

# 实验四 NAT&PAT的配置

---



# NAT (Network Address Translation)

---

- **NAT (Network Address Translation)** 网络地址翻译是指将一个内网私有**IP**地址转换成外网（公网）**IP**地址；
- **NAT**可将多个内部网络地址翻译（映射）成几个外网（公网）**IP**地址；
- **NAT**可将内部网络中的私有**IP**“伪造”成公网**IP**访问互联网，为网络带来了相对的安全。

# 静态NAT

---

- 静态NAT实现私有IP地址和公网IP地址之间一对一转换。
- 静态NAT主要用于内部网络，私有IP与公网IP是一对一关系，是固定的，不作改变。
- 若内网有服务器，并需要同时为内网和外网提供服务，通常采取这种方法。

# 静态NAT命令格式

- 命令格式:

端口模式下:

**ip nat inside**

将某端口定义为内部端口

**ip nat outside**

将某端口定义为外部端口

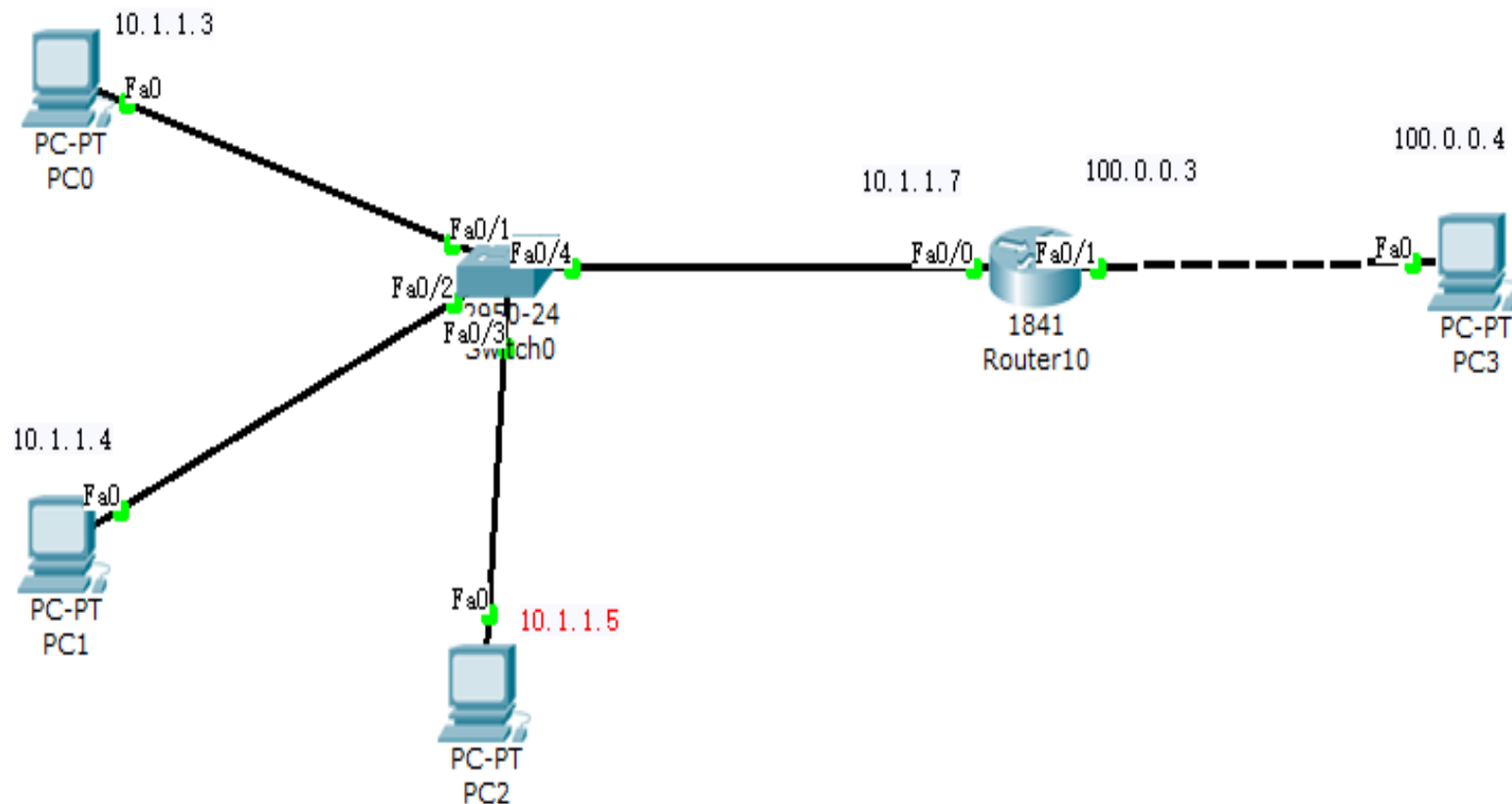
全局模式下:

