

《计算机网络安全技术》课后作业

2017 秋季 • 40240572 • 主讲：尹霞

姓名： 乔一凡

学号： 2015011398

作业题目：体验网络配置

任务一

首先小于 router3 的端口 1 配置错误。因为 20 开头的 IP 是公网 IP，不能用于内网。可以将 router3 的端口 1 的 IP 配置为 10.2.3.3。

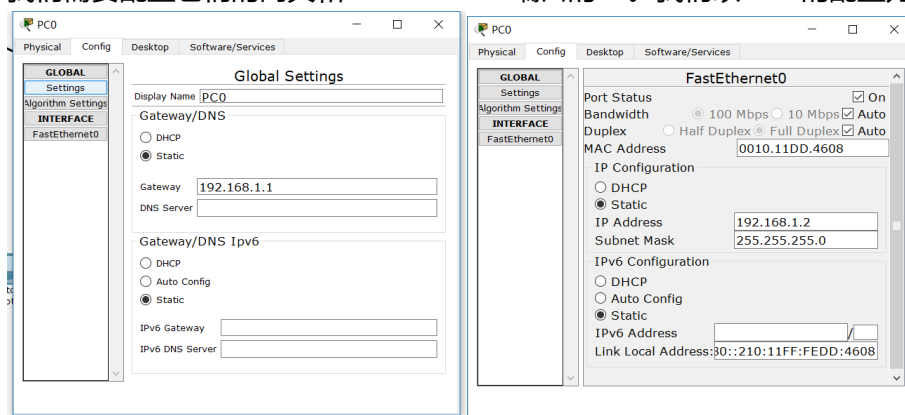
对于 router2 的端口 2，由于该端口是与 router3 相连的，故它们应当处于同一子网中，我们设置其 IP 应该为 10.2.3.x，其中 x 可以是 0-255 中 3 除外的任意值，我们这里选择其 IP 为 10.2.3.1。

Server0 处在 router1 的端口 1 所在的子网内，因此其网关应设置为 router1 的端口 1 的 IP，即 192.168.1.1。

网络铺设主要分为以下几个步骤：

1. 选择合适的设备和连线将网络整体结构搭建好，此时看到 router 的连线断电均为红色，说明网络还没有配置成功。以下我们分别配置 pc, server, laptop 和 router。
2. PC, server, laptop 的配置

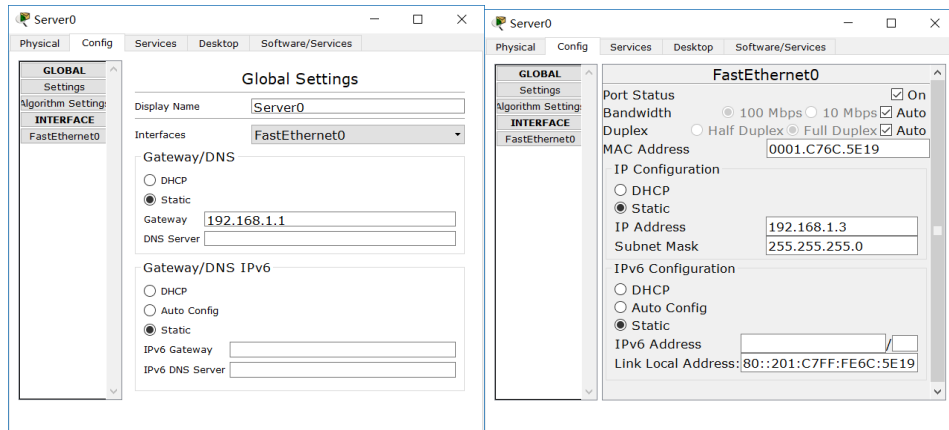
我们需要配置它们的网关和 FastEthernet 端口的 IP。我们以 PC0 的配置为例说明：



