

1

NAT网络地址转换

冯巾松

fengjinsong@tongji.edu.cn

技术原理1

2

- ➡ 网络地址转换 NAT (Network Address Translation)，被广泛应用于各种类型 Internet 接入方式和各种类型的网络中。
- ➡ 最初出现NAT的原因就是IPv4公有地址不够用。 NAT不仅完美地解决了IP地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。

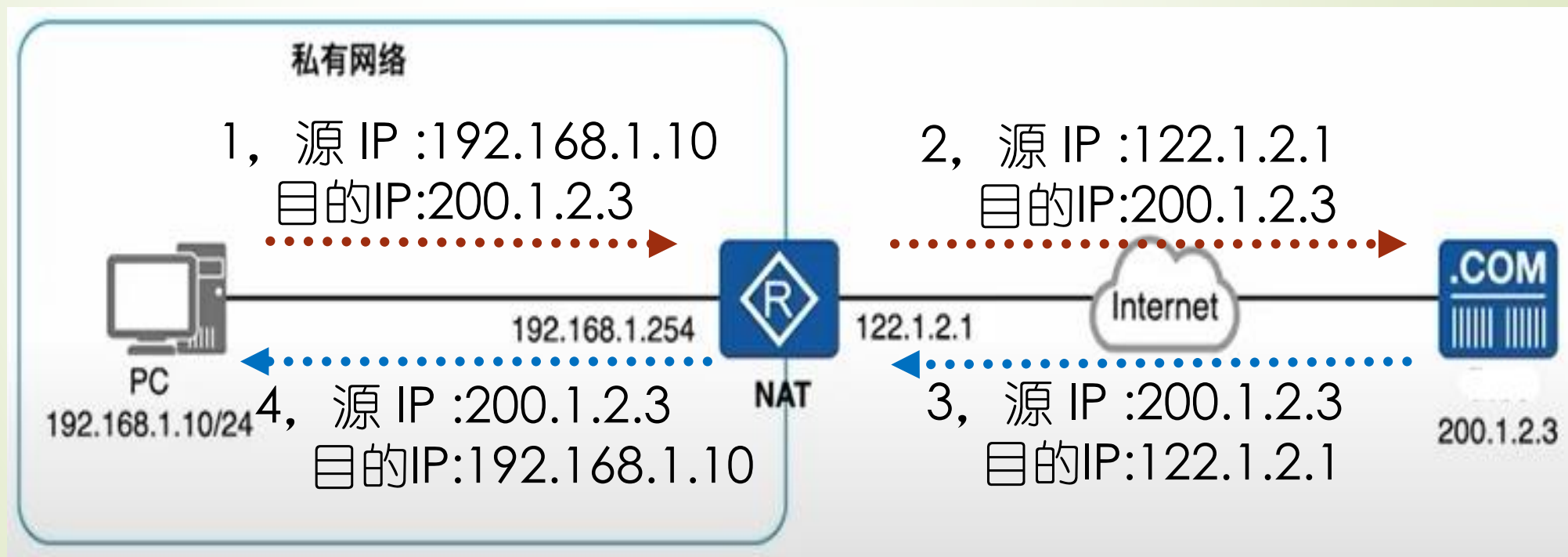
技术原理2

3

- 默认情况下，内部IP地址是无法被路由到外网的，内部主机要与外部网络或internet通信，IP包到达 NAT路由器时，IP包头的源地址被替换成一个合法的外网IP，并在NAT转换表中保存这条记录。
- 当外部主机发送一个应答到内网时，NAT路由器收到后，查看当前NAT转换表，用内网地址替换掉这个外网地址

技术原理3

➡ NAT将网络划分为内部网络和外部网络两部分，局域网主机利用NAT访问网络时，是将局域网内部的本地地址转换为全局地址（外部网络或互联网合法的IP地址）后转发数据包；



