计算机网络安全技术：实验一

刘泓尊 2018011446 计84

任务一

补全与纠错:

1.Server1的网关是Server0第一跳路由器的ip, 所以应该设置为Router1端口1的ip: `192.168.1.1`

2.Router2的端口2不应该配公网ip地址，可以改为`10.2.3.1`

3.Router3的端口1和Router2的端口2相连，应该处于一个子网内，设置为`10.2.3.2`

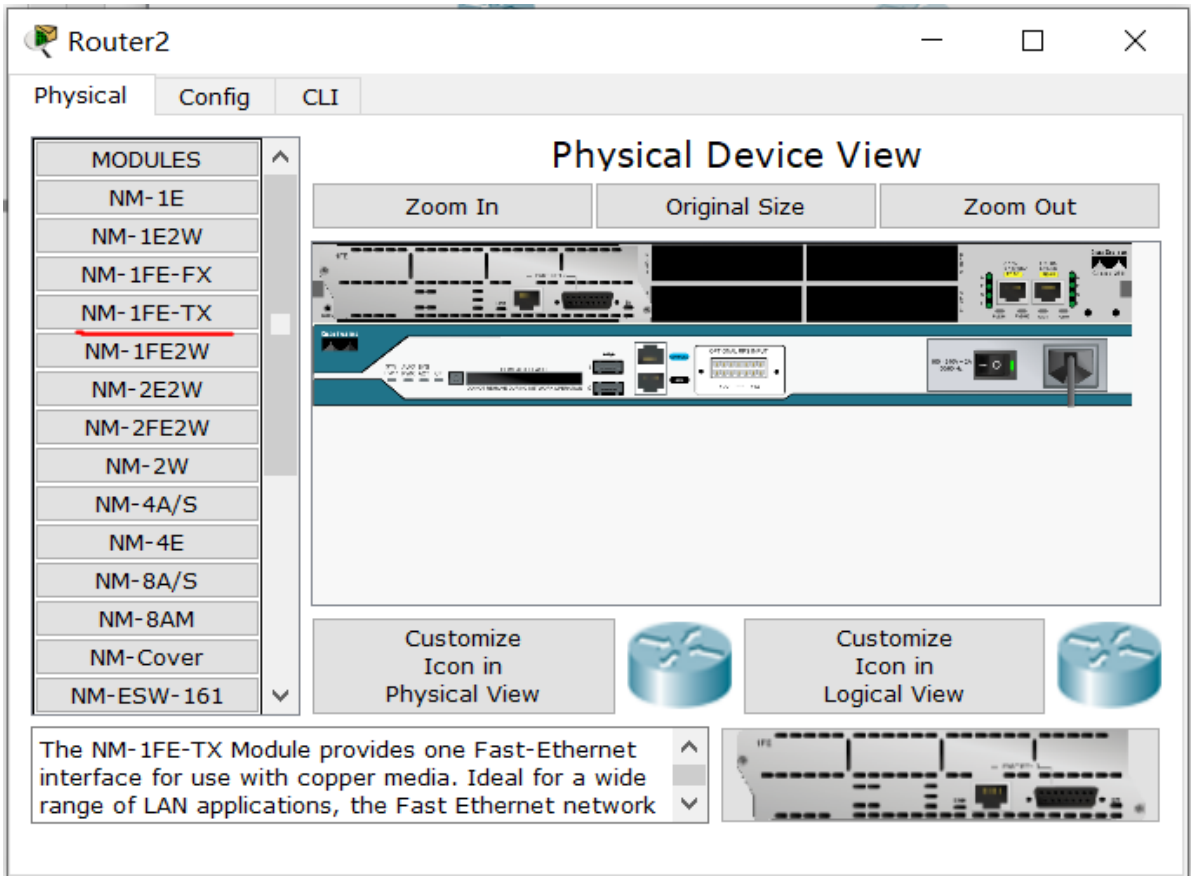
表格汇总如下:

Device	Port	IP	Mask	Gateway
Router1	port1	192.168.1.1	/24	---
	port2	10.0.1.1	/24	---
Router2	port1	10.0.1.2	/24	---
	port2	**10.2.3.1**	/24	---
	port3	192.168.2.1	/24	---
Router3	port1	**10.2.3.2**	/24	---
	port2	192.168.3.1	/24	---
PC1	port1	192.168.1.2	/24	192.168.1.1
PC2	port1	192.168.2.2	/24	192.168.2.1
PC3	port1	192.168.3.2	/24	192.168.3.1
Server1	port1	192.168.1.3	/24	**192.168.1.1**
Laptop1	port1	192.168.1.4	/24	192.168.1.1
Laptop2	port1	192.168.2.3	/24	192.168.2.1
Laptop3	port1	192.168.3.3	/24	192.168.3.1

任务二

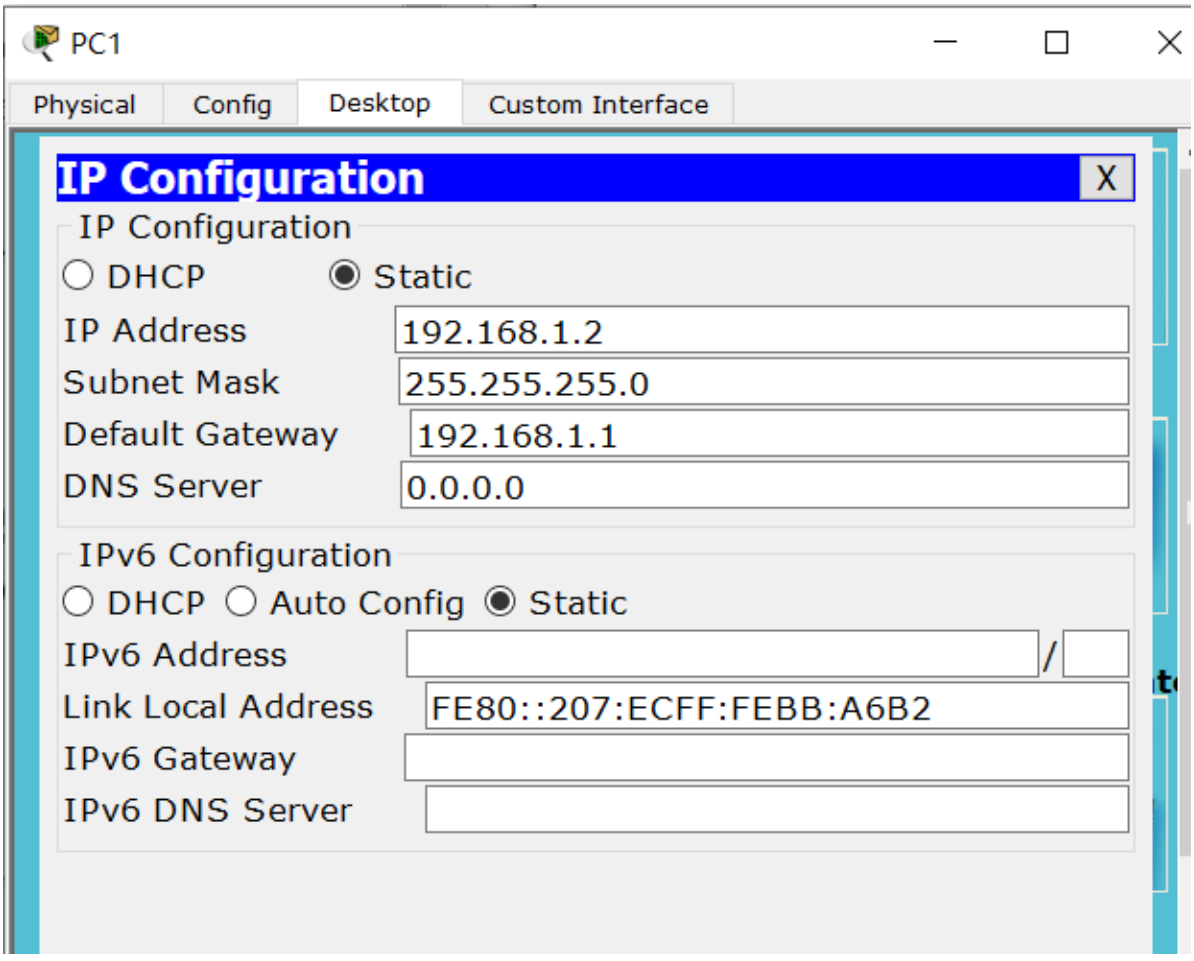
路由器型号`2811`, 交换机型号`2950T-24`

Router2需要增加一块`NM-1FE-TX`网卡，如下图所示

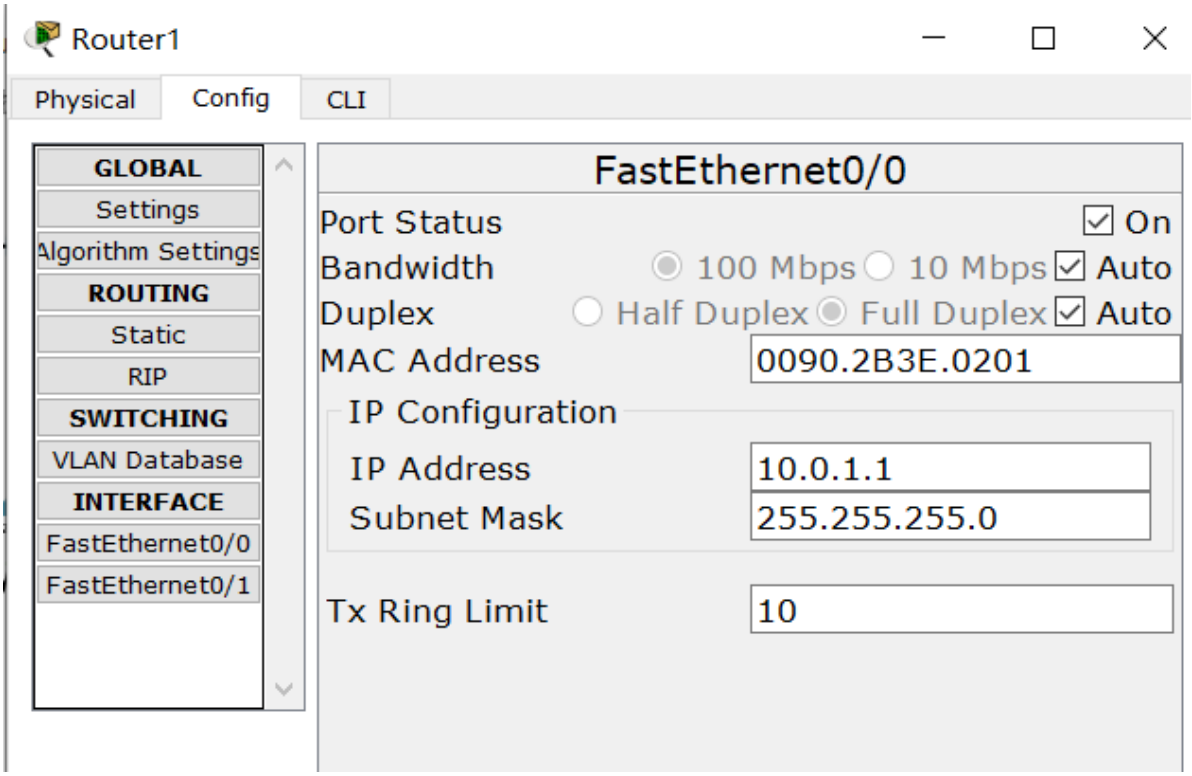


按上表的拓扑连接好之后，路由器之间尚不能通信，需要配置相应的IP。

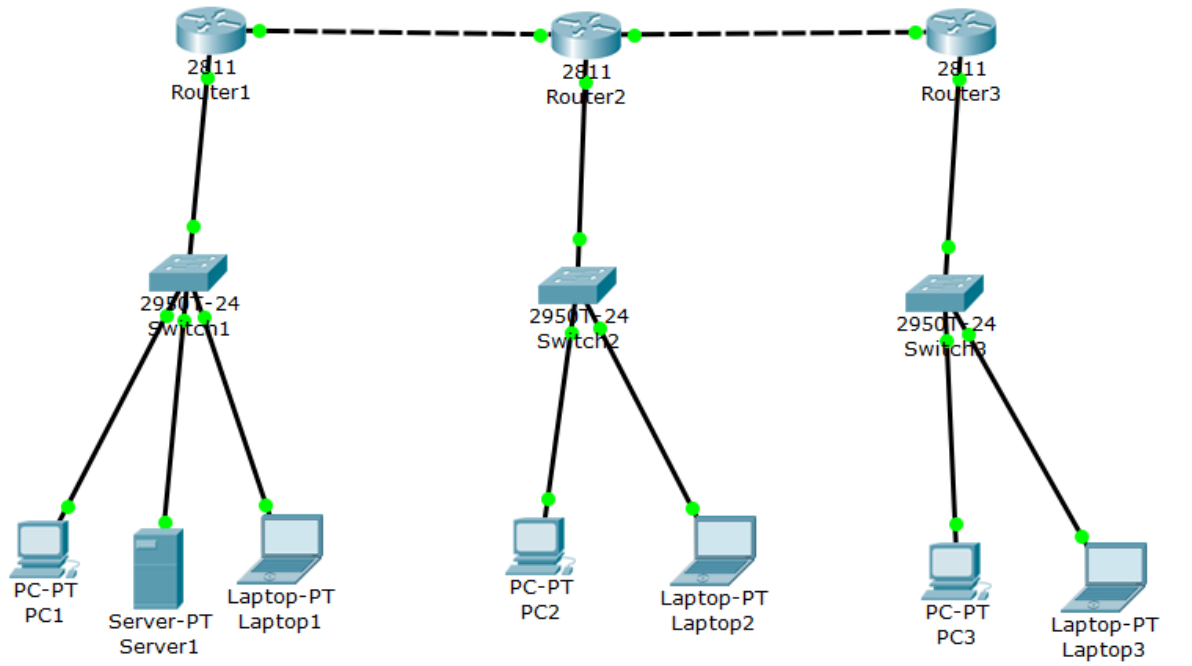
按照任务1中的表格对终端设备进行IP配置，IP选择静态，设置对应的IP地址、子网掩码和默认网关(即第一跳路由器ip)，以PC1为例：



