第一次实验

任务 1

截图

▪IP 分配方案

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	10.0.2.2	/24	-
	端口 3	192.168.2.1	/24	-
Router3	端口 1	10.0.2.1	/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	192.168.3.2	/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	192.168.2.1
Laptop3	端口 1	192.168.3.3	/24	192.168.3.1

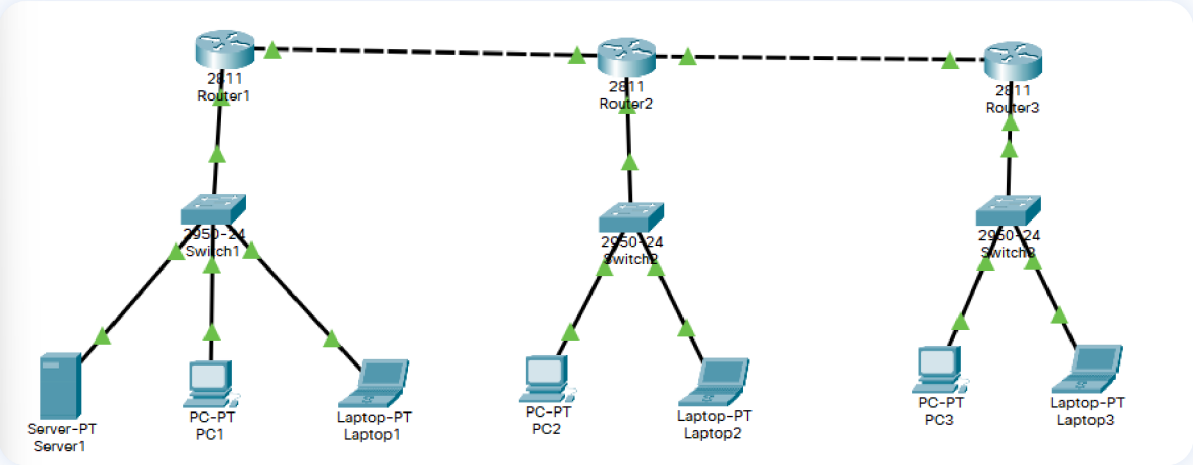
文字描述

红色部分为补全或修正的 IP 地址方案。错误的 IP 地址是因为不符合 IPv4 规范。

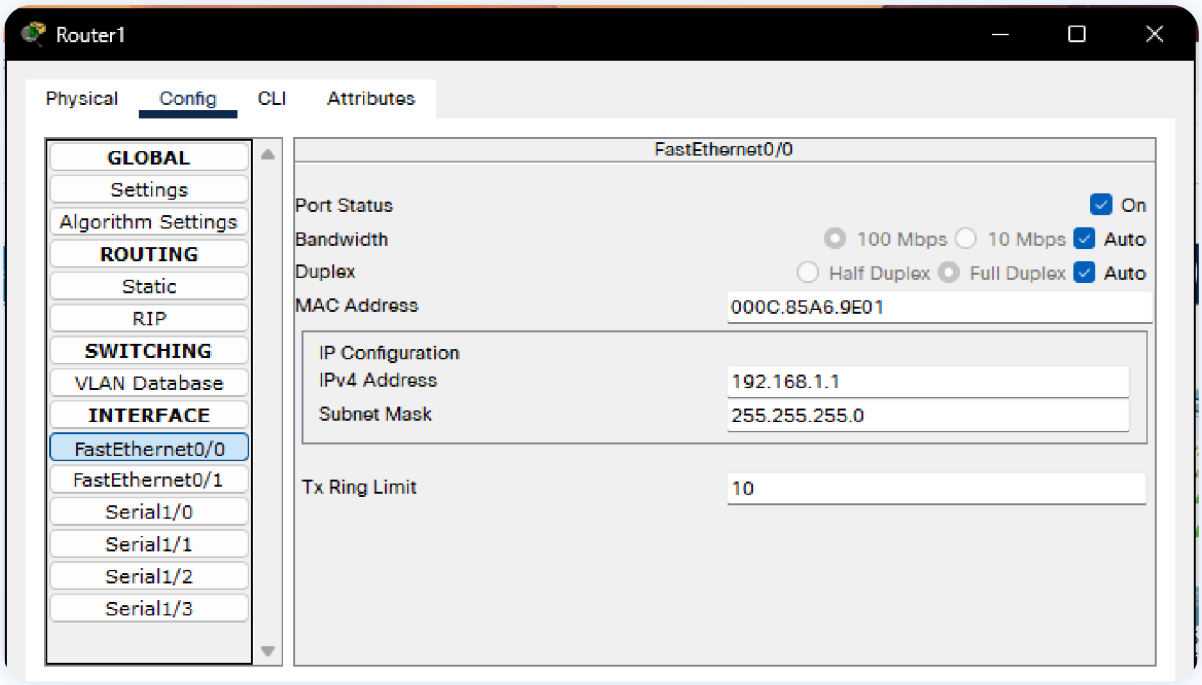
任务 2

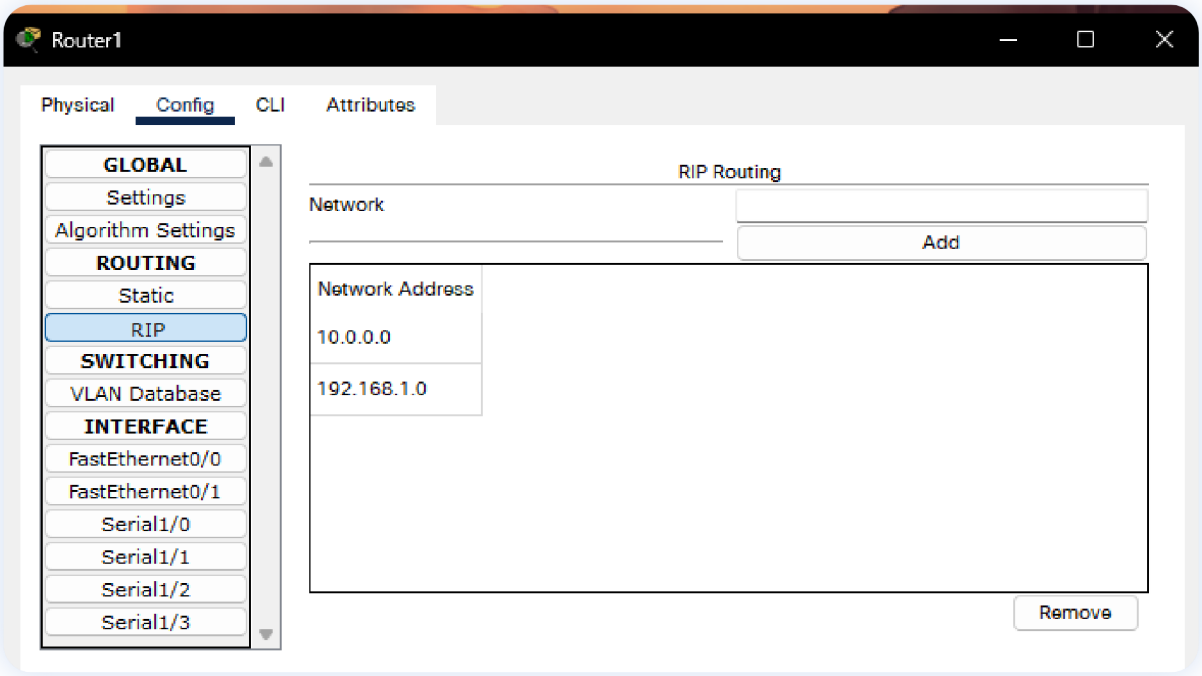
截图

1. 搭建图

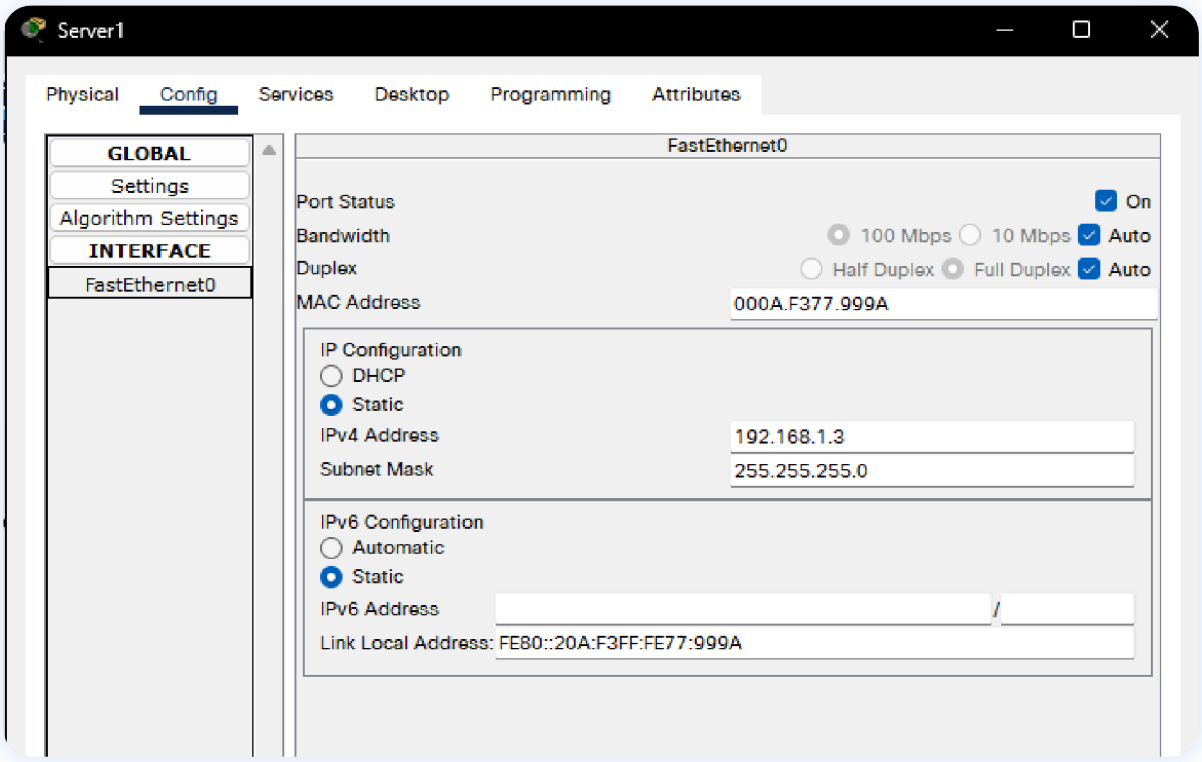