NAT优缺点

➡ 优点

- ✓ 节省公有地址
- ✓ 对外隐藏地址，提供安全性

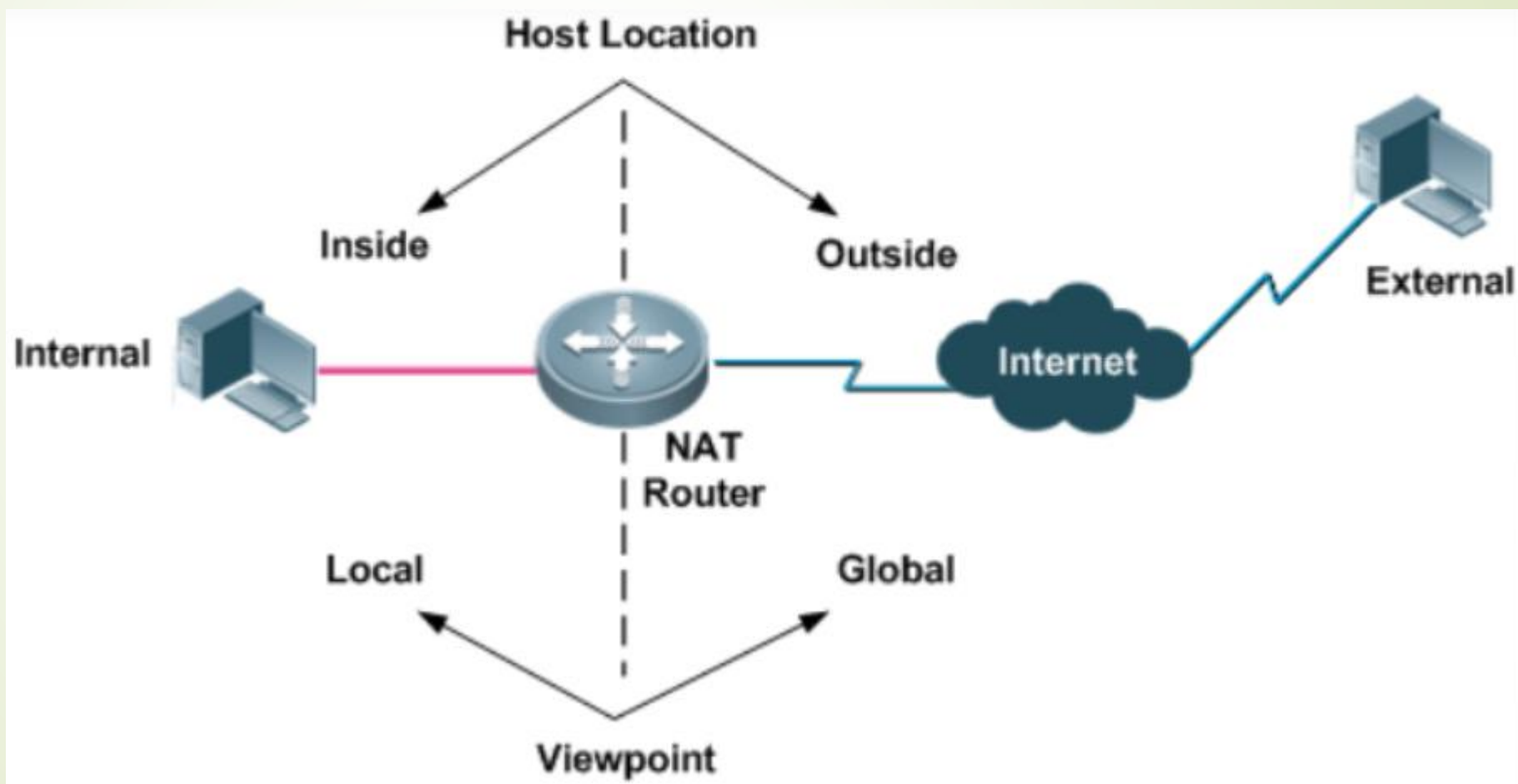
➡ 缺点

- ✓ 转换延迟和设备压力
- ✓ 无法执行端到端跟踪
- ✓ 影响特定的应用

NAT术语

6

- 内部/外部：主机相对NAT设备的物理位置
- 本地/全局：用户相对NAT设备的位置视角



NAT术语

7

内部本地地址：分配给内部网络中主机的地址，通常是私有地址

SA Inside local	DA outside local
--------------------	---------------------

PC-PT
PCA

inside outside

内部全局地址：对外代表一个或多个内部本地地址，通常是公有地址

SA Inside global	DA outside global
---------------------	----------------------

2960-24TT
SW

Server-PT
PCB

DA inside local	SA outside local
--------------------	---------------------

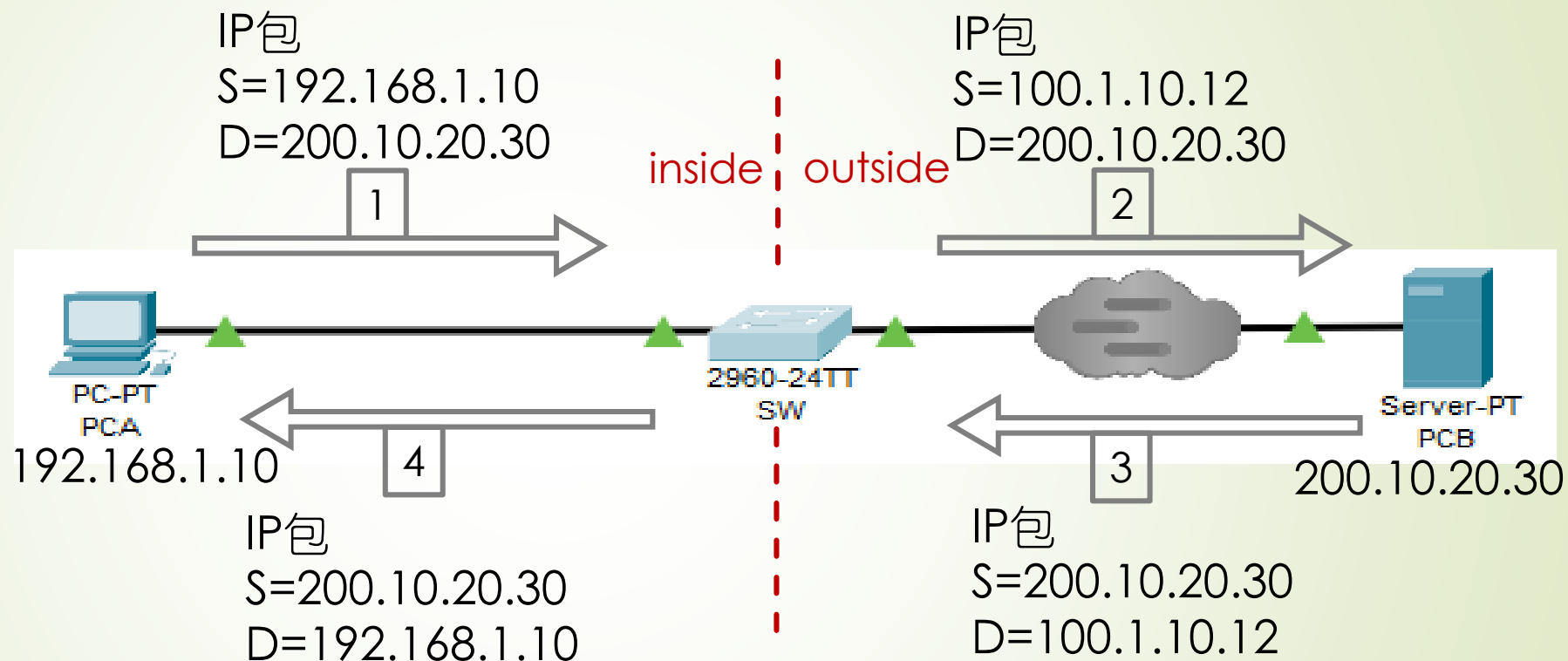
