



به نام خدا

گزارش آزمایش شماره ۶
آزمایشگاه شبکه‌های کامپیوتری
گروه ۴

ارشیا یوسف‌نیا ۴۰۱۱۱۰۴۱۵
محمدفرحان بهرامی ۴۰۱۱۰۵۷۲۹
امیرمهدی دارایی ۹۹۱۰۵۴۳۱

استاد درس: دکتر صفایی

۱	مقدمه	3
۲	Static Nat	3
۳	Dynamic NAT	5
۴	PAT	6
۵	سوالات	7
۱	۱	7
	دستور inside	7
	دستور outside	8
	دستور pool	8
۲	۲	8
	Standard Access List	8
	Extended Access List	9
	مثالی از کد	9
۳	۳	9
۴	۴	10
۶	منابع	10

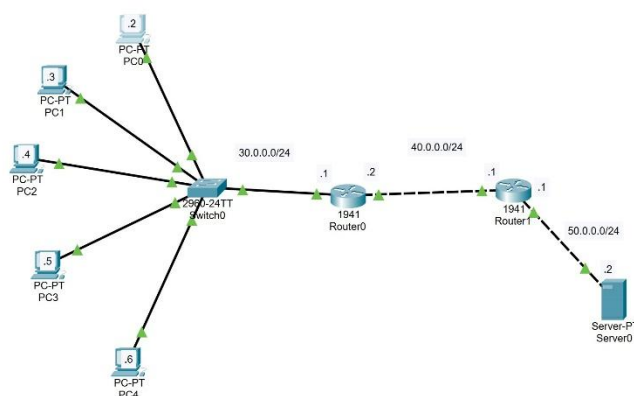
۱ مقدمه

هدف اصلی NAT، استفاده بهینه از تعداد محدود آدرس‌های عمومی و همچنین فراهم کردن امنیت نسبی برای کاربران شبکه داخلی در برابر تهدیدات خارجی است. از مزایای دیگر NAT می‌توان به جداسازی ساختار داخلی شبکه از دید بیرونی، جلوگیری از دسترسی مستقیم به کاربران داخلی و امکان تغییر سرویس‌دهنده اینترنت بدون نیاز به تغییر آدرس‌های IP داخلی اشاره کرد.

در این آزمایش، با انواع مختلف NAT شامل Static NAT، Dynamic NAT و PAT آشنا خواهیم شد. همچنین نحوه پیکربندی آن‌ها در تجهیزات شبکه مانند روترها بررسی می‌شود. با استفاده از ابزاری نظیر Cisco Packet Tracer، عملکرد NAT در شرایط مختلف عملیاتی مورد بررسی قرار می‌گیرد.

۲ Static Nat

ابتدا نمای کلی شبکه را طبق چیزی که در دستورکار گفته شده است، دستگاه‌ها و روترها و سویچ را آورده و با اتصالات آن‌ها را می‌بندیم و برای هر روتر و دستگاه‌های دیگر IP‌های آن‌ها را به همراه Subnet Mask مشخص می‌کنیم. و برای دستگاه‌ها نیز باید بخش Default Gateway را نیز همان آدرس روتر متصل قرار می‌دهیم. در نهایت شبکه ساخته شده در تصویر ۱ که مانند شبکه دستورکار است قابل مشاهده است.



