فرم گزارش کار آزمایشگاه شبکه

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 براي استفاده از سرویس هاي اینترنت بررسی عملکرد و پیکربندي مکانیسم NAT،PAT و پروتکل DHCP				
ابزارهای مورد نیاز	Cisco Packet Tracer				

شرح آزمایش

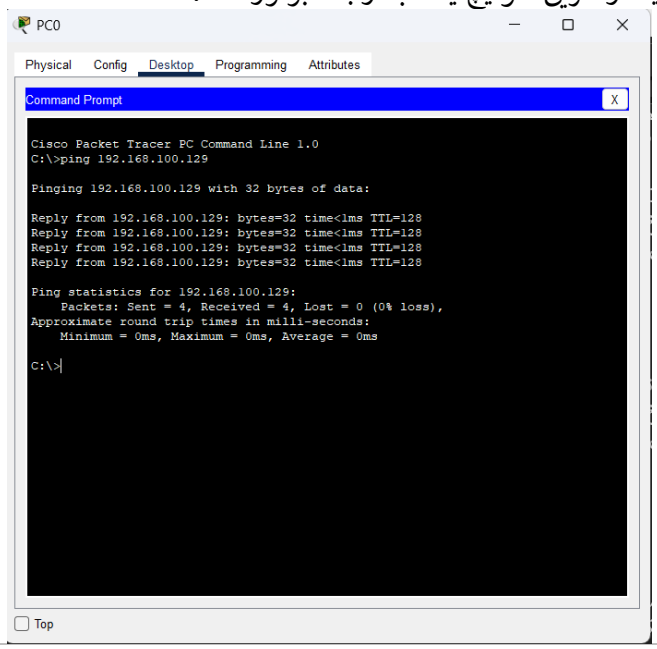
مکانیسم NAT ایستا :

سوال 1: واسط هاي دستگاهها مطابق آدرس هاي 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؟

جواب:

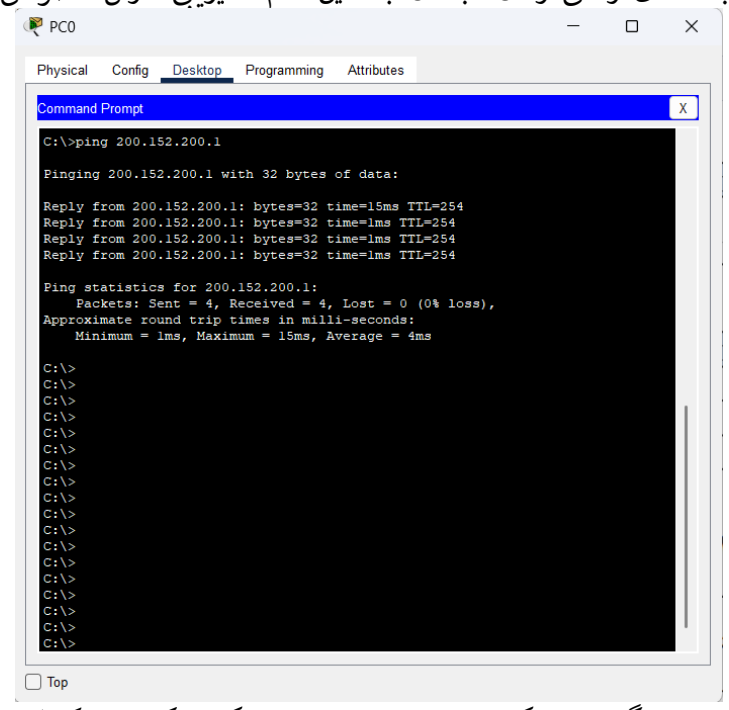
آیا PC1و PC2می‌توانند یکدیگر را Pingکنند؟

1. پاسخ :بله، PC1 و PC2 می‌توانند یکدیگر را Ping کنند.
2. دلیل:
   - هر دو دستگاه PC1 با آدرس 192.168.100.2 و PC2 با آدرس 192.168.100.129 در یک شبکه محلی(LAN) با subnet mask 255.255.255.0 قرار دارند.
   - از آنجا که آدرس‌های 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.