外部本地地址：在内部网络看到的外部主机地址

DA inside global	SA outside global
---------------------	----------------------

外部全局地址：外部网络中的真实地址

NAT术语

8



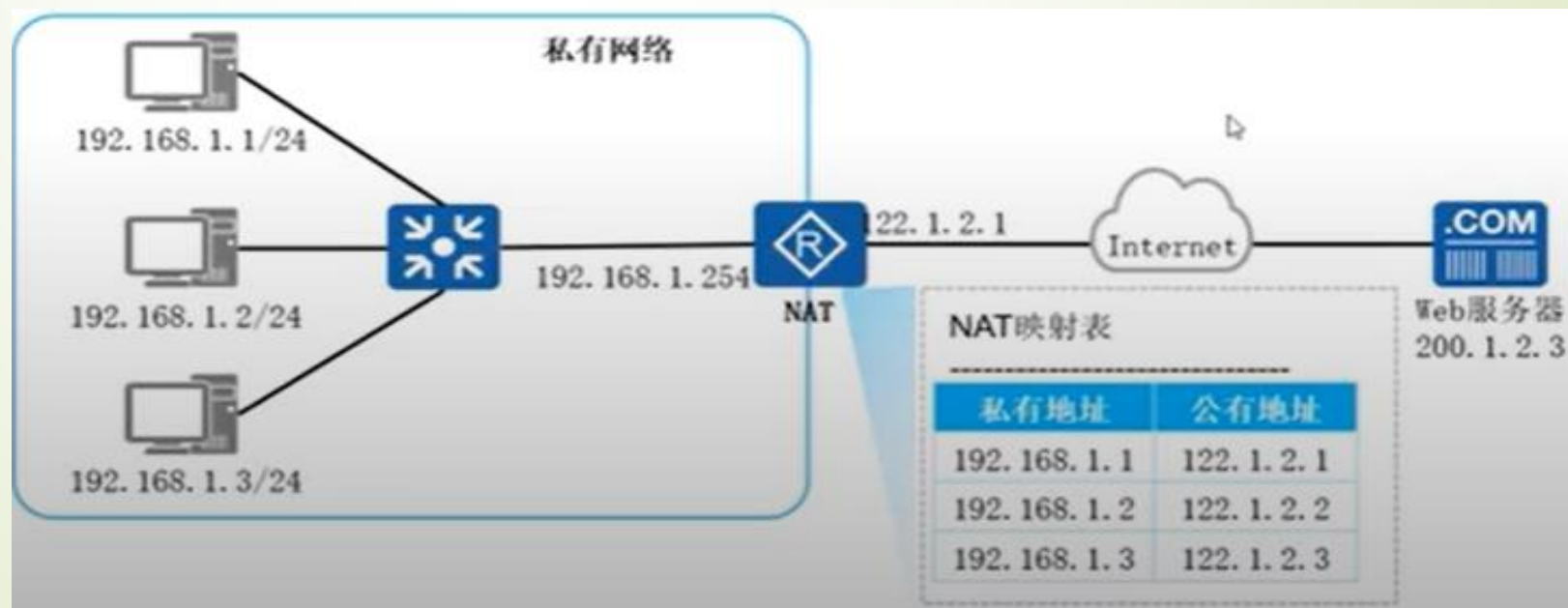
```
SW#show ip nat translations
```

NAT转换表

Pro	inside global	inside local	outside local	outside global
tcp	100.1.10.12:6004	192.168.1.10:6004	200.10.20.30:80	200.10.20.30:80

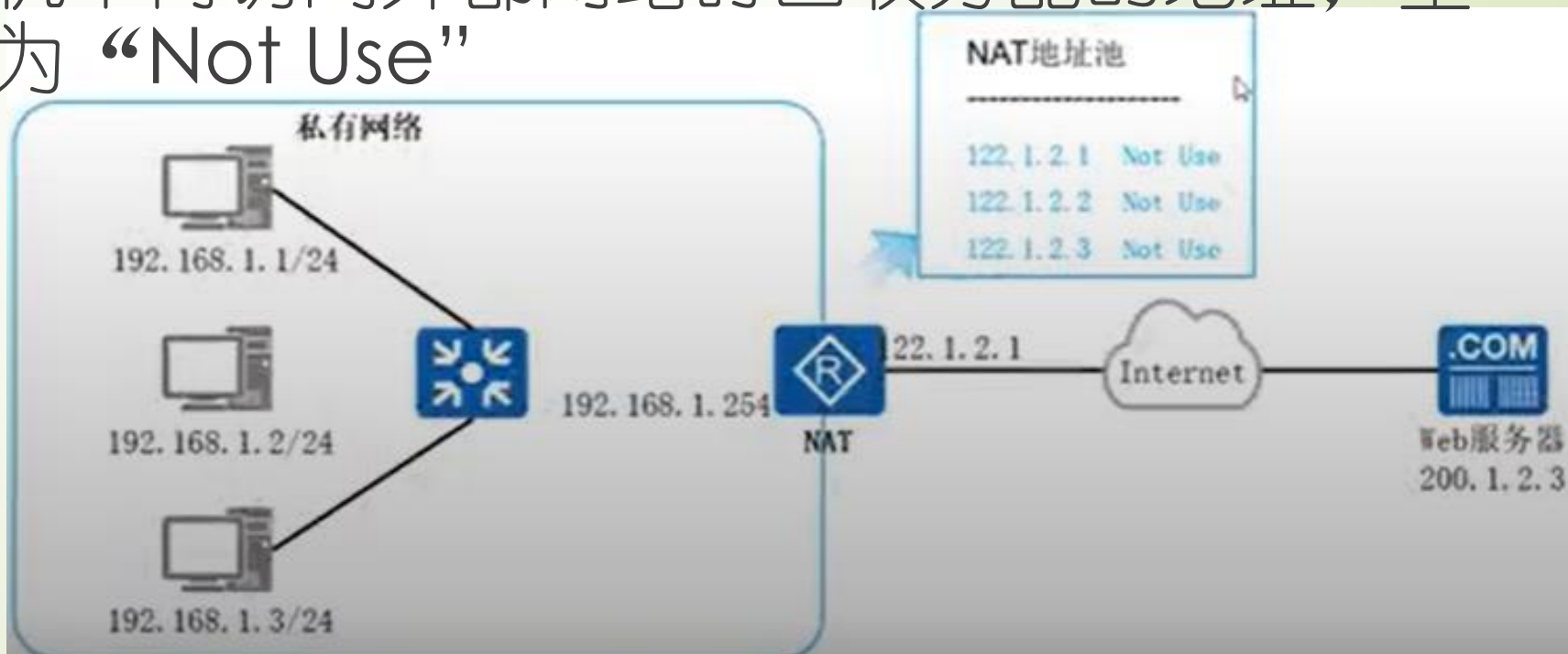
NAT分类 – 静态NAT

- 静态NAT将每个内部网络的私有地址与外部网络的公有IP地址**一对一**映射。现实中，一般都用于服务器；
- 支持双向互访：私有地址访问internet经过出口设备NAT转换时，会被转换从对应的公有地址。外部网络访问内部网络时，其报文中携带的公有地址（目的地址）也会被NAT设备转换成对应的私有地址。



