فصل چهارم

لایه شبکه

انجمن فناوری اطلاعات
INFORMATION TECHNOLOGY FORUM
www.it98.ir

کاملترین مجموعه نمونه سوالات بهمراه پاسخنامه تستی و تشریحی، جزوه، اسلاید، حل تمرین، گزارش آزمایشگاه و کارآموزی، پروژه و... در سایت:
www.it98.ir
مرجع دانشجویان رشته کامپیوتر دانشگاه پیام نور

در فصل انتقال دیدیم که این لایه انواع مختلفی سرویس ارتباطی پروسس به پروسس با استفاده از سرویس ارتباطی میزبان به میزبان لایه شبکه فراهم می آورد.ویاد گرفتیم که لایه انتقال هیچگونه اطلاعی از نحوه انجام سرویس توسط لایه شبکه ندارد در این فصل یاد خواهیم گرفت که این سرویس ارتباطی میزبان به میزبان چگونه پیاده سازی و اجرا می شود.در این فصل بر خلاف لایه انتقال خواهیم دید که بخشی از لایه شبکه در هر ماشین میزبان وهر روتر بین راه در شبکه وجوددارد. بهمین علت (که این لایه در تمام شبکه پخش شده است)دشوارترین وجالبترین پروتکل در مجموعه پروتکل ها می باشد. این فصل را با مروری بر لایه شبکه و سرویسهایی را که می تواند فراهم آورد شروع می نماییم سپس دو روش اصلی و ساخت یافته تحویل بسته لایه شبکه را بررسی می نماییم که شامل «مدل مدار مجازی» و«مدل دیتا گرام» می باشد.تمایز بین دو مفهوم «هدایت کردن» (forwarding) و «مسیر یابی» (routing) را خواهیم دید.

فورواردینگ به عمل انتقال بسته به لینک ورودی و ارسال به لینک مناسب خروجی در روتر گفته می شود در حالیکه مسیر یابی شامل عمل تمام روترها برای ارسال بسته از مبدأ به مقصد گفته می شود .سپس معماری و سازماندهی درون روتر را بررسی خواهیم نمود. پروتکل مسیر یابی اینترنت ip را بررسی خواهیم نمود ipv6 و ipv4 سپس پروتکل ترجمه آدرس شبکه (nrt) را خواهیم دید و پروتکل icmp

۴,۱مقدمه

شکل ۴,۱ شبکه ای با دو میزبان H1و H2 و تعدادی روتر در بین راه (مسیر) را نشان می دهد. H1 فرستنده و H2 گیرنده باشد.

www.it98.ir

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

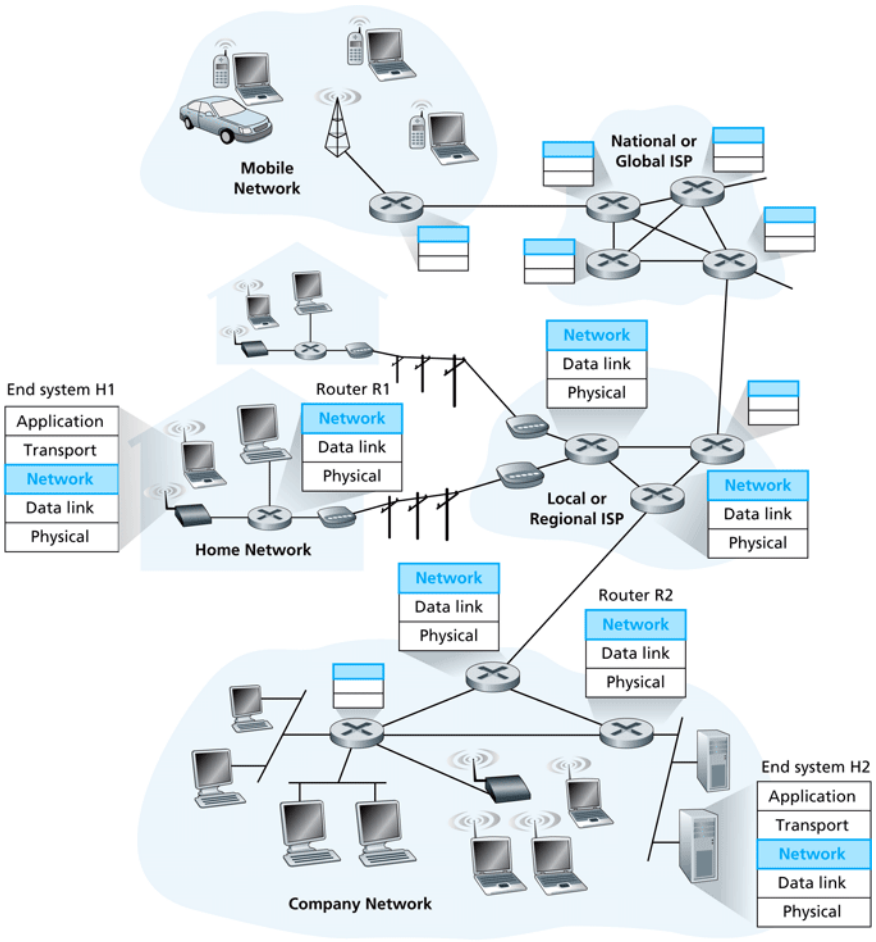


Figure 4.1 ♦ The network layer

لایه شبکه درH1سگمنت را از لایه انتقال در H1تحویل گرفته، آن را بسته بندی کرده و دیتا گرام ایجاد می نماید(همان بسته یا Packet) و به نزدیکترین مسیریاب ، R1 ارسال می دارد.

در گیرنده نیز در H2 لایه شبکه آن بسته را از نزدیکترین مسیریاب به خود یعنی R2 دریافت می دارد،سگمنت را از درون بسته جداسازی و استخراج کرده و آن را به لایه بالای خود (لایه انتقالدر h2تحویل می دهد. وظیفه ی اصلی روتر هدایت دیتای رام ها از لیک ورودیشان به لینک خروجیشان می باشد همان طور که در شکل ۴,۱ هم دیده میشود مجموعه پروتکلی روتر تا لایه سوم بیشتر نیست و معنی آن این است که برروی روترها برنامه های کاربردی و انتقالی اجرا نمی شوند.

۴,۱,۱ هدایت به جلو و مسیر یابی

نقش لایه شبکه در ظاهر بسیار ساده و فریبنده می نمایاند ، انتقال بسته ها از میزبان فرستنده به میزبان گیرنده برای انجام اینکار دو کارکرد اصلی لایه شبکه قابل شناسایی است.

*هدایت به جلو: زمانی یک بسته ای در لینک ورودی مسیریاب وارد میشود روتر باستی بسته را به مسیر خروجی مناسب انتقال دهد .

*مسیریابی : لایه شبکه بایستی مسیر را راهی را که بسته بایستی از فرستنده به گیرنده جریان می یابد را نماید .

الگوریتمهایی که این مسیرها را بدست می دهند. به نام الگوریتم های مسیر یابی معروف هستند.

این الگوریتم مسیر یابی بطور مثال تعیین می کند که بسته چگونه از h1 به h2حرکت نماید.

هر روزی دارای یک جدول هدایت به جلو می باشد.(forwarding table) هر روتر با بررسی فیلدی درون بخش هدر بسته ورودی و با اندیس کردن آن در جدول هدایت به جلو مسیر خروجی را بدست می آورد.

شکل۴,۲ این موضوع را نشان می دهد.

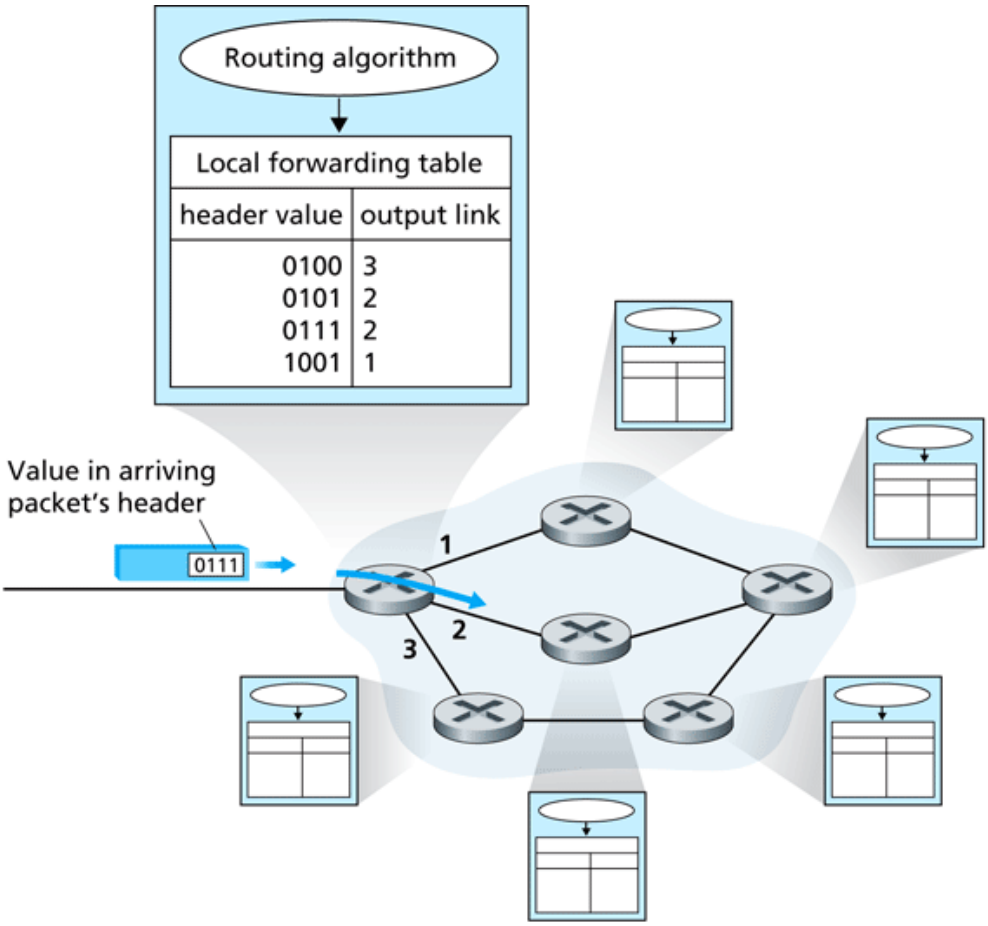


Figure 4.2 ♦ Routing algorithms determine values in forwarding tables.

مقدار این فیلد درون هدر بسته را الگوریتم مسیر یابی محاسبه و تعیین می نماید.الگوریتم های مسیر یابی می تواند بصورت متمرکز یا غیر متمرکز باشند.

همچنین ما از واژه سوئیچ بسته (packetsueetch) به عنوان دستگاهی که بسته ای را از لینک ورودی دریافت و بر اساس مقداری درون فیلد هدر به لینک خروجی می فرستد ، استفاده می نماییم.

