

计算机网络安全技术

实验一报告

2017011620 计 73 李家昊

2019 年 12 月 1 日

1 任务 1

需要修改三处地方：

- Router2 端口 2 不能设置为公网 ip，因此将其从 20.2.3.2 改为 10.2.3.2
- Router3 端口 1 与 Router 2 端口 2 处于同一子网，此处设为 10.2.3.1
- Server0 处于 Router1 端口 1 的子网内，因此网关为 192.168.1.1

修改后的 IP 分配方案如 Table 1 所示。

Device	Port	IP	Mask	Gateway
Router1	端口 1	192.168.1.1	/24	-
	端口 2	10.1.2.1	/24	-
Router2	端口 1	10.1.2.2	/24	-
	端口 2	10.2.3.2	/24	-
	端口 3	192.168.2.1	/24	-
Router3	端口 1	10.2.3.1	/24	-
	端口 2	192.168.3.1	/24	-
PC0	端口 1	192.168.1.2	/24	192.168.1.1
PC1	端口 1	192.168.2.2	/24	192.168.2.1
Server0	端口 1	192.168.1.3	/24	192.168.1.1
Laptop0	端口 1	192.168.1.4	/24	192.168.1.1
Laptop1	端口 1	192.168.2.3	/24	192.168.2.1
Laptop2	端口 1	192.168.3.2	/24	192.168.3.1
Laptop3	端口 1	192.168.3.3	/24	192.168.3.1

表 1: 修改后的 IP 分配方案

2 任务 2

选择路由器型号为 2911，交换机型号为 2950-24，按照网络预拓扑图搭建网络，初步搭建完成后，如 Figure 1 所示。

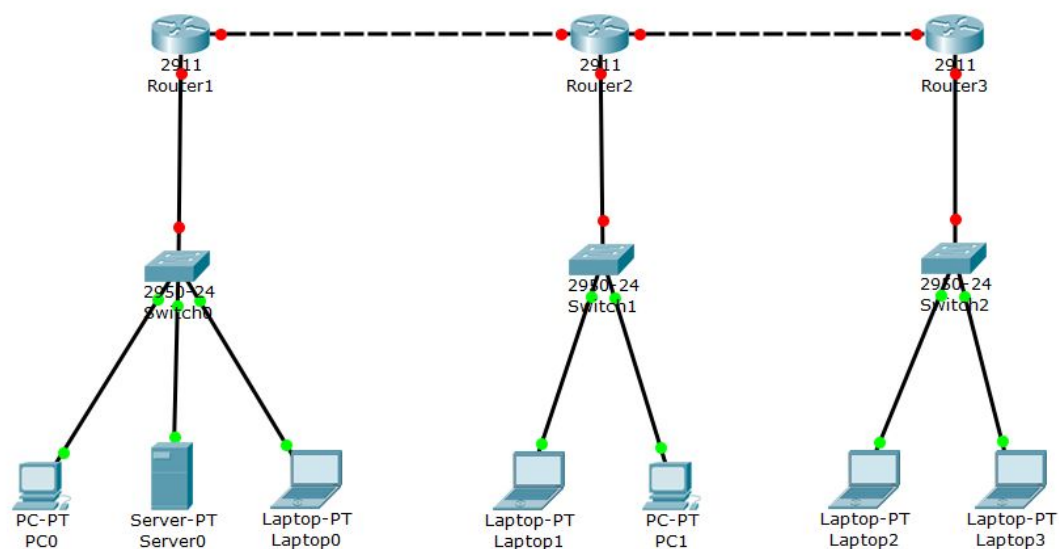


图 1: 初步搭建完成图

下面开启路由器端口并配置路由器 ip 地址，以 Router1 端口 1 的配置为例，打开路由器终端，运行以下指令：

```
Router>enable
Router#configure terminal
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.1.1 255.255.255.0
```

此时 Router1 已经配置完成，按照同样的步骤配置 Router2 和 Router3 即可。然后配置终端设备的 ip 地址，以 PC0 的配置为例，打开 Desktop > IP Configuration 界面配置即可，如 Figure 2 所示。