NAT分类 – 动态NAT

- 动态NAT：定义一个地址池，自动映射，也就是一对多。
- 当内部主机访问外部网络时临时分配一个地址池中的为使用的地址，并将该地址标记为 “In Use”。当该主机不再访问外部网络时回收分配的地址，重新标记为 “Not Use”



动态NAT转换

11

STEP1: 选择一个地址池中未使用的地址作为转换后的地址, 同时将该地址的标记变为 “In Use”

1, 源 IP :192.168.1.1
目的IP:200.1.2.3

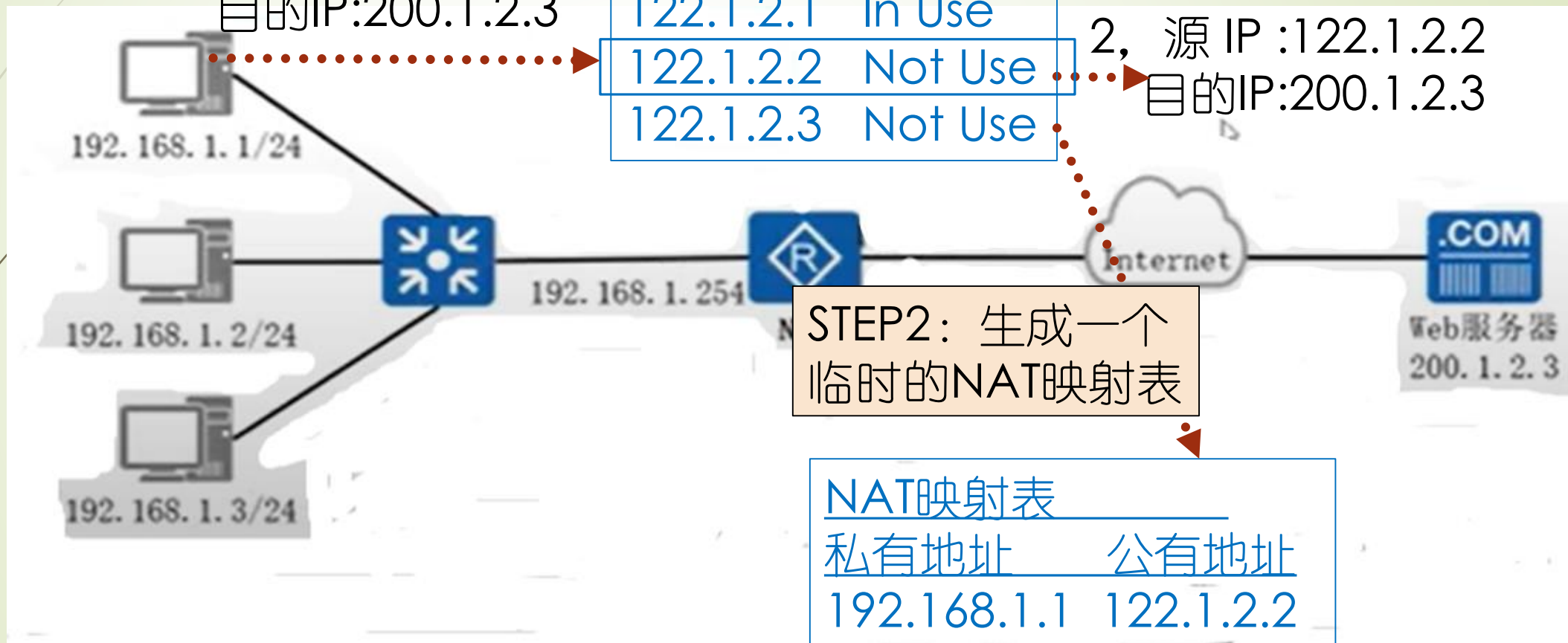
NAT地址池

122.1.2.1 In Use

122.1.2.2 Not Use

122.1.2.3 Not Use

2, 源 IP :122.1.2.2
目的IP:200.1.2.3



STEP2: 生成一个临时的NAT映射表

NAT映射表

私有地址	公有地址
192.168.1.1	122.1.2.2
192.168.1.2	122.1.2.1

动态NAT转换

NAT映射表

私有地址	公有地址
------	------

192.168.1.1	122.1.2.2
-------------	-----------

192.168.1.2	122.1.2.1
-------------	-----------

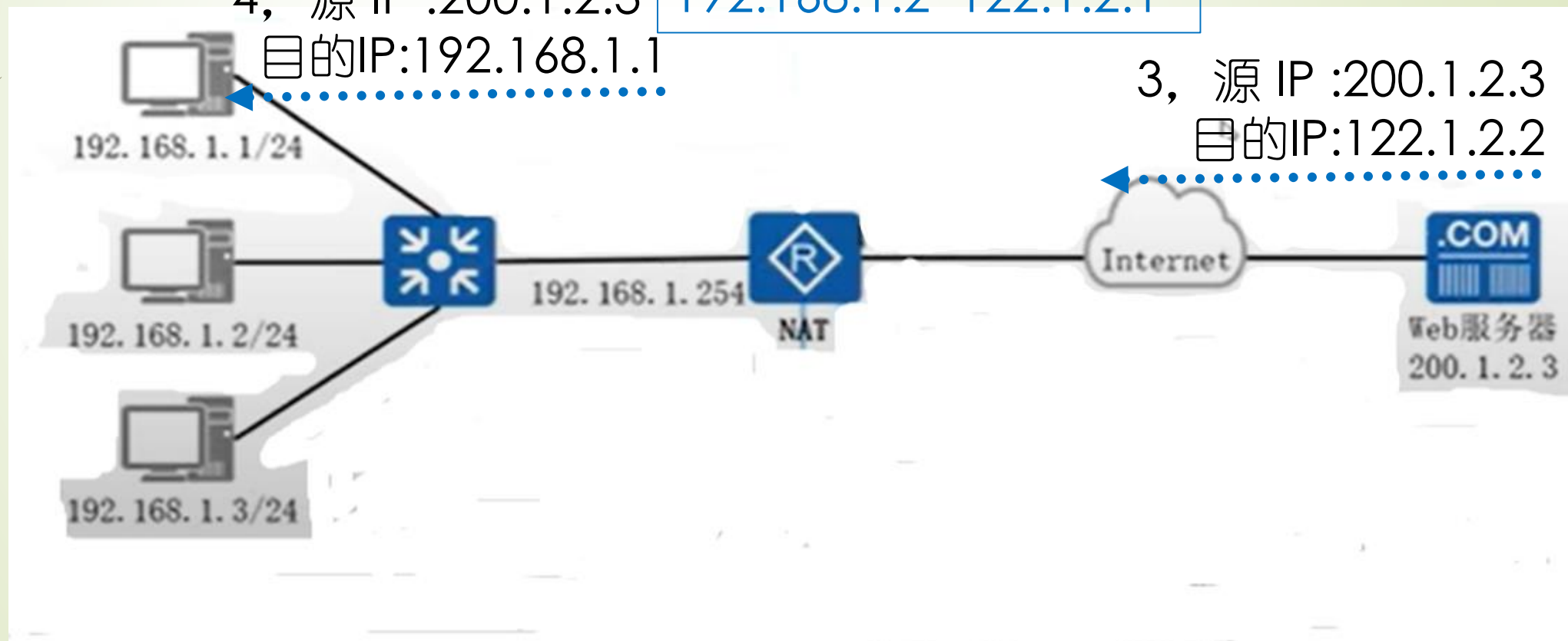
匹配

4, 源 IP :200.1.2.3

目的IP:192.168.1.1

3, 源 IP :200.1.2.3

目的IP:122.1.2.2



NAT分类 – NAT

13

- ➡ NAT (Network Address Port Translation)，即网络地址端口转换
