NAT的用途

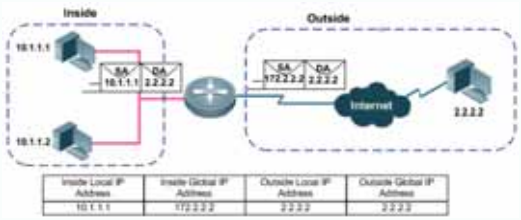
- 解决地址空间不足的问题
  - IPv4的空间已经严重不足，NAT可以大量节省公网IP
- 私有IP地址网络与公网互联
  - 私有IP网络无法直接在公网上通信，NAT技术可以将其转化为合法的公网地址使私有网络与公网实现互联
- 使用未注册的公网IP地址与公网互联
  - 内网使用的是未注册的公网IP，通过NAT技术也能正常与internet互联
- 网络改造中，避免更改地址带来的风险
  - 内网改造不需要重新更换与外网互联地址，只需更改映射关系
  - 内网改造出现地址重叠，NAT技术可以屏蔽重叠

内 容 Contents

NAT概念

- 地址空间不足带来的问题
  - 注册IP地址空间将要耗尽，而internet的规模仍在持续增长
  - 随着internet的增长，骨干互联网路由选择表中的IP路由条目也在增加，这引发了路由选择算法的扩展问题
- 网络地址转换NAT（Network Address Translation）
  - NAT是一种大型网络中节约注册IP地址数量，并简化IP寻址管理任务的机制。NAT已经标准化并在RFC1613中描述
  - 它是一个IETF(Internet Engineering Task Force, Internet工程任务组)标准，允许一个整体机构以一个公用IP地址出现在Internet上
  - 它是一种把内部私有网络地址翻译成合法公网IP地址的技术

NAT术语

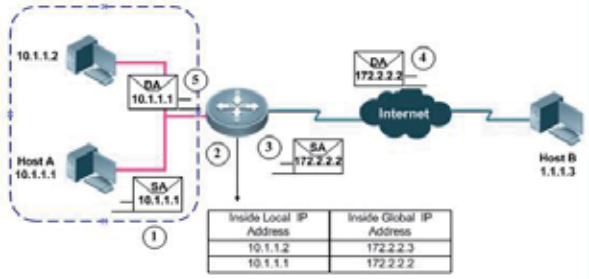


术语	定义
内部本地IP地址	分配给内部网络中的主机的IP地址，通常这种地址来自RFC 1918指定的私有地址空间。
内部全局IP地址	内部全局IP地址，对外代表一个或多个内部本地IP地址，通常这种地址来自全局惟一的地址空间，通常是ISP提供的。
外部全局IP地址	外部网络中的主机的IP地址，通常来自全局可路由的地址空间。
外部本地IP地址	在内部网络中看到的外部主机的IP地址
简单转换条目	将一个IP地址映射到另一个IP地址（通常被称为网络地址转换）的转换条目。
扩展转换条目	将一个IP地址和端口对映射到另一个IP地址和端口（通常被称为端口地址转换）对的转换条目。

NAT分类

- 根据NAT的映射方式可分为：
  - 静态NAT：手动建立一个内部IP地址到一个外部IP地址的映射关系
    - 该方式经常用于企业网的内部设备需要能够被外部网络访问到的场合
  - 动态NAT：将一个内部IP地址转换为一组外部IP地址（地址池）中的一个IP地址
    - 常用于整个公司共用多个公网IP地址访问Internet时
  - 超载（Overloading）NAT：动态NAT的一种特殊形式，利用不同端口号将多个内部IP地址转换为一个外部IP地址，也称为PAT、NAPT或端口复用NAT
    - 常用于整个公司共用1个公网IP地址访问Internet时

静态NAT的工作过程

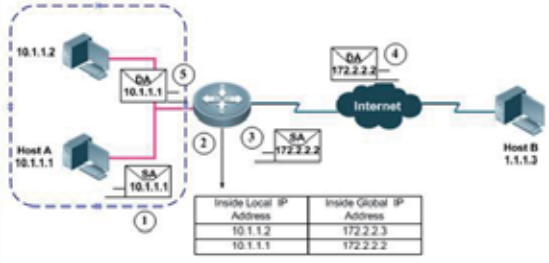


- HostA发数据包给HostB，通过路由器时，源地址10.1.1.1被转换为172.2.2.2
- HostB回复HostA，通过路由器时，目的地址172.2.2.2被转换为10.1.1.1

