گزارش سوم آزمایشگاه شبکه های کامپیوتری

اعضای گروه:
پارسا عصمت‌لو
سهیل شهرابی

فهرست مطالب

پیش گزارش آزمایش چهارم

سوال ۱)

این روش به روتر ها کمک میکند که بهترین راه را برای فوروارد کردن بسته ها پیدا کنند. وقتی که روتر از چند سورس اطلاعات مسیر را دریافت میکند باید مورد اعتماد ترین و قابل قبول ترین مسیر را انتخاب کند. Administrative distance یک واحد عددی میباشد که به پروتکل یا سورس داده میشود که مورد اعتماد بودن یا قابل استفاده بودن آن را بررسی میکند و هر چه این رقم پایین تر باشد بهتر میباشد.

سوال ۲)

در اینجا یک نمای کلی ساده از نحوه عملکرد پروتکل های distance vector وجود دارد:

- Initialization: هنگامی که روتر راه اندازی می شود یا به یک شبکه می پیوندد، جدول مسیریابی خود را مقداردهی اولیه می کند. در ابتدا، فقط در مورد شبکه های متصل مستقیم می داند و هزینه 0 را به آن مسیرها اختصاص می دهد.
- Advertisement: روترها به صورت دوره ای به روز رسانی مسیریابی را که به عنوان تبلیغات یا به روز رسانی مسیریابی شناخته می شوند، به روترهای همسایه خود ارسال می کنند. این به‌روزرسانی‌ها حاوی اطلاعاتی درباره شبکه‌هایی است که می‌شناسند و هزینه‌های مرتبط با آن‌ها.
- Neighbor Exchange: روترها به‌روزرسانی‌های مسیریابی را با همسایگان متصل خود مبادله می‌کنند. هر روتر جدول مسیریابی کامل خود یا فقط تغییرات را از آخرین به روز رسانی ارسال می کند.
- Distance Calculation: با دریافت به روز رسانی مسیریابی، یک روتر مسیرهای تبلیغ شده را بررسی می کند و کل هزینه رسیدن به هر مقصد را محاسبه می کند. هزینه معمولاً بر اساس عواملی مانند delay ،bandwidth ،hop countیا ترکیبی از این موارد است.
- Update and Selection: پس از محاسبه هزینه ها، روتر جدول مسیریابی خود را با مسیرهای جدید یا اصلاح شده به روز می کند. اگر مسیر بهتر (هزینه کمتر) به مقصدی کشف شود، جایگزین مسیر موجود در جدول مسیریابی می شود. روتر همچنین روتر همسایه ای را که از آن بهترین مسیر را دریافت کرده است، یادداشت می کند.
- Loop Prevention: پروتکل‌های distance vector از تکنیک‌های مختلفی برای جلوگیری از حلقه‌های مسیریابی استفاده می‌کنند، که زمانی رخ می‌دهد که روترها به طور مداوم مسیرها را برای یکدیگر تبلیغ می‌کنند. یکی از روش‌های رایج استفاده از محدودیت‌های تعداد پرش است، که در آن حداکثر تعداد پرش‌ها تعیین می‌شود و مسیرهایی که بیش از حد مجاز هستند غیرقابل دسترسی در نظر گرفته می‌شوند.
- Convergence: با گذشت زمان، روترها به تبادل به روز رسانی های مسیریابی و به روز رسانی جداول مسیریابی خود بر اساس اطلاعات دریافتی ادامه می دهند. در نهایت، روترها در یک مجموعه پایدار از مسیرها همگرا می شوند، جایی که هر روتر بهترین مسیر را برای رسیدن به هر مقصد شبکه تعیین کرده است.

سوال ۳)

برای حل Routing Loops در شبکه‌های کامپیوتری، می‌توان از روش‌ها و تکنیک‌های زیر استفاده کرد:

1) Split Horizon : در این روش، یک مسیریاب اطلاعات مربوط به یک مسیر را که از طریق یک رابط دریافت کرده، به همان مسیریاب برگردانده و در شبکه اعلام نمی‌کند. این باعث می‌شود که مسیریاب‌ها نتوانند به طور مداوم اطلاعات را به یکدیگر ارسال کنند و حلقه‌های مسیریابی ایجاد نشود.
2) Poison Reverse : در این روش، هنگامی که یک مسیریاب متوجه شود یک مسیر ناموفق است، این اطلاعات را به مسیریابی که از آن دریافت شده برمی‌گرداند، اما با استفاده از یک متریک بی‌نهایت یا به عنوان یک مسیر ناموجود. با این کار، مسیریاب‌ها به سرعت از شکست اطلاع‌رسانی مطلع می‌شوند و جداول مسیریابی خود را به روزرسانی کرده و حلقه‌های مسیریابی را از بین می‌برند.

3) Route Poisoning : در این روش، مسیریاب متوجه شکست یک مسیر می‌شود و متریک یا هزینه آن را به مقدار بی‌نهایت یا غیرقابل دسترس تنظیم می‌کند. با نشان دادن مسیر به عنوان غیرقابل دسترس، مسیریاب‌ها سریعاً جدول مسیریابی خود را بروزرسانی و از استفاده از مسیر ناموفق جلوگیری می‌کنند. این روش به جلوگیری از استفاده مداوم از یک مسیر ناموفق کمک می‌کند.
4) Hold-Down Timers : تایمرهای تاخیر برای مدتی جلوی پذیرش به‌روزرسانی‌های مربوط به یک مسیر را برمی‌دارند. وقتی مسیریاب اطلاعاتی دریافت کرد که نشان دهنده تغییر یا شکست یک مسیر است، تایمر تاخیر را شروع می‌کند. در طول این بازه زمانی، مسیریاب از هر گونه به‌روزرسانی یا اطلاعات مربوط به آن مسیر چشم‌پوشی می‌کند. این کار به استحکام جداول مسیریابی کمک می‌کند و از تغییرات سریع و ناپایدار در مسیرها جلومی‌گیرد.
5) Route Summarization : در این روش، چندین مسیر شبکه را در یک مسیر خلاصه تجمیع می‌کنند. با کاهش تعداد مسیرهای اعلام شده، احتمال حلقه‌های مسیریابی کاهش می‌یابد. خلاصه‌سازی مسیر معمولاً در طراحی شبکه‌های سلسله‌مراتبی استفاده می‌شود، که در آن مسیریاب‌های سطح بالاتر مسیرهای دریافت شده از مسیریاب‌های سطح پایین‌تر را خلاصه می‌کنند.
6) بهینه‌سازی پروتکل مسیریابی: برخی از پروتکل‌های مسیریابی پیشرفته مانند EIGRP از الگوریتم‌ها و تکنیک‌های پیشرفته استفاده می‌کنند تا بهینه‌سازی به‌روزرسانی جداول مسیریابی و جلوگیری از حلقه‌های مسیریابی. این پروتکل‌ها عموماً از الگوریتم‌هایی مانند الگوریتم به روزرسانی پخش شده (DUAL) برای محاسبه مسیرهای بدون حلقه و فراهم کردن همگرایی سریع استفاده می‌کنند.

