دانشگاه صنعتی شریف
دانشکدهٔ مهندسی کامپیوتر

گزارش‌کار آزمایشگاه شبکه

آزمایش شماره ۶

استاد محترم:

جناب آقای دکتر صفایی

اعضای تیم:

امیرمهدی نامجو ۹۷۱۰۷۲۱۲

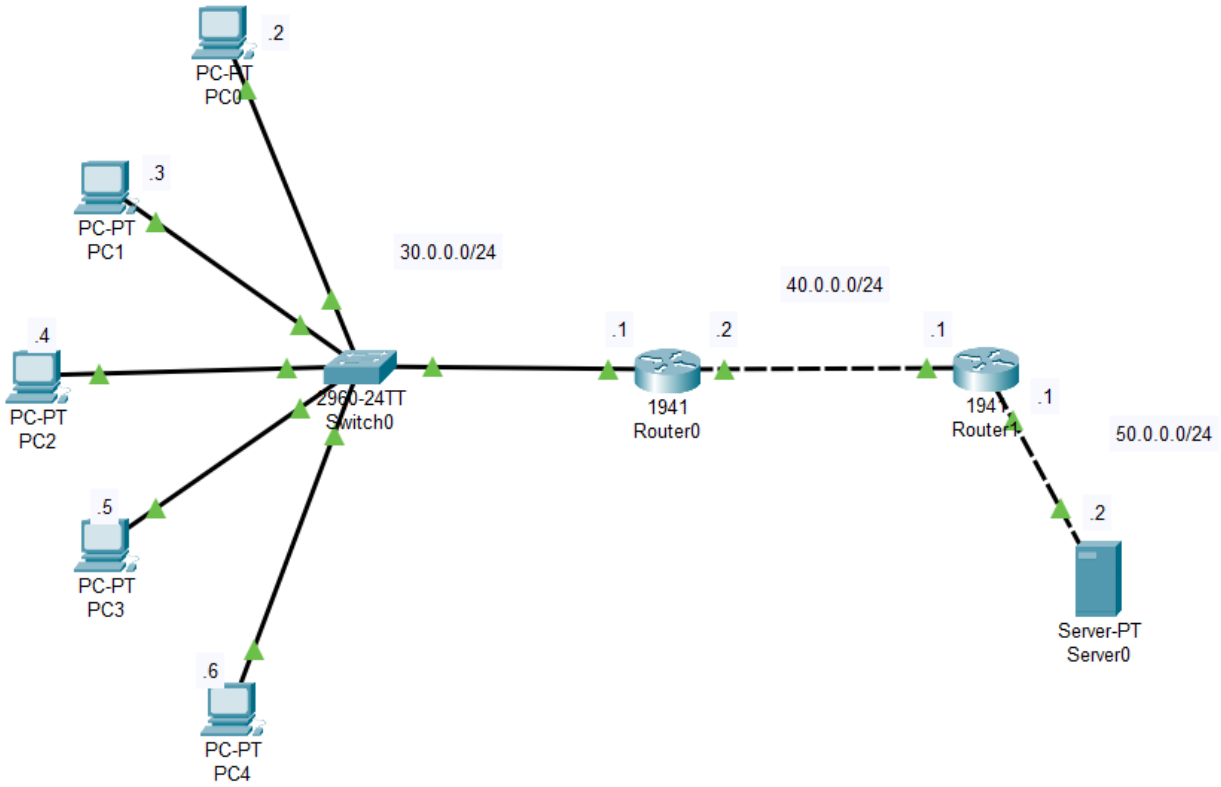
محمدسپهر پورقناد ۹۷۱۰۱۳۵۹

سپهر صفری ۹۷۱۰۸۲۶۳

نیم‌سال دوم تحصیلی ۱۴۰۰ـ۱۴۰۱

Static NAT

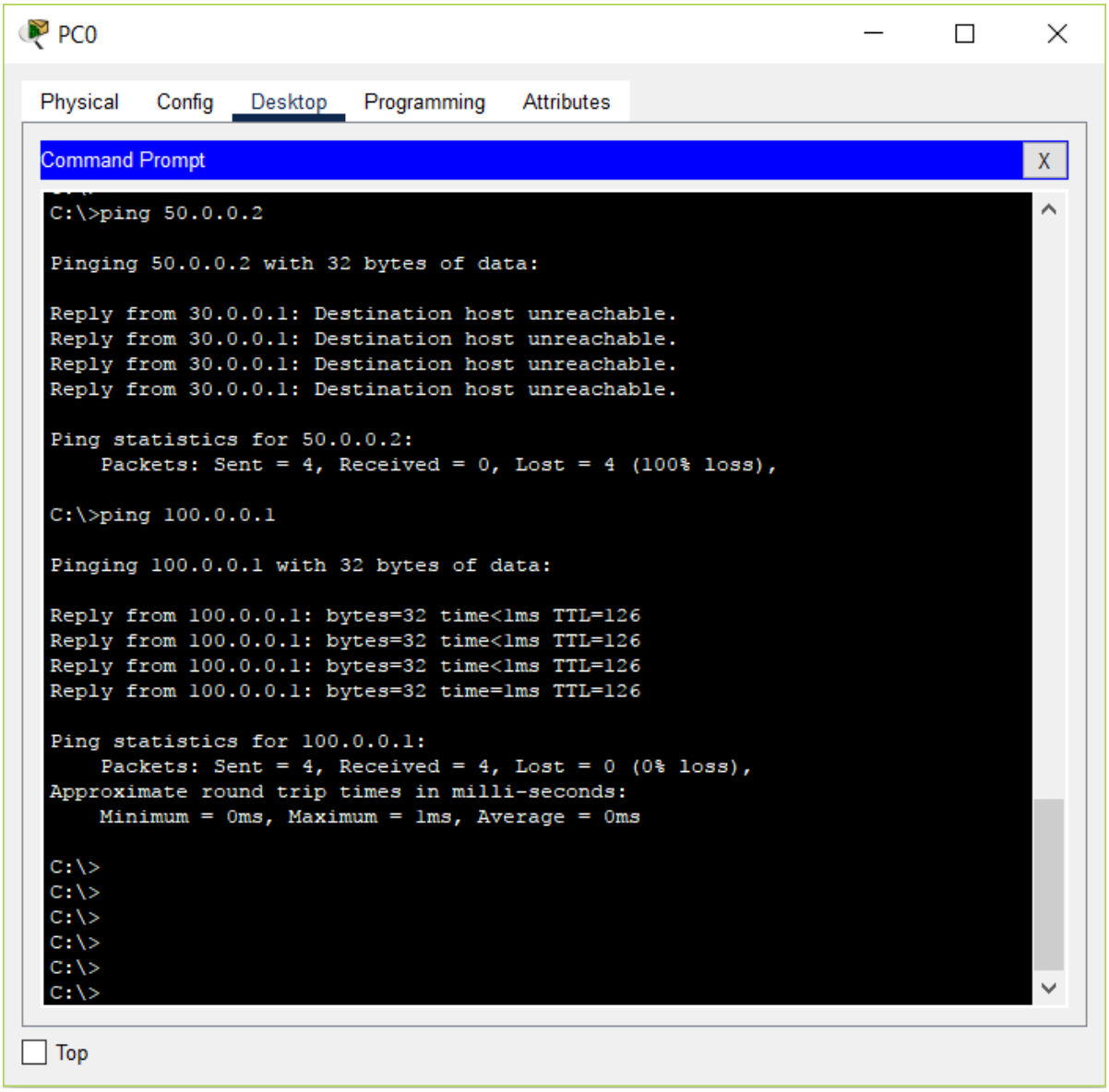
ابتدا شبکه را مانند طبق چیزی که مستند خواسته شده است، می‌سازیم:



شکل ۱.۱: شبکه

همچنین ip های هر یک از اینترفیس‌ها و دستگاه‌ها را طبق مستند تعیین می‌کنیم. لازم است به Router0 در قسمت Routing > Static قاعده 100.0.0.0/24 via 40.0.0.1 را اضافه کنیم. همچنین قاعده 30.0.0.0/24 via 40.0.0.2 را به Router1 اضافه می‌کنیم. در ادامه دستورات درون مستند را در Router1 اجرا می‌کنیم.

