بسمه تعالی

دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر

درس شبکه‌های کامپیوتری، نیمسال دوم سال تحصیلی ۱۴۰۴-۱۴۰۳

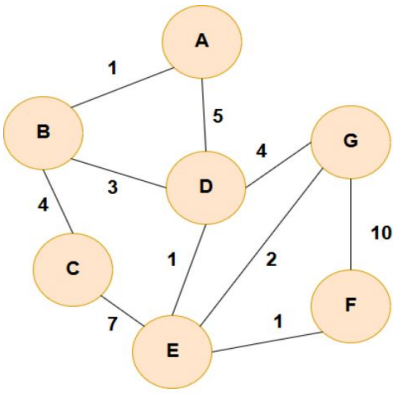
پاسخ تمرین سری هفتم

سوال ۱:

الف) شبه کد الگوریتم دایکسترا را بنویسید.

ب) الگوریتم مسیریابی سیل‌آسا، کاربرد آن و دو مورد از مشکلات آن را شرح دهید.

ج) شبکه زیر را در نظر بگیرید. با توجه به هزینه مشخص‌شده برای لینک‌ها، با استفاده از الگوریتم کوتاه‌ترین مسیر دایکسترا، کوتاه‌ترین مسیر از گره مبدأ A به همه گره‌های شبکه با ذکر تمام جزئیات به روز رسانی هزینه‌های رسیدن به گره‌های مقصد را محاسبه و جدول مربوط به گام‌های اجرای الکوریتم را بنویسید.



پاسخ:

الف)

```
Initialization:
  N' = {u}                  /* compute least cost path from u to all other nodes */
  for all nodes v:
     if v adjacent to u:    /* u initially knows direct-path-cost only to direct neighbors */
        D(v) = c(u,v)       /* but may not be minimum cost */
     else:
        D(v) = ∞

Loop:
  while (all nodes not in N'):
     find w not in N' such that D(w) is a minimum
     add w to N'
    for each neighbor v of w that is not in N':
          D(v) = min( D(v), D(w) + c(w,v) )
 */          new least-path-cost to v is either old least-cost-path to v,
            or known least-cost-path to w plus direct cost from w to v */
```

ب) درالگوریتم مسیریابی سیل‌آساهر گره با دریافت یک بسته، یک کپی از آن بسته ازطریق تمام پورت‌های خروجی به جز پورتی که ازطریق آن بسته را دریافت کرده، ارسال می‌کند. به این کار ارسال فراگیر مجدد (Rebroadcast) گفته می‌شود.

این الگوریتم در موارد زیر کاربرد دارد:

۱- اطلاع‌رسانی یک اطلاعات به همه گره‌های شبکه،به عنوان مثال، ارسال اطلاعات وضعیت لینک‌ها به همه گره‌های شبکه در پروتکل‌های مسیریابی.

۲- در زمان راه‌اندازی یک گره که اطلاعاتی از توپولوژی شبکه ندارد، نظیر دریافت آدرس یا تنظیمات اولیه.

۳- در کاربردهایی نظیر شبکه‌های بیسیم سیار که نرخ تغییرات توپولوژی زیاد است.

مشکل‌الگوریتم سیل‌آسا، سربار زیاد ارسال بسته‌ها Rebroadcast شده است که یک گره یک بسته را چندین بار دریافت و Rebroadcast می‌کند .یکی دیگر از مشکلات الگوریتم سیل‌آسااحتمال‌در Loop افتادن بسته‌ها است.

ج)

Step	N'	D(B) P(B)	D(C) P(C)	D(D) P(D)	D(E) P(E)	D(F) P(F)	D(G) P(G)
۰	A	1,A	∞	5,A	∞	∞	∞
۱	AB	-	5,B	4,B	∞	∞	∞
۲	ABD	-	5,B	-	5,D	∞	8,D
۳	ABDC	-	-	-	5,D	∞	8,D
۴	ABDCE	-	-	-	-	6,E	7,E
۵	ABDCEF	-	-	-	-	-	7,E
۶	ABDCEFG						

سوال ۲:

الف) مسیریابی ایستا (static) و پویا (dynamic) را از نظر نحوه به‌روزرسانی مقایسه کنید.

ب) چرا در برخی شبکه‌ها استفاده از الگوریتم‌های مسیریابی پویا نسبت به ایستا ترجیح داده می‌شود؟

ج) در الگوریتم‌های مسیریابی غیرمتمرکز مانند بردار فاصله (Distance Vector)، چگونه هر گره بهترین مسیر به مقصد را بدست می‌آورد؟ نقش گره‌های همسایه در این فرآیند چیست؟

پاسخ:

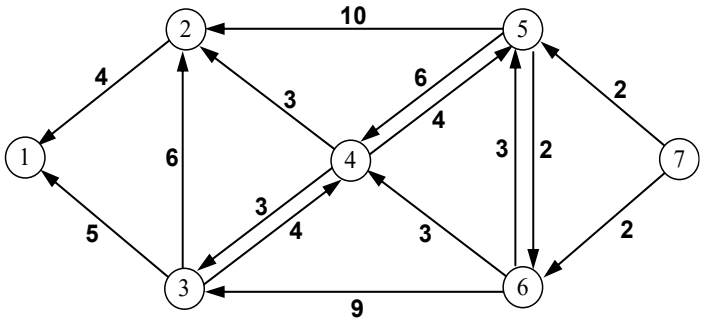
الف) در مسیریابی ایستا(static) ، مسیرها به صورت دستی توسط مدیر شبکه در جدول‌های جلورانی وارد می‌شوند و معمولاً در طول زمان تغییر نمی‌کنند، مگر اینکه مدیر شبکه شخصاً آن‌ها را به‌روزرسانی کند. اما در مسیریابی پویا(dynamic) ، مسیرها به‌صورت خودکار و پویا با توجه به تغییرات در توپولوژی شبکه و هزینه لینک‌ها به‌روزرسانی می‌شوند. این به‌روزرسانی‌ها از طریق اجرای الگوریتم‌های مسیریابی صورت می‌گیرند و نیازی به دخالت دستی ندارند.

ب) در شبکه‌هایی که توپولوژی آن‌ها به‌طور مداوم تغییر می‌کند (مانند شبکه‌های موبایل یا بی‌سیم)، استفاده از الگوریتم‌های پویا منطقی‌تر است؛ زیرا این الگوریتم‌ها می‌توانند به‌صورت خودکار مسیرهای جدید را کشف و تنظیم کنند. برای مثال، در یک شبکه ad-hoc که گره‌ها ممکن است جابه‌جا شوند یا خاموش شوند، استفاده از مسیریابی پویا باعث می‌شود مسیرها به‌روز باقی بمانند و ارتباطات بدون اختلال ادامه یابد. در حالی‌که الگوریتم‌های ایستا در چنین شرایطی ناکارآمد هستند.

ج) در این الگوریتم‌ها، هر گره فقط اطلاعات مربوط به همسایه‌های مستقیم خود و فاصله تا آن‌ها را دارد. هر گره به صورت دوره‌ای اطلاعات مربوط به جدول مسیریابی‌اش را برای همسایه‌هایش ارسال می‌کند. سپس هر گره، با دریافت اطلاعات از همسایگان، بهترین مسیر را بر اساس کمترین فاصله یا هزینه انتخاب کرده و جدول خود را به‌روزرسانی می‌کند. در واقع، هر گره با کمک داده‌های همسایگان، تخمینی از بهترین مسیر به هر مقصد ارائه می‌دهد.

سوال ۳:

کوتاه‌ترین مسیر از هر گره به گره (۱) را در گراف شکل زیر با استفاده از الگوریتم Bellman-Ford و Dijkstra بیابید.



پاسخ:

الگوریتم Dijkstra:

iteration	N’	D(1), P(1)	D(2), P(2)	D(3), P(3)	D(4), P(4)	D(5), P(5)	D(6), P(6)	D(7), P(7)
0	{1}	0, 1	4, 1	5, 1	inf	inf	inf	inf
1	{1, 2}	0, 1	4, 1	5, 1	7, 2	14, 2	inf	inf
2	{1, 2, 3}	0, 1	4, 1	5, 1	7, 2	14, 2	14, 3	inf
3	{1, 2, 3, 4}	0, 1	4, 1	5, 1	7, 2	13, 4	10, 4	inf
4	{1, 2, 3, 4, 6}	0, 1	4, 1	5, 1	7, 2	12, 6	10, 4	12, 6
5	{1, 2, 3, 4, 6, 5}	0, 1	4, 1	5, 1	7, 2	12, 6	10, 4	12, 6
6	{1, 2, 3, 4, 6, 5, 7}	0, 1	4, 1	5, 1	7, 2	12, 6	10, 4	12, 6

الگوریتم Bellman-Ford:

1. Initialization

$$D_i = \infty, \forall i \neq d$$
$$D_d = 0$$

2. Updating: For each $i \neq d$,

$$D_i = \min_j \{C_{ij} + D_j\}, \forall j \neq i$$

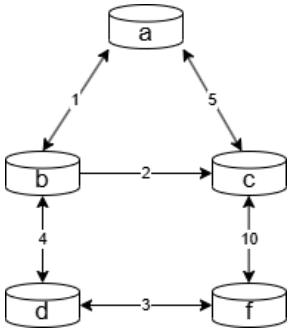
Repeat step 2 until no more changes occur in the iteration.