再进行路由器的IP 配置，按照网卡连接的不同子网设置对应的IP地址和子网掩码，最后将`On`状态勾选即配置完成。这里以Router1的`0/0`网卡为例:



对终端设备和路由器配置完成后，可以看到各端口均为绿色，配置成功。



任务三

先来解释一下凯撒的密码，实际上就是采用了**代换**，每个字母的密文是它后面的第3个字母, 如下表所示:

```
明文: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
密文: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

那么`YHQL, YLGL, YLFL`对应的明文就是`VENI, VIDI, VICI`。翻译成英文就是`I came, I saw, I conquered`这句话出自恺撒大帝征服潘特斯王国后写给元老院的信，只有这三个词"我来，我看见，我征服"。我们可以认为这三句话代表了不同的模式，同时考虑到我的姓名首拼`lhz`，因此我将密码置为:

1.用户模式`password1`: `lhzcame`

2.特权模式`password2`: `lhzconquer`

3.`telnet`用户模式`password3`: `lhzsaw`

下面在Router1上设置三种密码, 如果配置文件**不被泄露**，可以都以明文存储。

用户模式密码`password1`配置截图如下:

```
Router>en
Router#conf te
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#password lhzcame
Router(config-line)#login
Router(config-line)#end
```

`telnet`模式配置和特权模式配置过程如下:

```
Router#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable password lhzconquer
Router(config)#line vty 0 4
Router(config-line)#password lhzsaw
Router(config-line)#login
Router(config-line)#end
```

下面通过`show running-config`命令来确认密码设置正确:

查看`password2`:

```
Router#show running-config
Building configuration...

Current configuration : 625 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
enable password lhzconquer
!
!
```

查看`password1`和`password3`:

```
!
line con 0
 password lhzcame
 login
!
line aux 0
!
line vty 0 4
 password lhzsaw
 login
!
```

如果路由器配置文件**可能泄露**，那么可以加密存储，使用`service password-encryption`即可。下图是密码`lhzconquer`加密后的存储：

```
Router#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ser
Router(config)#service pass
Router(config)#service password-encryption
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
show runn
Router#show running-config
Building configuration...

