به نام خدا

دانشگاه تهران

پردیس فارابی

دانشکده مهندسی

گروه مهندسی کامپیوتر

دستور کار

آزمایشگاه شبکه‌های کامپیوتری

شماره

۱۳

آشنایی با NAT

Introduction to NAT
(Network Address Translation)

آدرس‌ها به دو دسته‌ی public و private دسته‌بندی شده‌اند. آدرس‌های public آدرس‌هایی هستند که در اینترنت قابلیت route شدن دارند، به عبارتی با آدرس‌های private نمی‌توان به اینترنت متصل شد.

NAT یک تکنولوژی است که با استفاده از آن آدرس‌های private می‌توانند به اینترنت دسترسی داشته باشند، زیرا می‌تواند source IP را عوض کند و source IP، private را می‌تواند به آدرس public ترجمه کند.

- Inside local: آدرس NAT نشده داخل سازمان است.
- Inside global: آدرس NAT شده داخل سازمان است.
- Outside local: آدرس سروری است که می‌خواهیم به آن مراجعه کنیم: مانند facebook, google, …
- Outside global: ممکن است خود سرور دارای NAT سروری باشد که این همان آدرس است.

NAT دارای ۳ مدل است:

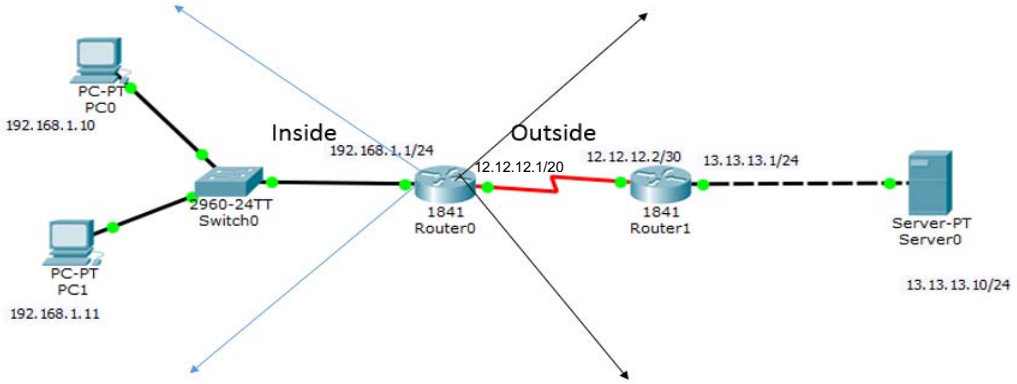
- Static NAT
- Dynamic NAT
- PAT

Static NAT

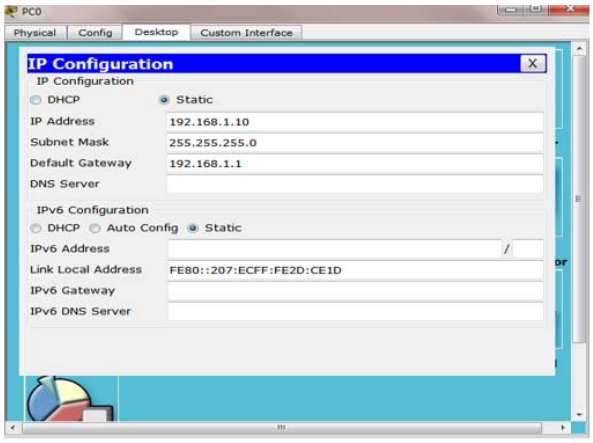
یک نگاشت یک به یک، برای آدرس‌های ما ایجاد می‌نماید. در واقع یک آدرس private را به یک آدرس public نگاشت می‌دهد. به ازای هر یک آدرس private یک آدرس public نیاز داریم.

