سؤال 1: فرض کنید که می­خواهید تعداد میزبان­های موجود در یک NAT را شناسایی کنید. می­دانیم که لایه­ی IP یک شماره­ی شناسایی را به ترتیب به هر بسته­ی IP اختصاص می­دهد. شماره­ی شناسایی مربوط به اولین بسته­ی IP که توسط یک میزبان تولید شده است، یک شماره­ی تصادفی بوده و شماره­ی بسته­های بعدی به ترتیب اختصاص داده می­شود. فرض کنید که همه­­ی بسته­های تولیدشده توسط میزبان­ها به بیرون از شبکه ارسال می­شوند.

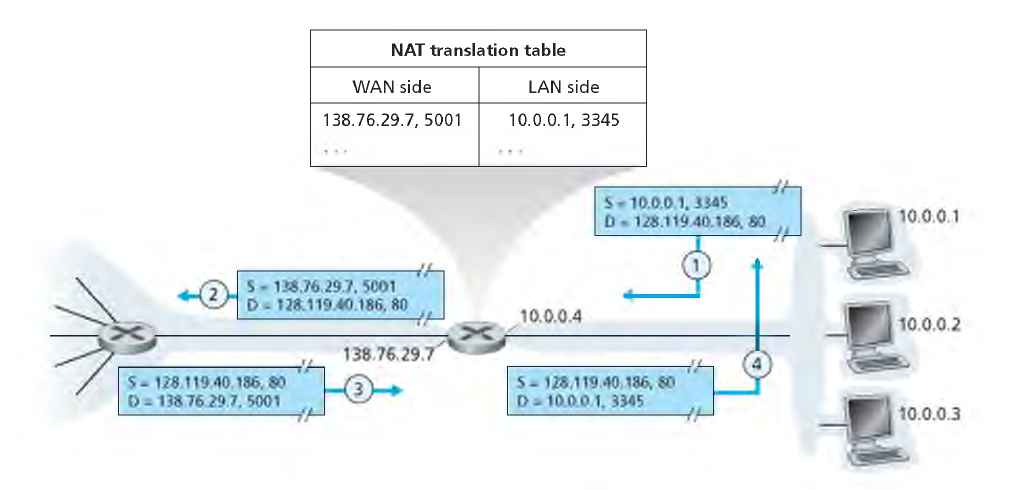
a. فرض کنید می­توان بسته­های ارسال شده از طرف NAT به بیرون از شبکه را شنود کرد. با چه تکنیکی می­توان تعداد میزبان­های یکتا پشت NAT را تشخیص داد؟

پاسخ: از آن­جایی که همه­ی بسته­های تولید شده به بیرون از شبکه ارسال می­شوند، می­توان تمام بسته­های IP تولیدشده توسط میزبان­های موجود در یک NAT را شنود کرد. از آن­جایی که هر میزبان مجموعه­ای از بسته­های IP را با شماره­های متوالی و شماره­ی شناسایی اولیه­ی منحصربه­فرد (به دلیل انتخاب آن از یک فضای بزرگ) تولید می­کند، می­توان بسته­های IP با شماره­­های شناسایی متوالی را در یک گروه قرار داد. تعداد گروه­ها، تعداد میزبان­های موجود در یک NAT را نشان می­دهد.

b. اگر شماره­های شناسایی به ترتیب اختصاص داده نشوند، بلکه به صورت تصادفی اختصاص داده شوند، آیا تکنیک پیشنهادی شما همچنان می­تواند شماره­ی میزبان­های موجود در NAT را شناسایی کند؟

پاسخ: اگر شماره­های شناسایی مربوط به بسته­های IP به صورت متوالی اختصاص داده نشود و به صورت تصادفی باشد، تکنیک پیشنهادشده در بخش قبلی، کارساز نخواهد بود. چون در این حالت امکان گروه­بندی بسته­های شنودشده وجود ندارد.

سؤال 2: ساختار شبکه­ی زیر را در نظر بگیرید. فرض کنید که ISP آدرس آی پی 24.34.112.235 را به روتر اختصاص می­دهد و آدرس مربوط به شبکه­ی خانگی 192.168.1/24 است.



a. آدرس مربوط به همه­ی واسط­ها را در شبکه­ی خانگی تعیین کنید.