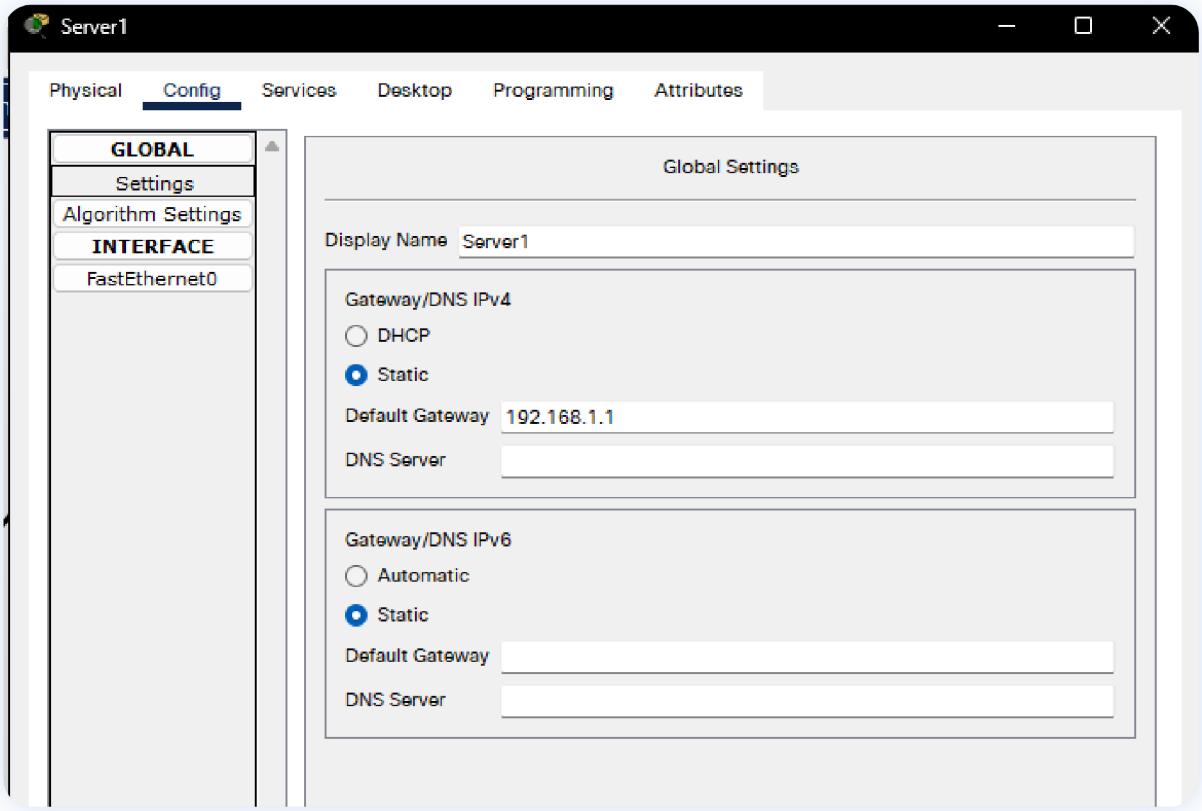
2. IP 与 RIP 配置，以 Router1 为例



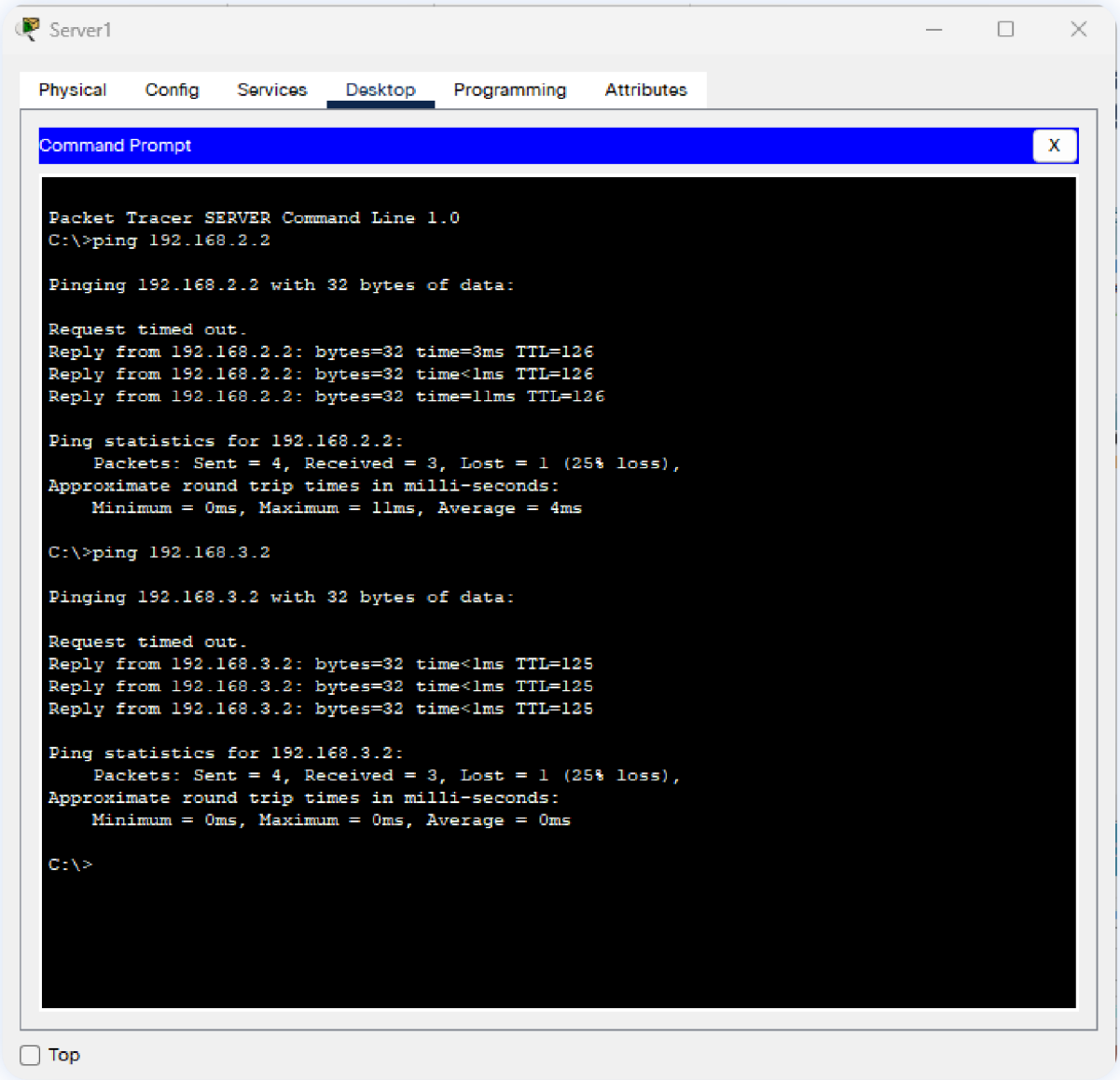


3. IP 与 Gateway 配置（以 Server1 为例）





4. ping 结果（以 Server1 到 PC2 和 PC3 为例）



文字描述

以以下步骤完成搭建：

1. 按照图例添加所需设备并进行连线，注意 Router2 应当增加模块；
2. 设置路由器的 IP 地址及 RIP 协议；
3. 设置终端设备的 IP 以及静态网关。

任务 3

截图

1. 设置密码

```
Router(config)#line console 0
Router(config-line)#password VENI
Router(config-line)#login
Router(config-line)#exit
Router(config)#enable password VIDI
Router(config)#line tty 0
                         ^
