به نام خدا

گزارش آزمایش ششم

آزمایشگاه شبکه

مبین قربانی - ۹۹۱۰۹۹۲۵

مهدی شکوفی - ۴۰۱۱۱۰۱۱۵

نیما هنرمند - ۴۰۱۱۰۶۷۰۳

هدف آزمایش

هدف از این آزمایش، آشنایی عملی با مفهوم **Network Address Translation (NAT)** و پیاده‌سازی انواع مختلف آن شامل **Dynamic NAT**، **Static NAT** و **PAT (Port Address Translation)** در یک شبکه‌ی چندبخشی است.
در این آزمایش یاد می‌گیریم چگونه با استفاده از NAT:

- آدرس واقعی سرور را از دید کاربران مخفی کنیم
- از تعداد محدودی IP معتبر برای چندین کاربر استفاده کنیم
- و با استفاده از PAT محدودیت تعداد IP را برطرف نماییم.

مشخصات کلی شبکه

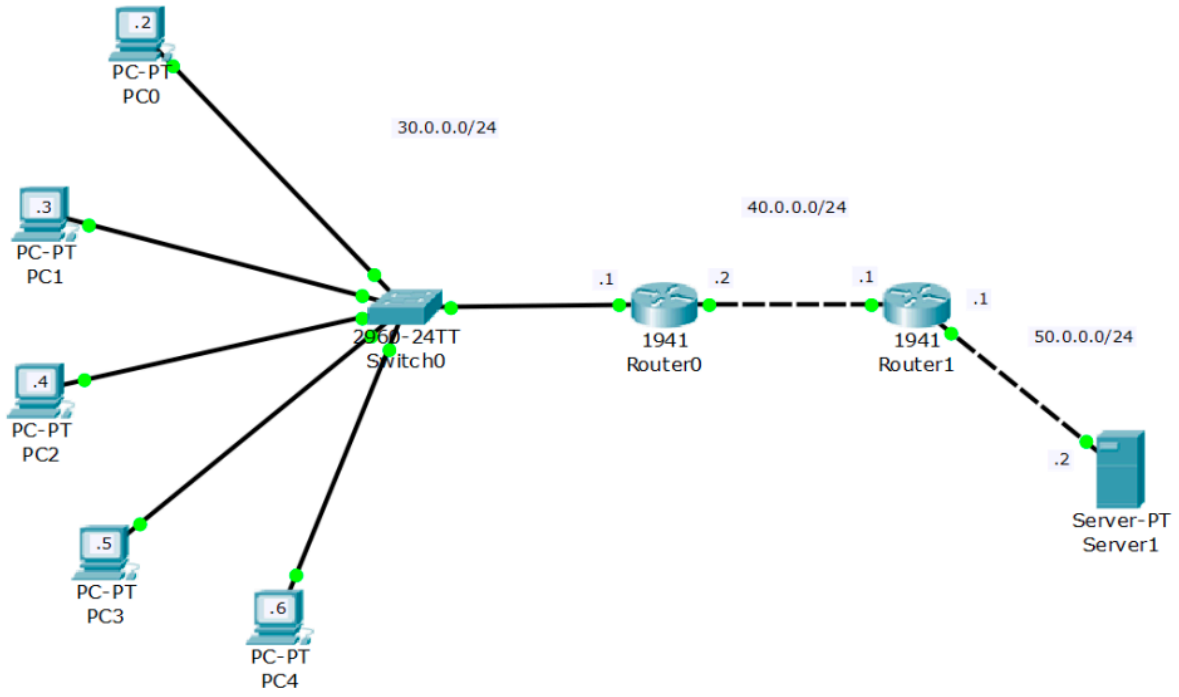
- شبکه کاربران: `30.0.0.0/24`
- لینک بین روترها: `40.0.0.0/24`
- شبکه سرور: `50.0.0.0/24`
- آدرس واقعی سرور: `50.0.0.2`
- آدرس جعلی (نمایشی) سرور: `100.0.0.1`

