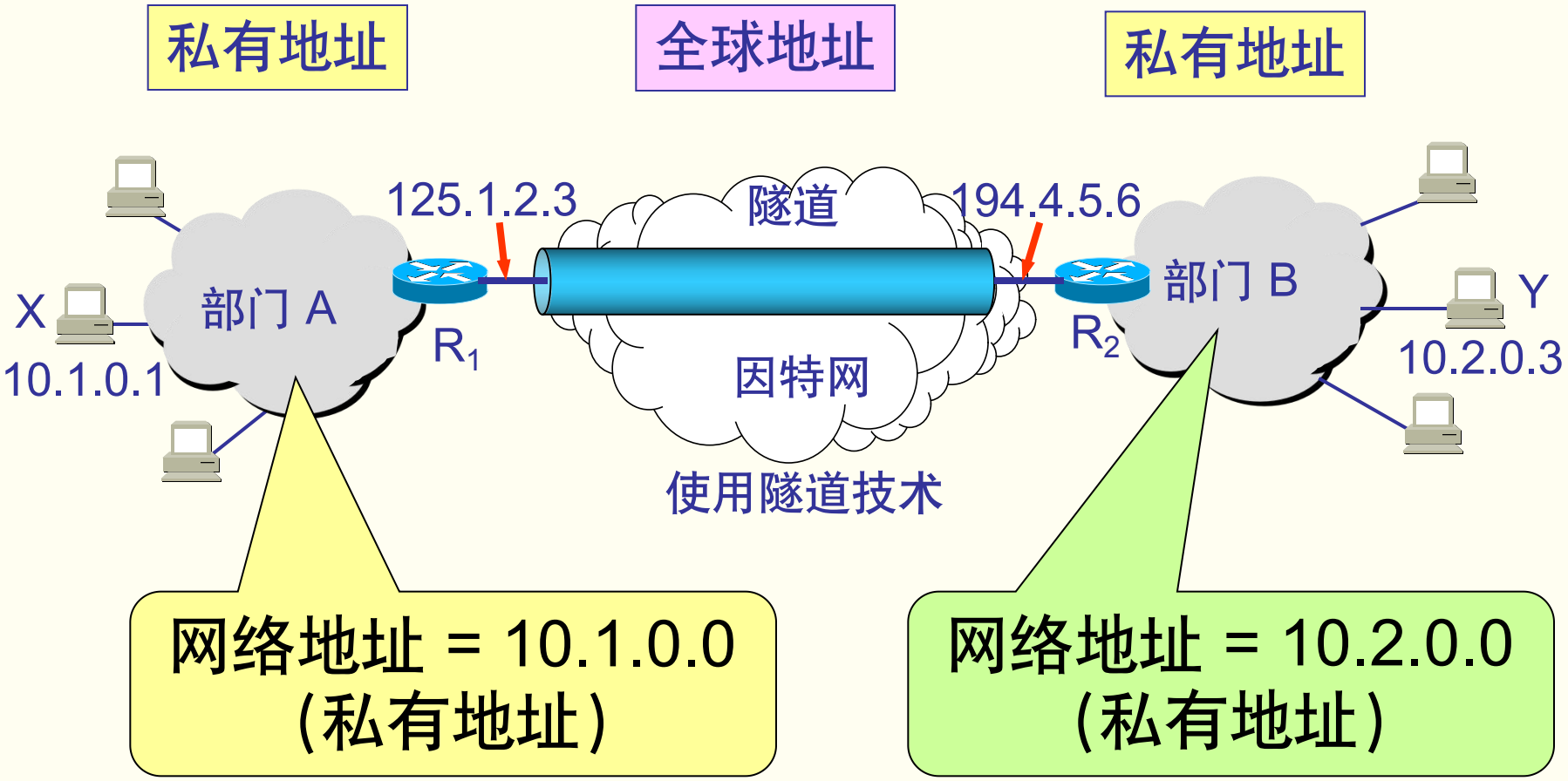
课程讲义5+实验5：
私有网络技术

卢美莲
北京邮电大学
计算机学院（国家示范性软件学院）
网络体系结构中心
mllu@bupt.edu.cn