Iteration	2	3	4	5	6	7
Initial	(-1, inf)	(-1, inf)	(-1, inf)	(-1, inf)	(-1, inf)	(-1, inf)
	(1, 4)	(1, 5) (2, inf) (4, inf)	(2, inf) (3, inf) (5, inf)	(2, inf) (4, inf) (6, inf)	(3, inf) (4, inf) (5, inf)	(5, inf) (6, inf)
1	**(1, 4)**	**(1, 5)**	**(-1, inf)**	**(-1, inf)**	**(-1, inf)**	**(-1, inf)**
	(1, 4)	(1, 5) (2, 10) (4, inf)	(2, 7) (3, 8) (5, inf)	(2, 14) (4, inf) (6, inf)	(3, 14) (4, inf) (5, inf)	(5, inf) (6, inf)
2	**(1, 4)**	**(1, 5)**	**(2, 7)**	**(2, 14)**	**(3, 14)**	**(-1, inf)**
	(1, 4)	(1, 5) (2, 10)	(2, 7) (3, 8)	(2, 14) (4, 13)	(3, 14) (4, 10)	(5, 16) (6, 16)

		(4, 11)	(5, 18)	(6, 16)	(5, 17)	
3	**(1, 4)**	**(1, 5)**	**(2, 7)**	**(4, 13)**	**(4, 10)**	**(5, 16)**
	(1, 4)	(1, 5) (2, 10) (4, 11)	(2, 7) (3, 8) (5, 17)	(2, 14) (4, 13) (6, 12)	(3, 14) (4, 10) (5, 16)	(5, 15) (6, 12)
4	**(1, 4)**	**(1, 5)**	**(2, 7)**	**(6, 12)**	**(4, 10)**	**(6, 12)**
	(1, 4)	(1, 5) (2, 10) (4, 11)	(2, 7) (3, 8) (5, 16)	(2, 14) (4, 13) (6, 12)	(3, 14) (4, 10) (5, 15)	(5, 14) (6, 12)
5	**(1, 4)**	**(1, 5)**	**(2, 7)**	**(6, 12)**	**(4, 10)**	**(6, 12)**

سوال ۴:

در شبکه زیر الگوریتم بردار فاصله (distance vector) را تا ۳ مرحله اجرا کنید (اگر زودتر همگرا شد نیازی به ادامه دادن نیست).



پاسخ:

DV in	To a	To b	To c	To d	To f
a	0	1	5	inf	inf
b	1	0	2	4	inf
c	5	inf	0	inf	10
d	inf	4	inf	0	3
f	inf	inf	10	3	0

DV in	To a	To b	To c	To d	To f
a	0	1	3 (b)	5 (b)	15(c)
b	1	0	2	4	7 (d)
c	5	6 (a)	0	13 (f)	10
d	5 (b)	4	6 (b)	0	3
f	15 (c)	7 (d)	10	3	0

DV in	To a	To b	To c	To d	To f
a	0	1	3 (b)	5 (b)	8 (b)
b	1	0	2	4	7 (d)

c	5	6 (a)	0	10 (a)	10
d	5 (b)	4	6 (b)	0	3
f	8 (d)	7 (d)	10	3	0

سوال ۵:

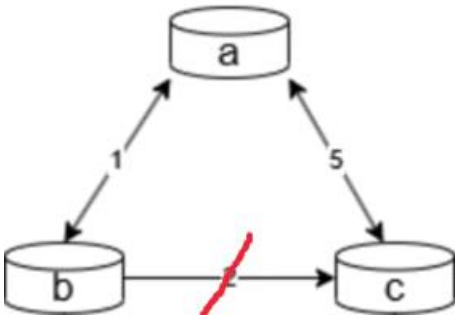
الف) در مسیریابی بردار فاصله، سناریویی پیدا کنید که در آن مسئله شمارش تا بینهایت رخ می‌دهد.

ب) برای مسئله شمارش تا بینهایت ۲ راه حل پیدا کنید و هر کدام را توضیح دهید. هر کدام از راه‌حل‌ها در چه شرایط و توپولوژی دچار مشکل می‌شوند؟

ج) مشکل قسمت (الف) را با استفاده از این دو راه حل، برطرف کنید.

پاسخ:

الف) بخش زیر را که در سوال قبل حل کرده اید را در نظر بگیرید. اگر مشکلی در لینک بین c و b پیش بیاید b از این خرابی مطلع میشود اما a از آن بی اطلاع هست.a به b اعلام می کند که راهی به c با هزینه 3 دارد و b در جدول خود برای مقصد c عدد ۴ را می گذارد و این فرایند تکرار می شود...



ب)

Split Horizon:

اگر روتر A از روتر B درباره یک مقصد اطلاعاتی دریافت کند، روتر A این مقصد را در به‌روزرسانی‌های ارسالی به روتر B شامل نمی‌کند. این کار حلقه‌های احتمالی را با جلوگیری از بازخورد اطلاعات نادرست قطع می‌کند.

اگر به‌روزرسانی‌های مسیریابی همگام نباشند یا تأخیر در انتشار به‌روزرسانی‌ها وجود داشته باشد، یک روتر ممکن است اطلاعات قدیمی را قبل از اعمال افق تقسیم منتشر کند، که منجر به شمارش تا بی‌نهایت می‌شود.

poisoned reverse:

در عکس مسمومیت، وقتی یک روتر مسیری را از یک همسایه آموخته است نه تنها از انتشار آن مسیر به همسایه اصلی خودداری می‌کند (مطابق روش قبل)، بلکه به صورت فعال آن مسیر را با متریک بی‌نهایت به همان همسایه انتشار می دهد. این کار به همسایه اطلاع می‌دهد که مسیر دیگر معتبر نیست.

