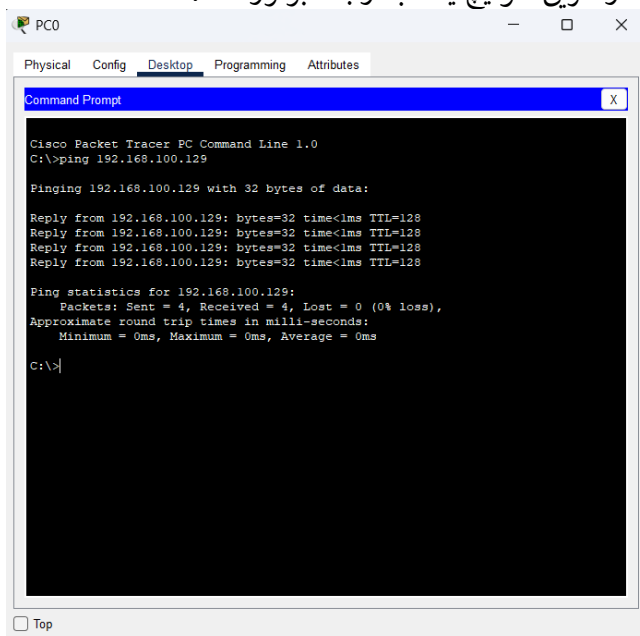


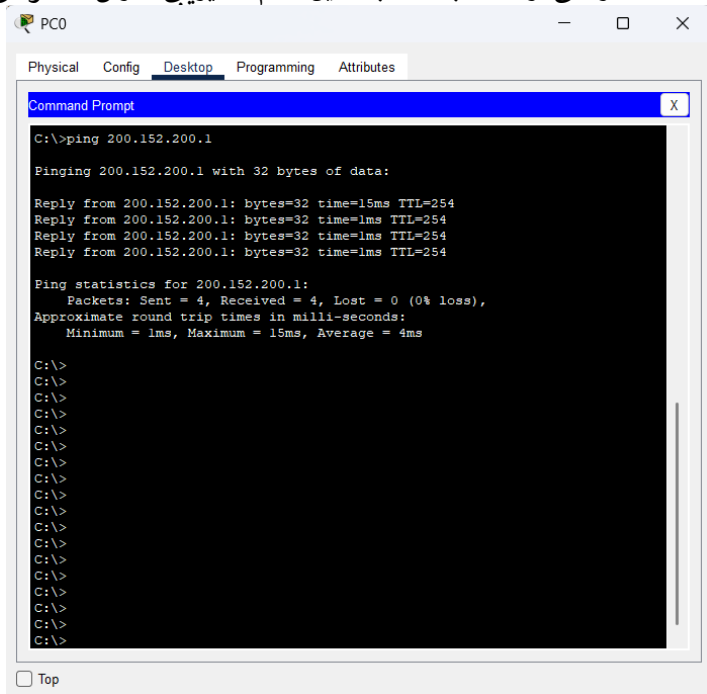
نام و نام خانوادگی	حسین تاتار	شماره دانشجویی	40133014	نام و شماره آزمایش	10-آشنایی با مکانیسم NAT و پروتکل DHCP
هدف آزمایش	آشنایی با آدرس دهی شبکه برای استفاده از سرویس های اینترنت بررسی عملکرد و پیکربندی مکانیسم NAT،PAT و پروتکل DHCP				
ابزارهای مورد نیاز	Cisco Packet Tracer				
شرح آزمایش	<p><b>مکانیسم NAT ایستا :</b></p> <p><b>سوال 1:</b> واسط های دستگاهها مطابق آدرس های داده شده در جدول 1 تنظیم شده است. آیا PC1 و PC2 قادر به Ping کردن یکدیگر هستند؟ چرا؟ آیا از PC1 میتوانید ISP را Ping کنید؟ چرا؟</p> <p><b>جواب:</b></p> <p>آیا PC1 و PC2 میتوانند یکدیگر را Ping کنند؟</p> <ol style="list-style-type: none"> <li>1. پاسخ: بله، PC1 و PC2 میتوانند یکدیگر را Ping کنند.</li> <li>2. دلیل:</li> </ol> <ul style="list-style-type: none"> <li>○ هر دو دستگاه PC1 با آدرس 192.168.100.2 و PC2 با آدرس 192.168.100.129 در یک شبکه محلی (LAN) با 255.255.255.0 subnet mask قرار دارند.</li> <li>○ از آنجا که آدرس های آنها در یک subnet است (192.168.100.0/24)، نیازی به مسیریابی (Routing) ندارند و میتوانند مستقیماً از طریق سوئیچ یا هاب ارتباط برقرار کنند.</li> </ul>				



