دانشکده‌ی مهندسی کامپیوتر

آزمایشگاه شبکه‌های کامپیوتری

آشنایی با مکانیزمNAT

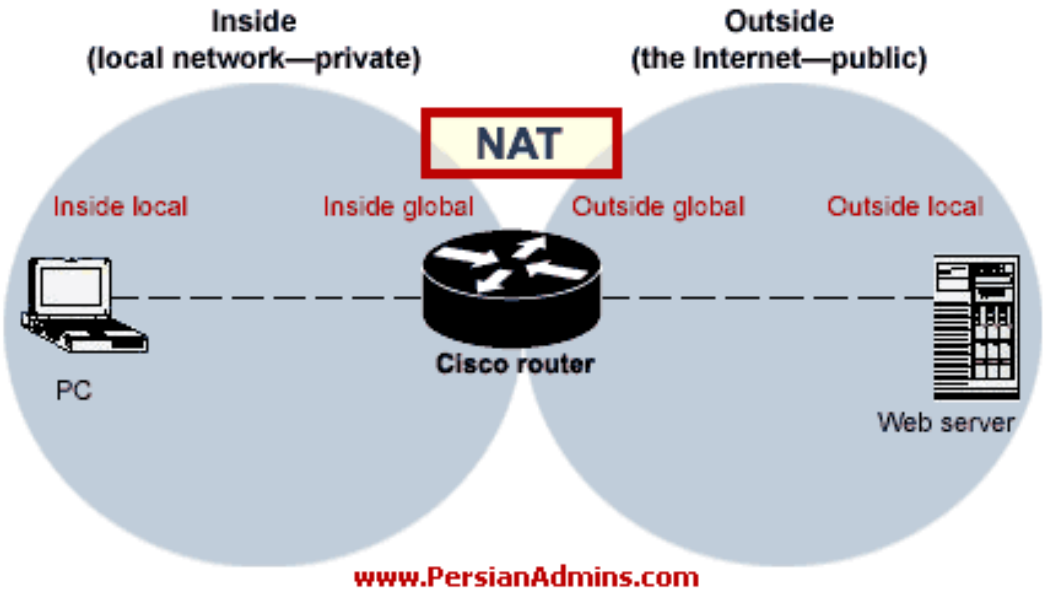
۱ مقدمه

NAT یا Network Address Translation پروتکلی است برای تبدیل آدرس‌های IP غیر معتبر به آدرس‌های معتبر برای استفاده کاربران از اینترنت که در لایه ۳ مدل OSI کار می‌کند.
این پروتکل زمانی مورد استفاده قرار می‌گیرد که کاربرانی که در یک شبکه دارای آدرس های معتبر نیستند، نیاز به برقراری ارتباط با اینترنت دارند.
این پروتکل نعداد آدرس آیپی داخلی را در قالب آدرس عمومی و معتبر به واسط خروجی خود ارسال (Forward) می‌کند.
درواقع هنگامی از این پروتکل استفاده می‌کنیم که تعداد کاربرانی که در شبکه‌ی ما احتیاج به اتصال به اینترنت دارند، کمتر از تعداد هایIP عمومی اختصاص یافته به این شبکه باشند.
بخشی از کاربردهای اصلی NAT را می‌توان به موارد زیر خلاصه نمود:

- ترجمه IP های Private به Public یا بلعکس
- تغییر مرکز سرویس دهنده اینترنت بدون نیاز به تغییر هایIP داخلی
- حفاظت از یک شبکه حساس در مقابل برخی حملات خارجی
- تغییر پورت مقصد بسته‌ها برای کاربران داخلی به صورت شفاف

برخی اصطلاحات مرتبط با NAT عبارتند از:

- **Inside Local:** به آدرسی(هایی) اطلاق می‌شود که بر روی کلاینت‌های شبکه داخلی تنظیم شده‌اند.
- **Inside Global:** به آدرسی اطلاق می‌شود که به واسط داخلی روتر که به شبکه داخلی متصل است داده شده است.
- **Outside Local:** به آدرس‌هایی که درون اینترنت یا شبکه Public قرار دارد گفته می‌شود.
- **Outside Global:** به آدرسی(هایی) که بر روی واسط خارجی روتری که به شبکه Public متصل است گفته می‌شود.