آیا از PC1 می‌توان ISP را Ping کرد؟

3. پاسخ :خیر، PC1نمی‌تواند ISP را Ping کند (مگر پس از تنظیمNAT)
4. دلیل:
   - آدرس ISP (25.16.59.1) 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 برای زمانی است که شبکه بنده تکمیل شده
و مکانیسم NAT روی ان پیاده سازی شده است.)

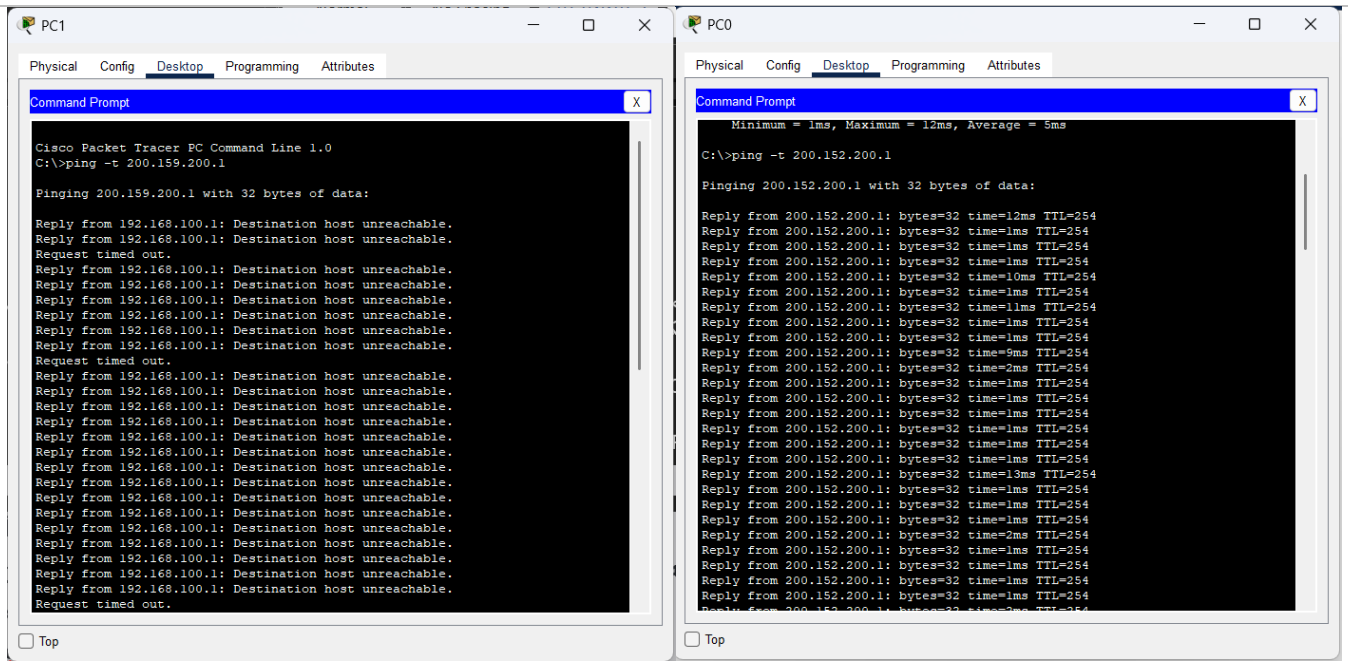
سوال 2: در محیط تنظیم عمومی مسیریاب RouterA دستور زیر را وارد کنید. با استفاده از این دستور صرفا آدرس IPمبدا در بسته خروجی از شبکه تغییر میکند.

ip nat inside source static 192.168.100.2 200.152.200.1

•از PC1وPC2مسیریاب ISPرا Pingکنید. چه اتفاق میافتد؟

جواب:

5. PC1 می‌تواند ISP را Ping کند.
6. دلیل:
   - آدرس (PC1) 192.168.100.2 به 200.152.200.1 ترجمه می‌شود.
   - ISP آدرس مبدأ را به عنوان 200.152.200.1می‌بیند (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 (PC2) 192.168.100.129در 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).