Current configuration : 872 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router
!
!
!

enable password 7 082D44540A160B06070E1E
!
```

此时所有密码都以加密形式存储在配置文件中，文件泄露时安全依然得到保障。

配置完成后回到初始状态验证密码设置成功：

```
User Access Verification

Password:

Router>en
Password:
Router#
```

试分析，当你使用如下四种复杂程度的密码进行配置时，攻击者暴力破 使用如下四种复杂程度的密码进行配置时，**攻击者暴力破解时间需求的变化**，假设暴力尝试一次密码为 1：

策略	密码组合数	破解单位时间
6位的纯数字	10^6	10^6
6位的数字、小写字母	36^6	36^6 约 2.2x10^9
6位的数字、大写字母、小写字母	62^6	62^6 约 5.7x10^10
8位的数字、大写字母、小写字母	62^8	62^8 约 2.2x10^14

任务四

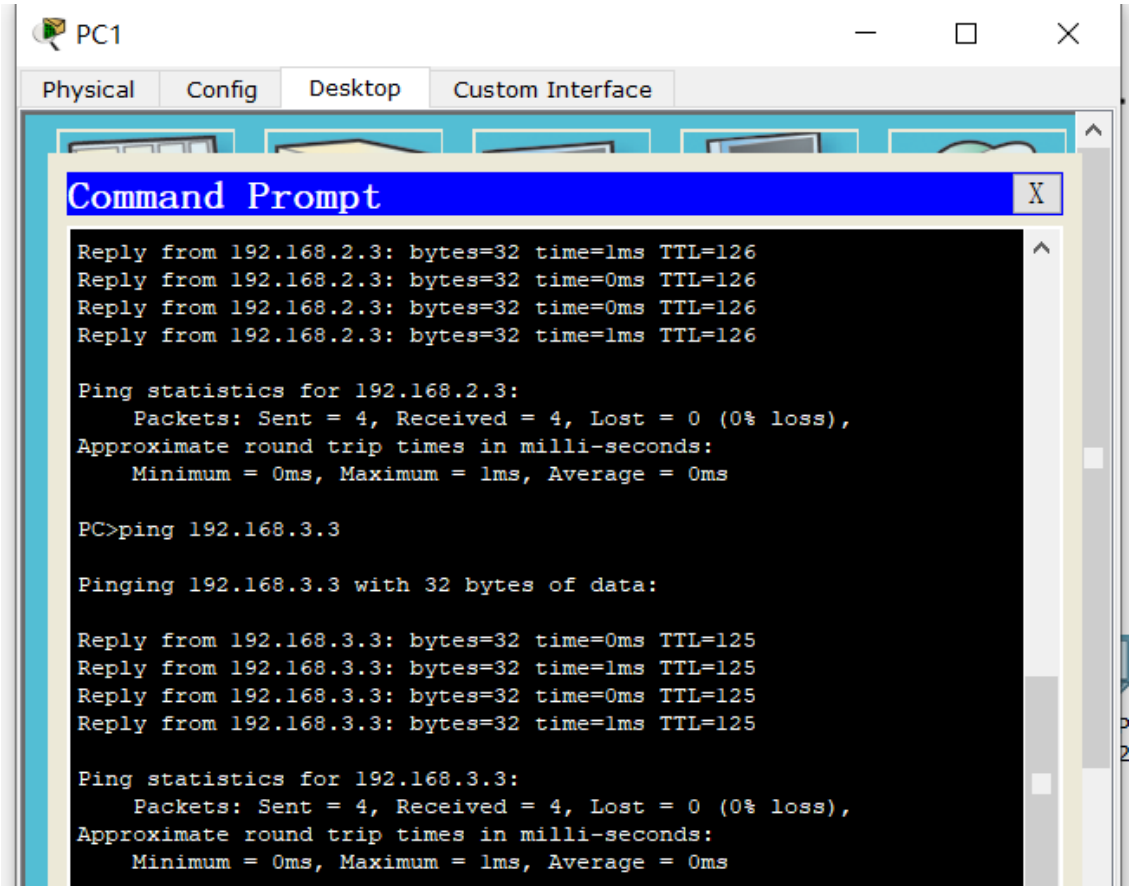
设置路由器静态路由表，将无法由该路由器直达的网段配置下一跳地址。以Router1为例, 配置到`192.168.3.0`， `192.168.2.2`，`10.2.3.0`的下一跳地址即可，然后使用`show ip route`命令确认配置正确:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip route 192.168.3.0 255.255.255.0 10.0.1.2
Router(config)#ip route 192.168.2.0 255.255.255.0 10.0.1.2
Router(config)#ip route 10.2.3.0 255.255.255.0 10.0.1.2
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
show ip route
Codes: C - connected, S - static, I - IGRP, 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

     10.0.0.0/24 is subnetted, 2 subnets
C       10.0.1.0 is directly connected, FastEthernet0/0
S       10.2.3.0 [1/0] via 10.0.1.2
C    192.168.1.0/24 is directly connected, FastEthernet0/1
S    192.168.2.0/24 [1/0] via 10.0.1.2
S    192.168.3.0/24 [1/0] via 10.0.1.2
Router#
```