配置静态NAT

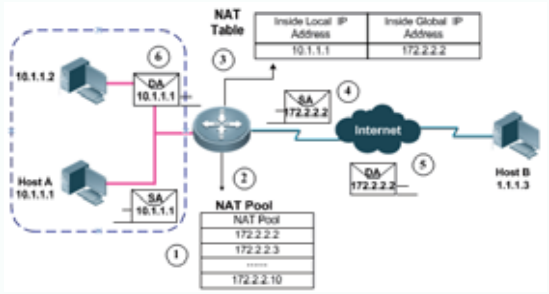
- **配置静态内部源地址转换**
  - 指定一个内部接口和一个外部接口
    - **(config-if)# ip nat** { **inside** | **outside** }
  - 配置静态转换条目
    - **(config)#ip nat inside source static** *local-ip* { **interface** *interface* | *global-ip* }
- **配置静态端口地址转换**
  - 指定一个内部接口和一个外部接口
    - **(config-if)# ip nat** { **inside** | **outside** }
  - 配置静态端口转换条目
    - **(config)# ip nat inside source static** { **tcp** | **udp** } *local-ip local-port* { **interface** *interface* | *global-ip* } *global-port [permit-side]*

配置静态NAT示例



- (config)#interface f0/0
- (config-if)#ip nat inside
- (config)#interface serial2/0
- (config-if)#ip nat outside
- (config)#ip nat inside source static 10.1.1.1 172.2.2.2

动态NAT的工作过程



- HostA发数据包给HostB，通过路由器时，源地址10.1.1.1被转换为地址池中的一个地址172.2.2.2
- HostB回复HostA，通过路由器时，目的地址172.2.2.2被转换为10.1.1.1

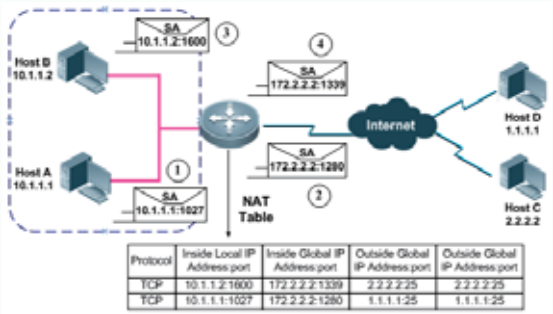
配置动态NAT

- **配置动态NAT**
  - 指定一个内部接口和一个外部接口
    - **(config-if)# ip nat** { **inside** | **outside** }
  - 定义IP访问控制列表
    - **(config)#access-list** *access-list-number* { **permit** | **deny** }
  - 定义一个地址池
    - **(config)# ip nat pool** *pool-name start-ip end-ip* { **netmask** *netmask* | **prefix-length** *prefix-length* }
  - 配置动态转换条目
    - **(config)# ip nat inside source list** *access-list-number* { **interface** *interface* | **pool** *pool-name* }

配置示例

```
Router#configure terminal
Router(config)#access-list 10 permit 10.1.1.0 0.0.0.255
Router(config)#ip nat pool ruijie 192.168.2.1 192.168.2.254 netmask 255.255.255.0
Router(config)#ip nat inside source list 10 pool ruijie
Router(config)#interface fastEthernet0/0
Router(config-if)#ip address 10.1.1.10 255.255.255.0
Router(config-if)#ip nat inside
Router(config-if)#interface Serial0/0
Router(config-if)#ip address 172.16.2.1 255.255.255.0
Router(config-if)#ip nat outside
Router(config-if)#end
```


NAPT 的工作过程



配置NAPT

- 指定一个内部接口和一个外部接口
  - **(config-if)# ip nat** { **inside** | **outside** }
- 定义IP访问控制列表
  - **(config)#access-list** *access-list-number* { **permit** | **deny** }
- 定义一个地址池
  - **(config)#ip nat pool** *pool-name start-ip end-ip* { **netmask** *netmask* | **prefix-length** *prefix-length* }
- 配置动态转换条目
  - **(config)#ip nat inside source list** *access-list-number* { **interface** *interface* | **pool** *pool-name* } **overload**