如上图所示配置。对于 server 和 laptop 来说也是同理。

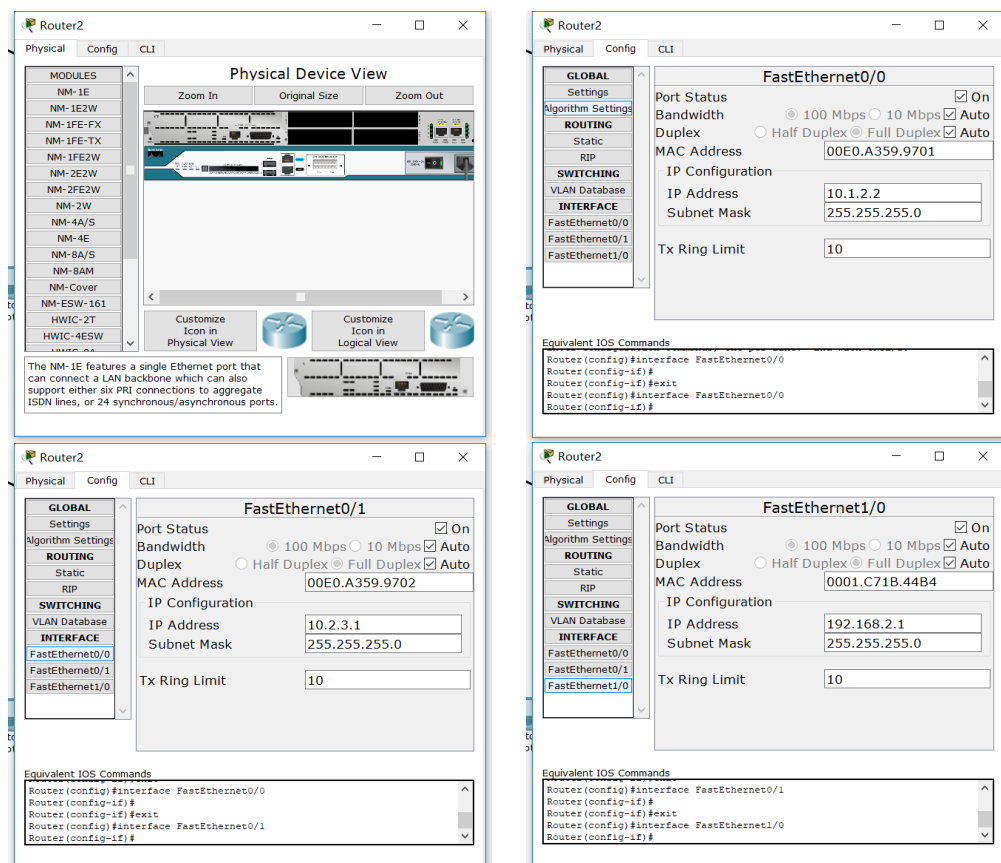
《计算机网络安全技术》课后作业

2017 秋季 • 40240572 • 主讲：尹霞



3. Router 的配置

对于 router，我们同样需要配置其端口的 IP 地址。我们这里以 router2 为例。由于 router2 需要 3 个 FastEthernet 端口，我们首先要给他增加一块 NM-1FE-TX 扩展模块，之后进行接线配置。设置如下：



