آزمایش شماره ۶

آز شبکه - دکتر بردیا صفایی

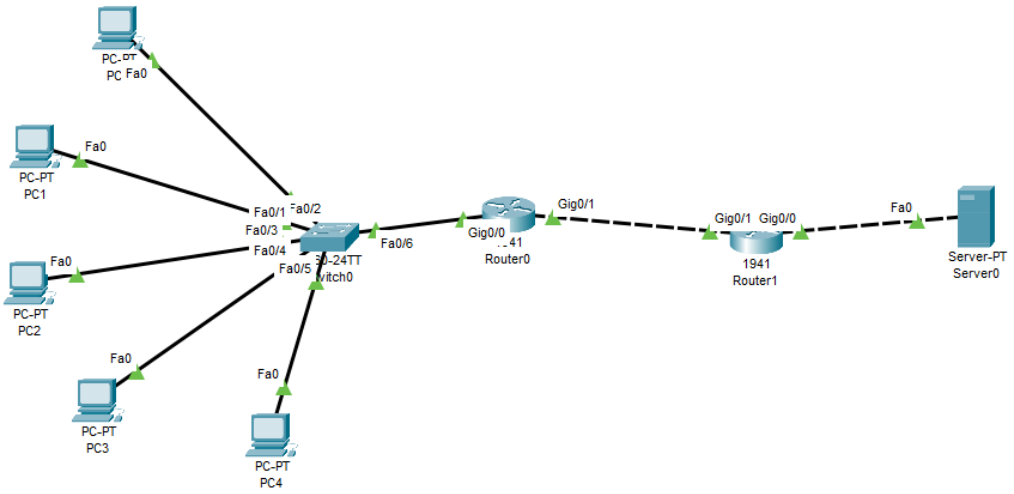
دانشکده مهندسی کامپیوتر
دانشگاه صنعتی شریف

نیم‌سال اول ۰۱-۰۲

گروه ۸:
مهرشاد میرمحمدی - ۹۸۱۰۹۶۳۴
پرهام صارمی - ۹۷۱۰۱۹۵۹
محمدرضا مفیضی - ۹۸۱۰۶۰۵۹

۱ Static Nat

ابتدا در محیط packet tracer سناریو گفته شده در کلاس را طراحی می‌کنیم. نتیجه‌ی طراحی را می‌توانید در شکل ۱ مشاهده کنید. به تمام interface ها هم ای‌پی‌ای همانند سناریوی مشخص شده می‌دهیم. سپس جداول مسیریابی مسیریاب‌ها را همان‌گونه که در آزمایش‌های قبلی یادگرفتیم، تنظیم می‌کنیم.