% Invalid input detected at '^' marker.

Router(config)#line tty 1
                         ^
% Invalid input detected at '^' marker.

Router(config)#line vty 0
Router(config-line)#password VICI
Router(config-line)#login
Router(config-line)#exit
Router(config)#
```

2. 展示密码配置

```
enable password VIDI
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2811/K9 sn FTX1017OARS-
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.0.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 clock rate 2000000
!
interface Serial1/1
 no ip address
 clock rate 2000000
!
interface Serial1/2
 no ip address
 clock rate 2000000
!
interface Serial1/3
 no ip address
 clock rate 2000000
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 network 10.0.0.0
 network 192.168.1.0
!
ip classless
!
ip flow-export version 9
!
!
!
!
```

```
!
!
!
!
line con 0
 password VENI
 login
!
line aux 0
!
line vty 0
 password VICI
```

3. 效果

```
Press RETURN to get started!



User Access Verification

Password:

Router>enable
Password:
Router#
```

4. 密文设置

```
Router(config)#service password-encryption
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#enable secret VIDI
             ^
% Invalid input detected at '^' marker.

Router#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable secret VIDI
The enable secret you have chosen is the same as your enable password.
This is not recommended.  Re-enter the enable secret.
Router(config)#no enable password VIDI
                                  ^
% Invalid input detected at '^' marker.

Router(config)#no enable password
Router(config)#enable secret VIDI
```