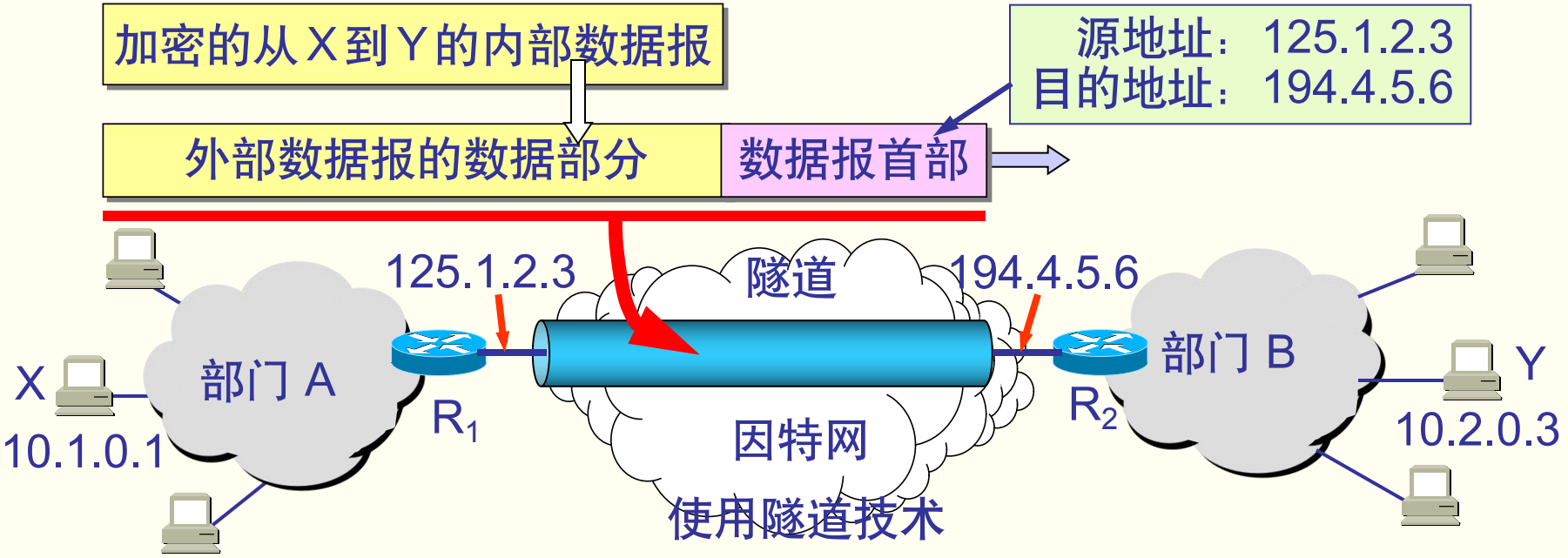
主要内容

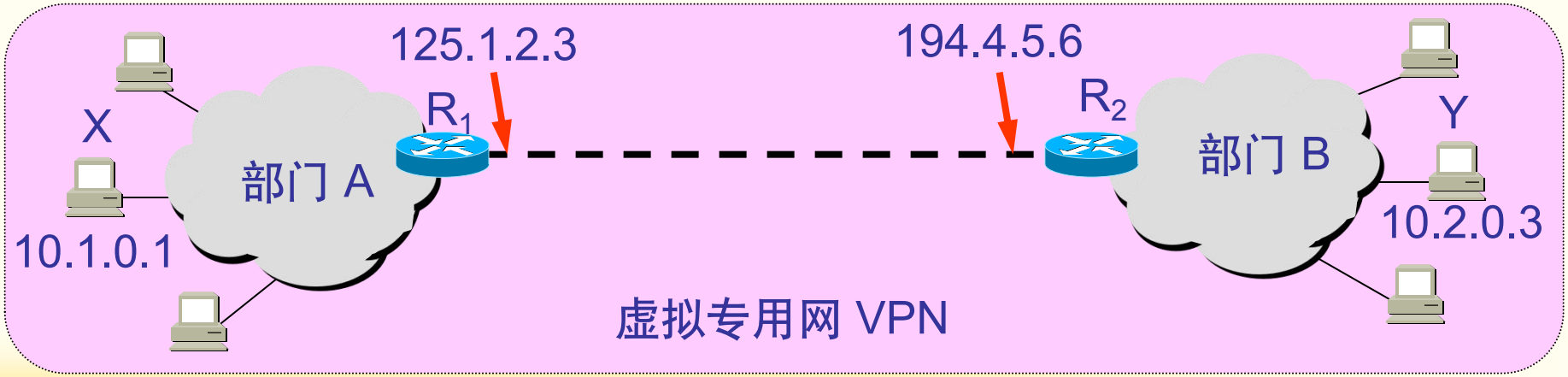
- NAT概述
- NAT配置命令
- 实验1：静态NAT配置
- 实验2：动态NAT配置
- 实验3：NAPT配置