بخش اول: Static NAT

هدف

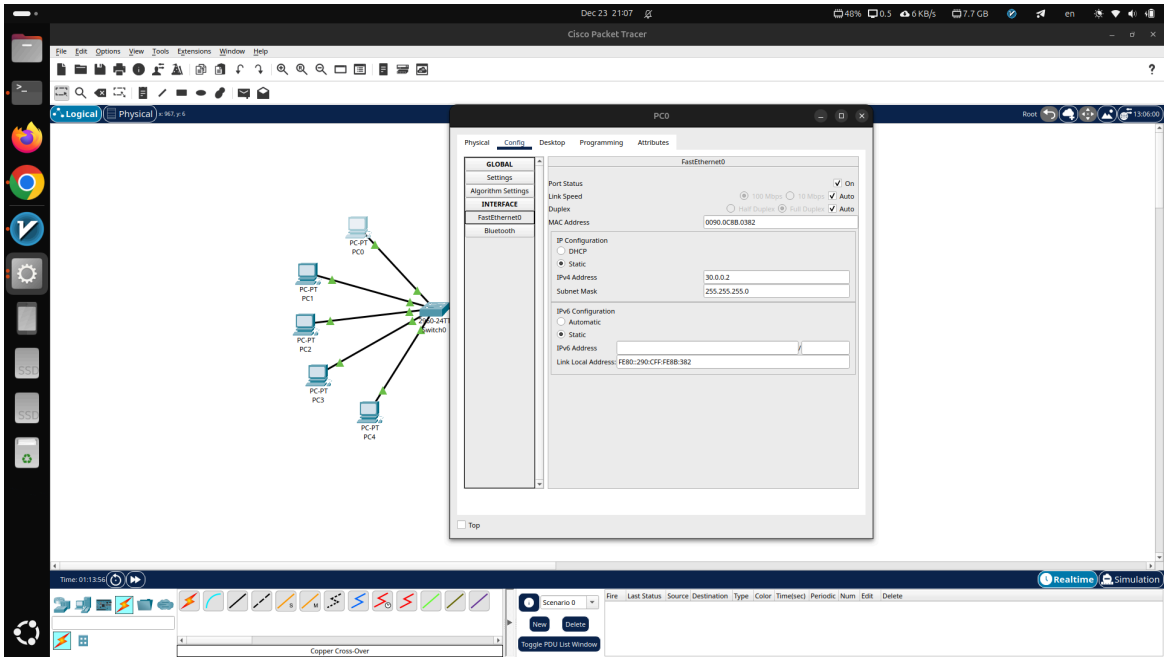
در این بخش هدف این است که کاربران، سرور را فقط با **آدرس جعلی 100.0.0.1** ببینند و به آدرس واقعی 50.0.0.2 دسترسی نداشته باشند.

پس برای شروع ابتدا شبکه مورد نظر (بدون کانفیگ) شامل تمام تجهیزات استفاده شده در سوال را پیاده سازی کردیم :



مراحل انجام کار

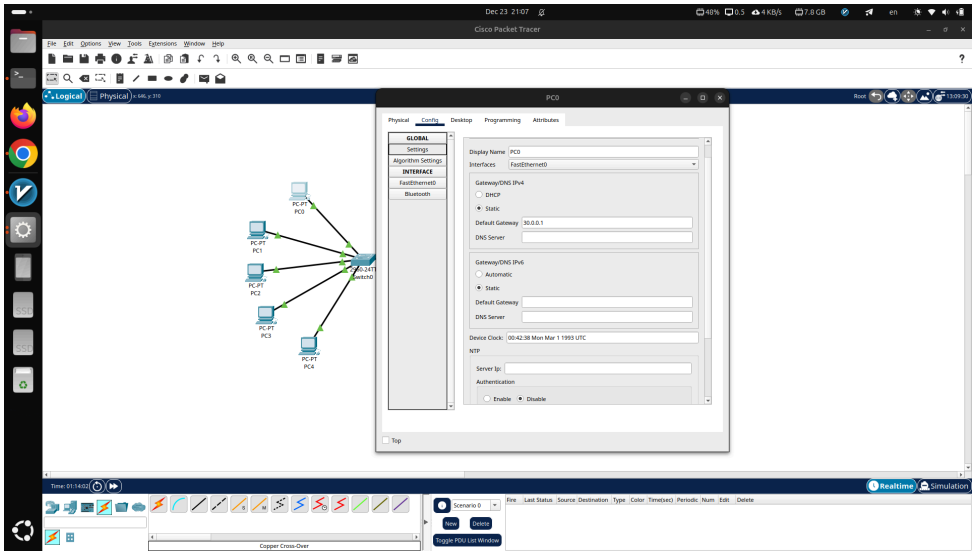
1. ابتدا آدرس های مختلف ۵ سیستم را تنظیم کردیم : `30.0.0.2 - 30.0.0.5`