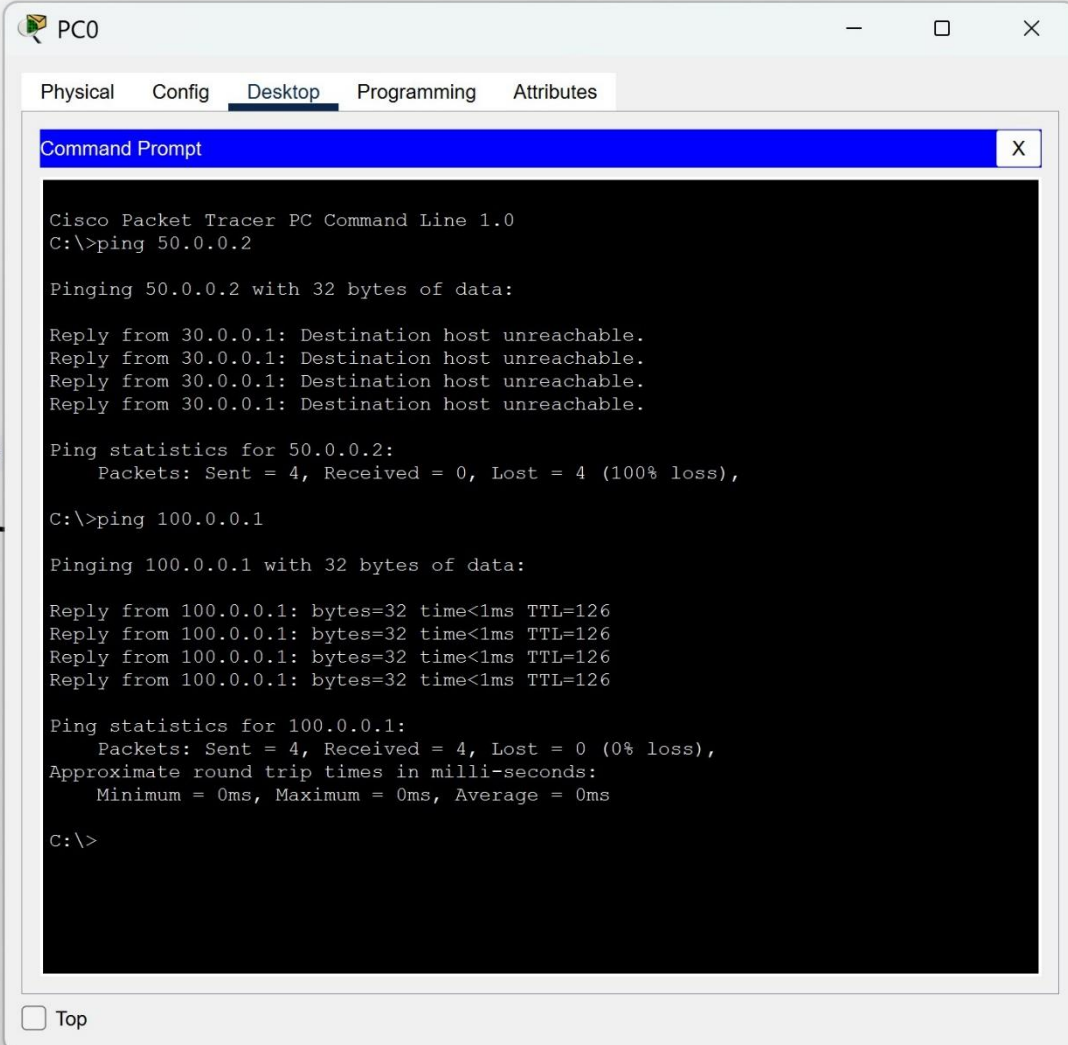
تصویر 1 ساختن شبکه مورد نیاز آزمایش

حال برای انجام آزمایش، وارد بخش CLI روتر 1 شده و با وارد کردن دستور enable و conf t به ترتیب، وارد ترمینال مربوط به تنظیمات روتر می‌شویم. سپس دستورهای گفته شده مربوط به این بخش را در ترمینال وارد کرده و در نهایت از CLI خارج می‌شویم. حال تنها کاری که نیاز است انجام دهیم، اصلاح Routing هر یک از روترها است. برای این کار، دوباره وارد روتر 1 شده و

به بخش Config، سپس به بخش Routing و در نهایت به بخش Static رفته و در قسمت Network باید 30.0.0.0 را وارد کرده و در بخش Mask باید 255.255.255.0 و در نهایت در Next Hop باید 40.0.0.2 را وارد کرده تا مسیریابی 30.0.0.0/24 via 40.0.0.2 را در این روتر انجام دهد.

