红茶三杯
Vinsoney

学习 沉淀 成长 分享

NAT网络地址转换

红茶三杯 http://weibo.com/vinsoney

Latest update: 2012-08-01

Content

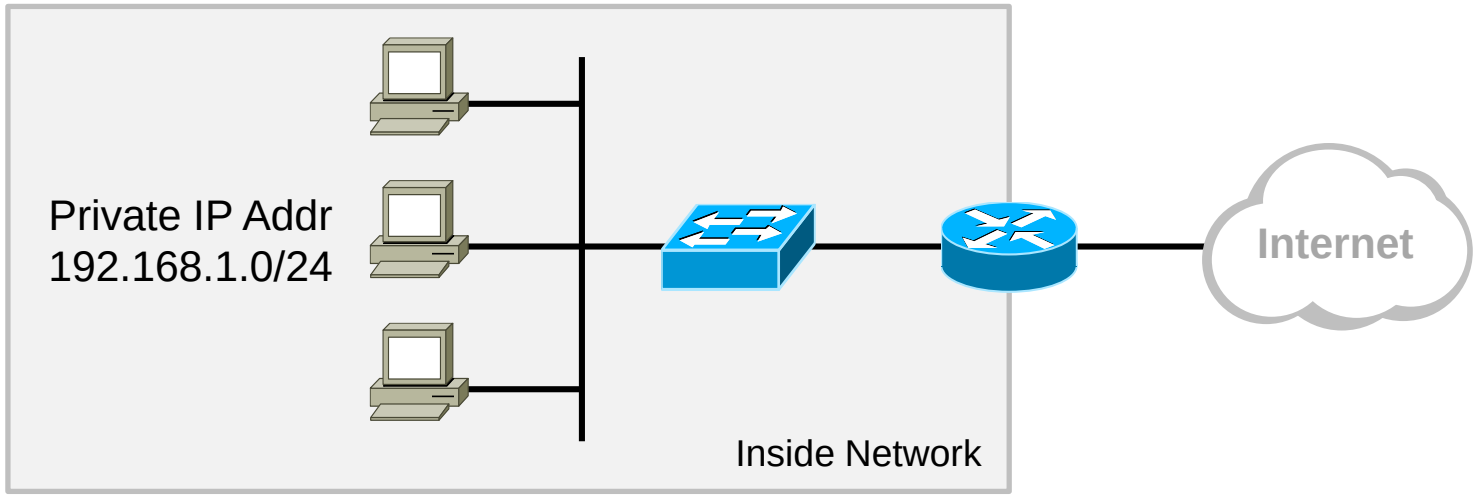
NAT概述

工作机制详解

配置及实现

NAT概述

NAT技术背景



- 私有IP地址的定义极大程度的缓解了IPv4地址紧缺的问题。
- 私有IP地址可以在本地局域网、私有网络内部随意使用，但是这些地址在公网上是不可被路由的，因此私有IP地址无法直接访问公网。
- NAT网络地址转换技术能够将数据包中的IP地址进行转换。

私有IPv4地址空间

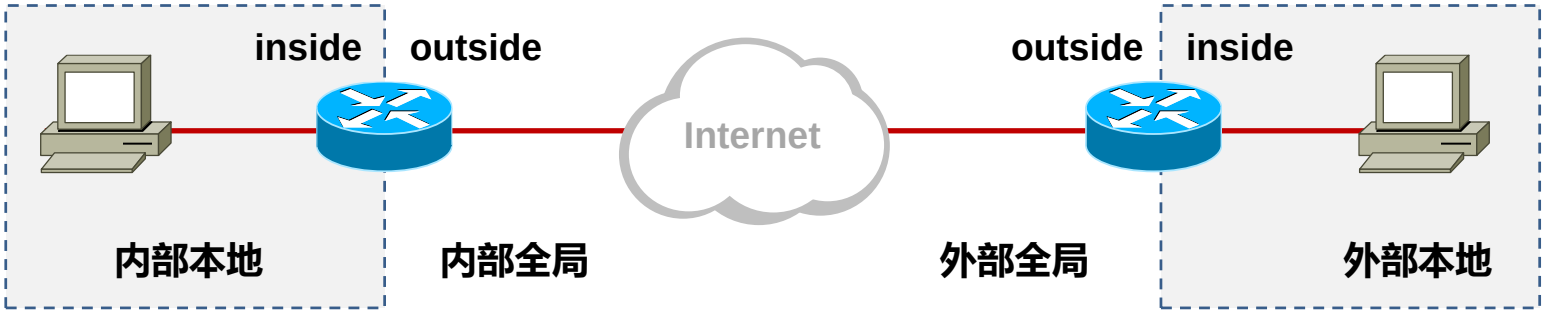
- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