使用隧道技术实现虚拟专用网



用隧道技术实现虚拟专用网（续）

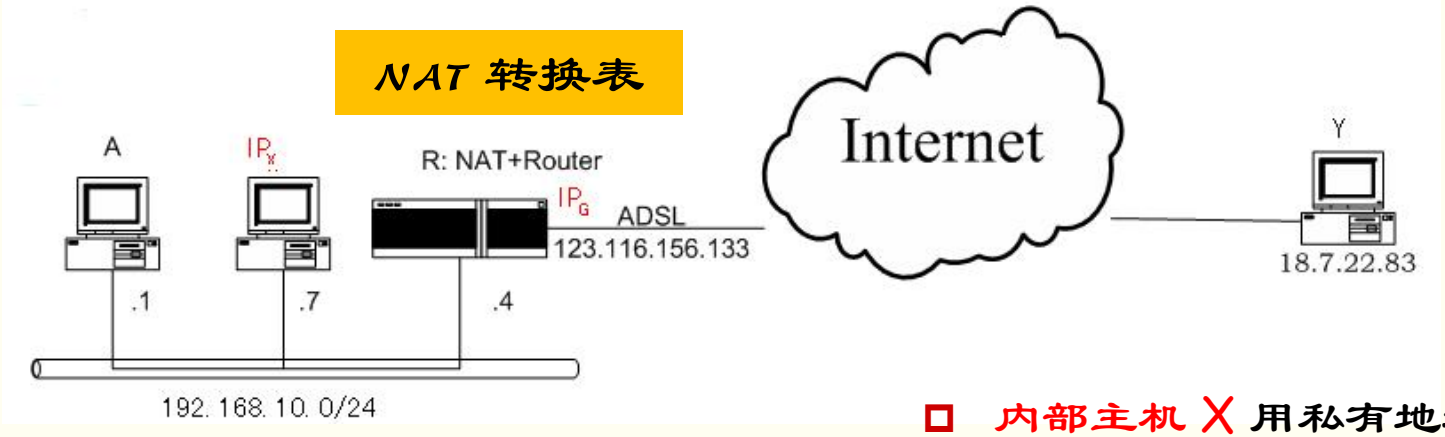




NAT概述

- 提出背景：接入Internet时IP地址受限
  - 随着Internet的飞速发展，网上丰富的资源具有巨大的吸引力，接入Internet成为当今信息业最为迫切的需求。但这受到IP地址的许多限制。
  - 首先，许多局域网在未联入Internet之前，就已经运行许多年了，局域网上的许多资源和应用程序的IP地址分配不符合Internet的国际标准，因而需要重新分配，这无疑是劳神费时的工作。
  - 其二，随着Internet的膨胀式发展，其可用的IP地址越来越少，要想在ISP处申请一个新的IP地址已不是很容易的事了。
- NAT（Network Address Translation，网络地址转换）
  - NAT于1994年提出，是IETF定义的一种把内部私有地址翻译成合法公有地址的技术，允许一个机构中Intranet的主机透明连接到公共区域中，无需内部主机拥有注册的Internet地址。
  - 简单的说，NAT是在局域网内部使用内部地址，而当内部节点要与外部网络进行通信时，在网关处将内部地址替换成公用地址，从而在外部公网正常使用。
  - NAT使多台计算机共享Internet连接。通过NAT，可以只申请一个合法IP地址，就把整个局域网中的计算机接入Internet中。这时，NAT屏蔽了内部网络，所有内部网计算机对于公共网络来说是不可见的，而内部网络的用户也不会意识到NAT的存在。

NAT概述（续）



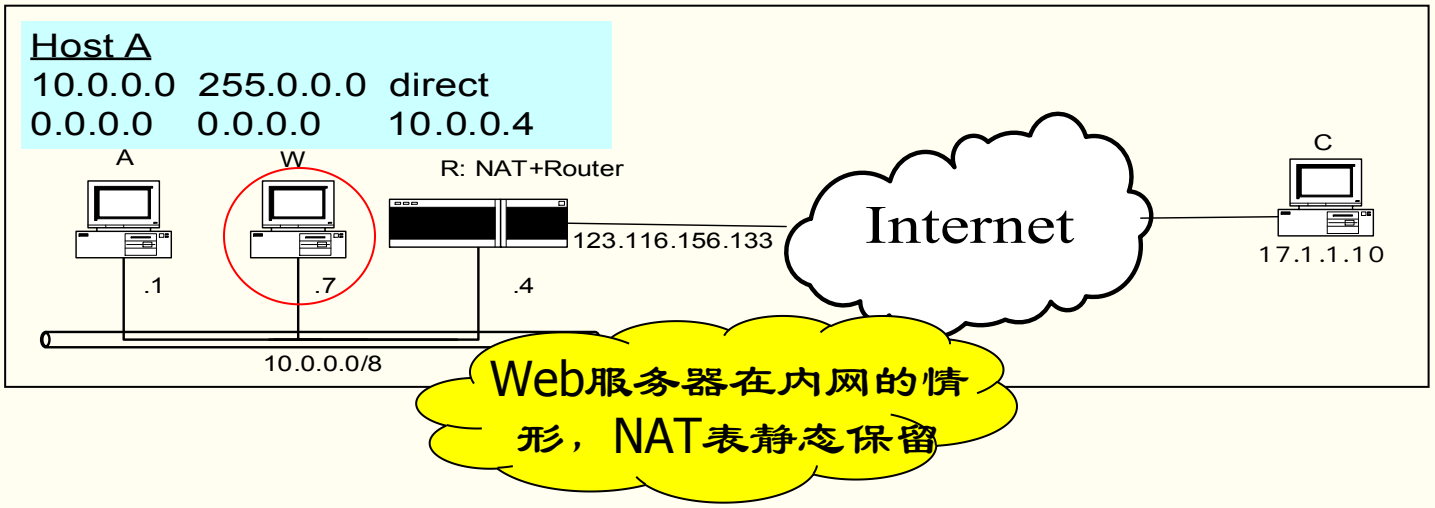
- 在专用网连接到因特网的路由器上需要安装 NAT 软件，装有 NAT 软件的路由器叫做 NAT 路由器
- NAT路由器至少有一个有效的外部全球地址 IP_G，所有使用本地地址的主机在和外界通信时都要在 NAT 路由器上将其本地地址转换成 IP_G 才能和因特网连接

- 内部主机 X 用私有地址 IP_X 和因特网上的主机 Y 通信时，所发送的数据报必须经过 NAT 路由器
- NAT 路由器将数据报的源地址 IP_X 转换成全球地址 IP_G，但目的地址 IP_Y 保持不变，然后发送到因特网
- NAT 路由器收到主机 Y 发回的数据报时，知道数据报中的源地址是 IP_Y，目的地址是 IP_G
- 根据 NAT 转换表，NAT 路由器将目的地址 IP_G 转换为 IP_X，转发给最终的内部主机 X

三种NAT类型

- 静态（Static）NAT
  - 最简单和最容易的一种NAT
  - 内部网络中的主机被永久映射成外部网络中的某个合法的地址
- 动态（Pooled）NAT
  - 为内部主机分配一个临时外部地址，并采用动态分配的方法映射到内部主机地址
  - 当连接远程用户时，动态NAT会分配给他一个外部IP地址，用户断开时，这个外部IP地址就会被释放而留待以后使用
- 网络地址端口转换NAPT（PortLevel NAT）
  - 把内部地址映射到外部网络的一个IP地址的不同端口上
  - NAPT普遍应用于接入设备中，它可以将中小型网络隐藏在一个合法的IP地址后面
  - 与动态NAT不同，它将内部连接映射到外部网络中的一个单独的IP地址上，并在该地址上加上一个由NAT设备选定的TCP端口号

静态NAT表项



R：设10.0.0.7为Web服务器

建立静态NAT表 (Local)10.0.0.7:8080—80(Global)