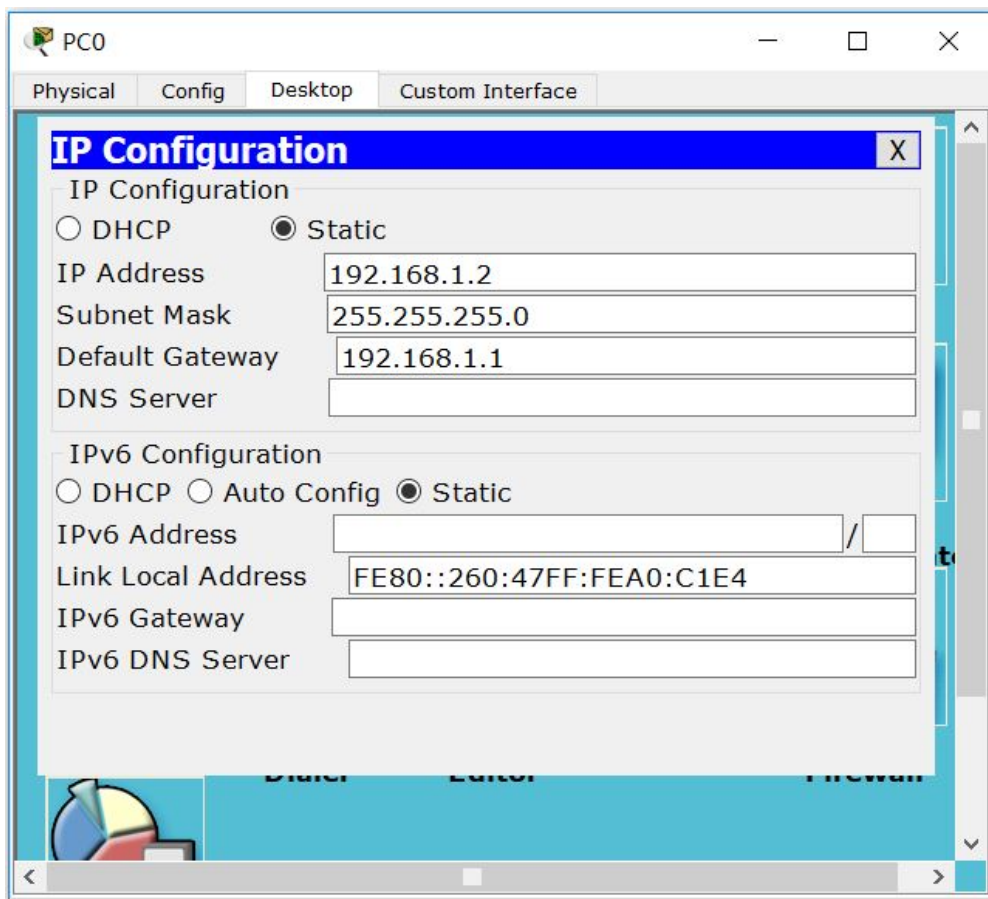


图 2: PC0 配置图

同理配置其他接入设备的 IP 地址，配置完成后，网络的红点全部变绿，如 Figure 3 所示。

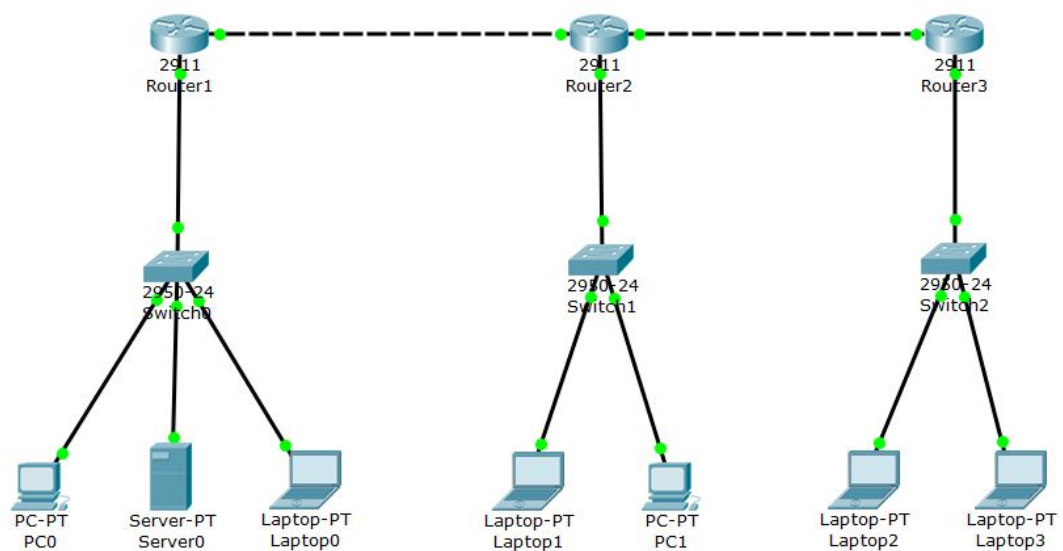


图 3: 配置完成后网络连接图

3 任务 3

3.1 密码配置

假设路由器配置文件不会泄露，在 Router1 上设置密码。

设置 console 密码 password1，在用户模式下运行：

```
>enable
#configure terminal
(config)#line console 0
(config-line)#password consolePwd1!
(config-line)#login
```

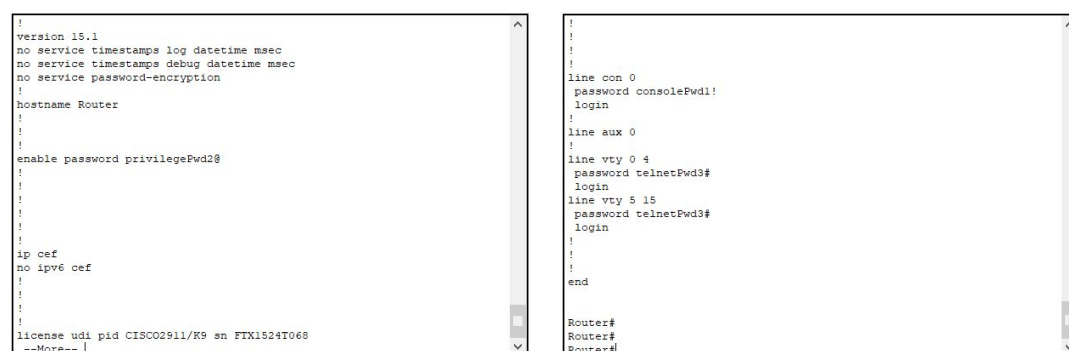
设置特权模式密码 password2，在用户模式下运行：

```
>enable
#configure terminal
(config)#enable password privilegePwd2@
```

设置 telnet 密码 password3，在用户模式下运行：

```
>enable
#configure terminal
(config)#line vty 0 15
(config-line)#password telnetPwd3#
(config-line)#login
```

设置完成后，在特权模式下运行 `show running-config` 查看配置，如 Figure 4 所示，可见密码已经以明文方式写入配置。



```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
enable password privilegePwd2@
!
!
!
ip cef
no ipv6 cef
!
!
!
license udi pid CISCO2911/K9 sn FTX1524T068
--More--

!
!
!
line con 0
 password consolePwd1!
 login
!
!
line aux 0
!
!
line vty 0 4
 password telnetPwd3#
 login
!
line vty 5 15
 password telnetPwd3#
 login
!
!
!
end

Router#
Router#
Router#
```