- 配置NAPT转换中，必须使用overload关键字，这样路由器才会将源端口也进行转换，已达到地址超载的目的。如果不指定**overload关键字**，路由器将执行动态NAT转换。

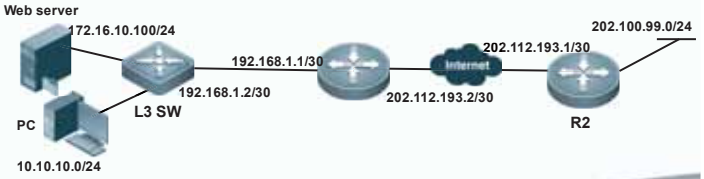
配置示例

```
Router#configure terminal
Router(config)#access-list 10 permit 10.1.1.0 0.0.0.255
Router(config)#ip nat pool ruijie 192.168.2.1 192.168.2.254 netmask 255.255.255.0
Router(config)#ip nat inside source list 10 pool ruijie overload
Router(config)#interface fastEthernet0/0
Router(config-if)#ip address 10.1.1.10 255.255.255.0
Router(config-if)#ip nat inside
Router(config-if)#interface Serial0/0
Router(config-if)#ip address 172.16.2.1 255.255.255.0
Router(config-if)#ip nat outside
Router(config-if)#end
```

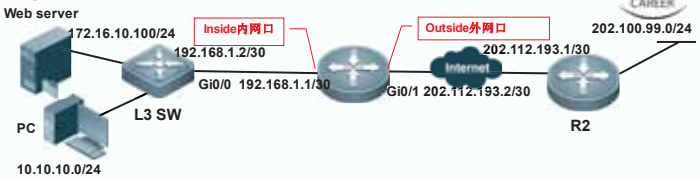

NAT配置案例

- 实现以下需求
- 1、内部主机（10.10.10.0/24）能访问公网
- 2、内部服务器私有ip：172.16.10.100，对外提供www服务。

Nat地址池pool为 202.112.192.0/24
Web server映射成202.112.194.1/24



定义接口和ACL



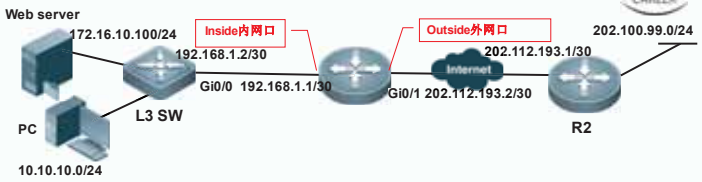
定义NAT设备的内外网口

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

定义进行NAT的ACL用户列表

```
ip access-list standard 1
 10 permit 10.10.10.0 0.0.0.255
```

定义地址池



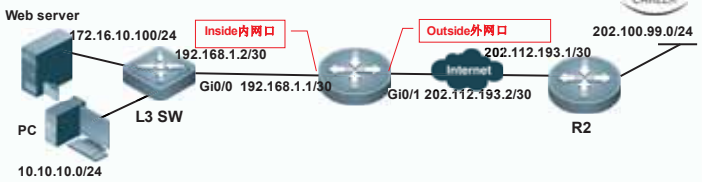
pool-name　　前缀长度

- 定义NAT地址池和服务器对外映射

ip nat pool natpool prefix-length 24
address 202.112.192.1 202.112.192.254 match interface GigabitEthernet 0/1

start-ip　　end-ip

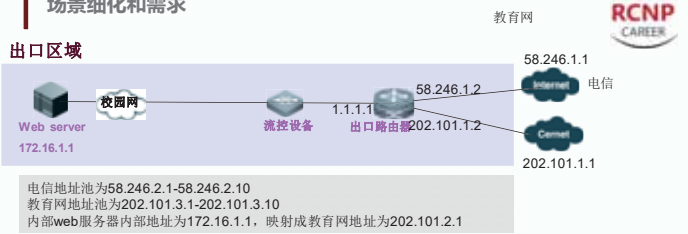
定义转换方法



- 定义转换方法及转换关联
- ip nat inside source list 1 pool natpool overload

ACL号　　pool-name

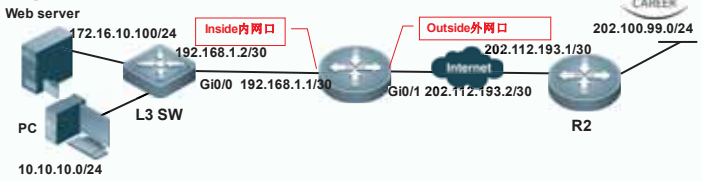
场景细化和需求



电信地址池为58.246.2.1-58.246.2.10
教育网地址池为202.101.3.1-202.101.3.10
内部web服务器内部地址为172.16.1.1，映射成教育网地址为202.101.2.1

