سیسکو به پارسی

آشنایی با NAT

نوشته:
شفق زندی

سایت سیسکو به پارسی http://blog.shafagh.com/persian
انجمن سیسکو به پارسی http://forum.shafagh.com

یک NAT ساده

برای اینکه با اینترنت بصورت مستقیم Packet رد و بدل کنیم به یک Public IP نیاز داریم (در ایران بنام Valid IP معروف است.) از آنجا که آدرس های IP در اینترنت رو به اتمام است (IP نسخه ۴) پس در بسیاری از موارد تعداد کاربر یک شبکه از تعداد IP های Public بیشتر شده و باید از NAT استفاده کرد.

بواسطه NAT میتوان از تنها یک Public IP اختصاص داده شده به روتر جهت اتصال کاربران به اینترنت استفاده کرد. در واقع روتر از سمتی به اینترنت وصل است و از سمت دیگر به شبکه کاربران، پس درخواست های کاربران را دریافت و آدرس فرستنده را در زمان ارسال به اینترنت با آدرس Public خود عوض کرده و در زمان دریافت جواب آدرس مقصد را به آدرس کاربر تغییر میدهد. کاربر از وقوع این پروسه بی خبر بوده و تنها در روتر نیاز به انجام تنظیمات وجود دارد. (Transparent to user)

NAT یا Network Address Translation استفاده های گوناگونی دارد و در امنیت شبکه Firewall ها از آن بهره میبرند. آدرس های فرستنده و یا گیرنده را به صورت Automatic از درون یک pool از آدرس های اختصاصی یا بصورت استاتیک میتوان ترجمه کرد.

Cisco in Persian

در مثال زیر بسته های ارسالی از FastEthernet0/1 به پورت متصل به اینترنت (FastEthernet0/0) ارسال و NAT میشوند:

۱. ابتدا IP Range داخلی که اجازه NAT شدن دارند را مشخص میکنیم:

```
Router(config)# access-list 1 permit 192.168.100.0 0.0.0.255
```

۲. آدرس FastEthernet0/1 را تنظیم و NAT را برای شبکه داخلی آماده میکنیم:

```
Router(config)# interface Ethernet0/1
Router(config-if)# ip address 192.168.100.1 255.255.255.0
Router(config-if)# ip nat inside
```

۳. آدرس FastEthernet0/0 را تنظیم و NAT را جهت خروج از این شبکه آماده میکنیم:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 123.234.0.2 255.255.0.0
Router(config-if)# ip nat outside
```

۴. سپس توسط دستور NAT آن Range را به آدرس FastEthernet0/0، ترجمه میکنیم:

```
Router(config)# ip nat inside source list 1 interface Ethernet0/0
overload
```

حال تنظیمات را مرور میکنیم:

```
interface FastEthernet0/0
 ip address 123.234.0.2 255.255.0.0
 ip nat outside
!
interface FastEthernet0/1
 ip address 192.168.100.1 255.255.255.0
 ip nat inside
!
ip route 0.0.0.0 0.0.0.0 123.234.0.1
!
!
ip nat inside source list 1 interface FastEthernet0/0 overload
!
access-list 1 permit 192.168.100.0 0.0.0.255
```

برای دیدن عملکرد NAT و ترجمه انجام شده (یا در حال انجام) از دستور زیر استفاده میکنیم:

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

برای پاک کردن NAT Table و از سرگیری ترجمه IP ها از دستور زیر استفاده میکنیم:

```
Router# clear ip nat translations *
```

Cisco in Persian

NAT on a Stick

خوب، تنظیم کردن NAT که بسیار ساده بود: یک Interface برای inside، دیگری برای outside و یک دستور IP Nat برای ترجمه بسته های داخل به خارج شبکه و برعکس آن.

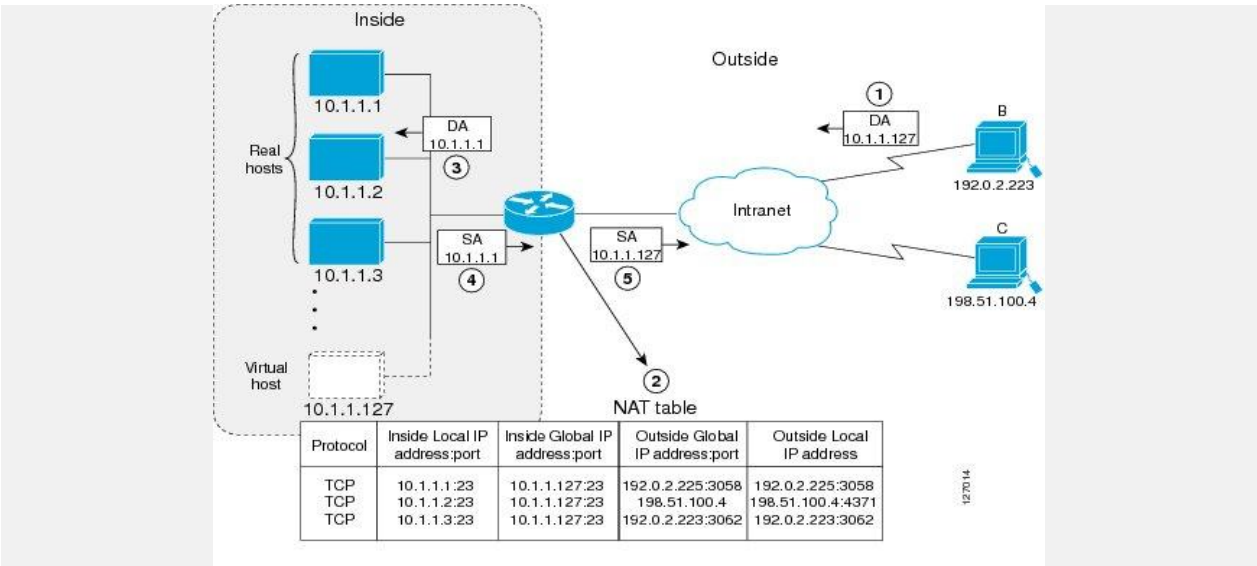
حال اگر یک Interface داشتیم چه کنیم؟ به این راه حل NAT on Stick میگوییم:

```
!
route-map NatTest permit 10
 match ip address 1
 set interface loopback0
!
interface FastEthernet 0/0
 ip address 123.234.0.2 255.255.255.0
 ip address 192.168.100.1 255.255.255.0 secondary
 ip nat outside
 ip policy route-map NatTest
!
interface Loopback0
 ip nat inside
!
ip nat inside source list 1 interface FastEthernet0/0 overload
!
access-list 1 permit 192.168.100.0 0.0.0.255
!
```

Cisco in Persian

Load-Balancing NAT

در این مثال سعی داریم به Destination NAT بپردازیم، در این روش بسته های ورودی از اینترنت، درون شبکه بین چند سرور Load-Balance میشوند. یعنی بار ورودی بین چند سرور پخش میشود. به عبارتی دیگر، درخواست های ورودی از اینترنت به یک Public IP یاValid-IP باید برای تقسیم بار بین چند سرور بالانس شوند.



NAT Process

Cisco in Persian

ابتدا لیست سرورهای داخلی را تعریف میکنیم:

```
ip nat pool LOCALSRV 192.168.1.3 192.168.1.6 prefix-length 24 type rotary
```

سپس لیست سرور مجازی همراه با آدرس Public را تنظیم میکنیم:

```
access-list 100 permit tcp any host 217.218.0.1 eq www
access-list 100 permit tcp any host 217.218.0.1 eq 443
ip nat inside destination list 100 pool LOCALSRV
```

تنظیم Interface ها بسادگی زیر:

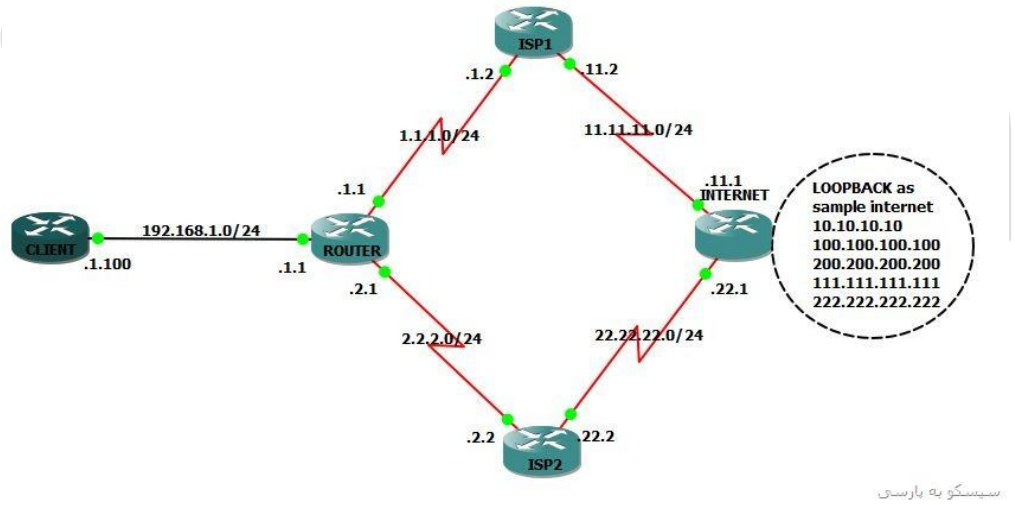
```
interface serial 0/0
ip nat outside
!
interface gigabitethernet 0/0
ip nat inside
```

Internet Load-Balancing

فرض کنیم دو اتصال به اینترنت داریم (دو ارتباط ADSL به دو سرویس دهنده مختلف) و بخواهیم هر دو را به یک روتر متصل کنیم. برای تقسیم بار بین این دو سرویس دهنده از چه روش هایی میتوان استفاده کرد؟ (ترکیب دو اینترنت متفاوت روی روتر)

با توجه به اینکه Public IP در اینترنت رو به اتمام است (آخرین Allocation های IPv4 اخیرا انجام شد) و بیش از نیمی از IP های Allocate شده در آمریکا پخش شدند، در دیگر کشور ها فراهم کردم یک آدرس Public IP ممکن است دشوار یا گران باشد و از طرفی دانش یا امکانات لازم برای برقراری BGP و پیاده سازی Multi Homing وجود نداشته باشد.

در صورتیکه آدرس اینترنتProvider Independent از RIR دریافت کرده باشید میتوانید از BGP با سناریوهای مختلف از چند سرویس دهنده با Policy های متفاوت استفاده کنید. اما در صورتیکه Dynamic IP یا IP آدرسی از سرویس دهنده خود دارید، باید از NAT و روش های Load Balancing آن که در IOS وجود دارد بهره ببرید.



در توپولوژی بالا روتر مشترک از طریق ISP1 و ISP2 به اینترنت متصل شده و به طبع آن برای هر لینک از یک IP مجزا استفاده میشود.

با توجه به سناریوی فوق، روتر مشترک را بدین صورت تنظیم میکنیم:

```
ip route 0.0.0.0 0.0.0.0 dialer1
ip route 0.0.0.0 0.0.0.0 dialer2
ip nat inside source route-map nat1 interface Dialer1 overload
ip nat inside source route-map nat2 interface Dialer2 overload
```

```
!
access-list 110 permit ip 192.168.1.0 0.0.0.255 any
!
route-map nat1 permit 10
match ip address 110
match interface Dialer1
!
route-map nat2 permit 10
match ip address 110
match interface Dialer2
```

در تنظیم بالا، Router قبل از ارسال بسته به اینترنت ابتدا لینک سرویس دهنده را انتخاب میکند (بر اساس Routing) و سپس برای بسته های بعدی به آن مقصد همیشه از همان میسر بهره میبرد. پس NAT فراموش نمیکند که یک ارتباط را از کدام مسیر برقرار کرده لذا Destination همیشه یک Source را در یک ارتباط میبیند.

Cisco in Persian