

گزارش ششم آزمایشگاه شبکه های کامپیوتری

اعضای گروه:

پارسا عصمتلو

سهیل شهرابی

فهرست مطالب

2.....	فهرست مطالب
3.....	پیش گزارش آزمایش هفتم
3.....	سوال ۱
4.....	سوال ۲
4.....	سوال ۳
5.....	سوال ۴
6.....	سوال ۵
6.....	پورت دسترسی یا Access Port
7.....	پورت ترانک یا Trunk Port
7.....	برچسبگذاری فریم یا Frame Tagging
8.....	سوال ۶
8.....	سوال ۷
9.....	سوالات تحلیلی آزمایش ششم
9.....	سوال ۱
10.....	سوال ۲
11.....	گزارش آزمایش ششم
11.....	مرحله اول-پایه سازی توپولوژی
11.....	گام اول
12.....	گام دوم
12.....	آی پی دهی هاست و نتورک-توضیحات تشریحی
12.....	آی پی دهی هاست و نتورک-جدول
13.....	گام سوم
13.....	آی پی دهی روتر ها-توضیحات تشریحی
13.....	گام چهارم
13.....	تنظیم روتینگ روتر ها
14.....	مرحله پایانی
14.....	پینگ گرفتن
14.....	مرحله دوم-static nat
14.....	راه اندازی
15.....	پینگ گرفتن
16.....	مرحله سوم-Dynamic nat

- 16..... راه اندازی
- 17..... بینگ گرفتن
- 18..... مرحله چهارم-Overloading nat
- 18..... راه اندازی
- 19..... بینگ گرفتن

پیش گزارش آزمایش هفتم

سوال ۱

وقتی از مفهوم "شبکه تخت" یا "شبکه صاف" (Flat Network) استفاده می‌شود، به یک معماری شبکه اشاره می‌کند که در آن همه‌ی دستگاه‌ها و سگمنت‌های شبکه در یک لایه فیزیکی و یا لایه دسترسی به شبکه قرار دارند. به این معنی که هیچ تقسیم‌بندی یا سازماندهی سلسله‌مراتبی از زیرشبکه‌ها وجود ندارد و همه دستگاه‌ها با یکدیگر در یک شبکه بزرگ و مساوی در ارتباط هستند. در یک شبکه تخت، همه دستگاه‌ها در یک دامنه پخش شبکه یا Broadcast Domain قرار دارند. بنابراین، هر بسته ارسالی یا درخواست شبکه به تمام دستگاه‌ها در شبکه تخت ارسال می‌شود و هر دستگاه باید تصمیم بگیرد که آیا بسته را پردازش کند یا نه.

بهره‌برداری از شبکه تخت می‌تواند سادگی مدیریت و کانفیگ شبکه را افزایش دهد، زیرا نیازی به تنظیمات پیچیده‌تر مانند VLAN ها یا Routing ندارد. همچنین، ارتباط بین دستگاه‌ها در شبکه تخت به طور مستقیم و بدون محدودیت است. اما، یکی از معایب شبکه تخت این است که با افزایش تعداد دستگاه‌ها و ترافیک در شبکه، ممکن است بهبود کارایی و کنترل ترافیک ضروری باشد. همچنین، امنیت شبکه نیز ممکن است به علت عدم تقسیم‌بندی مناسب شبکه تخت به خطر بیافتد، زیرا دستگاه‌ها به راحتی قابل دسترسی و هدف قرار می‌گیرند.

بنابراین، شبکه تخت به عنوان یک معماری ساده و در مقیاس کوچک می‌تواند مفید باشد، اما در شبکه‌های بزرگتر و پیچیده‌تر، استفاده از تقسیم‌بندی مجازی شبکه (VLAN) و مسیریابی مناسب می‌تواند بهترین راه برای ارتقای امنیت و کارایی شبکه باشد.

سوال ۲

VLAN یا تقسیم‌بندی مجازی شبکه در مدیریت شبکه‌های کامپیوتری به شما امکان می‌دهد تا شبکه را به چندین بخش کوچکتر تقسیم کنید و بین این بخش‌ها مرزهای مجازی ایجاد کنید. هر بخش یا VLAN می‌تواند شامل یک یا چند دستگاه باشد و ارتباط بین VLAN ها می‌تواند محدود شود یا به صورت کنترل شده انجام شود. استفاده از VLAN ها در مدیریت شبکه به شما این امکان را می‌دهد.

1. جداسازی ترافیک: با استفاده از VLAN ها می‌توانید ترافیک شبکه را جدا کنید و بین بخش‌های مختلف شبکه تفکیک کنید. این امر می‌تواند برای جلوگیری از تداخل ترافیک، بهبود عملکرد شبکه و افزایش امنیت مناسب باشد. به عنوان مثال، می‌توانید VLAN جداگانه‌ای برای دستگاه‌های مدیریتی، دستگاه‌های کاربران و سرویس‌های خاص ایجاد کنید.
2. کنترل دسترسی: با استفاده از VLAN ها می‌توانید کنترل دقیق‌تری بر روی دسترسی به منابع شبکه داشته باشید. می‌توانید به تمام دستگاه‌ها در یک VLAN دسترسی داشته باشید و به دستگاه‌های دیگر در VLAN دیگر دسترسی نداشته باشید، بنابراین امنیت شبکه را تقویت کنید.
3. مدیریت بهتر ترافیک: با تفکیک شبکه به VLAN ها، می‌توانید قوانین و سیاست‌های ترافیک مختلف را بر روی هر VLAN اعمال کنید. می‌توانید برای هر VLAN قوانین QoS (کیفیت خدمات)، نرخ باند و محدودیت‌های دیگر را تنظیم کنید تا بهترین استفاده را از پهنای باند شبکه داشته باشید.
4. افزایش امنیت: با استفاده از VLAN ها می‌توانید امنیت شبکه را بهبود بخشید. با ایجاد VLAN های جداگانه برای دستگاه‌های حساس و منابع مهم، می‌توانید به راحتی محدودیت‌ها و سیاست‌های امنیتی را اعمال کنید و از حملات دسترسی غیرمجاز جلوگیری کنید.