در نهایت ۲ دستور ping 50.0.0.2 و ping 100.0.0.1 را به ترتیب در ترمینال PC0 اجرا می‌کنیم و مشاهده می‌شود که خروجی طبق انتظار است:

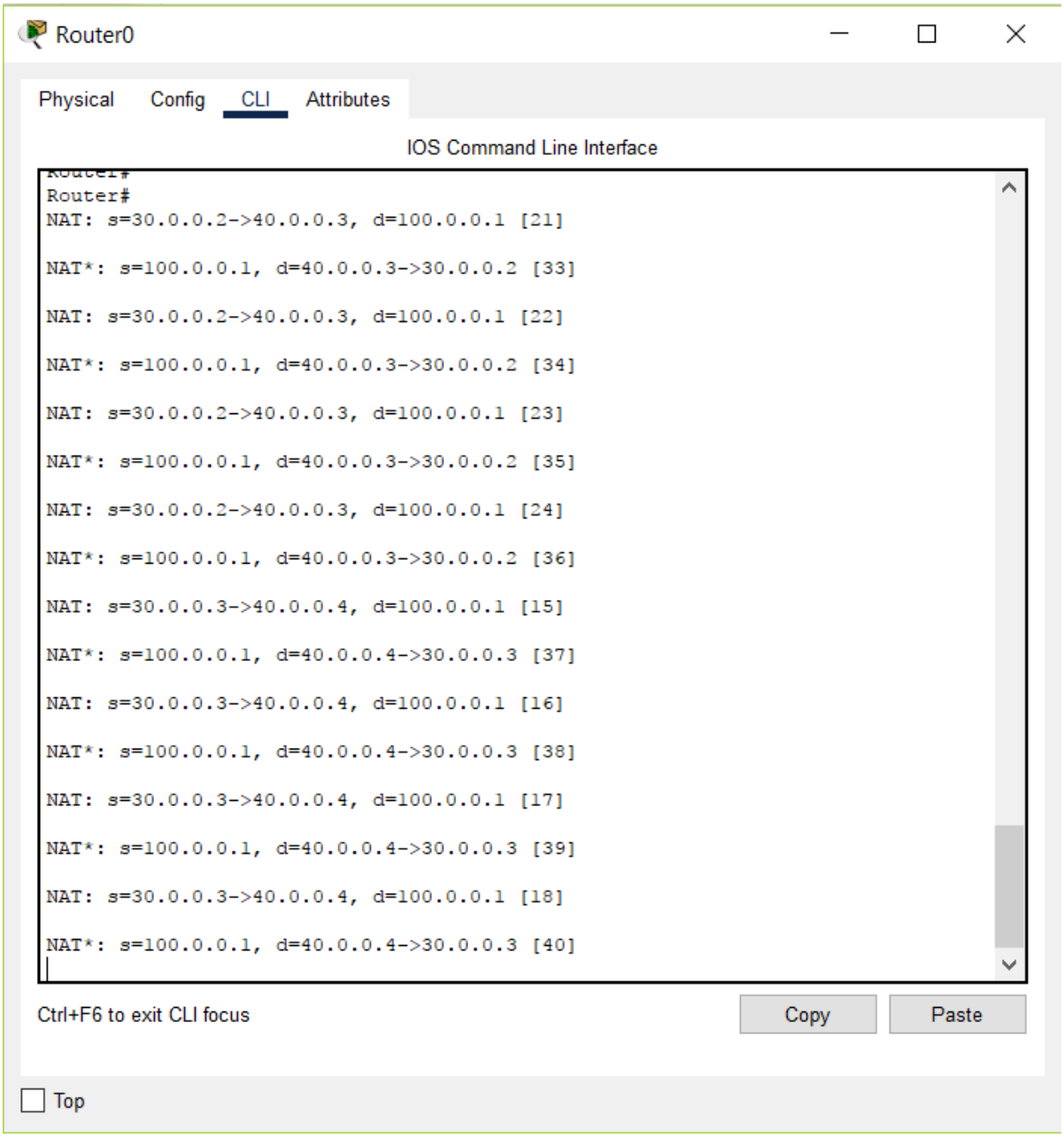


شکل ۲.۱: ping در حالت static nat

Dynamic NAT

ابتدا درون Router0 به جای قاعده 30.0.0.0/24 via 40.0.0.2 قاعده 40.0.0.0/24 via 40.0.0.2 را می‌نویسیم چرا که ip ی PC ها از این پس با این ip ها شناخته می‌شوند. در ادامه طبق مستند دستورات لازم را در Router0 وارد می‌کنیم.

در نهایت در PC0 و PC1 به ترتیب دستور ping 100.0.0.1 را اجرا می‌کنیم و در ترمینال Router0 خروجی زیر مشاهده می‌شود:

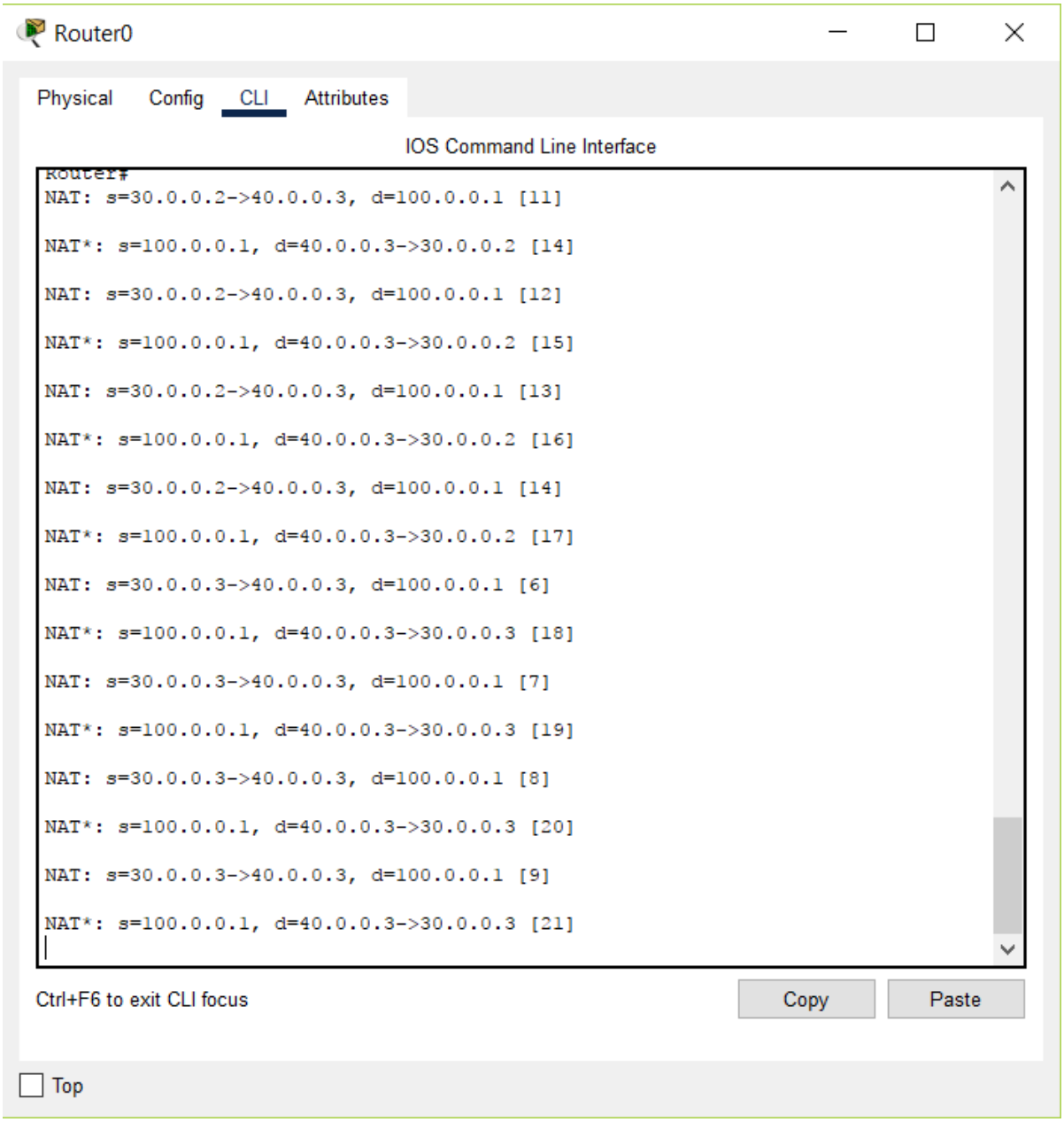


شکل ۳.۲: ping در حالت dynamic nat

مشاهده می‌شود که PC0 و PC1 به ترتیب آدرس‌های 40.0.0.3 و 40.0.0.4 را دریافت می‌کنند که همان چیزی است که انتظار داریم. اگر همین کار را برای تعداد بیشتری PC امتحان کنیم مشاهده می‌شود که ترجمه آدرس باز هم به درستی انجام می‌شود و اگر بیشتر از ۳ تا PC بخواهند همزمان ping کنند، بعضی مجبور هستند منتظر بمانند تا یکی از آدرس‌هایی که قبلا استفاده شده است، آزاد شود.

PAT

دستورات لازم را طبق مستند در Router0 وارد می‌کنیم، سپس دستور ping 100.0.0.1 را به ترتیب در PC0 و PC1 وارد می‌کنیم. در ترمینال Router0 خروجی زیر مشاهده می‌شود:



شکل ۴.۳: ping در حالت pat

همان‌گونه که مشاهده می‌شود برخلاف حالت dynamic nat که هر PC باید یک ip منحصر به فرد می‌داشت، اینجا PC0 و PC1 هردو آدرس 40.0.0.3 را دریافت کردند که یعنی هرکدام یک پورت از این آدرس را گرفته‌اند و ترجمه به درستی انجام شده است.

سوالات

۱.۴

این دستورات به ۳ دسته تقسیم می‌شوند:

۱) pool: به کمک این دسته از دستورات استخری از آدرس‌های معتبر تعریف می‌کنیم که شامل ۱ نوع دستور است:

1) ip nat pool <pool name> <start address> <end address> netmask <network mask>

با این دستور می‌توان آدرس‌هایی معتبر در بازه‌ای مشخص تعریف کرد. کارکرد پارامترهای این دستور هم طبق اسمشان قابل تشخیص هستند.