IOS Command Line Interface

```
enable secret 5 $1$mERr$1VYmEJsn5qXmHoa2nqQQ90
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2811/K9 sn FTX1017OARS-
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.0.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 clock rate 2000000
!
interface Serial1/1
 no ip address
 clock rate 2000000
!
interface Serial1/2
 no ip address
 clock rate 2000000
!
interface Serial1/3
 no ip address
 clock rate 2000000
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 network 10.0.0.0
 network 192.168.1.0
!
ip classless
!
ip flow-export version 9
!
!
```

```
!
!
!
!
!
!
line con 0
 password 7 0817696020
 login
!
line aux 0
!
line vty 0
 password 7 0817656D20
 login
```

文字描述

根据凯撒密码解码得到的明文是“VENI，VIDI，VICI”，于是将三处密码分别设置为这三句话。

设置明文密码的命令与效果如截图所示；当配置文件可能泄露时，应当使用密文保存，命令与效果如截图所示。

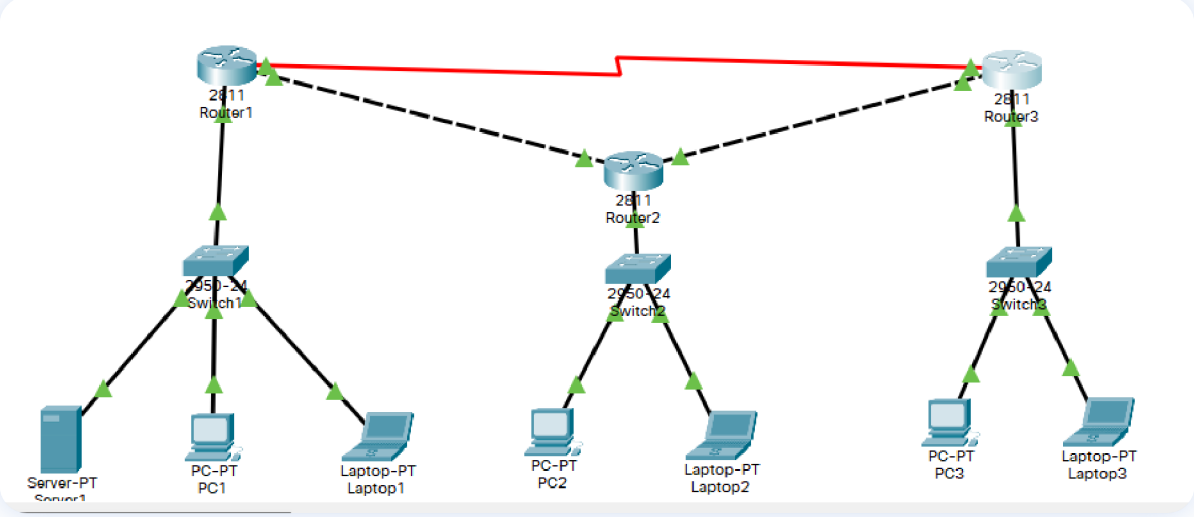
时间分析：

1. 10^6
2. $36^6 - 10^6 - 26^6$
3. $62^6 - 52^6 + 2 \times 26^6 - 2 \times 36^6 + 10^6$
4. $62^8 - 52^8 + 2 \times 26^8 - 2 \times 36^8 + 10^8$

任务 4

截图

1. 连线图



2. ODPF 设置

```
Router(config)#route ospf 1
Router(config-router)#network 192.168.1.0 255.255.255.0 area 0
Router(config-router)#network 10.0.1.0 255.255.255.0 area 0
```