2. آدرس‌دهی به اینترفیس‌های روترها:

   - Router0 (سمت کاربران): `30.0.0.1`

     یعنی gateway تمام 5 سیستم شد :



- Router0 سمت Router1
  `40.0.0.2`

- Router1 سمت Router0
  `40.0.0.1`

- Router1 (سمت سرور): `50.0.0.1`

3. تنظیم Routing:

طبق دستوراتی که در شرح آزمایش بود عمل کردیم.
روی Router0 فقط مسیر شبکه‌ی جعلی سرور تعریف شد:

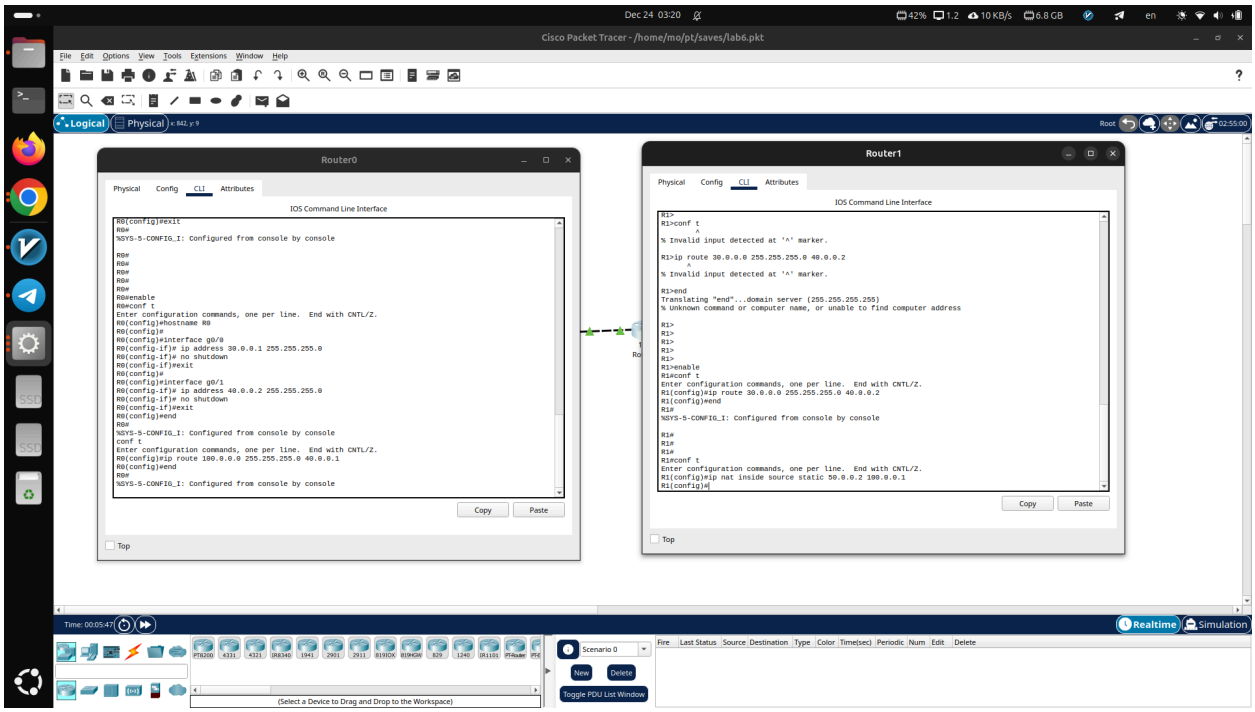
```
ip route 100.0.0.0 255.255.255.0 40.0.0.1
```

روی Router1 مسیر برگشت به کاربران:

```
ip route 30.0.0.0 255.255.255.0 40.0.0.2
```

پیاده‌سازی Static NAT روی Router1:

```
ip nat inside source static 50.0.0.2 100.0.0.1
```