این بار وارد روتر 0 شده و همان مراحل که در روتر 1 طی کردیم را انجام داده و در این روتر باید مسیریابی 100.0.0.0/24 via 40.0.0.1 را اضافه کنیم.

حال همه چیز آماده است تا نتیجه ping را ببینیم. برای این کار وارد Command Prompt مربوط به PC0 شده و یکبار باید 50.0.0.2 را ping را بررسی کنیم، که می‌بینیم این آدرس پینگ نمی‌شود. و بار دیگر 100.0.0.1 را ping را بررسی کرده و می‌بینیم این آدرس پینگ می‌شود. در تصویر ۲ می‌توانید خروجی این ۲ دستور ping را مشاهده کنید.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>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),

C:\>ping 100.0.0.1

Pinging 100.0.0.1 with 32 bytes of data:

Reply from 100.0.0.1: bytes=32 time<1ms TTL=126
Reply from 100.0.0.1: bytes=32 time<1ms TTL=126
Reply from 100.0.0.1: bytes=32 time<1ms TTL=126
Reply from 100.0.0.1: bytes=32 time<1ms TTL=126

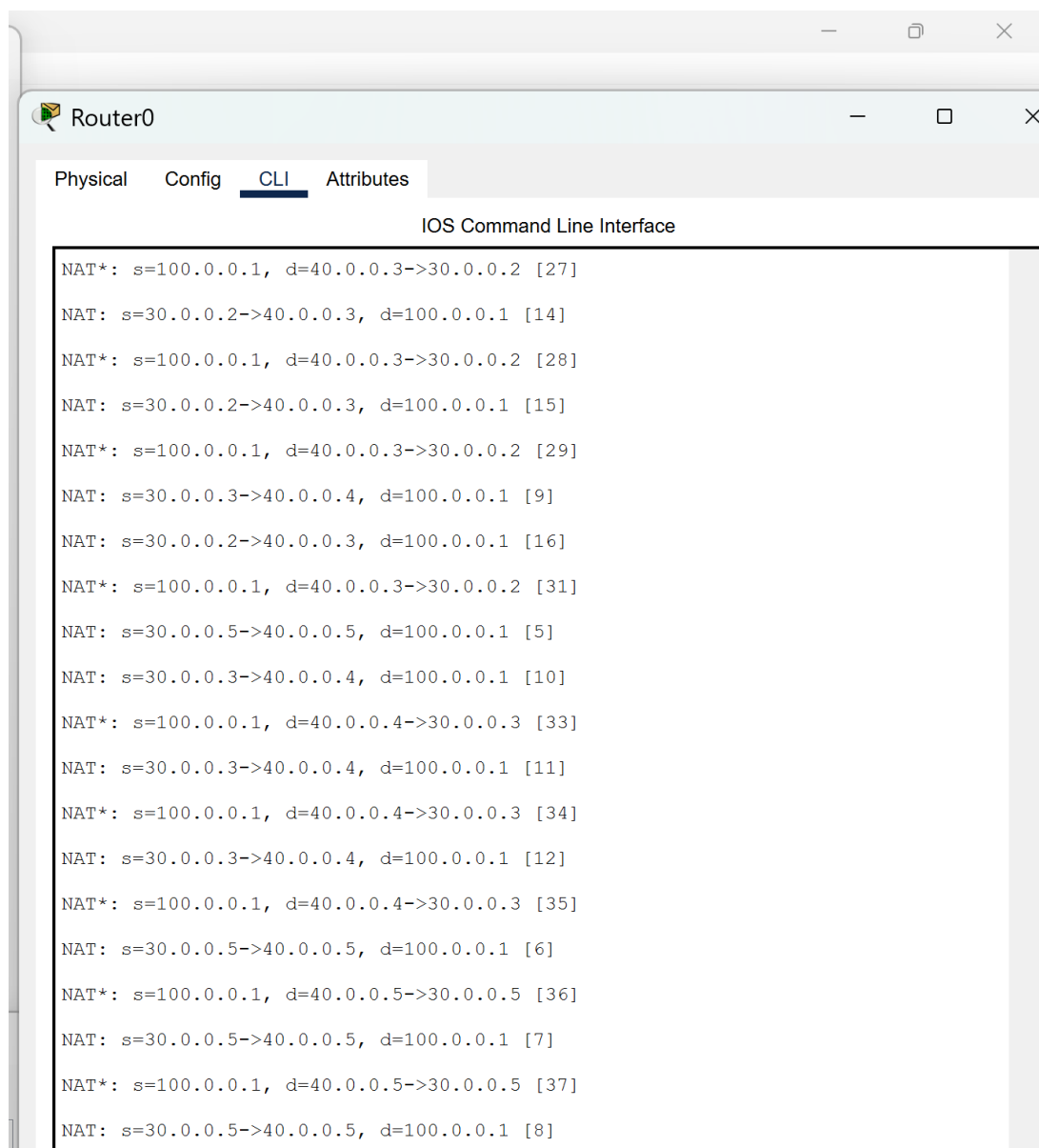
Ping statistics for 100.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