(a) Password 2

(b) Password 1, 3

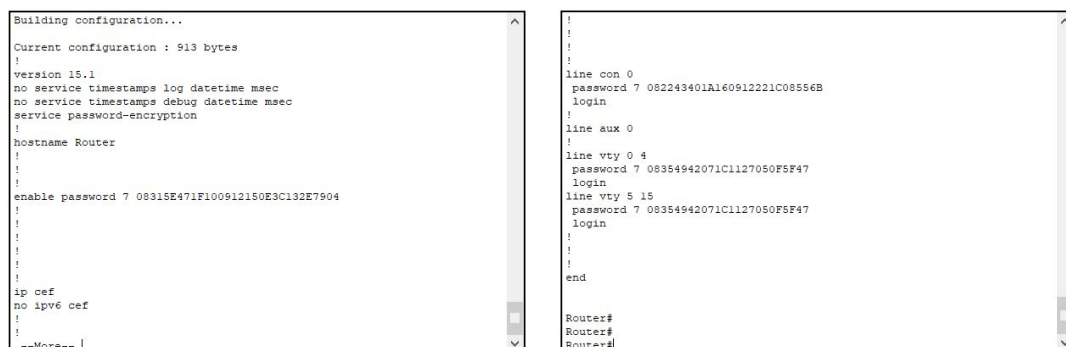
图 4: 明文存储的密码配置

3.2 加密存储

如果路由器配置文件可能泄露，则应当采用密文存储，在全局配置模式下运行

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

在特权模式下运行 `show running-config` 查看配置，如 Figure 5 所示，可见密码以密文方式存储。



```
Building configuration...
Current configuration : 913 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router
!
enable password 7 08315E471F100912150E3C132E7904
!
!
!
ip cef
no ipv6 cef
!
!
!
--More--

!
!
!
line con 0
password 7 082243401A160912221C08556B
login
!
line aux 0
!
line vty 0 4
password 7 08354942071C1127050F5F47
login
line vty 5 15
password 7 08354942071C1127050F5F47
login
!
!
!
end
Router#
Router#
Router#
```

(a) Password 2

(b) Password 1, 3

图 5: 加密存储的密码配置

3.3 破解分析

假设暴力尝试一次密码的时间为 1，对于下列四种复杂程度的密码，求暴力破解的时间需求：

1. 总长六位的纯数字密码

期望破解时间为 0.5×10^6

2. 总长六位的混合有数字及小写字母的密码

期望破解时间为 0.5×36^6

3. 总长六位的混合有数字、大写字母、小写字母的密码

期望破解时间为 0.5×62^6

4. 总长八位的混合有数字、大写字母、小写字母的密码

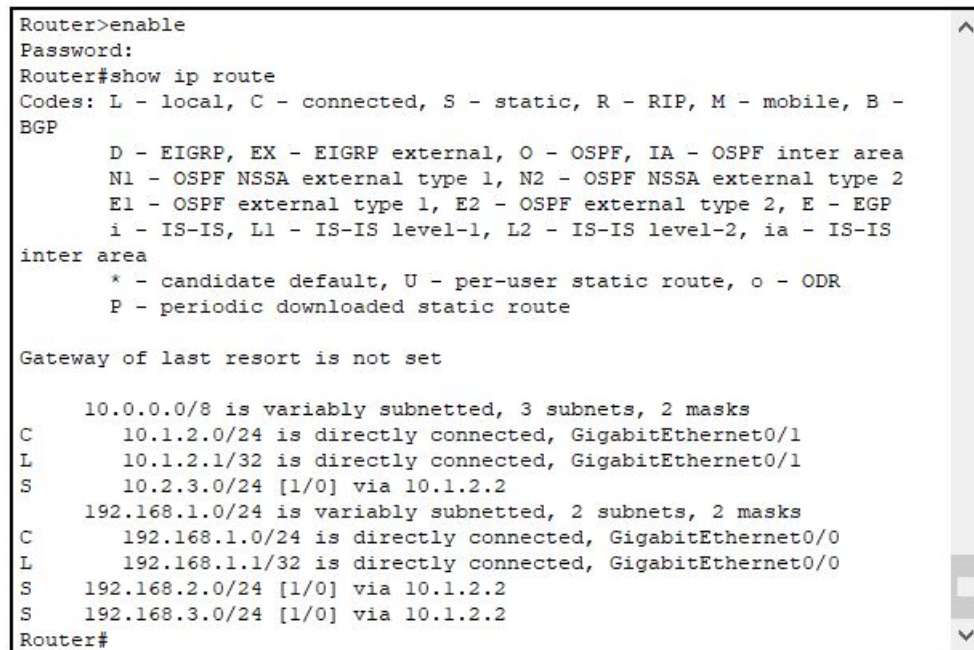
期望破解时间为 0.5×62^8

4 任务 4

配置 Router1 的静态路由，将所有 Router1 不可达的子网加进 Router1 的路由表。

```
Router(config)#ip route 192.168.2.0 255.255.255.0 10.1.2.2
Router(config)#ip route 192.168.3.0 255.255.255.0 10.1.2.2
Router(config)#ip route 10.2.3.0 255.255.255.0 10.1.2.2
```