مهم است به این نکته توجه کنید که این تکنیک‌ها ممکن است به صورت خاص برای پروتکل‌های مسیریابی خاصی طراحی شده باشند و ممکن است برای همه پروتکل‌های مسیریابی قابل اعمال نباشند. علاوه بر این، مدیران شبکه باید طراحی و پیکربندی مناسبی را برای توپولوژی شبکه خود انجام دهند تا احتمال ایجاد حلقه‌های مسیریابی در ابتدا به حداقل برسد.

سوال ۴)

Routing Information Protocol یا RIP یک پروتکل مسیریابی از نوع distance-vector است که در شبکه‌های کامپیوتری استفاده می‌شود. این پروتکل برای تبادل اطلاعات مسیریابی بین مسیریاب‌ها در یک شبکه طراحی شده است. RIP از معیار hop count برای تعیین مسیر مناسب به یک شبکه مقصد استفاده می‌کند.

اینجا چگونگی عملکرد RIP را بررسی می‌کنیم:

1) مسیریاب‌های همسایه اطلاعات مسیریابی را تبادل می‌کنند: مسیریاب‌های RIP به طور دوره‌ای اطلاعات مسیریابی خود را به مسیریاب‌های همسایه خود ارسال می‌کنند. این بروزرسانی‌ها شامل اطلاعاتی درباره شبکه‌هایی است که مسیریاب می‌تواند به آنها دسترسی داشته باشد و تعداد هاپ برای هر شبکه است.
2) محاسبه معیار: RIP از تعداد هاپ به عنوان معیار استفاده می‌کند تا بهترین مسیر به یک شبکه را تعیین کند. هر مسیریاب هنگام فوروارد کردن بروزرسانی مسیریابی به یک مسیریاب همسایه، تعداد هاپ را یک واحد افزایش می‌دهد. حداکثر تعداد هاپ مجاز در RIP برابر با ۱۵ است و یک تعداد هاپ ۱۶ به عنوان یک شبکه ناموجود در نظر گرفته می‌شود.
3) به‌روزرسانی جداول مسیریابی: وقتی یک مسیریاب بروزرسانی مسیریابی را از یک مسیریاب همسایه دریافت می‌کند، این بروزرسانی را با جدول مسیریابی موجود خود مقایسه می‌کند. اگر بروزرسانی دریافتی مسیر بهتری (تعداد هاپ کمتر) به یک شبکه را ارائه دهد، مسیریاب جدول مسیریابی خود را با اطلاعات جدید به‌روز می‌کند.
4) ارسال به‌روزرسانی‌های فوری: علاوه بر به‌روزرسانی‌های دوره‌ای، مسیریاب‌های RIP همچنین به‌روزرسانی‌های فوری را ارسال می‌کنند هنگامی که تغییری در توپولوژی شبکه رخ می‌دهد. این امر اطمینان می‌دهد که اطلاعات مسیریابی به سرعت در پاسخ به تغییرات شبکه به‌روزرسانی شود.

RIP از تایمرها برای کنترل عملکرد خود استفاده می‌کنتایمرهای پروتکل RIP عبارتند از:

1) تایمر به‌روزرسانی (Update Timer): این تایمر فاصله زمانی را کنترل می‌کند که مسیریاب‌ها به مسیریاب‌های همسایه خود به‌روزرسانی مسیریابی ارسال کنند. به طور پیش‌فرض، تایمر به‌روزرسانی به ۳۰ ثانیه تنظیم شده است، به این معنی که به‌روزرسانی‌های مسیریابی هر ۳۰ ثانیه یکبار ارسال می‌شوند.
2) تایمر نامعتبر (Invalid Timer): این تایمر تعیین می‌کند چقدر زمانی مسیریاب منتظر می‌ماند تا یک مسیر را به عنوان نامعتبر یا غیرقابل دسترس در نظر بگیرد. اگر یک مسیریاب برای یک مسیر دریافتی در زمان مشخص‌شده توسط تایمر نامعتبر بروزرسانی دریافت نکند، آن مسیر را به عنوان نامعتبر علامت‌گذاری می‌کند. مقدار پیش‌فرض برای تایمر نامعتبر ۱۸۰ ثانیه است (۶ برابر تایمر به‌روزرسانی).

علاوه بر این، RIP از تایمرهای دیگری مانند تایمر Hold-down و تایمر Flush برای مدیریت اطلاعات مسیریابی و جلوگیری از حلقه‌های مسیریابی استفاده می‌کند. این تایمرها به پایداری و همگرایی پروتکل مسیریابی RIP در شبکه کمک می‌کنند.

سوال ۵)

Routing Information Protocol یا RIP و Interior Gateway Routing Protocol یا IGRP هر دو پروتکل مسیریابی هستند که در شبکه‌های کامپیوتری استفاده می‌شوند، اما تفاوت‌هایی دارند:

1) الگوریتم مسیریابی:
- RIP: RIP از الگوریتم مسیریابی distance-vector استفاده می‌کند. بر اساس معیار تعداد هاپ، بهترین مسیر به یک شبکه مقصد را محاسبه می‌کند.
- IGRP: IGRP از یک الگوریتم مسیریابی پیشرفته به نام composite metric استفاده می‌کند. این الگوریتم با در نظر گرفتن عواملی مانند پهنای باند، تاخیر، قابلیت اطمینان و بار، بهترین مسیر را تعیین می‌کند.