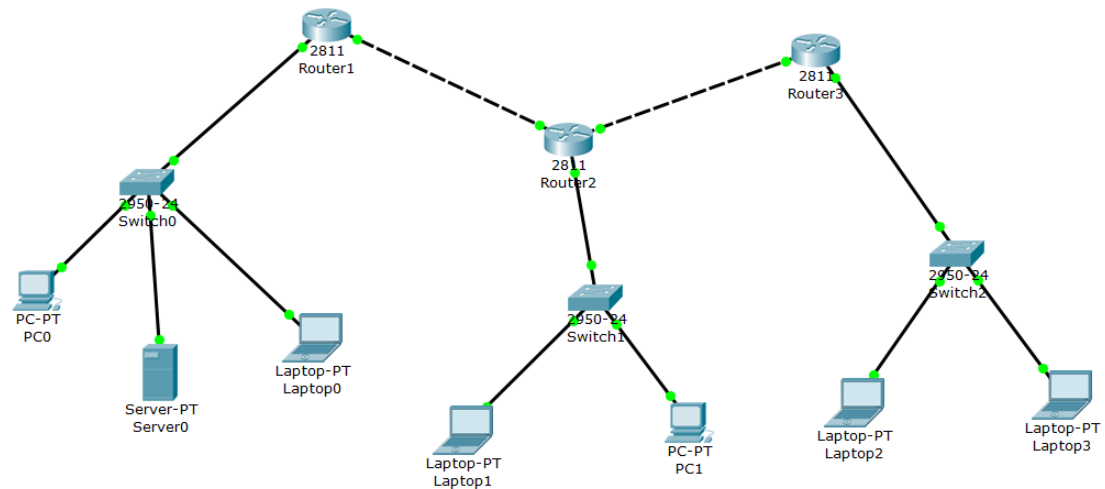
4. 最终网络连通，所有节点均为绿色。如下图所示：

任务二 公网网关安全

需要在 router1 的 CLI 界面设置三种口令。具体设置如下所示：

《计算机网络安全技术》课后作业

2017 秋季 • 40240572 • 主讲：尹霞



在 CLI 中如下操作：

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#password conspw
Router(config-line)#login
Router(config-line)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#enable password privpw
Router(config)#line vty 0 4
Router(config-line)#password telnpw
Router(config-line)#login
Router(config-line)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

设置后查看 running config: (节选)

Password2:

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

Current configuration : 721 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
enable password privpw
!
!
!
```

Password1 与 Password3:

《计算机网络安全技术》课后作业

2017 秋季 • 40240572 • 主讲：尹霞

```
line con 0
 password conspw
 login
!
line aux 0
!
line vty 0 4
 password telnpw
 login
!
!
!
end

Router#
```

可见设置成功。

但是从上面的过程我们也可以看到路由器的配置文件中密码使用明文保存, 如果配置文件泄露则密码也会公开, 故我们需要启用密码加密。

使用如下命令启用加密:

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

查看配置文件:

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

Current configuration : 748 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router
!
!
enable password 7 08315E471F0912
!
line con 0
 password 7 082243401A0912
 login
!
line aux 0
!
line vty 0 4
 password 7 08354942070912
 login
```

可见已经成功加密保存。

任务三 各部门正常通信

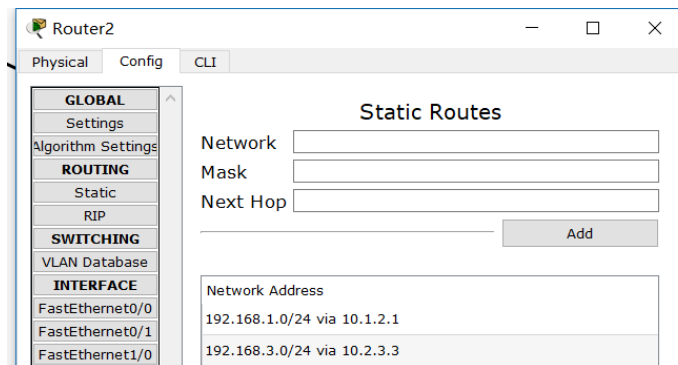
由于各个部门在不同的子网内, 在没有配置路由的情况下各个部门间无法通行, 仅能 ping 通子网内部的终端。

我们通过配置静态路由的方法实现配置。

《计算机网络安全技术》课后作业

2017 秋季 • 40240572 • 主讲：尹霞

以 router2 的静态路由表为例：



路由器识别发往不同部门子网的包，并将这些包向相应路由器的端口发送。其余两个路由器配置同理。最终连通后我们使用 pc0 对三个子网中的终端进行 ping 操作：

```
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=0ms TTL=126
Reply from 192.168.2.3: bytes=32 time=0ms TTL=126
Reply from 192.168.2.3: bytes=32 time=0ms TTL=126
Reply from 192.168.2.3: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=0ms TTL=125
Reply from 192.168.3.3: bytes=32 time=0ms TTL=125
Reply from 192.168.3.3: bytes=32 time=0ms TTL=125
Reply from 192.168.3.3: bytes=32 time=0ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

使用 laptop1 进行 ping：

《计算机网络安全技术》课后作业

2017 秋季 • 40240572 • 主讲：尹霞

