گزارش سوم آزمایشگاه شبکه های کامپیوتری

اعضای گروه:

پارسا عصمت‌لو

سهیل شهرابی

فهرست مطالب

پیش گزارش آزمایش پنجم

سوال ۱

این الگوریتم ،الگوریتم تکامل یافته distance vector میباشد و از link state نیز استفاده میکند و از نوع classless میباشد. از جمله ویژگی های این الگوریتم در پشتیبانی از شبکه های بزرگ میتوان به:

- پشتیبانی از vlsm و summarization
- پشتیبانی از چند as در یک روتر
- کشف و نگهداری روتر ها نام برد.

سوال ۲

EIGRP با استفاده از PDM میتواند از طریق IPV4,IPX و IPV6 مسیریابی کند.

و نقش های موثر آن:

- ایجاد لیست های دستیابی و فیلترسازی
- ایجاد packet با پروتکل تعیین شده
- ترجمه packet های ایجاد شده برای dual
- نگهداری همسایه هارو توپولوژی جدول های روتر EIGRP

سوال ۳

Neighbor discovery در EIGRP به منظور شناسایی و برقراری ارتباط با همسایگان در شبکه استفاده می‌شود. EIGRP، یکی از پروتکل‌های مسیریابی پویا در شبکه‌های کامپیوتری است که برای تبادل معلومات مسیریابی بین دستگاه‌ها استفاده می‌شود. فرآیند Neighbor discovery شامل چند مرحله می‌باشد:

1) Multicast Hellos: در این مرحله، دستگاه EIGRP پیام‌های Multicast Hello به همسایگان خود ارسال می‌کند. پیام Hello شامل اطلاعات مربوط به EIGRP است و توسط دستگاه‌های همسایه دریافت می‌شود.
2) Unicast Hellos: پس از دریافت پیام‌های Multicast Hello، دستگاه‌های همسایه پیام‌های Unicast Hello به دستگاه ارسال کننده برمی‌گردانند. این پیام‌ها به منظور

تأیید دریافت پیام‌های Multicast Hello و اعلام آمادگی برای ایجاد ارتباط استفاده می‌شوند.

3) Parameter Exchange: در این مرحله، دستگاه‌ها پارامترهای مورد نیاز برای ایجاد ارتباط را با یکدیگر مبادله می‌کنند. این پارامترها شامل شماره‌ی آی‌پی لینک، معلومات مربوط به EIGRP، و معلومات مربوط به توپولوژی شبکه است.
4) Reliable Transport: در این مرحله، دستگاه‌ها از پروتکل انتقال قابل اعتماد EIGRP برای ارسال و دریافت پیام‌ها استفاده می‌کنند. این پروتکل تضمین می‌کند که پیام‌ها به صورت صحیح و کامل دریافت و ارسال شوند.
5) Adjacency Formation: وقتی که دستگاه‌ها در مراحل قبلی موفق به تبادل پیام‌ها و مبادله پارامترها می‌شوند، ارتباط همسایگی بین آن‌ها برقرار می‌شود و وضعیت مجاورت شروع می‌شود. در این وضعیت، دستگاه‌ها معلومات مسیریابی را با یکدیگر به اشتراک می‌گذارند و امکان انتقال ترافیک بین آن‌ها برقرار می‌شود.

مراحل فوق نشان‌دهنده‌ی فرآیند Neighbor discovery در EIGRP می‌باشد. این فرآیند به دستگاه‌ها امکان می‌دهد تا همسایگان خود را در شبکه تشخیص داده و ارتباطات لازم را برای تبادل معلومات مسیریابی برقرار کنند.

سوال ۴

پروتکل RTP (Real-time Transport Protocol) یک پروتکل مخصوص انتقال داده‌های زمان واقعی در شبکه‌های کامپیوتری است. این پروتکل برای انتقال صوت، تصویر و داده‌هایی که نیاز به انتقال به صورت بلافاصله و بدون تاخیر دارند، استفاده می‌شود. RTP به همراه پروتکل کنترل RTCP (Real-time Transport Control Protocol) برای مدیریت و کنترل ارتباطات زمان واقعی استفاده می‌شود.