NAT优缺点

优点	缺点
节省IP地址空间	增加转发延迟
解决IP地址重叠问题	丧失端到端的寻址能力
增加网络的连入Internet的弹性	某些应用不支持NAT
网络变更的时候减少IP重编址带来的麻烦	需要一定的内存空间支持动态存储NAT表项
对外隐藏内部地址，增加网络安全性	需要耗费一定CPU资源进行NAT操作 需耗费一定的内存资源存储NAT表项

NAT术语

术语	解释
内部本地	转换之前内部源地址的名字
外部本地	转换之前目标主机的名字
内部全局	转换之后内部主机的名字
外部全局	转换之后外部目标主机的名字



红茶三杯
Vinsoney

NAT工作机制详解

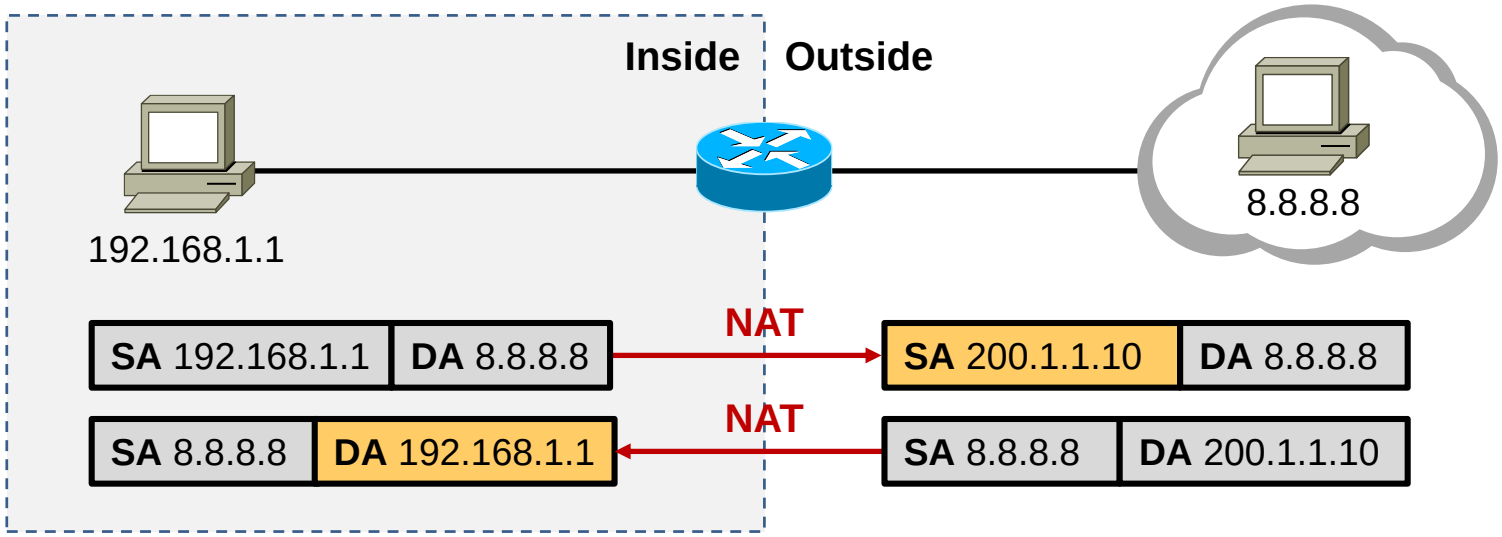
- 静态NAT
- 基于地址池的源地址转换
- PAT端口地址转换

Static NAT

- Static NAT，静态NAT，用于将内部本地地址（私有IP）与内部全局地址（公有IP）进行一对一的映射。缺点是需要每一个内部IP地址需独占一个宝贵的公网IP地址。即，如果某个合法IP地址已经被NAT静态地址转换定义，即使该地址当前没有被使用，也不能被用作其它的地址转换。而且这种方式是静态手工创建的NAT映射，可扩展性不高
- 这种方法主要用在内网中存在需要对公网提供服务的服务器的场景，类似的例子有WEB服务器、邮件服务器、FTP服务器等。
- Static NAT支持IP对IP的映射，以及端口对端口的映射。