آیا از PC1 می‌توان ISP را Ping کرد؟

- 3. پاسخ: خیر، PC1 نمی‌تواند ISP را Ping کند (مگر پس از تنظیم NAT)
- 4. دلیل:

- آدرس (25.16.59.1) ISP در یک شبکه متفاوت (25.16.59.0/30) قرار دارد.
- PC1 آدرس خصوصی (192.168.100.2) دارد که در اینترنت مسیریابی نمی‌شود. برای ارتباط با ISP، باید مکانیسم NAT روی RouterA فعال شود تا آدرس خصوصی PC1 به آدرس عمومی مثلاً (200.152.200.1) ترجمه شود.
- بدون NAT بسته‌های ارسالی از PC1 به ISP به دلیل عدم مسیریابی آدرس خصوصی در اینترنت، پاسخ نمی‌گیرند.



در اینجا پینگ می‌توان کرد زیرا این زمانی است که شبکه بنده تکمیل شده و مکانیسم NAT روی آن پیاده سازی شده است.

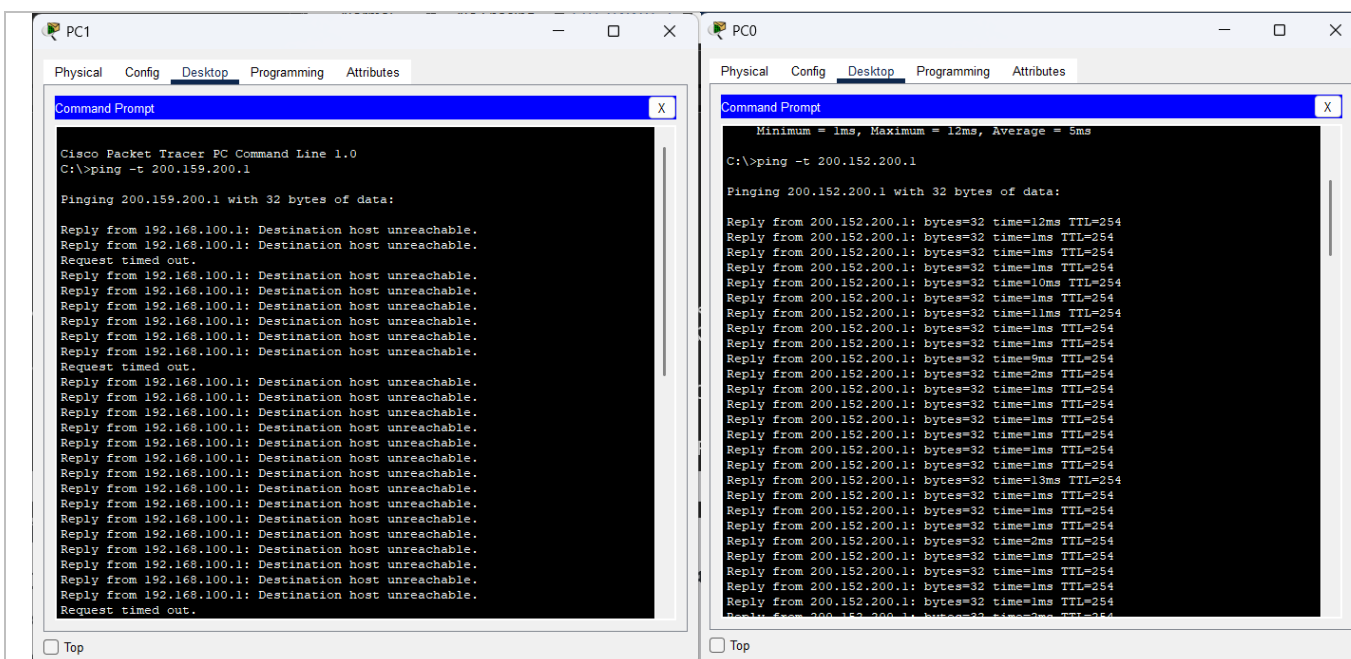
**سوال 2:** در محیط تنظیم عمومی مسیریاب RouterA دستور زیر را وارد کنید. با استفاده از این دستور صرفاً آدرس IP مبدا در بسته خروجی از شبکه تغییر می‌کند.