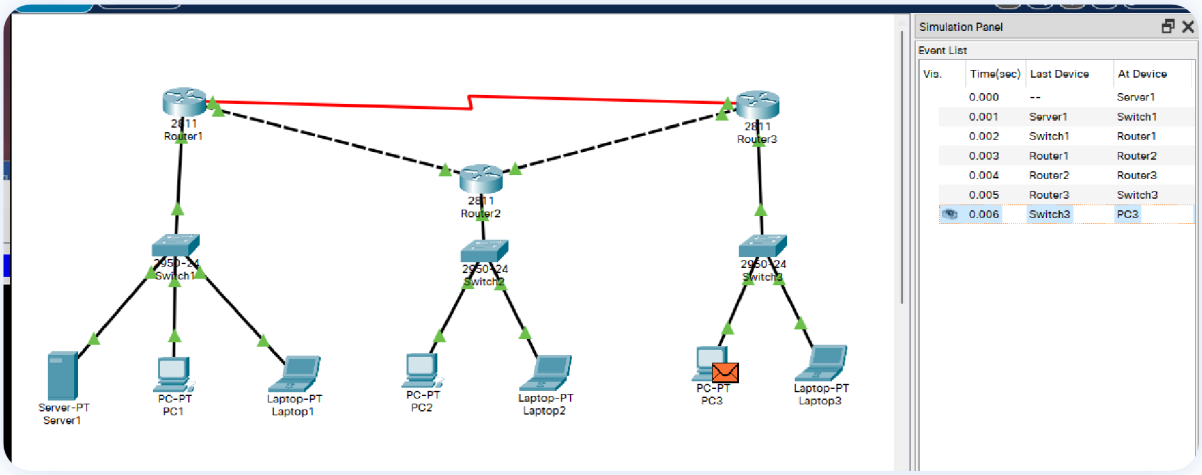
```
Router(config)#route ospf 1
Router(config-router)#network 10.0.1.0 255.255.255.0 area 0
Router(config-router)#network 10.0.1.0 255.255.255.0 area 0
00:47:49: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on FastEthernet0/0 from LOADING to
FULL, Loading Done

Router(config-router)#network 10.0.2.0 255.255.255.0 area 0
Router(config-router)#network 192.168.2.0 255.255.255.0 area 0
```

```
Router(config)#route ospf 1
Router(config-router)#network 10.0.2.0 255.255.255.0 area 0
Router(config-router)#network 10 255.255.255.0 area 0
00:48:16: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on FastEthernet0/0 from LOADING to
FULL, Loading Done
                                 ^
% Invalid input detected at '^' marker.

Router(config-router)#network 192.168.3.0 255.255.255.0 area
% Incomplete command.
Router(config-router)#network 192.168.3.0 255.255.255.0 area 0
```

3. 路径展示（经过 Router2）



文字描述

OSPF

为实现任务，依次进行如下操作：

1. 删除 RIP 协议；
2. 为 Router1 和 Router2 增加带有串口的模块并使用串口连接；
3. 配置 OSPF 协议，如截图所示。

凯撒的观点存在问题，RIP 协议要求子网之间的跳数不能超过 16，而不是终端的数量不能超过 16；

当前网路的最大跳数是 2，不超过 16，因此可以使用 RIP 协议。

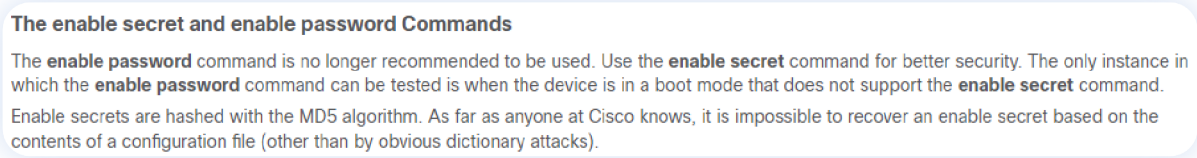
Bonus 1

IOS Command Line Interface

```
enable secret 5 $1$mERr$1VYmEJsn5qXmHoa2nqQQ90
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2811/K9 sn FTX1017OARS-
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.0.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 clock rate 2000000
!
interface Serial1/1
 no ip address
 clock rate 2000000
!
interface Serial1/2
 no ip address
 clock rate 2000000
!
interface Serial1/3
 no ip address
 clock rate 2000000
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 network 10.0.0.0
 network 192.168.1.0
!
ip classless
!
ip flow-export version 9
!
!
```

```
!
!
!
!
!
!
line con 0
 password 7 0817696020
 login
!
line aux 0
!
line vty 0
 password 7 0817656D20
 login
```