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

برخی سوئیچ های بسته تحت عنوان سوئیچ های لایه پیوند داده میباشند که کارکرد آنها براساس فیلدی درون لایه پیوند داده می باشند . (ونه بسته لایه سوم!) در این فصل ، روتر را یک سوئیچ بسته مورد استفاده قرار میدهیم .

برقراری ارتباط (connection setup)

در برخی از انواع شبکه های کامپیوتری عمل برقراری ارتباط سومین کارکرد مسیر یابها باشد (اولین و دومین آن هدایت به جلو ومسیر یاب بود) همانطوریکه در بخش tcp دیدیم. عمل دست تکانی سه مرحله ای برای ارتباط بین دو ماشین نهایی لازم بود. در لایه شبکه هم در برخی از شبکه ها (از جمله ATM و fram.relay) ونه اینترنت، روزها نیاز به برقراری ارتباط به منظور تبادل اطلاعات مورد نظر دارند.

۴,۱,۲ مدلهای سرویس شبکه

قبل از ادامه بحث اجازه دهید نگاهی به انواع سرویس هایی که لایه شبکه می تواند ارائه دهد داشته باشیم. زمانیکه لایه انتقال در ماشین میزبان فرستنده بسته ای را برای ارسال به لایه شبکه تحویل می دهد. آیا لایه انتقال برای تحویل بسته به مقصد باید بر روی لایه شبکه حساب کند یا خیر؟ آیا زمانیکه چندین بسته در فرستنده ارسال می شود ، آیا در مقصد به همان ترتیب دریافت می شوند یا خیر؟ آیا فاصله زمانی بین ارسال دو بسته در فرستنده برابر با فاصله زمانی دریافت دو بسته در گیرنده است؟

آیا شبکه هیچگونه فیدبکی در مورد وقوع ازدحام در شبکه بر می گرداند؟

جواب به این سوالات تعیین کنند. مدل سرویسی ارائه شده توسط لایه شبکه می باشد اجازه دهید برخی از سرویس های ممکن را بررسی نماییم.

*سرویس تحویل گارانتی شده : تضمین میکند که بسته در نهایت به مقصد خواهد رسید.

*سرویس تحویل گارانتی شده با تأخیر محدود: نه تنها تحویل بسته را تضمین می کند. بلکه آنرا زیر زمان مشخصی (مثلاًms ۱۰۰) تحویل می دهد. سرویسهای فوق برای تک تک بسته ها قابل اجراء است اما سرویس های زیر می تواند بر روی جریانی از بسته ها انجام شود:

*تحویل مرتب بسته ها: بسته ها به همان ترتیب که ارسال می شوند درگیرند هم تحویل داده میشود.

www.it98.ir

*حداقل پهنای باند تضمین شده: یک سرعت مشخصی را (مثلاً 1 mbs) برای ارسال داده از فرستنده به گیرنده تضمین می کند. (و همچنین بسته ها زیر تأخیرمشخص تحویل داده خواهد شد.)

*حداکثرلرزش تضمین شده : این سرویس تضمین میکند که مقدار فاصله زمان ارسال دو بسته در فرستنده معادل مقدار فاصله زمانی آن دو در گیرنده خواهد بود(و یا این زمان از یک حداکثری بیشتر نخواهد شد)

*سرویس های امنیتی: با داشتن یک کلید امنیتی مشخص برای ماشین میزبان ارسال کننده و دریافت کننده ، فرستنده می تواند داده ها را رمز کرده و مقدار در مقصد داده ها از رمز در آیند. موارد بالا فقط بخشی از سرویس های ممکن است و تعداد آنها می تواند بیشمار باشد. لایه شبکه در اینترنت تنها یک سرویس را فراهم می آوردتحت عنوان "مراکز تلاش" (best effort) و می تواند به این معنی باشد که در مجموع هیچ سرویسی را فراهم نمی آورد .

جدول ۴,۱ مد لهای سرویس مختلف برای اینترنت، ATM و...

Network Architecture	Service Model	Bandwidth Guarantee	No-Loss Guarantee	Ordering	Timing	Congestion Indication
Internet	Best Effort	None	None	Any order possible	Not maintained	None
ATM	CBR	Guaranteed constant rate	Yes	In order	Maintained	Congestion will not occur
ATM	ABR	Guaranteed minimum	None	In order	Not maintained	Congestion indication provided

Table 4.1 ♦ Internet, ATM CBR, and ATM ABR service models

معماریهای دیگر شبکه نظیر ATM ،مدلهای سرویس متنوعی را فراهم آورده اند.که بحث آنها ورای این کتاب است. هدف ما در اینجا این است که نشان دهیم غیر از سرویس "حداکثر تلاش" سرویسهای دیگری نیز موجود هستند.

*سرویس شبکه ATM با نرخ ارسال ثابت (CBR)

اولین سرویس ATM بود که منعکس کننده علاقه مندی شرکتهای تلفنی برای ارسال بیدرنگ ، ترافیک صدا و تصویر با نرخ سرعت ثابت می باشد. و هدف آن بطور خلاصه فراهم آوردن جریان بسته ها (در ادبیات ATM به آنها سلول گفته می شود) در یک خط لوله مجازی که دارای پهنای باند انتقال اختصاصی و ثابتی در طول شبکه از فرستنده تا گیرنده باشد سرویسهای تضمین شده ای در مورد تأخیر ولرزش فراهم می آورد.

سرویس شبکه ATM با نرخ بیت در دسترس (ABR)

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

همانند اینترنت که سرویس مراکز تلاش را ارائه میدهد .ATM هم سرویس کمی بهتری تحت عنوان "کمی بهتر از حداکثر تلاش" ارائه می هد. در این مدل ممکن است سلولها (نام بسته ها در ATM) از دست بروند اما ترتیب آنها در ارسال و دریافت حفظ می شود.یک حداقل نرخ انتقال تضمین میشود(MCR) .اگر منابع کافی موجود باشد می تواند سرعت بیشتری نسبت به MCR را هم فراهم آورد. و میتواند در مورد وجود ازدحام به فرستنده هم فید بک ارسال کند تا بتواند به حداکثر سرعت مجاز برسد.

۴,۲ شبکه های مدار مجازی (VC) و دیتا گرام (VERTUAL CIRCUIT AND DATAGRUM NETWORKS)

همانطور که در فصل سوم دیدیم ، لایه انتقال می تواند سرویس اتصالگر ویا غیر اتصالگر ارائه دهد.بطور مثال لایه انتقال در اینترنت TCP از نوع اتصالگر و UDP سرویس غیر اتصالگر ارائه میداد.به همین روش هم ، لایه شبکه می تواند چنین سرویسهایی را ارائه دهد.اگر چه این سرویس در لایه شبکه میتوانند به موازات سرویسهای مشابه در لایه انتقال باشند. اما تفاوتهای مهمی با هم دارند. درلایه انتقال این سرویس ها پروسس به پروسس بودند در حالیکه در لایه شبکه این سرویسها میزبان به میزبان می باشند.در بیشتر معماریهای شبکه لایه شبکه یا سرویس اتصالگر ارائه می دهند ویا غیر اتصالگر ونه هردو. شبکه های کامپیوتری که سرویس اتصالی را در لایه شبکه فراهم می آورند به نام " شبکه های مدار مجازی (VC) معروف هستند وآنهائیکه سرویس غیر اتصالی را ارائه می دهند (در لایه شبکه) به عنوان "شبکه دیتاگرام" معروف هستند.

پیاده سازی سرویس اتصالگر در لایه انتقال با سرویس اتصالی در لایه شبکه کاملاً متفاوت هستند .زیرا سرویس اتصالگرای لایه انتقال در "لبه شبکه" است ولی سرویس ا تصالی لایه شبکه در" هسته شبکه" می باشد.

۴,۲,۱ شبکه های مدار مجازی

قبلاً دیده بودیم که اینترنت یک شبکه دیتا گرام است .اما روشهای دیگری نیز بعنوان معماری شبکه موجود می باشد.از جمله آن atm است و همچنین(Farm Relay) که بصورت مدار مجازی میباشند.(VC)

یک (VC) شامل

۱)مسیری است (Path)(شامل یک سری لینکها وروزها) بین مبدأ و مقصد

۲) شماره VC است. یک شماره برای هر لینک در طول مسیر

www.it98.ir

۳) ورودیهایی در" جدول هدایت به جلو " در هر روز در طول مسیر بسته ای که متعلق به یک مدار مجازی باشد در هدر آن شماره VCقراردارد و از آنجاییکه بسته از لینکهای متعددی عبور میکند هر مسیریاب موظف است شماره VC جدید برای بسته را بروز نماید (با عبور از روتر)

به شکل ۴,۳ دقت کنید،فرض کنید که بین A و B مدار مجازی باشد A-R1-R1-B برقرارشده باشد .شماره های VC عبارتند از ۱۲-۲۲-۳۲ برای سه لینک موجود .زمانیکه بسته ای Aرا ترک می کند شماره ۱۲ بخود می گیـرد و زمانیکه به R1میرسد.شماره جدید آن ۲۲ خواهد شد.و درنهایت شماره ۳۲ را خواهد گرفت. اینکه چگونه روزها شماره جدید را انتخاب می نمایند ، با توجه به اینست که در هر روز یک جدول هدایت به جلو موجود است .برای مثـال بـرای روتر R1 این جدو ل بصورت زیر است:

جدول هدایت به جلو برای روتر R1

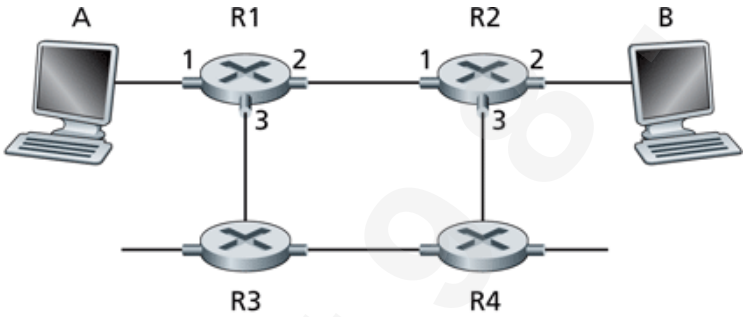


Figure 4.3 ♦ A simple virtual circuit network

Fragment	Bytes	ID	Offset	Flag
1st fragment	1,480 bytes in the data field of the IP datagram	identification = 777	offset = 0 (meaning the data should be inserted beginning at byte 0)	flag = 1 (meaning there is more)
2nd fragment	1,480 bytes of data	identification = 777	offset = 185 (meaning the data should be inserted beginning at byte 1,480. Note that 185 · 8 = 1,480)	flag = 1 (meaning there is more)
3rd fragment	1,020 bytes (= 3,980–1,480–1,480) of data	identification = 777	offset = 370 (meaning the data should be inserted beginning at byte 2,960. Note that 370 · 8 = 2,960)	flag = 0 (meaning this is the last fragment)

Table 4.2 ♦ IP fragments

برای هر مدارمجازی سه فاز قابل شناسایی است.