2) زمان همگرایی:
- RIP: زمان همگرایی RIP نسبتاً کندتر از IGRP است. زمان همگرایی به زمانی می‌گوید که پروتکل مسیریابی برای سازگار شدن با تغییرات شبکه و به‌روزرسانی جداول مسیریابی نیاز دارد.
- IGRP: IGRP زمان همگرایی سریعتری دارد به دلیل الگوریتم مسیریابی پیشرفته خود. این پروتکل به سرعت به تغییرات شبکه سازگار می‌شود و جداول مسیریابی را به‌روز می‌کند.

3) قابلیت مقیاس‌پذیری:
- RIP: RIP در مقیاس‌پذیری محدود است. حداکثر تعداد هاپ در RIP برابر با 15 است، به این معنی که فقط برای شبکه‌های نسبتاً کوچک مناسب است.
- IGRP: IGRP برای مدیریت شبکه‌های بزرگ طراحی شده است. حداکثر تعداد هاپ در IGRP برابر با 100 است که امکان پوشش مسافت‌های بزرگتر را فراهم می‌کند.

4. معیارها:

- RIP: RIP از معیار تعداد هاپ ساده برای تعیین بهترین مسیر استفاده می‌کند. تعداد روترها (هاپ‌ها) بین منبع و مقصد را محاسبه می‌کند. این معیار ممکن است واقعیت شرایط شبکه را به‌خوبی نشان ندهد.
- IGRP: IGRP از یک معیار composite metric استفاده می‌کند که عوامل متعددی از جمله پهنای باند، تاخیر، قابلیت اطمینان و بار را در نظر می‌گیرد. این امکان را می‌دهد که انتخاب مسیر بر اساس شرایط شبکه دقیق‌تر انجام شود.

به طور کلی، IGRP ویژگی های پیشرفته تر و مقیاس پذیری بهتری را در مقایسه با RIP ارائه می دهد. با این حال، RIP برای پیکربندی ساده‌تر است و به طور گسترده در میان فروشندگان مختلف پشتیبانی می‌شود. انتخاب بین RIP و IGRP به اندازه شبکه، پیچیدگی و الزامات خاص بستگی دارد.

سوالات تحلیلی آزمایش سوم

سوال ۱)

مزایا

- از آنجایی که مسیر یابی به صورت دستی است، از الگوریتم خاصی استفاده نمی‌شود، پس رفتار شبکه کاملا قابل پیش‌بینی است و می‌توان مسیر های بسته ها را از قبل پیش‌بینی کرد، به همین خاطر دیباگ و پیدا کردن منشا مشکل در این شبکه آسان است.
- به خاطر اینکه از الگوریتمی برای مسیریابی استفاده نمی‌شود، در این میان پردازش خاصی برای ران کردن این الگوریتم های مسیریابی وجود ندارد و سرعت بالاتر می‌رود. همچنین به همین خاطر از منابع کمتری استفاده می‌شود.

معایب

- تنظیم اولیه شبکه، اطلاق آی پی ها بسیار سخت است و با بزرگ تر شدن شبکه عملا غیر ممکن خواهد شد. همچنین در صورت بزرگ شدن شبکه، آپدیت کردن جدول مسیریابی روتر ها بسیار زمان بر (بخصوص برای شبکه های بزرگ) است.
- در ساخت جدول مسیریابی احتمال بروز خطا زیاد است و تست کردن تمامی connection های ممکن بسیار وقت گیر است. به همین علت نمی‌توانیم از درست بودن تمامی جداول مسیریابی اطمینان داشته باشیم چرا که مثلا اگر ۱۰۰ دیوایس در شبکه باشد باید ۹۹۰۰ اتصال را تست کنیم.
- وقتی در این شبکه مشکلی بوجود بیاید، مکانیزمی برای رفع مشکل وجود ندارد و باید تمامی تغییرات به صورت دستی به جداول مسیریابی اعمال شود.

سوال۲)

- اگر مقصد بسته دریافتی توسط روتر با هیچ یک از آی پی های اینترفیس های روتر مطابقت نداشت و همچنین شبکه آن در روت های نوشته شده در جدول مسیریابی موجود نبود، این بسته به Default route می‌رود. برای مثال گفته شده Default route این روتر برابر با ip 128.1.0.2 است، این عبارت به این معناست که روتر با یک بسته از شبکه ای روبرو شده که دقیقا تایین نشده این شبکه باید به کدام آدرس فرستاده شود. در شرایط بسته به صورت دیفالت به اینترفیس 128.1.0.2 ارسال می‌شود.
- وقتی که ترافیک شبکه بالا می‌رود و روتر تصمیم میگیرد بسته های دریافتی را Drop کند آنها را به مسیر Null می‌فرستد و در عمل بسته دریافتی miss می‌شود.
- اگر برای مقصد یک بسته بیش از یک مسیر در جدول مسیریابی وجود داشته باشه، روتر به مسیر های متفاوت اولویت های متغیری می‌دهد. در این شرایط یک مسیر مرجع نیز وجود دارد که اولویت آن می‌تواند تغییر کند.
- اگر مسیر های دیگر ترافیک سنگینی داشته باشند یا به هر دلیلی قطع باشند، روتر از مسیر Backup استفاده میکند. در صورتی که برای مسیریابی بسته بیش از یک مسیر وجود داشته باشد.