**ip nat inside source static inside\_ip  
outside\_ip**

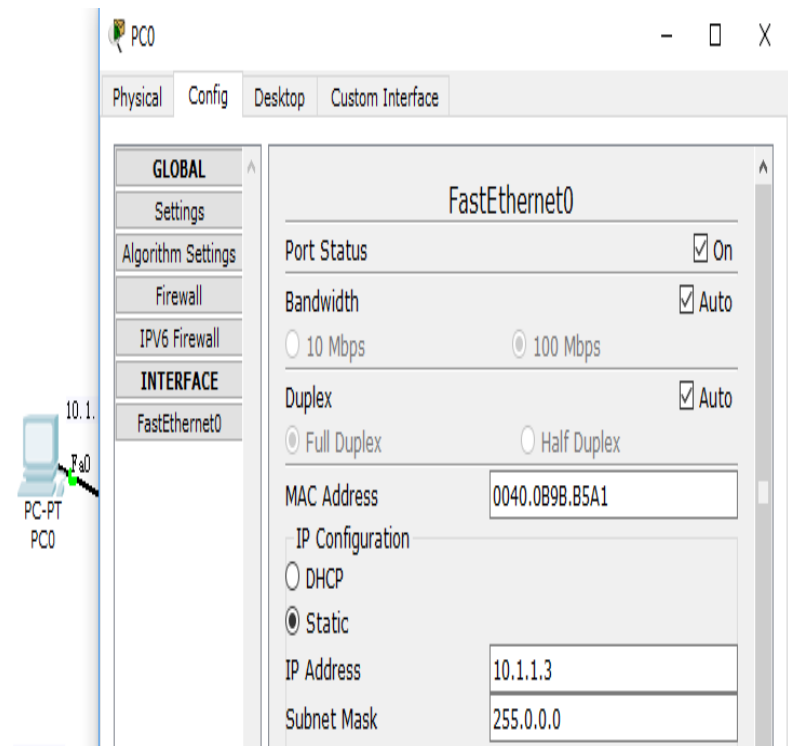
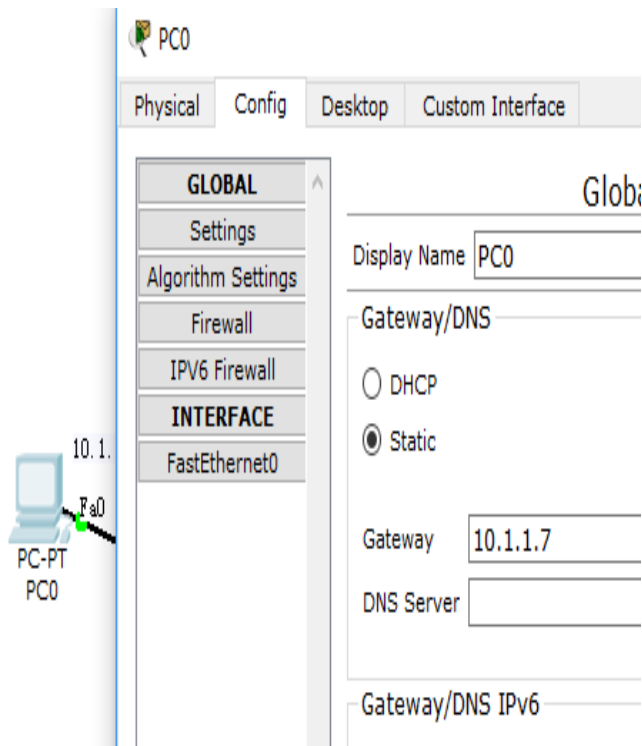
其中, **inside\_ip** 指的是内部IP地址;

**outside\_ip**指的是翻译成的外部IP地址。

# 静态NAT配置实例



# 静态NAT配置实例



# 静态NAT配置实例

## Router1的配置

```
Router>enable
```

```
Router#configure terminal
```

```
Router(config)#interface f0/0
```

```
Router(config-if)#ip address 10.1.1.7 255.0.0.0
```

```
Router(config-if)#no shutdown
```

```
Router(config-if)#ip nat inside
```

```
Router(config-if)#exi
```

```
Router(config)#interface f0/1
```

```
Router(config-if)#ip address 100.0.0.3 255.0.0.0
```

```
Router(config-if)#no shutdown
```

```
Router(config-if)#ip nat outside
```

```
Router(config-if)#exit
```

```
Router(config)#ip nat inside source static 10.1.1.4 100.0.0.7
```

```
Router(config)#ip nat inside source static 10.1.1.5 100.0.0.8
```

```
Router(config)#exit
```

# 静态NAT配置实例

```
Router#show ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
---	100.0.0.7	10.1.1.4	---	---
---	100.0.0.8	10.1.1.5	---	---

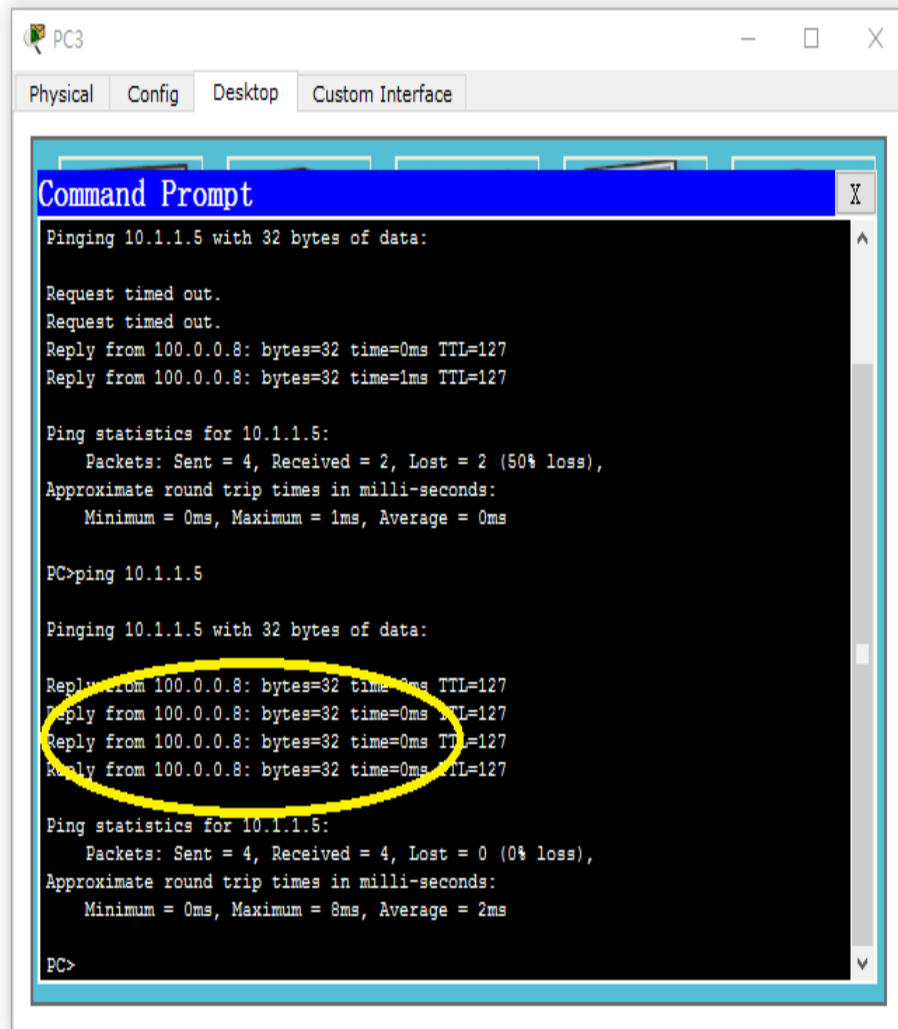
```
Router#
```

注意：静态NAT是一对一的地址转换，可以很好地隔离外网。



# 静态NAT配置实例

当网络地址转换产生后，查看**Router0**的NAT信息