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

*برپایی VC: در این فاز لایه انتقال در ارسال کننده با لایه شبکه خودش تماس گرفته و آدرس گیرنده را به آن اعلام میدارد و منتظر برپایی VC توسط لایه شبکه میشود. لایه شبکه مسیر بین فرستنده و گیرنده را تعیین کرده و (که شامل لینکها و روزهایی در مسیر را و همچنین شماره های VCمیباشد) در نهایت لایه شبکه یک ورودی به جدول هدایت به جلو در هر روتر بین راه اضافه می نماید. در حین فاز برپایی ، لایه شبکه ممکن است مشغول رزرو منابع (پهنای باند و...) در طول مسیر VCباشد.

*فاز انتقال داده ، مدار مجازی برقرار شده است و می توانند در طول VC جریان یابند.

*فاز قطع VC: زمانی انجام میشود که فرستنده (ویا دریافت کننده) به لایه شبکه اطلاع می دهند که مایل به پایان دادن VC هستند.لایه شبکه نیز به طور معمول به طرف دیگر برای قطع ارتباط اطلاع دارد. وسپس با حذف ورودیهای مسیر یابها این VC دیگر وجود نخواهد داشت.

شکل ۴,۱ برقراری مدار مجازی

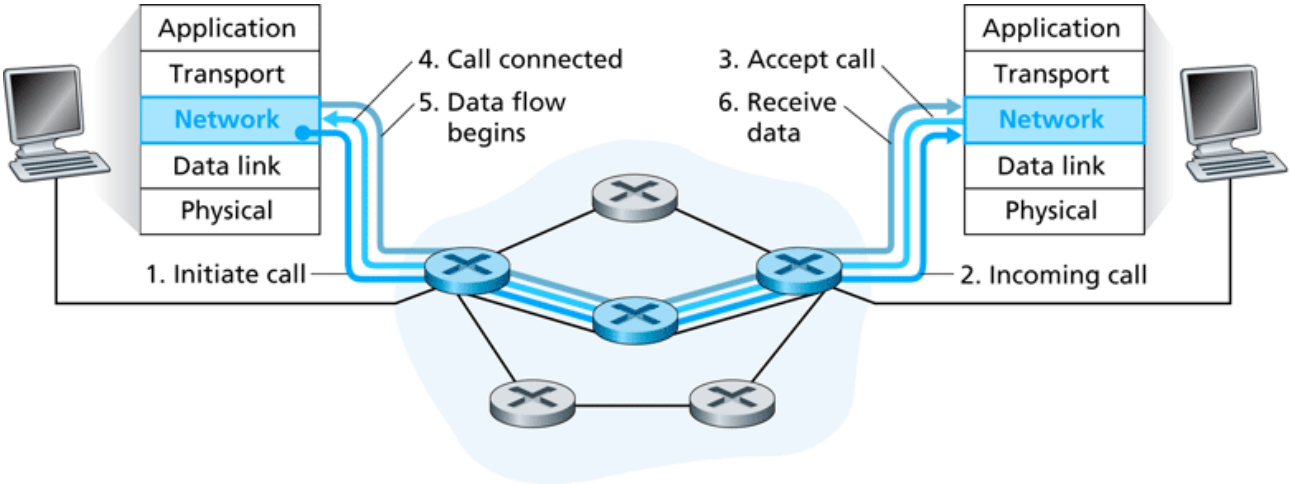


Figure 4.4 ♦ Virtual-circuit setup

۴,۲,۲ شبکه های دیتا گرام

در یک شبکه دیتا گرام ، هر زمان که یک سیستم پایانی بخواهد بخواهد بسته ای را ارسال نماید .بسته را با آدرس مقصد تمبرکرد. وب سته را بسوی شبکه ارسال می دارد. همانطوریکه در شکل ۴,۱ دیده می شود، هیچ نیازی به عمل برپایی VC نیست بسته ای که از مبدأ بسوی مقصد انتقال داده می شوداز میان تعدادی روتر عبور کرده و هر روز با بررسی آدرس مقصد بسته آن بسته را به جلو هدایت می نماید.

www.it98.ir

فرض کنیم که آدرس ها با طول ثابت BIT ۳۲ باشند .در بدترین حالت هر جدول هدایت به جلو در روتر ها بایستی ۴میلیارد ورودی برای هر آدرس باشد وفرض کنیم که هر روتر دارای ۴ لینک باشد(۰تا ۳) جدول هدایت به جلو می تواند بصورت زیر باشد.همانطوریکه از شکل مشخص است نیازی نیست که در جدول هدایت روترها ۴ میلیارد ورودی داشته باشیم .میتوان آنها را بصورت زیر خلاصه و ساده نمود:

جدول خلاصه شده :

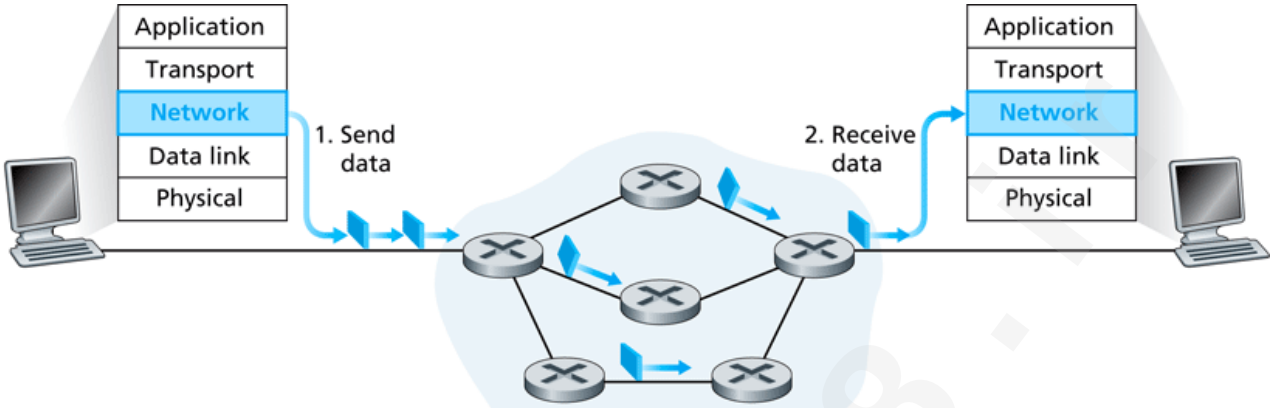


Figure 4.5 ♦ Datagram network

Destination Address Range	Link Interface
11001000 00010111 00010000 00000000 through 11001000 00010111 00010111 11111111	0
11001000 00010111 00011000 00000000 through 11001000 00010111 00011000 11111111	1
11001000 00010111 00011001 00000000 through 11001000 00010111 00011111 11111111	2
otherwise	3

در این حالت روتر با تطبیق پیشوند آدرس های مقصد با ورودیهای جدول اقدام به هدایت می نماید روترها در این روش هیچ نوع اطلاعاتی راجع به وضعیت ارتباطات نگهداری نمی کنند. (همانطور که در مداری مجازی انجام میشد) بلکه نیاز دارند که اطلاعات جدول هدایت را در خود داشته باشند.

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

۴,۳ نگاهی به درون روتر

بعد از مرور سرویسهای لایه شبکه بیایید نگاهی به انتقال واقعی بسته درون روتر از لینک ورودی به لینک خروجی آن باشیم. (عمل هدایت به جلو)

در این بخش اشاره می کنیم که عمل هدایت به جلو با عمل "سوئیچینگ" به یک معنی خواهند بود.در یک نگاه سطح بالا همانطوریکه در شکل ۴,۶ آمده است چهار مولفه در یک روتر قابل شناسایی است.

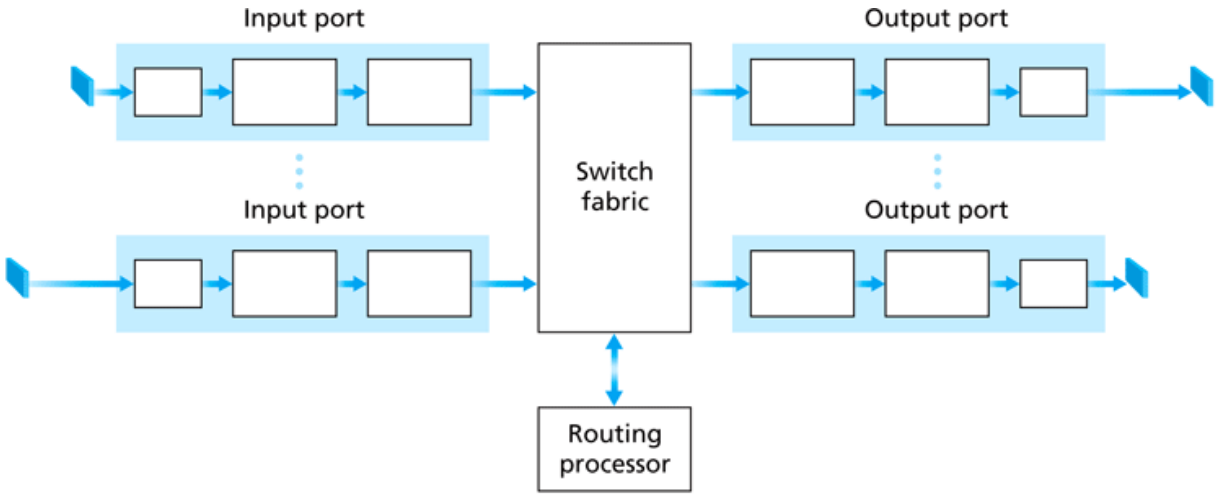


Figure 4.6 ♦ Router architecture

۱) پورت های ورودی -کارکردهای مختلفی دارد. ارتباط فیزیکی با لینک فیزیکی ورودی را برقرار مینماید. (اولین بخش در پورت ورودی)

همچنین کارکرد لایه پیوند داده را هم انجام مکیدهد.(توسط بخش میانی در این قسمت و همچنین توسط پورت خروجی) در ضمن کارکرد لوک آپ وهدایت را هم انجام میدهد. (باکس سوم در پورت ورودی)

*بخش سوئیچینگ : ارتباط بین پورتهای ورودی را به پورتهای خروجی انجام میدهد.

*پورتهای خروجی: بسته های خروجی که هدایت شده اند را نگهداری مینماید وسپس به لینک بعدی ارسال میدارد .این بخش هم شامل قسمتهای لایه پیوند داده و اینتر فیس های لایه فیزیکی می باشد. زمانیکه لینکی دو طرفه باشد ، معمولاً بصورت خروجی با پورت ورودی روی یک کارت خط ترکیب می شوند.

*پردازشگر مسیریابی: وظیفه اجرای پروتکلهای مسیریابی را بر عهده دارد و حاوی اطلاعات مسیریابی و جداول هدایت به جلو می باشد .همچنین وظایف مدیریت شبکه را نیز انجام می دهد.

www.it98.ir

بسته های ورودی در بخش صف پورت ورودی وبسته های خروجی هم در صف پورتهای خروجی بافر می شوند. اگـر سرعت ورود داده ها زیاد باشد ویا سرعت ارسال بسته ها کم باشد صف ها پر شده و در نهایت از دست رفتن بسته ها را خواهیم داشت.