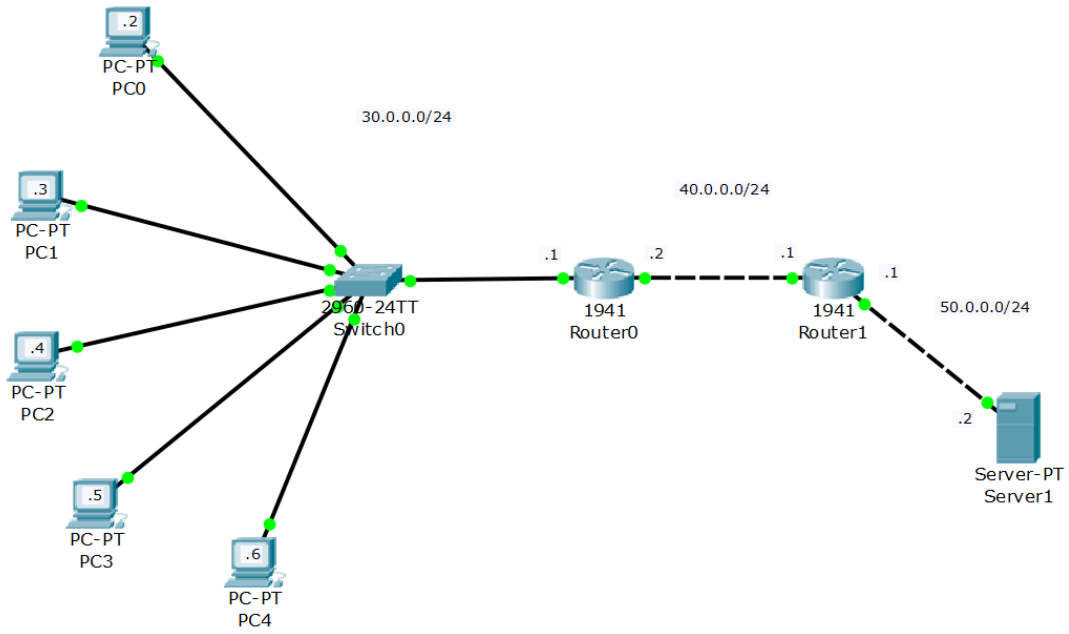
شکل ۱: اسامی نواحی در NAT

۲ Static NAT

این نوع NAT به صورت یک به یک عمل می‌کند. بدین صورت که یک آدرس inside-local را به یک outside-global ترجمه می‌کند. این نوع NAT زمانی کاربرد دارد که احتیاج است یک آدرس private به یک آدرس public تبدیل شود.

۱.۲ شرح آزمایش

برای اولین گام این آزمایش، می‌خواهیم در شبکه زیر آدرس واقعی IP سرور (گوشه سمت راست) را پنهان کرده و آدرس 100.0.0.1/24 را به عنوان آدرسی که دیگران سرور را با آن می‌شناسند، در نظر بگیریم. در گام اول باید آدرس هر کدام از عناصر موجود در شبکه را تعیین کرده و در مسیریاب‌های میانی، مسیرهای رفت و برگشت بسته‌های بین کاربران و سرور را وارد کنید. مراحل این کار در جلسات پیشین به صورت کامل توضیح داده شده است.
البته باید توجه داشته باشید به دلیل اینکه می‌خواهیم با آدرس غیر واقعی 100.0.0.1/24 با سرور در ارتباط باشیم، باید با استفاده از همین آدرس مسیریابی انجام شود. یعنی هیچ اطلاعات مسیری نباید در مورد آدرس واقعی سرور وجود داشته باشد.
سپس باید در نزدیک‌ترین مسیریاب به سرور (Router۱) تنظیمات مربوط به ترجمه آدرس را انجام دهیم:
ابتدا دستور مربوط به ترجمه آدرس را اجرا کرده و هر کدام از دو پورت خروجی و ورودی مسیریاب را با توجه به نواحی تقسیم‌بندی شده در NAT نام‌گذاری می‌کنیم.



شکل ۲: نمای کلی شبکه

```
1 R1(config)#ip nat inside source static 50.0.0.2 100.0.0.1
2 R1(config)#interface GigabitEthernet 0/0
3 R1(config-if)#ip nat inside
4 R1(config-if)#exit
5 R1(config)#interface GigabitEthernet 0/1
6 R1(config-if)#ip nat outside
```

دستور خط اول، آدرس واقعی را به آدرس غیرواقعی نگاشت می‌کند. دستورات بعدی برای تعیین نواحی روی مسیریاب هستند. برای مثال فرض کنید واسط با آدرس 50.0.0.1 از نوع inside و دیگری از نوع outside است.