- ➡ NAT使用不同的端口来映射多个内网IP地址到一个指定的外网IP地址，**多对一**
- ➡ NAT采用端口多路复用方式。内部网络的所有主机均可共享一个合法外部IP地址实现对Internet的访问，从而可以最大限度地节约IP地址资源。
- ➡ NAT又可隐藏网络内部的所有主机，有效避免来自Internet的攻击。
- ➡ 目前网络中应用最多的就是端口多路复用方式

基本配置步骤

- ➡ 1, 进入全局配置模式, 指定内部和外部接口: 使用interface命令配置内部和外部接口, 并使用ip nat inside和ip nat outside命令分别指定这些接口为NAT的内部和外部接口
- ➡ 2, 使用access-list命令创建一个访问控制列表, 指定需要进行NAT的内部IP地址范围
- ➡ 3, 应用NAT规则: 根据所需的NAT类型(静态、动态或PAT), 使用相应的命令将ACL与NAT池或接口关联起来

基本配置步骤

➡ 3.1 静态NAT配置

ip nat inside source static 内部本地地址 内部合法地址

➡ 3.2 动态NAT配置

- ✓ 使用 “ip nat pool 地址池名称 起始IP地址 终止IP地址 子网掩码” 命令创建一个NAT池
- ✓ 使用 “ip nat inside source list 访问列表标号 pool 内部合法地址池名字” 命令将ACL与NAT池关联起来

➡ 3.3 PAT配置

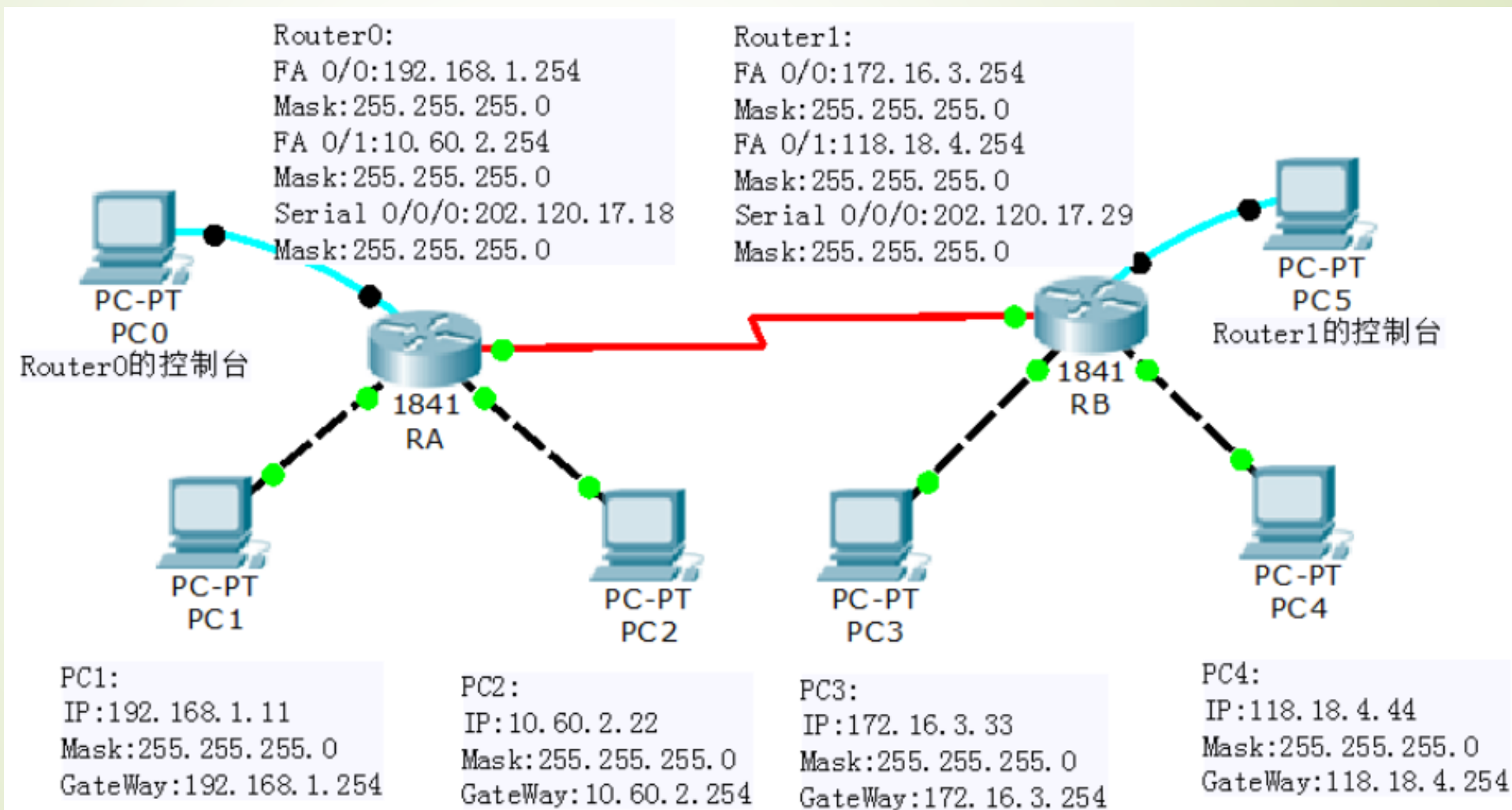
- ✓ 为PAT配置一个只包含一个公有IP地址的NAT池
- ✓ 在将ACL与NAT池关联的命令中使用overload关键字，以启用PAT功能