۴,۴) پروتکل اینترنت (IP) : هدایت به جلو و آدرس دهی در اینترنت

دو نسخه از پروتکل IP وجود دارد. IPV4 که بطور گسترده ای در حال کاربرد است و نسخه ی IPV6 که بعنـوان جایگزین اولی پیشنهاد شده است.

همانطوریکه در شکل ۴,۱۲ ملاحظه میشود .IP شامل سه مولفه مهم است. اولین مولفه پروتکل IP است. مولفه دوم مولفه مسیر یابی است که مسیر هدایت بسته از مبدأ به مقصد را تعیین می کند .مولفه آخر هم مولفه گزارش خطـا در ارسال بسته ها می باشد.

شکل ۴,۱۲ نگاهی به درون لایه شبکه اینترنت

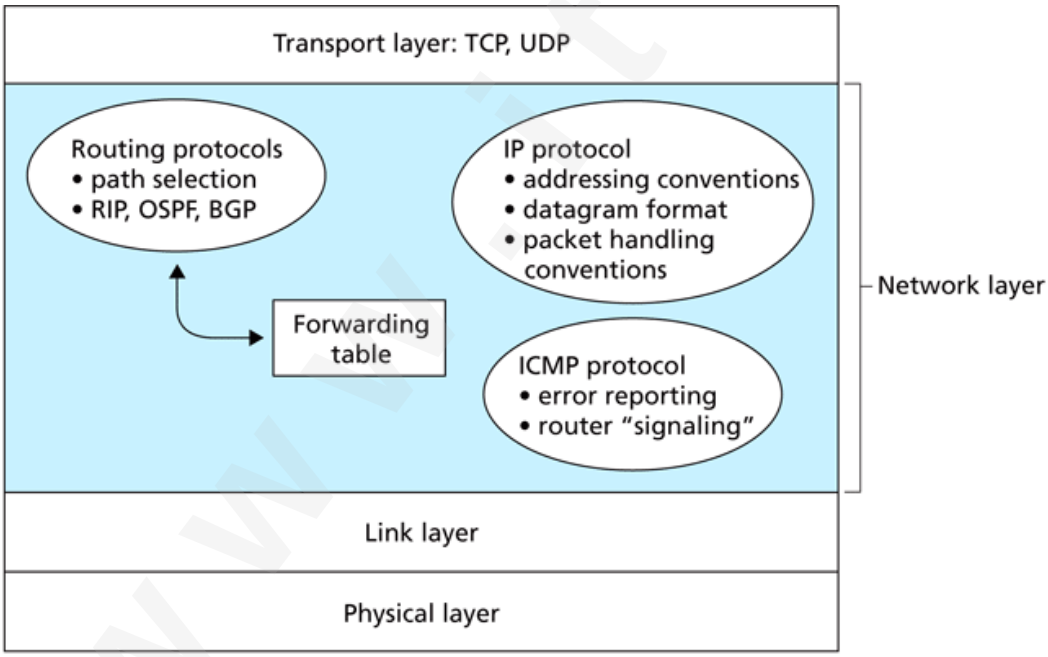


Figure 4.12 ♦ A look inside the Internet's network layer

۴,۴,۱ قالب دیتا گرام : مجدداً اشاره می کنیم که نام بسته در لایه شبکه دیتا گرام می باشد .

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

در شکل زیر قالب دیتا گرام در نسخه IPV4 نشان داده شده است.

قالب دیتا گرام IPV4

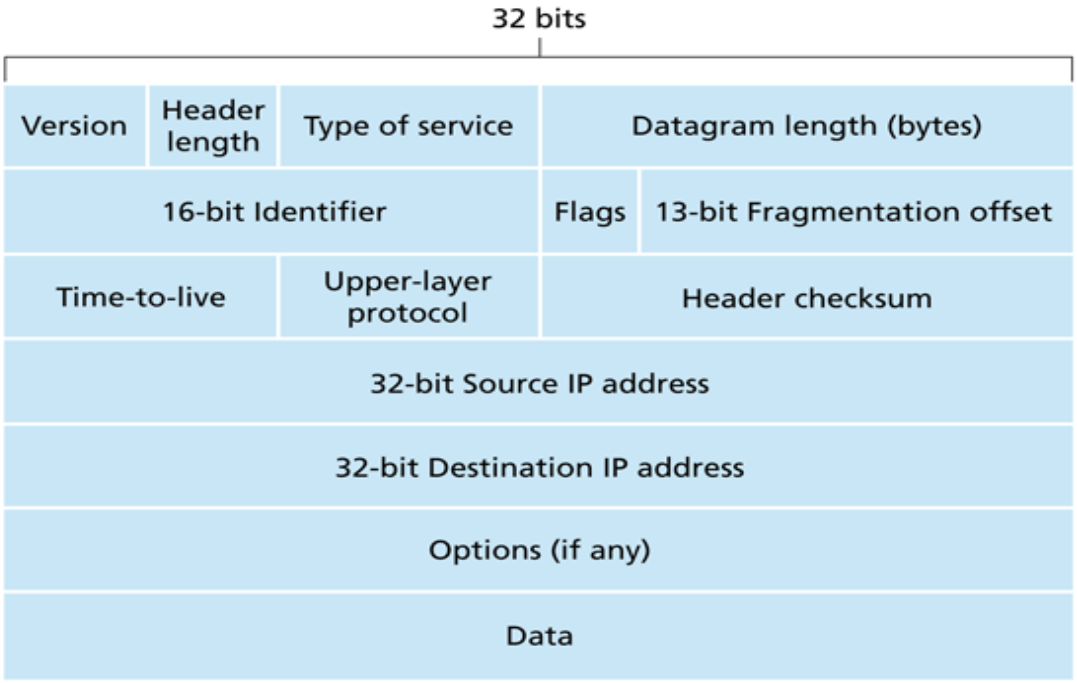


Figure 4.13 ♦ IPv4 datagram format

*شکستن دیتا گرام IP

در فصل ۵ خواهیم دید که تمام پروتکلهای لایه پیوند داده نمی توانند بسته های با همان اندازه پروتکل لایه شبکه را حل نمایند.

برخی پروتکلها می توانند دیتاگرام های بزرگ را حمل کنند در حالیکه پروتکلهای دیگر بسته های کوچک را حمل می کنند.

برای مثال در فریم اترنت فقط می توان حداکثر ۱۵۰۰ بایت داد. قرارداد MTU به حداکثر واحد انتقال که لایه پیوند داده شده می تواند ارسال کند گفته میشود. از آنجاییکه هر دیتاگرام IP بایستی در یک فریم لایه پیوند داده کپسوله شود بنابراین این MTU طول دیتا گرام IP را محدود می نماید.

این محدودیت طول دیتا گرام IP مشکل خاصی نیست بلکه مشکل زمانی است که هر لینک در طول مسیر از فرستنده تا گیرنده ممکن است از پروتکل های مختلف لایه پیوند داده استفاده کند و هر کدام از آنها MTU متفاوتی خواهند داشت.

www.it98.ir

فرض کنید که شما یک روتر هستید و به لینکهای متعددی متصل هستید ، و هر کدام MTU متفاوتی دارند. وشما یک دیتا گرام IP دریافت میکنید و متوجه می شود که MTU برای لینک خروجی کوچکتر از طول دیتا گرام است . چکار باید کرد؟ راه حل شکستن دیتا گرام به اندازه های کوچکتر وکبود کردن هر کدام در یک فریم لایه پیوند داده و ارسال فریم ها به سمت مقصد . به هر کدام از دیتا گرامها یک قطعه (سگمنت) گفته می شود. سگمنت ها بایستی قبل از تحویل به لایه انتقال در مقصد ، بازسازی شده و دیتا گرام اولیه را تشکیل دهند. زیرا پروتکل های TCPو UDP انتظار دیتا گرام های ناقص و شکسته را ندارند .

شکل ۴,۱۴ وجدول ۴,۲ این عملیات را نمایش می دهند.

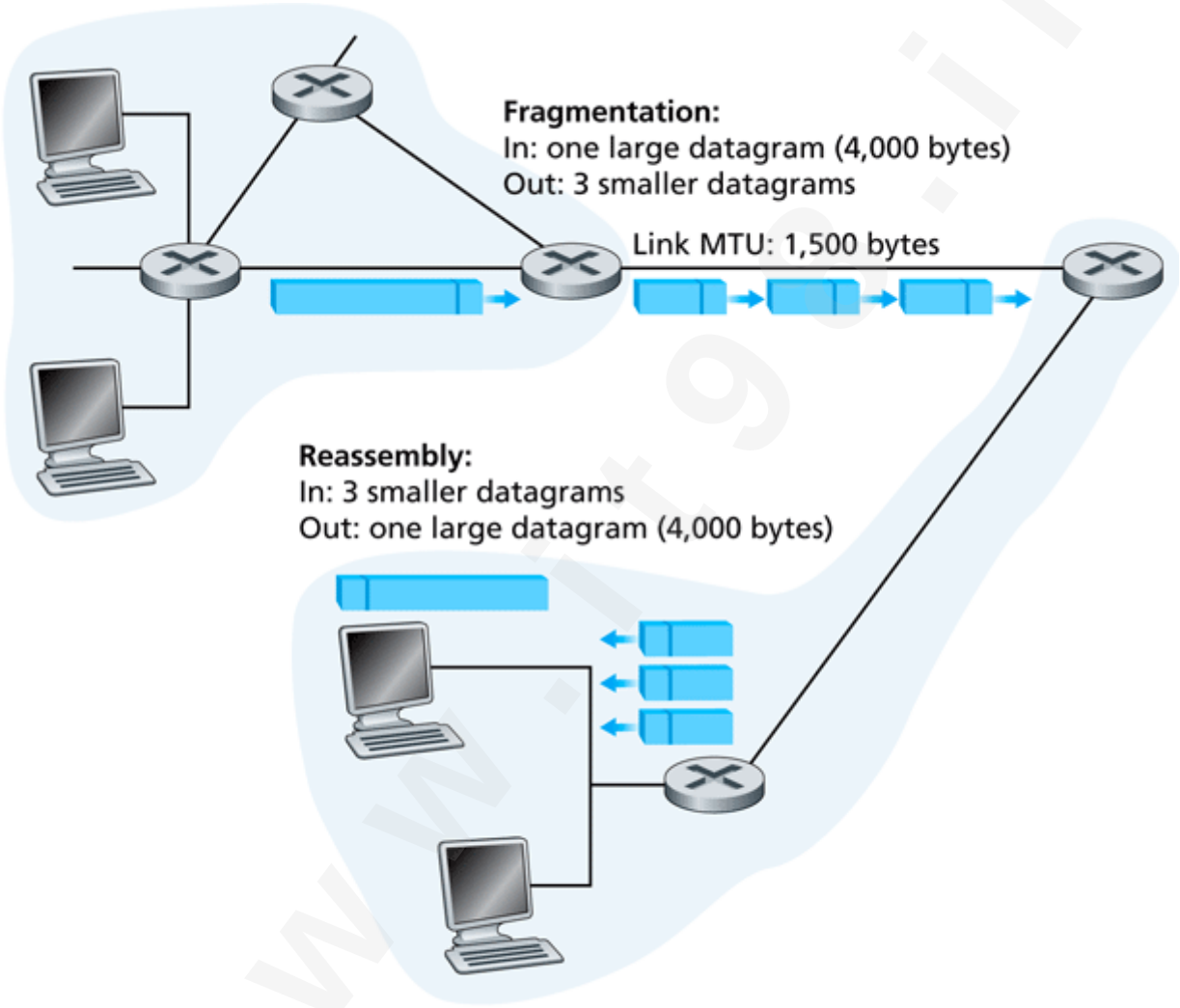


Figure 4.14 ♦ IP fragmentation and reassembly

www.it98.ir

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

Fragment	Bytes	ID	Offset	Flag
1st fragment	1,480 bytes in the data field of the IP datagram	identification = 777	offset = 0 (meaning the data should be inserted beginning at byte 0)	flag = 1 (meaning there is more)
2nd fragment	1,480 bytes of data	identification = 777	offset = 185 (meaning the data should be inserted beginning at byte 1,480. Note that 185 · 8 = 1,480)	flag = 1 (meaning there is more)
3rd fragment	1,020 bytes (= 3,980–1,480–1,480) of data	identification = 777	offset = 370 (meaning the data should be inserted beginning at byte 2,960. Note that 370 · 8 = 2,960)	flag = 0 (meaning this is the last fragment)

