

2019 年秋学期《计算机网络安全技术》实验一

网络搭建及路由协议 实验报告

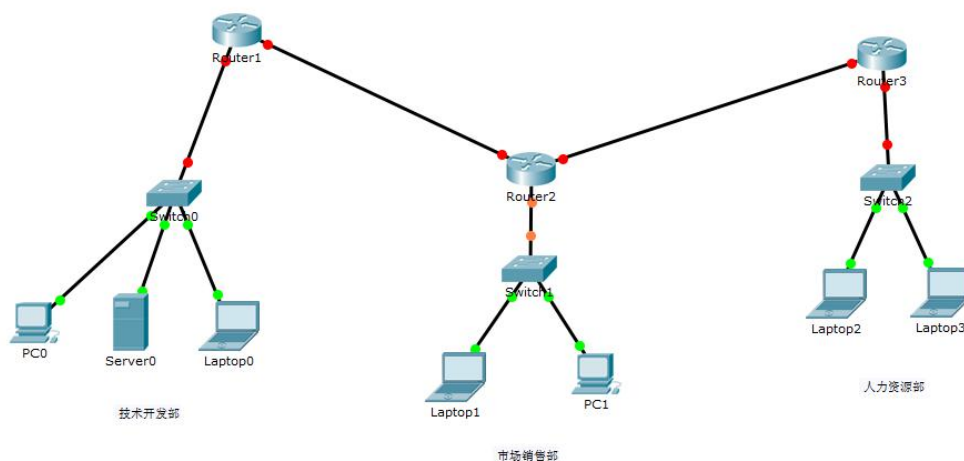
陈张萌 2017013678 计 74

请根据下面的实验介绍，完成各个任务。给出证明自己完成了实验的必要文字描述和截图。本实验要求提交实验报告，配置文件自存。

实验背景

近日，T 公司从大兴区搬迁至了宇宙中心五道口，因此身为公司网络管理员的你需要在公司新址进行内网的重新设计与部署。在这次重部署的过程中，你希望使公司网络能够更加安全、高效地发挥作用。目前公司主要分为三个部门：技术开发部、市场销售部和人力资源部。由于分工不同，各个部门均选用不同的子网便于管理。你的助手小杨已经为你拟定了一份设计草案如下：

网络预拓扑



技术开发部 (192.168.1.0/24) : Router1, Switch0, Server0, PC0, Laptop0

市场销售部 (192.168.2.0/24) : Router2, Switch1, PC1, Laptop1

人力资源部 (192.168.3.0/24) : Router3, Switch2, Laptop2, Laptop3

IP 分配方案

Device	Port	IP	Mask	Gateway	实际使用的 端口
Router1	端口 1	192.168.1.1	/24	-	0/0
	端口 2	10.1.2.1	/24	-	0/1
Router2	端口 1	10.1.2.2	/24	-	0/1
	端口 2	10.1.3.2	/24	-	1/0
	端口 3	192.168.2.1	/24	-	0/0
Router3	端口 1	10.1.3.1	/24	-	0/1
	端口 2	192.168.3.1	/24	-	0/0
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	

任务 1 粗心的小杨 3'

作为一名资深的网络管理员，你很快就发现小杨不小心将两滴墨水溅在了 IP 分配方案上，不仅如此，经验不足的他在分配 IP 时还出现了一个纰漏。请补全方案，并将方案有错的地方指出并更正。为了便于网络管理，请尽可能用便于记忆的方式规划 IP 地址。

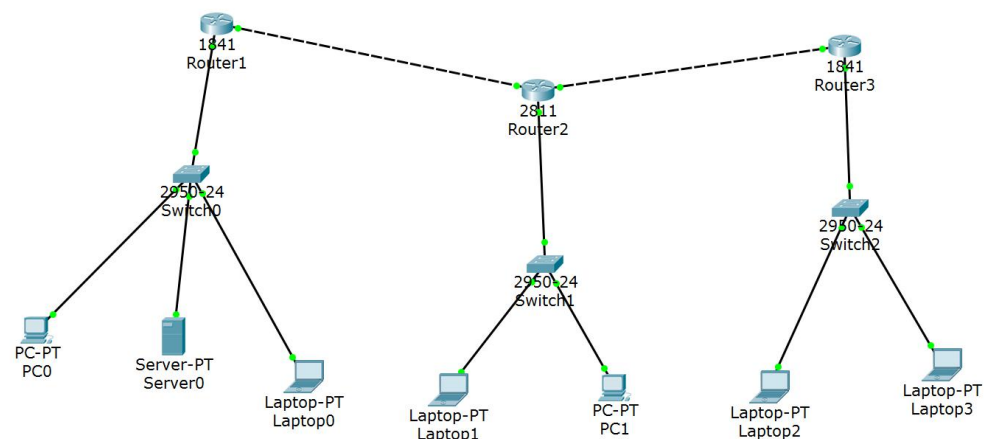
根据网络预拓扑图可以得到 Server0 的网关和 PC0 的网关是一样的，Router3 的端口 1 和 Router2 的端口 2 位于同一个子网当中，因此应该分配同一个子网当中的 ip。但是 Router2 的端口 2 使用了 20 开头的地址，这是一个公有 ip。因此将 Router2 的端口 2 和 Router3 的端口 1 都修改为私有 ip。

最终分配方案如上表所示。

任务 2 网络铺设 2'