به طور خلاصه، استفاده از VLAN ها در مدیریت شبکه‌های کامپیوتری به شما کمک می‌کند تا ترافیک را جدا کرده، دسترسی به منابع را کنترل کنید، مدیریت بهتری بر ترافیک داشته باشید و امنیت شبکه را تقویت کنید.

سوال ۳

تفاوت بین VLAN های استاتیک و دینامیک به روشی که VLAN ها مدیریت و پیکربندی می‌شوند، مربوط است.

1. VLAN استاتیک: در VLAN های استاتیک، شماره VLAN برای هر پورت یا دستگاه در سوئیچ به صورت دستی تنظیم می‌شود. به عبارت دیگر، مدیر شبکه باید به طور دستی VLAN مربوطه را برای هر پورت یا دستگاه تعیین کند. این تنظیمات VLAN ثابت است و تغییر نمی‌کند مگر اینکه مدیر شبکه آن را به طور دستی تغییر دهد. VLAN های استاتیک مناسب برای شبکه‌های کوچک تر و کاربردهای ساده است که تغییرات زیادی در ترکیب دستگاه‌ها و پورت‌ها انتظار نمی‌رود.
2. VLAN دینامیک: در VLAN های دینامیک، استفاده از یک پروتکل خاص مانند (VLAN Trunking Protocol (VTP یا مکانیزم دیگری امکان پذیر است. با استفاده از این پروتکل‌ها، سوئیچ‌ها توانایی ارسال اطلاعات VLAN به یکدیگر را دارند و تغییرات در VLAN ها به صورت خودکار در سراسر شبکه توزیع می‌شوند. به عبارت دیگر، وقتی یک VLAN جدید ایجاد می‌شود یا یک VLAN حذف می‌شود، تغییرات به صورت خودکار در سوئیچ‌های دیگر نیز اعمال می‌شود. VLAN های دینامیک معمولاً برای شبکه‌های بزرگتر و پیچیده‌تر استفاده می‌شوند که نیاز به انعطاف پذیری بیشتر در مدیریت VLAN ها دارند.

بنابراین، تفاوت اصلی بین VLAN های استاتیک و دینامیک در روش مدیریت و پیکربندی آنها است. VLAN استاتیک نیازمند تنظیم دستی شماره VLAN برای هر پورت یا دستگاه است، در حالی که VLAN دینامیک از پروتکل‌های خاصی برای توزیع و مدیریت VLAN ها در سراسر شبکه استفاده می‌کند.

سوال ۴

پارامترهای پویا در VLAN های پویا برای اختصاص عضویت در VLAN به دستگاه‌ها یا پورت‌ها استفاده می‌شوند. پارامترهای پویا زیر به طور معمول استفاده می‌شوند:

1. آدرس MAC: عضویت در VLAN می‌تواند بر اساس آدرس MAC دستگاه برای آن تعیین شود. زمانی که یک دستگاه به یک پورت سوئیچ متصل می‌شود، سوئیچ آدرس MAC آن را بررسی کرده و بر اساس مپ‌ها یا قوانین از پیش تعیین شده، آن را به VLAN مربوطه اختصاص می‌دهد.
2. شماره پورت: برخی از سوئیچ‌ها اجازه می‌دهند تا پورت‌ها را به VLAN های مختلف تعیین کنید. در این حالت، عضویت در VLAN بر اساس شماره پورتی که دستگاه به آن متصل است، تعیین می‌شود. به عنوان مثال، شماره پورت 1 ممکن است به VLAN 10 تعلق داشته باشد و شماره پورت 2 به VLAN 20 تعلق داشته باشد.

3. احراز هویت: در برخی از موارد، VLAN های پویا می‌توانند بر اساس اطلاعات احراز هویت که توسط دستگاه‌ها ارائه می‌شود، تعیین شوند. این اطلاعات می‌تواند شامل شناسه کاربری و رمز عبور یا گواهی‌های دیگر باشد. با احراز هویت دستگاه، سوئیچ می‌تواند بر اساس اطلاعات ارائه شده، دستگاه را به VLAN مناسب تخصیص دهد.

4. پروتکل‌های دیگر: برخی از پروتکل‌های شبکه دیگر مانند Dynamic Host Configuration Protocol (DHCP) نیز می‌توانند برای تعیین عضویت در VLAN استفاده شوند. این پروتکل‌ها می‌توانند اطلاعات مربوط به VLAN را به دستگاه‌ها ارسال کنند و آنها را به VLAN مناسب تخصیص دهند.

در کل، پارامترهای پویا در VLAN های پویا برای اختصاص عضویت در VLAN استفاده می‌شوند. این پارامترها شامل آدرس MAC، شماره پورت، احراز هویت و پروتکل‌های دیگر می‌شوند.

سوال ۵

پورت دسترسی یا Access Port

پورت دسترسی یا "Access Port" در شبکه‌های کامپیوتری به پورتهایی اشاره دارد که به دستگاه‌های پایانی (مثلاً کامپیوتر یا تلفن IP) متصل می‌شود. این پورت‌ها به طور معمول در سوئیچ‌های شبکه تنظیم می‌شوند و وظیفه اصلی آنها ارائه اتصال به VLAN مورد نظر است. پورت دسترسی در حالت پیش‌فرض به یک VLAN خاص اختصاص داده می‌شود و ترافیک دستگاه‌های متصل به آن پورت تنها در این VLAN جا به جا می‌شود. به عبارت دیگر، هر دستگاه متصل به پورت دسترسی به صورت پیش‌فرض در یک VLAN ثابت قرار می‌گیرد و از سایر VLAN ها جدا می‌شود.

پورت دسترسی به عنوان یک رابط بین دستگاه‌های پایانی و سوئیچ شبکه عمل می‌کند. این پورت‌ها تنها برای یک دستگاه مشخص تعیین می‌شوند و نباید با پورت‌های ترانک ("Trunk Ports") که برای انتقال ترافیک بین سوئیچ‌ها و VLAN ها استفاده می‌شوند، اشتباه گرفته شوند.

بنابراین، پورت دسترسی در شبکه‌های کامپیوتری به پورتهایی اشاره دارد که به دستگاه‌های پایانی متصل می‌شود و تنها در یک VLAN مشخص قرار دارد.