ip nat inside source static 192.168.100.2 200.152.200.1

• از PC1 و PC2 مسیریاب ISP را Ping کنید. چه اتفاقی می‌افتد؟

**جواب:**

- 5. PC1 می‌تواند ISP را Ping کند.
- 6. دلیل:
- آدرس (192.168.100.2) PC1 به 200.152.200.1 ترجمه می‌شود.
- ISP آدرس مبدأ را به عنوان 200.152.200.1 می‌بیند (که یک آدرس عمومی است) و پاسخ را ارسال می‌کند.
- RouterA پاسخ را به آدرس اصلی (192.168.100.2) برمی‌گرداند.
- 7. PC2 نمی‌تواند ISP را Ping کند.
- 8. دلیل:
- تنظیم NAT فقط برای (192.168.100.2) PC1 اعمال شده است.
- آدرس (192.168.100.129) PC2 در جدول NAT وجود ندارد، بنابراین ترجمه نشده و بسته‌ها با آدرس خصوصی به ISP می‌رسند.
- ISP نمی‌تواند به آدرس خصوصی پاسخ دهد (عدم مسیریابی در اینترنت).



**سوال 3:** با استفاده از دستور

Show ip nat translations

جدول NAT در RouterA را مشاهده کنید و آن را شرح دهید.

**جواب:** شرح جدول NAT نمایش داده شده در خروجی دستور show ip nat translations :

9. ساختار جدول NAT :

- جدول فوق ترجمه‌های NAT فعال روی روتر را نشان می‌دهد که شامل نگاشت بین آدرس‌های Inside Local (خصوصی) و Inside Global (عمومی) است.
- هر سطر مربوط به یک اتصال ICMP مانند Ping است که از دستگاه داخل شبکه (192.168.100.2) به مقصد خارجی (200.152.200.1) برقرار شده است.

10. ستون‌های جدول و تفسیر آنها:

- Pro: پروتکل مورد استفاده (در اینجا icmp برای Ping)
- Inside Global: آدرس عمومی ترجمه‌شده (200.152.200.1) + شماره پورت/شناسه ICMP
- Inside Local: آدرس خصوصی دستگاه مبدأ (192.168.100.2) + شماره پورت/شناسه ICMP متناظر.
- Outside Local & Outside Global: آدرس مقصد (در اینجا 200.152.200.1) که یکسان است، زیرا NAT فقط روی آدرس مبدأ اعمال شده است.

11. نتیجه‌گیری از داده‌ها:

- ترجمه‌ها مربوط به (192.168.100.2) PC1 هستند که به آدرس عمومی 200.152.200.1 نگاشت شده اند.
- شماره‌های پورت/شناسه ICMP (مثلاً 10 تا 30) نشان‌دهنده اتصالات متعدد Ping از PC1 است.
- این جدول تأیید می‌کند که تنها PC1 می‌تواند با خارج ارتباط برقرار کند (مطابق تنظیم Static NAT در سوال ۲)

```

Router2
Physical Config CLI Attributes
IOS Command Line Interface
Router#
Router#show ip nat translation
^
% Invalid input detected at '^' marker.

Router#
Router#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 200.152.200.1:10 192.168.100.2:10 200.152.200.1:10 200.152.200.1:10
icmp 200.152.200.1:11 192.168.100.2:11 200.152.200.1:11 200.152.200.1:11
icmp 200.152.200.1:12 192.168.100.2:12 200.152.200.1:12 200.152.200.1:12
icmp 200.152.200.1:13 192.168.100.2:13 200.152.200.1:13 200.152.200.1:13
icmp 200.152.200.1:14 192.168.100.2:14 200.152.200.1:14 200.152.200.1:14
icmp 200.152.200.1:15 192.168.100.2:15 200.152.200.1:15 200.152.200.1:15
icmp 200.152.200.1:16 192.168.100.2:16 200.152.200.1:16 200.152.200.1:16
icmp 200.152.200.1:17 192.168.100.2:17 200.152.200.1:17 200.152.200.1:17
icmp 200.152.200.1:18 192.168.100.2:18 200.152.200.1:18 200.152.200.1:18
icmp 200.152.200.1:19 192.168.100.2:19 200.152.200.1:19 200.152.200.1:19
icmp 200.152.200.1:20 192.168.100.2:20 200.152.200.1:20 200.152.200.1:20
icmp 200.152.200.1:21 192.168.100.2:21 200.152.200.1:21 200.152.200.1:21
icmp 200.152.200.1:22 192.168.100.2:22 200.152.200.1:22 200.152.200.1:22
icmp 200.152.200.1:23 192.168.100.2:23 200.152.200.1:23 200.152.200.1:23
icmp 200.152.200.1:24 192.168.100.2:24 200.152.200.1:24 200.152.200.1:24
icmp 200.152.200.1:25 192.168.100.2:25 200.152.200.1:25 200.152.200.1:25
icmp 200.152.200.1:26 192.168.100.2:26 200.152.200.1:26 200.152.200.1:26
icmp 200.152.200.1:27 192.168.100.2:27 200.152.200.1:27 200.152.200.1:27
icmp 200.152.200.1:28 192.168.100.2:28 200.152.200.1:28 200.152.200.1:28
icmp 200.152.200.1:29 192.168.100.2:29 200.152.200.1:29 200.152.200.1:29
icmp 200.152.200.1:30 192.168.100.2:30 200.152.200.1:30 200.152.200.1:30
--More--
Copy Paste
Top

```

### مکانیسم NAT پویا:

**سوال 4:** لیستی را که توسط کد زیر ایجاد کرده ایم چه نقشی دارد، توضیح دهید.

access-list 1 permit 192.168.1.0 0.0.0.255

**جواب:** این دستور یک لیست دسترسی استاندارد (Standard ACL) با شماره ۱ ایجاد می‌کند که به شرح زیر عمل می‌کند:

12. مجوز دسترسی (Permit):

○ دستگاه‌هایی که آدرس IP آنها در محدوده 192.168.1.0 تا 192.168.1.255 قرار دارد، اجازه دسترسی می‌دهد.

13. ماسک معکوس (Wildcard Mask):

○ 0.0.0.255 نشان می‌دهد که ۳ بایت اول آدرس IP ثابت هستند (یعنی 192.168.1) و بایت آخر می‌تواند هر مقداری داشته باشد (از ۰ تا 255)

14. کاربرد در NAT (ترجمه آدرس شبکه):

○ این لیست دسترسی معمولاً در تنظیمات NAT پویا یا PAT استفاده می‌شود تا مشخص کند کدام آدرس‌های داخلی

اجازه ترجمه به آدرس عمومی را دارند.

○ مثلاً در دستور ip nat inside source list 1 pool ABC، این لیست تعیین می‌کند که فقط دستگاه‌های با

آدرس 192.168.1.x می‌توانند از NAT استفاده کنند.

**سوال 5:** کد استفاده شده برای ایجاد pool را که در زیر آورده شده است را توضیح دهید.

ip nat pool abc 200.1.1.3 200.1.1.5 netmask 255.255.255.0

**جواب:** این دستور یک پول (مخزن) آدرس عمومی برای استفاده در NAT پویا روی روتر ایجاد می‌کند. اجزای آن به شرح زیر است:

اجزای دستور و معنی آنها:

15. ip nat pool abc:

○ ایجاد یک پول NAT با نام abc (نام انتخابی برای شناسایی پول)

200.1.1.3 200.1.1.5 16:

○ محدوده آدرس‌های عمومی قابل استفاده برای ترجمه:

▪ شروع 200.1.1.3

▪ پایان 200.1.1.5

○ یعنی ۳ آدرس عمومی در این پول وجود دارد که می‌توانند به دستگاه‌های داخلی اختصاص یابند.

17. 255.255.255.0 netmask:

○ سابنت ماسک شبکه مربوط به آدرس‌های عمومی (در اینجا 24/)

این پول به روتر می‌گوید که می‌تواند آدرس‌های داخلی مثلاً 192.168.1.x را به یکی از آدرس‌های عمومی موجود در پول 200.1.1.3 تا 200.1.1.5 ترجمه کند.