在完善铺设方案后，请选择合适的设备及连线将该网络铺设出来，并且为各个接口配置对应的 IP 等属性。请提供必要的截图向经理证明，在网络铺设过程中你亲自参与了铺设。

最终网络铺设结果如下图所示：



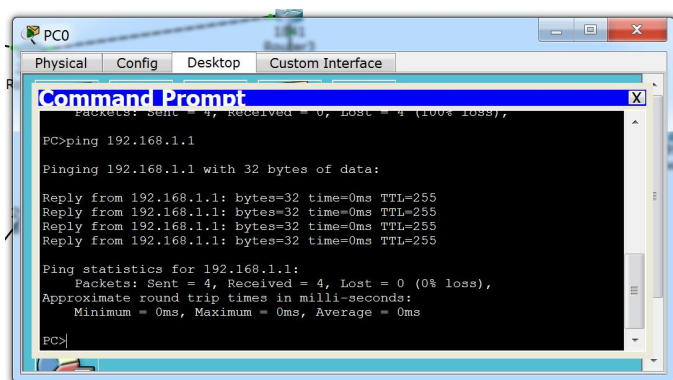
需要注意以下几点：

- 1.路由器和路由器之间应使用交叉线来连接，其他都应使用直连线
- 2.路由器连接均使用快速以太网口。子网 2 的路由器需要 3 个端口，为此选用 2811 型号的路由器（有 4 个快速以太网口）。为了防止混淆在题目所给的表格中我新加了一列用来表明实际使用的快速以太网口的名称。

以 Router1 为例命令行配置如下：

```
Router1
Physical Config CLI
IOS Command Line Interface
192.168.0.0>enable
192.168.0.0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
192.168.0.0(config)#interface FastEthernet0/0
192.168.0.0(config-if)#
192.168.0.0(config-if)#exit
192.168.0.0(config)#interface FastEthernet0/1
192.168.0.0(config-if)#
192.168.0.0(config-if)#exit
192.168.0.0(config)#interface FastEthernet0/1
192.168.0.0(config-if)#
192.168.0.0(config-if)#exit
192.168.0.0(config)#interface Serial0/0/1
192.168.0.0(config-if)#
192.168.0.0(config-if)#exit
192.168.0.0(config)#interface Serial0/0/1
192.168.0.0(config-if)#
192.168.0.0(config-if)#exit
192.168.0.0(config)#interface FastEthernet0/1
192.168.0.0(config-if)#ip address 10.1.1.1 255.0.0.0
192.168.0.0(config-if)#
192.168.0.0(config-if)#exit
192.168.0.0(config)#interface FastEthernet0/1
192.168.0.0(config-if)#ip address 10.1.1.1 255.255.255.0
192.168.0.0(config-if)#
192.168.0.0(config-if)#exit
192.168.0.0(config)#interface FastEthernet0/1
192.168.0.0(config-if)#
```

在配置完成后，每一子网内部的所有设备可以互相 ping 通。以 PC0 为例，ping 网关：



任务3 公网网关安全 7'

公网与公司内网的接入点位于技术开发部的 Router1 上，为了防止他人的恶意入侵，你需要至少给 Router1 设置登录口令。你一共需要为它设置三种口令：通过 console 口进入用户模式的口令 password1，用户模式进入特权模式的口令 password2，通过 telnet 方式登录路由器的口令 password3。

请至少在 Router1 上设置上述三种口令，在假设路由器配置文件不会泄露的情况下，自行用适合的口令保证路由器一定程度上的登录安全。如果路由器配置文件可能泄露，你的设置是否有所变化？