实验内容（静态NAT）

- ➡ 1 首先规划网络地址及拓扑图；
- ➡ 2 配置PC机、服务器及路由器IP地址；
- ➡ 3 在各路由器上配置静态路由协议，让pc间能相互 ping通；
- ➡ 4 在路由器上配置静态NAT；
- ➡ 5 在路由器上定义内外部网络接口；
- ➡ 6 验证主机之间的互通性

步骤1

网络拓扑及地址规划



实验过程1

- (1) 配置好PC的地址、网关及掩码；
- (2) 配置路由器的端口地址；

路由器A: interface FastEthernet0/0
ip address 192.168.1.254 255.255.255.0
interface FastEthernet0/1
ip address 10.60.2.254 255.255.255.0

路由器B: interface FastEthernet0/0
ip address 172.16.3.254 255.255.255.0
interface FastEthernet0/1
ip address 118.18.4.254 255.255.255.0

注意：端口要no shutdown

实验过程2

19

➡ (2) 配置路由器的串口端口地址；
路由器A： interface Serial 0/0/0
ip address 202.120.17.18 255.255.255.0
Clock rate 56000

路由器B： interface Serial 0/0/0
ip address 202.120.17.29 255.255.255.0
Clock rate 56000

注意： 端口要no shutdown；
Clock rate 56000 只需配一端即可。

实验过程3

➤ (3) 配置路由器的静态路由表

路由器A：
ip route 218.100.3.0 255.255.255.0 serial 0/0/0
ip route 118.18.4.0 255.255.255.0 serial 0/0/0

路由器B：
ip route 10.60.2.0 255.255.255.0 serial 0/0/0
ip route 210.120.1.0 255.255.255.0 serial 0/0/0

➤ (4) 配置路由器A的NAT的出入口；

路由器A：
interface FastEthernet0/0
ip nat inside
interface Serial 0/0/0
ip nat outside

实验过程4

21

➡ 路由器B:

```
Router(config)#interface fastethernet0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface serial0/0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#
```

实验过程5

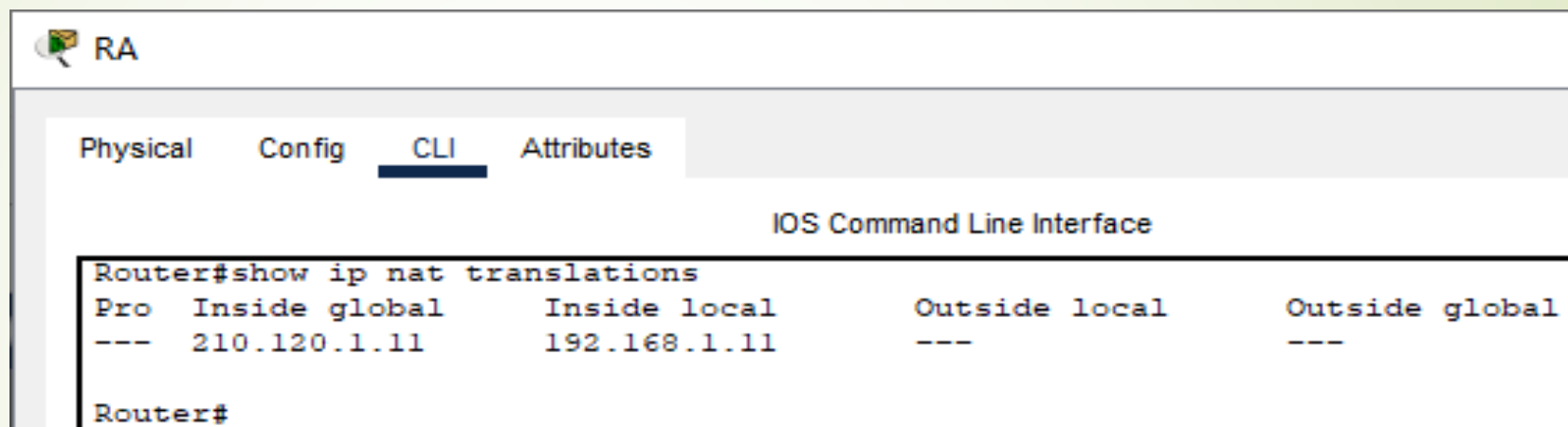
22

- (5) 配置路由器的NAT转换:
路由器A(在全局配置模式下配置NAT地址转换)
ip nat inside source static 192.168.1.11 210.120.1.11
路由器B(在全局配置模式下配置NAT地址转换)
ip nat inside source static 172.16.3.33 218.100.3.33