سوال ۳)

```
C:\Users\parsa>route print
===========================================================================
Interface List
 25...54 05 db 1d d8 7e ......Realtek PCIe GbE Family Controller
  3...00 ff 0b 3a ef 82 ......ExpressVPN TAP Adapter
  7............................Windscribe Windtun420
  9............................ExpressVPN TUN Driver
 18...00 ff a9 c6 1d 56 ......Windscribe VPN
 10...a4 b1 c1 3d dd 90 ......Microsoft Wi-Fi Direct Virtual Adapter
  6...a6 b1 c1 3d dd 8f ......Microsoft Wi-Fi Direct Virtual Adapter #2
 14...44 45 53 54 4f 53 ......Kerio Virtual Network Adapter
 17...a4 b1 c1 3d dd 8f ......Intel(R) Wi-Fi 6 AX201 160MHz
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1      192.168.1.3     50
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.1.0    255.255.255.0         On-link       192.168.1.3    306
      192.168.1.3  255.255.255.255         On-link       192.168.1.3    306
    192.168.1.255  255.255.255.255         On-link       192.168.1.3    306
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link       192.168.1.3    306
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link       192.168.1.3    306
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
  1    331 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

هنگامی که دستور print route را در cmd میزنیم سه بخش به ما نمایش داده میشود :

بخش اول تمام واسط های قابل استفاده در سیستم و اطلاعاتی از آنها نمایش داده میشود و در بخش های دو و سه route table های IPv4 و IPv6 را میبینیم.

دستور route ADD در cmd برای افزودن یک مسیر به جدول مسیریابی استفاده می‌شود. این دستور به شما امکان می‌دهد تا مسیرهای خاصی را به جدول مسیریابی سیستم اضافه کنید.

در ویندوز، برای استفاده از دستور route ADD به صورت زیر عمل می‌کنیم:

route ADD <مقصد> <ماسک زیر شبکه> <مسیر گره بعدی>

توضیحات:

- `<مقصد>`: آدرس IP مقصدی است که می‌خواهید مسیریابی کنید.

- `<ماسک زیر شبکه>`: ماسک زیر شبکه مربوط به مقصد را مشخص می‌کند.

- `<مسیر گره بعدی>`: IP آدرس گره بعدی (مسیریاب) است که بسته‌ها برای رسیدن به مقصد به آن هدایت می‌شوند.

به عنوان مثال، فرض کنید می‌خواهید مسیریابی برای آدرس IP 192.168.1.0 با ماسک زیرشبکه 255.255.255.0 و مسیر گره بعدی 192.168.0.1 را اضافه کنید. دستور زیر را در خط فرمان ویندوز اجرا کنید:

```
route ADD 192.168.1.0 MASK 255.255.255.0 192.168.0.1
```

با اجرای این دستور، مسیر مورد نظر به جدول مسیریابی سیستم عامل اضافه خواهد شد و بسته‌هایی که مقصد آن‌ها با مقصد مشخص شده در دستور مطابقت دارد، به آدرس گره بعدی هدایت خواهند شد.

برای مشاهده جدول مسیریابی فعلی سیستم، می‌توانید دستور زیر را در خط فرمان وارد کنید:

```
route print
```

با اجرای این دستور، جدول مسیریابی کنونی سیستم نمایش داده خواهد شد و می‌توانید مسیرهای اضافه شده را مشاهده کنید.

سوال ۴)

برنامه DHCP یک برنامه برای آی پی دهی خودکار در شبکه است. آی پی هایی که این برنامه به دستگاه های مختلف می‌دهد، رنج آنها و مدت اعتبار آن آی پی را می‌توان به طور کامل کانفیگ کرد. ذکر این نکته مهم است که حتما باید یک DHCP Server در شبکه وجود داشته باشد و اگر ۲ دیوایس موجود در شبکه هر دو DHCP Server داشته باشند، در شبکه خرابکاری رخ خواهد داد.
مراحل

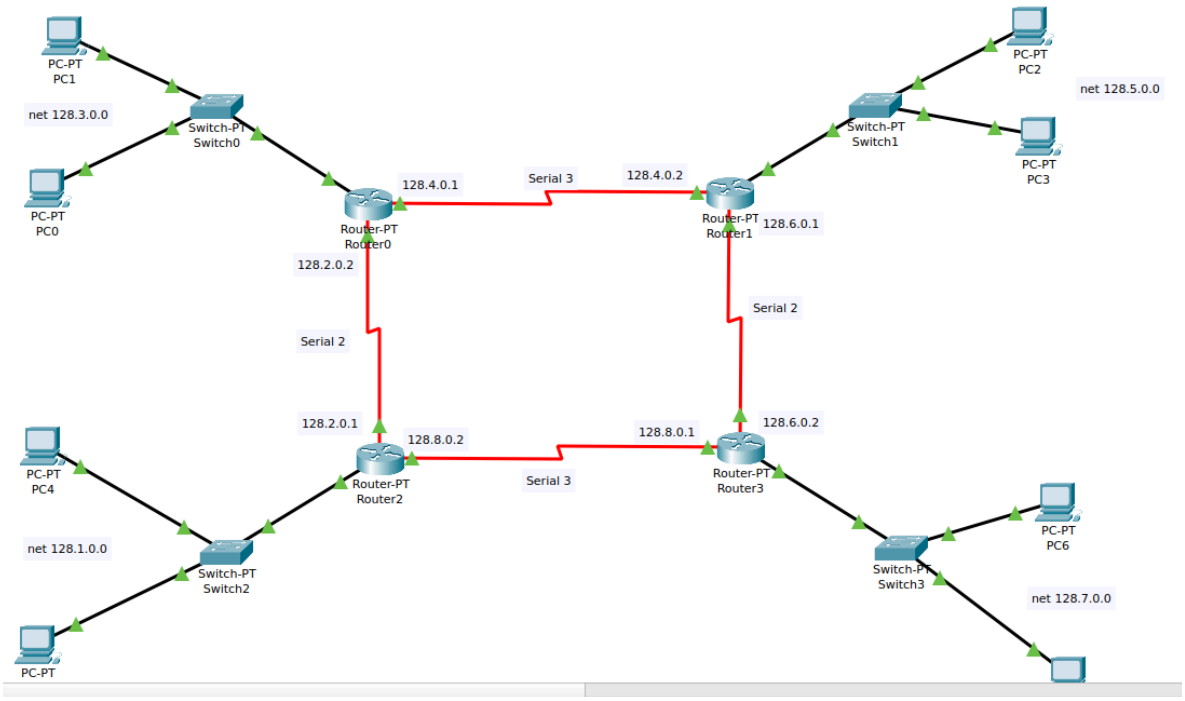
- یک دیوایس جدید وارد شبکه شده و یک بسته که بیانگر درخواست آی پی است را برودکست می‌کند.
- تنها DHCP Server موجود در شبکه به آن جواب می‌دهد و می‌گوید می‌توانی از آی پی x.x.x.x به مدت ذکر شده استفاده کنی.
- دیوایس جدید پیامی به معنی از آی پی x.x.x.x استفاده می‌کنم به DHCP Server بر می‌گرداند.
- DHCP Server در حافظه خود می‌نویسد که تا تاریخ ذکر شده آی پی x.x.x.x در اختیار دیوایس جدید است.

گزارش آزمایش سوم

مرحله اول

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

در مرحله دوم شروع به اطلاق IP به تک تک دیوایس ها و interface روتر ها به صورت Classfull شدیم. همانطور که در تصویر بالا مشخص است دیوایس های ۴ و ۵ در شبکه 128.1.0.0 دیوایس های ۰ و ۱ در شبکه 128.3.0.0 دیوایس های ۲ و ۳ در شبکه 128.5.0.0 و در نهایت دیوایس های ۶ و ۷ در شبکه 128.7.0.0 قرار دارند.