Static NAT

SA : Source IP Address
DA : Destination IP Address

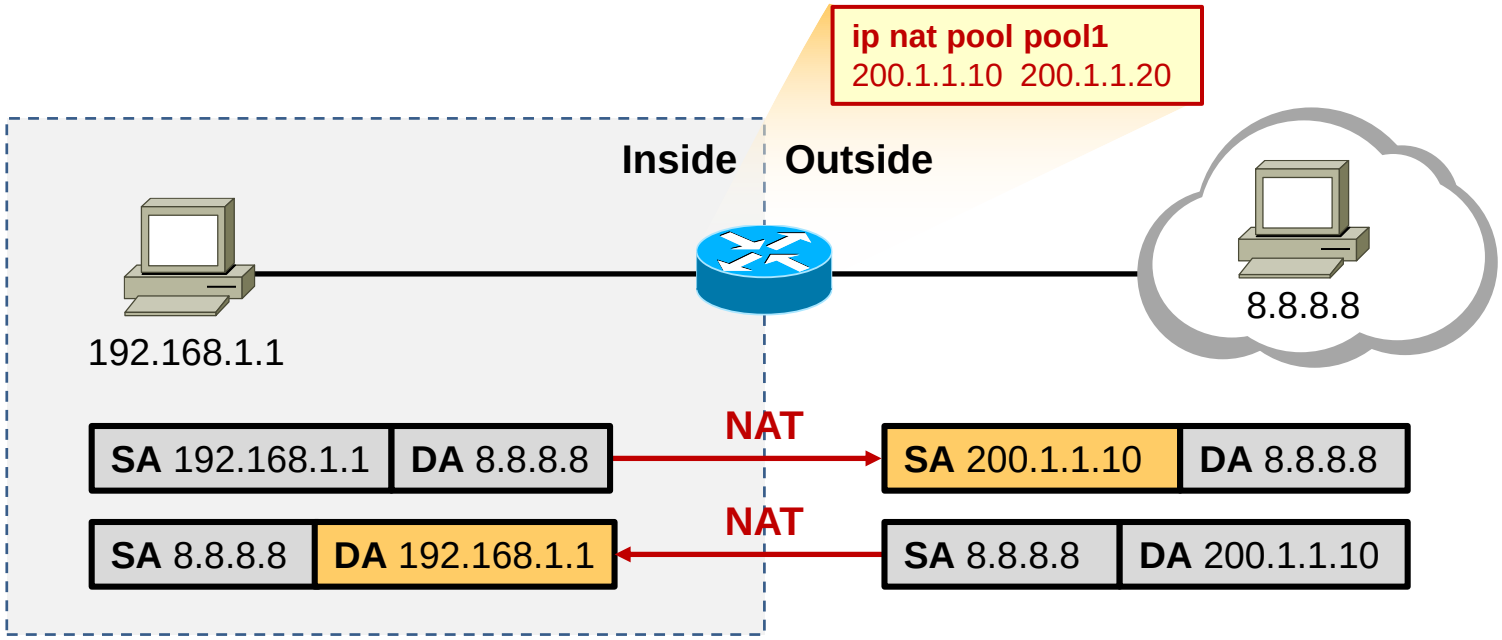


	Inside Local address	Inside Global Address
Static	192.168.1.1	200.1.1.10

基于地址池的源地址转换（一对一）

- 基于地址池的源地址转换（一对一）是一种动态NAT，其实也是一对一的映射关系。将公网地址放置在一个地址池中，在需要对外出数据包的源地址进行转换时，从地址池中取出一个公网地址供该私有地址专用，并形成NAT映射表项。
- 当已占用一个公网地址的用户在一定时间内没有数据传输时，该公网地址资源被收回到地址池中，供其他用户使用。
- 这种方式的NAT不会对数据报头部中的端口地址进行转换。