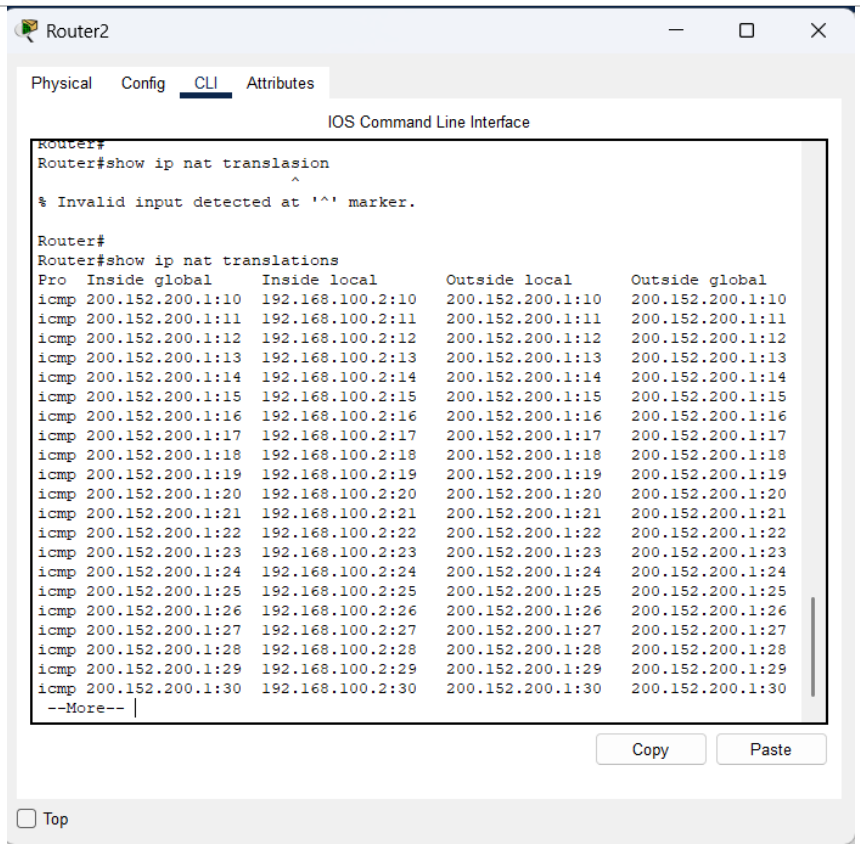
سوال 3: با استفاده از دستور

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 جدولNAT :
   - 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 200.152.200.1نگاشت 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)



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 شماره‌ی 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 براي ايجاد 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)

16. 200.1.1.5 200.1.1.3:
   - 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. netmask 255.255.255.0:
   - سابنت ماسک شبکه مربوط به آدرس‌های عمومی (در اینجا 24/)

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

سوال 6: در ترمینال تمامی PCها کد زیر را اجرا کنید، چرا یکی از این PCها قابلیت Pingکردن ندارد؟

ping -t 8.8.8.8

جواب: علت عدم موفقیت یکی ازPC 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 access-list 1مجاز هستند.
  - آدرس‌هایشان به یکی از آدرس‌های پول NAT (200.1.1.3 تا 200.1.1.5) ترجمه می‌شود.