- 场景需求：
- 1、内部宿舍区私有IP地址用户可以通过路由器访问公网，且访问电信资源走电信线路，访问教育网资源走教育网线路。
- 2、内部服务器网段172.16.0.0/16只走教育网线路，内部web服务器（172.16.1.1）对外提供web服务

定义端口映射



local-address　　global-address

ip nat inside source static tcp 172.16.10.100 80 202.112.194.1 80 permit-side

协议　　PORT　　PORT

2、出口区域的高级应用

出口区域的高级应用

需求分析

- 1、内部宿舍区私有IP地址用户可以通过路由器的两条线路访问公网，且访问电信资源走电信线路，访问教育网资源走教育网线路。
- 分析：宿舍区私有IP地址用户通过路由器的两条线路都可以访问公网，需要在路由器上配置NAT，且电信和教育网都需要配置NAT，配置两个地址池，并匹配两个接口。
- 2、内部服务器网段172.16.0.0/16只走教育网线路，内部web服务器（172.16.1.1）对外提供web服务
- 分析：
- 1、要求内部服务器网段只走教育网线路，传统的基于目的路由的模式不能满足此需要，需要配置策略路由，匹配源地址来进行路由转发。
- 2、要求内部web服务器对外提供web服务，而内部web服务器是私网地址，因此需要做基于端口的NAT静态映射。

出口区域的高级应用

双出口路由配置

- 内网到外网访问的数据流走向：

导入电信和教育网路由表。
最新的路由信息可以从网络上获取，通过文本编辑器批量修改为ip route x.x.x.x x.x.x.x格式，导入设备。

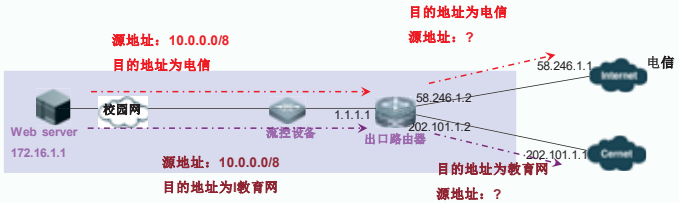
同时配置两条等价的缺省路由，不匹配电信和教育网地址库的，匹配两条等价缺省路由，自动负载到两条线路

```
ip route 0.0.0.0 0.0.0.0 58.246.1.1
ip route 0.0.0.0 0.0.0.0 202.101.1.1
```


出口区域的高级应用

双出口NAT配置

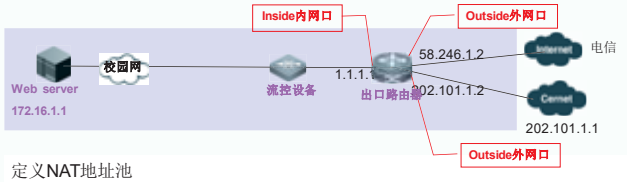
配置完了双出口的路由，我们下面来分析在NAT方面面临什么问题



从上图中数据流向可以看出，源地址为宿舍区私用地址10.0.0.0/8的网段，访问电信资源从路由器出去时需要做NAT，匹配电信的地址池；访问教育网资源从路由器出去时也需要做NAT，匹配教育网的地址池，否则私网地址在公网上无法路由，无法访问互联网。
因此，我们需要配置两个地址池，并对应的匹配两个接口。

出口区域的高级应用

双出口NAT配置

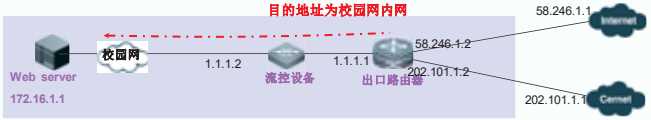


定义NAT地址池

```
ip nat pool sushe prefix-length 24
address 202.101.3.1 202.101.3.1 match interface gigabitEthernet 0/2
address 58.246.2.1 58.246.2.10 match interface gigabitEthernet 0/1
```