با استفاده از پروتکل RTP، داده‌های زمان واقعی به بسته‌های کوچکتر تقسیم می‌شوند و به صورت بسته به بسته با اضافه کردن اطلاعات مربوط به زمان‌بندی و ترتیب، ارسال می‌شوند. این اطلاعات شامل شماره دنباله (sequence number)، برچسب زمانی (timestamp) و اطلاعات اعتبارسنجی (validation information) هستند. دریافت کننده بر اساس این اطلاعات، بسته‌ها را بازسازی و به ترتیب صحیح مرتب می‌کند.

پروتکل RTP برای انتقال داده‌های زمان واقعی در برنامه‌ها و سرویس‌هایی مانند تماس‌های تلفنی اینترنتی (VoIP)، ویدیوکنفرانس، استریمینگ صوت و تصویر، بازی‌های آنلاین و دیگر

برنامه‌هایی که نیاز به ارسال داده‌های زمان واقعی دارند، استفاده می‌شود. این پروتکل از پورت‌های UDP (User Datagram Protocol) برای انتقال داده‌ها استفاده می‌کند و اطمینان می‌دهد که داده‌ها به صورت پیوسته و بدون تاخیر قابل توجیه انتقال می‌شوند.

سوال ۵

الگوریتم DUAL (Diffusing Update Algorithm) در پروتکل مسیریابی EIGRP (Enhanced Interior Gateway Routing Protocol) استفاده می‌شود. این الگوریتم برای محاسبه و انتخاب بهترین مسیر برای ارسال ترافیک در شبکه استفاده می‌شود. الگوریتم DUAL شامل مراحل زیر است:

1) اعلام فاصله (Advertised Distance): هر مسیریاب EIGRP مقدار Advertised Distance را برای هر مسیر معلوم می‌کند که نشان‌دهنده فاصله‌ی مسیر دریافت شده از مسیریاب دیگر است. این فاصله بر اساس معیارهایی مانند متریک (Metric)، پهنای باند (Bandwidth) و تأخیر (Delay) محاسبه می‌شود.
2) فاصلهٔ محلی (Feasible Distance): هر مسیریاب EIGRP مقدار Feasible Distance را برای هر مسیر محاسبه می‌کند. Feasible Distance شامل Advertised Distance مسیر فعلی به علاوهٔ متریک مسیر محلی است.
3) انتخاب بهترین مسیر (Best Path Selection): هر مسیریاب EIGRP بر اساس Feasible Distance، بهترین مسیر را انتخاب می‌کند. این مسیر به عنوان مسیر اصلی (Primary Path) برای ارسال ترافیک در نظر گرفته می‌شود.
4) پشتیبانی (Backup): در صورتی که مسیر اصلی قطع شود یا مسیر جدیدی با فاصله کمتر به دستگاه مسیریابی اعلام شود، مسیر جدید به عنوان مسیر پشتیبان (Backup Path) در نظر گرفته می‌شود. اگر مسیر اصلی مجدداً در دسترس قرار بگیرد، مسیر پشتیبان به عنوان مسیر اصلی جایگزین می‌شود.
5) Diffusing Update (انتشار به‌روزرسانی): در صورتی که مسیریابی تغییر کند و یا معیارهای مسیریابی تغییر کنند، این اطلاعات به دستگاه‌های همسایه انتشار داده می‌شود تا آن‌ها نیز بتوانند جدیدترین اطلاعات را دریافت کنند و محاسبات DUAL را انجام دهند.

با استفاده از الگوریتم DUAL ،EIGRP قادر است به صورت پویا و سریع به تغییرات در توپولوژی شبکه و وضعیت مسیریاب‌ها واکنش نشان دهد و بهترین مسیر را برای ارسال ترافیک انتخاب کند.

از کاربرد های DUAL میتواند به موارد زیر اشاره کرد:

- انتخاب و نگهداری بهترین مسیر
- انتخاب بهترین مسیر پشتیبان

- پشتیبانی ای vlsm
- درخواست مسیر جایگزین در نبود مسیر مناسب

سوال ۶

با اینکه این پیکربندی پیچیدگی های خودش را دارد ولی نکات مثبتی مانند :

هزینه سربار مسیریابی کمتر

سرعت بخشیدن به همگرایی شبکه

محدود کردن ناپایداری شبکه را نیز دارد

سوالات تحلیلی آزمایش چهارم

سوال ۱

- هدر بسته: هدر بسته ۴ بایت است و مشخص کننده نسخه پروتکل است.
- رزرو: رزرو۲ بایت است و برای استفاده‌های آینده رزرو شده است.