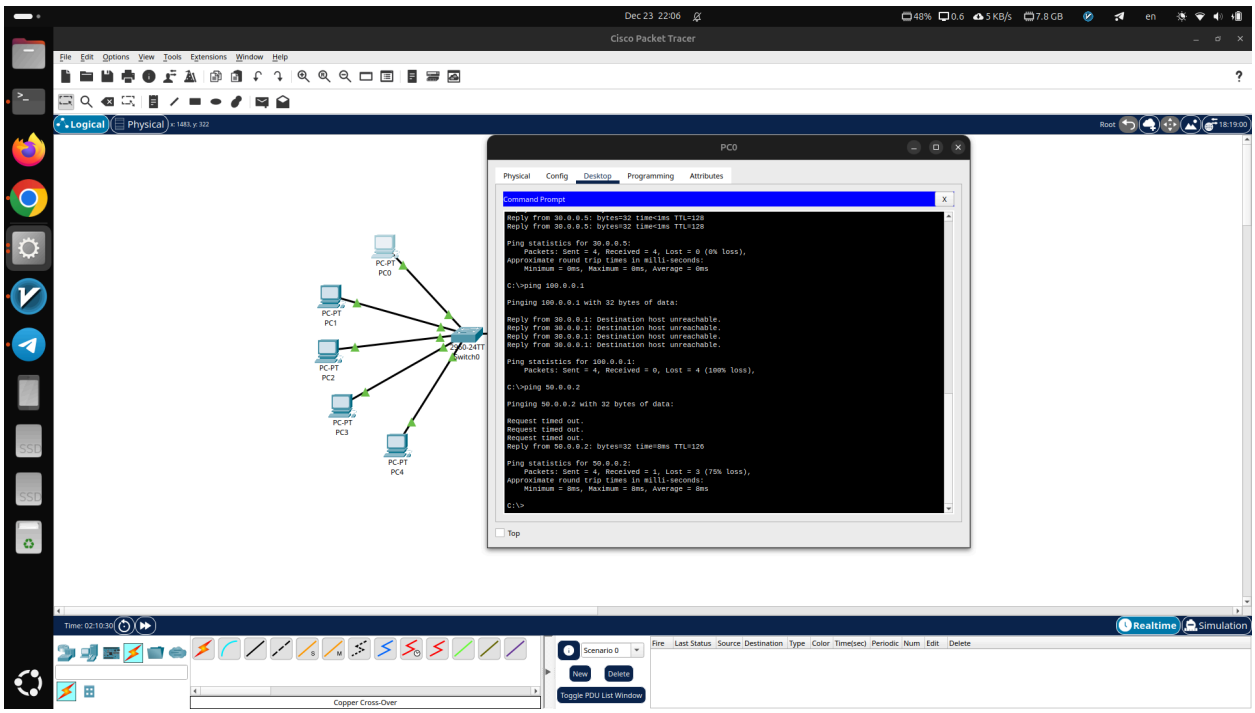


4. تعیین inside و outside:

- اینترفیس سمت سرور: `ip nat inside`
- اینترفیس سمت Router0: `ip nat outside`

نتیجه

- `ping 100.0.0.1` از سمت PCها موفق بود.
- `ping 50.0.0.2` ناموفق شد.
- پس NAT به درستی اعمال شد



همانطور که مشخص است 100.0.0.1 از سمت pc0 در دسترس و 50.0.0.2 اصلا به عنوان آدرس قابل قبول شناخته شده نیست.

بخش دوم: Dynamic NAT

هدف

استفاده از **تعداد محدودی IP معتبر** برای چند کاربر داخلی (نه لزوماً همزمان).

مراحل انجام کار (روی Router0)

تعریف Access List برای کاربران:

```
access-list 1 permit 30.0.0.0 0.0.0.255
```

تعریف NAT Pool:

```
ip nat pool test 40.0.0.3 40.0.0.5 netmask 255.255.255.0
```