**سوال 6:** در ترمینال تمامی PC ها کد زیر را اجرا کنید، چرا یکی از این PC ها قابلیت Ping کردن ندارد؟

ping -t 8.8.8.8

**جواب:** علت عدم موفقیت یکی از PC ها در Ping کردن 8.8.8.8 :

PC های دارای دسترسی:

▪ آدرس‌های 192.168.1.2 تا 192.168.1.5 طبق جدول می‌توانند 8.8.8.8 را Ping کنند، زیرا:

▪ در لیست دسترسی 1 access-list مجاز هستند.

▪ آدرس‌هایشان به یکی از آدرس‌های پول NAT (200.1.1.3 تا 200.1.1.5) ترجمه می‌شود.

PC فاقد دسترسی:

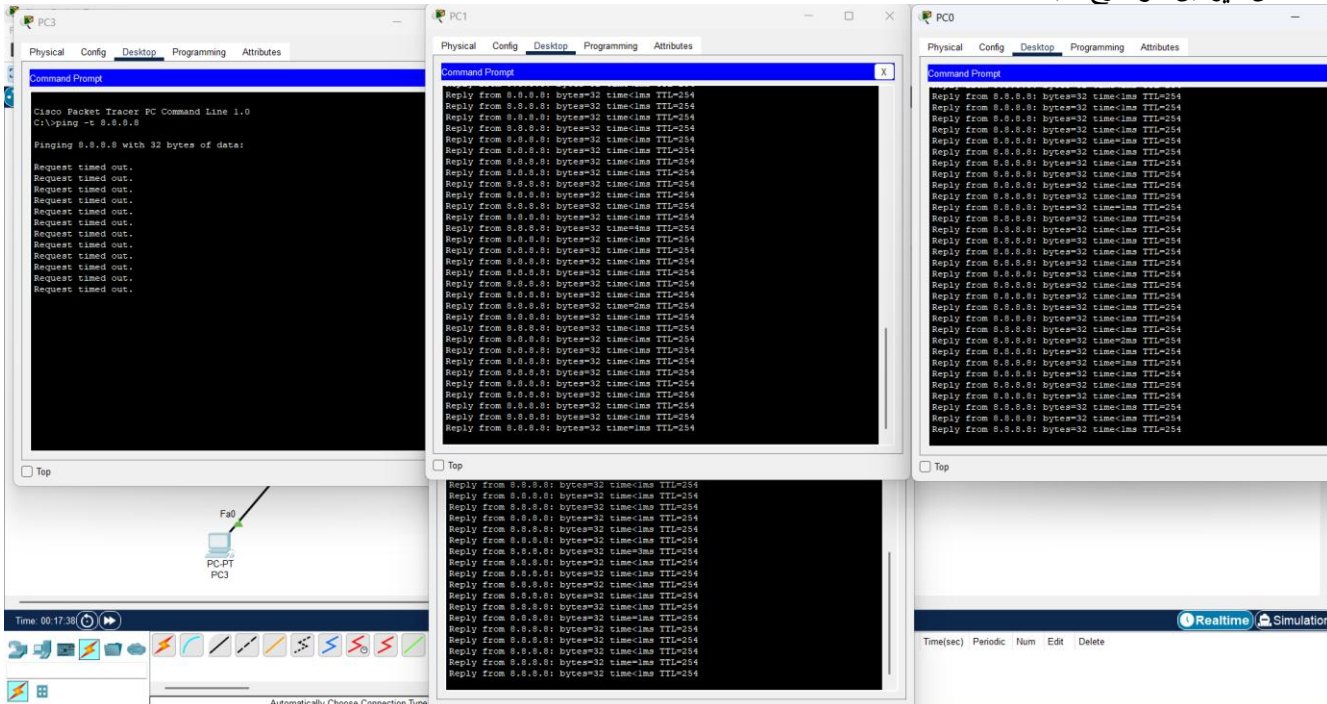
▪ اگر یکی از PC ها مثلاً 192.168.1.5 نتواند Ping کند، به دلیل زیر است:

▪ تمام آدرس‌های پول NAT اشغال شده‌اند (تنها ۳ آدرس عمومی موجود است).

دلیل اصلی محدودیت در تعداد آدرس‌های عمومی پول NAT است.