اکنون برای آزمون درست بودن تنظیمات، از PC0 سرور را با آدرس جعلی Ping می‌کنیم. این سرور باید به درستی Ping شود.

```
Packet Tracer PC Command Line 1.0
PC>ping 100.0.0.1
Pinging 100.0.0.1 with 32 bytes of data:
Reply from 100.0.0.1: bytes=32 time=141ms TTL=126
Reply from 100.0.0.1: bytes=32 time=80ms TTL=126
Reply from 100.0.0.1: bytes=32 time=109ms TTL=126
Reply from 100.0.0.1: bytes=32 time=125ms TTL=126

Ping statistics for 100.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 80ms, Maximum = 141ms, Average = 113ms
```

این بار سرور را با آدرس اصلی آن پینگ می‌کنیم. مشاهده می‌کنیم که عملیات با شکست مواجه می‌شود.

```
PC>ping 50.0.0.2
Pinging 50.0.0.2 with 32 bytes of data:
Reply from 30.0.0.1: Destination host unreachable.
Reply from 30.0.0.1: Destination host unreachable.
Reply from 30.0.0.1: Destination host unreachable.
Reply from 30.0.0.1: Destination host unreachable.

Ping statistics for 50.0.0.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

۳ Dynamic NAT

DNAT نیز همانند SNAT است اما با این تفاوت که در NAT به صورت Dynamic می‌توانیم یک یا چندین IP را به چندین IP دیگر ترجمه کنیم.
فرض کنید شما Admin یک ISP هستید و به دلیل کمبود IP نیاز به NAT دارید. بر فرض مثال شما دارای ۱۰ آدرس معتبر و ۱۰۰ غیرمعتبر هستید. ممکن است برای شما هم پیش آمده باشد که مدتی طولانی برای دانلود یک فایل از سایت Rapidshare.com انتظار بکشید.
دلیل این اتفاق این است که سایت Rapidshare.com تمامی کاربرهای شبکه شما را به چشم یک کاربر می‌بیند(چون یک آیپی به همه‌ی این کاربران اختصاص یافته است). برای رفع این مشکل می‌توانید تعداد بیشتری IP را به کاربران شبکه‌ی خود اختصاص دهید. Dynamic NAT معمولا آدرسهای معتبر را به وسیله IP nat pool مشخص و آدرسهای غیر معتبر را توسط یک Access-list مشخص می‌کند. دلیل استفاده از Access-list ایجاد امنیت بیشتر است.
تنها محدودیت DNAT این مساله است که تعداد کاربرانی که می‌توانند در یک لحظه به شبکه بیرون (اینترنت) متصل شوند حداکثر به تعداد آدرس‌های معتبر خواهد بود

۱.۳ شرح آزمایش

در این بخش از آزمایش می‌خواهیم با داشتن ۴ آدرس معتبر، ۵ کاربر (نه لزوما همزمان) را قادر به اتصال سرور کنیم. برای اینکار باید دستورات ترجمه آدرس را در مسیریاب Router0 اجرا کنیم تا آدرس‌های غیرمعتبر کاربران را به آدرس‌های معتبر ترجمه و نگاشت کند.

```
1 R0(config)#access-list 1 permit 30.0.0.0 0.0.0.255
2 R0(config)#ip nat pool test 40.0.0.3 40.0.0.5 netmask 255.255.255.0
3 R0(config)#ip nat inside source list 1 pool test
4 R0(config)#interface GigabitEthernet 0/0
5 R0(config-if)#ip nat inside
6 R0(config-if)#exit
7 R0(config)#interface GigabitEthernet 1/0
8 R0(config-if)#ip nat outside
```

خط اول برای ساخت یک Access-list و خط دوم برای مشخص کردن آدرس‌های معتبر می‌باشد. دستورات خطوط سوم به بعد نیز مانند آزمایش قبل تنظیمات پورت خروجی و ورودی است(با فرض اینکه پورت نزدیک به کاربرها پورت ورودی می‌باشد).
برای آزمایش درستی دستورات بالا، دستور زیر را در Router0 اجرا می‌کنیم. این دستور اطلاعات مربوط به اجرای ترجمه آدرس را در ترمینال چاپ می‌کند.