شکل ۱: تصویر پیاده‌سازی سناریو در محیط packet tracer

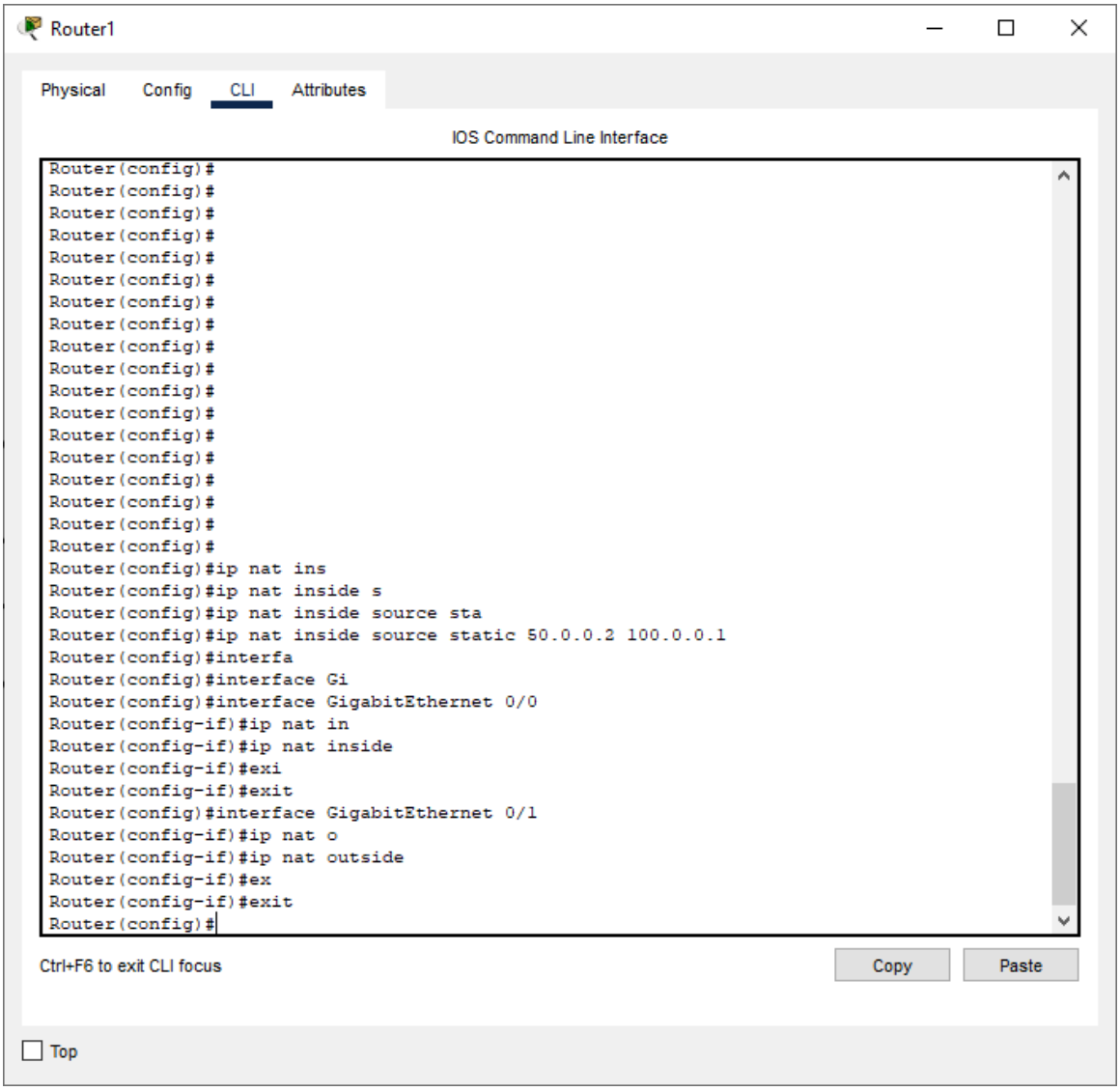
سپس دستورات مشخص شده در دستور آزمایش را مطابق تصویر ۲ در مسیریاب ۱ وارد می‌کنیم. در نهایت دستورهای ping 50.0.0.2 و ping 100.0.0.1 را اجرا می‌کنیم. همان‌طور که از تصویر ۳ مشخص است، نتایج مورد انتظار را بدست می‌آوریم.

۲ Dynamic Nat

ابتدا جداول مسیریابی را به روز می‌کنیم تا از ای‌پی‌های جدید هم پشتیبانی کنند. سپس دستورات مشخص شده را در مسیریاب صفر وارد می‌کنیم و وارد حالت debug ip nat می‌شویم. بعد از آن هم از سمت کاربران، سرور را ping می‌کنیم تا نتایج شکل ۴ حاصل شود. همان چیزی که انتظار داریم را مشاهده می‌کنیم. در نهایت هم از حالت debug ip nat خارج می‌شویم.

۳ PAT

تغییرات خواسته شده را در مسیریاب صفر وارد می‌کنیم و سپس از کاربران، سرور را ping می‌کنیم. همان طور که انتظار داریم، به درستی ترجمه اتفاق می‌افتد (تصویر ۵). توجه شود در این حالت ممکن است به یک آی‌پی چندین اتصال ترجمه شوند، برای مثال در تصویر ۵ به هر دو کاربر یک ای‌پی نسبت داده شده است. ولی در حالت قبلی به هر آی‌پی فقط یک ای‌پی دیگر می‌توانست ترجمه شود و بنابراین حداکثر به تعداد ای‌پی‌هایی که برای ترجمه داریم، می‌توانستیم اتصال هم‌زمان داشته باشیم.