پورت ترانک یا Trunk Port

پورت ترانک یا "Trunk Port" در شبکه‌های کامپیوتری به پورتهایی اشاره دارد که برای انتقال ترافیک بین سوئیچ‌ها و VLAN ها استفاده می‌شود. این پورت‌ها در سوئیچ‌ها تنظیم می‌شوند و امکان ارسال و دریافت ترافیک‌های متعددی را بین VLAN ها فراهم می‌کنند. پورت ترانک به عنوان یک رابط بین سوئیچ‌ها عمل می‌کند و اطلاعات ترافیک بین VLAN ها را انتقال می‌دهد. با استفاده از پروتکل‌های مناسب مانند IEEE 802.1Q، برچسب‌گذاری VLAN در بسته‌های شبکه (Network Packets) صورت می‌گیرد و

سوئیچ‌ها می‌توانند بسته‌هایی را که بین VLAN ها انتقال می‌یابند، تشخیص داده و به مقصد مورد نظر هدایت کنند.

پورت ترانک علاوه بر انتقال ترافیک بین VLAN ها، می‌تواند اطلاعات مدیریتی مانند پروتکل‌های Spanning Tree (STP) و VLAN های موجود را بین سوئیچ‌ها منتقل کند. همچنین، از پورت‌های ترانک برای اتصال به سوئیچ‌های مرکزی که تعداد زیادی VLAN را پشتیبانی می‌کنند، استفاده می‌شود.

بنابراین، پورت ترانک در شبکه‌های کامپیوتری به پورتهای اشاره دارد که برای انتقال ترافیک بین VLAN ها و سوئیچ‌ها استفاده می‌شود و قادر به برجسب‌گذاری و تشخیص VLAN در بسته‌های شبکه است.

برجسب‌گذاری فریم یا Frame Tagging

برجسب‌گذاری فریم یا "Frame Tagging" در شبکه‌های کامپیوتری به فرایند اضافه کردن اطلاعات ویژگی VLAN به فریم‌های شبکه (Ethernet Frames) ارسالی اشاره دارد. این عمل به سوئیچ‌ها امکان می‌دهد تا بتوانند بسته‌های شبکه را بین VLAN ها جا به جا کنند و ترافیک را به صورت مناسب به مقصد مورد نظر هدایت کنند. در فرایند برجسب‌گذاری فریم، یک برجسب VLAN به هدر فریم شبکه اضافه می‌شود. این برجسب شامل اطلاعاتی است که شناسه VLAN را مشخص می‌کند. با این برجسب‌گذاری، سوئیچ‌ها قادر به تفکیک و هدایت ترافیک بین VLAN ها می‌شوند.

یکی از پروتکل‌های معمول برای برجسب‌گذاری فریم، استاندارد IEEE 802.1Q است. در این استاندارد، یک برجسب VLAN به هدر فریم اضافه می‌شود و اطلاعات VLAN را به سوئیچ‌ها منتقل می‌کند. با استفاده از برجسب‌های VLAN، سوئیچ‌ها می‌توانند بسته‌های شبکه را به مقصد مورد نظر در محدوده مطلوب هدایت کنند.

برجسب‌گذاری فریم در شبکه‌های کامپیوتری به سوئیچ‌ها امکان می‌دهد تا ترافیک را بین VLAN ها جدا کرده و به صورت موثرتری مدیریت کنند. این فرایند باعث بهبود عملکرد شبکه، افزایش امنیت و قابلیت اطمینان شبکه می‌شود.

سوال ۶

VTA یا "Virtual Terminal Access" در شبکه‌های کامپیوتری به مجموعه‌ای از ویژگی‌ها و قابلیت‌هایی اشاره دارد که به کاربران اجازه می‌دهد تا از طریق شبکه به صورت مجازی به ترمینال‌ها یا دستگاه‌های پایانی دسترسی پیدا کنند. VTA برای ارتباط با ترمینال‌ها از پروتکل‌هایی مثل Telnet یا SSH استفاده می‌کند. ویژگی‌ها و قابلیت‌های VTA عبارتند از

1. دسترسی از راه دور: VTA به کاربران امکان می‌دهد از راه دور و از هر جایی که به شبکه دسترسی داشته باشند، به ترمینال‌ها و دستگاه‌های پایانی متصل شوند. این امکان به کاربران

اجازه می‌دهد که به صورت مجازی به اطلاعات و منابع مرتبط با دستگاه‌های پایانی دسترسی پیدا کنند.

2. مدیریت مرکزی: با استفاده از VTA، امکان مدیریت مرکزی و کنترل بر ترمینال‌ها و دستگاه‌های پایانی فراهم می‌شود. این قابلیت به مدیران شبکه اجازه می‌دهد تا از طریق ارتباطات از راه دور به ترمینال‌ها دسترسی داشته باشند، تنظیمات را تغییر دهند، اطلاعات را بروزرسانی کنند و مشکلات را رفع کنند.
3. امنیت: VTA از پروتکل‌های امنیتی مانند SSH (Secure Shell) استفاده می‌کند که ارتباطات را رمزنگاری کرده و از حفظ امنیت اطلاعات اطمینان حاصل می‌کند. این به کاربران اجازه می‌دهد تا با اعتماد به نفس بیشتری به ترمینال‌ها و دستگاه‌های پایانی متصل شوند.
4. انعطاف‌پذیری: VTA امکان‌اتی را برای تنظیم و پیکربندی ارتباطات با ترمینال‌ها فراهم می‌کند. این قابلیت به مدیران شبکه اجازه می‌دهد تا پارامترهای مربوط به ارتباطات و نحوه دسترسی به ترمینال‌ها را تنظیم کنند.

به طور خلاصه، VTA به کاربران اجازه می‌دهد تا از راه دور و به صورت مجازی به ترمینال‌ها و دستگاه‌های پایانی دسترسی پیدا کنند. این قابلیت باعث می‌شود تا مدیران شبکه بتوانند ترمینال VTA یا "Virtual Terminal Access" به مجموعه‌ای از ویژگی‌ها و قابلیت‌های مربوط به دسترسی به ترمینال‌ها یا دستگاه‌های پایانی از راه دور اشاره دارد. VTA از پروتکل‌هایی مانند SSH و Telnet برای برقراری ارتباط با ترمینال‌ها استفاده می‌کند.