基于地址池的源地址转换（一对一）

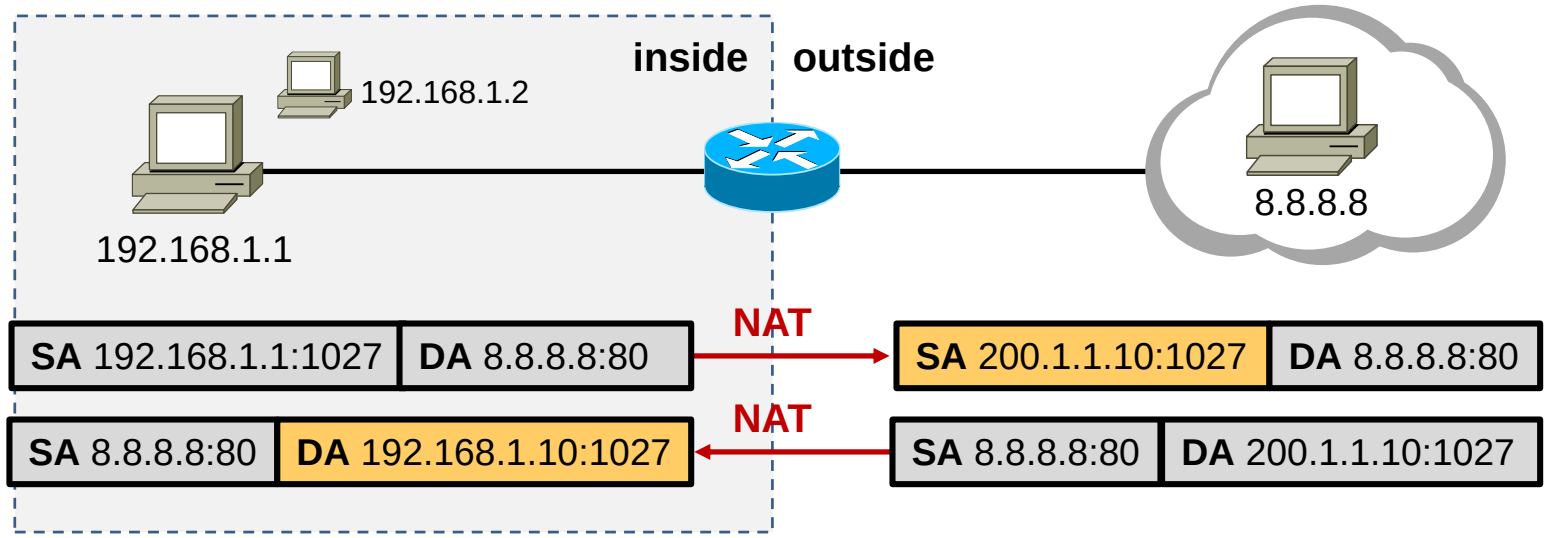


	Inside Local address	Inside Global Address
Dynamic	192.168.1.1	200.1.1.10

PAT

- 也称为端口地址转换（Port Address Translation，PAT），也即对数据包的源地址和端口均进行转换，通过这种转换，可以使多个内部本地地址同时共享同一个公网地址，通过IP+端口的方式来识别不通的源，也就是多对一的映射。
- 对于只申请到少量IP地址甚至只有一个合法IP地址却经常有很多用户同时要求上网的情况，这种转换方式非常有用。这种地址转换方式真正意义上缓解了IPv4地址紧缺的问题。在各种网络中被广泛采用。

PAT



	Inside Local address	Inside Global Address
Dynamic	192.168.1.1:1027	200.1.1.10:1027
Dynamic	192.168.1.2:1025	200.1.1.10:1025

红茶三杯
Vinsoney

NAT的配置及实现

配置静态NAT转换

- 创建NAT静态映射条目

```
Router(config)# ip nat inside source static local-ip global-ip
```