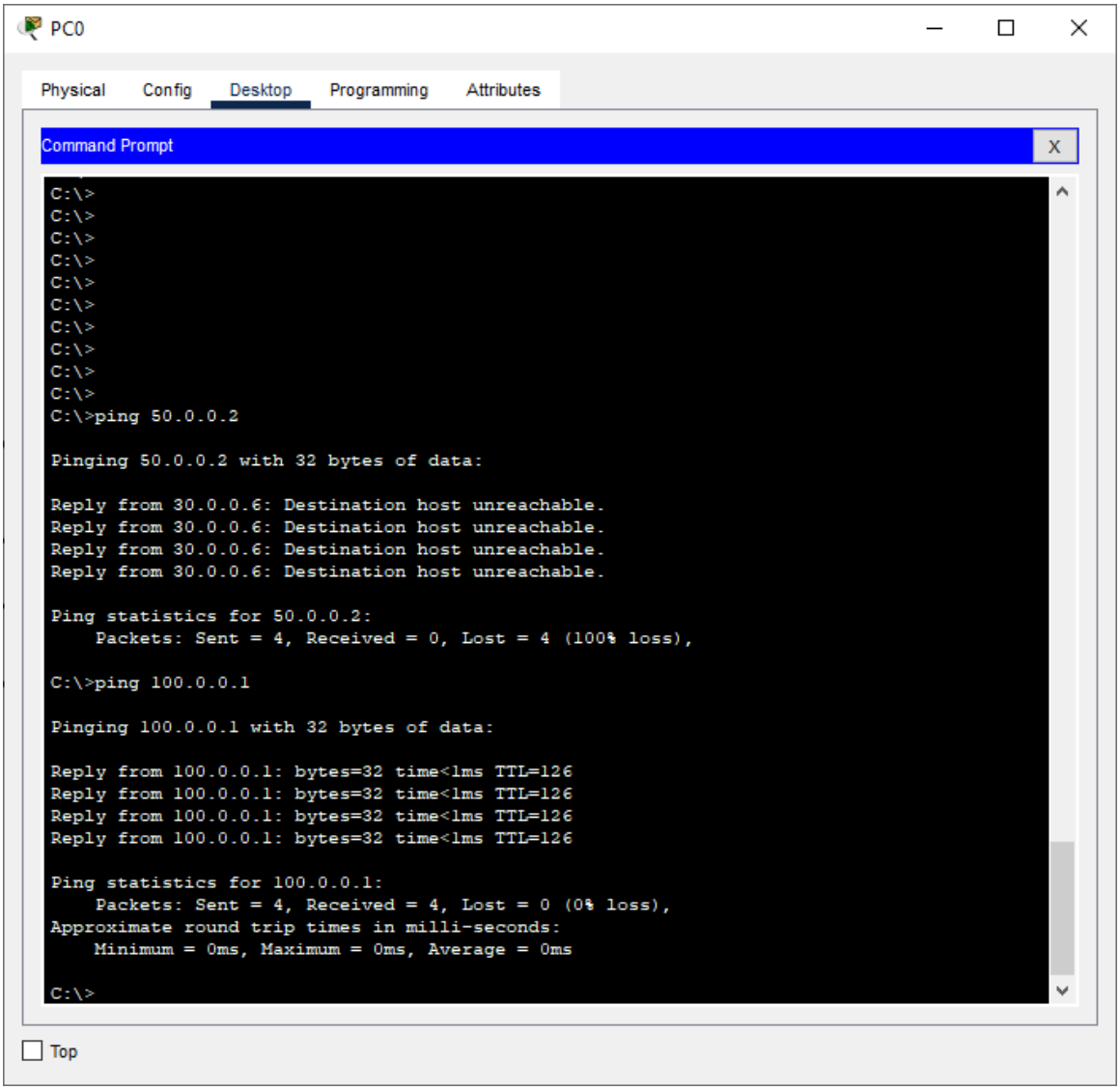
شکل ۲: اجرای دستورات آزمایش داخل مسیریاب اول

۴ سوالات

۱.۴

سه نوع دستور قابل تولید هستند: inside، outside ، pool دستور نوع inside برای ترجمه‌های مربوط به سمت inside مورد استفاده قرار می‌گیرم. دستور مشابه دیگر، نوع outside است که مشابه به دستور بالاست ولی برای ترجمه‌های سمت outside استفاده می‌شود. این دو نوع دستور رو به دو صورت می‌توان اجرا کرد.