配置成功后，在特权模式下运行 `show ip route` 查看路由配置，如 Figure 6 所示。



```
Router>enable
Password:
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.2.0/24 is directly connected, GigabitEthernet0/1
L       10.1.2.1/32 is directly connected, GigabitEthernet0/1
S       10.2.3.0/24 [1/0] via 10.1.2.2
O       192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
S       192.168.2.0/24 [1/0] via 10.1.2.2
S       192.168.3.0/24 [1/0] via 10.1.2.2
Router#
```

图 6: Router1 的路由配置

同理，配置 Router2 的静态路由

```
Router(config)#ip route 192.168.1.0 255.255.255.0 10.1.2.1
Router(config)#ip route 192.168.3.0 255.255.255.0 10.2.3.1
```

配置 Router3 的静态路由

```
Router(config)#ip route 192.168.1.0 255.255.255.0 10.2.3.2
Router(config)#ip route 192.168.2.0 255.255.255.0 10.2.3.2
Router(config)#ip route 10.1.2.0 255.255.255.0 10.2.3.2
```

配置完成后，用 Laptop0 ping Laptop1 和 Laptop2，如 Figure 7 所示，此时各个部门已经能够互相通信了。

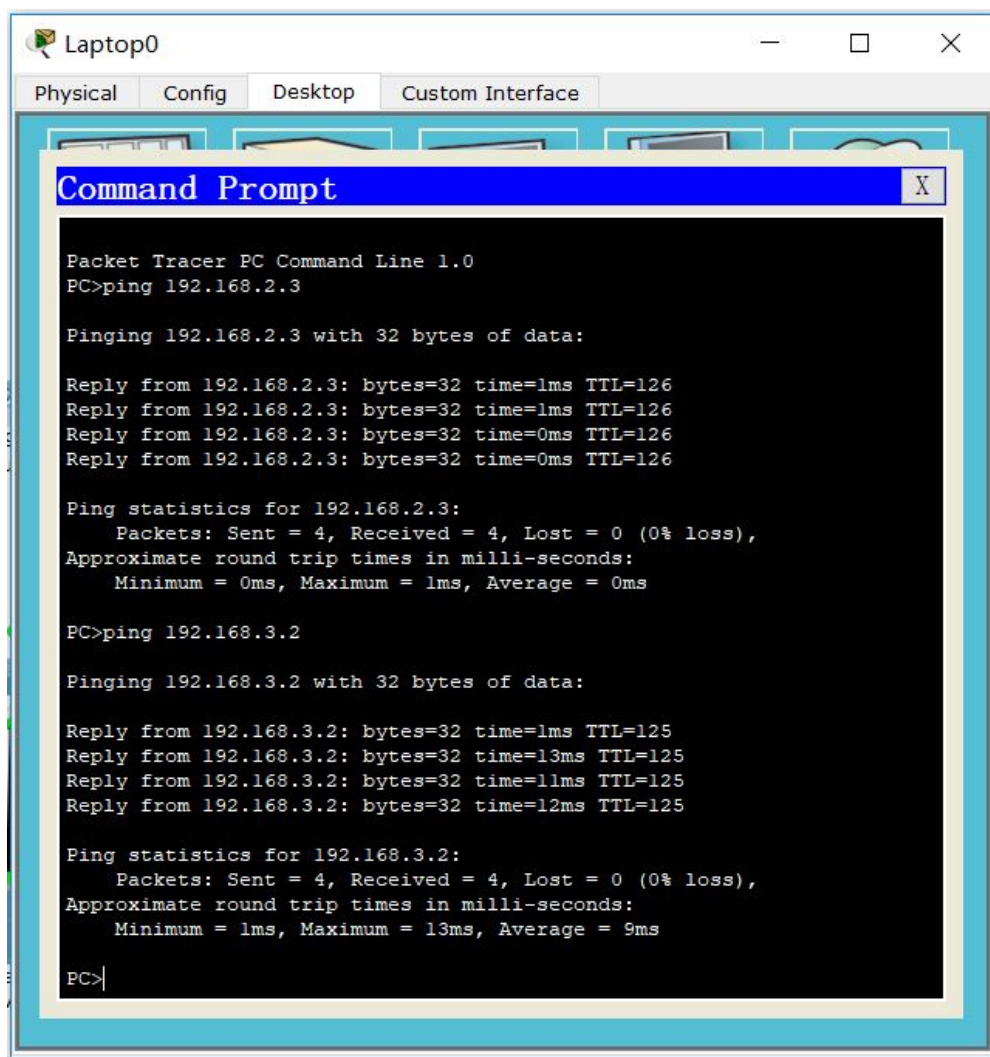


图 7: 静态路由通信测试

5 任务 5

小杨的观点存在问题，接入网络的设备数量跟网络跳数没有必然联系。RIP 协议仅支持小于 16 跳的网络，如果公司有多于 16 个路由器，它们连成一条链，而且两个接入设备恰好在这条链上的一头一尾，那么它们之间的网络跳数会超过 16 跳，此时不能使用 RIP 协议。换一个角度来说，如果公司有多于 16 台设备接入网络，但是它们都直接连在同一个路由器下，此时也能使用 RIP 协议。