۲) outside: به کمک این دسته از دستورات آدرس‌های بیرونی را ترجمه می‌کنیم که شامل ۲ نوع دستور است:

1) ip nat outside source static <protocl>? <outside global ip> <global port>? <outside local ip> <local port>?

با این دستور می‌توان ترجمه را به صورت ایستا انجام داد. پارامترهایی که جلوی آنها ? قرار دارد مربوط به پروتکل استفاده شده هستند که می‌توان از آن‌ها استفاده نکرد. در واقع یا همه آن‌ها نوشته می‌شوند و یا هیچ یک نوشته نمی‌شوند. همچنین پروتکل انتخاب شده باید tcp یا udp باشد.

2) ip nat outside source list <access list number or name> pool <pool name>

با این دستور می‌توان تعدادی لیستی از آدرس‌ها را به آدرس‌های درون یک استخر ترجمه کرد.

۳) inside: به کمک این دسته از دستورات آدرس‌های داخلی را ترجمه می‌کنیم که شامل ۳ نوع دستور است:

1) ip nat inside source static <protocol>? <inside local ip> <local port>؟ <inside global ip> <global port>؟

با این دستور می‌توان ترجمه را به صورت ایستا انجام داد. پارامترهایی که جلوی آنها ? قرار دارد مربوط به پروتکل استفاده شده هستند که می‌توان از آن‌ها استفاده نکرد. در واقع یا همه آن‌ها نوشته می‌شوند و یا هیچ یک

نوشته نمی‌شوند. همچنین پروتکل انتخاب شده باید tcp یا udp باشد.