- 指定内部接口

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

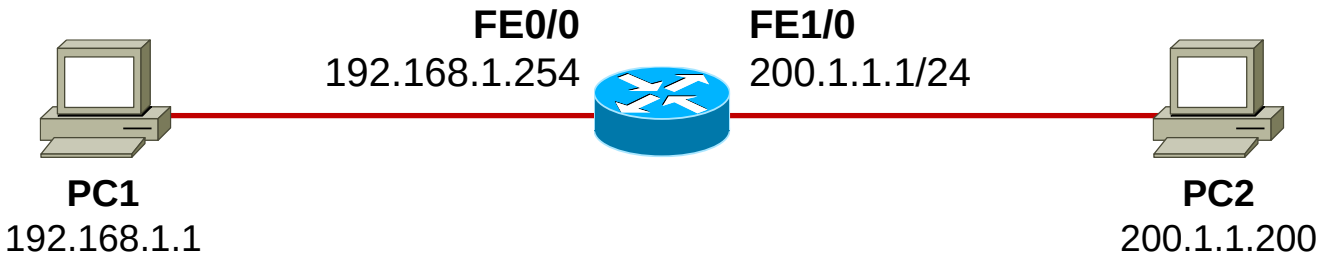
- 指定外部接口

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

- 查看nat映射

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

配置静态NAT转换（IP一对一映射）

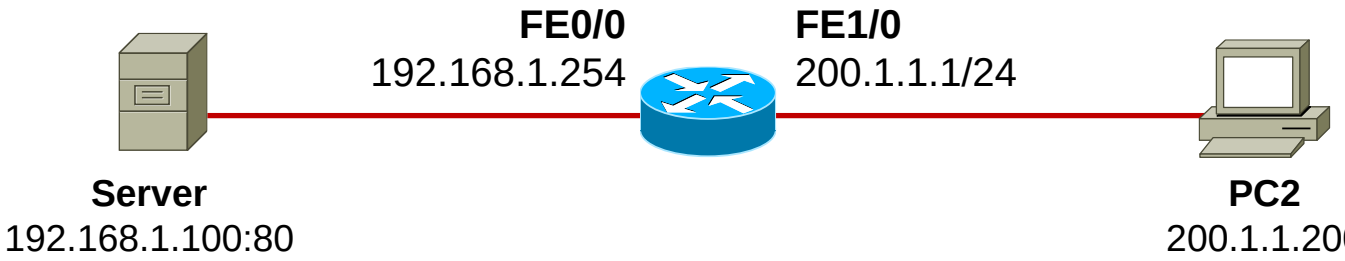



```
ip nat inside source static 192.168.1.1 200.1.1.10

interface FastEthernet 0/0
  ip nat inside
interface FastEthernet 1/0
  ip nat outside
```

```
Router# show ip nat translations
Pro  Inside global   Inside local    Outside local   Outside global
---  200.1.1.10      192.168.1.1     ---             ---
```

配置静态NAT转换（静态端口映射）




```
ip nat inside source static tcp 192.168.1.100 80  200.1.1.100 8080

interface FastEthernet 0/0
  ip nat inside
interface FastEthernet 1/0
  ip nat outside
```

```
Router# show ip nat translations
Pro   Inside global          Inside local        Outside local   Outside global
tcp   200.1.1.100:8080   192.168.1.100:80    ---                 ---
```

配置基于地址池方式的NAT（一对一）

- 创建NAT地址池

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

- 创建ACL 用于匹配允许NAT的内网地址

  Router(config-if)# **access-list** *acl-num* **permit** *source* [*source-wildcard*]