但是考虑到当前网络任意两个接入设备之间通信均不超过 16 跳，因此当前可以使用 RIP 协议，最终选择 RIP 路由协议维护公司目前的局域网。

以 Router1 为例，首先取消静态路由配置，再配置 RIP 协议。

```
Router(config)#no ip route 192.168.2.0 255.255.255.0 10.1.2.2
Router(config)#no ip route 192.168.3.0 255.255.255.0 10.1.2.2
Router(config)#no ip route 10.2.3.0 255.255.255.0 10.1.2.2
Router(config)#router rip
```



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

同理配置 Router2 的 RIP 协议。

```
Router(config)#no ip route 192.168.1.0 255.255.255.0 10.1.2.1
Router(config)#no ip route 192.168.3.0 255.255.255.0 10.2.3.1
Router(config)#router rip
Router(config-router)#network 192.168.2.0
Router(config-router)#network 10.0.0.0
```

同理配置 Router3 的 RIP 协议。

```
Router(config)#no ip route 192.168.1.0 255.255.255.0 10.2.3.2
Router(config)#no ip route 192.168.2.0 255.255.255.0 10.2.3.2
Router(config)#no ip route 10.1.2.0 255.255.255.0 10.2.3.2
Router(config)#router rip
Router(config-router)#network 192.168.3.0
Router(config-router)#network 10.0.0.0
```