فعال‌سازی Dynamic NAT:

```
ip nat inside source list 1 pool test
```

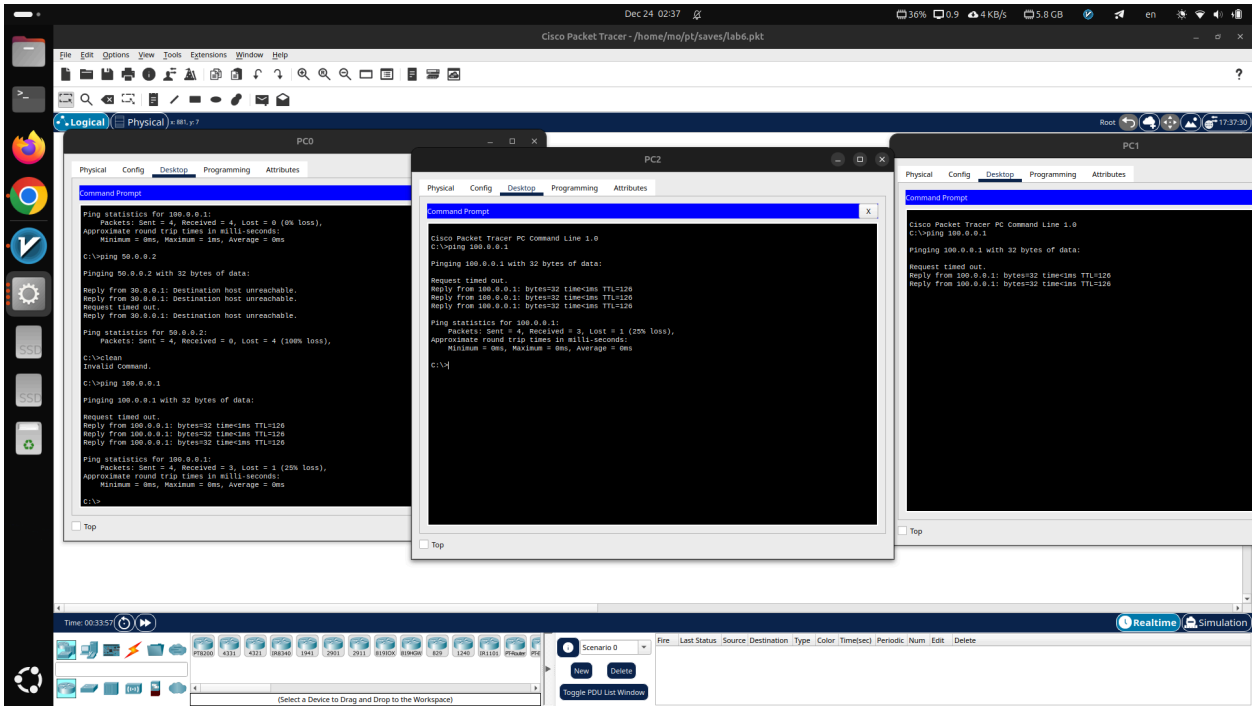
تعیین inside و outside:

1. سمت کاربران: `ip nat inside`
2. سمت Router1: `ip nat outside`

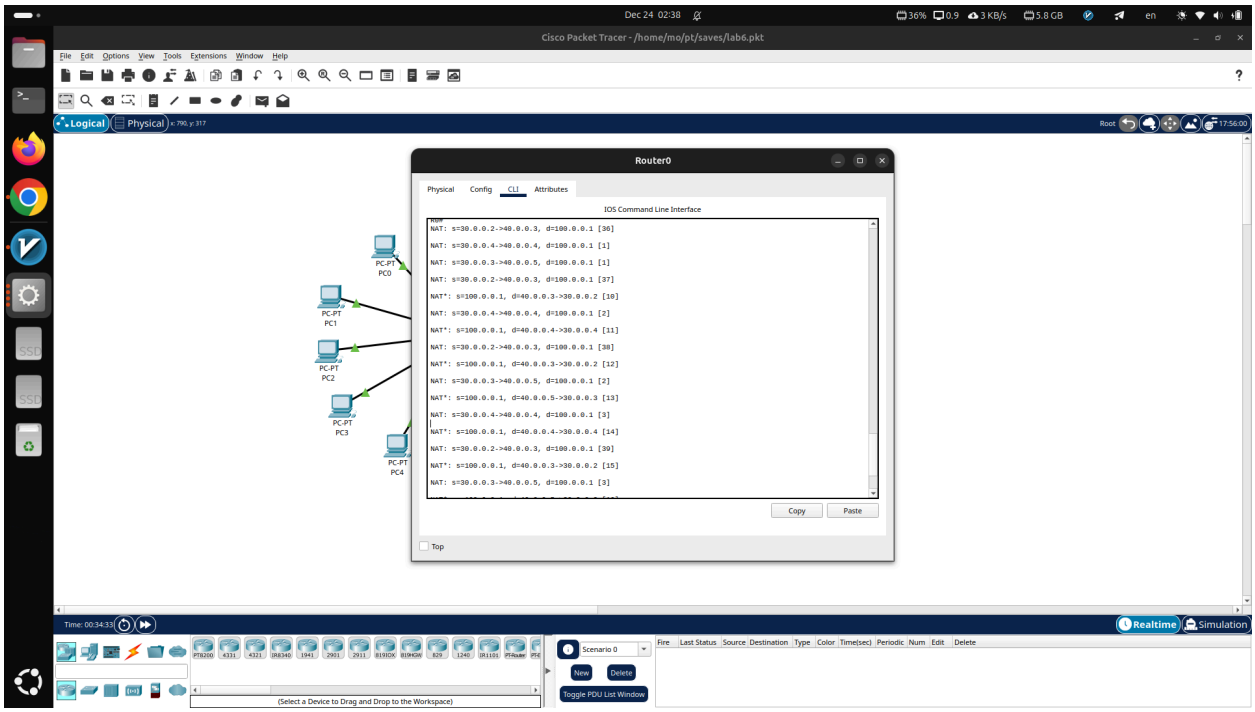
نتیجه

- هر کاربر در زمان ارتباط، یکی از IPهای pool را دریافت می‌کرد.
- در خروجی `debug ip nat` ترجمه‌ی IP کاربران به IPهای `40.0.0.3` تا `40.0.0.5` مشاهده شد.
- محدودیت Dynamic NAT در تعداد اتصال‌های همزمان مشخص شد.

در انتها به طور تقریبا همزمان از سه سیستم مختلف پینگ 100.0.0.1 گرفته شد و نتیجه به خوبی نشان دهنده فعال بودن Dynamic Nat بود



لاگ R0 به صورت زیر بود :



بخش سوم: NAT Overload (PAT)

هدف

رفع محدودیت Dynamic NAT با استفاده از **پورت‌ها** و امکان اتصال همزمان چندین کاربر با یک IP.

مراحل انجام کار (روی Router0)

حذف Dynamic NAT:

```
no ip nat inside source list 1 pool test
```

فعال‌سازی PAT:

```
ip nat inside source list 1 pool test overload
```

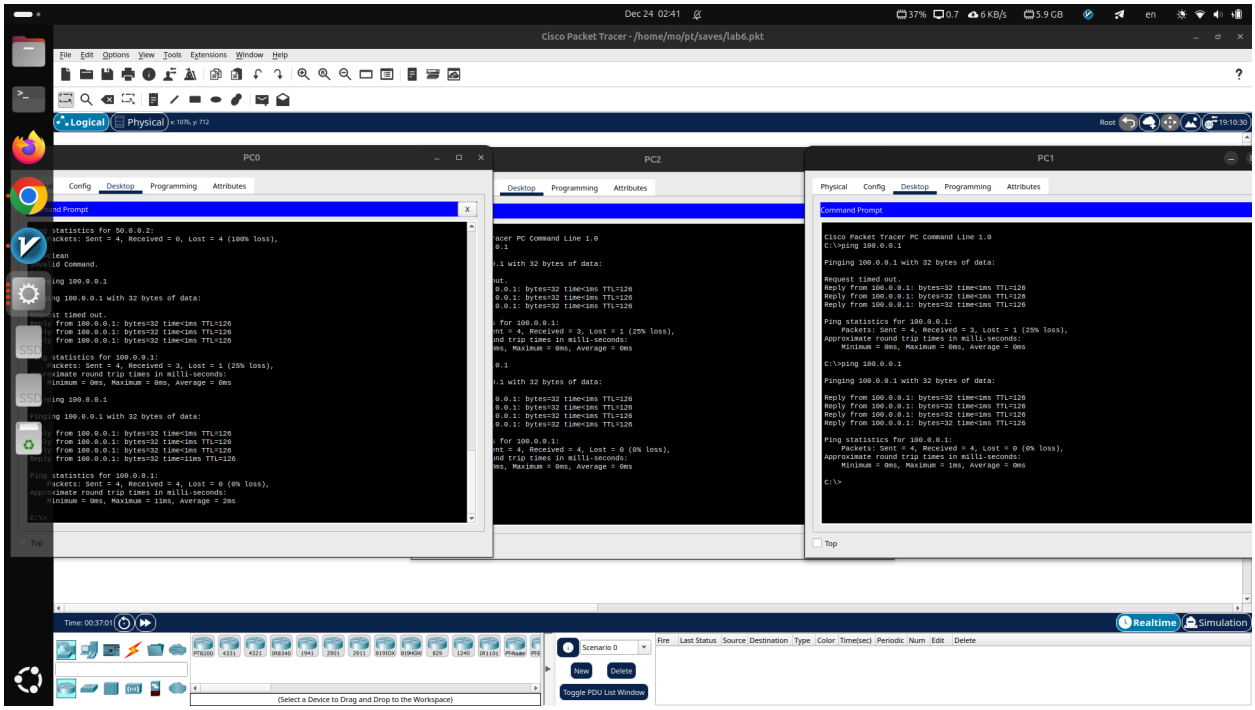
تست با ترافیک HTTP:

- روی سیستم به جای پینگ از وب برازر هم استفاده کردیم و در نهایت با show ip nat خروجی پورت ها را هم داشتیم
- اتصال کاربران به `http://100.0.0.1`

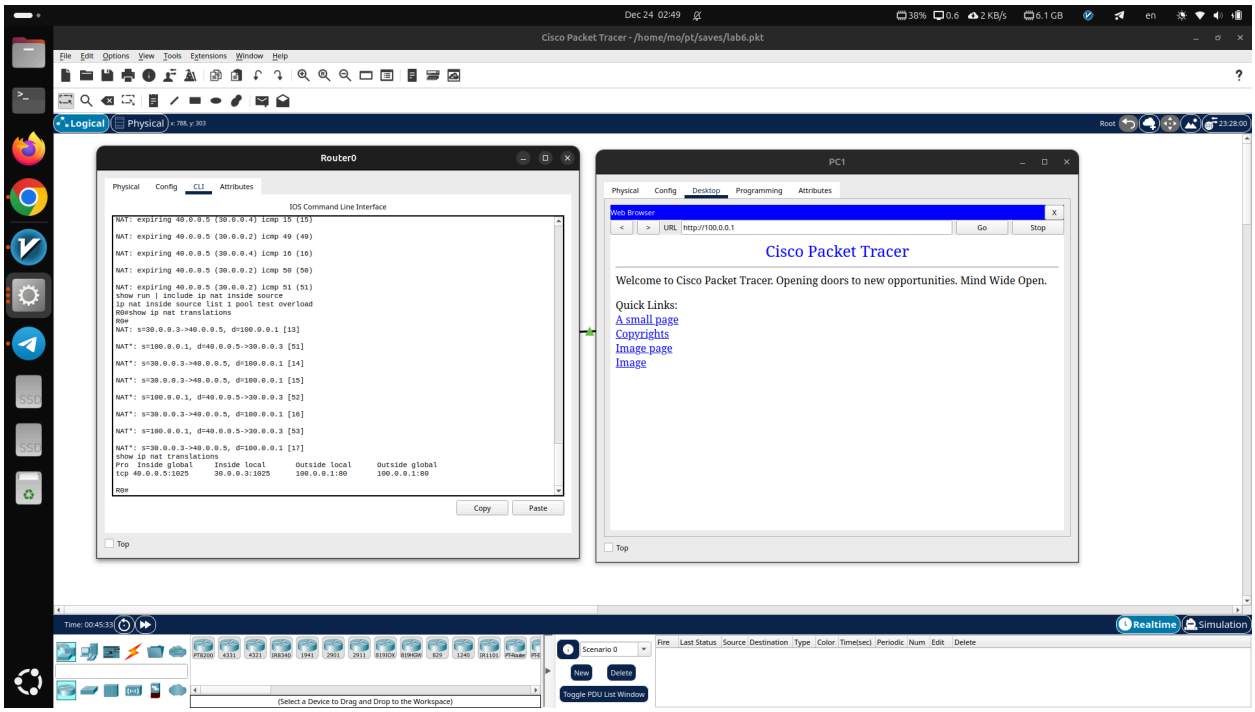
نتیجه

- در خروجی `show ip nat translations` مشاهده شد که:
  چندین کاربر با یک IP مشترک و پورت‌های متفاوت به سرور متصل شده‌اند.
- PAT مشکل کمبود IP را به‌طور کامل حل کرد.