```
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

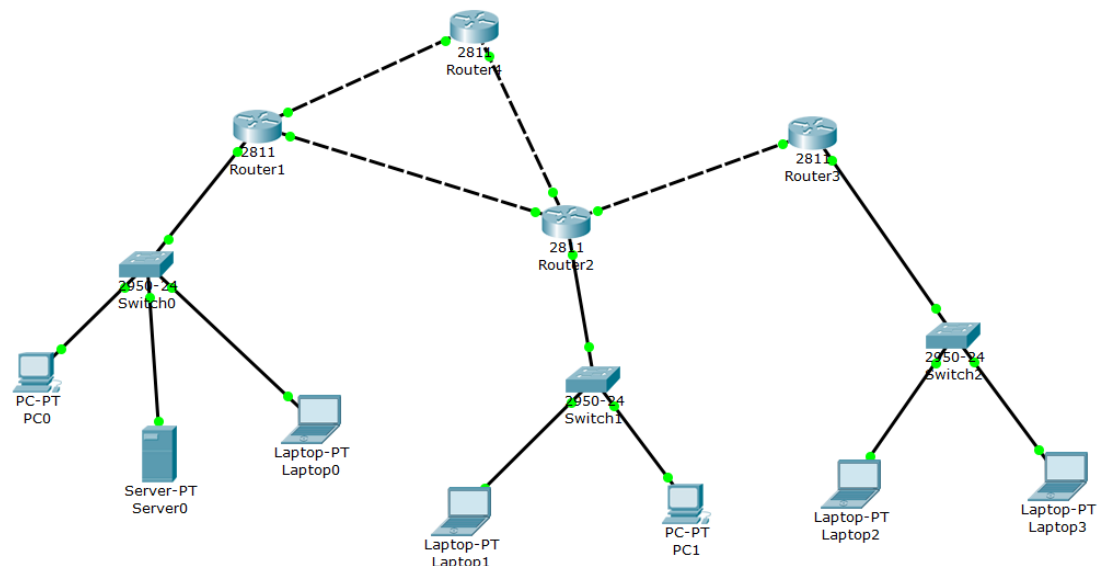
Reply from 192.168.1.1: bytes=32 time=0ms TTL=254
Reply from 192.168.1.1: bytes=32 time=0ms TTL=254
Reply from 192.168.1.1: bytes=32 time=1ms TTL=254
Reply from 192.168.1.1: bytes=32 time=0ms TTL=254