تصویر 2) ping کردن ۲ آدرس در حالت Static NAT

Dynamic NAT ۳

برای انجام این بخش، کافی است که وارد CLI روتر 0 شویم و دستورهای گفته شده در دستورکار را به ترتیب وارد کرده و سپس از حالت تنظیمات خارج شده و debug را فعال کنیم. حال ما همزمان ۴ تا از PCها را باز کرده و وارد بخش Command Prompt آنها شده و همزمان که ترمینال مربوط به روتر 0 در حالت debug است، در PCها 100.0.0.1 ping را وارد کرده و نتیجه را در ترمینال روتر مشاهده می‌کنیم.



The screenshot shows the CLI of Router0 with the 'CLI' tab selected. The output displays a series of NAT translation entries. Each entry consists of a line starting with 'NAT*' followed by source and destination IP addresses and a line starting with 'NAT:' followed by the same addresses. The source IP is consistently 100.0.0.1, and the destination IP is 40.0.0.3, which is translated to 30.0.0.2. The logs show multiple instances of this translation, indicating that the NAT is active and processing traffic.

```
Router0
Physical Config CLI Attributes
IOS Command Line Interface
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.2 [27]
NAT: s=30.0.0.2->40.0.0.3, d=100.0.0.1 [14]
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.2 [28]
NAT: s=30.0.0.2->40.0.0.3, d=100.0.0.1 [15]
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.2 [29]
NAT: s=30.0.0.2->40.0.0.3, d=100.0.0.1 [15]
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.2 [31]
NAT: s=30.0.0.3->40.0.0.4, d=100.0.0.1 [9]
NAT: s=30.0.0.2->40.0.0.3, d=100.0.0.1 [16]
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.2 [31]
NAT: s=30.0.0.5->40.0.0.5, d=100.0.0.1 [5]
NAT: s=30.0.0.3->40.0.0.4, d=100.0.0.1 [10]
NAT*: s=100.0.0.1, d=40.0.0.4->30.0.0.3 [33]
NAT: s=30.0.0.3->40.0.0.4, d=100.0.0.1 [11]
NAT*: s=100.0.0.1, d=40.0.0.4->30.0.0.3 [34]
NAT: s=30.0.0.3->40.0.0.4, d=100.0.0.1 [12]
NAT*: s=100.0.0.1, d=40.0.0.4->30.0.0.3 [35]
NAT: s=30.0.0.5->40.0.0.5, d=100.0.0.1 [6]
NAT*: s=100.0.0.1, d=40.0.0.5->30.0.0.5 [36]
NAT: s=30.0.0.5->40.0.0.5, d=100.0.0.1 [7]
NAT*: s=100.0.0.1, d=40.0.0.5->30.0.0.5 [37]
NAT: s=30.0.0.5->40.0.0.5, d=100.0.0.1 [8]
```

