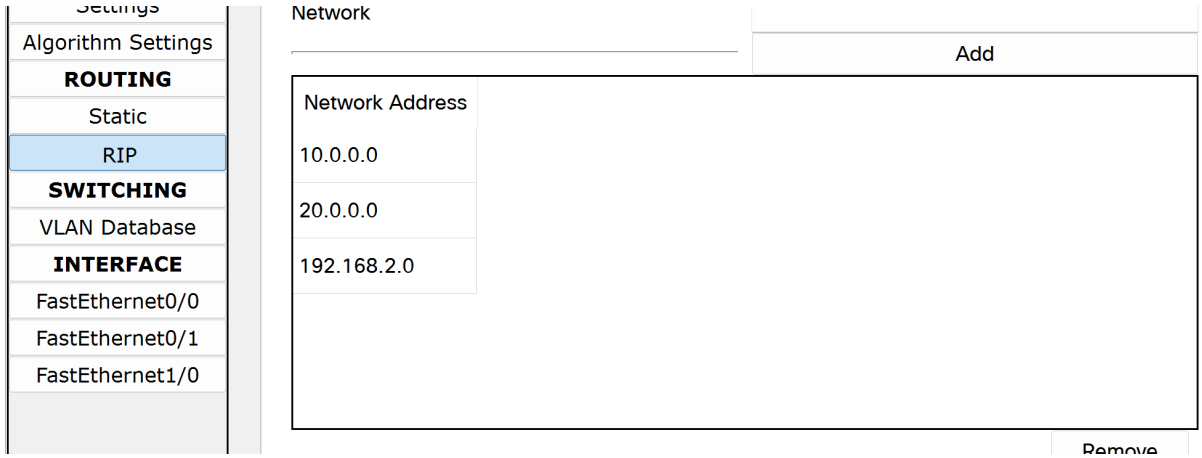


Router0设定




```
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 10.0.1.1 255.255.255.0
Router(config-if)#ip address 10.0.1.1 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#
```

Router1设定




```
Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 20.0.2.2 255.255.255.0
Router(config-if)#ip address 20.0.2.2 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 10.0.1.2 255.255.255.0
Router(config-if)#ip address 10.0.1.2 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#
```

Router2设定


```
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 20.0.2.1 255.255.255.0
Router(config-if)#ip address 20.0.2.1 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 192.168.3.1 255.255.255.0
```

其它设备（除了交换机外）按照任务一中给出的表格设置ip地址和默认网关

在等待一段时间让rip协议收敛后，可以在PC1上ping通同一子网内的设备，也可以ping通另一个子网内的设备（PC3）

```
C:\>
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time<1ms TTL=125
Reply from 192.168.3.2: bytes=32 time<1ms TTL=125
Reply from 192.168.3.2: bytes=32 time=1ms TTL=125
Reply from 192.168.3.2: bytes=32 time<1ms TTL=125

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 = 1ms, Average = 0ms

C:\>
```

任务三

根据提示，”YHQL, YLGL, YLFL“是凯撒加密算法在k=3时的结果，原码为凯撒名言"VENI, VIDI, VICI"（"I came, I saw, I conquered"）

因此我将三个密码设为如下值：

- password1: VENIVIDIVICI_console
- password2: VENIVIDIVICI_privileged
- password2: VENIVIDIVICI_telnet

设置命令的过程如下

```
Router>enable
Router#conf ter
Router#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#password
% Incomplete command.
Router(config-line)#password VENIVIDIVICI_console
Router(config-line)#login
Router(config-line)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#conf te
Router#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable password VENIVIDIVICI_privileged
Router(config)#line vty 0
Router(config-line)#password VENIVIDIVICI_telnet
Router(config-line)#login
Router(config-line)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#show running
Router#show running-config
```

通过 `show running-config` 命令可以看到密码在配置文件中以明文方式存储

```
line con 0
 password VENIVIDIVICI_console
 login
!
line aux 0
!
line vty 0
 password VENIVIDIVICI_telnet
 login
```

```
hostname Router
!
!
!
enable password VENIVIDIVICI_privileged
!
!
!
!
!
!
ip cef
no ipv6 cef
```

以上设置基于配置文件不会泄露的假设，但事实上在配置文件中明文存储密码是极其不安全的行为，通过运行指令`service password-encryption`可以将密码改为密文存储，加密后再次查看配置文件，可以看到密码已经以密文形式存储了

```
!
line con 0
 password 7 08176960202F2C333B3D2527031427273D262D1F02
 login
!
line aux 0
!
line vty 0
 password 7 08176960202F2C333B3D25270314302D3F3B2707
 login
line vty 1 4
 login
!
!
```

通过运行`copy running-config startup-config`保存配置文件，关机重启后可以看到需要密码验证，此时应该输入password1进入console界面

```
User Access Verification

Password:

Router>
```

进入特权模式需要输入password2

```
Password:

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

通过 PC1 使用 `telnet` 命令远程连接，需要输入password3

```
Invalid Command.