1.在路由器上通过 console 口进入用户模式的 password1

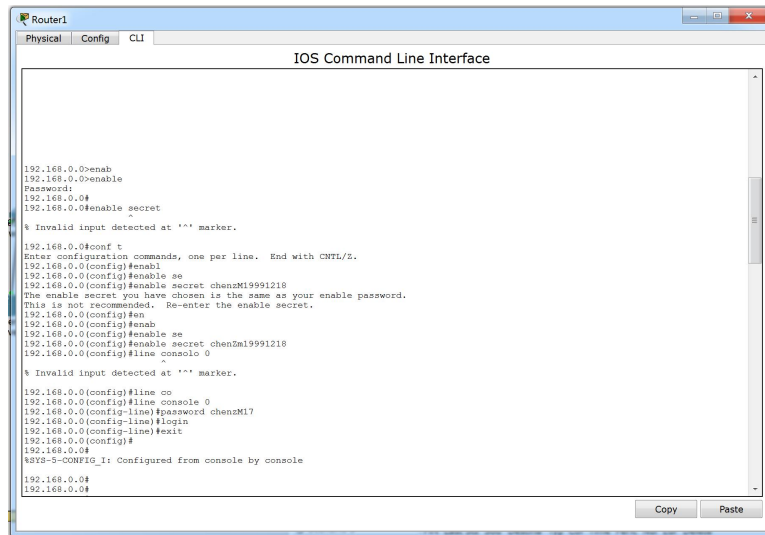
设置登陆密码为 chenzM17

2.在路由器上进入特权模式的 password2

设置登陆密码为 chenzM19991218.如果路由器配置文件可能泄露，设置 secret 为 chenzM19991218

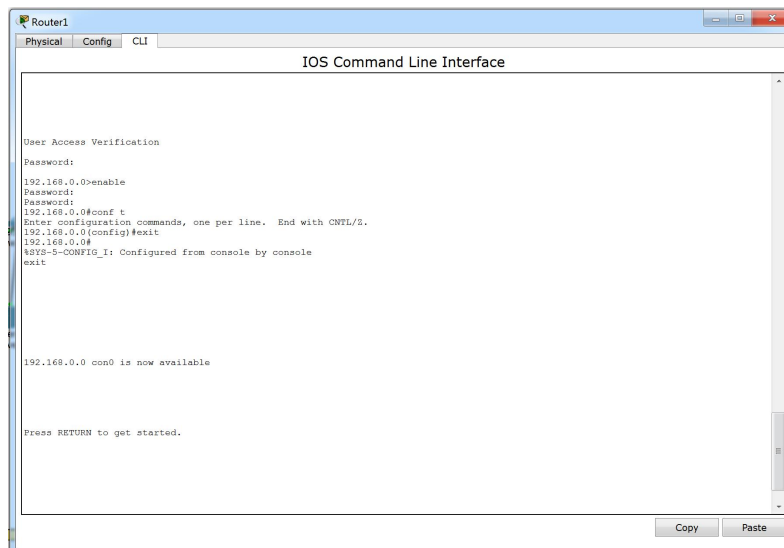


3.设置 telnet 方式访问路由器的登陆密码为 chenzM17

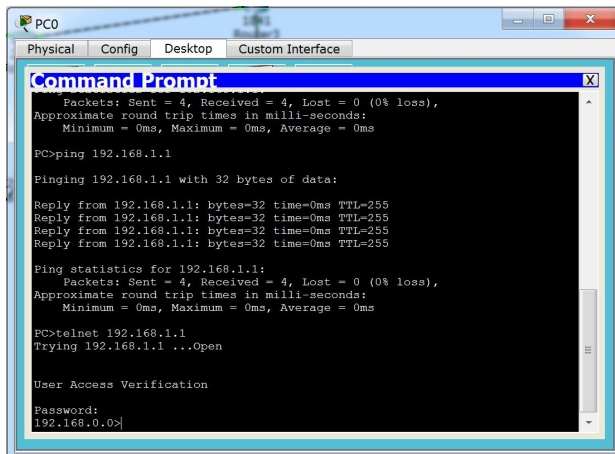


4.验证以上三种密码:

(1)进入用户模式和特权模式时需要输入密码。验证进入特权模式时的输入 password 不可以, 应当输入 secret。



(2)在 PC0 上使用 telnet 方式登录:



5.假设路由器的配置文件不会泄露，那么在进入特权模式时配置 password 即可。如果配置文件可能泄露，那么需要设置 secret，而且 secret 的密码不应该和 password 相同。

6.与 Route1 设置方式同理设置 Route2 和 Route3 的密码

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 (2) 总长六位的混合有数字及小写字母的密码 (3) 总长六位的混合有数字、大写字母、小写字母的密码 (4) 总长八位的混合有数字、大写字母、小写字母的密码

(1) 数字共有 10 个，破解时间为 10^6

(2) 数字和小写字母共 $10+26=36$ 个，破解时间为 $36^6=2.2 \times 10^9$

(3) 数字、小写字母、大写字母共 $10+26 \times 2=62$ 个，破解时间为 $62^6=5.7 \times 10^{10}$

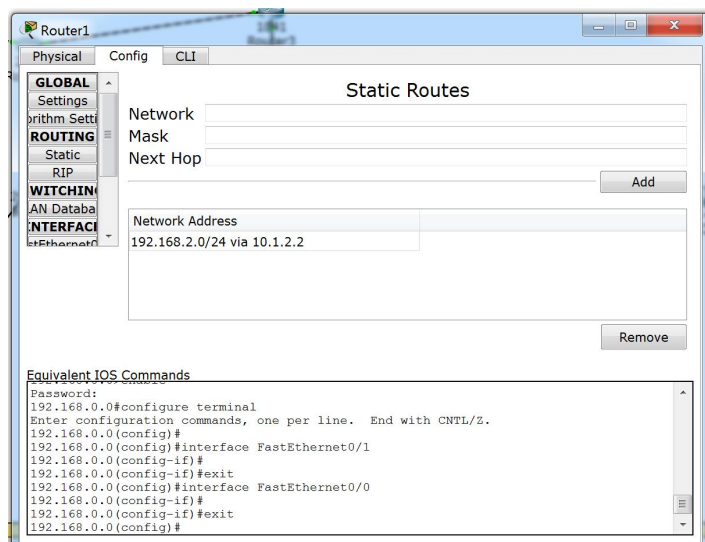
(4) 数字、小写字母、大写字母共 $10+26 \times 2=62$ 个，破解时间为 $62^8=2.2 \times 10^{14}$

以计算机每秒尝试 10^9 估计，破解(1)所用时间约 1ms，破解(2)所用时间约 2.2s，破解(3)所用时间约 1 分钟，破解(4)所用时间约 61h。

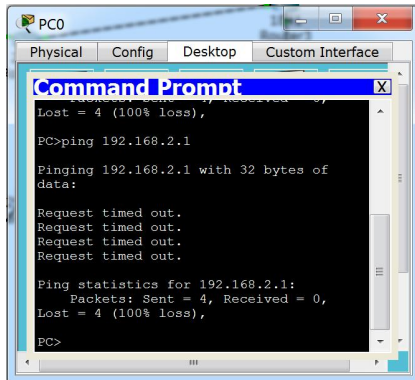
任务 4 静态路由能保障网络通信 4'