Table 4.2 ♦ IP fragments

۴,۲,۲ آدرس دهی IPV4

سر انجام به بحث اصلی یعنی آدرس دهی رسیدیم . در ابتدا فرض میشود که بحث آدرس دهی سرراست و ساده باشد. اما در واقع این چنین نیست.

نکاتی راجع به آدرس دهی ماشین های میزبان(Hosts) وروترها هر میزبان عموماً دارای یک لینک ارتباطی با شبکه میباشد.زمانیکه IP بخواهد از داخل ماشین میزبان ارسال یک دیتا گرام داشته باشد ، از طریق این لینک اینکار را انجام میدهد. مرزبین میزبان و لینک فیزیکی تحت عنوان اینترفیس (کارت شبکه) می باشد.

اما در مقابل در روترها به دلیل ماهیت کار در دریافت بسته از مسیری وارسال به مسیر دیگری می باشد، یک روز حداقل ۲و بیشتر لینک ارتباطی دارد مرز بین روتر ولینک فیزیکی هوم ایترفیس نامیده می شود. بنابراین روتر داری چندین اینرفیس می باشد(یکی برای هر لینک ارتباطی).

هر اینترفیس(در میزبان ویا روتر) برای ارسال و دریافت دیتا گرام نیاز به داشتن یک آدرس IPمی باشد.

هر آدرس IPحاوی ۳۲ بیت می باشد(معادل ۴ بایت) وبنابراین کل آدرس های IP ممکن ۲ به توان ۲۳ (حدود ۴ میلیارد) می باشد.

آدرس های IP عموماً توسط روش دهدهی با نقطه نمایش داده می شوند.

۱۹۳,۳۲,۲۱۶,۹ درواقع است. ۱۱۰۰۰۰۰۱۰۰۱۰۰۰۰۰۱۱۰۱۱۰۰۰۰۰۰۰۱۰۰۱

هر اینتر فیس روی هر میزبان و هر روتر، در اینترنت جهانی بایستی یک آدرس منحصر بفرد داشته باشیم .(به جز اینترفیس هایی که در پشت NAT قرار می گیرند.)

انتخاب آدرس نمی تواند بصورت دلخواه انجام پذیرد.

www.it98.ir

بخشی از آدرس IP توسط زیر شبکه ای که به آن متصل هستیم تعیین می شود . شکل ۴,۱۵ یک مثالی از آدرس دهی IP واینترفیس ها دارد. از یک روتر برای اتصال ۷ میزبان استفاده شده است. با دقت در شکل نکات زیر بدست آورده خواهد شد.

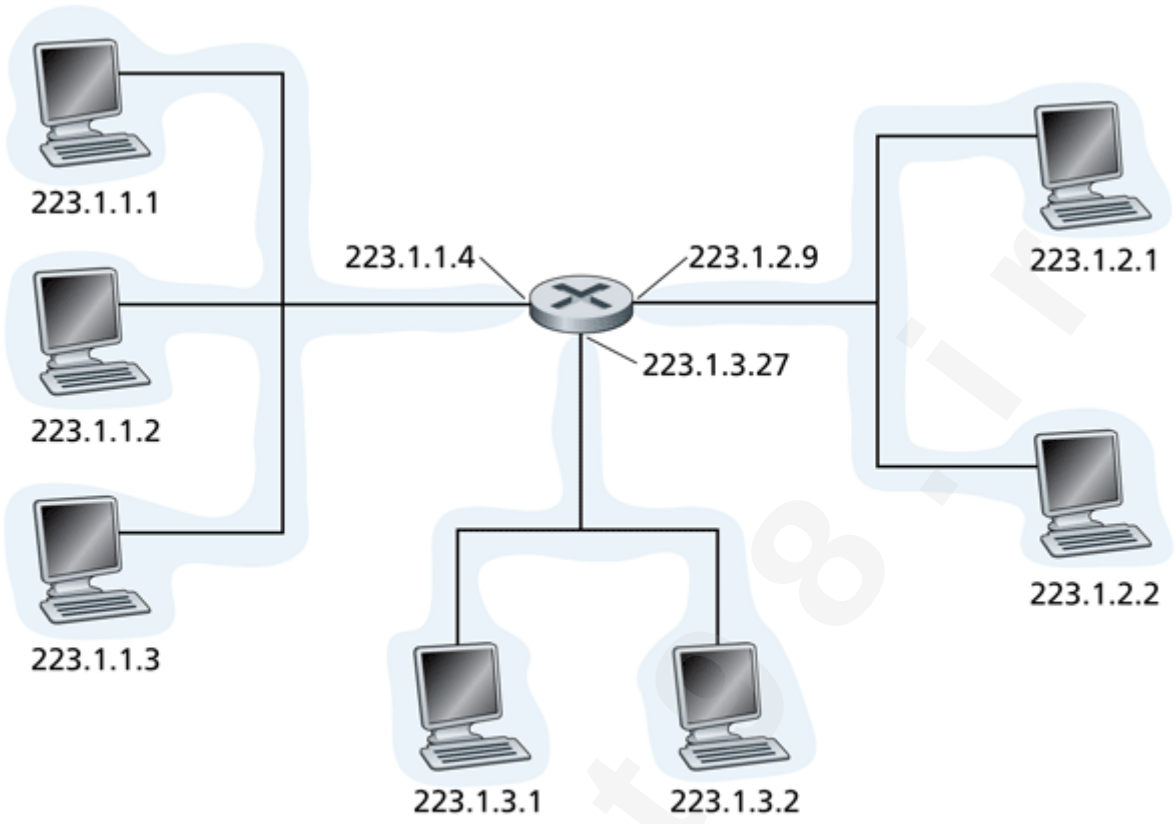


Figure 4.15 ♦ Interface addresses and subnets

* سه میزبان در سمت چپ شکل و اینترفیس روتر همگی XXX ۲۲۳,۱,۱ دارند. یعنی اینکه همگی ۲۴ بیت آدرس IP آنها یکسان است.

این ۴ اینترفیس از طریق شبکه ای که حاوی روتر نیست بهم متصل شده اند. (در دنیای اترنت اینها می توانند از طریق هاب و یا سوئیچ بهم متصل شوند.) در ادبیات آدرس دهی IP به آنها یک زیر شبکه SUBNET گفته می شود.

*آدرس IP اختصاص داده شده به این زیرشبکه ۲۲۳,۱,۱,۰/۲۴ می باشد. ۲۴/ نشان دهنده ماسک زیر شبکه است. SUBNET MASK که نشان دهنده این است که ۲۴ بیت از ۳۲ آدرس IP این زیر شبکه یکسال است.