C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Password:
Router>
```

原文

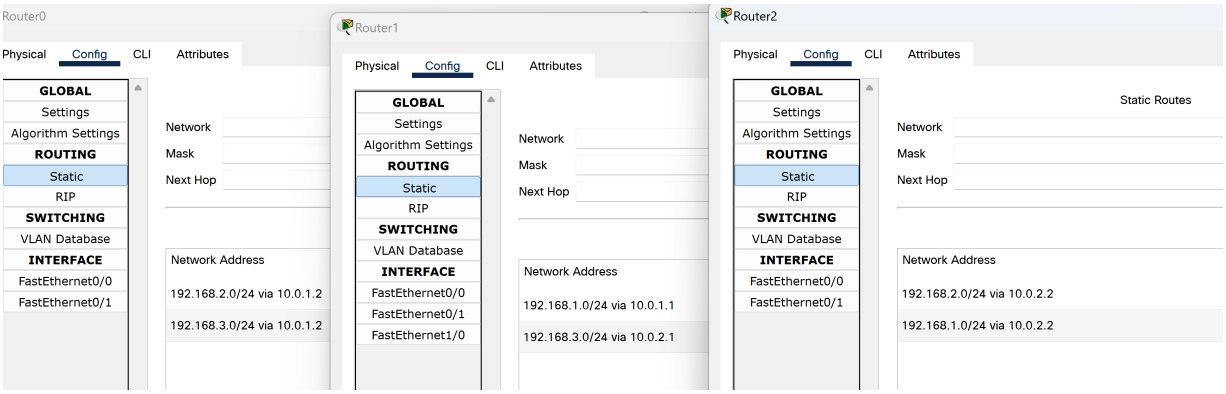
> 注意题目中的混合，考虑容斥原理

密码复杂度分析，根据提示，需要排除纯数字、纯字母的情况：

- 总长六位的纯数字密码：1×10^6
- 总长六位的混合有数字及小写字母的密码：$(10+26)^6 - 10^6 - 26^6 \approx 1.8 \times 10^9$
- 总长六位的混合有数字、大写字母、小写字母的密码：
  $(10+26+26)^6 - 10^6 - 26^6 - 26^6 - 2 \times ((10+26)^6 - 10^6 - 26^6) - ((26+26)^6 - 26^6 - 26^6) \approx 3.3 \times 10^{10}$
- 总长八位的混合有数字、大写字母、小写字母的密码：
  $(10+26+26)^8 - 10^8 - 26^8 - 26^8 - 2 \times ((10+26)^8 - 10^8 - 26^8) - ((26+26)^8 - 26^8 - 26^8) \approx 1.6 \times 10^{14}$

任务四

静态路由配置如下



在PC1上pingPC3

```
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=125
Reply from 192.168.3.2: bytes=32 time<1ms TTL=125
Reply from 192.168.3.2: bytes=32 time<1ms TTL=125
Reply from 192.168.3.2: bytes=32 time<1ms TTL=125

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
```

在PC3上pingPC2

```
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=30ms TTL=126
Reply from 192.168.2.2: bytes=32 time=2ms 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 = 30ms, Average = 8ms