پاسخ: آدرس مربوط به شبکه­ی خانگی: 192.168.1.1 و 192.168.1.2 و 192.168.1.3 و آدرس مربوط به واسط به روتر: 192.168.1.4

b. فرض کنید که هر میزبان دو ارتباط TCP به پورت 80 در آدرس 128.119.40.86 دارد. 6 عدد از مدخل­های مربوط به جدول NAT را بیان کنید.

پاسخ:

|  |  |
| --- | --- |
| NAT translation table | |
| LAN Side | WAN Side |
| 192.168.1.1, 3345 | 24.34.112.235, 4000 |
| 192.168.1.1, 3346 | 24.34.112.235, 4001 |
| 192.168.1.2, 3345 | 24.34.112.235, 4002 |
| 192.168.1.2, 3346 | 24.34.112.235, 4003 |
| 192.168.1.3, 3345 | 24.34.112.235, 4004 |
| 192.168.1.3, 3346 | 24.34.112.235, 4005 |

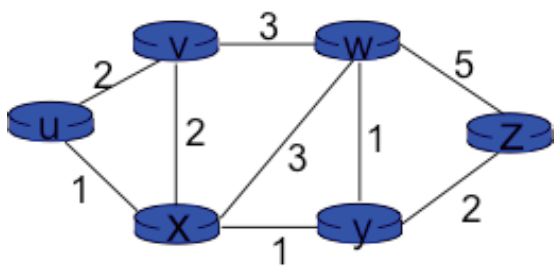
سؤال 3: آدرس IP و MAC مربوط به مقصد درخواست ارسال شده توسط کلاینت DHCP (discovery request) چیست؟ آدرس IP و MAC مربوط به مبدأ پاسخ ارسال شده از طرف سرور DHCP (discovery request) چیست؟

پاسخ:

IP: 255.255.255.255, MAC: FF:FF:FF:FF:FF:FF

IP: آدرس IP مربوط به سرور DHCP و MAC: آدرس MAC مربوط به سرور DHCP

سؤال 4: زمانی که یک بسته مسیریاب NAT را ترک می­کند، این بسته باید از طریق اینترنت به سمت مقصدش که سرور وب است، هدایت شود. برای این مسأله شکل زیر را در نظر بگیرید:



فرض کنید که گره u، مسیریاب مربوط به NAT بوده و سرور وب به گره z متصل است. با توجه به الگوریتم کوتاه­ترین مسیر دایجسترا، جدول زیر را تکمیل کرده و کوتاه­ترین مسیر را از u به z مشخص کنید.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | Step |
| ∞ | ∞ | 1, u | ∞ | 2, u |  | 0 |
| ∞ | 2, x |  | 4, x | 2, u | ux | 1 |
| 4, y |  |  | 3, y | 2, u | uxy | 2 |
| 4, y |  |  | 3, y |  | uxyv | 3 |
| 4, y |  |  |  |  | uxyvw | 4 |
|  |  |  |  |  | uxyvwz | 5 |

سؤال 5: به سؤالات زیر پاسخ دهید.

الف) الگوریتم‏های مسیریابی Distance-Vector و Link-State را با هم مقایسه کنید.

ب) پیام‏های اعلان استفاده شده در پروتکل‏های RIP و OSPF را باهم مقایسه کنید.

ج) BGP چگونه از نشان‏های AS-PATH و NEXT-HOP استفاده می‏کند؟

د) زمانی که یک میزبان به یک گروه Multicast ملحق می‏شود، آیا ضروری است که آدرس IP خود را به آدرس این گروه Multicast تغییر دهد ؟

پاسخ:

الف) الگوریتم‏های Link State، محاسبات کم‏هزینه‏ترین مسیر بین مبدأ و مقصد را بر اساس دانش سراسری و کامل از شبکه انجام می‏دهند. الگوریتم‏های Distance-Vector این کار را به صورت تکرارشونده و توزیع‌شده انجام می‏دهند.

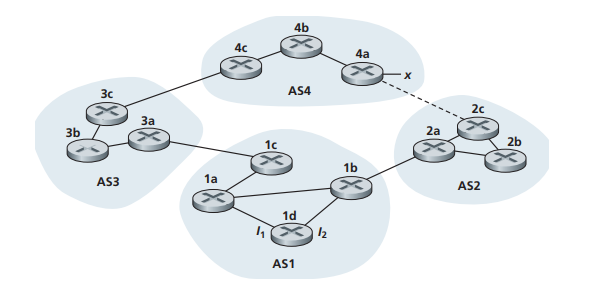
ب) در پروتکل OSPF، مسیریاب‏ها به صورت متناوب اطلاعات مسیریابی را، نه فقط به مسیریاب‏های همسایه، بلکه به تمام مسیریاب‏های داخل AS همه پخشی می‏کنند. این اطلاعات مسیریابی، یک مدخل به ازای هر لینک همسایه دارد که فاصله‏ی مسیریاب همسایه از این مسیریاب در آن قرار دارد. در پیام اعلان RIP، اطلاعات تمامی شبکه، صرفاً به مسیریاب‏های همسایه ارسال می‏شود.