```
PC3
Physical Config Desktop Custom Interface

Command Prompt
Pinging 10.1.1.5 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 100.0.0.8: bytes=32 time=0ms TTL=127
Reply from 100.0.0.8: bytes=32 time=1ms TTL=127

Ping statistics for 10.1.1.5:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

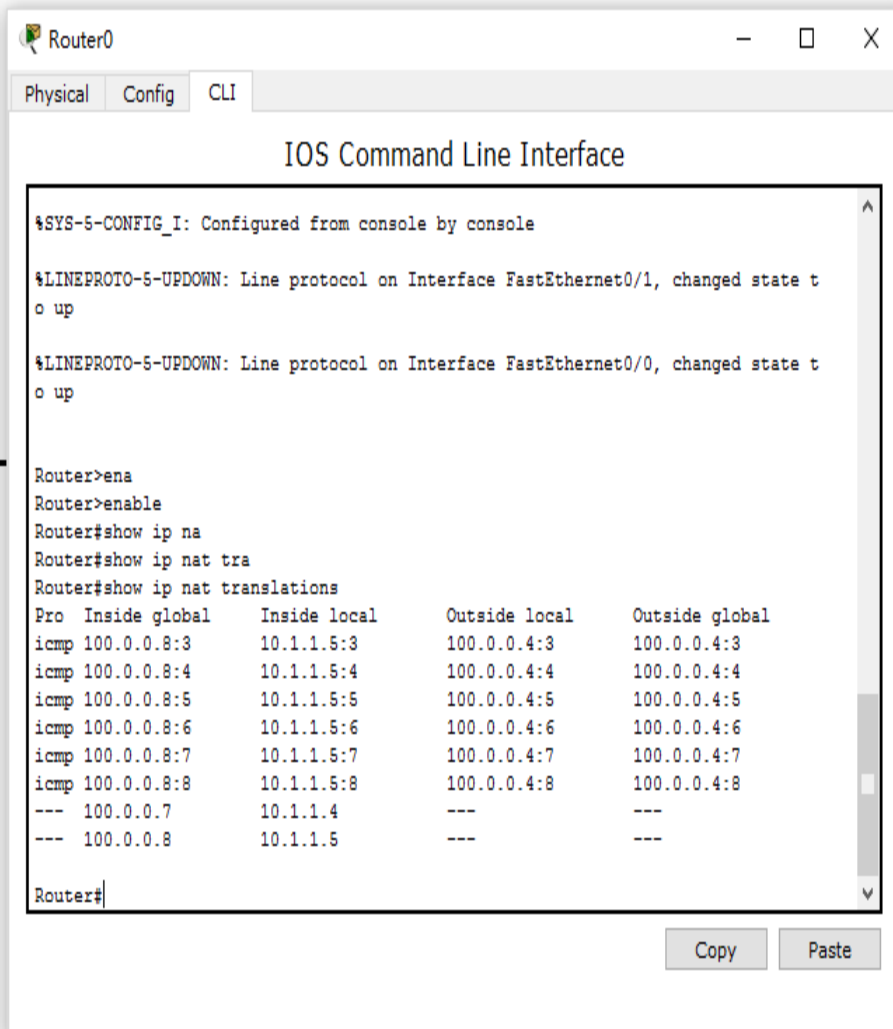
PC>ping 10.1.1.5

Pinging 10.1.1.5 with 32 bytes of data:

Reply from 100.0.0.8: bytes=32 time=0ms TTL=127
Reply from 100.0.0.8: bytes=32 time=0ms TTL=127
Reply from 100.0.0.8: bytes=32 time=0ms TTL=127
Reply from 100.0.0.8: bytes=32 time=0ms TTL=127

Ping statistics for 10.1.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms

PC>
```



```
Router0
Physical Config CLI

IOS Command Line Interface

%SYS-5-CONFIG_I: Configured from console by console

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router>ena
Router>enable
Router#show ip na
Router#show ip nat tra
Router#show ip nat translations

Pro  Inside global      Inside local       Outside local      Outside global
icmp 100.0.0.8:3          10.1.1.5:3         100.0.0.4:3        100.0.0.4:3
icmp 100.0.0.8:4          10.1.1.5:4         100.0.0.4:4        100.0.0.4:4
icmp 100.0.0.8:5          10.1.1.5:5         100.0.0.4:5        100.0.0.4:5
icmp 100.0.0.8:6          10.1.1.5:6         100.0.0.4:6        100.0.0.4:6
icmp 100.0.0.8:7          10.1.1.5:7         100.0.0.4:7        100.0.0.4:7
icmp 100.0.0.8:8          10.1.1.5:8         100.0.0.4:8        100.0.0.4:8
---  100.0.0.7            10.1.1.4           ---                ---
---  100.0.0.8            10.1.1.5           ---                ---