اگر به‌روزرسانی‌های مسموم شده به دلیل ازدحام شبکه یا از دست رفتن بسته‌ها به برخی روترها نرسد، ممکن است همچنان حلقه‌های موقتی شکل بگیرند و در توپولوژی های توری شد زمانی که شبکه بسیار بزرگ هست از آنجا که روتر ها به صورت دائم در حال اعلام مسیر هایی که مسموم شده اند هستند بار زیادی برای انتقال این اطلاعات به روی شبکه می آید.

ج) در روش split horizon روتر a اطلاعی از مسیری که از طریق b به c میرسد به b نمی دهد پس b جدول خود را با اطلاعات منقضی شده پر نمی کند.

در روش عکس مسمویست روتر a به b اعلام می کند که مسیری که به c دارد inf هست و b جدول خود را با اطلاعات منقضی شده پر نمی کند.

سوال ۶:

توضیح دهید که چگونه یک مسیریاب مخرب می‌تواند در الگوریتم بردار فاصله (distance vector) بردارهای فاصله را دستکاری کند تا باعث ایجاد خرابی در مسیریابی شود. توضیح دهید چرا الگوریتم وضعیت لینک (Link state) نسبت به این گونه حملات مقاوم‌تر است.

پاسخ:

یک مسیریاب مخرب می‌تواند به دروغ ادعا کند که به مقصدی خاص (مثلا شبکه X) با متریک بسیار پایین (مثلاً ۱) دسترسی دارد، حتی اگر به آن مقصد متصل نباشد یا مسیر واقعی هزینه بالاتری داشته باشد. با این کار شبکه دچار اختلال می شود به طور مثال زمانی که متریک بسیار پایینی قرار می دهد روتر های شبکه همه بسته های خود را به این روتر مخرب می فرستند. اما از آنجا که الگوریتم وضعیت لینک دارای تأیید مستقل مسیرها و انتشار اطلاعات لینک‌های مستقیم هست مقاومت بیشتری در برابر حملات مخرب دارد. این ویژگی‌ها تشخیص و رد اطلاعات جعلی را آسان‌تر می‌کنند.

سوال ۷:

الف) سیستم خودمختار یا مستقل (Autonomous System) را تعریف کنید و انواع آن را نام ببرید.

ب) پروتکل‌های بین‌دامنه‌ای و داخل‌دامنه‌ای را از لحاظ سیاست، مقیاس، و عملکرد مقایسه کنید.

ج) در پروتکل BGP چهار نوع پیام رد و بدل می‌شود. هر پیام را نام برده و کاربرد آن را توضیح دهید.

پاسخ:

الف) سیستم خودمختار (AS) گروهی از روترها هستند که تحت یک کنترل مدیریتی واحد قرار دارند. اغلب، روترهای یک ارائه‌دهنده خدمات اینترنت (ISP) و لینک‌های ارتباطی بین آن‌ها، یک AS واحد را تشکیل می‌دهند. با این حال، برخی از ISPها ممکن است شبکه خود را به چندین AS تقسیم کنند. به عنوان مثال، بعضی از ISPهای Tier-1 از یک AS بزرگ برای کل شبکه خود استفاده می‌کنند، در حالی که برخی دیگر، ISP خود را به ده‌ها AS متصل به هم تقسیم می‌کنند.

هر سیستم خودمختار با یک شماره سیستم خودمختار (ASN) منحصربه‌فرد جهانی شناسایی می‌شود .شماره‌های AS، مانند آدرس‌های IP، توسط رجیستری‌های منطقه‌ای ICANN اختصاص داده می‌شوند.

روترهای درون یک AS، همگی از یک الگوریتم مسیریابی مشابه استفاده می‌کنند و از اطلاعات مربوط به یکدیگر آگاه هستند. الگوریتم مسیریابی که در داخل یک سیستم خودمختار اجرا می‌شود، پروتکل مسیریابی درون سیستم خودمختار (intra-autonomous system routing protocol) نامیده می‌شود.

ب) سیاست (Policy):

در میان سیستم‌های خودمختار (AS)، مسائل مربوط به سیاست‌ها حرف اول را می‌زند. ممکن است بسیار مهم باشد که ترافیک مبدأ گرفته از یک AS خاص، به طور مشخص از یک AS خاص دیگر عبور نکند. به طور مشابه، یک AS خاص ممکن است بخواهد کنترل کند که چه ترافیک عبوری را بین ASهای دیگر حمل می‌کند. دیدیم که BGP به طور خاص ویژگی‌های مسیر را حمل می‌کند و توزیع کنترل‌شده اطلاعات مسیریابی را فراهم می‌سازد تا چنین تصمیمات مسیریابی مبتنی بر سیاست گرفته شود. در داخل یک AS، همه چیز اسماً تحت یک کنترل مدیریتی قرار دارد و بنابراین مسائل مربوط به سیاست نقش بسیار کم‌اهمیت‌تری در انتخاب مسیرها در داخل AS ایفا می‌کنند.