- 将ACL与NAT地址池进行关联

  Router(config-if)# **ip nat inside source list** *acl-num* **pool** *name*

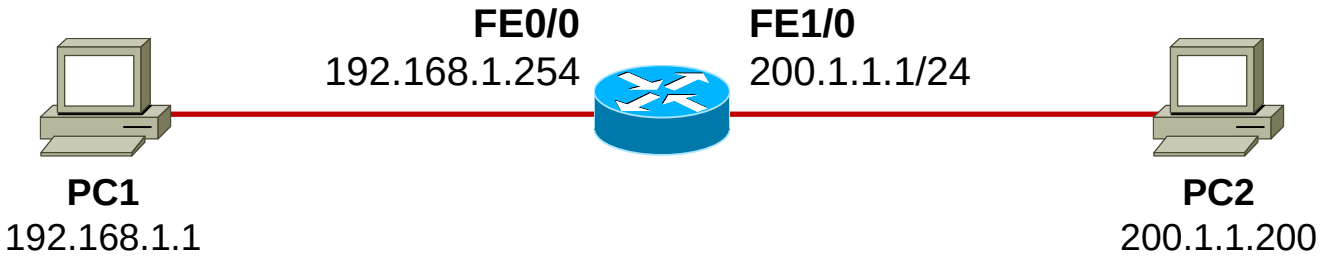
- 指定内部接口

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

- 指定外部接口

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

配置基于地址池方式的NAT（一对一）

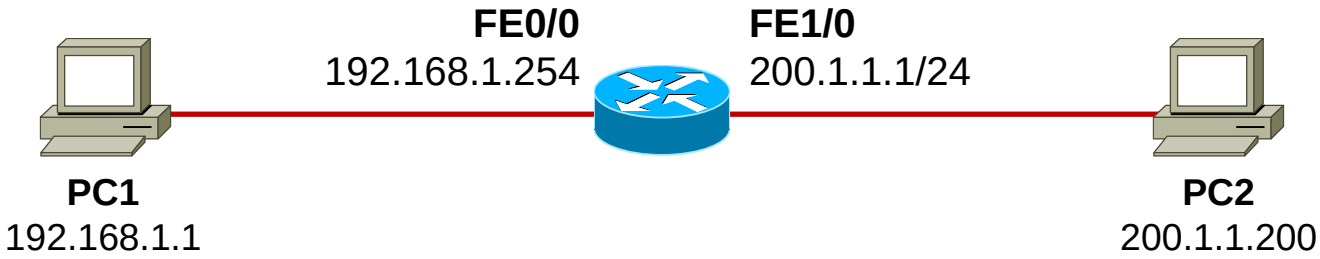



```
ip nat pool natpool 200.1.1.10 200.1.1.20 netmask 255.255.255.0

access-list 1 permit 192.168.1.0 0.0.0.255

ip nat inside source list 1 pool natpool
interface FastEthernet 0/0
  ip nat inside
interface FastEthernet 1/0
  ip nat outside
```

配置基于地址池方式的NAT（多对一）

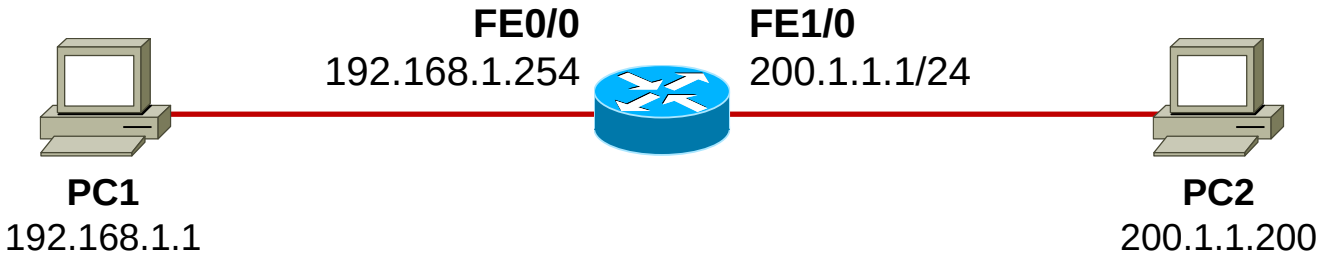



```
ip nat pool natpool 200.1.1.10 200.1.1.20 netmask 255.255.255.0

access-list 1 permit 192.168.1.0 0.0.0.255

ip nat inside source list 1 pool natpool overload
interface FastEthernet 0/0
  ip nat inside
interface FastEthernet 1/0
  ip nat outside
```

配置接口Overload




```
access-list 1 permit 192.168.1.0 0.0.0.255

ip nat inside source list 1 interface fastethernet1/0 overload

Interface FastEthernet 0/0
  ip nat inside
interface FastEthernet 1/0
  ip nat outside
```