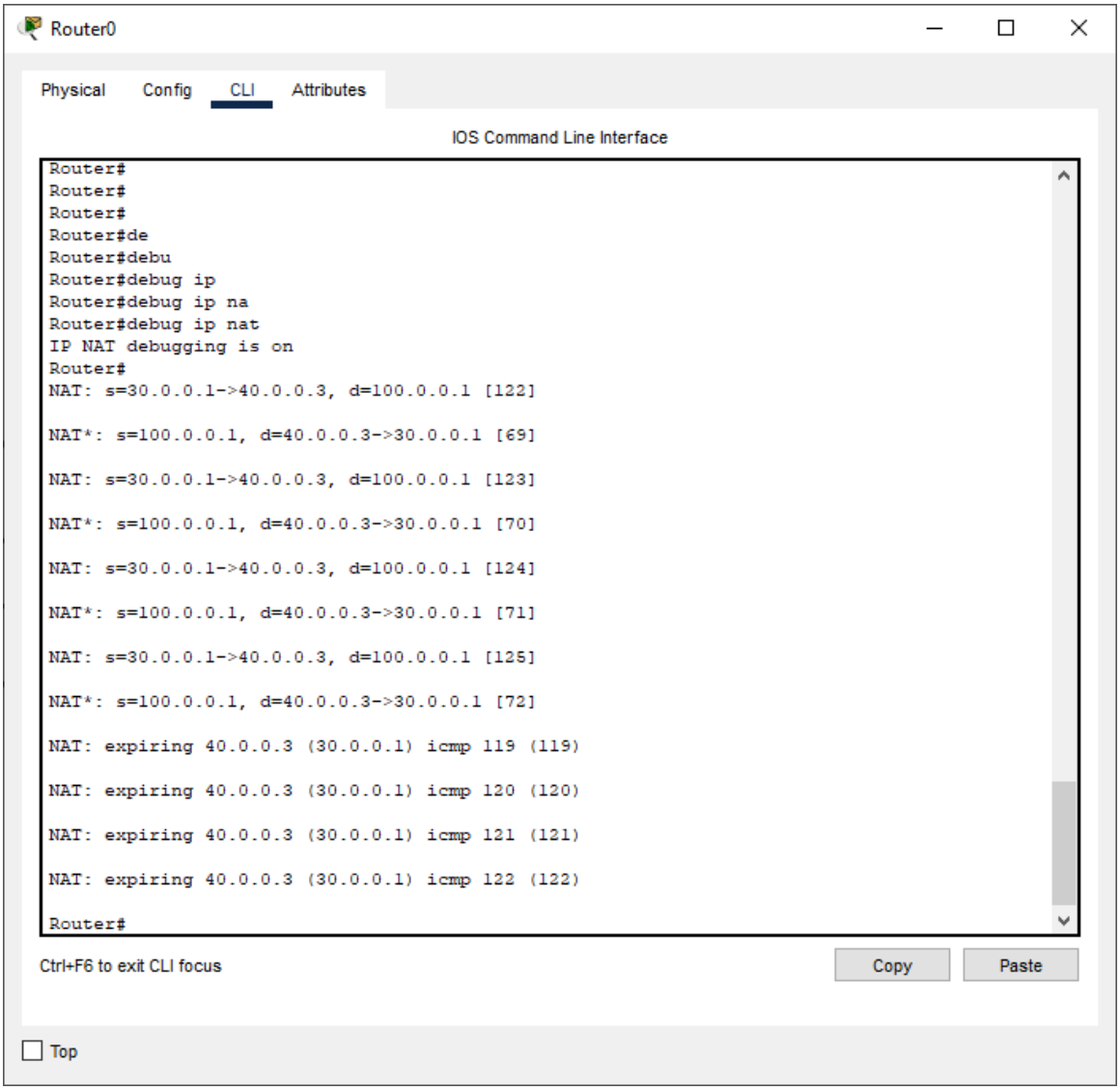
- حالت اول: ترجمه‌ی یک به یک است که به صورت زیر استفاده می‌شود.



شکل ۳: حاصل اجرای دستورهای ping در حالت Static Nat

ip nat inside/outside source static <real ip address> <nat ip address>
همچنین در این حالت می‌توان پروتوکل و پورت‌ها را هم مشخص کرد که دستور به صورت زیر می‌شود.
ip nat inside/outside source static <protocl>? <outside global ip> <global port>? <outside local ip> <local port>?