مقیاس (Scale):

توانایی یک الگوریتم مسیریابی و ساختارهای داده آن برای مقیاس‌پذیری جهت مدیریت مسیریابی به/در میان تعداد زیادی از شبکه‌ها، یک مسئله حیاتی در مسیریابی بین ASها است. در داخل یک AS، مقیاس‌پذیری نگرانی کمتری است. اولاً، اگر یک دامنه مدیریتی واحد بیش از حد بزرگ شود، همیشه می‌توان آن را به دو AS تقسیم کرد و مسیریابی بین ASها را بین دو AS جدید انجام داد.

عملکرد (Performance)

از آنجا که مسیریابی بین AS به شدت سیاست‌محور است، کیفیت (به عنوان مثال، عملکرد) مسیرهای مورد استفاده اغلب در درجه دوم اهمیت قرار دارد (یعنی، یک مسیر طولانی‌تر یا پرهزینه‌تر که معیارهای سیاست خاصی را برآورده می‌کند، ممکن است بر مسیری که کوتاه‌تر است اما آن معیارها را برآورده نمی‌کند، ارجحیت داده شود). در واقع، دیدیم که در میان ASها، حتی مفهوم اولویت یا هزینه‌های مرتبط با مسیرها وجود ندارد. با این حال، در داخل یک AS واحد، چنین نگرانی‌های سیاستی را می‌توان نادیده گرفت و به مسیریابی اجازه می‌دهد تا بیشتر بر سطح عملکردی که در یک مسیر محقق می‌شود، تمرکز کند.

ج) پروتکل BGP چهار نوع پیام را تعریف می‌کند: OPEN، UPDATE، NOTIFICATION و KEEPALIVE.

OPEN

همتایان BGP با استفاده از پروتکل TCP و شماره پورت ۱۷۹ با یکدیگر ارتباط برقرار می‌کنند. بنابراین TCP تبادل پیام قابل اعتماد و کنترل‌شده با ازدحام را بین همتایان فراهم می‌کند. در مقابل، دو همتای RIP از طریق UDP غیرقابل اعتماد ارتباط برقرار می‌کنند. هنگامی که یک گیت‌وی BGP می‌خواهد برای اولین بار با یک همتای BGP ارتباط برقرار کند (مثلاً پس از اینکه خود گیت‌وی یا یک لینک اتصال به تازگی راه‌اندازی شده است)، یک پیام OPEN به همتا ارسال می‌شود. پیام OPEN به یک گیت‌وی BGP اجازه می‌دهد تا خود را شناسایی و احراز هویت کند و اطلاعات تایمر را ارائه دهد. اگر پیام OPEN برای همتا قابل قبول باشد، یک پیام KEEPALIVE به عنوان پاسخ ارسال خواهد کرد.

UPDATE

یک گیت‌وی BGP از پیام UPDATE برای تبلیغ مسیری به یک مقصد مشخص (مثلاً XY1Y2Y3Z) به همتای BGP استفاده می‌کند. پیام UPDATE همچنین می‌تواند برای پس گرفتن مسیرهایی که قبلاً تبلیغ شده بودند (یعنی برای اطلاع دادن به یک همتا که مسیری که قبلاً تبلیغ کرده بود دیگر معتبر نیست) استفاده شود.

KEEPALIVE

این پیام BGP برای اطلاع دادن به یک همتا استفاده می‌شود که فرستنده فعال است اما اطلاعات دیگری برای ارسال ندارد. همچنین به عنوان تأییدیه برای یک پیام OPEN دریافت شده عمل می‌کند.

NOTIFICATION

این پیام BGP برای اطلاع دادن به یک همتا استفاده می‌شود که خطایی شناسایی شده است (مثلاً در یک پیام BGP قبلاً ارسال شده) یا اینکه فرستنده قصد دارد جلسه BGP را ببندد.

سوال ۸:

الف) تفاوت اصلی بین iBGP و eBGP چیست؟ تفاوت نقش هر یک در BGP را توضیح دهید.

ب) چرا در BGP از TCP برای انتقال پیام‌ها استفاده می‌شود؟

ج) چرا BGP را یک پروتکل "بردار مسیر" (Path Vector) می‌نامند؟

د) چرا Hot Potato Routing در BGP می‌تواند باعث کاهش کارایی شود؟

ه) چگونه می‌توان از رسیدن یک مسیر خاص به یک AS خاص در BGP جلوگیری کرد؟

پاسخ:

الف) iBGP بین مسیریاب‌های یک AS است ولی eBGP بین ASهای متفاوت برقرار می‌شود. اهمیت eBGP در سیاست‌ها و خط‌مشی شبکه، اعلان مسیر و forward کردن بسته‌هاست، ولی در iBGP اطلاعات مسیریابی تنها برای مسیریاب‌های داخل یک AS بصورت یکسان منتشر می‌شود.