*در شکل دو زیر شبکه دیگرهم داریم. ۲۴/ ۲۲۳,۱,۲,۰

شکل۴,۱۶ این موضوع را نشان میدهد. ۲۴/ ۲۲۳,۱,۳,۰

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

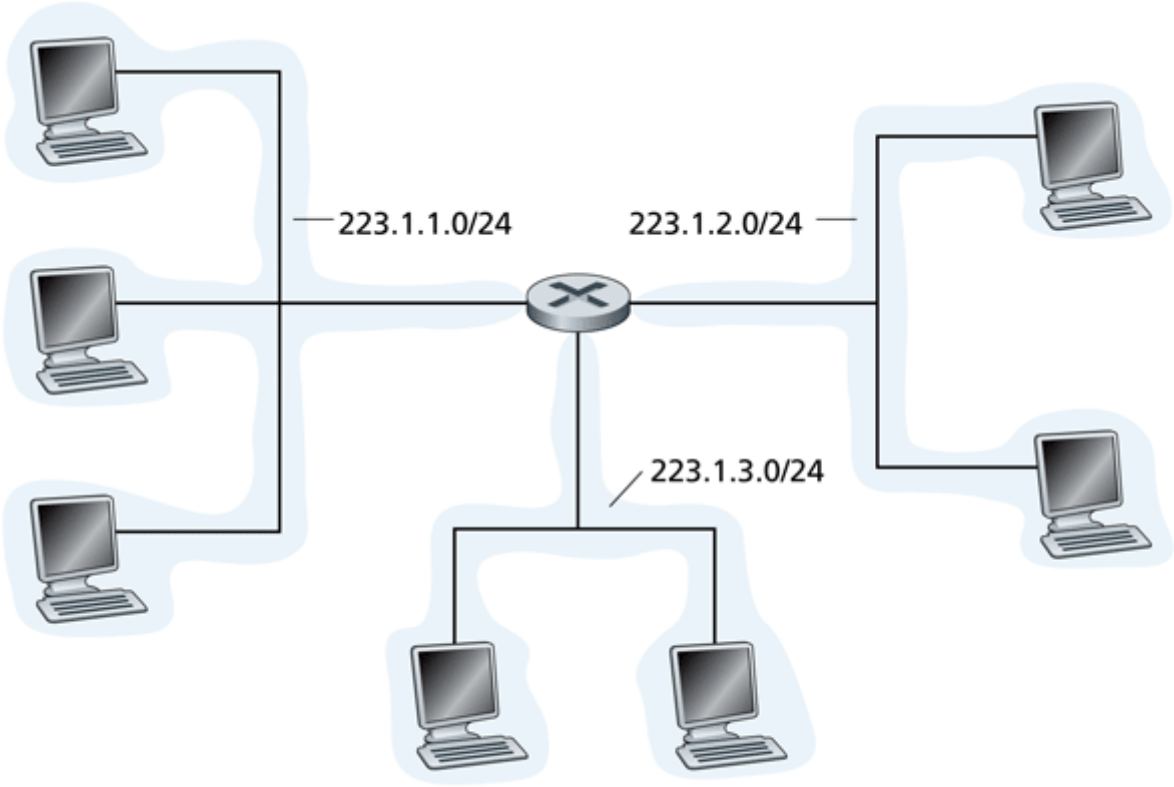


Figure 4.16 ♦ Subnet addresses

به شکل ۴,۱۷ نگاه کنید. چند زیر شبکه در آن وجود دارد؟ سه تا؟

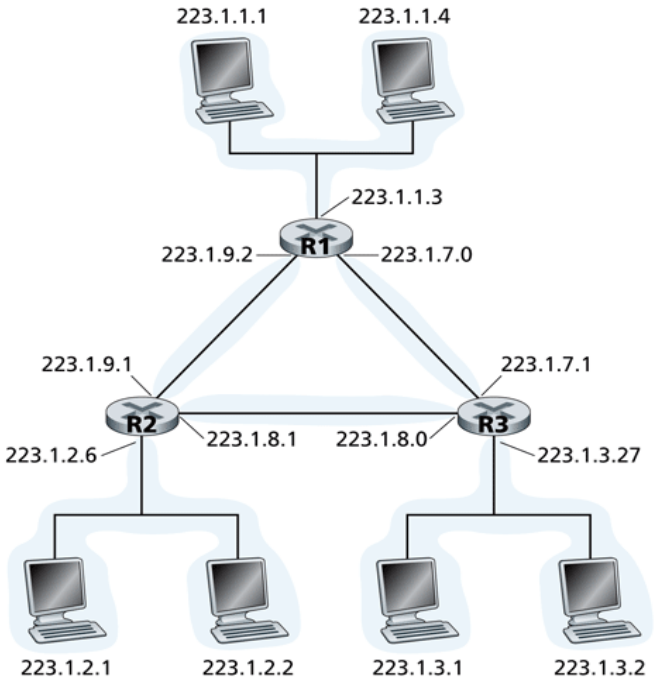


Figure 4.17 ♦ Three routers interconnecting six subnets

www.it98.ir

۲۲۳,۱,۲,۰/۲۴ و۲۲۳,۱,۱,۰/۲۴و۲۲۳,۱,۳,۰/۲۴با دقت بیشتر متوجه میشویم که سه ساب نت دیگر هم داریم.

۲۲۳,۱,۷,۰/۲۴و۲۲۳,۱,۸,۰/۲۴و۲۲۳,۱,۹,۰/۲۴ دقت داشته باشید که روش تعیین زیر شبکه بدین صورت است که اینترفیس ها را از میزبان یا روتر جدا کرده وآنها شبکه های مجزایی ایجاد خواهد شد. هر کدام از این شبکه های مجزا یک زیر شبکه می باشد. توجه داشته باشید که زیر شبکه ها بایستی آدرسهای زیر شبکه کاملاً تفاوتی داشته باشند.

مثال بحث :

بدست آوردن یک بلوک آدرس (گرفتن)

برای دریافت یک بلوک آدرس IP برای استفاده جهت زیر شبکه سازمانتان ، مدیر شبکه بایستی با ISP تماس گرفته (که آن هم دارای مجموعه بزرگتری از بلوکهای آدرس IP است) و درخواست آدرس نماید.

آدرس های IP تحت مدیریت و حاکمیت (ICANN) می باشد. وظیفه این شرکت نه تنها اختصاص آدرسهای IP است ، بلکه مدیریت سرورهای ریشه DNS نیز می باشد.

ICANN آدرسهای IP را به شرکتهای ثبت کننده منطقه ای اینترنت اختصاص داد.(مانند ARIN ,RIPE,APNIC,LACNIC) که همگی با هم تشکیل سازمان پشتیبان کنند . آدرس های ICANN را تشکیل می دهند.

و آنها در آن منطقه خود رسیدگی و مدیریت آدرس های مربوطه را انجام می دهند.

*بدست آوردن آدرس یک میزبان (پروتکل پیکربندی دینامیک میزبان)

بعد از اینکه یک سازمان یک بلوک آدرس را بدست آورد بایستی این آدرس ها را به تک تک این میزبانها اختصاص دهد.

مدیر شبکه معمولاً برای روترها (وسرورها) آدرس های IP را بطور دستی تنظیم می نماید .آدرسهای میزبانها می تواند دستی باشد. اما عموماً اینکار توسط پروتکل DHCP و بطور اتوماتیک به آنها انتساب میشود.

مدیر شبکه میتواند DHCP را تنظیم نموده ، که هر گاه ماشین میزبان وارد شبکه شد یک آدرس IP را دریافت نماید.

میتوان طوری تنظیم نمود که هر بار همان آدرس را بگیرد ویا اینکه آدرس موقتی بوده و هر بار متفاوت باشد. علاوه بر اختصاص و انتساب آدرس IP توسط DHCP ، می توان اطلاعات دیگری را هم برای ماشین های میزبان فراهم آورد. .(نظیر ماسک زیر شبکه ، آدرس دروازه خروجی ،آدرس سرویس دهنده DNS)

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

پروتکل DHCPیک پروتکل مشتری سرویس دهنده می باشد .

در شکل ۴,۲۰ سرویس دهنده DHCP به زیر شبکه ۲۲۳,۱,۲/۲۴ متصل شده است وروتر به عنوان عامل رله برای مشتریان زیر شبکه های ۲۲۳,۱,۱/۲۴ و ۲۲۳,۱,۳/۲۴ عمل می نماید. در بحث زیر فرض می نماییم که در هر زیر شبکه سرویس دهنده DHCPموجود می باشد.

برای یک میزبان واردشونده پروتکل DHCP ، فرایندی ۴ مرحله ای است . که در شکل ۴/۲۱ نشان داده شده است . در این شکل yiadd(نشان دهنده Your Internet Addrss) است.

*مرحله اول کشف سرویس دهنده DHCP

اولین و فیلم میزبان تازه وارد ، پیدا کردن سرویس دهنده DHCP است.برای اینکار از پیام (کشف DHCP) استفاده می کند.

این پیام با بسته UDP به پورت ۶۷ ارسال می شود. اما این بسته به چه کسی ارسال میشود؟ میزبان تازه وارد حتی آدرس هح خود را هم نمی داند. بنابر این از آدرس انتشار گسترده با آدرس مقصد ۲۵۵,۲۵۵,۲۵۵,۲۵۵(یعنی به هم وهر سیستمی) استفاده می نماید. وبرای خود از آدرس"این میزبان " با شماره 0.0.0.0 استفاده می نماید سپس این بسته را به لایه پیوند داده ، داده که به هم نودهی متصل به زیر شبکه ارسال نماید.

۲- پیشنهادهای سرور DHCP -یک سرویس دهنده DHCP که پیام کشف DHCP را دریافت کند با "پیام ارائه DHCP " به آن پاسخ میدهد.بصورت انتشار سراسری (به همه نودها) اگر چندین سرویس دهنده DHCP موجود باشند. مشتری ممکن است تعداد پیشنهاد را دریافت کند و می تواند از بین آنها یکی را انتخاب نماید. در هر بسته پیشنهادی یک شماره تراکنش ومدت زمان اجازه آدرس IP وجود دارد.

۳- درخواست DHCP – مشتری تازه وارد بعد از انتخاب یک پیشنهاد و با ارسال پیام درخواست DHCP به آن جواب می دهد.

۴- پاسخ DHCP – سرویس دهنده DHCP هم به همین دخواست که از طرف مشتری آمده با "پیام مثبت DHCP " جواب می دهد.

ترجمه آدرس شبکه (NAT)

زمانیکه شما شبکه ای را نصب می کند و بخواهید به آن آدرس بدهید بایستی بلوکی از آدرس را از ISP تان دریافت کنید. ممکن است چنین بلوکی وجود نداشته باشد .ویا قبلاً بلوکی را دریافت کرده باشید و بخواهید آنرا گسترش دهید . ممکن است چنین امکانی وجود نداشته باشد.

www.it98.ir

در ضمن ممکن دریافت چنین تعداد آدرس IP عملاً امکانپذیر می باشد. در این حالت کافی است روتری با قابلیت (NAT) داشته باشیم وبرای آن اینترفیس که به اینترنت متصل است یک آدرس IP داشته باشیم .

برای اینترفیس دیگرش که به شبکه ما متصل است می توانیم از آدرس 10.0.0.0 / 24 استفده نماییم . در داخل شبکه و ارتباط بین میزبانها و سرورها از آدرسهای 10.0.0.0 / 24 استفاده نماییم .

در داخل شبکه و ارتباط بین میزبانها وسرورها از آدرسهای 10.0.0.0/24 استفاده می شود اما برای ارتباط با اینترنت این آدرس با آدرس IP روتر جایگزین شده وبسوی مقصد ارسال میشود .بسته های ورودی هم با آدرس IP روتر وارد شده وسپس توسط روتر ویا مکانیزم NAT به میزبان مناسب در داخل شبکه تحویل داده میشود.

شکل ۴,۲۲ مکانیزم کارکرد NAT

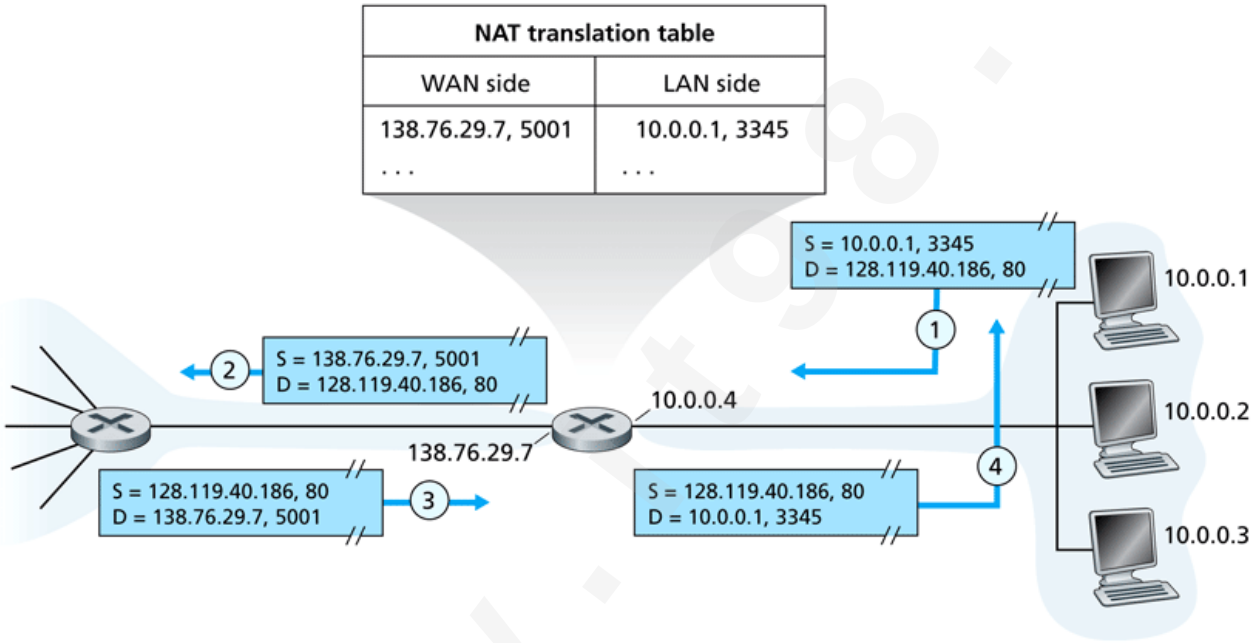


Figure 4.22 ♦ Network address translation

بدلیل استفاده از پورت ها توسط NAT می توان با یک آدرس IP حدود ۶۰/۰۰۰ اتصال همزمان با اینترنت برقرار نموده (دارای اشکالات تداخل لایه ها می باشد.)