پیاده سازی این بخش نیز بسیار ساده بود و صرفا یک دستور را با اضافه کردن overload جایگزین کردیم.
در عکس ها هم http و هم ping گذاشته شده :



که در نهایت با تست browser هم خروجیمان به مانند زیر شد :



سؤال ۱

دستور `ip nat` در سیستم‌عامل Cisco IOS برای پیکربندی فرآیند ترجمه آدرس‌ها در مسیریاب استفاده می‌شود و زیردستورهای مختلفی دارد که هرکدام نقش مشخصی در پیاده‌سازی NAT ایفا می‌کنند. با استفاده از `ip nat inside` و `ip nat outside` مشخص می‌شود که کدام اینترفیس در سمت شبکه داخلی و کدام در سمت شبکه خارجی قرار دارد و این تفکیک جهت انجام صحیح ترجمه بسته‌ها ضروری است. دستور `ip nat inside source static` برای ایجاد یک نگاشت ثابت و دائمی میان یک آدرس واقعی و یک آدرس جعلی به کار می‌رود که در پیاده‌سازی Static NAT استفاده می‌شود. همچنین دستور
`ip nat inside source list` به همراه `pool` برای Dynamic NAT به کار می‌رود و امکان ترجمه چندین آدرس داخلی به مجموعه‌ای از آدرس‌های معتبر را فراهم می‌کند. افزودن کلیدواژه `overload` به این دستور باعث فعال شدن PAT می‌شود که در آن چندین ارتباط هم‌زمان با استفاده از یک آدرس معتبر و پورت‌های متفاوت امکان‌پذیر می‌گردد.

سؤال ۲

Access List ابزاری برای کنترل و فیلتر کردن ترافیک شبکه در مسیریاب‌ها است و به طور کلی به دو نوع Standard و Extended تقسیم می‌شود. Standard ACL تنها بر اساس آدرس مبدأ تصمیم‌گیری می‌کند و معمولاً برای فیلترهای ساده به کار می‌رود، در حالی که Extended ACL امکان فیلتر کردن ترافیک بر اساس آدرس مبدأ، مقصد، نوع پروتکل و شماره پورت را فراهم می‌کند و کنترل دقیق‌تری روی ترافیک شبکه ارائه می‌دهد. به عنوان مثال، برای جلوگیری از برقراری ارتباط کاربران با سرور روی پورت TCP شماره 80، می‌توان با استفاده از یک Extended ACL بسته‌های مربوط به پروتکل TCP که مقصد آن‌ها سرور و پورت آن‌ها 80 است را مسدود کرد و سپس این لیست دسترسی را روی اینترفیس مناسب اعمال نمود تا بسته‌ها پیش از رسیدن به مقصد فیلتر شوند.

سؤال ۳

در آزمایش PAT مشاهده شد که برخلاف Dynamic NAT که هر کاربر به یک آدرس معتبر جداگانه نیاز دارد، در PAT چندین کاربر می‌توانند به صورت هم‌زمان از یک آدرس معتبر مشترک استفاده کنند. این کار با استفاده از ترجمه شماره پورت‌ها انجام می‌شود، به این معنا که هر ارتباط خروجی با یک شماره پورت یکتا شناسایی می‌شود و مسیریاب با استفاده از این پورت‌ها می‌تواند بسته‌های برگشتی را به کاربر صحیح هدایت کند. در خروجی گزارش‌گیری NAT مشاهده می‌شود که اگرچه آدرس بیرونی ثابت است، اما پورت‌های متفاوت برای هر اتصال ثبت شده‌اند که نشان‌دهنده عملکرد صحیح PAT و افزایش مقیاس‌پذیری شبکه با حداقل مصرف آدرس‌های IP است.

سؤال ۴

مشخص کردن صحیح اینترفیس‌های inside و outside در NAT اهمیت بسیار بالایی دارد، زیرا این تعیین جهت مشخص می‌کند که ترجمه آدرس‌ها در کدام سمت و با چه منطقی انجام شود. اینترفیس inside معمولاً در سمتی قرار می‌گیرد که آدرس‌های واقعی یا خصوصی وجود دارند، در حالی که اینترفیس outside به سمت شبکه بیرونی یا آدرس‌های ترجمه‌شده متصل است. در صورتی که این دو به اشتباه جابجا شوند، فرآیند NAT به درستی انجام نخواهد شد و بسته‌ها یا ترجمه نمی‌شوند یا مسیر برگشت آن‌ها از بین می‌رود. به همین دلیل در Static NAT سرور، اینترفیس متصل به سرور به عنوان inside و اینترفیس متصل به کاربران به عنوان outside تعریف می‌شود، در حالی که در Dynamic NAT و PAT کاربران به عنوان inside در نظر گرفته می‌شوند و این تفاوت دقیقاً وابسته به محل انجام NAT و نوع ترجمه مورد نظر است.