ب) می‌داتیم connection-oriented BGP است، برای همین استفاده از TCP قابلیت اطمینان، ترتیب، و کنترل جریان را فراهم می‌کند. این باعث می‌شود پیام‌های BGP گم یا دوباره ارسال نشوند.

ج) چون به‌جای ارسال فقط هزینه یا فاصله، لیستی از ASهایی را که مسیر باید از آن‌ها عبور کند (AS-PATH) دارد. این باعث کنترل بهتر مسیر و جلوگیری از حلقه می‌شود.

د) چون روتر ترافیک را از اولین دروازه ممکن بیرون می‌فرستد، بدون توجه به این‌که مسیر کلی به مقصد بهینه هست یا نه. این ممکن است باعث تأخیر بیشتر شود.

ه) با اعمال خط‌مشی روی مسیر خروجی (Export Policy) و عدم اعلام آن مسیر به آن AS. یا با دست‌کاری AS-PATH و فیلتر کردن آن در ورود به AS مقصد.

سوال ۹:

شبکه زیر را در نظر بگیرید. فرض کنید AS3 و AS2 از پروتکل OSPF برای مسیریابی درون دامنه‌ای (intra-domain) خود، و AS1 و AS4 از پروتکل RIP برای مسیریابی درون دامنه‌ای خود استفاده می‌کنند. همچنین فرض کنید از BGP (eBGP و iBGP) به عنوان پروتکل مسیریابی بین دامنه‌ای (inter-domain) استفاده می‌شود. در هر یک از موارد زیر پروتکل مورد نظر را با ذکر دلیل مشخص کنید.

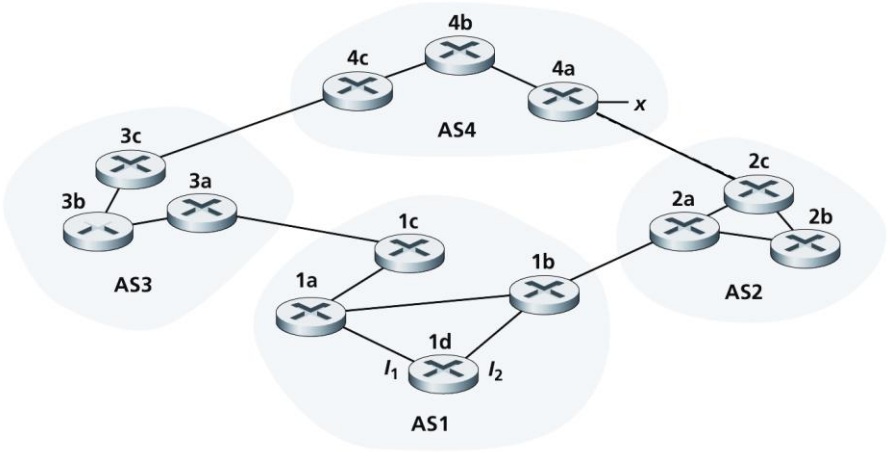
الف) مسیریاب 2c از طریق کدام پروتکل مسیریابی درباره پیشوند x مطلع می‌شود؟

ب) مسیریاب 2a از طریق کدام پروتکل مسیریابی درباره پیشوند x مطلع می‌شود؟

ج) مسیریاب 1b از طریق کدام پروتکل مسیریابی درباره پیشوند x مطلع می‌شود؟

د) مسیریاب 1a از طریق کدام پروتکل مسیریابی درباره پیشوند x مطلع می‌شود؟

ه) مسیریاب 4b از طریق کدام پروتکل مسیریابی درباره پیشوند x مطلع می‌شود؟



پاسخ:

الف) eBGP

ب) iBGP

ج) eBGP

د) iBGP

ه) RIP

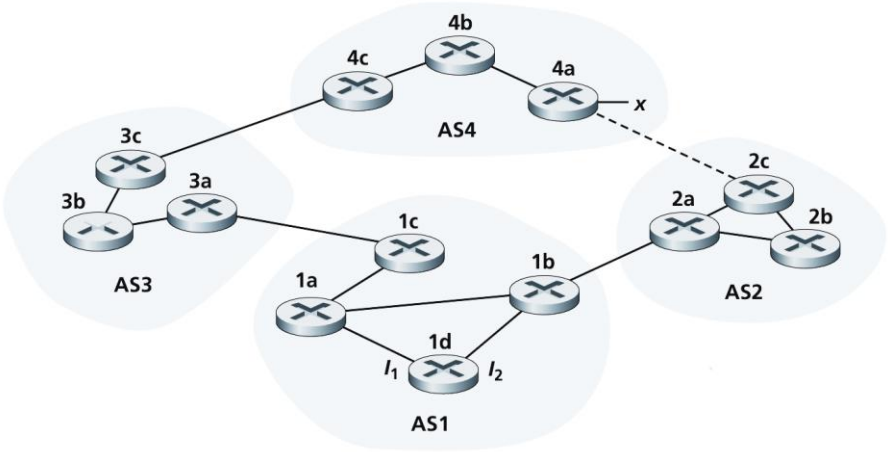
سوال ۱۰:

شبکه زیر را در نظر بگیرید. فرض کنید AS3 و AS2 از پروتکل OSPF برای مسیریابی درون دامنه‌ای (intra-domain) خود، و AS1 و AS4 از پروتکل RIP برای مسیریابی درون دامنه‌ای خود استفاده می‌کنند. همچنین فرض کنید از پروتکل BGP (eBGP و iBGP) به عنوان پروتکل‌های مسیریابی بین دامنه‌ای (inter-domain) استفاده می‌شود. می‌دانیم وقتی مسیریاب 1d درباره x مطلع می‌شود، یک ورودی (x, I) به جدول جلورانی خود اضافه می‌دهد.