NAT维护

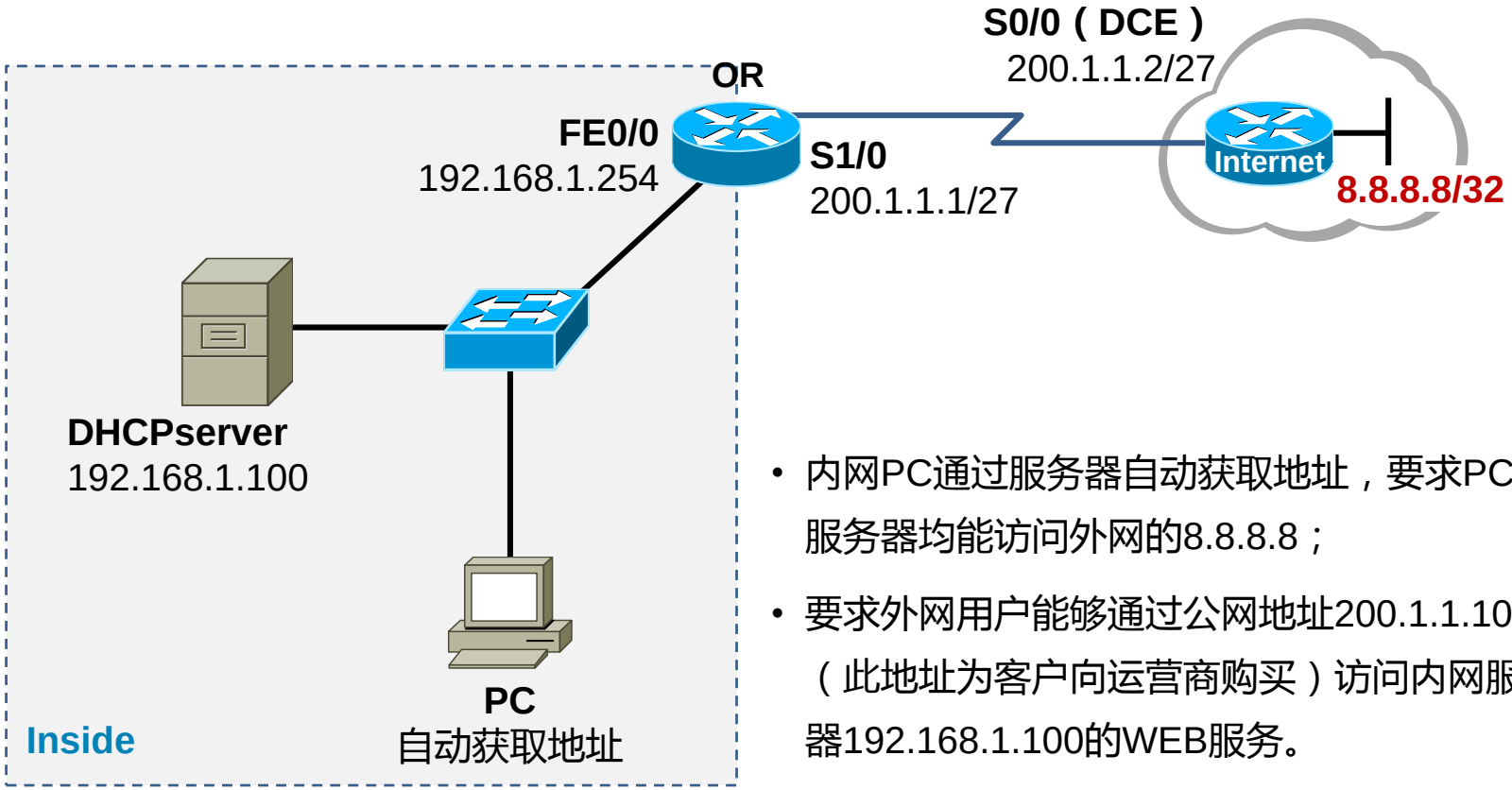
- 清楚所有动态NAT表项

```
Router# clear ip nat translation *
```