سوال ۷

VTA (Virtual Terminal Access) یک سیستم است که امکان دسترسی به ترمینال‌های مجازی را برای کاربران فراهم می‌کند. این سیستم می‌تواند در حالت‌های مختلف عمل کند، که به طور عمده به نحوه اتصال کاربران و نحوه مدیریت سیستم مرتبط است. در زیر توضیح داده شده است.

1. Single-User Mode (حالت تک‌کاربره): در این حالت، سیستم VTA فقط به یک کاربر اجازه می‌دهد که به ترمینال مجازی دسترسی پیدا کند. این حالت به کاربر امکان می‌دهد تا در یک جلسه تنها با سیستم تعامل کند.
2. Multi-User Mode (حالت چند کاربره): در این حالت، سیستم VTA به چندین کاربر به صورت همزمان اجازه می‌دهد که به ترمینال‌های مجازی دسترسی پیدا کنند. هر کاربر می‌تواند در جلسه‌ای مستقل با سیستم تعامل کند و دستورات خود را اجرا کند.
3. Remote Access Mode (حالت دسترسی از راه دور): در این حالت، کاربران از راه دور می‌توانند به سیستم VTA دسترسی پیدا کنند. این شامل دسترسی از طریق شبکه‌های اینترنت یا شبکه داخلی سازمانی می‌شود. کاربران می‌توانند ترمینال‌های مجازی را از هر مکانی راه‌اندازی کنند و با سیستم تعامل کنند.

4. **Administrative Mode** (حالت مدیریتی): این حالت برای مدیران سیستم VTA و مدیران شبکه قابل دسترسی است. آن‌ها می‌توانند تنظیمات سیستم را مدیریت کنند، کاربران را مدیریت کنند، محدودیت‌ها و سطوح دسترسی را تنظیم کنند و فعالیت‌های کاربران را نظارت کنند.
5. **Logging Mode** (حالت ثحالت‌های مختلف VTA یا همان Virtual Terminal Access) می‌توانند شامل موارد زیر باشند.

سوالات تحلیلی آزمایش ششم

سوال ۱

مزایا

1. حفاظت از آدرس IP و منابع شبکه: NAT به عنوان یک فایروال صفحه‌بندی (stateful firewall) عمل کرده و با ایجاد یک حاجز بین شبکه داخلی و شبکه بیرونی، تهدیدهای امنیتی را کاهش می‌دهد و منابع شبکه را محافظت می‌کند.
2. مدیریت آدرس‌دهی IP: با استفاده از NAT، می‌توان یک آدرس IP عمومی را برای یک شبکه داخلی استفاده کرد و برای تمام دستگاه‌ها درون شبکه آدرس‌های IP خصوصی اختصاص داد. این به مدیران شبکه امکان می‌دهد تا آدرس‌دهی IP را به راحتی مدیریت کنند و از تعداد محدود آدرس‌های IP عمومی استفاده کنند.
3. اشتراک اینترنت: NAT به میزبانان در شبکه داخلی اجازه می‌دهد تا از یک آدرس IP عمومی به عنوان مسیر خروجی برای دسترسی به اینترنت استفاده کنند. این به شرکت‌ها و خانواده‌ها که برای اتصال به اینترنت از یک آدرس IP عمومی محدود استفاده می‌کنند، امکان می‌دهد تا بیشترین بهرهوری را از این آدرس ببرند.

معایب

1. مسائل ارتباطی: استفاده از NAT ممکن است باعث کاهش کیفیت ارتباطات شبکه شود. این موضوع مخصوصاً در برخی از برنامه‌ها و خدماتی که برای اتصال به شبکه دیگری نیاز دارند (مانند برنامه‌های P2P)، مشکل ساز می‌شود.
2. پیچیدگی پیکربندی: NAT نیازمند پیکربندی صحیح است و پیکربندی نادرست می‌تواند منجر به مشکلات در شبکه شود. تنظیمات پیش فرض NAT ممکن است برای برخی از برنامه‌ها و سرویس‌ها به‌درستی کار نکند و نیاز به تنظیمات خاص داشته باشد.
3. محدودیت‌ها در اتصالات ورودی: NAT معمولاً به عنوان روشی برای سهولت در اتصال دستگاه‌ها در شبکه داخلی به اینترنت استفاده می‌شود، اما در برخی موارد ممکن است محدودیت‌هایی به وجود آید. مثلاً در صورتی که بیش از حد تعداد اتصالات همزمان

به اینترنت در شبکه داخلی وجود داشته باشد، NAT ممکن است محدودیت‌هایی در این اتصالات ایجاد کند.

4. کاهش کارایی: استفاده از NAT ممکن است منجر به کاهش کارایی شبکه شود. هنگامی که بسته‌ها بین شبکه داخلی و شبکه بیرونی منتقل می‌شوند، NAT باید اطلاعات مربوط به پورت‌ها و آدرس‌ها را تغییر دهد و این عملیات ممکن است زمان و منابع سیستم را بگیرد.

به طور کلی، استفاده از NAT در شبکه‌های کامپیوتری می‌تواند مزایا و معایبی داشته باشد و بسته به محیط و نیازهای شبکه، می‌تواند به عنوان یک راه‌حل مناسب مدنظر قرار گیرد یا نه.

سوال ۲

UPnP یا Universal Plug and Play یک پروتکل شبکه است که به دستگاه‌ها در شبکه اجازه می‌دهد تا به صورت خودکار با یکدیگر ارتباط برقرار کنند و به اشتراک بگذارند. با استفاده از UPnP، دستگاه‌ها می‌توانند خودکار تنظیمات شبکه را پیکربندی کنند و به صورت اتوماتیک دریافت‌کننده‌ها و ارائه‌دهنده‌هایی را کشف کنند. UPnP در ارتباط با NAT در شبکه کاربرد دارد. یکی از مشکلات NAT این است که ارتباطات ورودی به دستگاه‌های داخلی شبکه را محدود می‌کند. این بدان معنی است که دستگاه‌های بیرونی نمی‌توانند به طور مستقیم به دستگاه‌های داخلی متصل شوند.

UPnP به عنوان یک راه حل برای این مشکل ایجاد شده است. با استفاده از UPnP، دستگاه‌های داخلی می‌توانند درخواست‌ها و ارتباطات خود را به روتر یا دروازه شبکه ارسال کنند و UPnP دروازه را به صورت خودکار تنظیم می‌کند تا به دستگاه داخلی ارتباط برقرار کند. این به دستگاه‌های بیرونی این امکان را می‌دهد تا به طور شفاف و بدون نیاز به تنظیمات دستی به دستگاه‌های داخلی در شبکه دسترسی پیدا کنند.