```
R0#debug ip nat
```

حال از طرف کاربرها، سرور را با آدرس جعلی پینگ می‌کنیم. (به خاطر داشته باشید که تنظیمات مربوط به مسیریابی روی هر دو مسیریاب به خاطر ترجمه انجام شده روی آدرس‌های کاربران، نیاز به بازنگری و تغییر دارند)
سپس، نتیجه زیر را در ترمینال Router0 خواهیم دید.

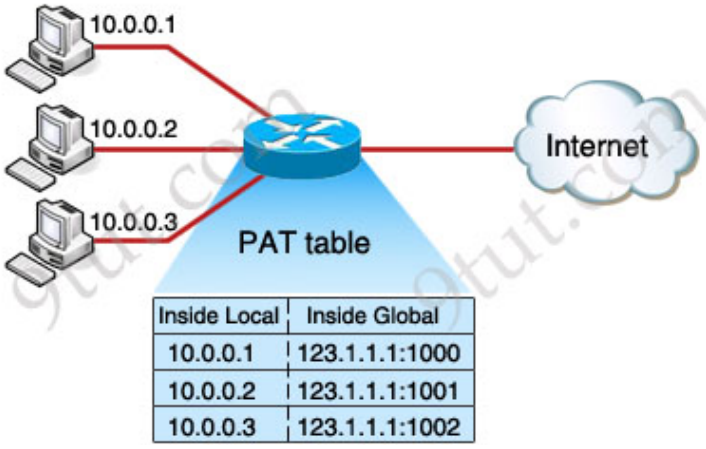
```
IP NAT debugging is on
NAT: s=30.0.0.2->40.0.0.3, d=100.0.0.1[1]
NAT*: s=100.0.0.1, d=50.0.0.1->30.0.0.2[1]
NAT: s=30.0.0.2->40.0.0.3, d=100.0.0.1[1]
NAT*: s=100.0.0.1, d=50.0.0.1->30.0.0.2[1]
NAT: s=30.0.0.2->40.0.0.3, d=100.0.0.1[1]
NAT*: s=100.0.0.1, d=50.0.0.1->30.0.0.2[1]
NAT: s=30.0.0.2->40.0.0.3, d=100.0.0.1[1]
NAT*: s=100.0.0.1, d=50.0.0.1->30.0.0.2[1]
```

بعد از اتمام آزمون، گزارش‌گیری از ترجمه را غیر فعال کنید.

```
R0#no debug ip nat
```

۴ PAT

این نوع از NAT محدودیت DNAT را با اضافه کردن پورت‌ها به فرآیند ترجمه آدرس حل می‌کند.
ممکن است ما به شرایطی برخورد کنیم که تنها ۱ عدد آدرس Valid در اختیار داشته باشیم و مجبور به NAT کردن آدرس مذکور به چندین آدرس شویم. در چنین شرایطی باید از قابلیت Overload استفاده کنیم.
در این حالت روتر برای ورود و خروج هر آدرس Invalid، یک پورت مجزا در نظر می گیرد و تمامی این پورت‌ها و آدرس‌ها را در جدولی به ثبت می‌رساند. به این ترتیب هر بسته که از روتر به مقصد اینترنت خارج می‌شود دقیقا در هنگام بازگشت به همان آدرس Invalid که صادر کننده آن است باز می‌گردد. هر خط در جدول مذکور در واقع یک ارتباط به حساب می‌آید. در سخت‌افزارهای مختلف برای تعداد این ارتباطات محدودیت‌های مختلفی در نظر گرفته شده است.



شکل ۳: یک نمونه جدول ترجمه آدرس PAT

۱.۴ شرح آزمایش

برای تبدیل DNAT به PAT در Router0 ابتدا دستور ترجمه (که در خط سوم آزمایش قبلی به آن اشاره شده است) را لغو می‌کنیم. سپس دستور ترجمه آدرس جدید را اجرا می‌کنیم.

```
R0(config)#no ip nat inside source list 1 pool test
R0(config)#ip nat inside source list 1 pool test overload
```

کلمه overload به معنی استفاده از فضای پورت‌ها در فرآیند ترجمه آدرس است. این‌بار نیز برای بررسی اجرای درست دستورات از گزارش‌گیری در مسیریاب مناسب استفاده کنید و نتایج را مشاهده کنید.

۵ سوالات

۱. با استفاده از گذاشتن علامت سوال بعد از هر کلمه در دستورات زیر، انواع دستورات قابل تولید را لیست کرده و موارد استفاده شده و نتیجه اجرای هر یک را توضیح دهید.

```
R0(config)#ip nat
```

۲. Access-list ها چند نوع هستند و برای چه مواردی استفاده می‌شوند؟ با استفاده از Access-list قطعه کدی بنویسید که برقراری ارتباط کاربران شبکه با پورت tcp ۸۰ سرور ممکن نباشد. (بسته‌های از این نوع در مسیریاب فیلتر شوند)

۳. نتایجی که از گزارش‌گیری در آزمایش PAT مشاهده کردید را توضیح دهید.

۴. مشخص کردن پورت‌های ورودی و خروجی در مسیریاب برای اجرای ترجمه آدرس‌ها، چه اهمیتی دارند؟ دستورات آزمایش ۲ و ۳ را با در نظر گرفتن تعویض پورت خروجی و ورودی Router0 بازنویسی کنید.