C：因特网上的客户端C发送TCP数据包：

17.1.1.10:3598->123.116.156.133:80

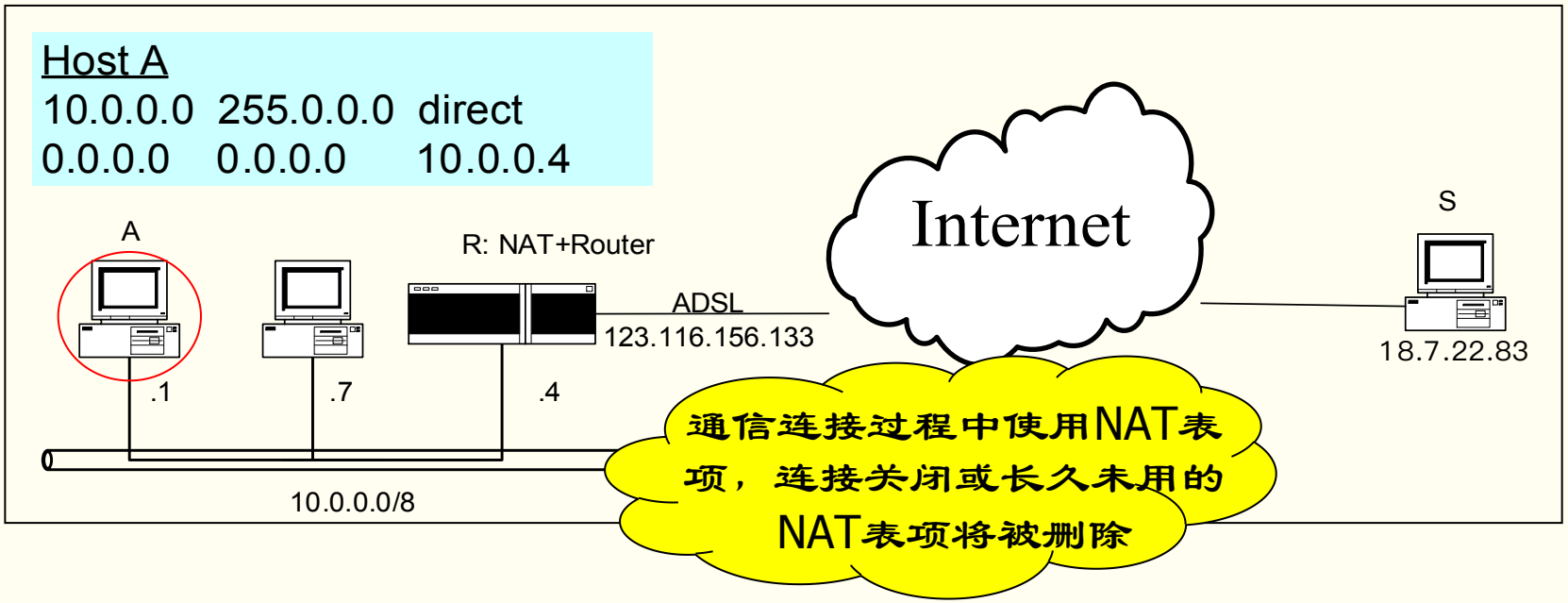
R：查 NAT表，修改17.1.1.10:3598->10.0.0.7:8080

W：Web服务器回数据10.0.0.7:8080->17.1.1.10:3598

R：查 NAT表，修改123.116.156.133:80->17.1.1.10:3598

C：收到返回TCP数据包123.116.156.133:80->17.1.1.10:3598

动态NAT表项



A：发送TCP数据包 10.0.0.1:3723-->18.7.22.83:80

R：路由器动态创建NAT表项:

(Local)10.0.0.1:3723—33120(Global)

修改TCP数据包 123.116.156.133:33120-->18.7.22.83:80

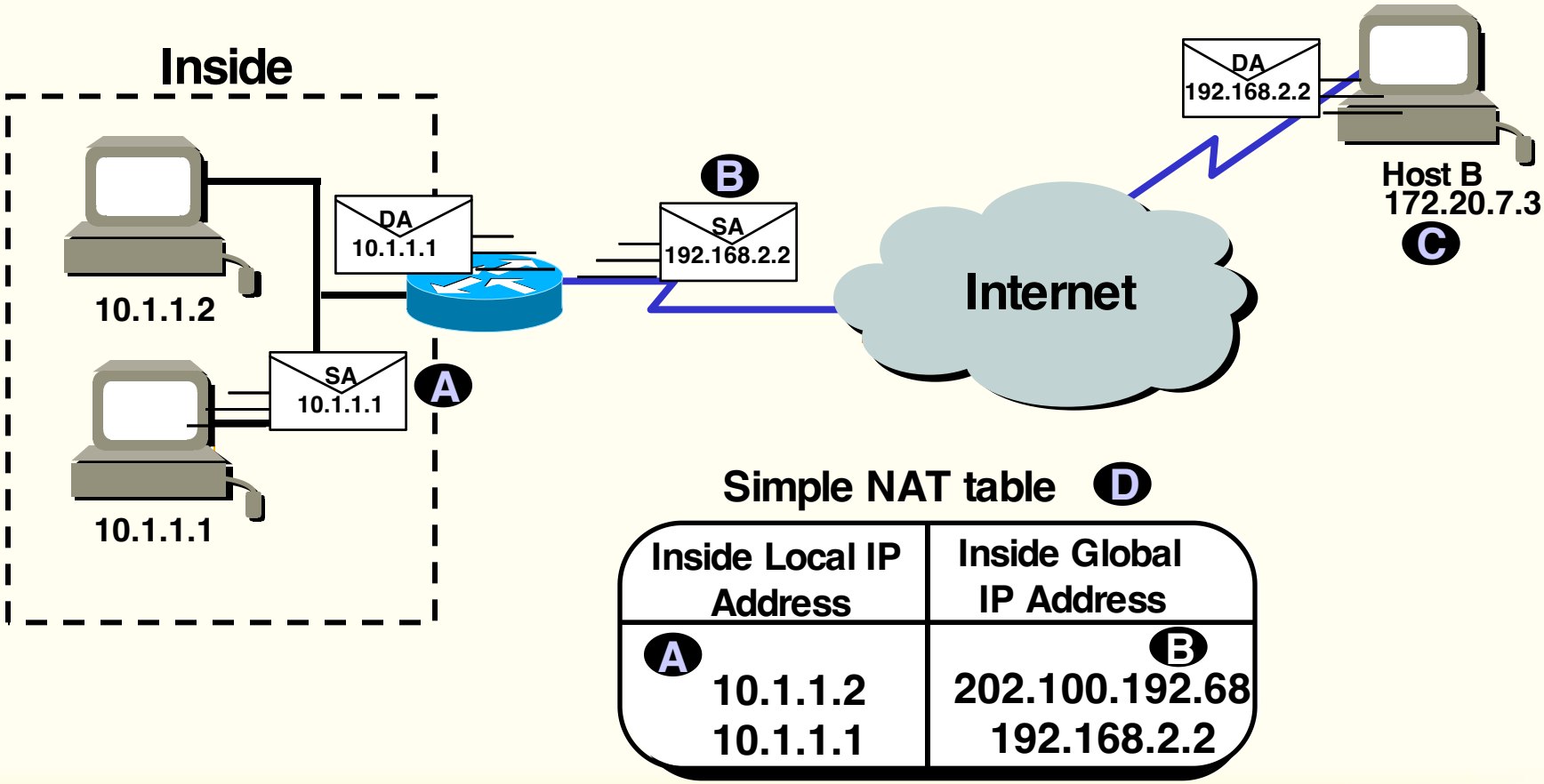
S：服务器S回数据18.7.22.83:80-->123.116.156.133:33120