فیلدهای درخواست و پاسخ: این فیلدها مربوط به درخواست و پاسخ‌های مرتبط با بسته جاری هستند. هر بسته می‌تواند حاوی حداکثر ۲۵ Entry از جدول مسیریابی RIP باشد. فیلدهای خالی با مقدار صفر پر می‌شوند.

- ورودی Entry: هر Entry در بسته دارای طول 20 بایت است و اطلاعات مربوط به مسیرها را نشان می‌دهد. این فیلدها شامل Subnet Mask، NextHop، Metric و IP هستند.
- رمزنگاری و احراز هویت: RIPv2 از امکانات رمزنگاری و احراز هویت برای اطمینان از اصالت داده‌های مبادله شده استفاده می‌کند.

سوال ۲

- RIPv2 از احراز هویت استفاده می‌کند ولی RIPV1 از احراز هویت پشتیبانی نمی‌کند.
- در RIPv2 امکان تنظیم Summarization route وجود دارد اما در RIPV1 این امکان وجود ندارد.
- در RIPv2 آدرس دهی Classless وجود دارد اما در RIPV1 این امکان وجود ندارد.
- RIPv2 از VLSM پشتیبانی می‌کند ولی RIPV1 از احراز هویت پشتیبانی نمی‌کند.

سوال ۳

- از RIPv2 برای استفاده در شبکه‌های IPv4 استفاده می‌شود ولی از RIPng در شبکه‌های IPv6 استفاده می‌شود.
- در RIPv2 پیام‌ها و جداول مسیریابی مطابق با استاندارد RIPv1 ساخته شده‌اند، ولی در RIPv2 پیام‌ها و جداول مسیریابی به طور کامل برای IPv6 بازبینی و بازسازی شده‌اند.
- در RIPv2 تعداد هاپ‌های مجاز برای عبور از یک مسیر به حداکثر ۱۵ هاپ محدود شده است ولی در RIPng محدودیت تعداد هاپ‌ها حداکثر ۱۵ هاپ است و این محدودیت از RIPv2 به ارث برده شده است.

سوال ۴

استفاده از تایمرها در پروتکل IGRP برای اعمال محدودیت‌های زمانی در فرایندهای مختلف ارتباطی این پروتکل استفاده می‌شود. این تایمرها برای موارد مختلفی از جمله اعلام تغییرات در شبکه، بررسی سلامتی ارتباطات، و به‌روزرسانی جداول مسیریابی استفاده می‌شوند. از جمله تایمرهای مهم در IGRP عبارتند از:

- Hold-down Timer (تایمر نگهداشت): این تایمر برای مهار تغییرات نوسانی در جداول مسیریابی استفاده می‌شود. هنگامی که یک مسیر از دسترس خارج می‌شود، مسیریاب به مدت hold-down timer از به روزرسانی جدول مسیریابی خودداری می‌کند تا اطمینان حاصل شود که هیچ اطلاعات نادرستی وارد جدول نشود.
- Update Timer (تایمر به‌روزرسانی): این تایمر برای زمان‌بندی ارسال پیام‌های به‌روزرسانی به مسیریاب‌های دیگر در شبکه استفاده می‌شود. این پیام‌ها شامل اطلاعات مسیریابی جدید یا تغییرات در شبکه هستند.
- Invalid Timer (تایمر نامعتبر): این تایمر برای مشخص کردن مدت زمانی که یک مسیر به عنوان نامعتبر در نظر گرفته می‌شود، استفاده می‌شود. زمان این تایمر مشخص می‌کند که مسیری که دیگر در جدول مسیریابی معتبر نیست، باید از جدول حذف شود.
- Flush Timer (تایمر خروج): این تایمر برای مشخص کردن مدت زمانی استفاده می‌شود که یک مسیر باید از جدول مسیریابی حذف شود. این تایمر زمانی را که مسیر به عنوان نامعتبر شناخته می‌شود، به همراه تایمر نامعتبر محاسبه می‌کند.