在铺设好网络之后，你想要测试一下公司的各个部门网络是否联通，ICMP 协议为你提供了合适的网络控制信息进行探测。由于公司的网络结构相对简单，你决定使用静态路由保证内网的正常通信。然而静态路由的不当使用容易给网络维护带来不便，例如，当公司网络进行扩展时，冗余的静态路由也可能对新网络产生影响。因此，请在不使用冗余的静态路由的前提下，让三个部门能够相互通讯。

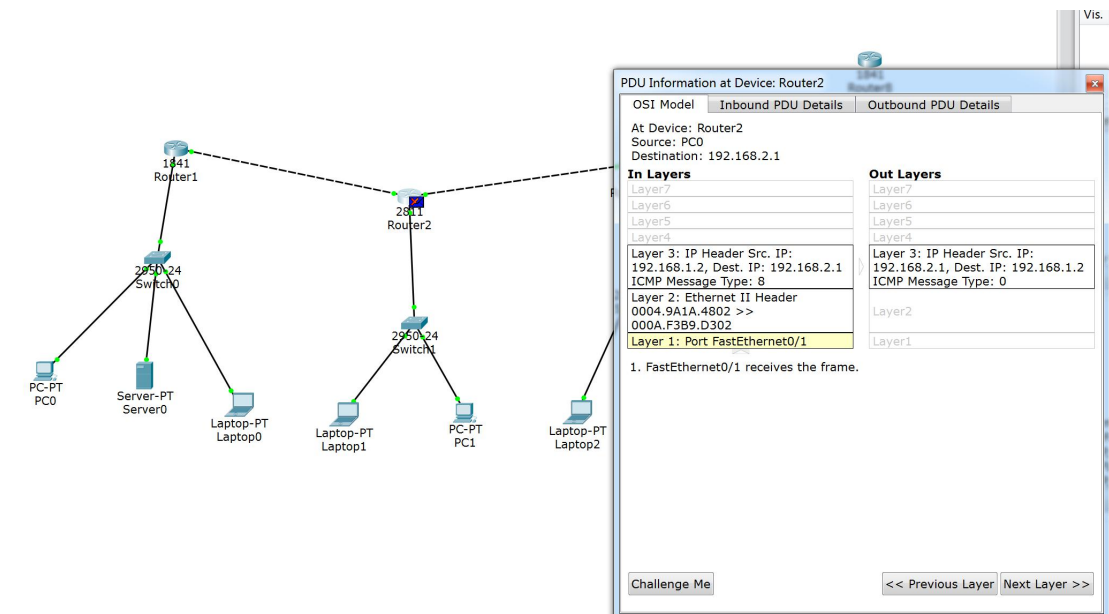
先配置子网 1 到子网 2 之间的静态路由。配置 Router1 的路由表，配置完成后结果如下：



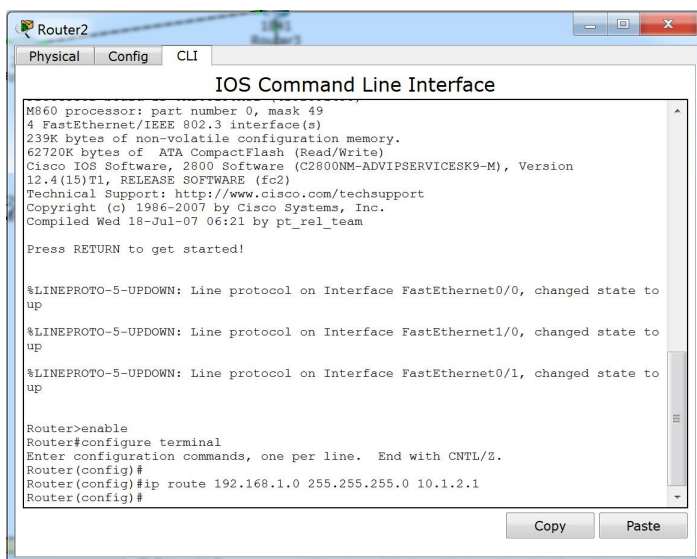
使用 PC0 尝试 ping 子网 2 的网关，发现请求超时。



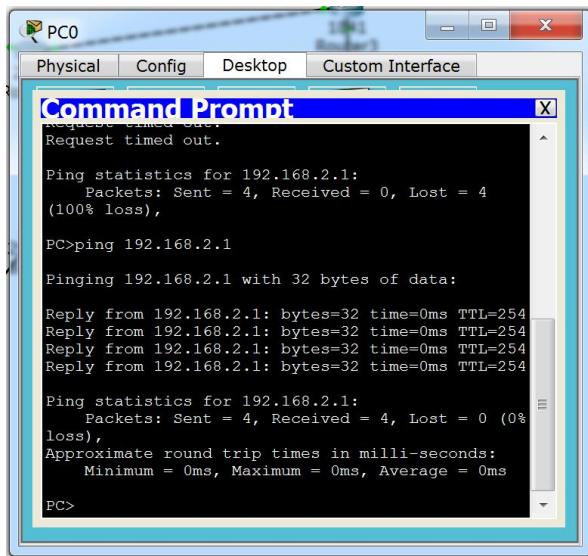
使用仿真工具发送包，发现可以包可以成功发送到 Router2，但是在 Router2 处出错。打开包发现报错信息如下：