Router#
```

# 动态NAT

- 动态NAT实现私有IP和公网IP之间一一对应的转换，但是它们的关系不是固定的，就是说私有IP访问外网时要转换成公网IP，但是转换时不是转换成固定某一个IP，而是随机的。
- 动态NAT的原理：动态NAT定义了一个地址池（pool），其中地址池中的地址是一组连续的外网IP地址，所有内网中允许的IP都可以使用地址池中的任意一个进行转换。
- 所谓允许的IP指可以在路由器上使用访问控制列表来定义，允许那一部分内网IP使用这个地址池进行转换。允许的IP一般是某个网段，如：192.168.0.0/24等。
- 若需要访问外网的内部主机有100台，私有IP地址当然也是100个，访问控制列表允许这100台访问外网。但只能申请到50个公网IP地址，即最多同时有50台内部计算机可以转换成公网IP访问外网。通过动态NAT的设置，既保证有效地访问了外网，又节约了部分公网IP资源。
- 静态NAT和动态NAT可以共存，如果有需要内外网都访问的服务器，可以采取静态，其它可以采取动态。

# 动态NAT命令格式

- 命令格式:

端口模式下:

Ip nat inside            将某端口定义为内部端口  
Ip nat outside          将某端口定义为外部端口

- 全局模式下:

1、 Ip nat pool name start\_ip end\_ip netmask netmask

Ip nat pool name start\_ip end\_ip prefix\_length 子网掩码位数

其中: name 指的是地址池的名字;

start\_ip和end\_ip指的是地址池开始和结束地址;

netmask指的是地址池的IP地址的子网掩码, 子网掩码位数指的是如果不用子网掩码表示, 可以用位数表示。如: /24表示255.255.255.0。

2、 access\_list number permit source wildcard

其中, number指的是访问控制列表的号码, 1-99;

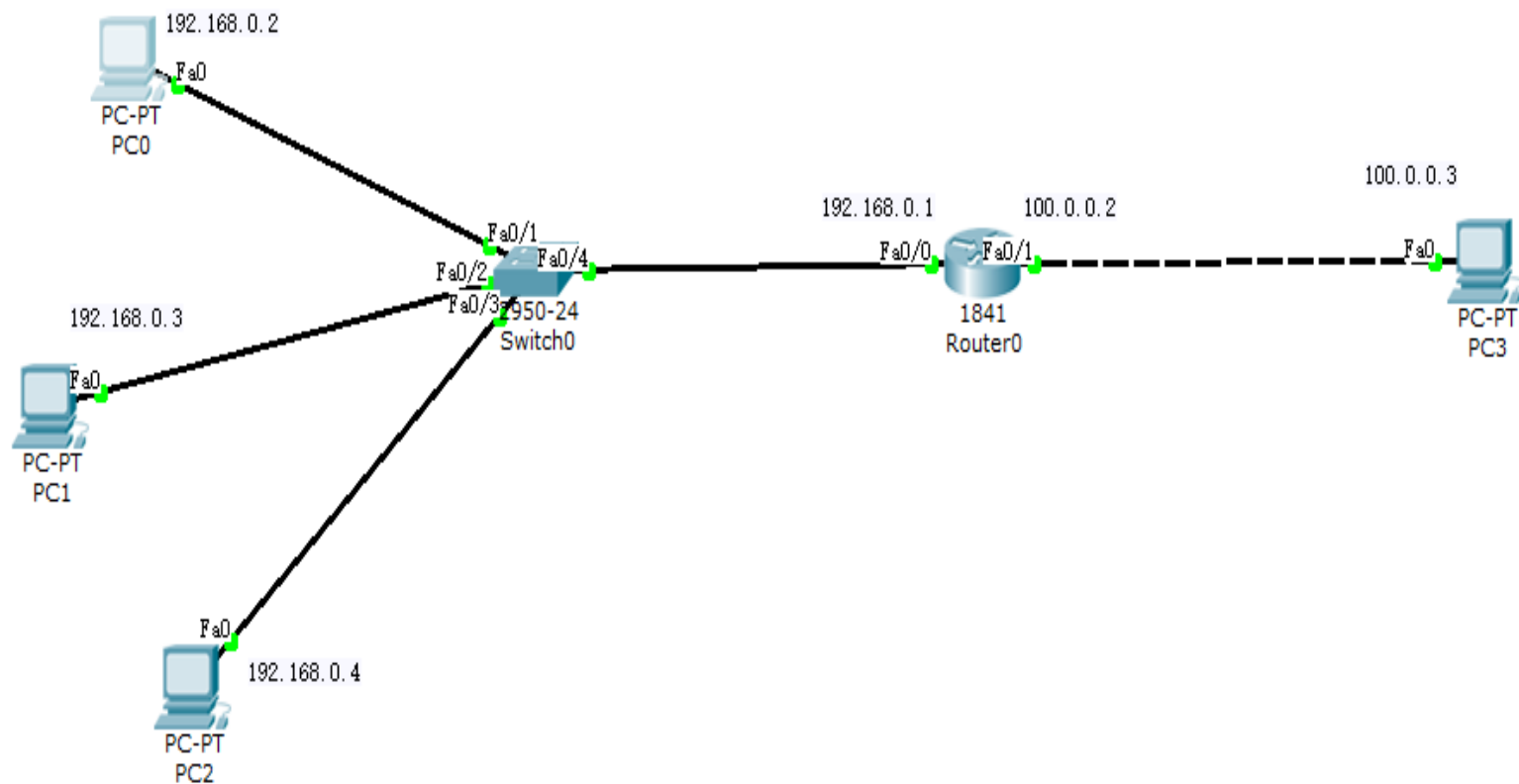
source wildcard 指的是允许地址转换的地址段和对应的通信符与OSPF路由的意思是一样的。

3、 ip nat inside source list number pool name

其中, number还是2号命令中的访问控制列表号;

name还是1号命令中的地址池的名字。

# 动态NAT配置实例-1



# 动态NAT配置实例-1

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface f0/0

Router(config-if)#ip address 192.168.0.1 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#ip nat inside