سوال ۵

با توجه به انتخاب مسیر یا مسیریابی معیارهای مختلفی وجود دارد که می‌تواند چگونگی مدیریت مسیر در پروتکل IGRP را متحت تأثیر قرار دهد. هر یک از این معیارها ارتباط یافتن مسیرهای مختلفی براساس ویژگی‌های ابعادی مختلفی از شبکه را ممکن می‌سازند؛ اما بهترین تعیین مسیر نیازمند به مشخص شدن وزن‌های ارتباطی وزن‌های معیارهای واقعی از شبکه است. این اطلاعات از طریق مکانیزم‌های مختلفی از جمله Distance Vector و بودن اعتماد قابل اعتمادی برای انتقال اطلاعات از منبع به مقصد منتقل

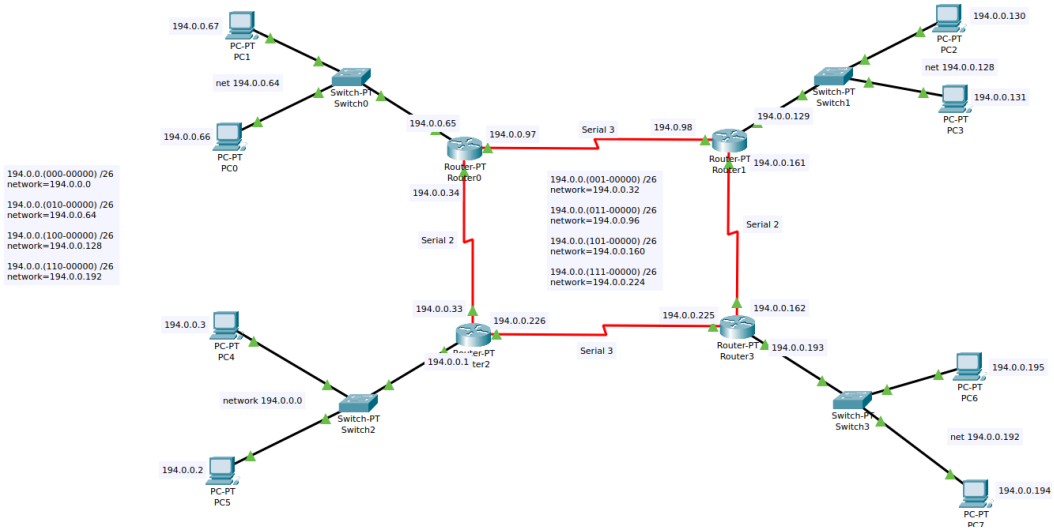
می‌شوند. مراحل تصمیم‌گیری تحت تأثیر مسیریابی در شبکه، بر اساس وزن‌های معیارهای مربوطه می‌تواند تنظیم شود. فرمول‌های مربوطه در Administrative Distance و پهنای باند شامل ارتباط بین تاخیر و پهنای باند است که اطلاعات مرتبط با آنها برای مسیریابی معتبر محسوب می‌شود.

گزارش آزمایش چهارم

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 Classless شدیم. از آنجایی که ما نیاز به ۸ شبکه داشتیم و برای آی پی دهی Classless می‌توانیم با دقت بیت به هاست ها و شبکه ها آدرس بدهیم، پس ۳ بایت اول و ۳ بیت بایت چهارم را برای آدرس دهی هاست ها در نظر گرفتیم، به این صورت که در آی پی های داده شده به تمامی دستگاه ها، ۳ بایت اول همه یکسان است، و در بایت

چهارم، از ۸ بیت باقیمانده، ۳ بیت دیگر برای هاست و ۵ بیت برای آدرس دهی هاست های درون هر شبکه است.
در ادامه ما برای مقدار دهی به ۳ بیت، بایت چهارم شبکه های محلی که میان end device ها و روتر متصل به آنهاست، از اعداد زوج و برای شبکه های میان روتر ها از اعداد فرد استفاده کردیم. همانطور که در تصویر بالا مشخص است دیوایس های ۴ و ۵ در شبکه 194.0.0.0 قرار دارند که معادل 000 برای ۳ بیت بالای بایت چهارم است، دیوایس های ۰ و ۱ در شبکه 194.0.0.64 قرار دارند که معادل 010 برای ۳ بیت بالای بایت چهارم است، دیوایس های ۲ و ۳ در شبکه 194.0.0.128 قرار دارند که معادل 100 برای ۳ بیت بالای بایت چهارم است،و در نهایت دیوایس های ۶ و ۷ در شبکه 194.0.0.192 قرار دارند که معادل 110 برای ۳ بیت بالای بایت چهارم است.