C:\>
```

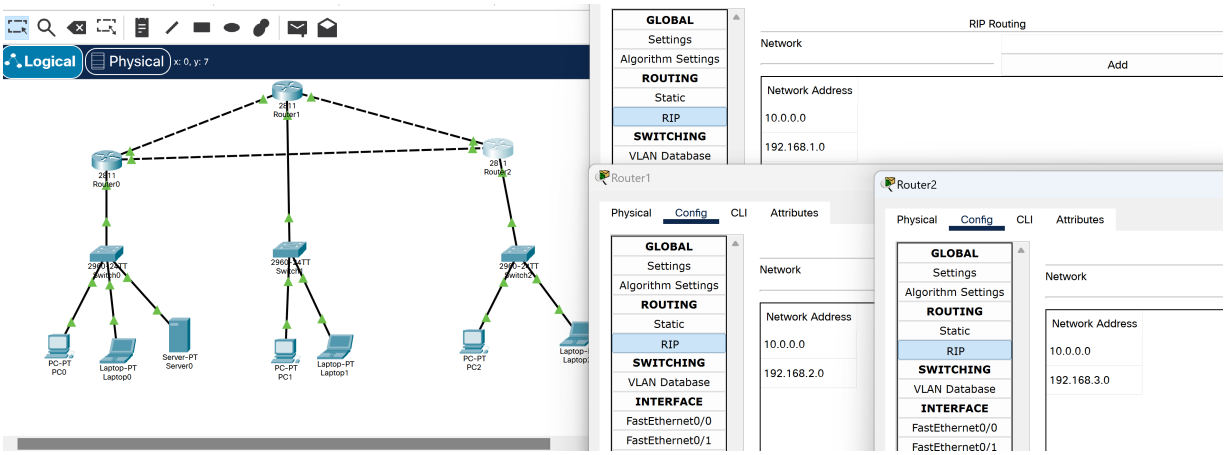
在PC2上pingPC1

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=18ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 18ms, Average = 4ms

C:\>
```