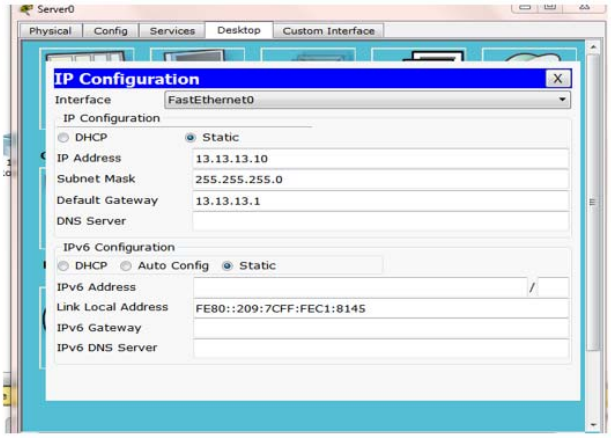
روش راه‌اندازی Static NAT:

می‌خواهیم با استفاده از سناریوی زیر به مفهوم static NAT بپردازیم:

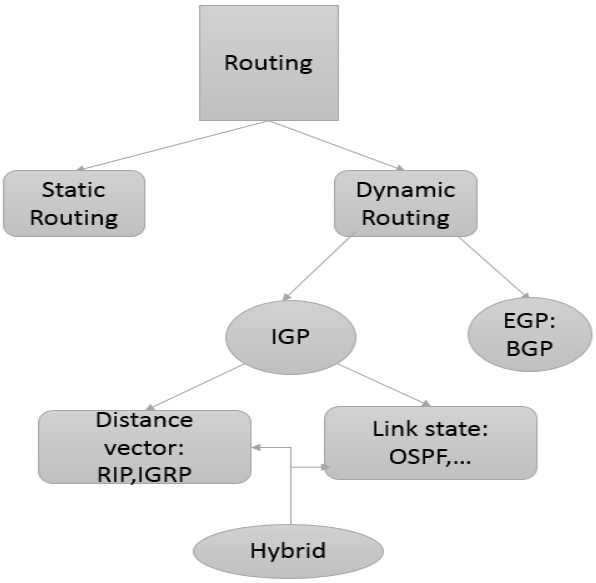


ابتدا همان‌طور که در شکل مشخص است به کامپیوترها و سرور موجود IPهای ذکر شده و gateway را تخصیص می‌دهیم:





می‌دانیم که روترها عملیات مسیریابی را با استفاده از جدولی به نام routing table انجام می‌دهند، این جدول به دو صورت استاتیک و داینامیک پر می‌شود .



روترها در جدول خود شبکه‌هایی که مستقیماً به خود متصل هستند را می‌شناسند و برایشان در جدول مسیری دارند، اما هنگامی که برای روتر بسته‌ای ارسال شود که روتر مقصد آن را بلد نباشد، بسته drop می‌شود (فرض کنید در شبکه‌ای یک کامپیوتر می‌خواهد google.com را باز کند، وقتی بسته به روتر شبکه می‌رسد چون نمی‌داند google.com کجاست آن را drop می‌کند: Destination host unreachable)، برای حل این مشکل یک راه این است که آدرس همه‌ی وب سایت‌ها و مسیرها را در static route به روتر بدهیم (چند میلیون خط) و راه دیگر این است که هر چه را بلد نیست به روتر بعدی بفرستد که این همان default route است.

```
Router(config-if)#ip route 0.0.0.0 0.0.0.0  “next hop IP”
```

بدین معنی که «هر IP با هر subnetmask را بفرست به روتر بعدی».

در هر دو روتر :روتر را خاموش نموده و یک ماژول سریال به آن اضافه می‌کنیم (WIC-2T).

با استفاده از کابل DCE دو روتر را به هم متصل می‌کنیم.