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 = 1ms, Average = 0ms
```

可见各部门可以正常通信。

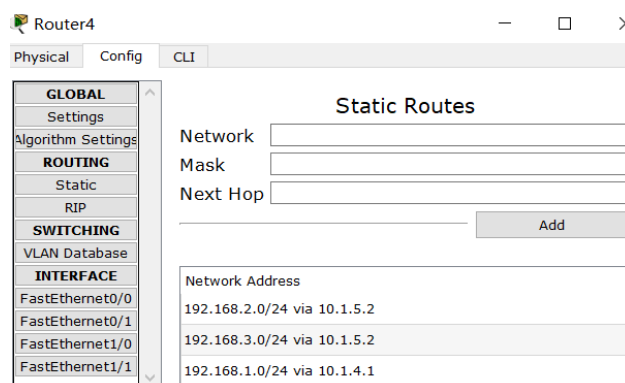
任务四 避免设备故障带来的影响

需要新加一个路由器，并于 router1 和 router2 相连，作为一条备用链路。连接如下：



仍需要按照上面的方式配置 router4 的端口 IP 和路由表，同时在 router1 与 router2 中添加向 router4 发送的路由表项。

以对 router4 的配置为例：

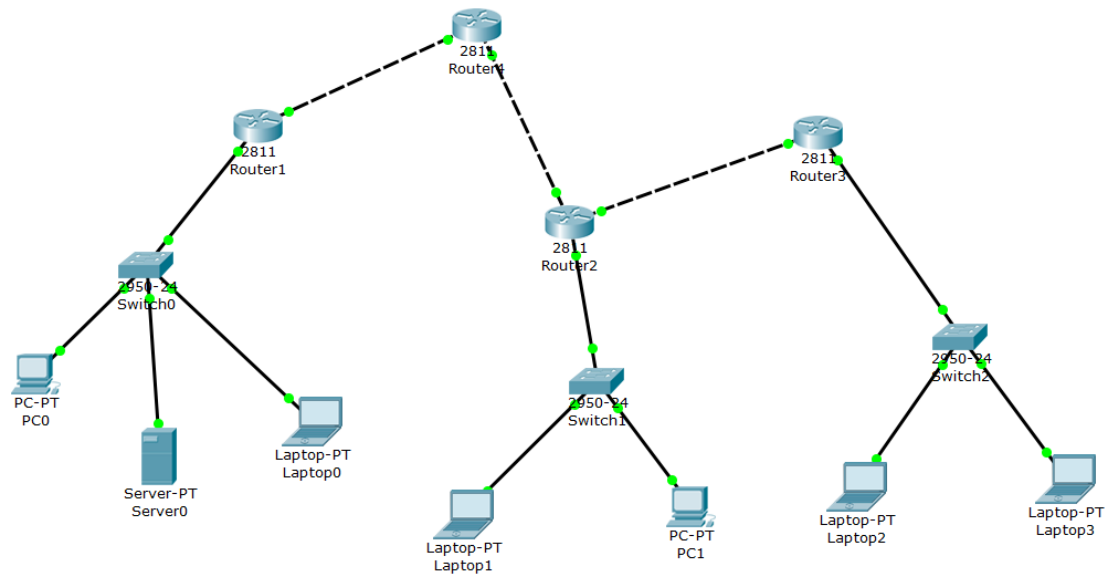


《计算机网络安全技术》课后作业

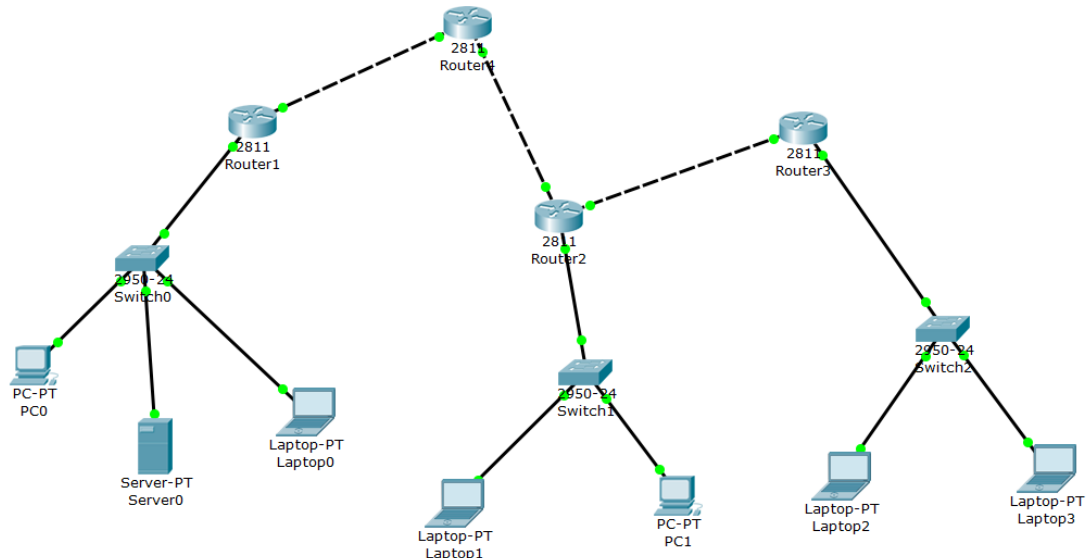
2017 秋季 • 40240572 • 主讲：尹霞

FastEthernet0/0		FastEthernet0/1	
Port Status	<input checked="" type="checkbox"/> On	Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto	Bandwidth	<input type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input type="radio"/> Half Duplex <input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto	Duplex	<input type="radio"/> Half Duplex <input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
MAC Address	0002.1765.6A01	MAC Address	0002.1765.6A02
IP Configuration		IP Configuration	
IP Address	10.1.4.2	IP Address	10.1.5.1
Subnet Mask	255.255.255.0	Subnet Mask	255.255.255.0
Tx Ring Limit	10	Tx Ring Limit	10

最终配置完成后网络如下：



假设 router1 与 router2 中间线路出现故障，删去这条连线：



使用 PC0 对其他子网主机进行 ping 操作，成功。

任务五 人员精简计划

此时对于访问控制的要求规则较为复杂，使用扩展 IP ACL 进行流量控制。对 router3 配

《计算机网络安全技术》课后作业

2017 秋季 • 40240572 • 主讲：尹霞

置如下：

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip ac
Router(config)#ip access-list 10
Router(config)#access-l
Router(config)#access-list 100 permit ip 192.168.3.3 0.0.0.0 192.168.1.2
0.0.0.0
Router(config)#access-list 100 permit ip 192.168.3.3 0.0.0.0 192.168.2.2
0.0.0.0
Router(config)#inter
Router(config)#interface fa0/0
Router(config-if)#ip acces
Router(config-if)#ip access-group 100 out
Router(config-if)#exit
Router(config)#
```