2) ip nat inside source list <access list name> pool <pool name> [overload]

3) ip nat inside source list <access list name> interface <interface> [overload]

با این دو دستور می‌توان ترجمه آدرس را برای لیستی از آدرس‌ها انجام داد. در دستور اول از استخری از آدرس‌ها در ترجمه استفاده می‌شود و در دستور دوم از interface. دقت شود کلمه overload در آخر دو دستور می‌تواند باشد یا نباشد و در صورت وجود ترجمه به صورت PAT انجام می‌شود.

۲.۴

۲ نوع وجود دارد:

۱) Standard: این نوع به ip مبدا توجه می‌کنند و با توجه به آن کل بسته را قبول یا رد می‌کنند. این نوع لیست دسترسی نسبت به پروتکل بی‌تفاوت است. اگر از عددی در بازه ۱ـ۹۹ یا ۱۳۰۰ـ۱۹۹۹ استفاده کنیم، روتر می‌فهمد که لیست دسترسی از نوع استاندارد است و ip مشخص شده همان ip مبدا است.

۲) Extended: این نوع به ip مبدا و مقصد و پورت مبدا و مقصد توجه می‌کند. همچنین پروتکل‌های بسته‌ها مانند TCP ، UDP و HTTP را هم مدنظر قرار می‌دهد. اگر از عددی در بازه ۱۰۰ـ۱۹۹ یا ۲۰۰۰ـ۲۶۹۹ استفاده کنیم، روتر می‌فهمد که لیست دسترسی از نوع Extended است.

لازم به ذکر است نوعی دیگر از دسته‌بندی لیست‌های دسترسی هم وجود دارد که آن‌ها را به دو دسته عددی و اسمی تقسیم می‌کند. در نوع عددی اگر بخواهیم قاعده‌ای از لیست دسترسی حذف کنیم، ناچاریم کل لیست دسترسی را حذف کنیم در حالی که در نوع اسمی این محدودیت وجود ندارد.

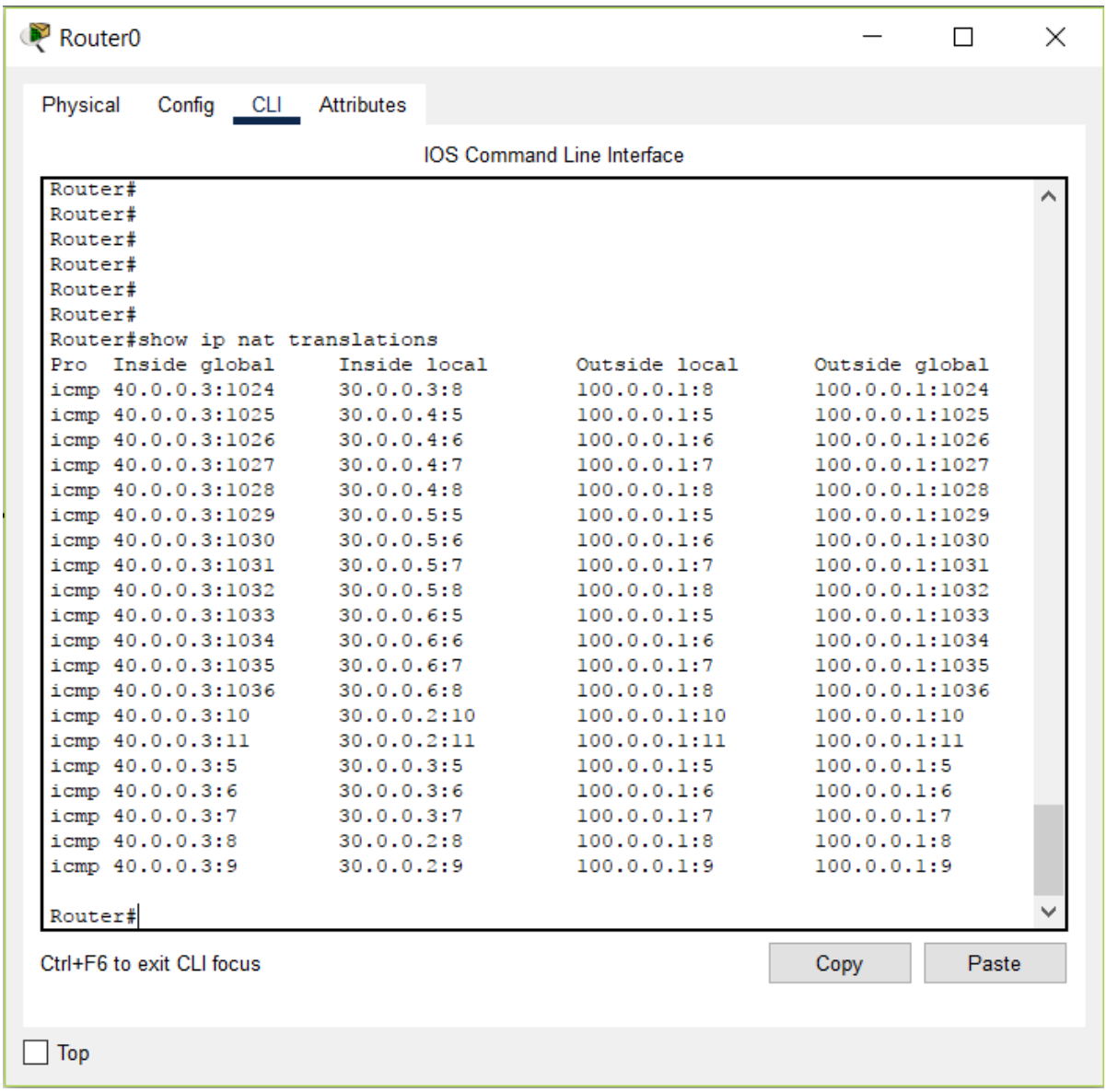
دستور خواسته شده به صورت زیر خواهد بود:

access-list 100 deny tcp any 100.0.0.1 0.0.0.0 eq 80

در این دستور deny به معنی اینست که بسته‌ای که طبق مشخصات ذکر شده باشد قبول نخواهد شد. any به معنای همه آدرس‌های مبدا است و 100.0.0.1 آدرس مقصد که همان سرور است را مشخص می‌کند، دقت شود 0.0.0.0 همان wildcard mask آن است. eq 80 هم یعنی که پورت مقصد برابر با ۸۰ باشد.

۳.۴

جدول ترجمه ipها در زیر نمایش داده شده است:



شکل ۵.۴: جدول ترجمه ipها

ستون inside local همان PCها هستند. ستون inside global هم آدرس تخصیص داده شده به PC مربوطه را نشان می‌دهد. می‌توان دید که همه PCها آدرس 40.0.0.3 را دریافت کرده‌اند که یعنی همه از یک آدرس استفاده می‌کنند و محدودیت dynamic nat وجود ندارد. این به خاطر اینست که هر PC پورت متفاوتی از آدرس 40.0.0.3 را دریافت کرده است که همان چیزی است که از PAT انتظار داریم.

۴.۴

اهمیت این پورت‌ها اینست که مسیریاب هر پورت ورودی را با یک پورت خروجی جفت می‌کند و با کمک جدولی که از این جفت پورت‌ها تشکیل داده عمل ترجمه را انجام می‌دهد. همچنین از نظر امنیتی هم مهم است که دستگاه‌های داخل nat از چه پورتی داده می‌فرستند و یا روی کدام پورت خود داده را دریافت می‌کنند تا حملات

مختلفی که روی بعضی پورت‌های خاص رخ می‌دهد، انجام نشود.

در نهایت تعویض تغییر پورت ورودی و خروجی کافی است دستورات access-list را در آزمایش ۲ و ۳ عوض کنیم و قواعد دلخواه را به آن‌ها اضافه کنیم، مثلا اجازه عبور بسته‌های tcp روی پورت خاصی را ندهیم. به این صورت مسیریاب تنها اجازه استفاده از پورت‌های مشخصی را به دستگاه‌های داخل و خارج nat می‌دهد.