- 清楚特定的NAT表项

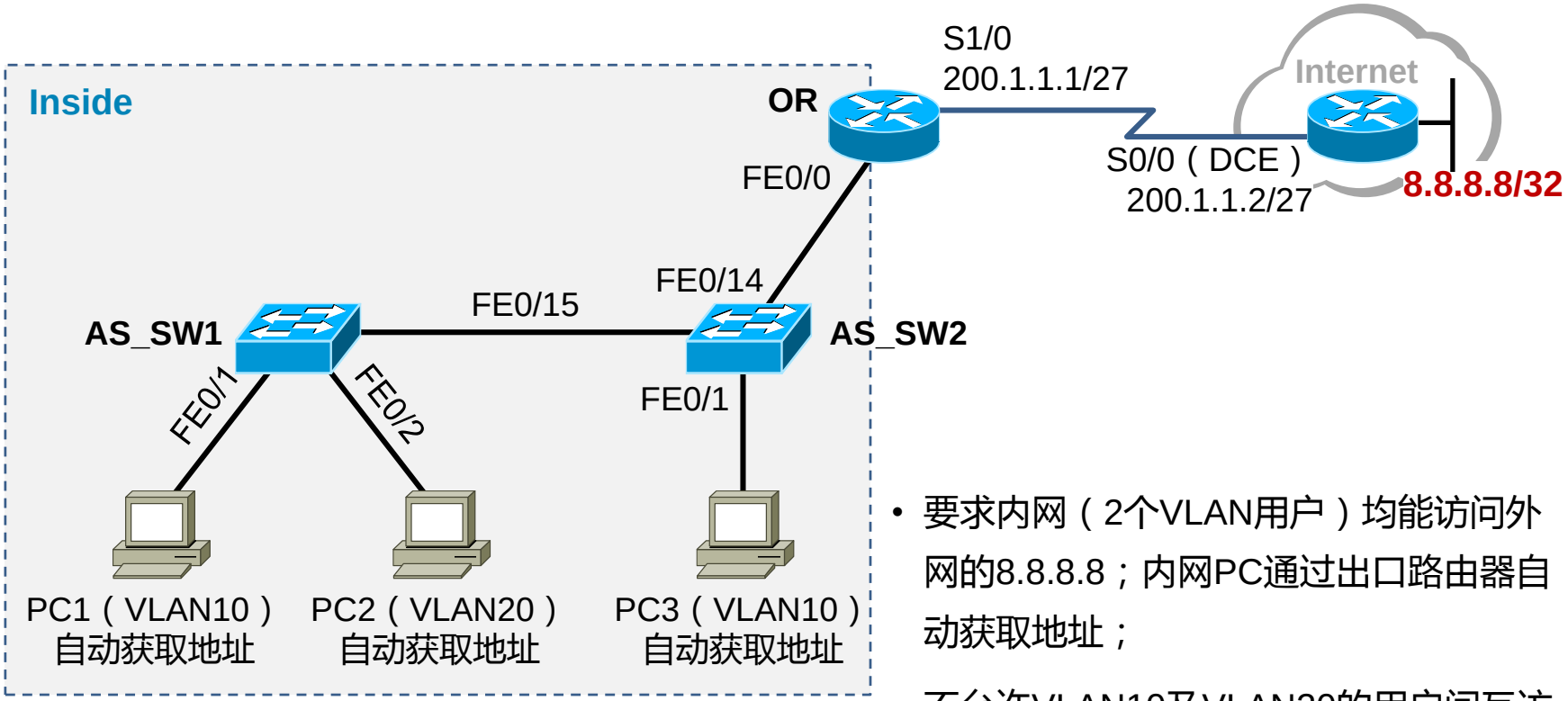
```
Router# clear ip nat translation ?
```

NAT综合小实验1



- 内网PC通过服务器自动获取地址，要求PC及服务器均能访问外网的8.8.8.8；
- 要求外网用户能够通过公网地址200.1.1.10（此地址为客户向运营商购买）访问内网服务器192.168.1.100的WEB服务。

NAT综合小实验2



- 要求内网（2个VLAN用户）均能访问外网的8.8.8.8；内网PC通过出口路由器自动获取地址；
- 不允许VLAN10及VLAN20的用户间互访。

红茶三杯
Vinsoney

学习 沉淀 成长 分享

关注@红茶三杯：weibo.com/vinsoney

Thank You