Router2和Router3同理，这里不再赘述。

3个子网之间的**Ping测试**均成功，下面以2-1，1-3截图为例。

1. `PC1` ping `Laptop3`



2. `Router2` ping `Router1`

```
Router#ping 10.0.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

任务五

凯撒的观点存在问题。RIP协议的上限是16跳，以用于防止环路。如果一个网络的直径不超过15就可以使用RIP协议。如果存在16个设备连成一条链，那么就不能使用RIP协议。此小型网络可以使用RIP协议，但是应该注意到，RIP记录路由器上转发的次数，在子网内使用的是广播，不会计算在跳数中。所以得出“16台”的统计不准确，不应囊括子网内的终端设备。

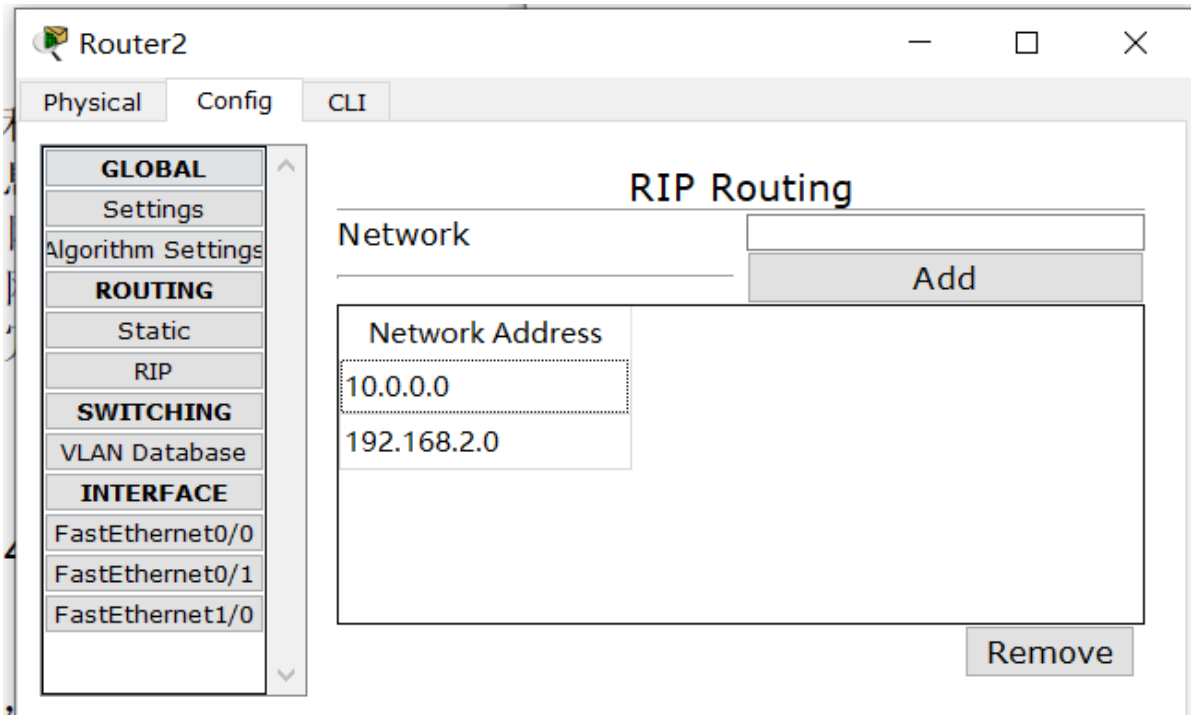
当前网络有3个路由器，最多跳2次，可以使用RIP协议。

因此我最终选择**RIPv2路由协议**维护目前的局域网。下面进行协议的配置。

为了保证设备之间能够通信，需要对每个路由器设置动态路由。首先**删除静态路由**。