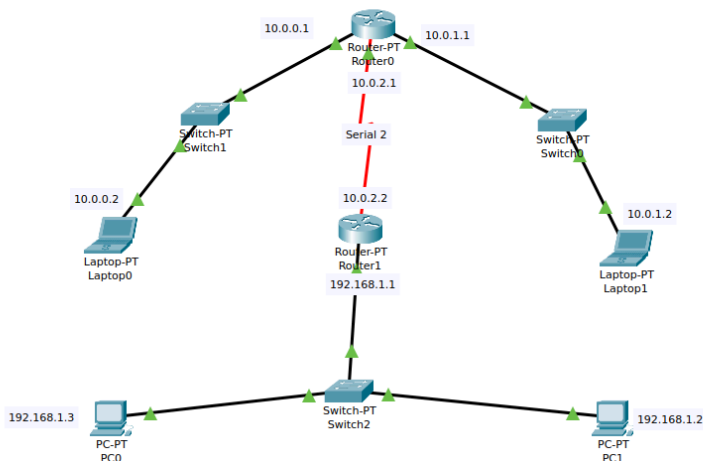
به طور مثال، اگر یک دستگاه در شبکه داخلی با UPnP مجهز باشد و یک برنامه‌ی پخش رسانه‌ای روی آن دستگاه اجرا شود، UPnP می‌تواند به طور خودکار پورت‌های مورد نیاز را در روتر باز کند و اجازه دسترسی به این برنامه را از سایر دستگاه‌ها در شبکه بدهد. به طور خلاصه، UPnP که به عنوان یک پروتکل شبکه عمل می‌کند، با استفاده از NAT می‌تواند به دستگاه‌ها در شبکه داخلی امکان دسترسی از بیرون را بدهد و ارتباطات بین دستگاه‌ها را تسهیل کند.

گزارش آزمایش ششم

مرحله اول-پایاده سازی توپولوژی

گام اول

در گام اول تمامی روترها، سوئیچ ها end device ها و اتصالات میان آنها را مطابق شکل صورت آزمایش در جای خود قرار دادیم. شکل ذیل حالت نهایی است.



گام دوم

آی پی دهی هاست و نتورک-توضیحات تشریحی

در مرحله دوم شروع به اطلاق IP به تک تک دیوایس ها و interface روتر ها به صورت Classfull کردیم. ما تنها نیاز به یک شبکه میان ۲ روتر مان و ۳ شبکه (یکی پرایویت و ۲ شبکه دیگر public) برای هاست های متصل به سوئیچ ها داشتیم. شبکه پرایویت را برابر 192.168.1.0، و برای ۳ شبکه دیگر از آدرس های شبکه 10.0.0.0، 10.0.1.0 و 10.0.2.0 استفاده کردیم. همانطور که در تصویر بالا مشخص است دیوایس های ۴ و ۵ در شبکه 194.0.0.0 قرار دارند که معادل 0000 برای ۴ بیت بالای بایت چهارم است، لپ تاپ ۰ دارای آی پی 10.0.0.2 لپ تاپ ۱ دارای آی پی 10.0.1.2 و PC های ۰ و ۱ به ترتیب دارای آی پی های 192.168.1.3 و 192.168.1.2

و 192.168.1.2 هستند. پس از این گام، Default Gateway را برای هر دیوایس معادل آی پی اینترفیس روتر متصل به آن شبکه قرار دادیم

قسمت اول static nat

آی پی دهی هاست و نتورک-جدول

Device name	Ip	Mask	Default Gateway	Network	Port	Connector Router
PC0	192.168.1.3	255.255.255.0	192.168.1.1	192.168.1.0	FastEthernet0	Router 1
PC1	192.168.1.2	255.255.255.0	192.168.1.1	192.168.1.0	FastEthernet0	Router 1
Laptop0	10.0.0.2	255.255.255.0	10.0.0.0	10.0.0.1	FastEthernet0	Router 0
Laptop1	10.0.1.2	255.255.255.0	10.0.1.0	10.0.1.1	FastEthernet0	Router 0

گام سوم

آی پی دهی روتر ها-توضیحات تشریحی

در مرحله سوم شروع کردیم به اطلاق IP به تمامی اینترفیس های روتر هایی که از آنها استفاده کردیم. همانطور که در تصویر بالا مشخص است **جفت** روتر ۱ و ۰ در شبکه 10.0.2.0 قرار دارند.

گام چهارم

تنظیم روتینگ روتر ها

در این مرحله با فعال کردن پروتکل RIP بر روی روتر ها، روتینگ را در هر روتر انجام دادیم، به این منظور، در روتر ۰ دستورات ذیل را اعمال کردیم:

```
en
config t
router rip
version 2
Network 10.0.0.0
Network 10.0.1.0
Network 10.0.2.0
```

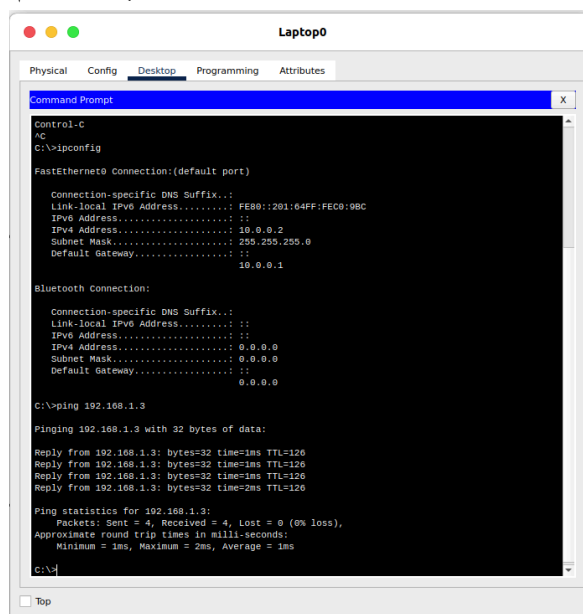
و همینطور در روتر ۱ دستورات ذیل را وارد کردیم:

```
en
config t
router rip
version 2
Network 10.0.2.0
Network 192.168.1.0
```