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

- هر ۲ دیوایس از شبکه 194.0.0.0 آی پی های 194.0.0.2 و 194.0.0.3 دارند و اینترفیس روتر متصل به آن 194.0.0.1 است.
- هر ۲ دیوایس از شبکه 194.0.0.64 آی پی های 194.0.0.66 و 194.0.0.67 دارند و اینترفیس روتر متصل به آن 194.0.0.65 است.
- هر ۲ دیوایس از شبکه 194.0.0.128 آی پی های 194.0.0.130 و 194.0.0.131 دارند و اینترفیس روتر متصل به آن 194.0.0.129 است.
- هر ۲ دیوایس از شبکه 194.0.0.192 آی پی های 194.0.0.194 و 194.0.0.195 دارند و اینترفیس روتر متصل به آن 194.0.0.193 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 194.0.0.195 باشد Default Gateway اش برابر 194.0.0.193 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	3 High bits
Router 2 & 0	194.0.0.32	194.0.0.34		194.0.0.33		001

Router 0 & 1	194.0.0.96	194.0.0.97	194.0.98			011
Router 1 & 3	194.0.0.160		194.0.0.161		194.0.0.162	101
Router 3 & 2	194.0.0.224			194.0.0.226	194.0.0.225	111

گام نهایی

در مرحله نهایی برای تمامی روتر های شبکه خود پروتکول آدرس دهی RIP2 را فعال کردیم. علت فعال کردن RIP ورژن ۲ بخاطر این بود که RIP ورژن ۱ قابلیت پشتیبانی از آدرس دهی classless را نداشت. پس برای هر روتر با اجرای دستورات ذیل در محیط Command line روتر، پروتکل RIP را فعال کردیم و شبکه هایی که به صورت مستقیم به روتر متصل بودند را معرفی کردیم.
دستورات:

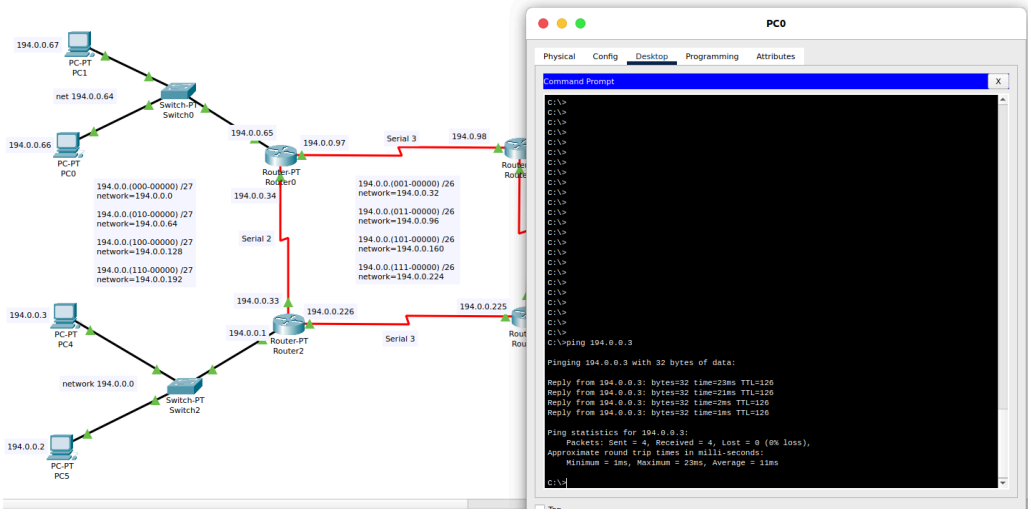
```
en
config t
router rip
Version 2
```

در نهایت با دستور network و سپس آدرس آن شبکه، شبکه را برای روتر معرفی کردیم. برای مثال برای روتر ۲ که به شبکه های 194.0.0.32، 194.0.0.224 و 192.0.0.0 متصل بود، دستورات ذیل را دادیم.

```
en
config t
router rip
version 2
network  192.0.0.0
network  192.0.0.32
network  192.0.0.224
```

پینگ گرفتن

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



به عنوان مثال در تصویر بالا، دیوایس صفر، دیوایس ۴ را که از یک شبکه دیگر است پینگ گرفته و موفقیت آمیز بوده.