برای رفع این مشکل، یا باید آدرس‌های عمومی بیشتری تعریف کرد یا از PAT استفاده نمود.

در عکس زیر این موضوع قابل مشاهده است:



**مکانیسم PAT:**

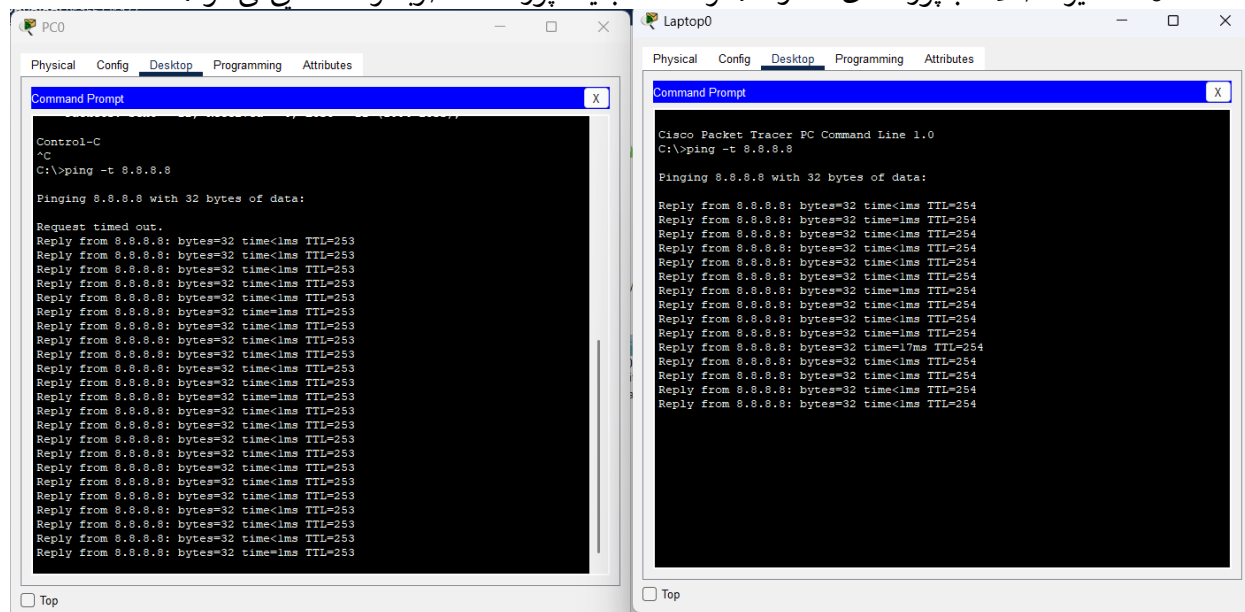
**سوال 7:** بین لپ تاب ها و کامپیوتر ها مسیریاب ISP را Ping کنید. چه اتفاقی می‌افتد؟

- جواب:** نتایج Ping از لپ‌تاپ‌ها و کامپیوترها به: (8.8.8.8) ISP
- تمام دستگاه‌ها PC ها و لپ‌تاپ‌ها می‌توانند ISP را Ping کنند.
  - دلیل موفقیت:

○ PAT با دستور overload روی اینترفیس خارجی (f0/1) فعال شده است:

ip nat inside source list 1 interface f0/1 overload

- آدرس داخلی 192.168.1.0/24 و 192.168.2.0/24 به آدرس عمومی اینترفیس f0/1 مثلاً 200.1.1.1 ترجمه.
- تمایز اتصالات با پورت‌های متفاوت: هر دستگاه با یک پورت منحصر به فرد شناسایی می‌شود.



**سوال 8:** با استفاده از دستور

show ip nat translations

جدول NAT را مشاهده کنید و با آزمایش قبلی مقایسه کنید.