آی پی تک تک دیوایس ها و اینترفیس روتر متصل به آن شبکه:

- هر ۲ دیوایس از شبکه 128.1.0.0 آی پی های 128.1.0.1 و 128.1.0.2 دارند و اینترفیس روتر متصل به آن 128.1.0.3 است.
- هر ۲ دیوایس از شبکه 128.3.0.0 آی پی های 128.3.0.1 و 128.3.0.2 دارند و اینترفیس روتر متصل به آن 128.3.0.3 است.

- هر ۲ دیوایس از شبکه 128.5.0.0 آی پی های 128.5.0.1 و 128.5.0.2 دارند و اینترفیس روتر متصل به آن 128.5.0.3 است.
- هر ۲ دیوایس از شبکه 128.7.0.0 آی پی های 128.7.0.1 و 128.7.0.2 دارند و اینترفیس روتر متصل به آن 128.7.0.3 است.

از طرفی Default Gateway را برای هر دیوایس معادل آی پی اینترفیس روتر متصل به آن شبکه قرار دادیم.
(برای مثال اگر آی پی دیوایس برابر 128.3.0.2 باشد Default Gateway اش برابر 128.3.0.3 خواهد شد).

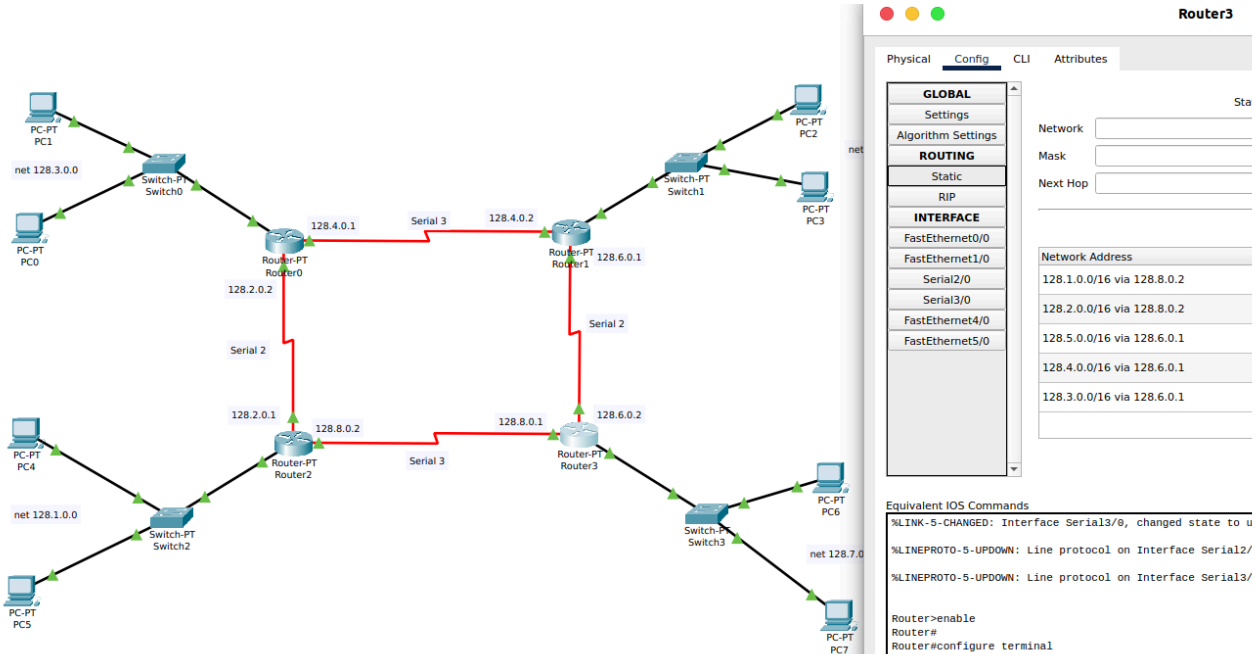
گام سوم

در گام سوم برای هر جفت interface متصل به هم میان روتر ها، یک شبکه دیگر تعریف کردیم. خود شبکه و آی پی های اطلاق شده به اینترفیس روتر ها در جدول ذیل آمده است.

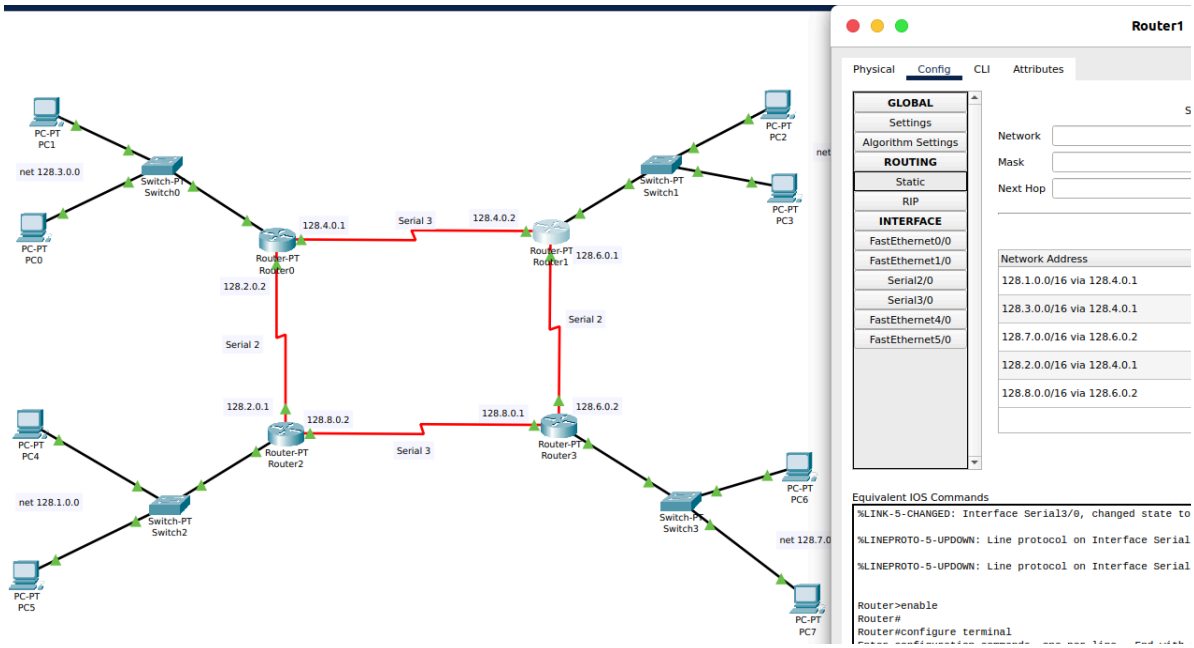
	Network	Router 0	Router 1	Router 2	Router 3
Between Router 2 & 0	128.2.0.0	128.2.0.2		128.2.0.1	