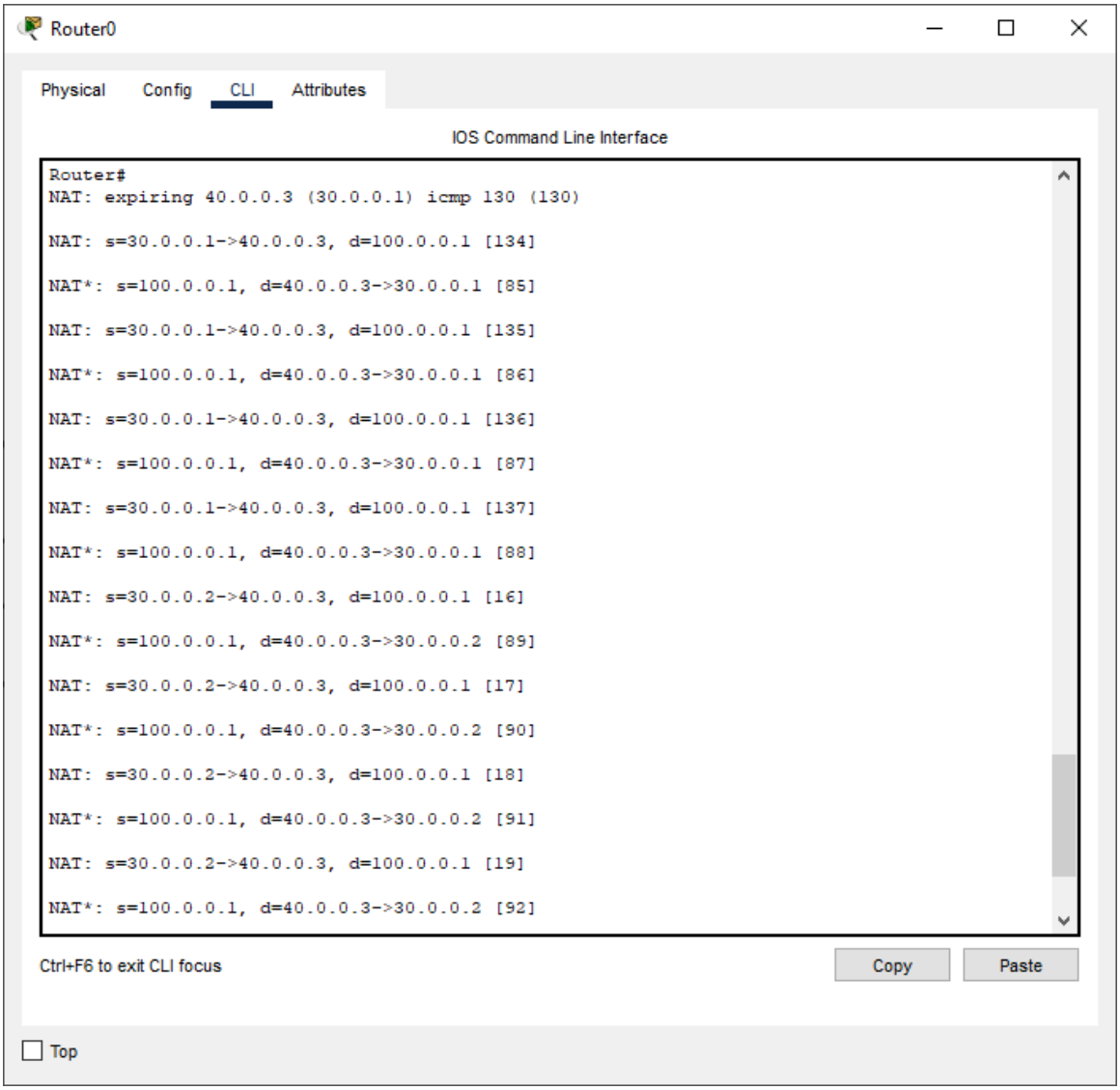
- حالت دوم: ترجمه با استفاده از access listها و pool و interface است. access listها برای مشخص کردن اتصالاتی است که قرار است ترجمه شوند و همچنین pool هم لیست آدرس‌های قابل استفاده به عنوان ترجمه را می‌دهد. استفاده‌ی آن به صورت زیر است.
ip nat inside/outside source list <access list number or name> pool <pool name>



شکل ۴: حاصل گزارش‌گیری از ترجمه در حالت Dynamic Nat

ip nat inside/outside source list <access list name> interface <interface>
در این حالت هم می‌توان با اضافه کردن کلمه‌ی overload به انتهای دستور، از حالت PAT استفاده کرد.