Router(config-if)#exit

Router(config)#interface f0/1

Router(config-if)#ip address 100.0.0.2 255.255.255.0

Router(config)#interface FastEthernet0/1

Router(config-if)#no shutdown

Router(config-if)#ip nat outside

Router(config-if)#exit

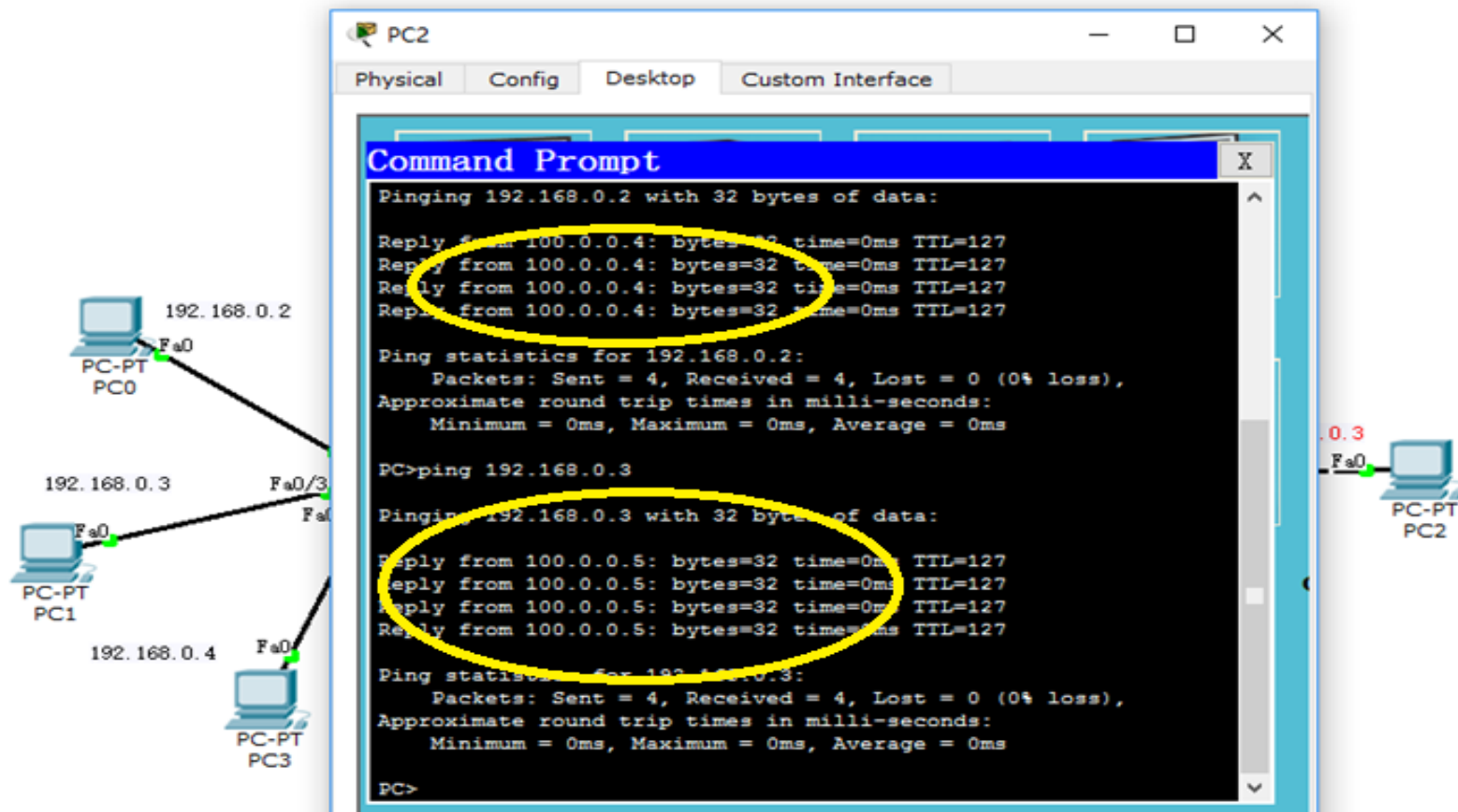
Router(config)#ip nat pool AAA 100.0.0.2 100.0.0.100 netmask 255.0.0.0

Router(config)#access-list 10 permit 192.168.0.0 0.255.255.255

Router(config)#ip nat inside source list 10 pool AAA

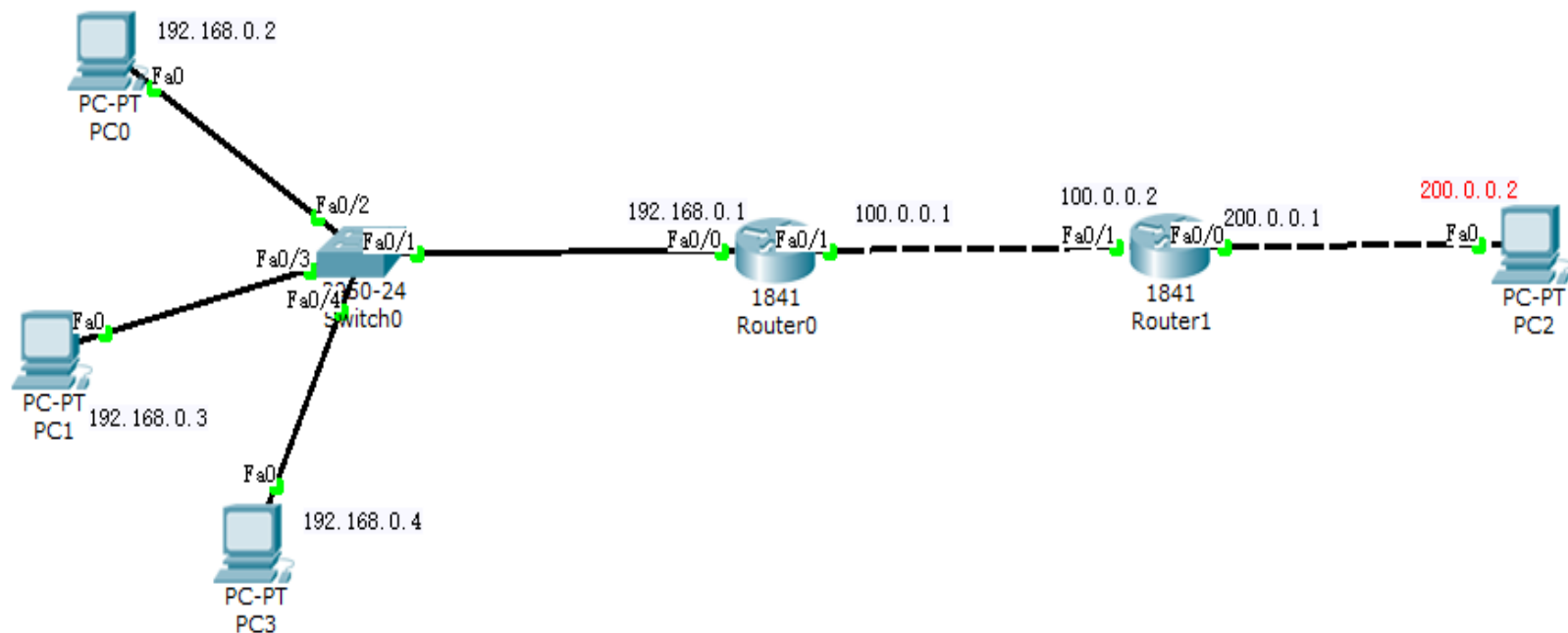
Router(config)#exit

# 动态NAT配置实例-1



通过地址池内某一随机地址的转换实现了访问

# 动态NAT配置实例-2





# 动态NAT配置实例-2

## Router0的配置

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface f0/0

Router(config-if)#ip address 192.168.0.1 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#ip nat inside

Router(config-if)#exit

Router(config)#interface f0/1

Router(config-if)#ip address 100.0.0.1 255.0.0.0

Router(config)#interface FastEthernet0/1

Router(config-if)#no shutdown

Router(config-if)#ip nat outside

Router(config-if)#exit

Router(config)#ip nat pool AAA 100.0.0.1 100.0.0.100 netmask 255.0.0.0

Router(config)#access-list 10 permit 192.168.0.0 0.255.255.255

Router(config)#ip nat inside source list 10 pool AAA

Router(config)#ip route 0.0.0.0 0.0.0.0 f0/1

Router(config)#exit



# 动态NAT配置实例-2

## Router1的配置