مرحله پایانی

پینگ گرفتن

در پایان برای اطمینان از اتصالات و کانفیگ ها هاست های مختلف را پینگ گرفتیم و موفقیت آمیز بود.



```
Command Prompt
control-c
AC
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::201:64FF:FE00:9BC
    IPv4 Address. . . . .: 10.0.0.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .:
                                10.0.0.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .:
    IPv6 Address. . . . .:
    IPv4 Address. . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .:
                                0.0.0.0

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

مرحله دوم-static nat

راه اندازی

در این مرحله با دستورات ذیل static nat را در روتر متصل به شبکه پرایوت خود راه اندازی کردیم.

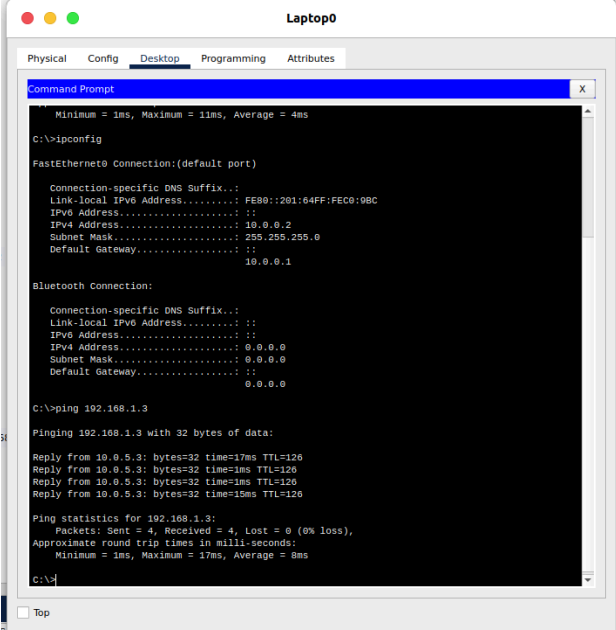
```
int fa0/0
ip nat inside
```

```
exit
int se2/0
ip nat outside
exit
```

```
ip nat inside source static 192.168.1.3 10.0.5.3
ip nat inside source static 192.168.1.2 10.0.5.2
ip nat inside source static 192.168.1.1 10.0.5.1
```

همانطور که مشخص است، ابتدا جهت ورود و خروج را برای روتر مشخص کرده و پس از آن برای تک تک آی پی های درون شبکه 192.168.1.0 یک آی پی معادل در نظر گرفتیم.

پینگ گرفتن



```
Minimum = 1ms, Maximum = 11ms, Average = 4ms

C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . . : FE80::201:64FF:FEC0:9BC
    IPv4 Address. . . . . : 10.0.0.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.0.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . . :
    IPv6 Address. . . . . :
    IPv4 Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 0.0.0.0

C:\>ping 192.168.1.3

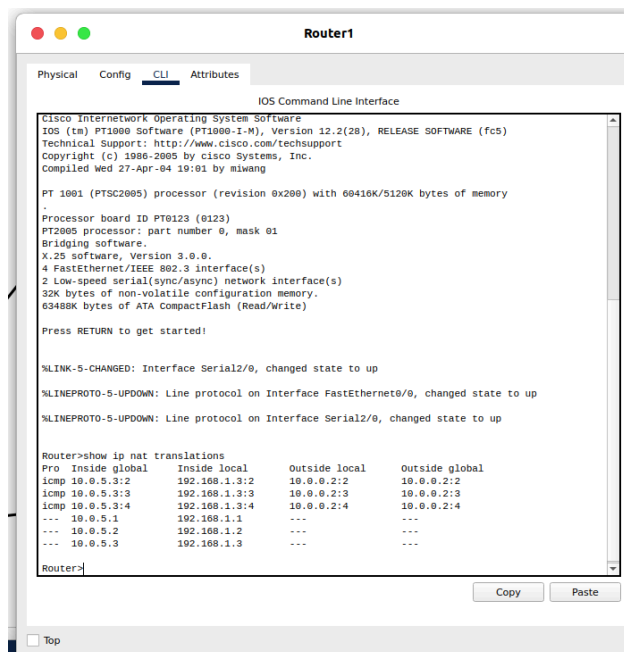
Pinging 192.168.1.3 with 32 bytes of data:

Reply from 10.0.5.3: bytes=32 time=17ms TTL=120
Reply from 10.0.5.3: bytes=32 time=1ms TTL=120
Reply from 10.0.5.3: bytes=32 time=1ms TTL=120
Reply from 10.0.5.3: bytes=32 time=15ms TTL=120

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 17ms, Average = 8ms

C:\>
```

همانطور که در تصویر بالا مشخص است، ما آی پی 192.168.1.3 را پینگ کردیم، اما پاسخ برگشته شده با آی پی 10.0.5.3 می باشد.



همانطور که در تصویر بالا مشخص شده، ۳ بسته icmp که در ping گرفتن رد و بدل خواهد شد ارسال شده که در آن خروجی چه آی پی لوکال چه آی پی پرایوت آن 10.0.0.2 است که همان هاستی است که از آن 192.168.1.3 را پینگ کردیم. از طرف مقابل ورودی یا همان دیوایسی که آنرا پینگ گرفتیم، در لوکال همان 192.168.1.3 است که آی پی گلوبال آن برابر 10.0.5.3 یا همان آی پی ای که به صورت static در nat اعمال کردیم است.

مرحله سوم-dynamic nat

راه اندازی

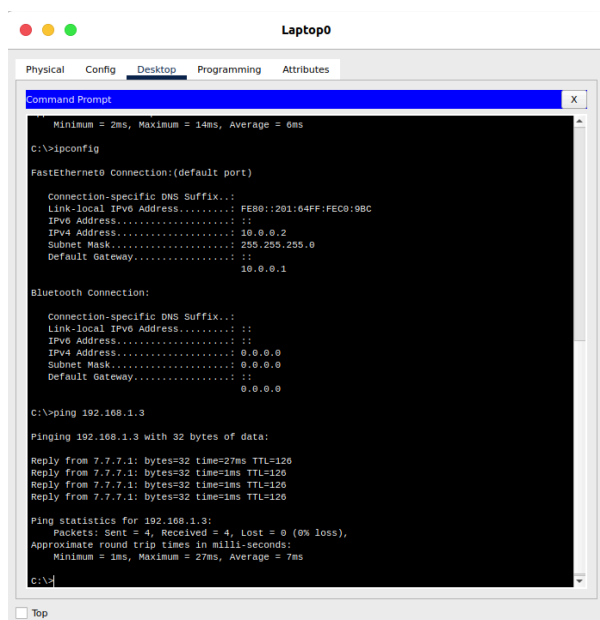
در این مرحله با دستورات ذیل dynamic nat را در روتر متصل به شبکه پرایوت خود راه اندازی کردیم.