ج) از AS-PATH برای تشخیص و جلوگیری از ایجاد حلقه در ارسال پیام‏های اعلان و همچنین برای انتخاب بین چندین مسیر منتهی به یک شبکه (پیشوند) استفاده می‏شود. NEXT-HOP نشان‏دهنده‏ی آدرس IP اولین مسیریاب در مسیر اعلان شده به یک پیشوند است.

د) خیر نیازی به این کار نیست.

سؤال 6: شبکه زیر را در نظر بگیرید. فرض کنید که AS3 و AS2 برای پروتکل مسیریابی intra-AS از OSPF استفاده می­کند و AS1 و AS4 برای پروتکل مسیریابی intra-AS از RIP استفاده می­کند. همچنین فرض کنید که در پروتکل مسیریابی inter-AS از eBGP و iBGP استفاده شده است. از ابتدا فرض شده است که AS1 از AS4 قابل دسترس نیست.

* 1. مسیریاب 3c از طریق کدام پروتکل مسیریابی پیشوند x را یاد می­گیرد.
  2. مسیریاب 3a از طریق کدام پروتکل مسیریابی پیشوند x را یاد می­گیرد.
  3. مسیریاب 1c از طریق کدام پروتکل مسیریابی پیشوند x را یاد می­گیرد.
  4. مسیریاب 1d از طریق کدام پروتکل مسیریابی پیشوند x را یاد می­گیرد.



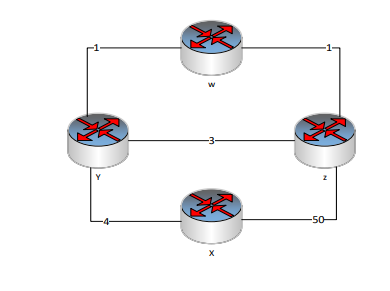
پاسخ:

1. eBGP
2. iBGP
3. eBGP
4. iBGP

سؤال 7: شبکه زیر را در نظر بگیرید که هزینه‌ی مربوط به لینک­ها در آن مشخص شده است. فرض کنید که از poisoned reverse در الگوریتم مسیریابی distance vector استفاده می­شود.

الف) پس از همگرایی الگوریتم مسیریابی distance vector ،مسیریابw ،y و z فاصله­های خود تا x را به یکدیگر اطلاع می­دهند. مقدار آن‌ها را مشخص کنید.

ب) حال فرض کنید که هزینه لینک بین x و y به 60 افزایش می­یابد. آیا در صورت استفاده از poisoned reverse مشکل count-to-infinity وجود دارد؟ چرا؟ اگر این مشکل وجود دارد، مسیریابی distance vector به چه تعداد تکرار نیاز دارد تا دوباره به حالت پایدار برسد؟ پاسخ خود را توضیح دهید.



پاسخ:

|  |  |
| --- | --- |
| Router z | Informs w, Dz(x)=∞ |
| Informs y, Dz(x)=6 |
| Router w | Informs y, Dw(x)=∞ |
| Informs z, Dw(x)=5 |
| Router y | Informs w, Dy(x)=4 |
| Informs z, Dy(x)=4 |