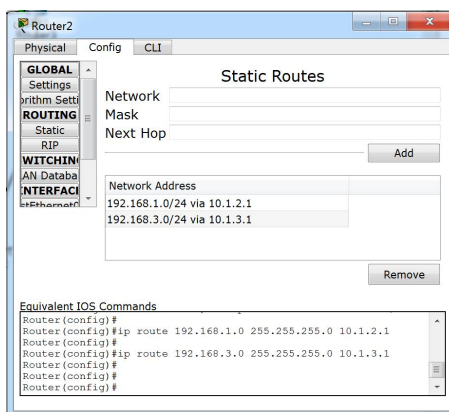
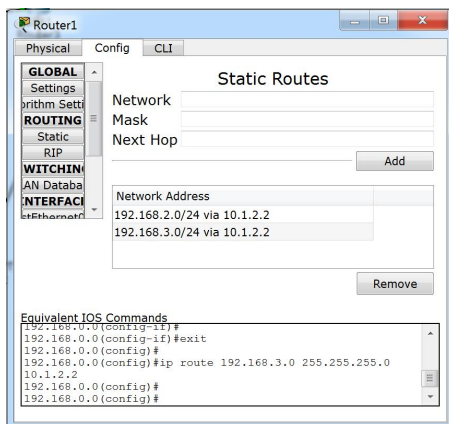
原因在于 Router2 没有配置路由表，ping 之后的确认包无法发送回 PC0。因此配置 Router2 到子网 1 的静态路由：

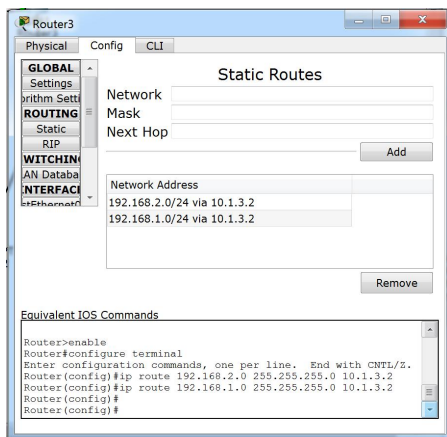


配置完成后可以成功发送包了。



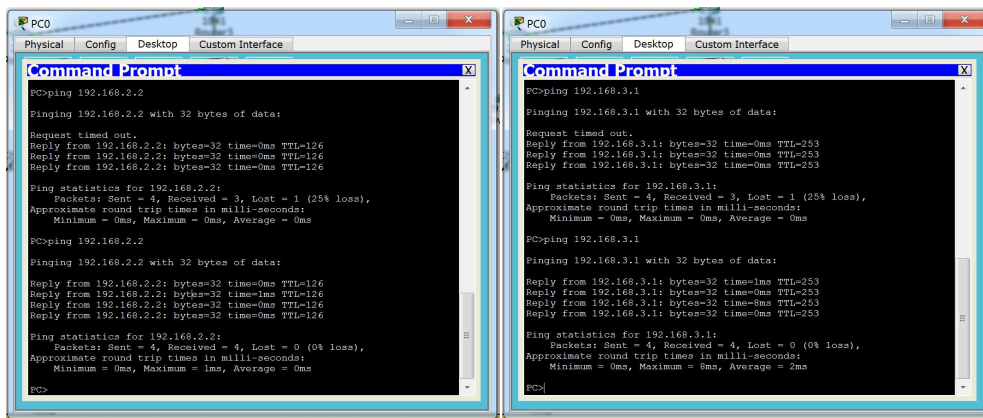
与以上方法同理配置子网 1 和子网 3、子网 2 和子网 3 之间通信所需要的路由表项。配置文件如下：