```
int fa0/0
ip nat inside
exit
int se2/0
ip nat outside
exit
ip nat pool mypool 7.7.7.1 7.7.7.5 netmask 255.255.255.0
access-list 1 permit 192.168.1.0 0.0.0.255
```

ip nat inside source list 1 pool mypool

همانطور که مشخص است، ابتدا جهت ورود و خروج را برای روتر مشخص کرده و پس از آن یک poll در بازه 7.7.7.1 تا 7.7.7.5 تعریف کردیم و پس از آن یک access list برای شبکه پرایوت تعریف کردیم و در گام نهایی access list را به poll تعریف شده متصل کردیم.

پینگ گرفتن



```
Minimum = 2ms, Maximum = 14ms, Average = 6ms

C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::201:04FF:FE08:9BC
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 18.0.0.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                   18.0.0.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                   0.0.0.0

C:\>ping 192.168.1.3

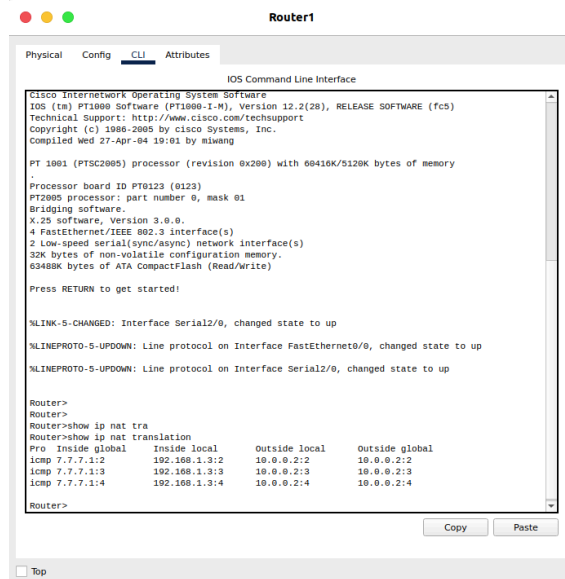
Pinging 192.168.1.3 with 32 bytes of data:

Reply from 7.7.7.1: bytes=32 time=27ms TTL=126
Reply from 7.7.7.1: bytes=32 time=1ms TTL=126
Reply from 7.7.7.1: bytes=32 time=1ms TTL=126
Reply from 7.7.7.1: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 27ms, Average = 7ms

C:\>
```

همانطور که در تصویر بالا مشخص است، ما آی پی 192.168.1.3 را پینگ کردیم، اما پاسخ برگشته شده با آی پی 7.7.7.1 می باشد.



همانطور که در تصویر بالا مشخص شده، ۳ بسته icmp که در ping گرفتن رد و بدل خواهد شد ارسال شده که در آن خروجی چه آی پی لوکال چه آی پی پرایوت آن 10.0.0.2 است که همان هاستی است که از آن 192.168.1.3 را پینگ کردیم. از طرف مقابل ورودی یا همان دیوایسی که آنرا پینگ گرفتیم، در لوکال همان 192.168.1.3 است که آی پی گلوبال آن برابر 7.7.7.1 یا یکی از آی پی هایی که به صورت dynamic در بازه pool اعمال کردیم است.

مرحله چهارم-Overloading nat

راه اندازی

در این مرحله با دستورات ذیل Overloading nat را در روتر متصل به شبکه پرایوت خود راه اندازی کردیم.

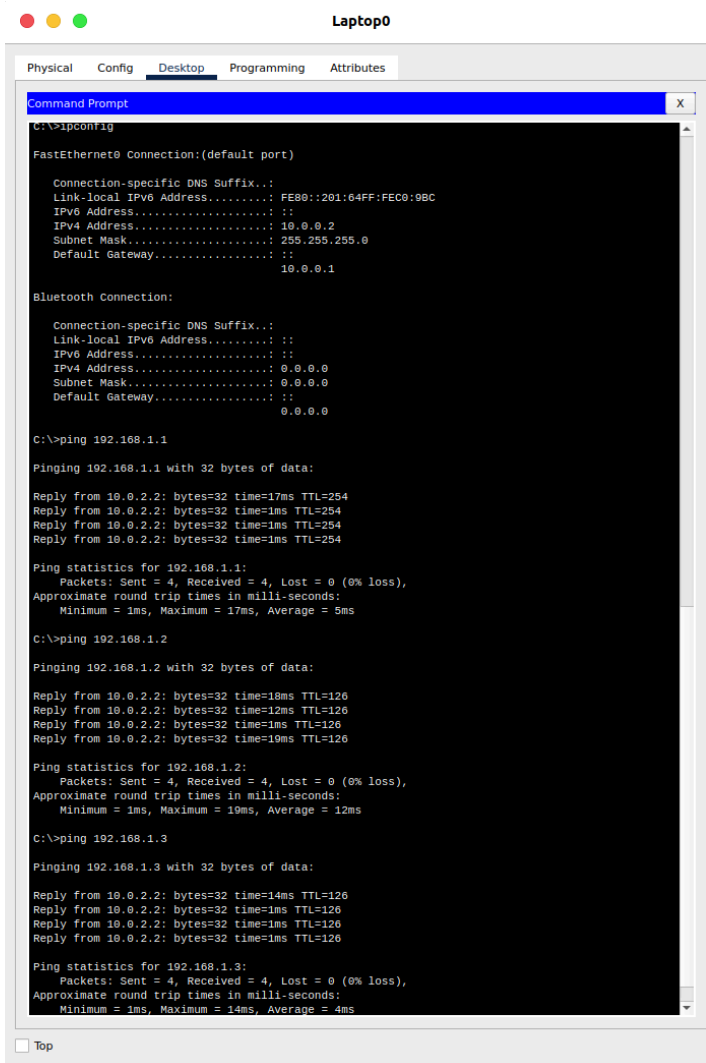
```

int fa0/0
ip nat inside
exit
int se2/0
ip nat outside
exit
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 interface se2/0 overload

```

همانطور که مشخص است، ابتدا جهت ورود و خروج را برای روتر مشخص کرده و پس از آن ابتدا یک access list برای شبکه پرایوت به همراه wild card تعریف کردیم و در گام نهایی access list را به اینترفیس Serial 2 روتر ۱ با آی پی 10.0.2.2 وصل کردیم.

پینگ گرفتن