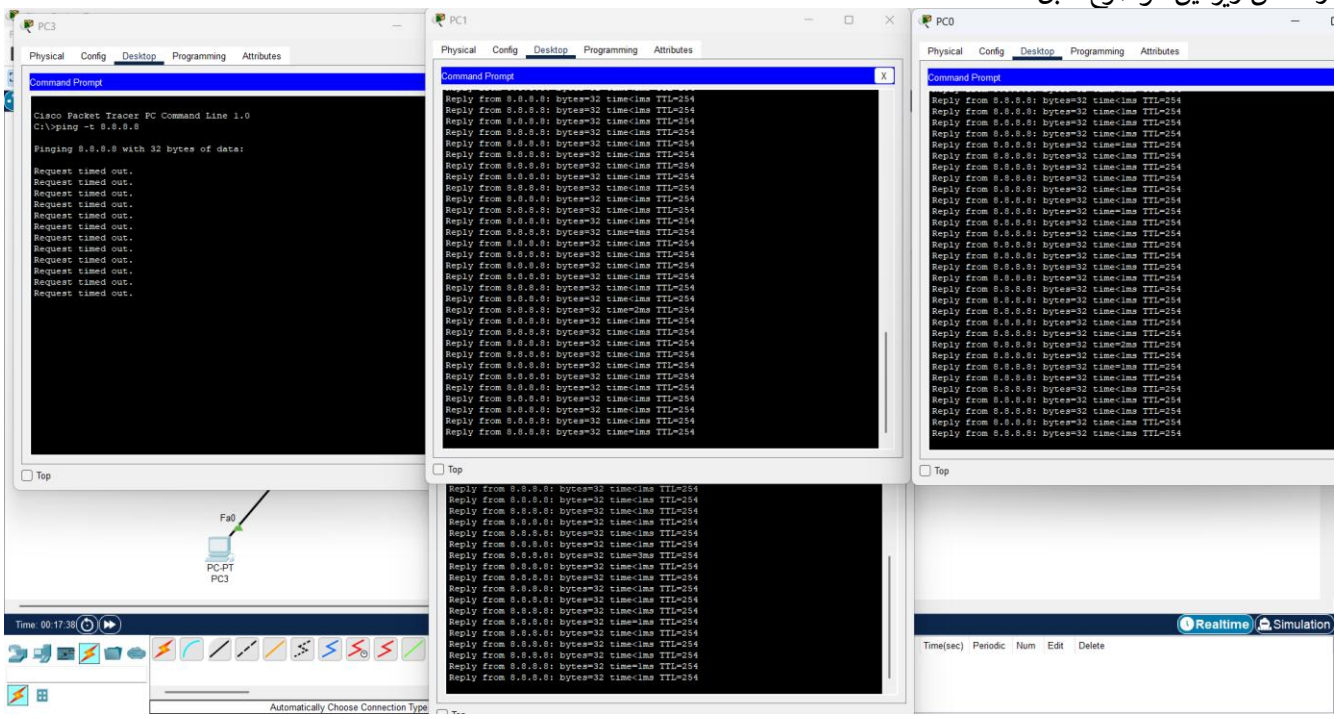
PC فاقد دسترسی:

- اگر یکی ازPC 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:

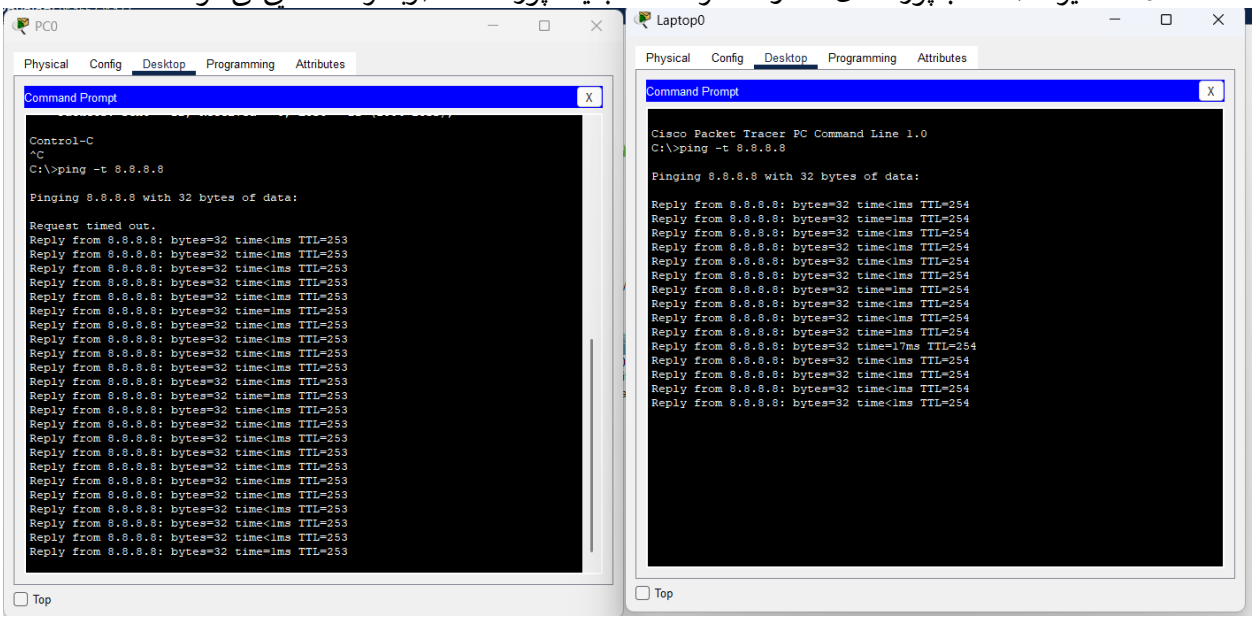
سوال 7: بین لپ تاپ ها و کامپیوتر ها مسیریاب ISPرا Pingکنید. چه اتفاق میافتد؟