```
Router#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip route 192.168.1.0 255.255.255.0 10.0.1.1
Router(config)#no ip route 192.168.3.0 255.255.255.0 10.2.3.2
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
 show ip route
Codes: C - connected, S - static, I - IGRP, 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

     10.0.0.0/24 is subnetted, 2 subnets
C       10.0.1.0 is directly connected, FastEthernet0/0
C       10.2.3.0 is directly connected, FastEthernet1/0
C    192.168.2.0/24 is directly connected, FastEthernet0/1
Router#
```

再使用`network xxx.xxx.xxx.xxx`命令**配置动态路由**对应的网段。这里以Router2为例，配置网段`192.168.2.0`和`10.0.0.0`即可。



3个子网之间的**Ping测试**均成功，下面以3-2，1-3截图为例。

`Laptop3` ping `PC2`：

```
PC>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=0ms TTL=126
Reply from 192.168.2.2: bytes=32 time=0ms TTL=126
Reply from 192.168.2.2: bytes=32 time=0ms TTL=126
Reply from 192.168.2.2: bytes=32 time=0ms 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
```

`Router1` ping `Laptop3`

```
Router>ping 192.168.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Bonus

1.使用`secret`指令在配置文件中进行加密存储，并探究加密方式。

当密码明文为`lhzconquer`时，对应的密文如下图所示：

```
Router(config)#enable secret lhzconquernew
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
show run
Router#show running-config
Building configuration...

Current configuration : 827 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
enable secret 5 $1$mERr$pwTRL090R8tIxU4yiEGBQ.
enable password lhzconquer
!
```

下面探究密码用何种方式加密，我测试了密码`abc`,`abd`,`abe`的密文：

```
Router(config)#enable secret abc
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
show run
Router#show running-config
Building configuration...

Current configuration : 872 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router
!
!
!
enable secret 5 $1$mERr$Dbe7RlLE8b8xdz/DJoO0U0
```

对应关系如下

```
abc: enable secret 5 $1$mERr$Dbe7RlLE8b8xdz/DJoO0U0
abd: enable secret 5 $1$mERr$cbUmFZ.XJu464pawQrOkQ0
abe: enable secret 5 $1$mERr$JTqCLq..XVxuhAJRfJN7C0
```

查阅资料得知，`secret 5`和`1`指MD5，`mERr`是salt，在ubuntu下使用`openssl`验证:

```
lhz@lhz:/mnt/c/Users/lenovo/Desktop$ openssl passwd -1 -salt mERr -table abc
abc      $1$mERr$Dbe7RlLE8b8xdz/DJoO0U0
lhz@lhz:/mnt/c/Users/lenovo/Desktop$ openssl passwd -1 -salt mERr -table abd
abd      $1$mERr$cbUmFZ.XJu464pawQrOkQ0
lhz@lhz:/mnt/c/Users/lenovo/Desktop$ openssl passwd -1 -salt mERr -table abe
abe      $1$mERr$JTqCLq..XVxuhAJRfJN7C0
```