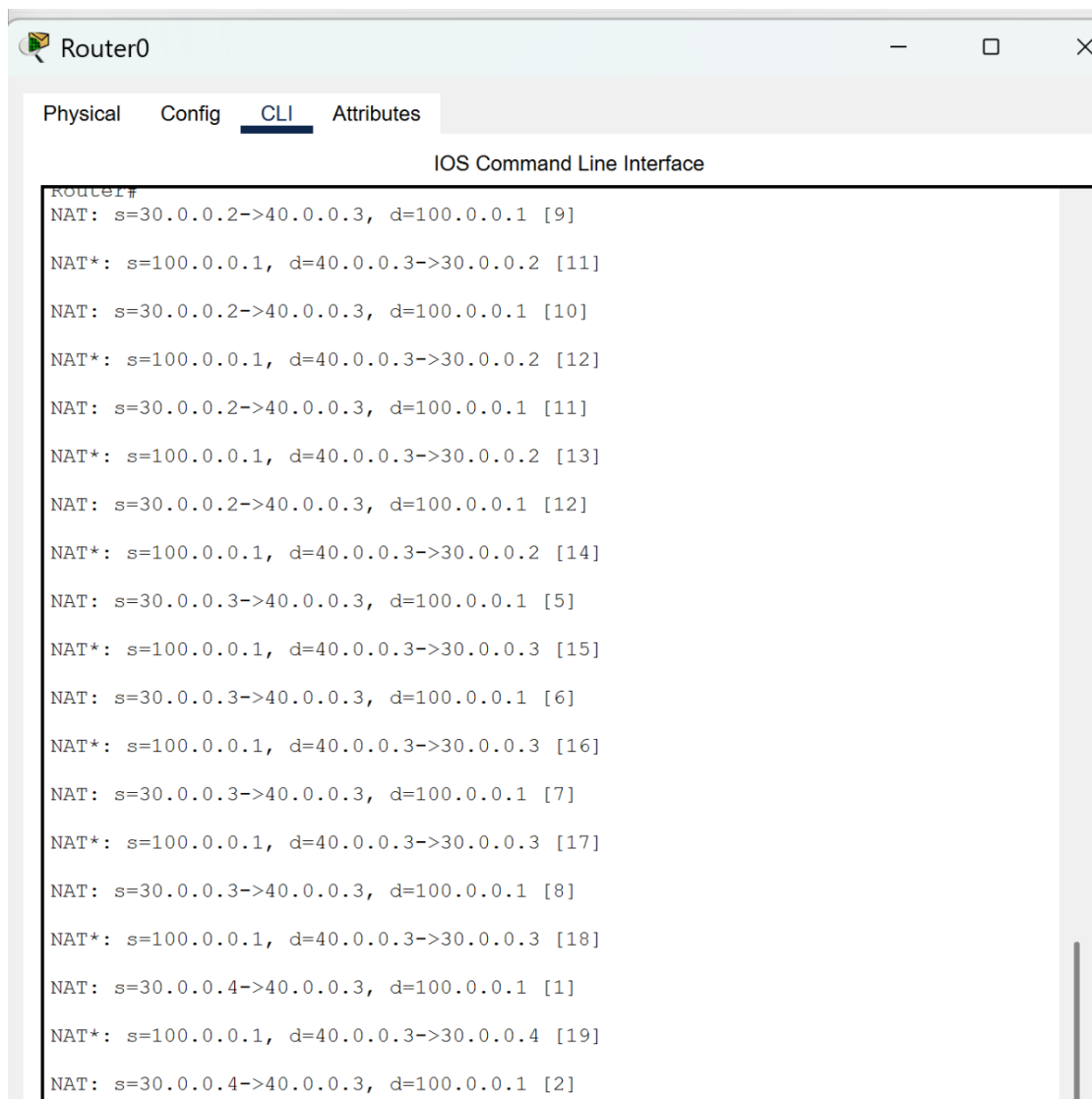
تصویر 3) ping دهی PCها در حالت Dynamic NAT