此时经过测试，除 PC0 与 PC1 外的中断都无法访问 laptop0。

为了使 server0 可以 ping 到 laptop0，我们设置 CBAC 允许 icmp 协议包通过，如下：

```
Router(config)#ip inspect name CBAC icmp
Router(config)#inte
Router(config)#interface fa0/0
Router(config-if)#ip insp
Router(config-if)#ip inspect CBAC in
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

配置后 server0 可以 ping 通 laptop0。

任务六 利用协议进行路由管理

使用 RIPv2 协议配置动态路由。对每个路由器配置。以 router1 为例：

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#no auto-summary
Router(config-router)#net 192.168.1.0
Router(config-router)#net 10.1.2.0
Router(config-router)#net 10.1.4.0
Router(config-router)#exit
Router(config)#
Router(config)#no ip route 192.168.2.0 255.255.255.0 10.1.4.2
Router(config)#no ip route 192.168.3.0 255.255.255.0 10.1.2.2
Router(config)#no ip route 192.168.3.0 255.255.255.0 10.1.4.2
Router(config)#no ip route 192.168.2.0 255.255.255.0 10.1.2.2
```

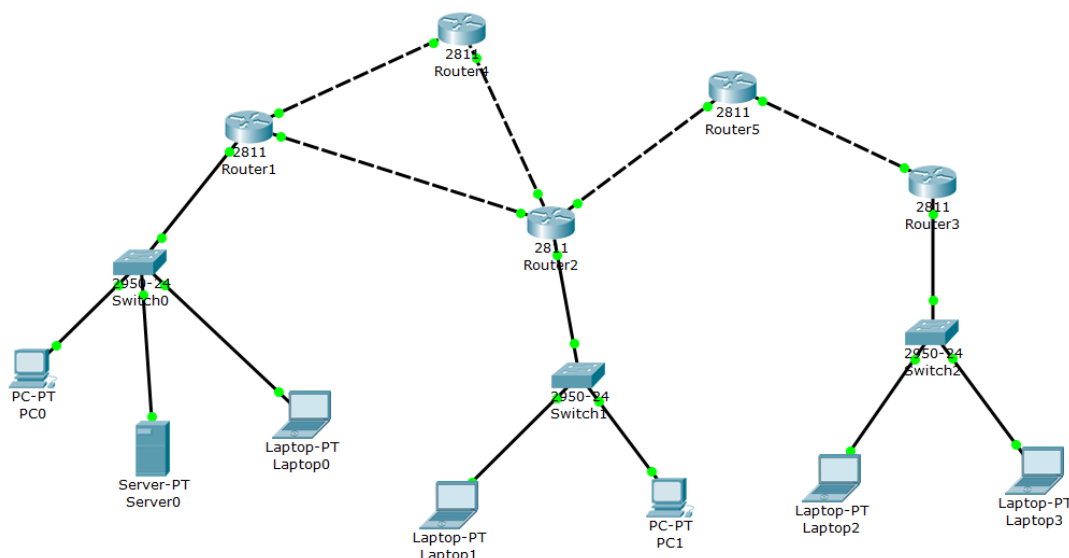
配置完成后使用 PC0 对 laptop0 进行 ping，成功，说明 RIP 配置路由正确。

任务七 IPsec VPN 跨越公网

设置 router2 的公网 IP 为 100.0.0.1，router3 的公网 IP 为 100.0.1.1，并使用 router5 表示公网路由，模拟公网，在其中不配置子网路由的 IP。此时的网络拓扑图如下：