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:
  - PATبا دستور overloadروی 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 منحصربه‌فرد شناسایی می‌شود.



سوال 8: با استفاده از دستور

show ip nat translations

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

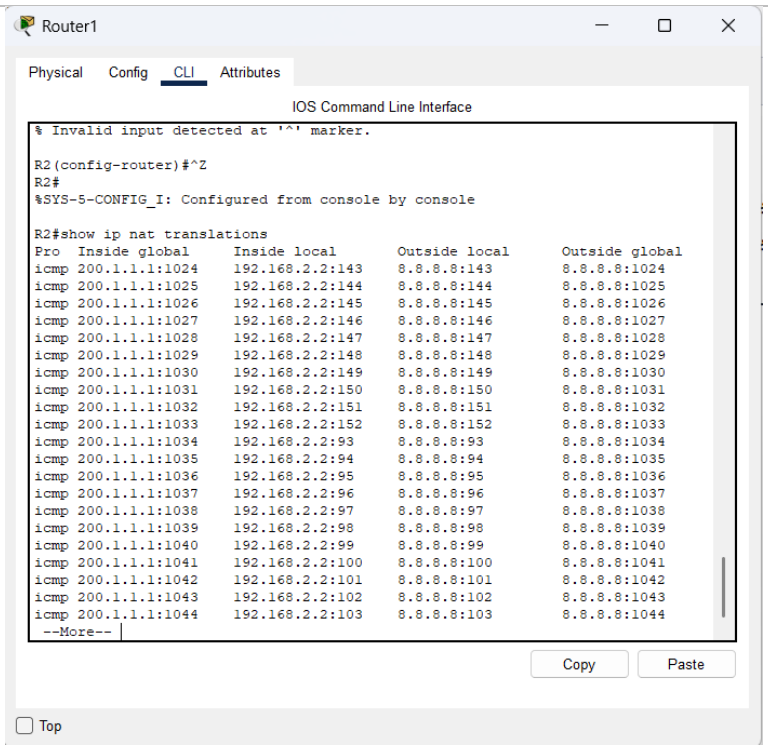
جواب: مقایسه جدول NAT در آزمایش PAT (سناریوی شکل ۴) با آزمایش NAT پویا سوال ۶:

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 منحصربه‌فرد 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	حداکثر به تعداد آدرس‌های پول	بی‌نظیر (پورت‌های ۱۶ ~ ۶۵۵۳۶-bit اتصال)
پیکربندی	ip nat pool abc ... + ip nat inside source list 1 pool abc	ip nat inside source list 1 interface f0/1 overload

نتیجه‌گیری:

- PATکارایی بهتری دارد زیرا با یک آدرس عمومی، همه دستگاه‌ها می‌توانند همزمان به اینترنت متصل شوند.
- NATپویا برای شبکه‌های کوچک با آدرس‌های عمومی کافی مناسب است.