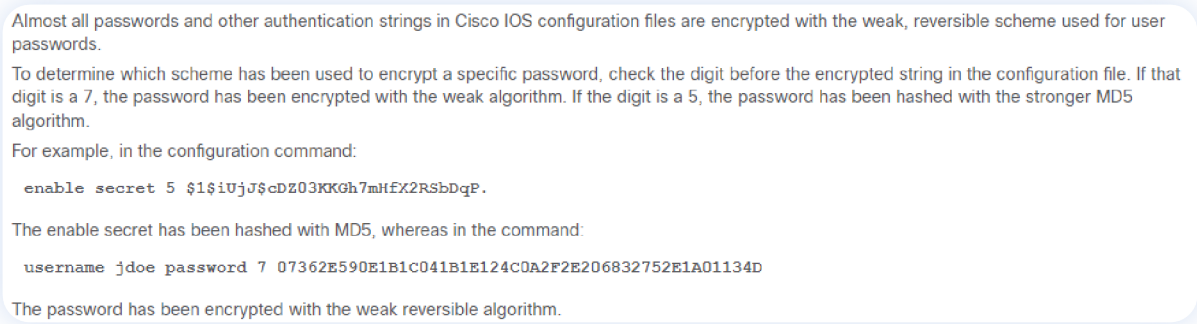
如上图所示，可以看到哈希值前的标记为 `5`，通过查阅思科的手册可知该密码由 `MD5` 加密得到，



The enable secret and enable password Commands

The **enable password** command is no longer recommended to be used. Use the **enable secret** command for better security. The only instance in which the **enable password** command can be tested is when the device is in a boot mode that does not support the **enable secret** command.

Enable secrets are hashed with the MD5 algorithm. As far as anyone at Cisco knows, it is impossible to recover an enable secret based on the contents of a configuration file (other than by obvious dictionary attacks).



Almost all passwords and other authentication strings in Cisco IOS configuration files are encrypted with the weak, reversible scheme used for user passwords.

To determine which scheme has been used to encrypt a specific password, check the digit before the encrypted string in the configuration file. If that digit is a 7, the password has been encrypted with the weak algorithm. If the digit is a 5, the password has been hashed with the stronger MD5 algorithm.

For example, in the configuration command:

```
enable secret 5 $1$iUjJ$cDZ03KKGh7mHfX2RSbDqP.
```

The enable secret has been hashed with MD5, whereas in the command:

```
username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D
```

The password has been encrypted with the weak reversible algorithm.

然而 MD5 算法得到的结果应该只包含数字和小写字母，同时长度为 32，显然密文 `$1$mERr$1VYmEJsn5qXmHoa2nqQQ90` 不是 `VIVD` 经过简单的 `MD5` 算法一步得到的结果。进一步查找资料了解到，思科的加密方式可能是多次带盐的 MD5 哈希算法，首先确定这一思路：

```
In [1]: import crypt

In [2]: crypt.crypt("VIVD", "$1$mERr$")
Out[2]: '$1$mERr$iSyX5wwi/MyMMvaCWM6g40'

In [3]: crypt.crypt("VIVD", "mERr$")
Out[3]: 'mET19uI7dLpFw'

In [4]: len("$1$mERr$1VYmEJsn5qXmHoa2nqQQ90") ==
len("$1$mERr$iSyX5wwi/MyMMvaCWM6g40")
Out[4]: True
```

发现加密后的密文长度与所需密文长度一致，可以假设盐值为 `$1$mERr$`

进一步实验：

```
In [5]: target = "$1$mERr$1VYmEJsn5qXmHoa2nqQQ90"

In [6]: sault = "$1$mERr$"

In [7]: init = "VIVD"

In [8]: n = 0

In [9]: while n < 10000:
    ...:     tmp = crypt.crypt(init, sault)
    ...:     if tmp==target:
    ...:         print(n)
    ...:         break
    ...:     init = tmp[8:]
    ...:     n+=1

In [10]: tmp
Out[10]: '$1$mERr$WTRqFislGnsxWvOeXkqCN1'

In [11]: len(tmp)
Out[12]: 30
```

尽管发现 10000 次的带盐 MD5 加密始终未能得到正确答案...但从其形式上可以看出思科的加密方式应该是连续多次带盐的 MD5 加密。

Bonus 2

如任务 4 实现。