出口区域的高级应用

双出口路由配置
到内网的回指路由：




```
ip route 10.0.0.0 255.0.0.0 1.1.1.2
ip route 172.16.0.0 255.255.0.0 1.1.1.2
ip route 192.168.0.0 255.255.0.0 1.1.1.2
```


出口区域的高级应用

双出口NAT配置

定义NAT设备的内外口

```
interface GigabitEthernet 0/0
ip nat inside
interface GigabitEthernet 0/1
 ip nat outside
interface GigabitEthernet 0/2
 ip nat outside
```


出口区域的高级应用

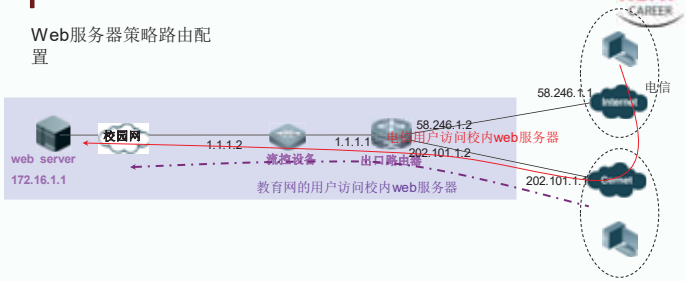
双出口NAT配置

内部web服务器（172.16.1.1）对外提供web服务


```
ip nat inside source static tcp 172.16.1.1 80 202.101.2.1 80
```

出口区域的高级应用

Web服务器策略路由配置



从上图中可以看出：
若是教育网的用户发起到校内web服务器的访问，数据从web服务器返回，到达路由器的时候，路由器查找路由表，发现目的地址是教育网，从而从教育网线路出去，由于web服务器在教育网线路上做了NAT静态映射，因此数据可以正常返回，没有问题。

出口区域的高级应用

本例中的服务器段策略路由配置

定义重分布路由图

route-map-name　　sequence

```
NPEconfig)# route-map server permit 10
```

定义路由图每个策略的匹配规则或条件

```
ip access-list standard 10
 10 permit 172.16.0.0 0.0.255.255
```

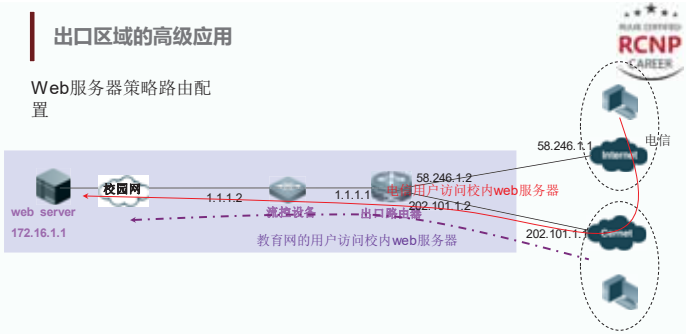

出口区域的高级应用

回顾和提问

1、为什么要导入电信和教育网路由表？
2、什么情况下需要策略路由？同普通目的路由有何本质区别？
3、双出口NAT需要注意些什么？

出口区域的高级应用

Web服务器策略路由配置



若是电信用户发起到校内web服务器的访问，因为web服务器映射出去的是教育网的，因此进来的数据会先绕到教育网线路，然后再从路由器进来，到达web服务器，数据从web服务器返回，到达路由器的时候，路由器查找路由表，发现目的地址是电信用户，应该从电信线路出去，但web服务器未在电信线路上做NAT静态映射，因此数据无法返回到电信用户。
因此我们需要一种策略，来让web服务器的数据强制走教育网线路，这个策略就是---**策略路由**

出口区域的高级应用

本例中的服务器段策略路由配置

定义满足匹配规则后，路由器对符合规则的数据包进行IP优先值和下一跳的设置

access-list-number

```
Ruijieconfig)# route-map server permit 10
Ruijie(config-route-map)# match ip address 10
Ruijie(config-route-map)# set ip  next-hop 202.101.1.1
```

ip-address

在指定接口中应用路由图

```
interface GigabitEthernet 0/0
 ip policy route-map server
```


Ruijie Networks Certification Center
Addr: 北京海淀区复兴路29号中意鹏奥大厦东塔A座11层 邮编：100036
university.ruijie.com.cn