```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::201:64FF:FEC0:9BC
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 10.0.0.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                10.0.0.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .:
    IPv6 Address . . . . .:
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .:
                                0.0.0.0

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 10.0.2.2: bytes=32 time=17ms TTL=254
Reply from 10.0.2.2: bytes=32 time=1ms TTL=254
Reply from 10.0.2.2: bytes=32 time=1ms TTL=254
Reply from 10.0.2.2: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 17ms, Average = 5ms

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 10.0.2.2: bytes=32 time=18ms TTL=126
Reply from 10.0.2.2: bytes=32 time=12ms TTL=126
Reply from 10.0.2.2: bytes=32 time=1ms TTL=126
Reply from 10.0.2.2: bytes=32 time=19ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 19ms, Average = 12ms

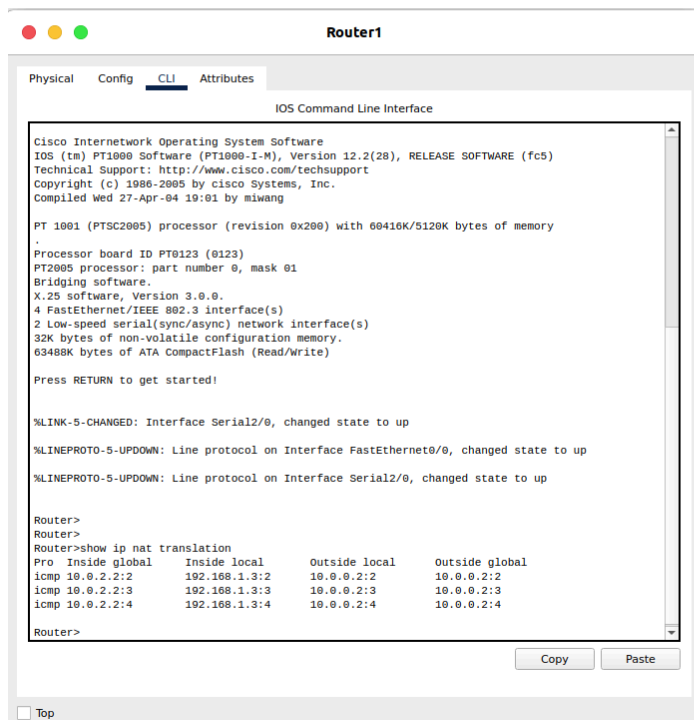
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 10.0.2.2: bytes=32 time=14ms TTL=126
Reply from 10.0.2.2: bytes=32 time=1ms TTL=126
Reply from 10.0.2.2: bytes=32 time=1ms TTL=126
Reply from 10.0.2.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 14ms, Average = 4ms
```

همانطور که در تصویر بالا مشخص است، ما تمام آی پی های داخل شبکه 192.168.1.0 یعنی 192.168.1.1، 192.168.1.2 و 192.168.1.3 را پینگ کردیم، و در تمامی این پینگ ها، پاسخ برگشته شده با آی پی 10.0.2.2 بود.



همانطور که در تصویر بالا مشخص شده، ۳ بسته icmp که در ping گرفتن رد و بدل خواهد شد ارسال شده که در آن خروجی چه آی پی لوکال چه آی پی پرایوت آن 10.0.0.2 است که همان هاستی است که از آن 192.168.1.3 را پینگ کردیم. از طرف مقابل ورودی یا همان دیوایسی که آنرا پینگ گرفتیم، در لوکال همان 192.168.1.3 است که آی پی گلوبال آن برابر 10.0.2.2 یا همان آی پی اینترفیس Serial 2 روتر ۱ است که در تنظیمات nat به صورت Overload وارد کردیم.

در این بخش برای Overloading از اینترفیس روتر متصل به شبکه پرایوت بجای استفاده از Pool استفاده کردیم. چند مورد از دلایل این کار می‌توان به موارد ذیل اشاره کرد:

1. انعطاف پذیری: رابط‌ها امکاناتی را برای کنترل مختلف نوع ترافیک شبکه فراهم می‌کنند.
2. انتزاع: رابط‌ها جزئیات اجرایی خاص را پنهان می‌کنند و این امکان را فراهم می‌کنند که به راحتی مرتبط با رفتار سیستم باشد. این انتزاع می‌تواند طراحی را ساده‌تر کرده و به تدارک آن ارزیابی راحت‌تری فراهم کند.
3. مقیاس‌پذیری: رابط‌ها می‌توانند به مقیاس‌پذیری کمک کنند با اینکه امکان اضافه کردن پیاده‌سازی‌های جدید را بدون تأثیر بر کد موجود فراهم می‌کنند. این به خصوص در حالت‌هایی مفید است که نیاز به پشتیبانی از پروتکل‌ها یا فناوری‌های جدید در شبکه باشد بدون اینکه موجب ایجاد اختلال شود.
4. مدولاریت: رابط‌ها با جدا کردن منطق کنترل ترافیک شبکه از مکانیزم‌های خاص استفاده شده برای ترجمه، مدولاریت را ترویج می‌دهند. این جداکردن مسائل اهمیتی دارد و می‌تواند سازماندهی کد را بهبود بخشد و آن را بهتر قابل مدیریت و گسترش بیشتری کند.

5. آزمایش و اشکال زدایی: استفاده از رابطه‌ها می‌تواند آزمایش و اشکال زدایی را آسان‌تر کند زیرا امکان دارد که رابطه را برای این اهداف آزمایشی مساحتی دهیم. این امکان را فراهم می‌کند که به طور جامع‌تر رفتار سیستم را تحت شرایط مختلف آزمایش کنیم.