可以看到密文完全一致。

因此`enable secret`命令是将密码用**加盐(`mERr`)的MD5算法**加密的。

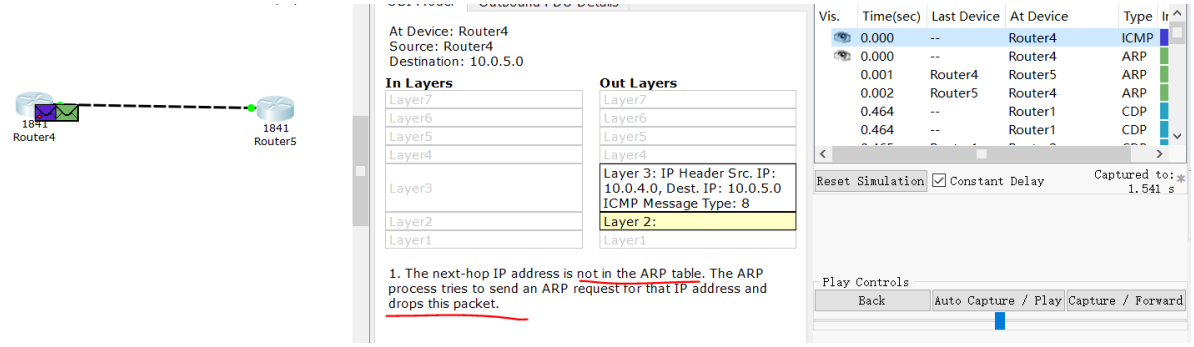
2.任务4中，配置好静态路由后，在第一次发起ping测试时会出现丢包的象。 请用你掌握的网络知识来解释这一情况。

ping第一个是ARP广播包，建立MAC地址和IP地址对应表。因为一开始是不知道对方的MAC地址，所以会丢包。

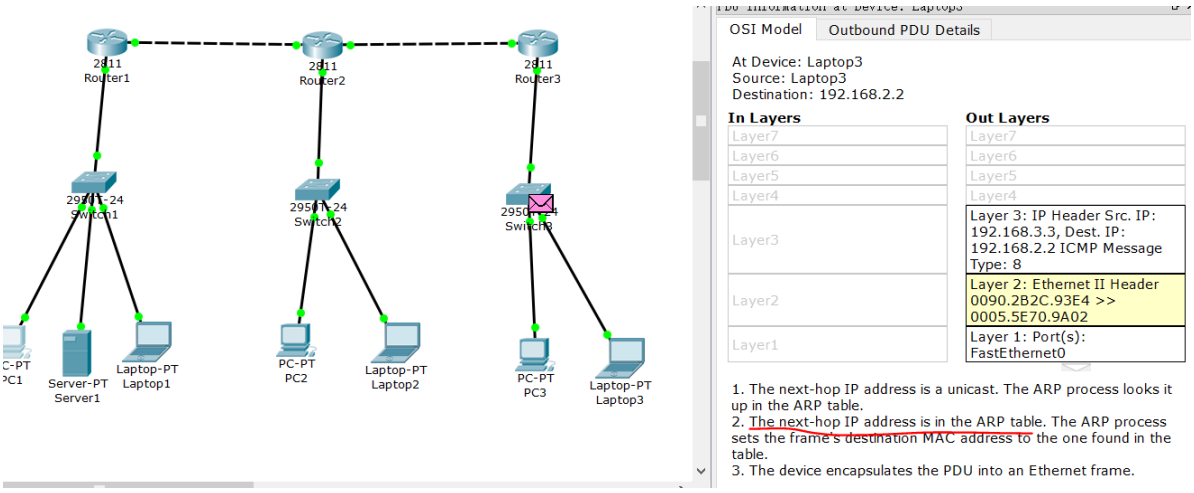
具体来讲，当ICMP将数据交给IP要求发出的时候，在互联网层是要经过路由决策的。数据链路层在封装之前要检查目标IP地址是否在本地的ARP缓存中。因为在发送第一个包时是没有ARP映射的，于是ARP将会发起一个请求用于获取目标MAC地址，并且丢弃这个数据包。

下面用该软件simulation功能进行**模拟**, 因为前面的设备都已经ping过，所以我另外**构建了2个路由器的简单拓扑**进行**第一次Ping测试**。

如下图所示，可以看到在**第一次Ping测试**的时候，因为下一跳IP地址不在ARP table中，所以ARP会发起请求获得目标IP地址，并且**丢包**。



如果是**第二次发起ping测试**的，可以看到下图显示IP地址已经在ARP Table中，所以成功ping到。



实验小结

本次实验充满趣味性又锻炼了能力，让我在网安课上学到的知识有了实践性的感悟，也让我对计网课上学到的较为枯燥的IP、路由等知识有了更加深刻的理解。非常感谢老师和助教们的精心设计和悉心指导，让我感受到了网络与网络安全的实用性与魅力！