همانطور که در تصویر ۳ مشاهده می‌کنید، PC0، PC1 و PC3 به ترتیب آدرس‌های 40.0.0.3، 40.0.0.4 و 40.0.0.5 را دریافت کرده که این همان چیزی است که انتظار داشتیم.

همچنین باید در نظر گرفت که PC2 نیز منتظر این است تا یکی از آدرس‌های گرفته شده آزاد شود تا بتواند از آن استفاده کند. که این نیز منطقی است چون بیشتر از ۳ تا PC نمی‌توانند همزمان ping کنند.

PAT ۴

برای انجام این بخش کافی است که دستورکار را دنبال کنیم و کارهایی که گفته شده را در روتر 0 انجام داده و بار دیگر حالت debug را فعال کرده و دوباره ۴ تا از PC ها را همزمان باز کرده و دستور ping 100.0.0.1 را در آن‌ها وارد می‌کنیم.



The screenshot shows the CLI of Router0 with the 'CLI' tab selected. The title bar says 'Router0'. Below the tabs, it says 'IOS Command Line Interface'. The main area displays the output of the 'show ip nat translations' command, showing a list of NAT translations. The translations are as follows:

```
Router#
NAT: s=30.0.0.2->40.0.0.3, d=100.0.0.1 [9]
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.2 [11]
NAT: s=30.0.0.2->40.0.0.3, d=100.0.0.1 [10]
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.2 [12]
NAT: s=30.0.0.2->40.0.0.3, d=100.0.0.1 [11]
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.2 [13]
NAT: s=30.0.0.2->40.0.0.3, d=100.0.0.1 [12]
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.2 [14]
NAT: s=30.0.0.3->40.0.0.3, d=100.0.0.1 [5]
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.3 [15]
NAT: s=30.0.0.3->40.0.0.3, d=100.0.0.1 [6]
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.3 [16]
NAT: s=30.0.0.3->40.0.0.3, d=100.0.0.1 [7]
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.3 [17]
NAT: s=30.0.0.3->40.0.0.3, d=100.0.0.1 [8]
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.3 [18]
NAT: s=30.0.0.4->40.0.0.3, d=100.0.0.1 [1]
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.4 [19]
NAT: s=30.0.0.4->40.0.0.3, d=100.0.0.1 [2]
```

تصویر 4) ping دهی PC ها در حالت Dynamic PAT

همانطور که در تصویر ۴ مشاهده می‌کنید، برخلاف حالت Dynamic که باید هر PC یک آدرس یکتا داشته باشد، در PAT همه‌ی PC ها آدرس 40.0.0.3 را دریافت کرده‌اند که یعنی هر کدام یک پورت را از آدرس گرفته و ترجمه به درستی انجام شده است.

۵ سوالات

۱.

وارد ترمینال شده و دستور ? ip nat را وارد کرده و خروجی به صورت زیر است:

```
Router(config)#ip nat ?
      inside      Inside address translation
      outside     Outside address translation
      pool        Define pool of addresses
```

دستور inside

این دستور مربوط به ترجمه آدرس‌های سمت داخل شبکه است. معمولاً برای مشخص کردن منبع^۱ NAT استفاده می‌شود و تنظیم اصلی NAT در این بخش انجام می‌شود. فرمت کلی آن به صورت:

ip nat inside source ...

می‌باشد، که به سه دستور تقسیم می‌شود:

۱. Static NAT

ip nat inside source static [private-ip] [public-ip]

هر بار که بسته‌ای از IP داخلی ارسال می‌شود، با IP عمومی مشخصی جایگزین می‌شود. برای سرورها یا دستگاه‌هایی که نیاز به IP عمومی دائمی دارند.