الف) I برابر I_1 خواهد بود یا I_2 ؟ دلیل خود را در یک جمله توضیح دهید.

ب) اگر فرض کنیم بین AS2 و AS4 یک لینک فیزیکی وجود دارد (خط چین)، در این حالت که 1d دو راه برای دسترسی به x دارد مقدار I چه خواهد بود؟ دلیل خود را در یک جمله توضیح دهید.

ج) اگر فرض کنیم یک AS دیگر به نام AS5 به شبکه و در مسیر بین AS2 و AS4 وجود دارد که به 2c و 4a متصل است. در این حالت برای 1d مقدار I برابر I_1 می‌شود یا I_2؟ دلیل خود را در یک جمله توضیح دهید.



پاسخ:

الف) I_1 زیرا این ورودی مسیر با کمترین هزینه از 1d به روتر 1c را دارد.

ب) I_2 زیرا هر دو مسیر طول AS-PATH یکسان دارند اما I_2 مسیری را شروع می‌کند که NEXT-HOP روتر کمتری دارد.

ج) I_1 زیرا این ورودی، مسیری را طی می‌کند که کوتاه‌ترین طول AS-PATH را دارد.

سوال ۱۱:

کامپیوتری با آدرس آی‌پی 192.168.10.10 در یک شبکه خصوصی سعی دارد با استفاده از ابزار traceroute مسیر عبوری به سرویس‌دهنده‌ی با آدرس آی‌پی 8.8.8.8 را بررسی نماید. در جدول زیر، اطلاعات مربوط به زمان پاسخ‌دهی هر مسیریاب میانی برای ۵ گام اول آورده شده است:

گام (Hop)	آدرس آی‌پی مسیریاب	مقدار TTL ارسال‌شده	زمان پاسخ (ms)	نوع پاسخ ICMP دریافتی
1	192.168.10.1	1	3	Time Exceeded
2	10.0.0.1	2	5	Time Exceeded
3	172.16.0.1	3	8	Time Exceeded
4	203.0.113.1	4	14	Time Exceeded
5	8.8.8.8	5	21	Port Unreachable

الف) تفاوت نوع پیام‌های ICMP در پاسخ‌های مرحله ۱ تا ۴ با مرحله ۵ را توضیح دهید. چرا این تفاوت رخ داده است؟

ب) کل زمان رفت و برگشت (RTT) تا رسیدن به مقصد نهایی را محاسبه کنید. فرض کنید زمان رفت و برگشت هر Hop مستقل است و مجموع آنها RTT کل است.

ج) اگر اندازه هر پیام ICMP برابر ۶۴ بایت باشد و ابزار traceroute برای هر Hop سه بار این بسته را ارسال کند، مجموع کل داده‌هایهٔ ICMP ارسالی برای این مسیر چقدر است؟ (برحسب بایت و بیت)

د) اگر نرخ تأخیر در شبکه به صورت خطی افزایش یابد، مقدار تخمینی تأخیر در Hop 6 چقدر خواهد بود؟ (فرض کنید تأخیر افزایشی از Hop به Hop به صورت یکنواخت است.)

ه) با توجه به اینکه پاسخ‌های Time Exceeded توسط کدام تجهیزات ایجاد می‌شوند و چه فیلدهایی از بسته را تغییر می‌دهند، نقش TTL در عملکرد traceroute را دقیقاً توضیح دهید.

پاسخ:

الف) در چهار گام اول پاسخ ICMP از نوع Time Exceeded – Type 11, Code 0 است، چون هر روتر پس از کم کردن TTL بسته و رسیدن آن به صفر، بسته را دور انداخته و پیام Time Exceeded برمی‌گرداند. در گام پنجم بسته به مقصد واقعی (۸/۸/۸/۸) رسیده و چون Traceroute از پورت UDP بالای ۳۳۴۳۴ استفاده می‌کند و سرویسی در آن پورت گوش نمی‌دهد، میزبان مقصد پیام Destination Unreachable – Port Unreachable (Type 3, Code 3) می‌فرستد. بنابراین تفاوت پیام‌ها ناشی از این است که در گام‌های ۱-۴ TTL صفر می‌شود ولی در گام ۵ بسته تحویل مقصد می‌شود و مقصد است که نبودِ سرویس را اعلام می‌کند.