配置完成后，用 Laptop0 ping Laptop1 和 Laptop2，结果如 Figure 8 所示，可以看出 RIP 配置已经成功。

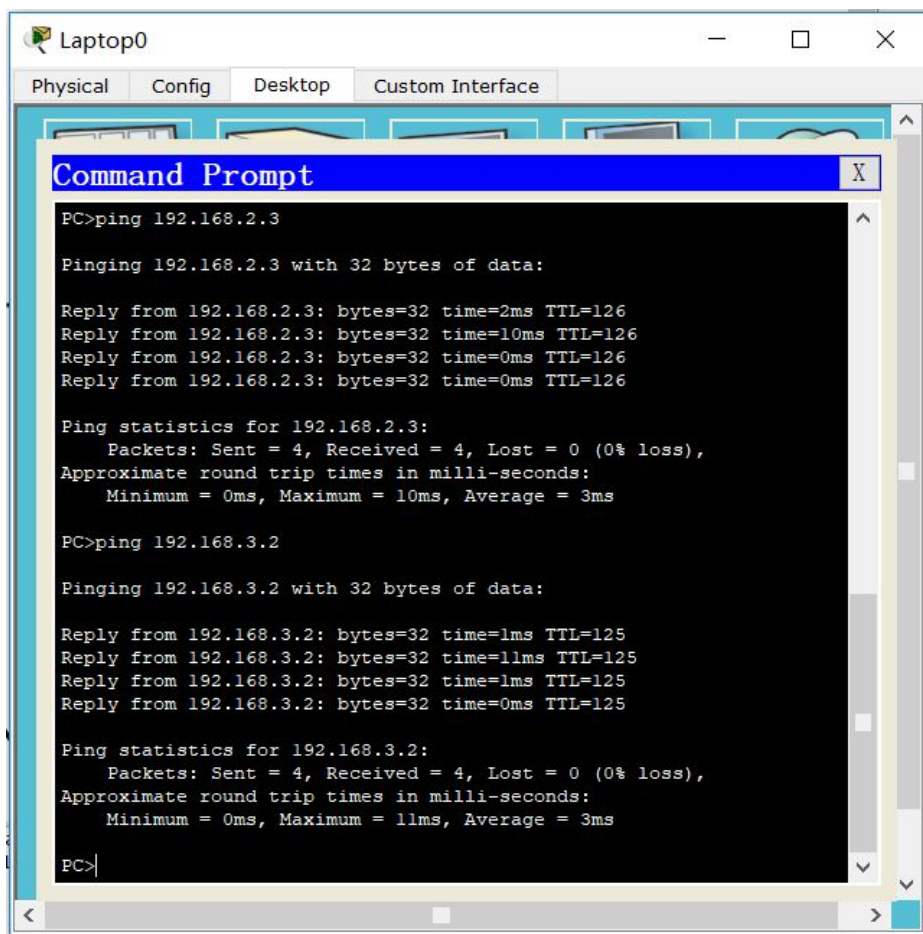


图 8: RIP 协议通信测试

6 Bonus

6.1 Bonus 1

设置 secret 为 123456，并查看配置

```
Router(config)#enable secret 123456
Router(config)#exit
Router#show running-config
```

得到

```
enable secret 5 $1$mERr$H7PDx17VYMqaD3id4jJVK/
```

在另一个路由器下设置 secret 为 654321，并查看配置，得到

```
enable secret 5 $1$mERr$SI6kKbhlkuiS3Lv8zc1kp1
```

可以观察得出 `1mERr$` 是一个固定的前缀，与密文和路由器无关。通过查找资料得出，1 代表 MD5，mERr 是盐，用 `openssl` 验证：

```
lijiahao@lijiahao:~$ openssl passwd -1 -salt mERr -table 123456
123456 $1$mERr$H7PDx17VYMqaD3id4jJVK/
lijiahao@lijiahao:~$ openssl passwd -1 -salt mERr -table 654321
654321 $1$mERr$SI6kKbhlkuiS3Lv8zc1kp1
```

与密文一致，可以断定此密码由 MD5 加盐生成。

6.2 Bonus 2

第一次 ping 测试的时候，由于源主机不知道目标主机的 MAC 地址，所以会发一个地址解析协议（ARP）请求，这个 ARP 请求会被广播到对方的子网内，子网内的所有主机会检查 ARP 请求中的 IP 是否与自己的一致，若一致，则将自己的 MAC 地址发送回去，源主机收到目标主机的 MAC 地址后，将 IP 和 MAC 地址的映射更新 ARP 缓存。由于没有 MAC 地址，第一次 ping 必然会出现丢包现象，但是当 ARP 缓存更新后，以后的每次 ping 都无需发送 ARP 请求，因此不会丢包。

接下来用 packet tracer 验证，当第一次用 Laptop0 ping Laptop1 时，可以看到 Laptop0 发出两个包，分别为 ARP 包和 ICMP 包，如 Figure 9 所示。