```
Router>enable
```

```
Router#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#interface f0/0
```

```
Router(config-if)#ip address 100.0.0.2 255.255.255.0
```

```
Router(config-if)#no shutdown
```

```
Router(config-if)#exit
```

```
Router(config)#interface f0/1
```

```
Router(config-if)#ip address 200.0.0.1 255.255.255.0
```

```
Router(config)#interface FastEthernet0/1
```

```
Router(config-if)#no shutdown
```

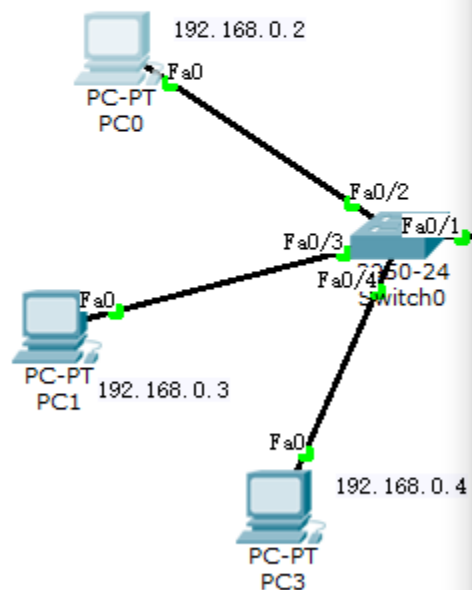
```
Router(config-if)#exit
```

```
Router(config)#ip route 0.0.0.0 0.0.0.0 f0/1
```

```
Router(config)#exit
```

# 动态NAT配置实例-2

PC1>ping 200.0.0.2



Physical Config CLI

## IOS Command Line Interface

```
icmp 100.0.0.4:11 192.168.0.3:11 200.0.0.2:11 200.0.0.2:11
icmp 100.0.0.4:12 192.168.0.3:12 200.0.0.2:12 200.0.0.2:12
icmp 100.0.0.4:9 192.168.0.3:9 200.0.0.2:9 200.0.0.2:9

Router#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 100.0.0.4:10 192.168.0.3:10 200.0.0.2:10 200.0.0.2:10
icmp 100.0.0.4:11 192.168.0.3:11 200.0.0.2:11 200.0.0.2:11
icmp 100.0.0.4:12 192.168.0.3:12 200.0.0.2:12 200.0.0.2:12
icmp 100.0.0.4:9 192.168.0.3:9 200.0.0.2:9 200.0.0.2:9

Router#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 100.0.0.4:10 192.168.0.3:10 200.0.0.2:10 200.0.0.2:10
icmp 100.0.0.4:11 192.168.0.3:11 200.0.0.2:11 200.0.0.2:11
icmp 100.0.0.4:12 192.168.0.3:12 200.0.0.2:12 200.0.0.2:12
icmp 100.0.0.4:9 192.168.0.3:9 200.0.0.2:9 200.0.0.2:9

Router#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 100.0.0.4:10 192.168.0.3:10 200.0.0.2:10 200.0.0.2:10
icmp 100.0.0.4:11 192.168.0.3:11 200.0.0.2:11 200.0.0.2:11
icmp 100.0.0.4:12 192.168.0.3:12 200.0.0.2:12 200.0.0.2:12
icmp 100.0.0.4:9 192.168.0.3:9 200.0.0.2:9 200.0.0.2:9