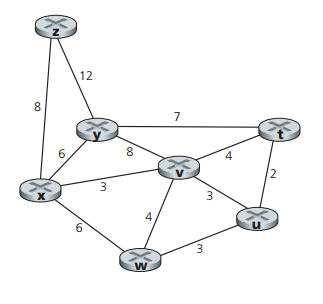
2. بله، این مشکل وجود دارد. جدول زیر مراحل مربوط به همگرایی مسیریابی را مشخص می­کند. فرض کنید که در لحظه­ی ، هزینه­ی لینک تغییر می­کند. در لحظه­ی ، y هزینه­ی لینک­ها را به­روزرسانی می­کند و به همسایه­های خود (w,z) اطلاع می­دهد. در جدول زیر ‘🡪’ نشان‌دهنده اطلاعاتی است که به گره دیگر رسیده است.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| time | t0 | t1 | t2 | t3 | t4 |
| Z | 🡪 w, Dz(x)=∞ |  | No change | 🡪 w, Dz(x)=∞ |  |
|  | 🡪 y, Dz(x)=6 |  |  | 🡪 y, Dz(x)=11 |  |
| W | 🡪 y, Dw(x)=∞ |  | 🡪 y, Dw(x)=∞ |  | No change |
|  | 🡪 z, Dw(x)=5 |  | 🡪 z, Dw(x)=10 |  |  |
| Y | 🡪 w, Dy(x)=4 | 🡪 w, Dy(x)=9 |  | No change | 🡪 w, Dy(x)=14 |
|  | 🡪 z, Dy(x)=4 | 🡪 z, Dy(x)= ∞ |  |  | 🡪 z, Dy(x)= ∞ |

همان­طور که مشاهده می­کنید، گره­های y,w,z برای محاسبه­ی هزینه­ تا مسیریاب x یک حلقه را ایجاد می­کنند. اگر به این تکرار ادامه دهیم، همان­طور که در جدول بالا مشاهده می­کنید، در لحظه­ی ، z متوجه می­شود که کمترین هزینه­اش به x با یک لینک مستقیم، برابر با 50 است. در لحظه­ی ، کوتاه­ترین مسیر از w به x از طریق z برابر با 51 است و در لحظه­ی ، کوتاه‌ترین مسیر از y به x از طریق w برابر با 52 است. در نهایت در لحظه­ی هیچ به­روزرسانی وجود ندارد.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| time | t27 | t28 | t29 | t30 | t31 |
| Z | 🡪 w, Dz(x)=50 |  |  |  | via w, ∞ |
|  | 🡪 y, Dz(x)=50 |  |  |  | via y, 55  via z, 50 |
| W |  | 🡪 y, Dw(x)=∞ | 🡪 y, Dw(x)=51 |  | via w, ∞ |
|  |  | 🡪 z, Dw(x)=50 | 🡪 z, Dw(x)= ∞ |  | via y, ∞  via z, 51 |
| Y |  | 🡪 w, Dy(x)=53 |  | 🡪 w, Dy(x)= ∞ | via w, 52 |
|  |  | 🡪 z, Dy(x)= ∞ |  | 🡪 z, Dy(x)= 52 | via y, 60  via z, 53 |

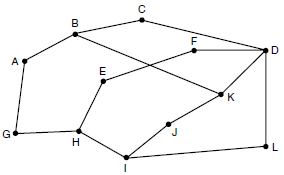
سؤال 8: شبکه­­ی زیر را در نظر بگیرید. با توجه به هزینه­ی مشخص شده برای لینک­ها، با استفاده از الگوریتم کوتاه­ترین مسیر Dijkstra، کوتاه­ترین مسیر را از x به همه­ی گره­های شبکه محاسبه کنید. با استفاده از جدولی مشابه جدول 4.3 کتاب مرجع (نسخه­ی 6) نشان دهید که الگوریتم چگونه کار می­کند.



پاسخ:

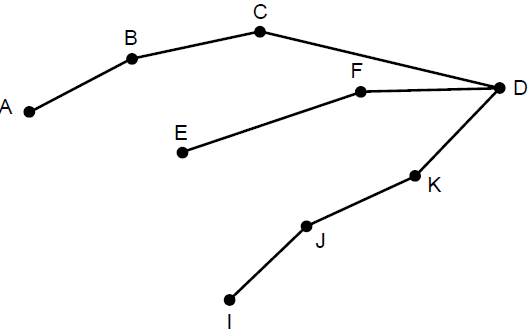
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| *Step* | *N’* | *D(t),p(t)* | *D(u),p(u)* | *D(v),p(v)* | *D(w),p(w)* | *D(y),p(y)* | *D(z),p(z)* |
| 0 | x | ∞ | ∞ | 3,x | 6,x | 6,x | 8,x |
| 1 | xv | 7,v | 6,v |  | 6,x | 6,x | 8,x |
| 2 | xvu | 7,v |  |  | 6,x | 6,x | 8,x |
| 3 | xvuw | 7,v |  |  |  | 6,x | 8,x |
| 4 | xvuwy | 7,v |  |  |  |  | 8,x |
| 5 | xvuwyt |  |  |  |  |  | 8,x |
| 6 | xvuwytz |  |  |  |  |  |  |

سؤال 9: با در نظر گرفتن شکل زیر، درخت پوشای Multicast را برای مسیریاب C محاسبه کنید. گروه Multicast شامل مسیریاب‏های A، B، C، D، E، F، I و K است.