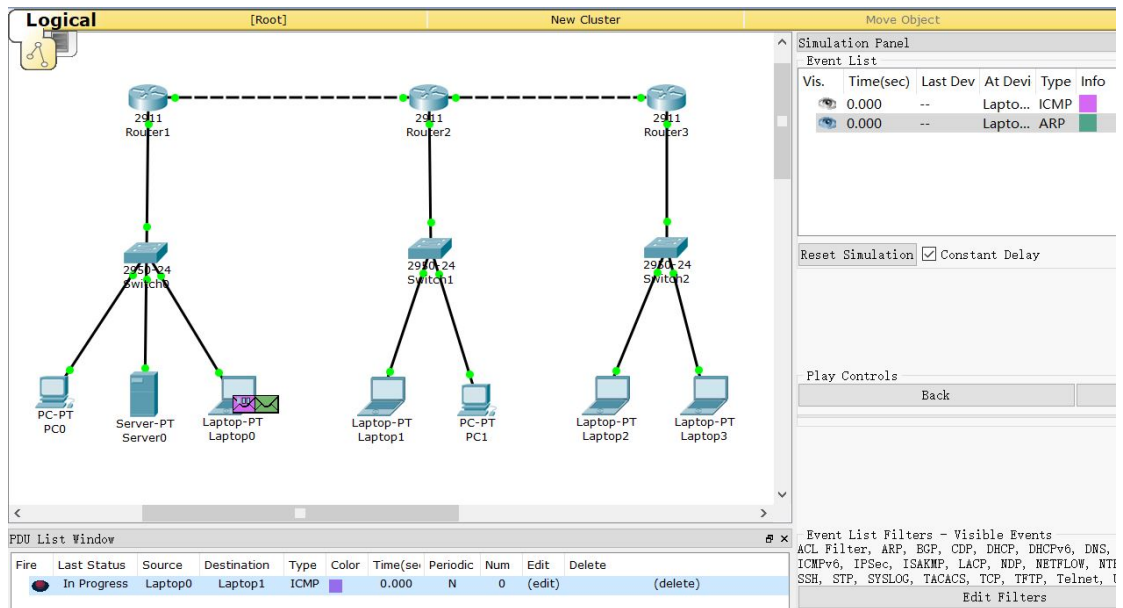


图 9: 第一次 ping 时发出 ARP 和 ICMP 包

第二次用 Laptop0 ping Laptop1 时, Laptop0 则只发出一个 ICMP 包, 如 Figure 10所示。

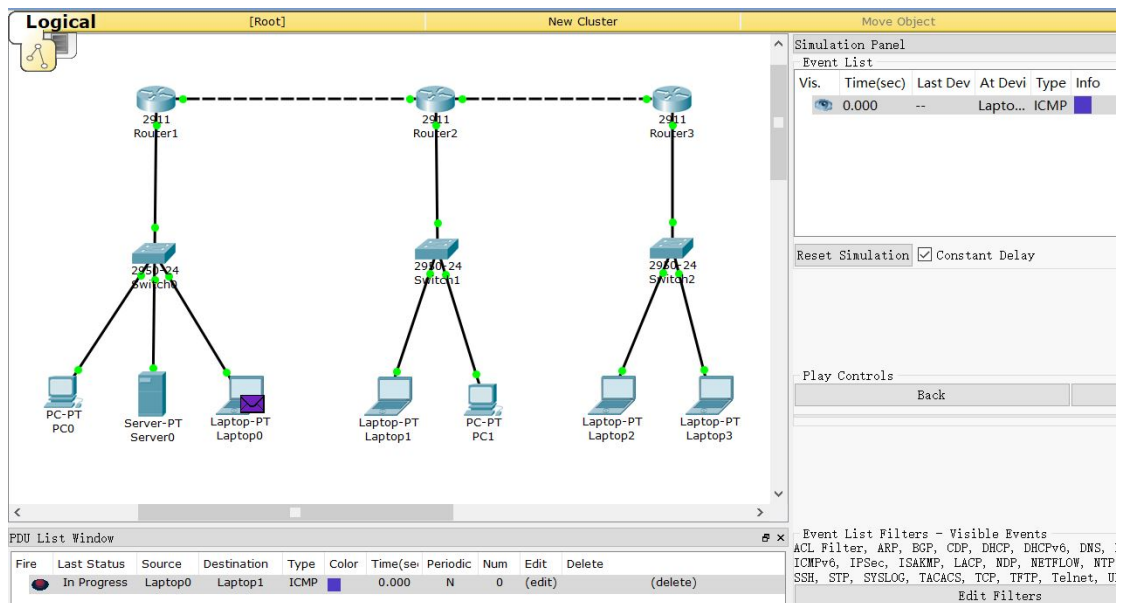


图 10: 第二次 ping 时只发出 ICMP 包