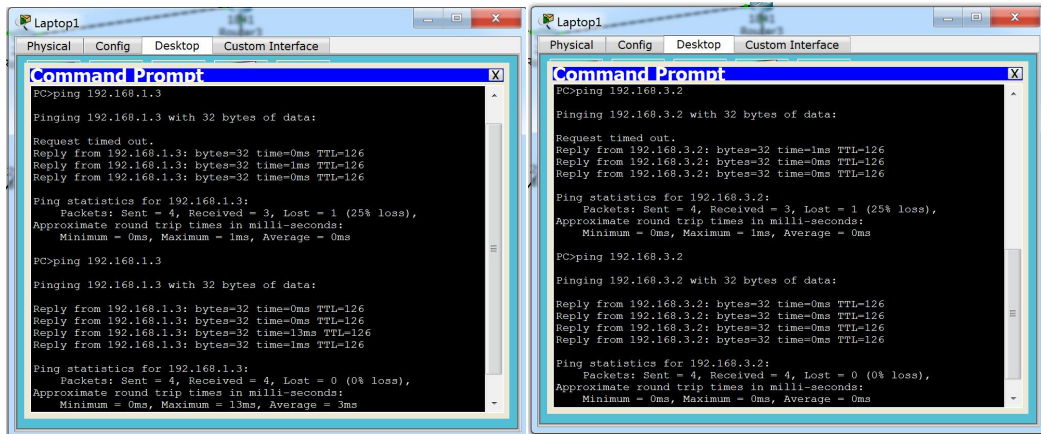


配置完成后，尝试不同子网之间的设备互相 ping 验证路由表的配置：

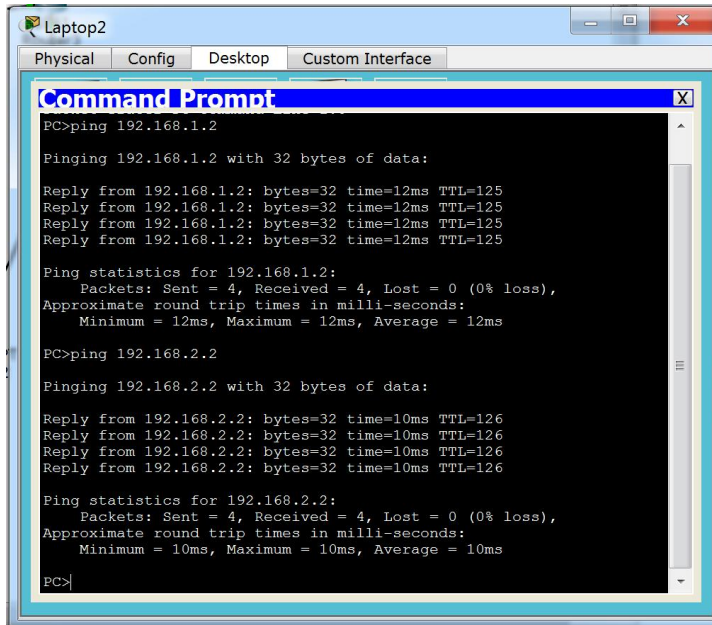
(1) 子网 1 到子网 2、3



(2) 子网 2 到子网 1、3



(3) 子网 3 到子网 1、2



任务 5 路由协议能高效保障通信 4'

为了减轻网络的维护成本，你和助手小杨讨论决定使用路由协议动态地管理和维护路由。在讨论使用何种路由协议时，小杨提出“由于公司目前网络规模较小，接入网络的 PC、笔记本和服务器加起来还不到 16 台，可以使用适合小型网络的路由协议 RIP 进行管理”。你认为小杨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？

是存在问题的。因为 RIP 协议计算的到目的网络的跳数，也就是在路由器上转发的次数，在子网内部发送使用的是广播，不会计算在跳数里面。

当前能够使用 RIP 作为路由协议。因为局域网中只有 3 个路由器，最多能够存在的跳数为 2，所以可以使用 RIP 协议。

经过一番讨论之后，你最终决定选择__RIP__路由协议维护公司目前的局域网。请完成协议的配置，并检验是否能够达到需求。

协议配置并查看路由表：

Router1

Physical Config CLI

IOS Command Line Interface

```
192.168.0.0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
192.168.0.0(config)#router rip
192.168.0.0(config-router)#exit
192.168.0.0(config)#exit
192.168.0.0#
%SYS-5-CONFIG_I: Configured from console by console

192.168.0.0#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       10.1.2.0 is directly connected, FastEthernet0/1
R       10.1.3.0 [120/1] via 10.1.2.2, 00:00:11, FastEthernet0/1
C       192.168.1.0/24 is directly connected, FastEthernet0/0
R       192.168.2.0/24 [120/1] via 10.1.2.2, 00:00:11, FastEthernet0/1
R       192.168.3.0/24 [120/2] via 10.1.2.2, 00:00:11, FastEthernet0/1
192.168.0.0#
```

Copy Paste

Router2

Physical Config CLI

IOS Command Line Interface

```
Router>enable
Router#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       10.1.2.0 is directly connected, FastEthernet0/1
C       10.1.3.0 is directly connected, FastEthernet1/0
R       192.168.1.0/24 [120/1] via 10.1.2.1, 00:00:10, FastEthernet0/1
C       192.168.2.0/24 is directly connected, FastEthernet0/0
R       192.168.3.0/24 [120/1] via 10.1.3.1, 00:00:14, FastEthernet1/0
Router#
```

Copy Paste

Router3

Physical Config CLI

IOS Command Line Interface

```
Router#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

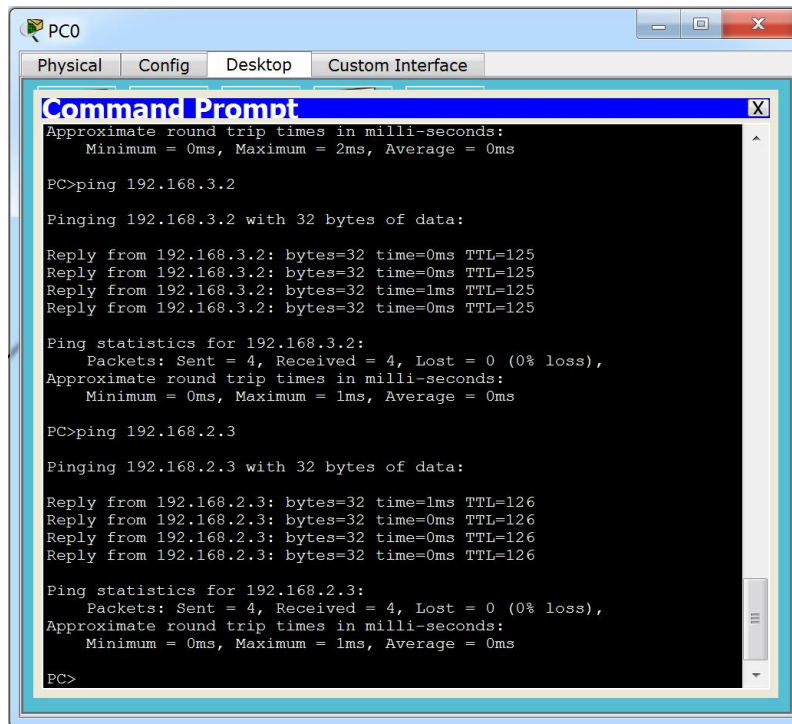
Gateway of last resort is not set

    10.0.0.0/24 is subnetted, 2 subnets
R       10.1.2.0 [120/1] via 10.1.3.2, 00:00:02, FastEthernet0/1
C       10.1.3.0 is directly connected, FastEthernet0/1
R       192.168.1.0/24 [120/2] via 10.1.3.2, 00:00:02, FastEthernet0/1
R       192.168.2.0/24 [120/1] via 10.1.3.2, 00:00:02, FastEthernet0/1
C       192.168.3.0/24 is directly connected, FastEthernet0/0
Router#
```