实验过程6

23

➡ 路由器A: show ip nat translations

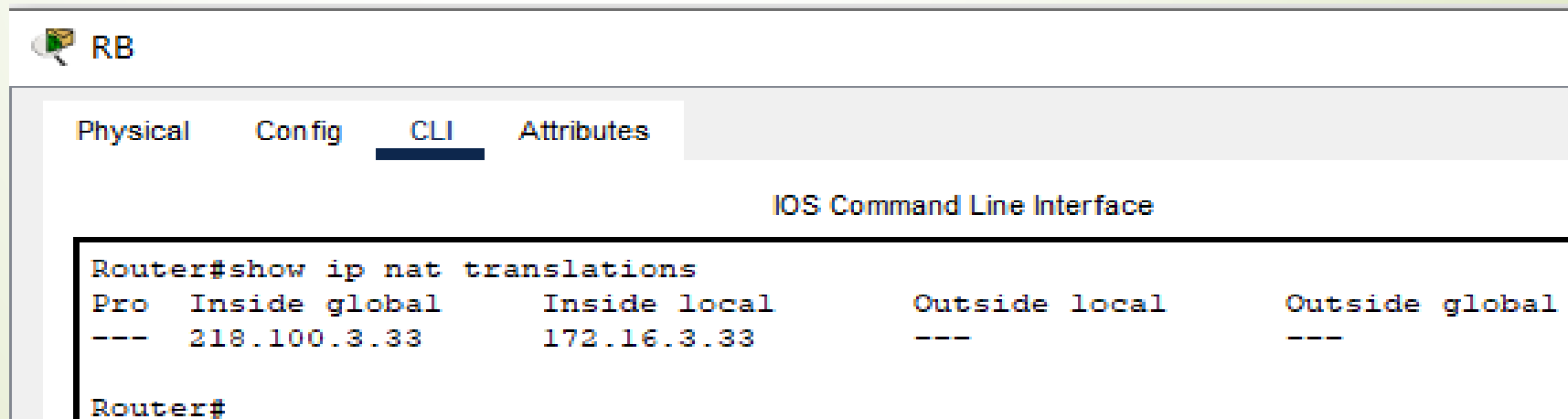


The screenshot shows the CLI of Router A (RA). The 'CLI' tab is selected. The command 'show ip nat translations' has been executed, displaying the following output:

Pro	Inside global	Inside local	Outside local	Outside global
---	210.120.1.11	192.168.1.11	---	---

The prompt 'Router#' is visible at the bottom of the output.

➡ 路由器B: show ip nat translations



The screenshot shows the CLI of Router B (RB). The 'CLI' tab is selected. The command 'show ip nat translations' has been executed, displaying the following output:

Pro	Inside global	Inside local	Outside local	Outside global
---	218.100.3.33	172.16.3.33	---	---

The prompt 'Router#' is visible at the bottom of the output.

问题讨论分析

➡ 在各自PC端访问：

ping 192.168.1.11

ping 210.120.1.11

ping 10.60.2.22

ping 172.16.3.33

ping 218.100.3.33

ping 118.18.4.44

➡ 比较结果并解释原因

NAPT配置步骤

- ➡ 1, 配置接口IP地址：为路由器的各个接口配置IP地址，并确保接口已经启用
例如：

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

```
Router(config-if)# ip address 192.168.1.1 255.255.255.0
```

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

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

- ➡ 2, 定义NAT地址池：NAT地址池是动态NAPT配置中用于分配外部IP地址的范围。

例如：

```
Router(config)# ip nat pool yx 192.168.1.1  
192.168.1.10 netmask 255.255.255.0
```

NAPT配置步骤

➡ 3. 定义访问控制列表（ACL）：用于指定哪些内部IP地址和端口号需要进行NAPT转换。

例如：`Router(config)#access-list 101 permit 196.168.1.0 0.0.0.255`

➡ 4. 配置动态NAPT：将访问控制列表与NAT地址池关联，并启用PAT（端口地址转换），这是NAPT的实现方式。

例如：

`Router(config)#ip nat inside source list 101 pool yx overload`

NAPT配置步骤

- ➡ 5, 配置NAT方向: 指定哪些接口是内部接口 (inside) 和外部接口 (outside)

例如: Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# ip nat outside
Router(config-if)# exit