R：查NAT表：修改TCP数据包 18.7.22.83:80-->10.0.0.1:3723

A：收到TCP数据包18.7.22.83:80-->10.0.0.1:3723

NAT术语

- 内部本地地址：私有IP，不能直接用于互连网
- 内部全局地址：用来代替内部本地IP地址，对外或在互联网上是合法的IP地址



主要内容

- NAT概述
- **NAT配置命令**
- 实验1：静态NAT配置
- 实验2：动态NAT配置
- 实验3：NAPT配置

NAT配置命令

- 配置接口的类型

  Router(config-if)#ip nat {inside|outside}

- 配置内部全局地址池

  Router(config)#ip nat pool pool-name start-ip end-ip {netmask netmask | prefix-length prefix-length }

  pool-name：地址池的名称
  start-ip，end-ip：地址池的起始地址和结束地址
  netmask：网络掩码
  prefix-length：网络占用的二进制位数

NAT配置命令

- **配置内部源地址转换**

  Router(config)#ip nat inside source {list access-list-number pool-name [overload] | static local-ip global-ip }

  access-list-number：访问列表编号
  overload：允许将多个内部本地地址转换为一个内部全局地址
  static：静态地址转换
  local-ip：内部本地地址
  global-ip：内部全局地址

- **配置使用单一内部全局地址的内部源地址转换**

  Router(config)#ip nat inside source list access-list-number interface interface-type [overload]

NAT配置命令

- 配置NAT超时时间

  Router(config)#ip nat translation timeout seconds

- 查看生效的NAT设置

  Router(config)#show ip nat translations

- 查看NAT统计信息

  Router(config)# show ip nat statistics

- 清除所有动态NAT配置

  Router(config)# clear ip nat translation *

- 清除单个动态NAT配置

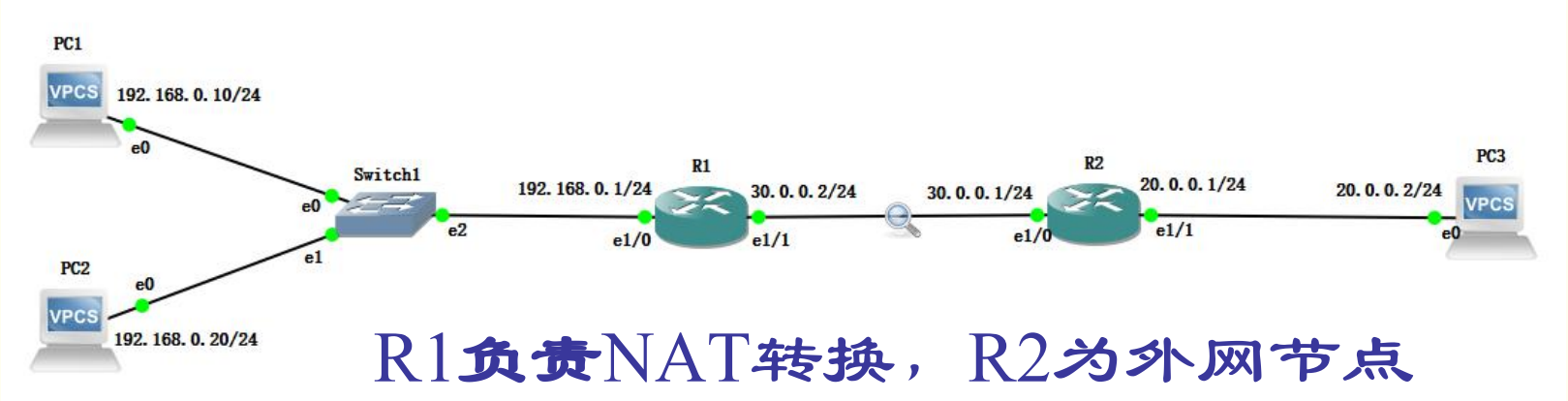
  Router(config)# clear ip nat translation <global-ip>