Copy Paste

验证子网之间相互通信:

(1) 子网 1 ping 子网 2、3 中的设备



The screenshot shows a Windows PC window titled 'PC0' with tabs for 'Physical', 'Config', 'Desktop', and 'Custom Interface'. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the execution of two ping commands. The first command is 'ping 192.168.3.2', which results in four successful replies with 0% loss and an average round trip time of 0ms. The second command is 'ping 192.168.2.3', which also results in four successful replies with 0% loss and an average round trip time of 0ms.

```
PC0
Physical Config Desktop Custom Interface
Command Prompt
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

PC>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=0ms TTL=125
Reply from 192.168.3.2: bytes=32 time=0ms TTL=125
Reply from 192.168.3.2: bytes=32 time=1ms TTL=125
Reply from 192.168.3.2: bytes=32 time=0ms 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

PC>ping 192.168.2.3

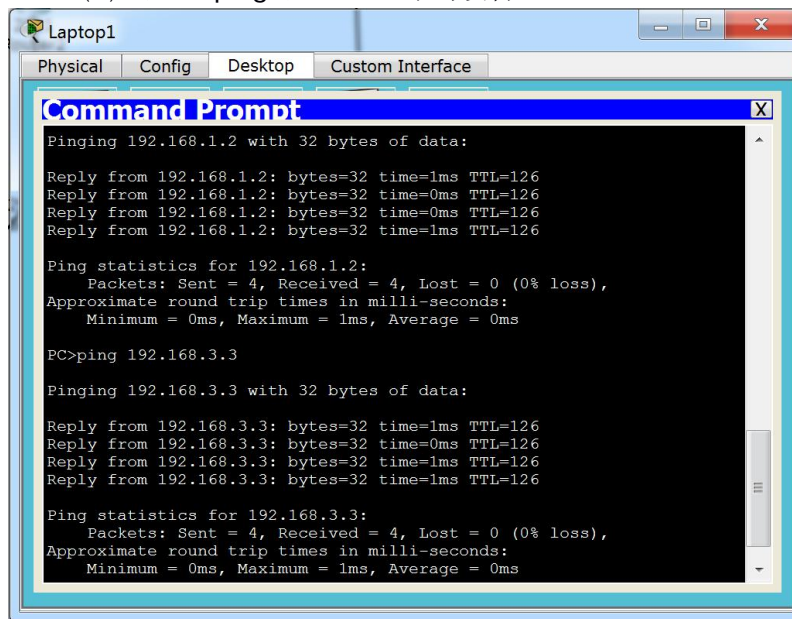
Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=1ms 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 = 1ms, Average = 0ms

PC>
```

(2) 子网 2 ping 子网 1、3 中的设备



The screenshot shows a Windows Laptop window titled 'Laptop1' with tabs for 'Physical', 'Config', 'Desktop', and 'Custom Interface'. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the execution of two ping commands. The first command is 'ping 192.168.1.2', which results in four successful replies with 0% loss and an average round trip time of 0ms. The second command is 'ping 192.168.3.3', which also results in four successful replies with 0% loss and an average round trip time of 0ms.

```
Laptop1
Physical Config Desktop Custom Interface
Command Prompt
Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=0ms TTL=126
Reply from 192.168.1.2: bytes=32 time=0ms 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 = 1ms, Average = 0ms

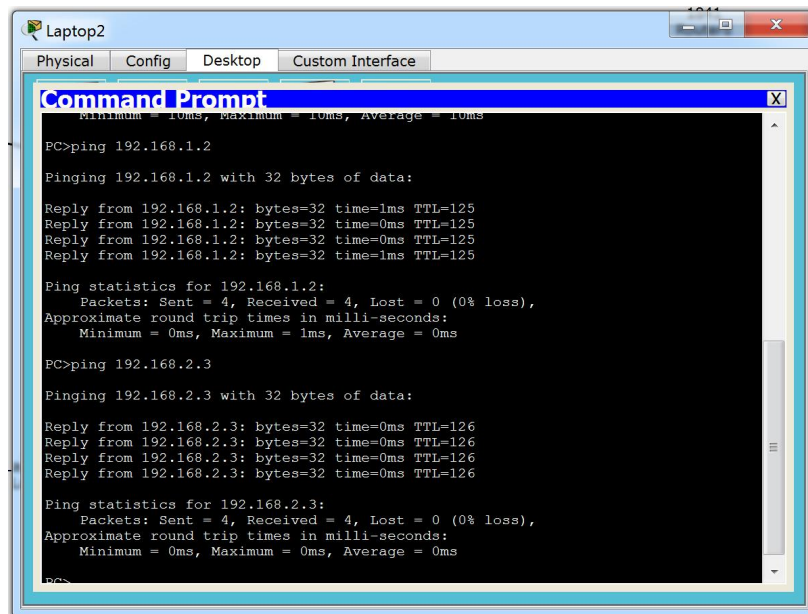
PC>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=0ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126

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 = 1ms, Average = 0ms
```