Between Router 0 & 1	128.4.0.0	128.4.0.1	128.4.0.0		
Between Router 1 & 3	128.6.0.0		128.6.0.1		128.6.0.2
Between Router 3 & 2	128.8.0.0			128.8.0.2	128.8.0.1

گام نهایی

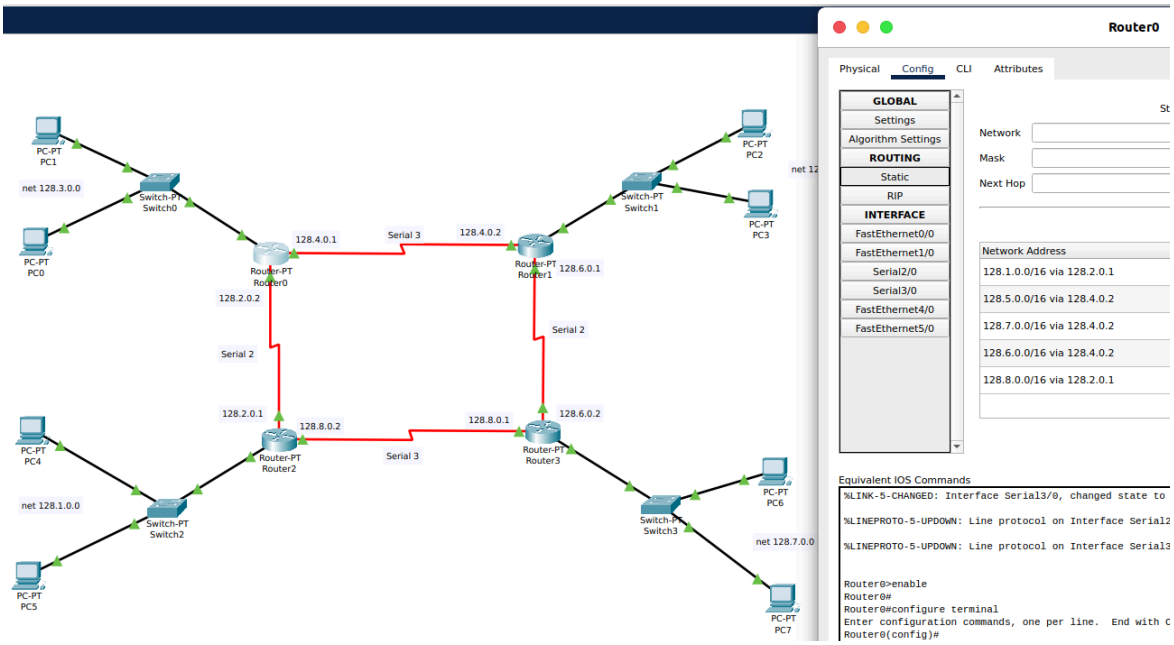
در مرحله نهایی روت دهی را برای تک تک روتر ها انجام دادیم. در این مرحله باید برای هر روتر گفته شود که، بسته هایی به مقصد شبکه های متصل به سایر روتر ها، به کدام آی پی فرستاده شود، طبیعیست از آنجایی که هر روتر تنها به ۲ روتر مجاور خود متصل است، باید آی پی اینترفیس متصل به خود یکی از این ۲ روتر را انتخاب کند. در تصویر ذیل تمامی روت های روتر ها مشخص است.



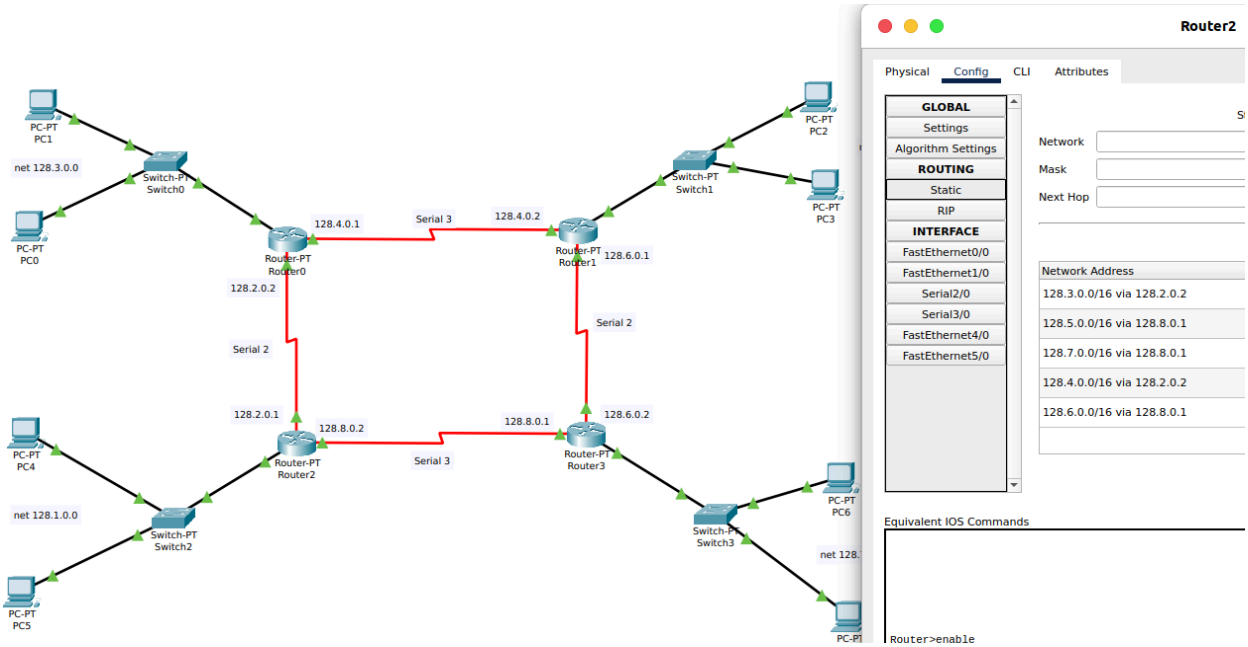
برای روتر ۳ اگر مقصد در شبکه ۳ یا ۵ بود، بسته به روتر ۱ با آی پی 128.6.0.1 ارسال خواهد شد و اگر در شبکه ۱ بود، به روتر ۲ با آی پی 128.8.0.2 ارسال خواهد شد.



برای روتر ۱ اگر مقصد در شبکه ۳ یا ۱ بود، بسته به روتر ۰ با آی پی 128.4.0.1 ارسال خواهد شد و اگر در شبکه ۷ بود، به روتر ۳ با آی پی 128.6.0.2 ارسال خواهد شد.



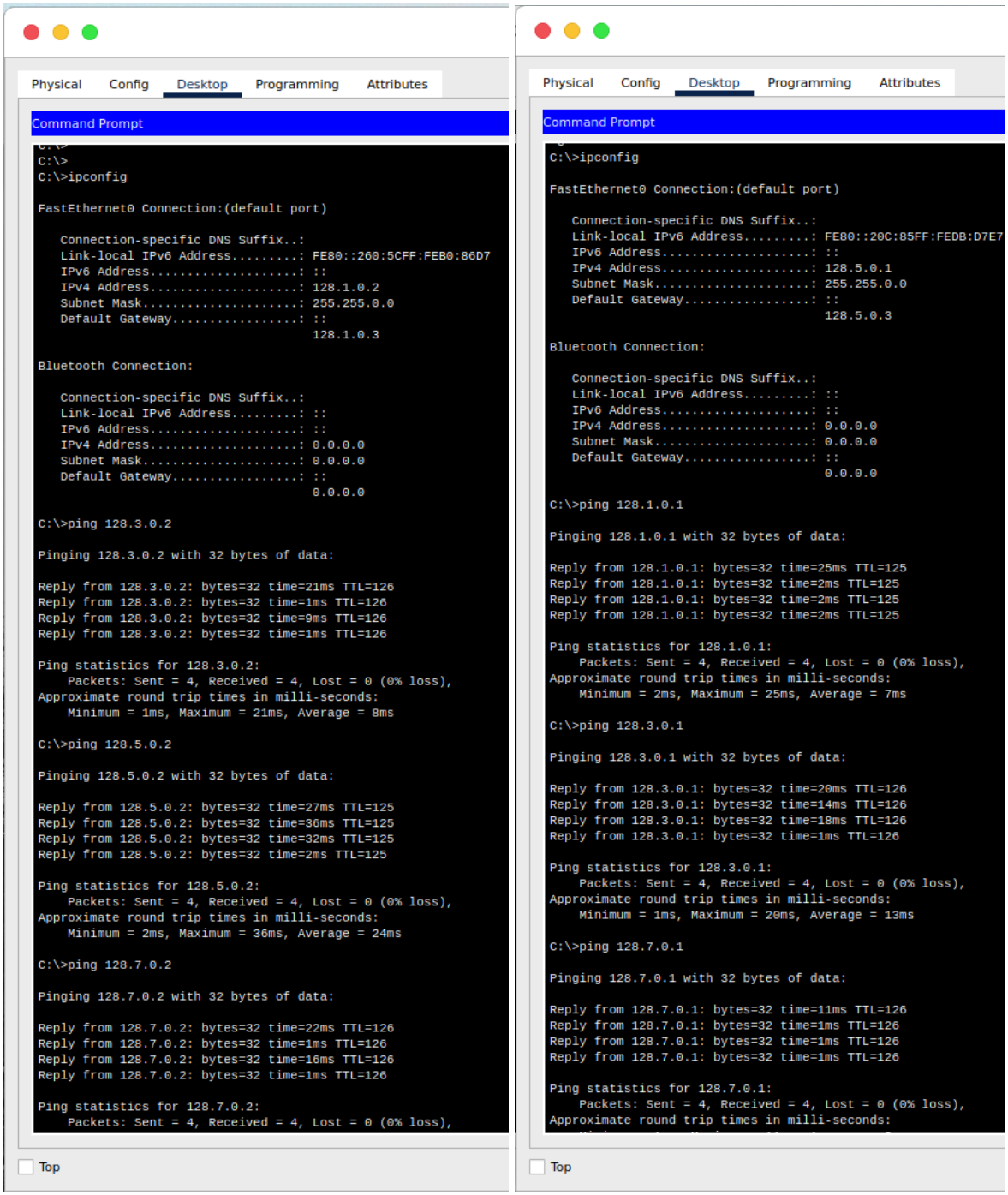
برای روتر ۰ اگر مقصد در شبکه ۵ یا ۷ بود، بسته به روتر ۱ با آی پی 128.4.0.2 ارسال خواهد شد و اگر در شبکه ۱ بود، به روتر ۲ با آی پی 128.2.0.1 ارسال خواهد شد.