در عکس زیر خروجی قابل مشاهده است:



DHCP پروتکل:

سوال 9: دلیل استفاده از 2دستور 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 آدرس‌های 192.168.1.1 و 192.168.2.1:

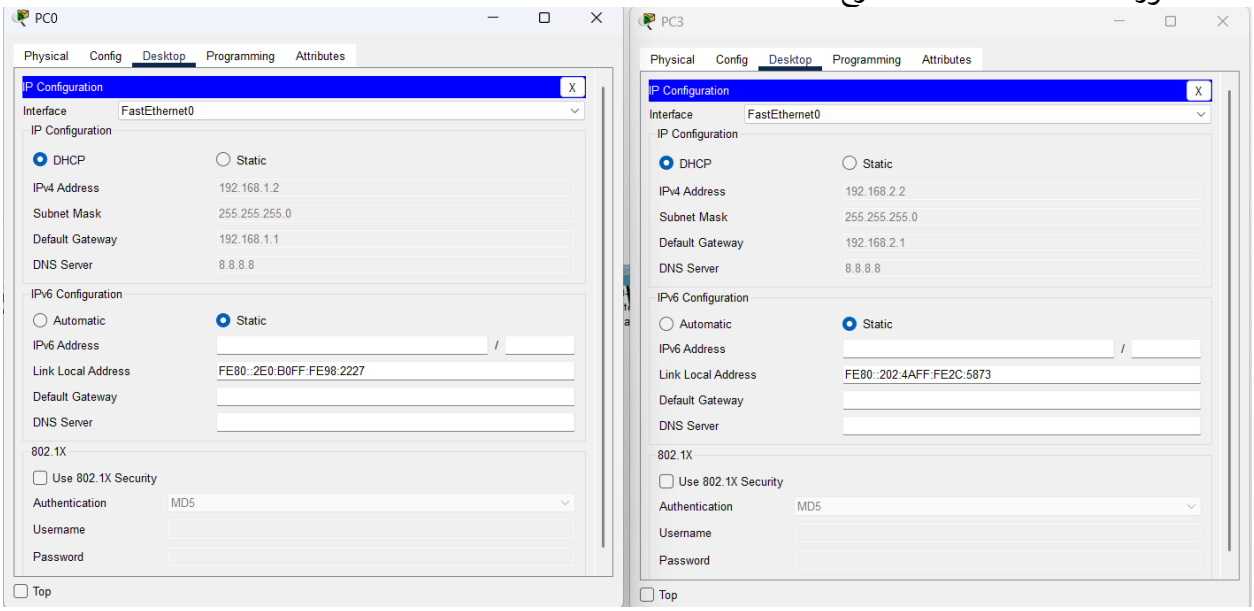
1. هدف اصلی این دستورات:
   - ممانعت از اختصاص خودکار آدرس‌های مشخص شده به دستگاه‌های متصل به شبکه توسط DHCP
   - این آدرس‌ها معمولاً برای راه‌اندازی دستی (Static) روی دستگاه‌های حیاتی مانند روترها، سوئیچ‌ها، یا سرورها رزرو می‌شوند.
2. توضیح دستورات:
   - ip dhcp excluded-address 192.168.1.1:
     - آدرس 192.168.1.1 گیت‌وی پیش‌فرض شبکه 192.168.1.0/24 را از DHCP حذف می‌کند.
   - ip dhcp excluded-address 192.168.2.1:
     - آدرس 192.168.2.1 گیت‌وی شبکه 192.168.2.0/24 را نیز از DHCP خارج می‌کند.
3. چرا این آدرس‌ها باید حذف شوند؟
   - پیشگیری از تداخل آدرس IP: اگر DHCP سرور یکی از این آدرس‌ها را به دستگاه‌ای اختصاص دهد، گیت‌وی شبکه غیرقابل دسترس می‌شود.
   - دستگاه‌های حیاتی: روترها و سوئیچ‌ها معمولاً آدرس ثابت (Static IP) دارند تا همیشه در دسترس باشند.

سوال 10: وارد قسمت تنظیمات IPهر کدام از PCها بشوید، آیا dhcp به درستی IPهاي مورد نیاز را اختصاص میدهد؟ گزارش دهید.

جواب: در عکس زیر قابل مشاهده است که:

- DHCP به درستی کار می‌کند وIP ها را مطابق پیکربندی اختصاص می‌دهد.
- تمامی دستگاه‌ها آدرس IP ، گیت‌وی، و DNS را دریافت کرده‌اند.

- آدرس‌های رزرو شده مانند 192.168.1.1و 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؟ براي اين كار در PC3كد زير را وارد كنيد.

ping 192.168.1.2

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