**جواب:** مقایسه جدول NAT در آزمایش PAT (سناریوی شکل ۴) با آزمایش NAT پویا سوال ۶:

ویژگی	NAT پویا (آزمایش قبلی)	PAT (آزمایش فعلی)
تعداد آدرس‌های عمومی	محدود (مثلاً ۳ آدرس در پول abc)	یک آدرس عمومی (مثلاً اینترفیس f0/1)
شناسایی دستگاه‌ها	با آدرس IP عمومی متفاوت	با پورت‌های منحصر به فرد روی یک آدرس مشترک
نمونه جدول NAT	Inside Global: آدرس‌های مختلف مثلاً 200.1.1.3	Inside Global: آدرس یکسان + پورت مثلاً 200.1.1.1:1234
محدودیت اتصال پیکربندی	حداکثر به تعداد آدرس‌های پول ip nat pool abc ... + ip nat inside source list 1 pool abc	بی‌نظیر (پورت‌های ۱۶ ~ bit-۶۵۵۳۶ اتصال) ip nat inside source list 1 interface f0/1 overload

نتیجه‌گیری:

- PAT کارایی بهتری دارد زیرا با یک آدرس عمومی، همه دستگاه‌ها می‌توانند همزمان به اینترنت متصل شوند.
  - NAT پویا برای شبکه‌های کوچک با آدرس‌های عمومی کافی مناسب است.
- در عکس زیر خروجی قابل مشاهده است:



```

Router1
Physical Config CLI Attributes
IOS Command Line Interface
% Invalid input detected at '^' marker.
R2(config-router)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 200.1.1.1:1024 192.168.2.2:143 8.8.8.8:143 8.8.8.8:1024
icmp 200.1.1.1:1025 192.168.2.2:144 8.8.8.8:144 8.8.8.8:1025
icmp 200.1.1.1:1026 192.168.2.2:145 8.8.8.8:145 8.8.8.8:1026
icmp 200.1.1.1:1027 192.168.2.2:146 8.8.8.8:146 8.8.8.8:1027
icmp 200.1.1.1:1028 192.168.2.2:147 8.8.8.8:147 8.8.8.8:1028
icmp 200.1.1.1:1029 192.168.2.2:148 8.8.8.8:148 8.8.8.8:1029
icmp 200.1.1.1:1030 192.168.2.2:149 8.8.8.8:149 8.8.8.8:1030
icmp 200.1.1.1:1031 192.168.2.2:150 8.8.8.8:150 8.8.8.8:1031
icmp 200.1.1.1:1032 192.168.2.2:151 8.8.8.8:151 8.8.8.8:1032
icmp 200.1.1.1:1033 192.168.2.2:152 8.8.8.8:152 8.8.8.8:1033
icmp 200.1.1.1:1034 192.168.2.2:93 8.8.8.8:93 8.8.8.8:1034
icmp 200.1.1.1:1035 192.168.2.2:94 8.8.8.8:94 8.8.8.8:1035
icmp 200.1.1.1:1036 192.168.2.2:95 8.8.8.8:95 8.8.8.8:1036
icmp 200.1.1.1:1037 192.168.2.2:96 8.8.8.8:96 8.8.8.8:1037
icmp 200.1.1.1:1038 192.168.2.2:97 8.8.8.8:97 8.8.8.8:1038
icmp 200.1.1.1:1039 192.168.2.2:98 8.8.8.8:98 8.8.8.8:1039
icmp 200.1.1.1:1040 192.168.2.2:99 8.8.8.8:99 8.8.8.8:1040
icmp 200.1.1.1:1041 192.168.2.2:100 8.8.8.8:100 8.8.8.8:1041
icmp 200.1.1.1:1042 192.168.2.2:101 8.8.8.8:101 8.8.8.8:1042
icmp 200.1.1.1:1043 192.168.2.2:102 8.8.8.8:102 8.8.8.8:1043
icmp 200.1.1.1:1044 192.168.2.2:103 8.8.8.8:103 8.8.8.8:1044
--More--
Copy Paste
☐ Top