主要内容

- NAT概述
- NAT配置命令
- **实验1：静态NAT配置**
- 实验2：动态NAT配置
- 实验3：NAPT配置

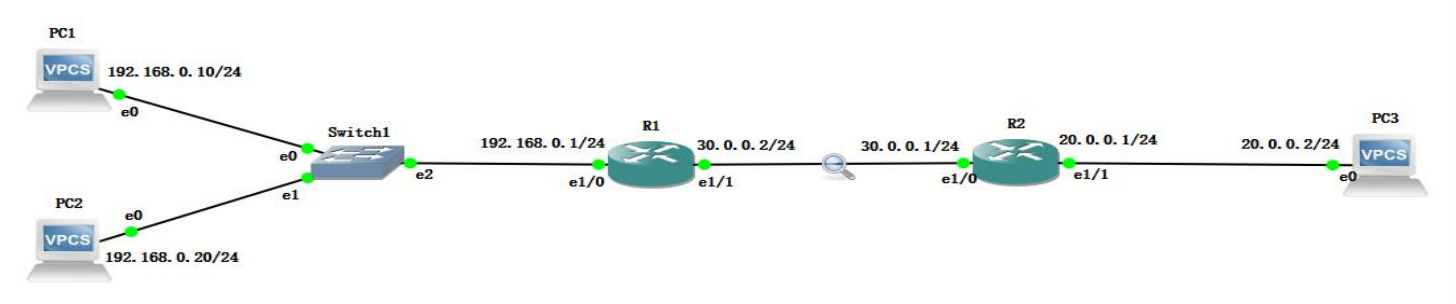
实验1：静态NAT配置

- 静态NAT：将内部主机IP一对一地翻译成外部地址
  - 在内部主机连接到外部网络时，当数据包到达NAT路由器时，路由器检查它的NAT表，因为NAT是静态配置的，可以查询出来
  - 然后路由器将数据包的内部本地IP（源地址）更换成内部全局地址，再转发出去
  - 外部主机接收到数据包后，用内部全局地址来响应，NAT接收到外部回来的数据包，再根据NAT表把数据包的外部全局IP翻译成内部本地IP



要求：通过静态NAT实现 192.168.0.10 到 20.0.0.2（外网）的访问

实验1：静态NAT配置

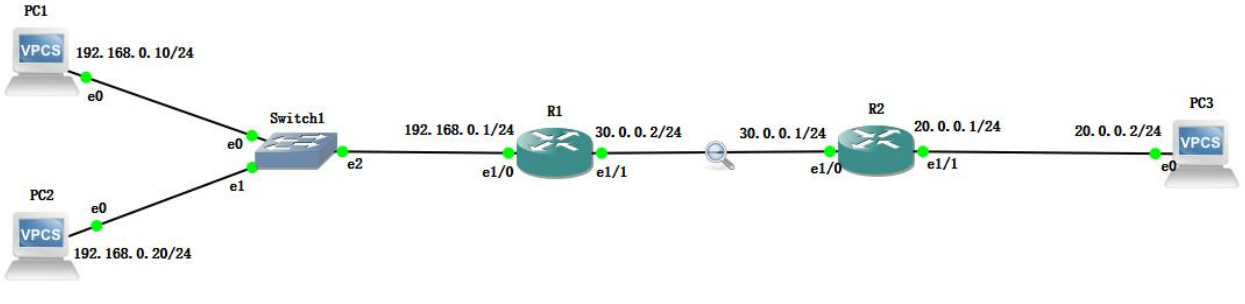



```
R1(config)#interface e1/0
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#ip nat inside      //指定路由器的内部接口

R1(config)#interface e1/1
R1(config-if)#ip address 30.0.0.2 255.0.0.0
R1(config-if)#ip nat outside     //指定路由器的外部接口

R1(config-if)#exit
R1(config)#ip nat inside source static 192.168.0.10  30.0.0.3
R1(config)#ip nat inside source static 192.168.0.20  30.0.0.4
```

//建立静态映射，其中内部本地地址是192.168.0.10和192.168.0.20，内部全局地址是30.0.0.3和30.0.0.4

实验1：静态NAT配置

- 测试：



PC1#ping 20.0.0.2
R1#debug ip nat
R1#

02:15:51: NAT*: s=192.168.0.10->30.0.0.3, d=20.0.0.2 [509]
02:15:51: NAT*: s=20.0.0.2, d=30.0.0.3->192.168.0.10 [509]
…

//R1把PC1发送的源地址为192.168.0.10的IP包转换为源地址为30.0.0.3 的IP包，其目的地址为20.0.0.2

//PC3将收到源地址为30.0.0.3的请求，并回应。

//R1把从R2传来的目标地址为30.0.0.3的IP包转换为目的地址为192.168.0.10的IP包

实验1：静态NAT配置实

R1#show ip nat statistics

Total act translations: 2 (2 static, 0 dynamic; 0 extended)
Outside interfaces:
  Ethernet1/1
Inside interfaces：
  Ethernet1/0
…