۴,۴,۳ پروتکل پیام کنترلی اینترنت (ICMP)

قبلاً دیدیم که لایه شبکه در اینترنت ۳ مولفه اصلی دارد . پروتکل IP ، پروتکلهای مسیر یابی و پروتکل ICMP

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

ICMP توسط روترها ومیزبانها برای ارتباط با هم استفاده می شود.عمده کاربرد این پروتکل برای گزارش خطاهای اتفاق افتاده در شبکه (عموماً به مبدأ وفرستنده) می باشد.

برای مثال ممکن است در یک جلسه FTP . Telnet و یا HTTP به پیام شبکه مقصد قابل دسترس نیست برخورد کرده باشید،این از طرف پروتکلICMPتولید شده است عموماً ICMP بعنوان بخشی از IPدر نظر می گیرند. اما معماری آن در بالای IPبوده وپیامهای ICMPدر درون IPکپسوله شده و حمل می شوند.

پیامهای ICMPحاوی فیلدهای Type و Code می باشند.

دستور معروف Ping از پیام ICMP با Type=8وCode=0 به میزبان مورد نظر ارسال می شود.

در فصل ۱دیدیم که برنامه Traceroute به ما اجازه دنبال کردن مسیر از هر میزبان دیگر را میدهد .این دستور در واقع از ICMP برای اینکاراستفاده می نماید.

برای تعیین نام وآدرس روزهای بین راه (مبداءو مقصد) این دستور تعدادی بسته ipمعمولی را به مقصد ارسال میدارد. هرکدام از بسته ها یک سگمنت با شماره پورت نامربوط را حمل می نمایند.اولین دیتا گرام دارای TTL=1،در بین بسته TTL=2 و ....در فرستنده نیز بلافاصله تایمر روشن می شود (به ازای هر بسته) زمانیکه n امین دیتاگرام به nامین روتر برسد روتر با بررسی TTL متوجه می شود که عمر آن پایان یافته میشود .

بنابراین طبق پروتکل IP پیامی خطا توسط ICMP درست کرده و به (type=11,code=0) مبدأ باز می گرداند. زمانیکه این بسته به ما میرسد می توانیم زمان رفت و برگشت را اندازه گیری کرد و آدرس n امین روز را هم از بسته ارسال خطای آن بدست آوریم.

IPV6 ۴,۴,۴

در اوایل دهه ۱۹۹۰ (IETF) (بازوی مهندسی اینترنت) اقدام به توسعه نسخه جدیدی ازIPV4 نمود. انگیزه اصلی اینکار هم این بود که فضای آدرس ip در حال استفاده و تمام شدن بود ودیگر زیر شبکه های جدیدی نمی توانستند به اینترنت متصل شوند. برای پاسخ گویی به این مشکل نسخه جدید IPV6 با فضای آدرس IP بسیار بزرگی طراحی شد.

آنها (دو گروه) تخمین زده بودند که آدرسها در سال ۲۰۰۳و۲۰۱۸ به پایان خواهد رسید .در سال ۱۹۹۶ ثبت کننده آدرسها در آمریکا ARIN گزارش داد .که آدرسهای کلاس a تماماً اختصاص داده شده اند. ، از کلاس b ، ۶۲ درصد واز کلاس c مقدار۳۷ درصد اختصاص یافته اند.

www.it98.ir

- قالب دیتا گرام IPV6 در شکل ۴/۲۴ نشان داده شده است .

مهمترین تغییرات عبارتند از:

افزایش قابلیتهای آدرس دهی: در این نسخه طول فیلد آدرس از ۳۲ بیت به ۱۲۸ بیت افزایش یافته است .واین اطمینان را می دهد که دنیا هیچ زمان بدون آدرس IP نخواهد ماند هم اکنون حتی هر دانه شن در روی سیاره زمین نیز می تواند حاوی آدرس IP باشد!

علاوه بر آنکه ازunicast و multicast پشتیبانی مینماید از آدرس دهی anycast که اجازه میدهد دیتاگرام به هر گروه از میزبانها تحویل داده شود نیز پشتیبانی می نماید.(بطور مثال با این قابلیت میتوان با دستور(HTTPGET) تقاضا را به نزدیکترین سایت برای دریافت یک سند ارسال نمود.

* هدر ثابت ۴۰ بایتی: باعث پردازش سریعتر دیتا گرام در روترها میشود.

*برچسب گذاری جریان و اولویت: IPV6 یک تعریف زیرکانه ای از جریان (flow) دارد. و اجازه برچسب گذاری (شماره گذاری) بسته های متعلق به یک جریان خاص را که فرستنده درخواست کرده را میدهد. بطور مثال برای سرویسهای بلادرنگ . بعنوان نمونه می توان صوت و تصاویر ویدئویی را به عنوان جریان تعریف نمود که بتوان سریعتر آنها را ارسال و دریافت نمود.اما کاربردهایی مانند دریافت فایل و اسناد وب نیازی به جریان بودن ندارند.علاوه بر آن IPV6 فیلد "کلاس ترافیک" نیز موجود است که مشابه فیلد tos در

IPV4 می باشد. ومیتوان از آن برای دادن اولویت به دیتا گرام ها مورد استفاده قرار داد.

شکل ۴/۲۴ قالب دیتا گرام IPV6

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

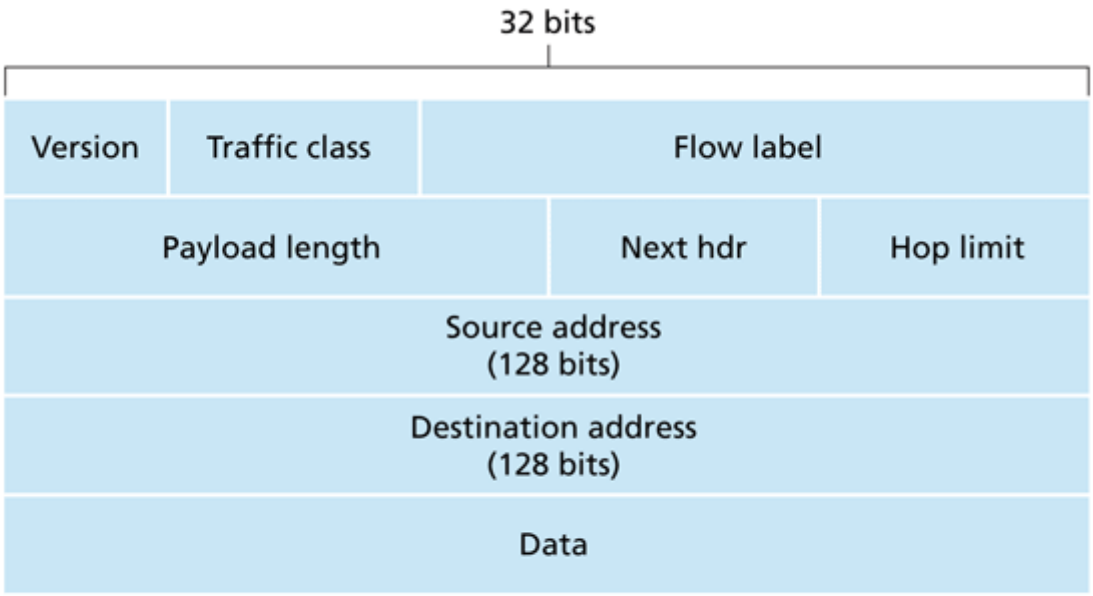


Figure 4.24 ♦ IPv6 datagram format

www.it98.ir

فیلدها:

Next hdr : نشاندهنده پروتکلی است که این دیتا گرام بایستی بـه آن تحویـل داده شـود.برای مثـال (TCP یـا UDP)

Hop limit : همانند TTL است وبا هر بار عبور از روتری یکی از مقدار آن کاسته می شود واگر بـه صـفر برسـد ، دیتا گرام را حذف می نمایند.در IPV6 موارد زیر دیگر برقرار نیست.

شکستن و بازسازی بسته ها : IPV6 این اجازه را نمی دهد. واگر دیتا گرامی با طول بیشتر از مقدار مربوط به لینک خروجی دریافت کند بطور ساده روتر آنرا حذف کرده و به فرستنده پیام "بسته بزرگ است" را میدهد. (توسط پروتکل ICMP) و فرستنده آنگاه خود بایستی اقدام به اصلاح طول بسته نماید.

سر جمع در هدر: از آنجائیکه در لایه انتقال وهمچنین لایه پیوند داده عملیات خطایابی بسـته هـا انجـام مـی شـود .طراحان IPV6 احساس نمودند که این قابلیت ، افزونگی داشته و آنرا حذف نمود ه اند.

فیلد Option : حذف این فیلد بخاطر ثابت بودن طول هدر انجام شده است . در صورت نیاز به این فیلد می توانند که از فیلد Next hdr استفاده نمایند.

انتقال از IPV4 به IPV6

اجازه بدهید بعد از دیدن جزئیات فنی مسئله به موضوع بسیار عملی بپردازیم .چگونه اینترنتی که بـاipv4 در حـال کار است به ipv6 منتقل شود. این موضوع درحالی است که بسته ای ipv6 قادر به پشـتیبانی از ipv4 هسـتند .امـا بسته های ipv4 قادر به پردازش دیتا گرام های ipv6 نیستند.

انتخاب روز خاص و اعلام آن به همه و ارتقاء همه سیستم هـا از ipv4 بـه ipv6 : تجربـه حتـی اینترنـت کوچـک (مربوط به سالهای پیش – ۲۵سال پیش) نشان داد که انجام عمل چنین کاری امکانپذیر نیست .

دو روش دیگر می ماند که می توان هرکدام را ویا با هم مورد استفاده قرار داد.

شاید سر راست ترین راه ، روش دو پشته ای باشد dual stack: از آنجائیکه نودهـای ipv6 قـادر بـه پشـتیبانی کامل از ipv4 هستند. و بصورتهای نودهای ipv6/ipv4 شناخته میشوند . زمانیکه با نور ipv4 سروکار دارند از دیتا گرام v4 وزمانیکه با نور ipv6 سر و کار دارند از v6 استفاده نمایند. نودهای ipv6/ipv4 بایستی دارای هر دو نوع آدرس باشند و علاوه بر آن هر نود بایستی قادر باشد بداند نود بعدی از چه نو عی میباشد که اینکار مـی توانـد توسـط dns امکان پذیر باشد.