```

## DHCP پروتکل:

**سوال 9:** دلیل استفاده از 2 دستور زیر را توضیح دهید.

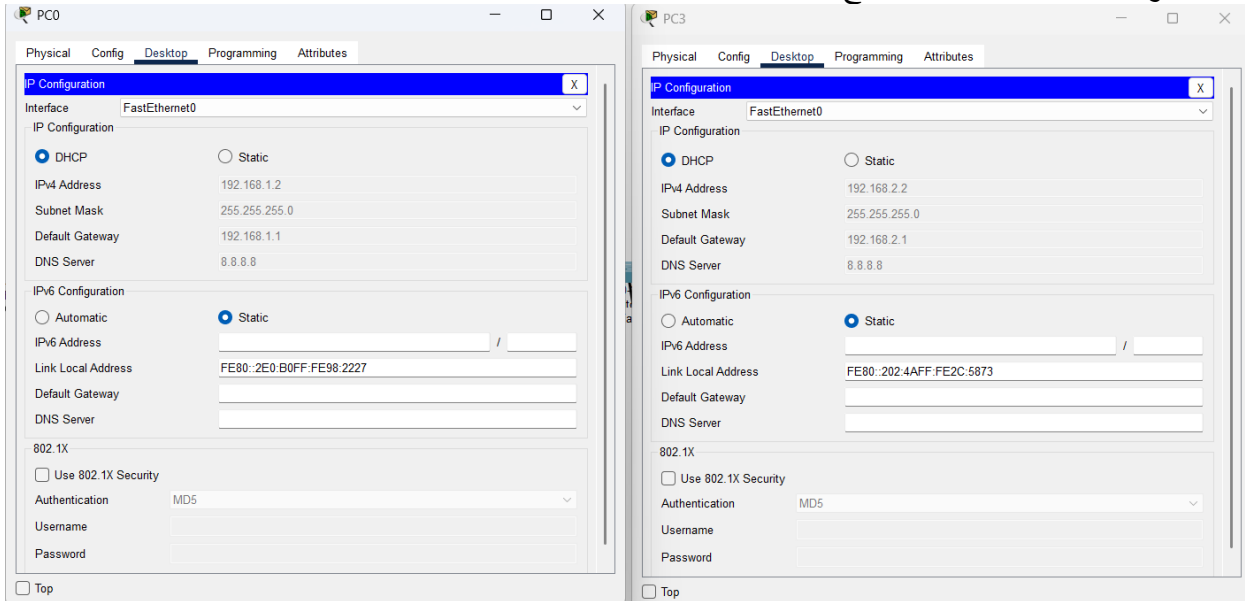
ip dhcp excluded-address 192.168.1.1

ip dhcp excluded-address 192.168.2.1

**جواب:** دلیل استفاده از دستورات ip dhcp excluded-address برای آدرس های 192.168.1.1 و 192.168.2.1:

- هدف اصلی این دستورات:
    - ممانعت از اختصاص خودکار آدرس های مشخص شده به دستگاه های متصل به شبکه توسط DHCP
    - این آدرس ها معمولاً برای راه اندازی دستی (Static) روی دستگاه های حیاتی مانند روترها، سوئیچ ها، یا سرورها رزرو می شوند.
  - توضیح دستورات:
    - ip dhcp excluded-address 192.168.1.1: آدرس 192.168.1.1 گیت وی پیش فرض شبکه 192.168.1.0/24 را از DHCP حذف می کند.
    - ip dhcp excluded-address 192.168.2.1: آدرس 192.168.2.1 گیت وی شبکه 192.168.2.0/24 را نیز از DHCP خارج می کند.
  - چرا این آدرس ها باید حذف شوند؟
    - پیشگیری از تداخل آدرس IP: اگر DHCP سرور یکی از این آدرس ها را به دستگاه ای اختصاص دهد، گیت وی شبکه غیر قابل دسترس می شود.
    - دستگاه های حیاتی: روترها و سوئیچ ها معمولاً آدرس ثابت (Static IP) دارند تا همیشه در دسترس باشند.
- سوال 10:** وارد قسمت تنظیمات IP هر کدام از PC ها بشوید، آیا dhcp به درستی IP های مورد نیاز را اختصاص می دهد؟ گزارش دهید.
- جواب:** در عکس زیر قابل مشاهده است که:
- DHCP به درستی کار می کند و IP ها را مطابق پیکربندی اختصاص می دهد.
  - تمامی دستگاه ها آدرس IP، گیت وی، و DNS را دریافت کرده اند.

- آدرس‌های رزرو شده مانند 192.168.1.1 و 192.168.2.1 به دستگاه‌های دیگر اختصاص نیافته‌اند که این اتفاق مطابق دستورات excluded-address رخ داده است.



**سوال 11:** آیا ارتباط بین کامپیوترها موجود است؟ برای این کار در PC3 کد زیر را وارد کنید.

ping 192.168.1.2

**جواب:** ارتباط موفقیت‌آمیز است (پکت‌های ارسالی پاسخ دریافت کرده‌اند)