دستور نوع آخر هم برای تعریف کردن pool استفاده می‌شود. این دستور به صورت زیر می‌تواند استفاده شود.
ip nat pool <pool name> [<ip address>] netmask <ip netmask>



شکل ۵: حاصل گزارش‌گیری از ترجمه در حالت Pat

۲.۴

دو نوع Standard و Extended دارند. در حالت استاندارد فقط می‌توان بر حسب ای‌پی مبدا فیلتر کرد. این لیست‌ها از نظر پردازشی کم‌هزینه‌تر هستند. اگر از عددی در بازه ۱ـ۹۹ یا ۱۳۰۰ـ۱۹۹۹ استفاده کنیم، به معنای استفاده کردن از حالت استاندارد است.
اما حالت دیگر، حالت گسترش‌یافته است که امکان فیلتر کردن بر حسب آی‌پی و پروت مبدا و مقصد و همچنین پروتوکل را می‌دهد. اگر از عددی در بازه ۱۰۰ـ۱۹۹ یا ۲۰۰۰ـ۲۶۹۹ استفاده کنیم، به معنی استفاده از حالت گسترش یافته است. البته این امکانات بیشتر باعث شده تا از نظر محاسباتی، هزینه‌برتر هم باشند.
کاربرد حالت اول زمانی است که بر اساس آی‌پی بخواهیم فیلتر کنیم، برای مثال فقط به اتصالاتی که از ماشین خاصی برقرار شده

باشند، پاسخ دهیم. حالت دوم ولی زمانی مورد استفاده قرار می‌گیرد که به امکانات بیشتری نیاز باشد. برای مثال زمانی که اجازه ندهیم تا به پورت خاصی، دست‌رسی پیدا شود. چون بر روی آن پورت ممکن است سرور حساسی که نیاز امنیتی دارد، وجود داشته باشد.
دستور access-list 42 deny tcp any 100.0.0.1 0.0.0.0 eq 80 بسته‌هایی که از پروتوکل tcp استفاده می‌کنند، از هر مبدای باشند، و مقصداشان 100.0.0.1 باشد با wildcard ۰.۰.۰.۰ و پروت ۸۰ داشته باشند را نمی‌گذارد رد بشوند. اگر می‌خواستیم می‌توانستیم آدرس مقصدی هم مشخص نکنیم و آن را هم any بگذاریم.

۳.۴

همان‌طور که قبل‌تر هم گفته شد، در این حالت ممکن است اتصالات مختلف به یک آی‌پی ترجمه شوند اما پورت‌های مختلفی داشته باشند. این خیلی خوب است چون مشکل IPv۴ را تا حد زیادی برطرف می‌کند. همان طور که در تصویر ۵ هم می‌بینیم، به هر دو کاربر یک و دو، یک ای‌پی داده شده است بنابراین شماره پورت متفاوتی داشته‌اند. اگر بخواهیم می‌توانیم با استفاده از دستور show ip nat translations به صورت دقیق‌تر ببینیم که هر ای‌پی و پروت‌ای به چه ای‌پی و پورت‌ای ترجمه شده‌است.

۴.۴

پورت‌هایی از NAT که از شبکه‌ی خارجی در دست‌رس است، اهمیت زیادی دارند. چرا که پورت‌های مختلف می‌توانند سرورهای گوش به فرمان مختلفی را داشته باشند که نباید بتوان از دنیای بیرون به آنها متصل شد. همچنین پورت‌های داخلی فقط در داخل NAT معنی دارند و پورت‌های خارجی هم در دنیای بیرون معنی دارند.
برای تعویض پورت خروجی و ورودی هم کافیست پورت‌های مورد انتظار را در زمان ساخت access list همان‌گونه که در حالت گسترش‌یافته در سوال دو دیدیم، اضافه کنیم.