Router#
```

Copy

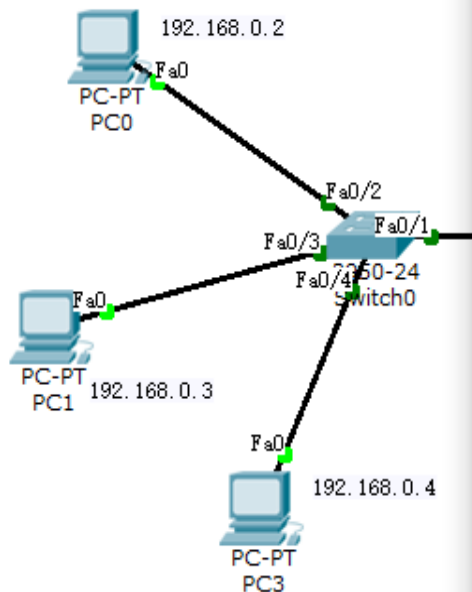
Paste

PC1

X

# 动态NAT配置实例-2

PC2>ping 192.168.0.4 (PC3)



PC2

Physical Config Desktop Custom Interface

### Command Prompt

```
Pinging 192.168.0.4 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 100.0.0.4: bytes=32 time=1ms TTL=126
Reply from 100.0.0.4: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.0.4:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 6ms

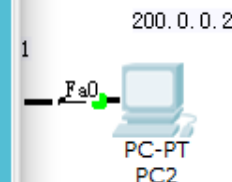
PC>ping 192.168.0.4

Pinging 192.168.0.4 with 32 bytes of data:

Reply from 100.0.0.5: bytes=32 time=0ms TTL=126
Reply from 100.0.0.5: bytes=32 time=0ms TTL=126
Reply from 100.0.0.5: bytes=32 time=1ms TTL=126
Reply from 100.0.0.5: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```



# PAT的配置

- 伴随着互联网技术的发展，IP地址短缺问题变得越来越严重。因此需要大量的公网IP，但实际情况是很多单位根本申请不到那么多公网IP，往往只能申请一个IP，而静态NAT与动态NAT能部分地解决。
- 在NAT技术中有一种特殊的方法，可以将一段私有IP转换一个或少数几个公网IP地址，从而节省了公网的IP地址资源，这种技术叫PAT（Port Address Translation 端口地址翻译），也可称为NAPT（Network Address Port Translation）。使用PAT（Port Address Translation端口地址翻译），可以允许多个内网私有IP地址映射到同一个公网IP上。
- 实际上PAT和动态NAT几乎是一样的，只不过在地址转换的时候地址池内只有一个地址，所有的私有地址都转换成同一个公网地址，转换时对网关路由器的外网接口IP地址进行复用（overload）。

# PAT的命令格式

- 命令格式:

端口模式下:

**ip nat inside**            将某端口定义为内部端口

**ip nat outside**        将某端口定义为外部端口

- 全局模式下:

1、**ip nat pool name start\_ip end\_ip netmask netmask**

**ip nat pool name start\_ip end\_ip prefix\_length** 子网掩码位数

其中: **name** 指的是地址池的名字;

**start\_ip**和**end\_ip**指的是地址池开始和结束地址;

**netmask**指的是地址池的IP地址的子网掩码, 子网掩码位数指的是如果不用子网掩码表示, 用位数表示。如: /24表示255.255.255.0。

2、**access\_list number permit source wildcard**

其中, **number**指的是访问控制列表的号码, 1-99;

**source wildcard** 指的是允许地址转换的地址段和对应的通信符与OSPF路由的意思是一样的。

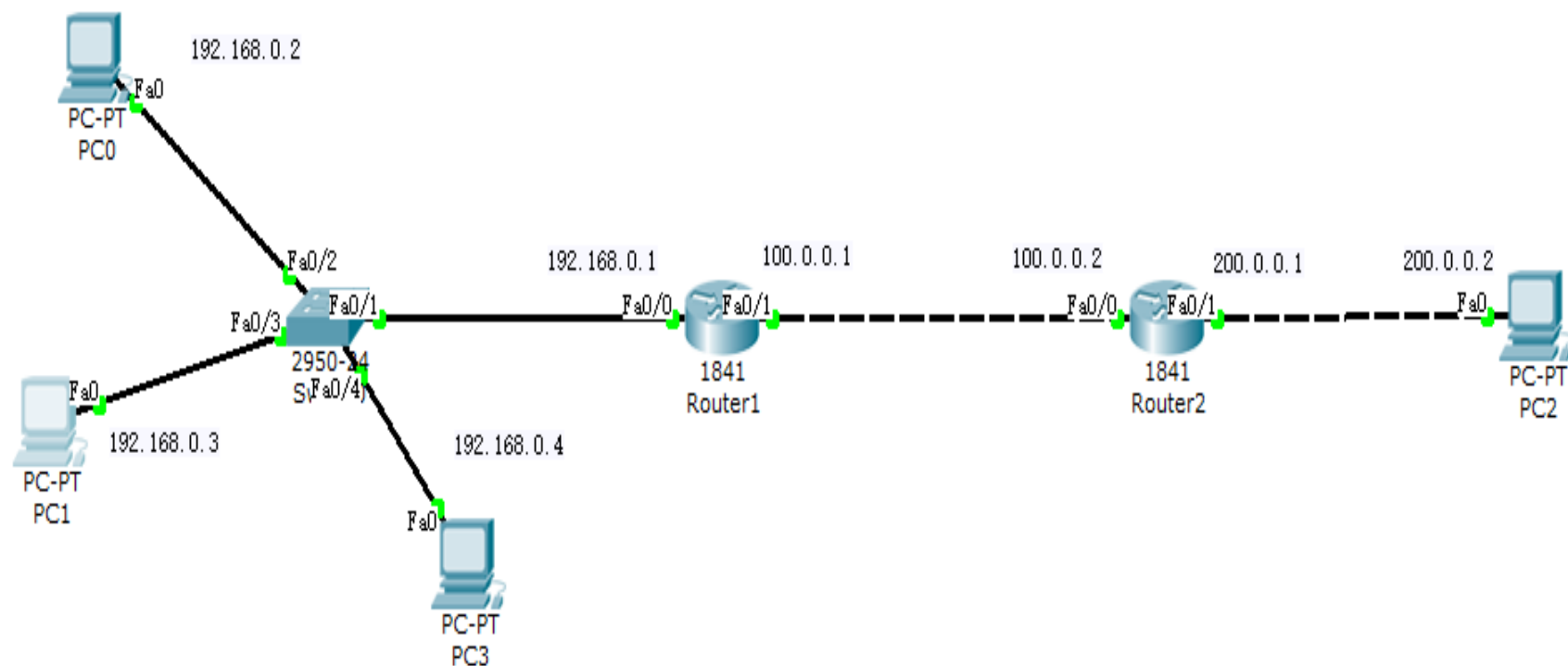
3、**ip nat inside source list number pool name overload**