ب) کل RTT تا مقصد (جمع RTTهای مستقل هر Hop)

$$3\ \text{ms} + 5\ \text{ms} + 8\ \text{ms} + 14\ \text{ms} + 21\ \text{ms} = 51\ \text{m}$$

ج) تعداد بسته‌های ICMP:

$$3 \times 5\ \text{hop} = 15\ \text{packets}$$
$$15 \times 64 = 960\ \text{bytes} = 7680\ \text{bits}$$

د) افزایش میانگین تأخیر بینHop ها:

$$(2 + 3 + 6 + 7)/4 = 4.5\ \text{ms}$$

(خطی مفروض) پس زمان پاسخ Hop 6 :

$$21 + 4.5 = 25.5\ \text{ms}$$

ه) Traceroute مقدار TTL بسته نخست را ۱ می‌گذارد. هر روتر هنگام عبور، TTL را ۱ واحد کم می‌کند؛ اگر TTL به صفر برسد، روتر بسته را دور می‌اندازد و یک ICMP Time Exceeded برای مبدأ می‌فرستد که آدرس همان روتر را آشکار می‌کند. با افزایش تدریجی TTL (۱, ۲, ۳, ...) هر بار روتر دورتر پاسخ می‌دهد تا سرانجام خود مقصد با ICMP Port Unreachable پاسخ دهد. به این ترتیب، فیلد TTL به طور مستقیم تعداد گام‌های قابل طی شدن را محدود می‌کند و مبنای کشف مسیر در Traceroute است.

سوال ۱۲:

فرض کنید یک مدیر شبکه در یک سازمان متوسط با حدود ۱۰۰ دستگاه متصل، مسئول طراحی و پیاده‌سازی سیستم مدیریت شبکه است و تصمیم دارد از مدل SNMP (Simple Network Management Protocol) برای پایش (monitoring) و کنترل تجهیزات شبکه استفاده کنید.

الف) مدل SNMP را با توجه به نقش‌های زیر توضیح دهید:

- مدیر (Manager)
- عامل (Agent)
- پایگاه داده مدیریتی (MIB (Management Information Base))
- پیام تله (Trap message)

ب) چه تفاوتی بین عملیات‌های Get، Set و Trap در SNMP وجود دارد؟ نقش هرکدام را در پایش شبکه توضیح دهید.

ج) اگر یکی از سوییچ‌های شبکه دچار قطعی ناگهانی شود، چگونه این اتفاق در چارچوب SNMP به مدیر شبکه اطلاع داده می‌شود؟

د) چرا پروتکل SNMP برای ارسال پیام‌هایش از UDP به جای TCP استفاده می‌کند. این انتخاب چه مزایا و معایبی دارد؟

پاسخ:

الف)

Manager (مدیر): نرم‌افزاری متمرکز روی ایستگاه مدیریت شبکه (NMS) که پایگاه داده را می‌خواند، متغیرها را Poll می‌کند و به عامل‌ها فرمان می‌دهد.

Agent (عامل): فرایندی روی هر تجهیز (سوئیچ، روتر، سرور) که اطلاعات محلی را گردآوری کرده و درخواست‌های SNMP را پاسخ می‌دهد.

MIB (Management Information Base): پایگاه داده سلسله‌مراتبی متغیرهای قابل مدیریت؛ هر گره دارای OID یکتاست.

Trap message: پیامی غیرهمزمان است که Agent هنگام بروز رویداد (مانند قطع لینک) بی‌درنگ برای Manager می‌فرستد تا اخطار دهد.

ب) Set پیامی است که Manager می‌فرستد تا مقدار یک MIB-variable را در Agent تغییر دهد؛ کاربرد آن کنترل و پیکربندی است.Trap پیامی است که Agent به‌طور خودکار و بدون درخواست مدیر می‌فرستد؛ نقش آن هشدار و مانیتورینگ رویدادهاست.

ج) وقتی سوئیچ مشکلی پیدا کند (مثلاً پورت از کار بیفتد) عاملِ SNMP روی سوئیچ یک Trap یا Inform با OID مربوط به رویداد (مثل linkDown) برای آدرس مدیر می‌فرستد. مدیر با دریافت این پیام بلافاصله هشدار می‌دهد و در صورت نیاز متغیرهای بیشتر را با پیام Get درخواست می‌کند.

د) SNMP روی UDP کار می‌کند زیرا UDP بدون اتصال، کم‌هزینه و ساده است؛ پیاده‌سازی در تجهیزات کوچک آسان و سربار حافظه/پردازش اندک است. از دست رفتن بسته‌ها معمولاً مشکل بزرگی نیست، چون برای Pollهای تناوبی، مدیر می‌تواند بسته را دوباره بفرستد و برای Trapها، برخی نسخه‌ها (SNMPv2c Inform, SNMPv3) مکانیزم تأیید دارند.

مزایا: سربار کمتر، پیاده‌سازی ساده، عدم نیاز به نگهداری وضعیت اتصال.

معایب: عدم تضمین تحویل، ترتیب یا یکتایی بسته‌ها؛ ممکن است پیام‌های حیاتی گم شوند مگر با مکانیزم تأیید یا تکرار در لایه کاربرد.