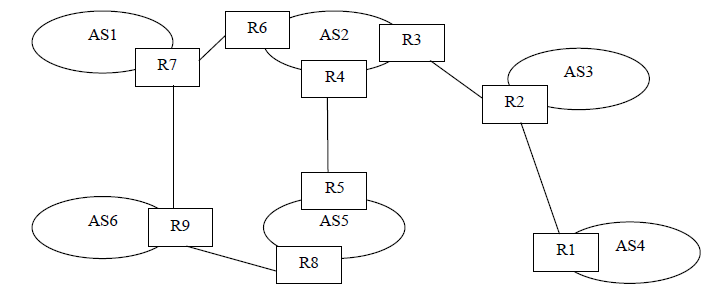


پاسخ:

درخت‏های مختلفی قابل تشکیل است. یک مثال به صورت زیر است.



سؤال 10: شکل زیر را در نظر بگیرید.



الف) در صورتی که یک پیشوند مشخص در AS4 نیاز به اعلان داشته باشد، این اعلان از چه مسیرهایی عبور می‏کند تا تمامی مسیریاب‏ها این پیشوند را ذخیره کنند؟

ب) فرض کنید لینک بین R1 و R2 خراب شود. آیا بین AS1، AS2، AS5 و AS6 حلقه تشکیل می‏شود ؟ توضیح دهید.

پاسخ:

الف) R1 پروتکل eBGP را اجرا کرده و یک ارتباط TCP با R2 برقرار می‏سازد تا اطلاعات مسیریابی را ردوبدل کند. R2 پیام دریافتی را با یک ارتباط TCP مبتنی بر پروتکل eBGP به R3 ارسال می‏کند. R3 این اطلاعات را از طریق iBGP به R4 و R6 ارسال می‏کند. R6 اطلاعات را به R9 و R4 به R5 از طریق eBGP اعلان می‏کند. نهایتاً R5 از طریق iBGP و R9 از طریق eBGP اطلاعات را به R8 ارسال می‏کنند.

ب) با استفاده از مسیریابی path-vector، هرگاه یک مسیریاب BGP یک پیام حاوی AS-PATH دریافت کند که شامل AS Number همین مسیریاب باشد، یک حلقه تشکیل شده است. مسیریاب BGP از این مسیر چشم‏پوشی می‏کند و این اطلاعات دریافتی را دور می‏اندازد.

سؤال11: پروتکل مسیریابی RIP از پروتکل UDP استفاده می‏کند. BGP از TCP استفاده کرده و پروتکل OSPF روی IP اجرا می‏شود. دلیل این انتخاب‏ها را در هر یک از پروتکل‏های RIP، BGP و OSPF شرح دهید.

RIP پروتکلی توزیع‌شده مبتنی بر distance-vector است. پیام‏ها تنها بین همسایه‏ها و به صورت متناوب (یا در صورت بروز یک تغییر) ردوبدل می‏شوند. UDP برای تبادل پیام بدون تضمین تحویل پیام مناسب است. با توجه به اینکه پیام‌ها به صورت متناوب ارسال می‏شوند، نرسیدن یک پیام اهمیت چندانی ندارد زیرا مجدداً ارسال خواهد شد.

OSPF مبتنی بر استفاده از یک پروسه‏ی قابل اطمینان سیلابی است که اطلاعات link-state را بین تمامی مسیریاب‏ها توزیع کند. این پروسه‏ی قابل اطمینان نیازمند ارتباط و هماهنگی نزدیک با عملیات مسیریاب‏ها است. در نتیجه کارکرد آن بر بستر IP، به حالتی که در لایه‏ی انتقال کار کند ترجیح داده شده است.

همتاهای BGP کل اطلاعات جدول مسیریابی BGP را در ابتدای کار ردوبدل می‏کنند. برای کاهش استفاده از پهنای باند، پیام‏های به‌روزرسانی افزایشی به جای پیام‏های متناوب ارسال می‏شوند. پیام‏های کوچک متناوب KEEP ALIVE برای مشخص کردن اینکه همتاها زنده هستند استفاده می‏شود. ارسال مطمئن اطلاعات مسیریابی برای کمینه کردن استفاده از پهنای باند ضروری است. در نتیجه از پروتکل TCP برای این انتقال مطمئن استفاده می‏شود.