其中, **number**还是2号命令中的访问控制列表号;

**name**还是1号命令中的地址池的名字;

**overload**是实现PAT的关键字, 不能省略。

# PAT的配置实例



# PAT的配置实例

## Router1

Router>enable

Router#configure terminal

Router(config)#interface f0/0

Router(config-if)#ip address 192.168.0.1 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#ip nat inside

Router(config-if)#EXIT

Router(config)# interface f0/1

Router(config-if)# ip address 100.0.0.1 255.0.0.0

Router(config-if)# no shutdown

Router(config-if)# ip nat outside

Router(config-if)#EXIT

Router(config)#ip nat pool AAA 100.0.0.1 100.0.0.1 netmask 255.0.0.0

Router(config)#access-list 10 permit 192.168.0.0 0.255.255.255

Router(config)#ip nat inside source list 10 pool AAA overload

Router(config)#ip route 0.0.0.0 0.0.0.0 f0/1

# PAT的配置实例

---

## Router2

Router>enable

Router#configure terminal

Router(config)#interface f0/0

Router(config-if)#ip address 100.0.0.2 255.0.0.0

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface f0/1

Router(config-if)#ip address 200.0.0.1 255.255.255.0

Router(config-if)#no shutdown

Router(config)#exit

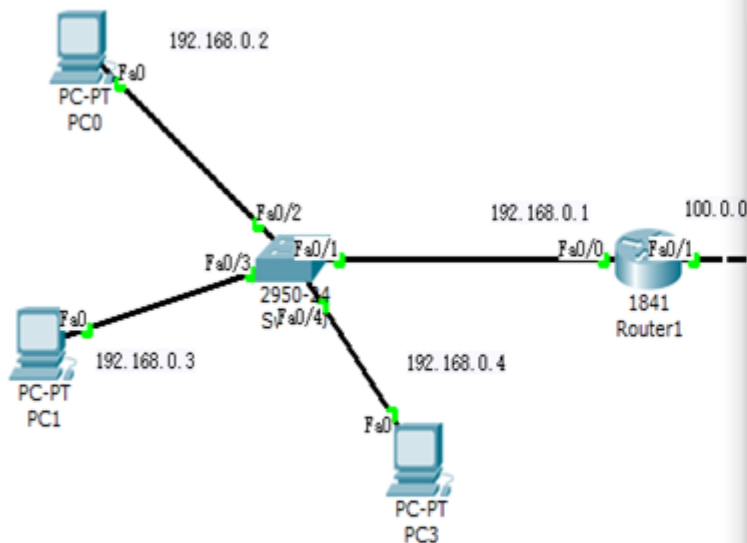
Router(config)#ip route 0.0.0.0 0.0.0.0 f0/0

Router(config)#exit



# PAT的配置实例

PC2>ping 192.168.0.3



PC2

Physical Config Desktop Custom Interface

### Command Prompt

```
Pinging 192.168.0.4 with 32 bytes of data:
Request timed out.
Reply from 100.0.0.1: bytes=32 time=0ms TTL=126
Reply from 100.0.0.1: bytes=32 time=0ms TTL=126
Reply from 100.0.0.1: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.0.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:
Request timed out.
Reply from 100.0.0.1: bytes=32 time=0ms TTL=126
Reply from 100.0.0.1: bytes=32 time=0ms TTL=126
Reply from 100.0.0.1: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.0.3:
```

# PAT的配置实例

当网络地址转换产生后，查看Router1的PAT信息

- Router#show ip nat translations
- | Pro  | Inside global | Inside local   | Outside local | Outside global |
|------|---------------|----------------|---------------|----------------|
| icmp | 100.0.0.1:41  | 192.168.0.3:41 | 200.0.0.2:41  | 200.0.0.2:41   |
| icmp | 100.0.0.1:42  | 192.168.0.3:42 | 200.0.0.2:42  | 200.0.0.2:42   |
| icmp | 100.0.0.1:43  | 192.168.0.3:43 | 200.0.0.2:43  | 200.0.0.2:43   |
| icmp | 100.0.0.1:44  | 192.168.0.3:44 | 200.0.0.2:44  | 200.0.0.2:44   |
- Router#

# 作业内容与要求

---

- 1.理解并熟练掌握路由器的IOS操作命令;
- 2.使用Cisco Paket Tracer平台, 自行设计网络拓扑结构图。网络内至少包含两台路由器设备及若干台终端;
- 3.注明各网段地址和各端口地址;
- 4.配置各终端的网卡地址和网关, 并给出图示;
- 5.使用默认路由使全网互通;
- 6.使用NAT/PAT技术, 通过转换访问Internet, 并给出配置过程。

邮箱: luxq@bupt.edu.cn

- 
- 邮箱: [luxq@bupt.edu.cn](mailto:luxq@bupt.edu.cn)



谢谢！