۲. Dynamic NAT

ip nat inside source list [ACL] pool [pool-name]

آدرس‌های داخلی به صورت پویا از طریق یک Access-list و Pool ترجمه می‌شوند یعنی آدرس‌های داخل شبکه به صورت به یکی از IP‌های عمومی موجود در pool تبدیل می‌شوند.

۳. PAT

ip nat inside source list [ACL] pool [pool-name] overload

با استفاده از یک آدرس عمومی، چندین کاربر داخلی می‌توانند همزمان به اینترنت متصل شوند. overload ترجمه پورت‌ها را فعال می‌کند.

¹ source

دستور outside

این دستور به ما کمک می‌کند تا آدرس‌های بیرونی را ترجمه کنیم که فرمت کلی آن به صورت

ip nat inside source ...

است، که به ۲ دستور تقسیم می‌شود:

۱. Static NAT:

وقتی می‌خواهیم آدرس IP خارجی که وارد شبکه ما می‌شود، به یک IP دیگر ترجمه شود.

ip nat outside source static [public-ip] [private-ip]

۲. Dynamic NAT:

برای ترجمه داینامیک آدرس‌های سمت بیرونی به مجموعه‌ای از IPهای داخلی.

ip nat outside source list [ACL-number] pool [pool-name]

دستور pool

این دستور برای تعریف یک مجموعه از IPهای عمومی استفاده می‌شود که در Dynamic NAT یا PAT برای ترجمه آدرس‌های داخلی به کار می‌روند.

ip nat pool [name] [start-ip] [end-ip] netmask [mask]

۲.

۳ نوع ACL اصلی وجود دارد که به صورت زیر است:

Standard Access List

ساده‌ترین نوع است که فقط بر اساس آدرس IP مبدا تصمیم‌گیری می‌کند. این نوع ACL نمی‌تواند پروتکل‌ها یا شماره پورت‌ها را تشخیص دهد و تنها بررسی می‌کند که ترافیک از چه IP فرستاده شده است. به همین دلیل، کنترل محدودی بر نوع ترافیک دارد و بیشتر برای فیلتر کلی دسترسی کاربران یا دستگاه‌های خاص استفاده می‌شود. شماره این نوع access-list معمولاً در بازه 1 تا 99 یا 1300 تا 1999 تعریف می‌شود. از آنجایی که این نوع ACL فقط مبدا را بررسی می‌کند، باید نزدیک به مقصد اعمال شود تا اثرگذاری دقیق‌تری داشته باشد.

Extended Access List

پیشرفته‌تر از نوع Standard است و می‌تواند بر اساس چندین پارامتر مختلف مانند IP مبدأ، IP مقصد، نوع پروتکل (TCP، UDP، ICMP و ...)، شماره پورت، و حتی نوع بسته تصمیم‌گیری کند. این نوع ACL برای فیلتر دقیق ترافیک‌های خاص، یا فقط اجازه دادن به ترافیک از یک سرور خاص، کاربرد دارد. شماره‌های آن در بازه 100 تا 199 یا 2000 تا 2699 هستند. Extended ACL معمولاً نزدیک به مبدأ قرار می‌گیرد تا قبل از اینکه ترافیک غیرمجاز به مسیر اصلی برسد، فیلتر شود.

مثالی از کد

```
access-list 110 deny tcp any 192.168.1.0 0.0.0.0 eq 80
```

این دستور یک قانون در یک Extended Access List به شماره 110 است که مشخص می‌کند تمام ترافیک‌های TCP از هر IP مبدأ که قصد دارد به آدرس مقصد "192.168.1.0" (دقیقاً یک IP خاص است، چون wildcard آن "0.0.0.0" است)، روی پورت 80 برود، باید مسدود شود.