برای روتر ۲ اگر مقصد در شبکه ۵ یا ۷ بود، بسته به روتر ۳ با آی پی 128.8.0.1 ارسال خواهد شد و اگر در شبکه ۳ بود، به روتر ۰ با آی پی 128.2.0.2 ارسال خواهد شد.

پینگ گرفتن

در پایان برای اطمینان از صحت درستی اتصالات ping گرفتیم و موفقیت آمیز بود.

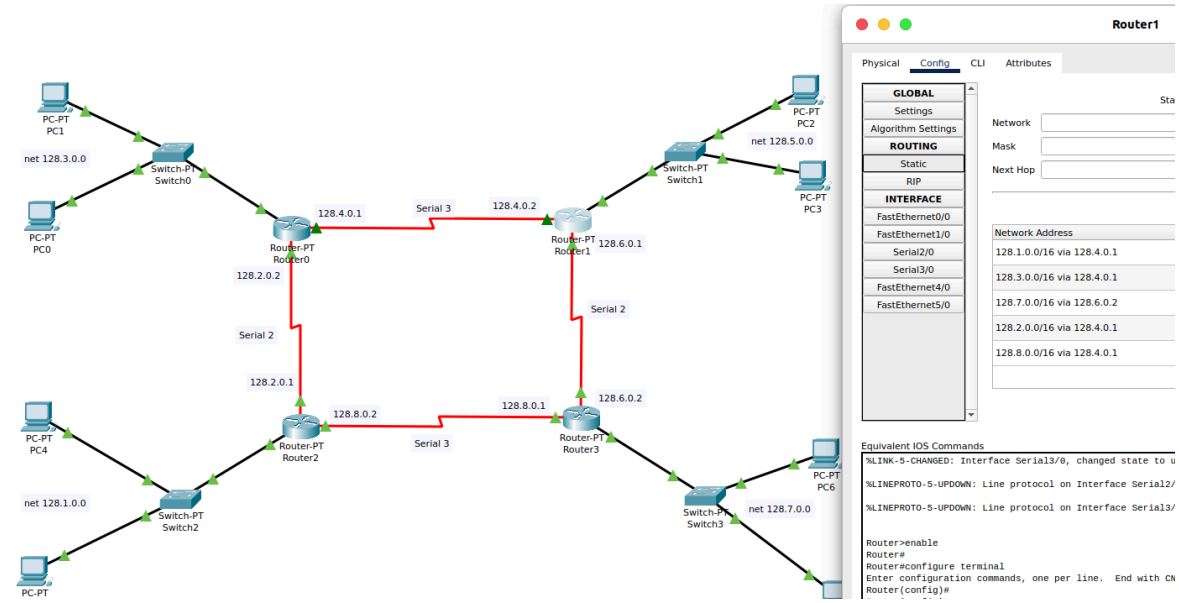


در تصویر سمت چپ یک کلاینت از شبکه ۱ و در تصویر سمت راست یک کلاینت از شبکه ۵ هرکدام ۳ کلاینت دیگر را از ۳ شبکه مجاور ping کردند و تمامی ping ها پاسخشان برگشته است.

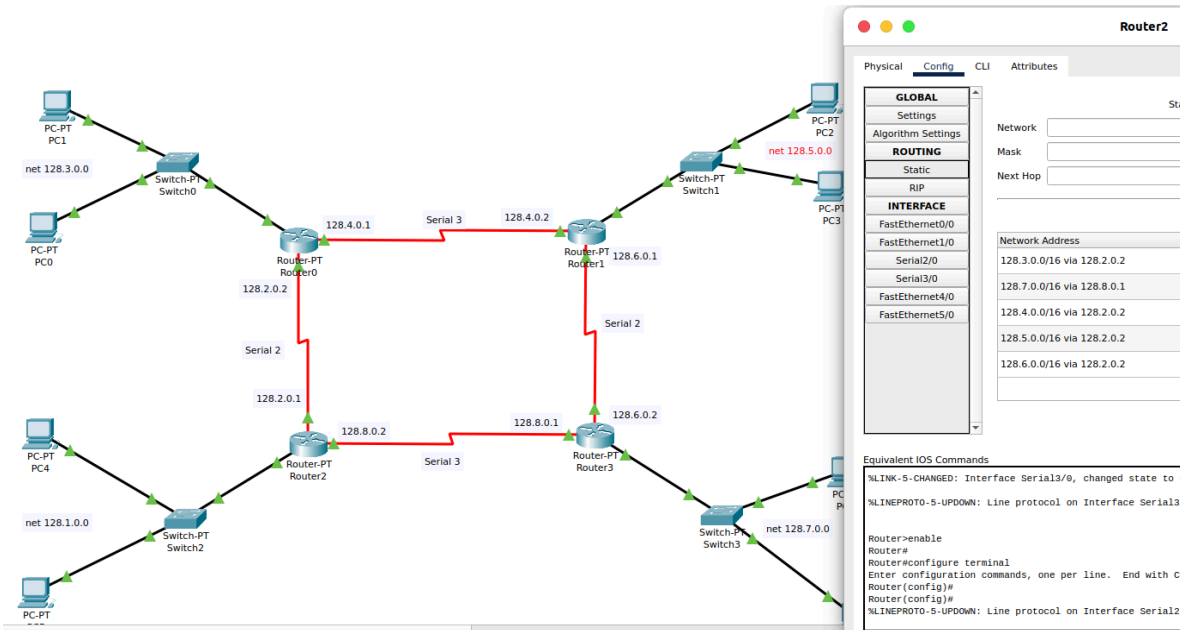
مرحله دوم

توضیحات

در مرحله دوم کافی بود تا کمی روت های نوشته شده برای روتر های متصل به روتر ۳ تغییر کند تا در صورت کار داشتن با هر روتری (به غیر از روتر ۳) بسته را به روتر ۳ ارسال نکنیم. برای این منظور روت های، روتر ۱ و ۲ به صورت ذیل آپدیت شد:



همانطور که مشخص است، در روت های روتر ۱ تنها در صورتی که با دیوایس های متصل به روتر ۳ کار داشته باشیم پیام را به روتر ۳ یعنی آی پی 128.6.0.2 می‌فرستیم.



همانطور که مشخص است، در روت های روتر ۲ تنها در صورتی که با دیوایس های متصل به روتر ۳ کار داشته باشیم پیام را به روتر ۳ یعنی آی پی 128.8.0.1 می‌فرستیم.

پینگ گرفتن

در پایان از PC5 واقع در شبکه ۱ اینترفیس های 128.6.0.1 و 128.6.0.2 را با استفاده از دستور tracert پینگ میکنیم تا مطمئن شویم تا بسته مسیر طولانی تری را طی می‌کند تا به مقصد برسد.