سؤال 12: پروتکل‏های RIP و OSPF را، از نظر زمان همگرایی و تعداد پیام‏های رد و بدل شده، در 3 حالت زیر با هم مقایسه کنید.

الف) خرابی لینک

ب) خرابی گره

ج) اضافه شدن یک لینک جدید

پاسخ:

الف) زمان همگرایی OSPF نسبت به RIP کمتر است. زمانی که یک لینک خراب شود، مسیریاب OSPF مربوطه، به‌روزرسانی link-state را به تمامی همتاهای خود ارسال می‏کند و مسیریاب‏های همتا، پایگاه داده‌های خود را به‌روزرسانی می‏کنند. این پروسه باعث می‏شود که اطلاعات خرابی لینک به سرعت به مسیریاب‌ها برسد. اما در RIP، مسیریاب RIP مربوطه distance vector مربوط به خود را به‌روزرسانی می‏کند و به‌روزرسانی را صرفاً به مسیریاب‏های همسایه ارسال می‏کند. مسیریاب‏های همسایه، جدول مسیریابی خود را به‌روزرسانی می‏کنند، مقادیر جدید distance vector را محاسبه کرده و این مقادیر به‌روزرسانی شده را به همسایه‏های خود ارسال می‏کنند. سربار پردازش و توزیع پیام در RIP باعث می‏شود که زمان همگرایی RIP زیاد باشد. البته همگرایی سریع در OSPF هزینه‏ی پخش سیل‏آسای پیام‏های به‌روزرسانی در سطح شبکه را دارد.

ب) همگرایی OSFP سریع‌تر است. OSPF هر 10 ثانیه یک پیام HELLO ارسال می‏کند. این زمان برای RIP 30 ثانیه است. زمانی که یک گره خراب می‏شود، OSPF می‏تواند آن را در کمتر از 10 ثانیه تشخیص دهد. در حالی که RIP در بدترین حالت 180 ثانیه برای تشخیص خرابی گره زمان نیاز دارد. دلیل این زمان زیاد، استفاده‏ی RIP از UDP است که تضمینی برای تحویل پیام به مقصد ندارد. در عوض OSPF پیام‏های بیشتری ردوبدل می‏کند.

ج) OSPF همگرایی سریع‏تری از RIP دارد. وقتی یک لینک جدید اضافه می‏شود، مسیریاب‏های OSPF متصل به این لینک شروع به ارسال پیام‏های HELLO می‏کنند. سپس این مسیریاب‏ها پیام‏های توصیف پایگاه link-state را ردوبدل می­کنند. همچنین برای سرآیندهای LSA که در پایگاه ‏داده‏ی link-state مربوطه‏ی خود نیستند، پیام‏های درخواست link-state ارسال می‏کنند. پس از به‌روزرسانی و همگام‏سازی پایگاه ‏داده‏ها، این مسیریاب‏های OSPF، بسته‏های توصیف پایگاه ‏داده‏‏ی بروزرسانی شده را به همسایه‏های خود ارسال می‏کنند و الگوریتم‏های مسیریابی را برای پیدا کردن کوتاه‏ترین مسیر اجرا می‏کنند. این در حالی است که مسیریاب RIP باید در ابتدا محاسبات مربوط به مسیریابی مبتنی بر distance vector را انجام دهد. سپس distance-vector به روزرسانی شده را به همسایه‏های خود ارسال می‏کند. به دلیل سربار پردازشی در هر مسیریاب RIP، این پروتکل کندتر از OSPF است.

جدول زیر مقایسه‏ای از این دو پروتکل را نمایش می‏دهد:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| رویداد مورد نظر | زمان همگرایی | | تعداد پیام‏های ردوبدل شده | |
| RIP | OSPF | RIP | OSPF |
| خرابی لینک | کندتر | سریع‏تر | کمتر | بیشتر |
| خرابی گره | کندتر | سریع‏تر | کمتر | بیشتر |
| اضافه شدن لینک جدید | کندتر | سریع‏تر | کمتر | بیشتر |

**در صورت هرگونه مشکل یا سؤال درخصوص تمرین‌ها و پروژه‌های درس شبکه‌های کامپیوتری 1 با تدریسیاران درس تماس بگیرید.**

**فرشید صانعی (sanei@aut.ac.ir)، فاطمه امیدوار (omidvar73@aut.ac.ir).**