۳.

Pro	Inside global	Inside local	Outside local	Outside global
icmp	40.0.0.3:1024	30.0.0.5:1	100.0.0.1:1	100.0.0.1:1024
icmp	40.0.0.3:1025	30.0.0.5:2	100.0.0.1:2	100.0.0.1:1025
icmp	40.0.0.3:1026	30.0.0.5:3	100.0.0.1:3	100.0.0.1:1026
icmp	40.0.0.3:1027	30.0.0.5:4	100.0.0.1:4	100.0.0.1:1027
icmp	40.0.0.3:10	30.0.0.2:10	100.0.0.1:10	100.0.0.1:10
icmp	40.0.0.3:11	30.0.0.2:11	100.0.0.1:11	100.0.0.1:11
icmp	40.0.0.3:12	30.0.0.2:12	100.0.0.1:12	100.0.0.1:12
icmp	40.0.0.3:1	30.0.0.4:1	100.0.0.1:1	100.0.0.1:1
icmp	40.0.0.3:2	30.0.0.4:2	100.0.0.1:2	100.0.0.1:2
icmp	40.0.0.3:3	30.0.0.4:3	100.0.0.1:3	100.0.0.1:3
icmp	40.0.0.3:4	30.0.0.4:4	100.0.0.1:4	100.0.0.1:4
icmp	40.0.0.3:5	30.0.0.3:5	100.0.0.1:5	100.0.0.1:5
icmp	40.0.0.3:6	30.0.0.3:6	100.0.0.1:6	100.0.0.1:6
icmp	40.0.0.3:7	30.0.0.3:7	100.0.0.1:7	100.0.0.1:7
icmp	40.0.0.3:8	30.0.0.3:8	100.0.0.1:8	100.0.0.1:8
icmp	40.0.0.3:9	30.0.0.2:9	100.0.0.1:9	100.0.0.1:9

Router#

☐ Top

Copy Paste

تصویر 5) جدول ترجمه IPها در PAT

تصویر ۵ همان جدول ترجمه IPها را نشان می‌دهد. در سمت چپ یعنی inside global همان آدرس‌های IP هستند که به PCها داده شده است و همانطور که می‌بینیم همگی از یک IP ولی با پورت‌های مختلف استفاده می‌کنند و ترجمه به درستی انجام شده است.

همچنین ستون inside local نیز همان آدرس IP مربوط به PCها است. در نهایت می‌توان نتیجه گرفت که در حالت PAT برخلاف حالت Dynamic NAT محدودیت آدرس نداریم، چون قابلیت استفاده از پورت در ترجمه را داریم.

۴.

اهمیت مشخص کردن پورت‌های ورودی و خروجی در مسیریاب برای اجرای NAT بسیار زیاد است زیرا NAT وظیفه دارد آدرس‌های IP داخلی شبکه را به آدرس‌های عمومی ترجمه کند (و برعکس) تا ارتباط با اینترنت برقرار شود. برای انجام این ترجمه، مسیریاب باید دقیقاً بداند که بسته‌های داده باید از کدام پورت وارد (ورودی) و از کدام پورت خارج (خروجی) شوند. اگر پورت‌ها اشتباه تعیین شوند، NAT ممکن است بسته‌ها را به اشتباه ترجمه یا مسیردهی کند که موجب قطع ارتباط یا عدم دسترسی به سرویس‌های خارجی یا داخلی می‌شود.

در نهایت با پورت‌های ورودی و خروجی در Router0، باید دستورات مربوط به access list را نیز تعویض کنیم تا آزمایش دوباره به درستی کار کند. و حتی می‌توان قانون‌هایی را نیز برای اجازه عبور بسته‌ها با پورت‌های خاص را ندهیم.

۶ منابع

[1] https://en.wikipedia.org/wiki/Network_address_translation

[2] <https://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html>

[3] https://gaia.cs.umass.edu/kurose_ross/ppt.php