//总的NAT活动转换数为2，其中静态转换数为2，其余类型的转换数为 0。内部接口为e1/0，外部接口为e1/1。

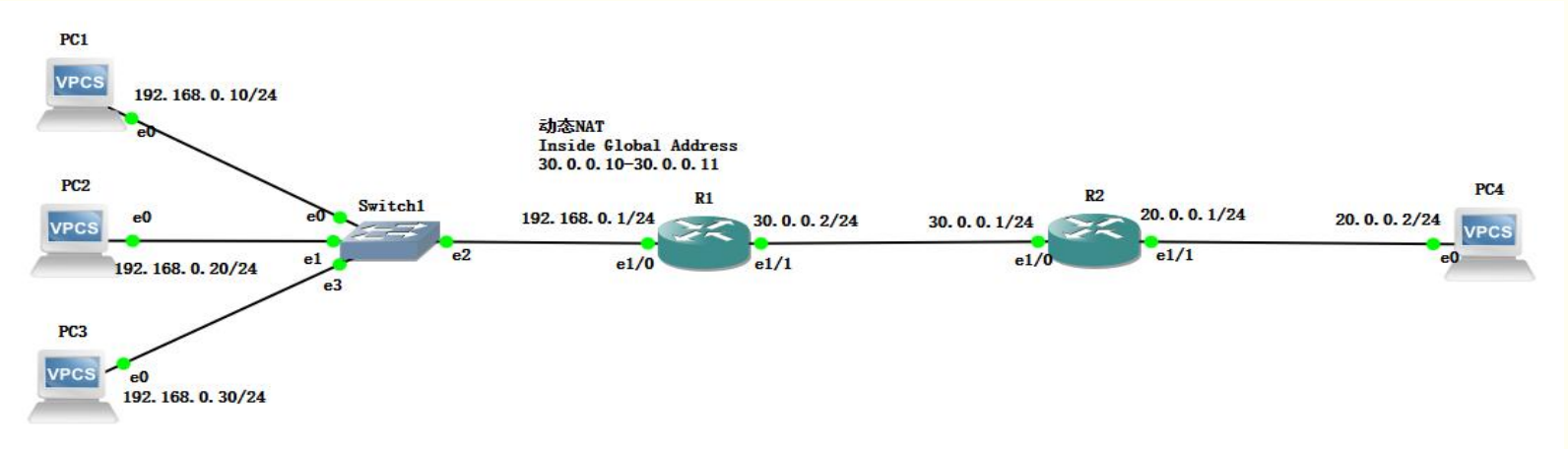
R1#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	30.0.0.3	192.168.0.10	---	---
---	30.0.0.4	192.168.0.20	---	---

主要内容

- NAT概述
- NAT配置命令
- 实验1：静态NAT配置
- **实验2：动态NAT配置**
- 实验3：NAPT配置

实验2：动态NAT配置



#interface e1/0　　#interface e1/1

#ip nat inside　　#ip nat outside

R1(config)#ip nat pool test 30.0.0.10 30.0.0.11 netmask 255.255.255.0

//定义一个名为test的NAT地址池

R1(config)#ip nat inside source list 1 pool test

//指定动态地址转换，由访问列表1定义的地址范围内的内网地址允许进行地址转换，转换后的地址是名为test的地址池中的IP地址，方式为动态转换。

R1(config)#access-list 1 permit 192.168.0.0 0.0.0.255

//定义192.168.0.0/24网段，即内网网段

实验2：动态NAT配置

- 在PC1上使用ping，用192.168.0.10作为源地址访问20.0.0.2

R1#sh ip nat translation

Pro	Inside global	Inside local	Outside local	Outside global
---	30.0.0.10	192.168.0.10	---	---

```
R1#show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
icmp 30.0.0.10:62371   192.168.0.10:62371 20.0.0.2:62371     20.0.0.2:62371
icmp 30.0.0.10:62627   192.168.0.10:62627 20.0.0.2:62627     20.0.0.2:62627
icmp 30.0.0.10:62883   192.168.0.10:62883 20.0.0.2:62883     20.0.0.2:62883
icmp 30.0.0.10:63139   192.168.0.10:63139 20.0.0.2:63139     20.0.0.2:63139
icmp 30.0.0.10:63395   192.168.0.10:63395 20.0.0.2:63395     20.0.0.2:63395
--- 30.0.0.10          192.168.0.10       ---                ---
```

- 在PC2上使用ping，用192.168.0.20作为源地址访问20.0.0.2

R1#sh ip nat translation

Pro	Inside global	Inside local	Outside local	Outside global
---	30.0.0.10	192.168.0.10	---	---
---	30.0.0.11	192.168.0.20	---	---

//可以查看到又建立起一个NAT翻译。

```
R1#show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
--- 30.0.0.10          192.168.0.10       ---                ---
icmp 30.0.0.11:53670   192.168.0.20:53670 20.0.0.2:53670     20.0.0.2:53670
icmp 30.0.0.11:53926   192.168.0.20:53926 20.0.0.2:53926     20.0.0.2:53926
icmp 30.0.0.11:54182   192.168.0.20:54182 20.0.0.2:54182     20.0.0.2:54182
icmp 30.0.0.11:54438   192.168.0.20:54438 20.0.0.2:54438     20.0.0.2:54438
icmp 30.0.0.11:54694   192.168.0.20:54694 20.0.0.2:54694     20.0.0.2:54694
--- 30.0.0.11          192.168.0.20       ---                ---
```

实验2：动态NAT配置

- 继续在PC3上使用ping，用192.168.0.30作为源地址访问外网20.0.0.2，将会观察到访问失败，同时在R1上通过debug将会观察到翻译失败。

  原因：地址池内只有两个地址，被耗尽后，余下的内网主机将无法被翻译，不能访问外网。

R1#clear ip nat translation *

//动态建立的映射的生存周期缺省为24小时，清空动态映射后，查看NAT转换信息，发现列表是空的，没有任何映射存在，从R2向地址池中的任何地址发出的ping测试都是失败的，表明从外网到内网的方向上不能进行动态NAT转换。