任务五

使用Rip路由协议维护“共和国”目前的局域网

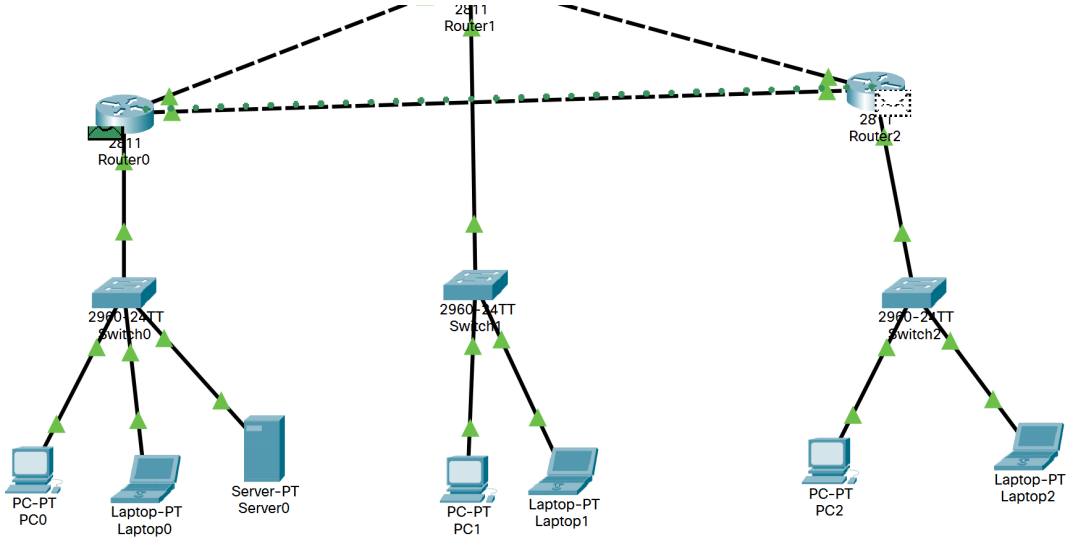
网络拓扑和rip路由配置如下

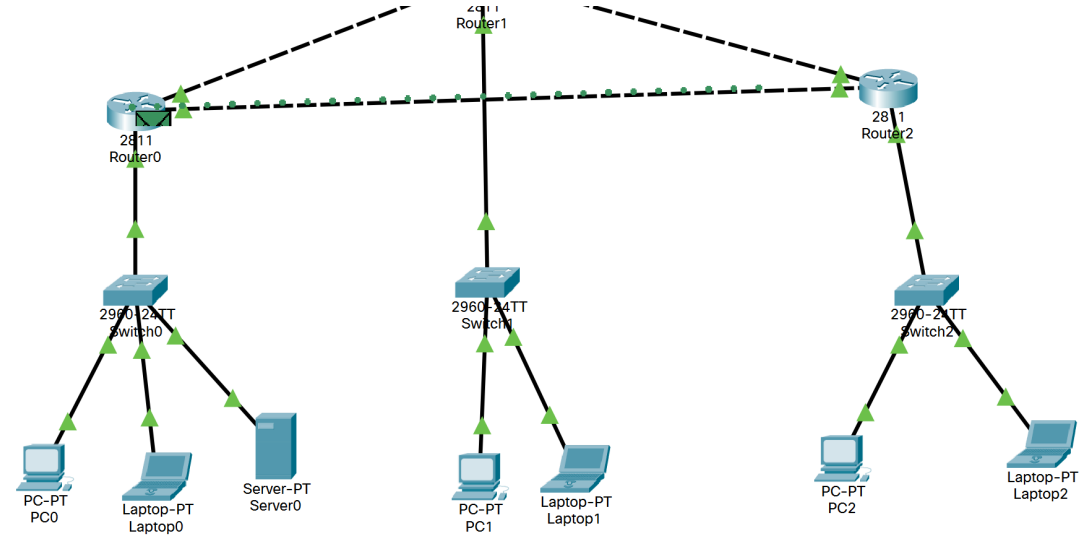


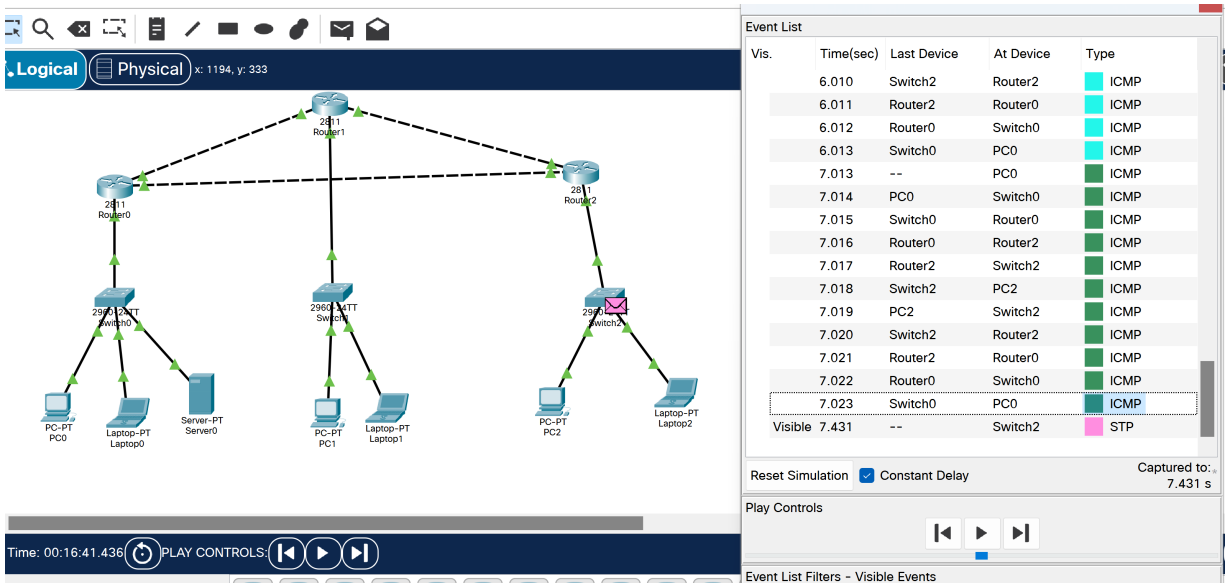
在路由收敛稳定后，各PC可以相互ping通

```
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=20ms TTL=126
Reply from 192.168.3.2: bytes=32 time=13ms 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 = 20ms, Average = 8ms

C:\>
```

尝试用PC1 ping PC3，从动画和事件列表中都可以看到，通信路径没有经过执政官首府（Router1）







凯撒的观点存在一定的问题，Rip协议要求路径跳数少于16跳，凯撒只考虑了接入网络的PC、笔记本和服务器，但实际上如果路由器过多，网络拓扑过于复杂，使得跳数超过16也会导致rip协议失效。

当前网络可以使用rip协议，最远跳数只有2跳，因此可以使用rip路由协议维护“共和国”目前的局域网。

Bonus

使用 `enable secret` 加密，观察配置文件可以看到密文存储的密码

```
no service timestamps debug datetime msec
service password-encryption
!
hostname Router
!
!
!
enable secret 5 $1$mERr$GVWExmKkCuROr/ZNUB8j50
!
!
!
!
```

通过查阅资料，该指令加密算法为md5，其中 1 表示MD5，$mERr$ 为salt，在linux环境下可以验证使用的的确是该加密算法

```
root@DESKTOP-PL4SP56  ~   openssl passwd -1 -salt mERr -table VENIVIDIVICI_privileged
VENIVIDIVICI_privileged $1$mERr$GVWExmKkCuROr/ZNUB8j50
```

其中 `-1` 表示 MD5-based password algorithm