بر روی روتر اول:

```
Router(config)#interface fastethernet 0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#exit
Router(config)#interface serial 0/1/0
Router(config-if)#no shutdown
Router(config-if)#ip address 12.12.12.1 255.255.255.252
Router(config-if)#exit

Router(config)#ip route 0.0.0.0 0.0.0.0 12.12.12.2
```

برروی روتر دوم:

```
Router(config)#interface fastethernet 0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 13.13.13.1 255.255.255.0
Router(config-if)#exit
Router(config)#interface serial 0/1/0
Router(config-if)#no shutdown
Router(config-if)#ip address 12.12.12.2 255.255.255.252
```

(هیچ روتی بر روی روتر نوشته نشد و فقط دو تا connected خودش است و می‌شناسد.)

```
Router#show ip route
```

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     12.0.0.0/30 is subnetted, 1 subnets
C       12.12.12.0 is directly connected, Serial0/1/0
     13.0.0.0/24 is subnetted, 1 subnets
C       13.13.13.0 is directly connected, FastEthernet0/0
Router#
```

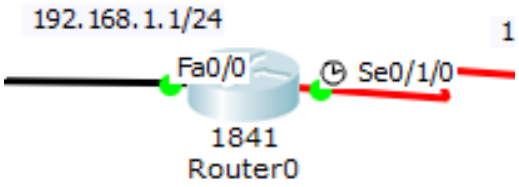
حال از روتر اول show running-config را اجرا می‌کنیم و تغییرات را ملاحظه می‌کنیم.

از کامپیوتر با آدرس IP، 192.168.1.10، سرور را ping می‌کنیم. خواهیم دید که پینگ برقرار نیست.

```
ping 13.13.13.10
```

که به دلیل همان آدرس‌های public و private است. حال بر روی روتر اول رفته و تنظیمات NAT را انجام می‌دهیم.

گام اول: مشخص نمودن inside و outside



اینترفیس داخلی را با دستور زیر مشخص می‌کنیم:

```
Router(config)#interface fastethernet 0/0
Router(config-if)#ip nat inside

Router(config)#interface serial 0/1/0
Router(config-if)#ip nat outside
Router(config-if)#exit
```

گام دوم: ساخت NAT table

باید در استاتیک یک نگاشت یک به یک انجام بدهیم و به‌عبارتی جدول NAT را بسازیم:

```
Router(config)#ip nat inside source static 192.168.1.10 12.12.12.1
```

حال مجدداً ping می‌کنیم. خواهیم دید که این بار برقرار است:

```
Pinging 13.13.13.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 13.13.13.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 13.13.13.10

Pinging 13.13.13.10 with 32 bytes of data:

Reply from 13.13.13.10: bytes=32 time=41ms TTL=126
Reply from 13.13.13.10: bytes=32 time=2ms TTL=126
Reply from 13.13.13.10: bytes=32 time=11ms TTL=126
Reply from 13.13.13.10: bytes=32 time=2ms TTL=126

Ping statistics for 13.13.13.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 41ms, Average = 14ms
```

Dynamic NAT

در همان سناریو می‌خواهیم این بار به صورت Dynamic عملیات NAT را انجام دهیم. توجه کنید که inside و outside برای هر سه روش یکسان است و لزومی به واردکردن مجدد نیست:

مراحل:

۱) inside و outside را مشخص می‌کنیم.

ابتدا با دستور زیر Static NAT را برمی‌داریم:

```
Router(config)# no ip nat inside source static 192.168.1.10 12.12.12.1
```

۲) برای روتر رنج IPها را برای public و private مشخص می‌کنیم.
۳) برای private IP یک ACL می‌نویسیم.

برای آدرس داینامیک می‌خواهیم یک محدوده در نظر بگیریم. با ACL این کار را انجام می‌دهیم.

✍ **نکته**: Access Control List (ACL) در روترهای سیسکو برای امنیت و فیلتر کردن استفاده می‌شود.

در ACL از wildcard mask استفاده می‌شود که نحوه‌ی به‌دست آوردن آن به طور خلاصه کم‌کردن 255.255.255.255 از الگوی Subnet Mask است.

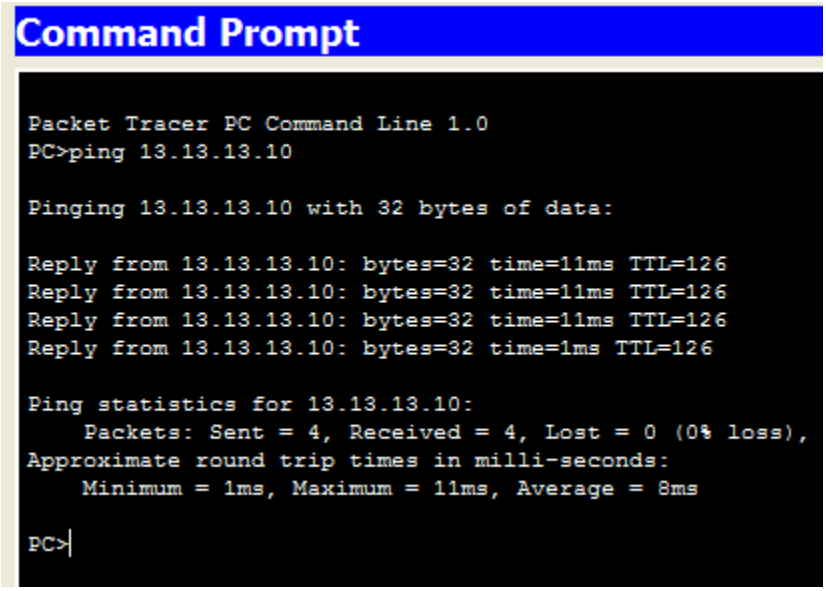
```
Router(config)#access-list ACl-num permit Net ID Wildcard mask
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

۴) در روتر یک pool از public IPها تعریف می‌کنیم.

حال یک access-list داریم که اینترفیس‌های مجاز و داخلی را شامل می‌شود و هم یک pool که شامل محدوده‌ی آدرس‌هایی است که NAT می‌شوند.

```
Router(config)#ip nat pool test 12.12.12.1 12.12.12.10 netmask 255.255.255.0
Router(config)#ip nat inside source list 1 pool test
```

توجه کنید که در این سناریو به علت این‌که ما تنها یک آدرس public داریم تنها یک کامپیوتر به طور همزمان می‌تواند عملیات NAT را انجام دهد و ما تنها از یک کامپیوتر می‌توانیم تست بگیریم.



از کامپیوتر دوم سرور را پینگ می‌کنیم. داینامیک نگاشت یک به یک است

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

PAT

حال در همان سناریور حالت داینامیک را برمی‌داریم تا با PAT تست کنیم.

```
Router(config)#no ip nat inside source list 1 pool test
Router(config)#ip nat inside source list 1 pool test overload
```

و یا

```
Router(config)#ip nat inside source list 1 interface serial 0/1/0 overload
```

از دستور show ip nat translations می‌توان برای گزارش‌گیری از عملیات NAT استفاده کرد:

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 12.12.12.1:10     192.168.1.11:10    13.13.13.10:10     13.13.13.10:10
icmp 12.12.12.1:11     192.168.1.11:11    13.13.13.10:11     13.13.13.10:11
icmp 12.12.12.1:12     192.168.1.11:12    13.13.13.10:12     13.13.13.10:12
icmp 12.12.12.1:13     192.168.1.10:13    13.13.13.10:13     13.13.13.10:13
icmp 12.12.12.1:14     192.168.1.10:14    13.13.13.10:14     13.13.13.10:14
icmp 12.12.12.1:15     192.168.1.10:15    13.13.13.10:15     13.13.13.10:15
icmp 12.12.12.1:16     192.168.1.10:16    13.13.13.10:16     13.13.13.10:16
icmp 12.12.12.1:9      192.168.1.11:9     13.13.13.10:9      13.13.13.10:9

Router#
```

از هر دو PC، سرور را ping کنید. خواهیم دید که امکان‌پذیر است و ping برقرار خواهد بود.