R1#clear ip nat translation inside 30.0.0.10 192.168.0.30

//在清除NAT翻译后，余下主机可以访问外网。

R1 (config)#ip nat translation timeout 60

//设置NAT的超时时间，单位为秒

//通过适当设置超时时间，可及时清除空闲连接，提供给有需要的内网主机。

主要内容

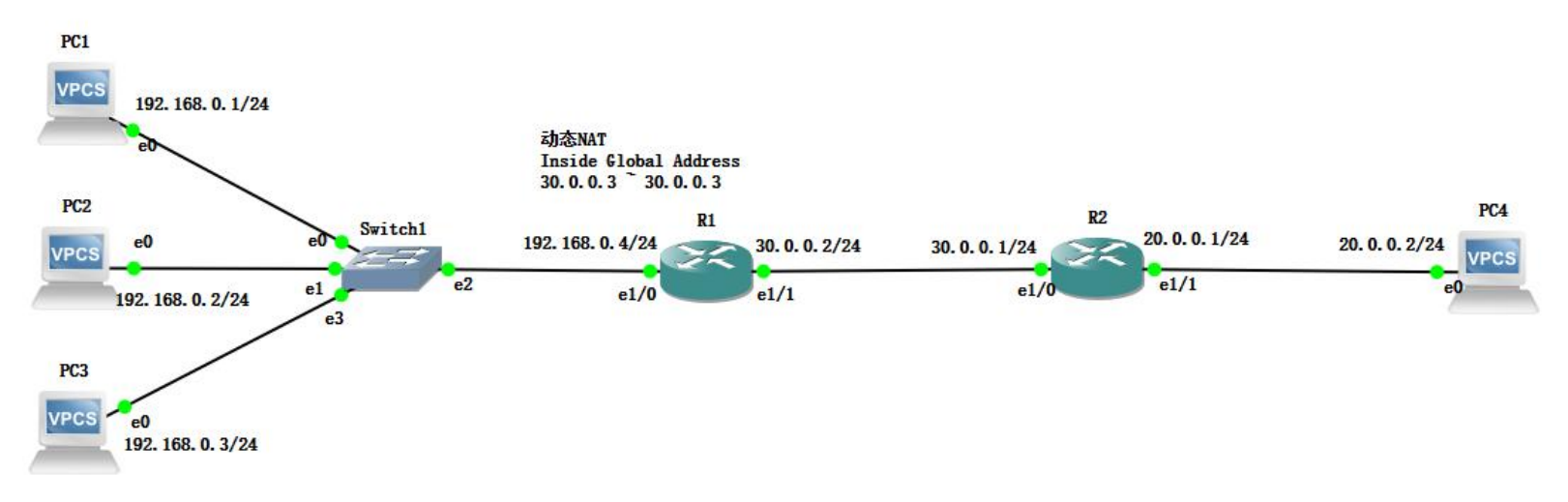
- NAT概述
- NAT配置命令
- 静态NAT配置
- 动态NAT配置
- **实验3：NAPT配置**

实验3：NAPT配置

- NAPT代表网络地址端口转换。它是一种NAT，允许专用网络中的多个设备共享单个公共IP地址，NAPT 通过使用 IP 地址和端口号的组合来执行转换。

- 内部全局地址复用（overloading inside global addresses）使用地址和端口，将多个内部地址映射到比较少的外部地址，也是所谓的PAT（Port Address Translation）
- 和内部地址翻译一样，路由器同样也负责查表和翻译内部IP地址，唯一的区别就是由于使用了复用，路由器将复用同样的内部全局IP地址

实验3：NAPT配置



R1(config)#ip nat pool test 30.0.0.3 30.0.0.3 netmask 255.0.0.0

//定义一个名为test的NAT地址池

R1(config)#ip nat inside source list 1 pool test overload

//关键字overload，启用地址复用功能。由访问列表 access-list-1定义的地址范围内的内网IP地址将被地址转换，转换后的地址是NAT地址池中的IP地址，方式为动态转换。

R2(config)#access-list 1 permit 192.168.0.0 0.0.0.255

- 在PC1上使用ping，用192.168.0.1作为源地址访问20.0.0.2

R1#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
icmp	30.0.0.3:58564	192.168.0.1:58564	20.0.0.2:56564	20.0.0.2:58564

```
R1#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 30.0.0.3:58564    192.168.0.1:58564  20.0.0.2:58564     20.0.0.2:58564
icmp 30.0.0.3:59076    192.168.0.1:59076  20.0.0.2:59076     20.0.0.2:59076
icmp 30.0.0.3:59588    192.168.0.1:59588  20.0.0.2:59588     20.0.0.2:59588
icmp 30.0.0.3:60100    192.168.0.1:60100  20.0.0.2:60100     20.0.0.2:60100
icmp 30.0.0.3:60356    192.168.0.1:60356  20.0.0.2:60356     20.0.0.2:60356
```

- 在PC1上也使用ping，用192.168.0.2作为源地址访问20.0.0.2

R1#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
icmp	30.0.0.3:20422	192.168.0.2:20422	20.0.0.2:20242	20.0.0.2:20242
icmp	30.0.0.3:30918	192.168.0.2:30918	20.0.0.2:30918	20.0.0.2:30918

```
R1#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 30.0.0.3:20422    192.168.0.1:20422  20.0.0.2:20422     20.0.0.2:20422
icmp 30.0.0.3:20934    192.168.0.1:20934  20.0.0.2:20934     20.0.0.2:20934
icmp 30.0.0.3:21190    192.168.0.1:21190  20.0.0.2:21190     20.0.0.2:21190
icmp 30.0.0.3:21446    192.168.0.1:21446  20.0.0.2:21446     20.0.0.2:21446
icmp 30.0.0.3:21702    192.168.0.1:21702  20.0.0.2:21702     20.0.0.2:21702
icmp 30.0.0.3:29894    192.168.0.1:29894  20.0.0.2:29894     20.0.0.2:29894
icmp 30.0.0.3:30150    192.168.0.1:30150  20.0.0.2:30150     20.0.0.2:30150
icmp 30.0.0.3:30406    192.168.0.1:30406  20.0.0.2:30406     20.0.0.2:30406
icmp 30.0.0.3:30662    192.168.0.2:30662  20.0.0.2:30662     20.0.0.2:30662
icmp 30.0.0.3:30918    192.168.0.2:30918  20.0.0.2:30918     20.0.0.2:30918
```

可见PC1和PC2复用了同一个Inside Global Address