(3) 子网 3 ping 子网 1、2 中的设备



Bonus 任务 加密探究 2'

1. 尹董事近日来突然对公司内网的密码安全产生了兴趣，在她的要求下，公司内网的特权模式密码应使用 **secret** 指令在配置文件中具有一定程度的加密存储。试探究使用该指令存储的密码是用何种方式进行加密。

查看 Router 的配置文件中，这里可以看到 **secret** 是通过 MD5 加密的。

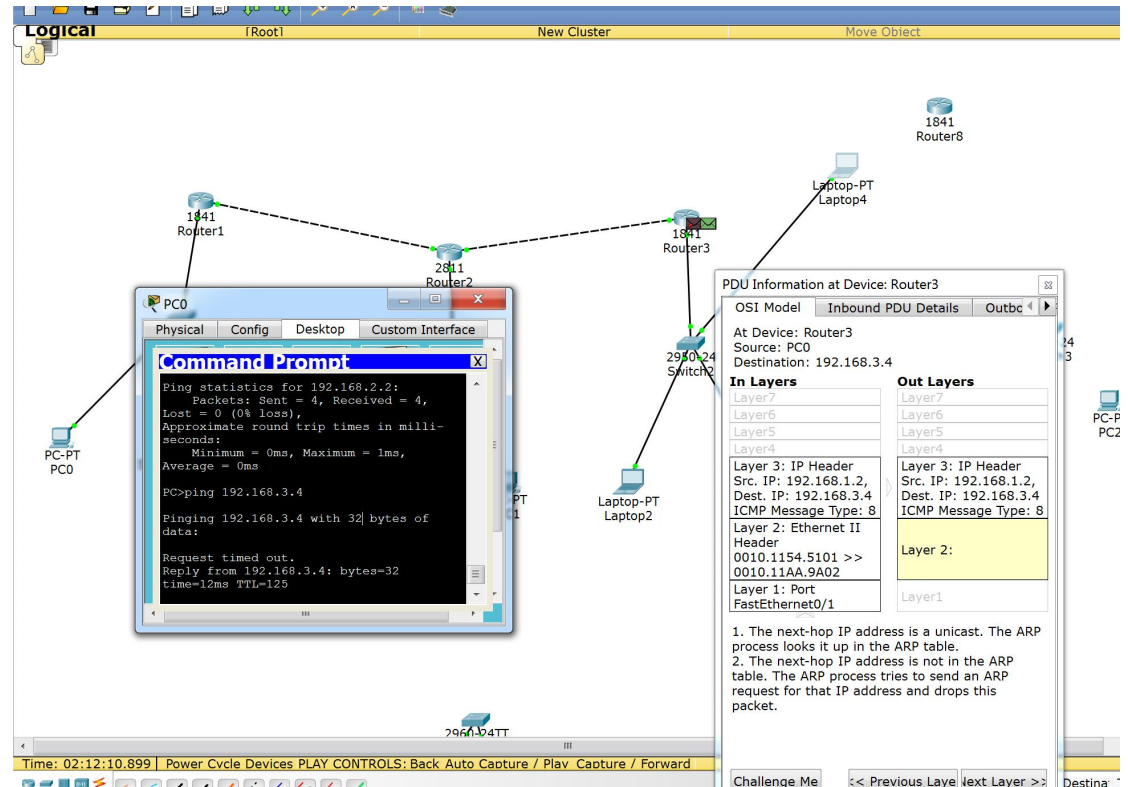


2. 任务 4 中，配置好静态路由后，在第一次发起 ping 测试时会出现丢包的现象。请用你掌握的网络知识来解释这一情况。

因为 ping 命令针对的是 ip, 在 ping 命令发起之后, 数据链路层会在封装之前检查目的 ip 地址是否在本地的 ARP 缓存中, 如果没有的话就会先发送一个请求用于获取目标的 MAC 地址, 建立 ip 地址和 Mac 地址之间的对应, 并且丢弃这个包。

在模拟器上新加入一个 Laptop4, 连接在子网 3 上, 分配静态 ip 为 192.168.3.4, 使用 PC0 尝试 ping, 结果如下:

可以看到在 Router3 尝试转发包时, 发现不知道 ip 对应的 MAC 地址, 因此丢弃了这个包, 并发送 ARP 请求获取 Laptop4 的 MAC 地址。



参考资料:

《Computer Networks (5th Edition) 》

路由器设置密码:

<https://www.cnblogs.com/mchina/archive/2012/07/13/2590916.html>

https://blog.csdn.net/saya_wj/article/details/44345359

https://blog.csdn.net/qq_41745698/article/details/83210807

配置静态路由表:

<https://blog.csdn.net/lx1315998513/article/details/87196354>

RIP 协议相关:

<https://blog.csdn.net/N1neDing/article/details/80793055>

https://blog.csdn.net/d5_j9/article/details/90763720

<https://www.cnblogs.com/santiaog/p/11774395.html>

https://blog.csdn.net/qq_41745698/article/details/83691935

为什么首次 ping 会丢包:

https://blog.csdn.net/weixin_30302609/article/details/101077545

<https://blog.51cto.com/dashu666/2115375>