- ➡ 6, 验证配置: 配置完成后, 可用以下命令验证NAT转换记录

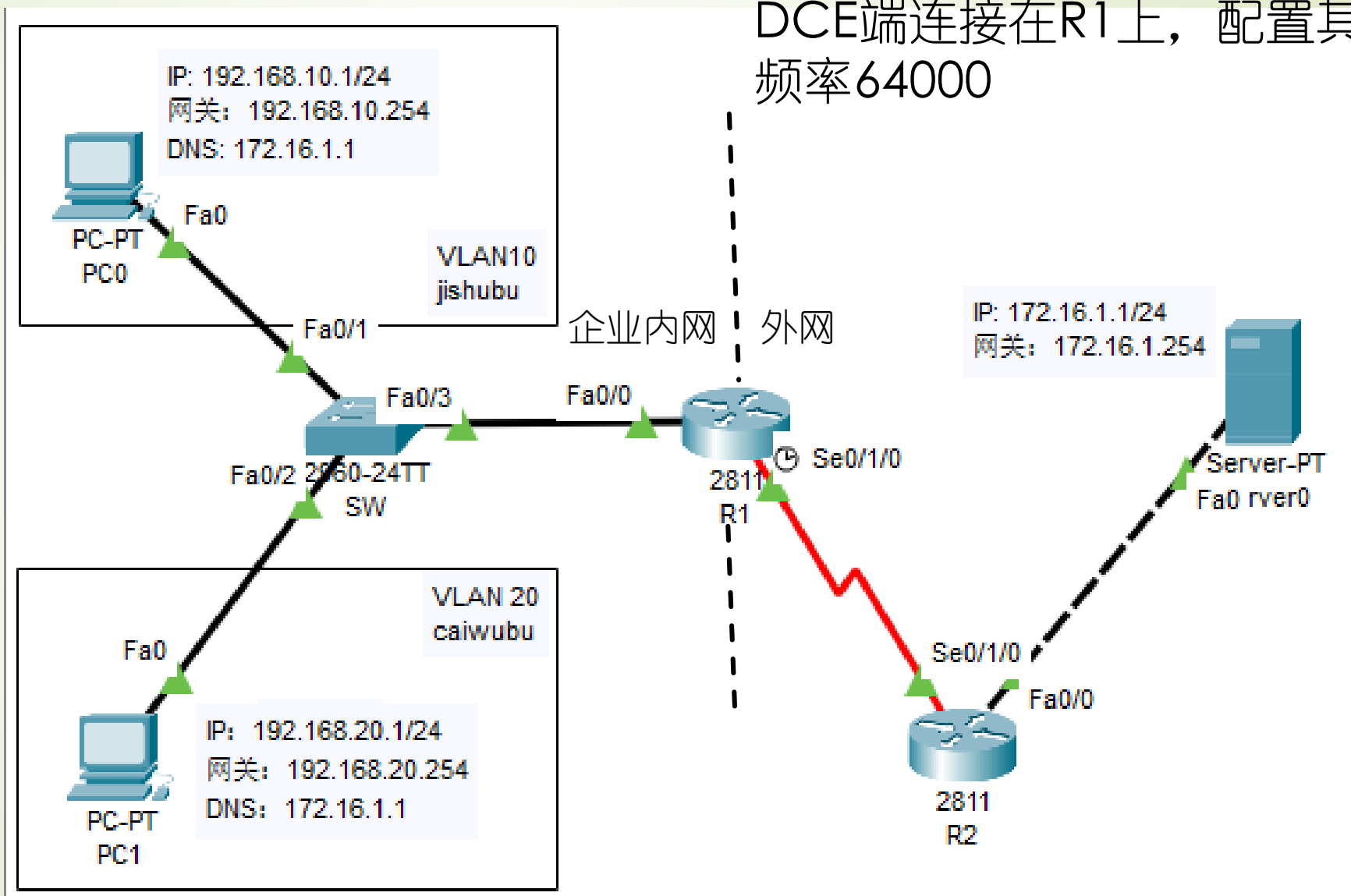
Router# show ip nat translations

实验内容 (NAPT)

- 1, 首先规划网络地址及拓扑图;
- 2, 配置PC机、服务器及路由器接口IP地址;
- 3, 在各路由器上配置静态路由协议, 让PC间能相互Ping通;
- 4, 在R1上配置NAPT。
- 5, 在R1上定义内外网络接口。
- 6, 验证主机之间的互通性。
- 7, 验证NAT转换记录

步骤1，实验拓扑

R1为公司出口路由器，其与ISP路由器之间通过电缆串口连接，DCE端连接在R1上，配置其时钟频率64000



SW配置

Switch>en

Switch#configure terminal

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

Switch(config)#hostname SW

SW(config)#vlan 10

SW(config-vlan)#name jishubu

SW(config-vlan)#exit

SW(config)#vlan 20

SW(config-vlan)#name caiwubu

SW(config-vlan)#exit

SW(config)#interface fa0/1

SW(config-if)#switchport access vlan 10

SW(config-if)#exit

SW(config)#interface fa0/2

SW(config-if)#switchport access vlan 20

SW(config-if)#exit

SW(config)#interface fa0/3

SW(config-if)#switchport mode trunk

SW(config-if)#exit

R1配置

```
Router>enable
Router#configure terminal
Router(config)#interface fa0/0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fa0/0.1
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.254 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/0.2
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.254 255.255.255.0
Router(config-subif)#exit
Router(config)#interface s0/1/0
Router(config-if)#no shutdown
Router(config-if)#ip address 100.1.1.1 255.0.0.0
Router(config-if)#clock rate 64000
Router(config-if)#ip route 172.16.1.0 255.255.255.0 100.1.1.2
Router(config)#exit
Router#
```

封装协议设置为dot1q允许通过的vlan为10

R2配置

```
Router>enable
```

```
Router#configure terminal
```

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

```
Router(config)#hostname R2
```

```
R2(config)#interface s0/1/0
```

```
R2(config-if)#ip address 100.1.1.2 255.0.0.0
```

```
R2(config-if)#no shutdown
```

```
R2(config-if)#exit
```

```
R2(config)#ip route 192.168.0.0 255.255.0.0 100.1.1.1
```

```
R2(config)#interface fa0/0
```

```
R2(config-if)#no shutdown
```

```
R2(config-if)#ip address 172.16.1.254 255.255.255.0
```

```
R2(config-if)#exit
```

```
R2(config)#
```


步骤4-5, R1配置NAPT

Router>enable 命令格式: ip nat inside source list [ACL号] interface [外部接口] overload

Router#configure terminal

Router(config)#ip access-list extended gby

Router(config-ext-nacl)#permit ip 192.168.0.0 0.0.255.255 host 172.16.1.1

Router(config)#ip nat inside source list gby int s0/1/0 overload

Router(config)#interface fa0/0.1

Router(config-subif)#ip nat inside

内网接口(连接内网)

Router(config-subif)#exit

Router(config)#interface fa0/0.2

Router(config-subif)#ip nat inside

内网接口(连接内网)

Router(config-subif)#exit

Router(config)#interface s0/1/0

Router(config-if)#ip nat outside

外部接口(连接ISP)

Router(config-if)#exit

Router(config)#

步骤7, 验证

PC1

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.1.1

Pinging 172.16.1.1 with 32 bytes of data:

Reply from 172.16.1.1: bytes=32 time=1ms TTL=126
Reply from 172.16.1.1: bytes=32 time=14ms TTL=126
Reply from 172.16.1.1: bytes=32 time=10ms TTL=126
Reply from 172.16.1.1: bytes=32 time=16ms TTL=126

Ping statistics for 172.16.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 16ms, Average = 10ms

C:\>
```

R1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router#show ip nat translations
Pro  Inside global      Inside local          Outside local          Outside global
icmp 100.1.1.1:1         192.168.20.1:1       172.16.1.1:1          172.16.1.1:1
icmp 100.1.1.1:2         192.168.20.1:2       172.16.1.1:2          172.16.1.1:2
icmp 100.1.1.1:3         192.168.20.1:3       172.16.1.1:3          172.16.1.1:3
icmp 100.1.1.1:4         192.168.20.1:4       172.16.1.1:4          172.16.1.1:4

Router#
```