《计算机网络安全技术》课后作业

2017 秋季 • 40240572 • 主讲：尹霞



分别在 router2 和 router3 上配置 IPsec VPN 如下 (以 router3 为例):

主要思路是先设置 IKE 协商策略, 设置加密算法为 des, 认证算法为 md5, 同时设置对端地址为另一个 router (router2 则设置 router3 的地址, router3 设置 router2 的地址, 同时确保加密密钥匹配。

之后配置 IPsec 传输模式, 定义 VPN 的认证类型。

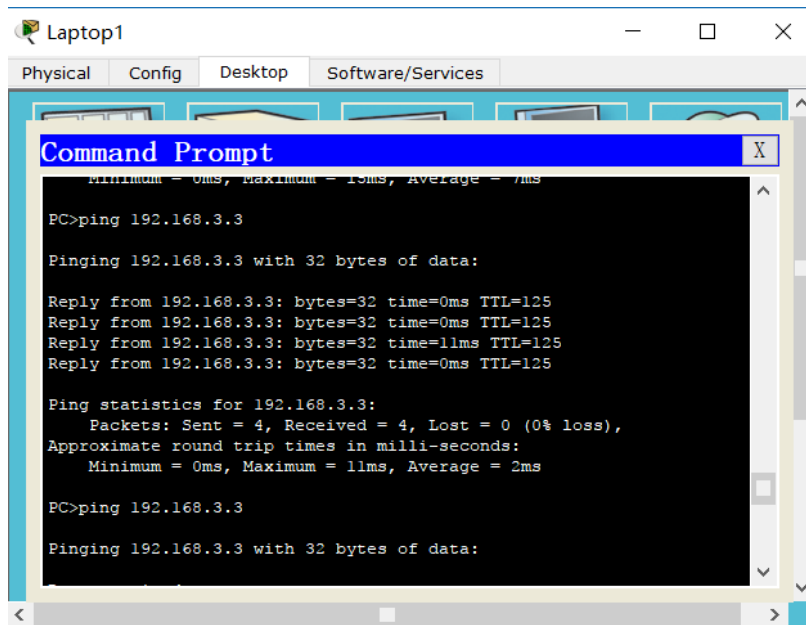
在最后配置加密映射 crypto map, 并将其应用到对应公网接口上, 使 VPN 生效。

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#enc
Router(config-isakmp)#encryption des
Router(config-isakmp)#hash md5
Router(config-isakmp)#auth
Router(config-isakmp)#authentication pre
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 10000
Router(config-isakmp)#exit
Router(config)#crypto isakmp key qyfvpn address 100.0.0.1
Router(config)#access-1
Router(config)#access-list 100 permit ip 192.168.3.3 0.0.0.255
192.168.2.1 0.0.0.255
Router(config)#crypto ipsec tra
Router(config)#crypto ipsec transform-set qyfvpn esp-des esp-sha-hmac
Router(config)#crypto ipsec sec
Router(config)#crypto ipsec security-association lifetime seconds 1800
Router(config)#crypto map qyfmap 1 ipsec isakmp
Router(config-crypto-map)#set peer 100.0.0.1
Router(config-crypto-map)#set tra
Router(config-crypto-map)#set transform-set qyfypn
ERROR: transform set with tag qyfypn does not exist.
Router(config-crypto-map)#set transform-set qyfvpn
Router(config-crypto-map)#match address 100
Router(config-crypto-map)#exit
Router(config)#int fa0/0
Router(config-if)#crypto map qyfmap
*Jan 3 07:16:26.785: %CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
Router(config-if)#exit
```

最终配置完成后使用 Laptop1 去 ping Laptop0 (此时已删除之前的 ACL), 可以 ping 通, 且通过抓包发现流量为 ipsec 流量, 配置完成。

《计算机网络安全技术》课后作业

2017 秋季 • 40240572 • 主讲：尹霞



```
PC>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=0ms TTL=125
Reply from 192.168.3.3: bytes=32 time=0ms TTL=125
Reply from 192.168.3.3: bytes=32 time=11ms TTL=125
Reply from 192.168.3.3: bytes=32 time=0ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 2ms

PC>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:
```