شکل ۴/۲۵ این روش را انجام می دهد.

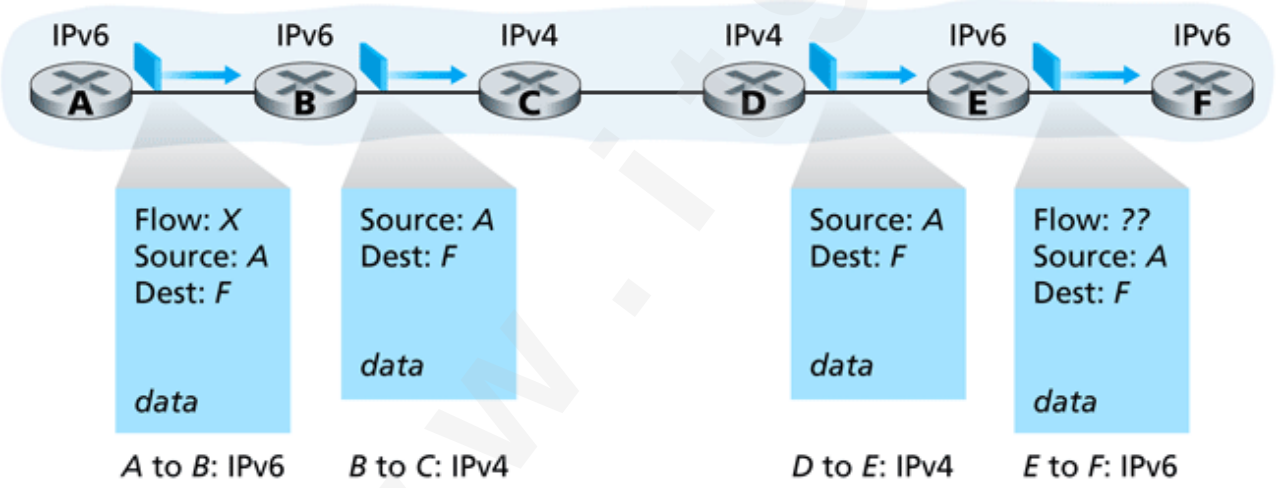


Figure 4.25 ♦ A dual-stack approach

به هر حال در این ترکیب فیلدهای اختصاصی ipv6 دیگر در مقصد معتبر نخواهند بود.

روش دیگر استفاده از تونل زنی می باشد: فرض کنید دو روتر ipv6 بخواهند با هم ارتباط داشته باشـند ولـی بـین آنها روترهای ipv6 باشند . در این حالت روتر ارسال کننده ipv6 می تواند دیتا گرام خود را دریک دیتا گرام ipv4

wWw.it98.ir

کبود کرده و توسط روترهای میانی که ipv4 هستند ارسال کند ودر روتر مقصد که ipv6 هست ، این دیتا گرام تونل زده شده را بازیابی نماید.

شکل ۴/۲۶ مکانیزم تونل زنی ipv6/ipv4 :

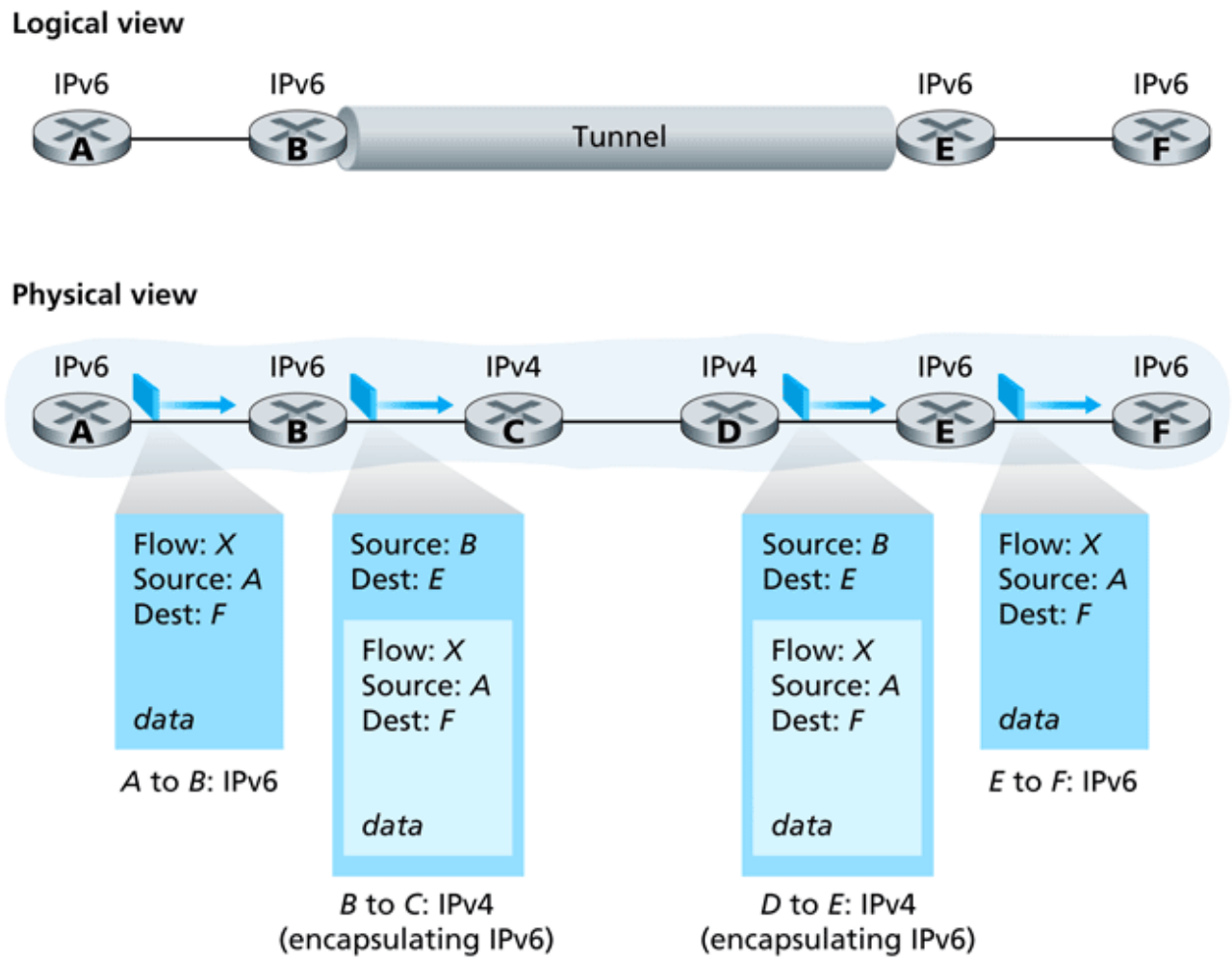


Figure 4.26 ♦ Tunneling

اما بهر حال به نظر می رسد ، انتقال کامل از ip4 به ipv6 به این سادگیها و زودیها در عمل امکانپذیر نباشد.

www.it98.ir

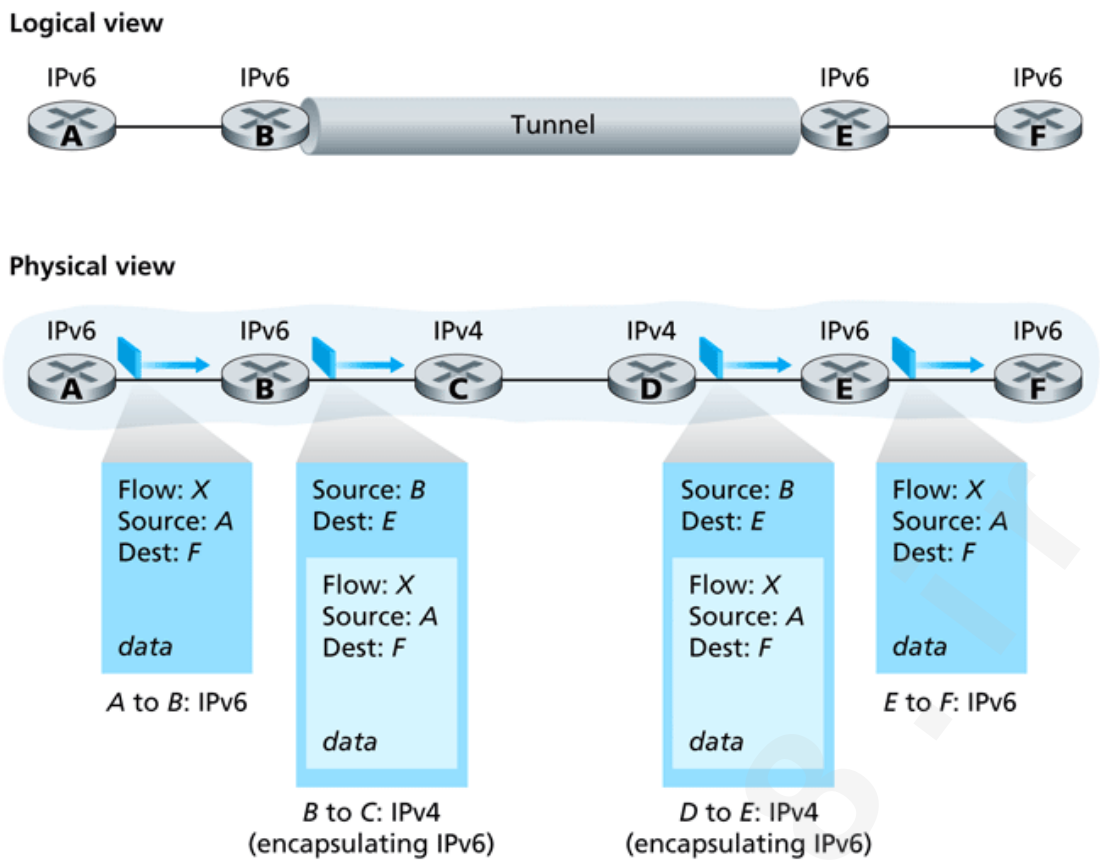


Figure 4.26 ♦ Tunneling

دخالت (وجود) روترهای IPv4 در تونل باعث می شود دیتاگرام (داده های) این IPv4 میان خودشان مسیر یابی شود ، به همان اندازه آنها می توانند هر دیتاگرام دیگری را مسیر یابی کنند ، خوشبختانه به صورت ناخوداگاه دیتاگرام این IPv4 ها خودشان شامل دیتاگرام کامل IPv6 هستند. گره IPv6 در سمت دریافت تونل نهایتا دیتاگرام IPv4 را دریافت میکنند (این سرنوشت دیتاگرام IPv4 است!) ، مشخص است که دیتاگرام IPv4 شامل دیتاگرام IPv6 است ، دیتاگرام IPv6 را استخراج و پس از آن دیتاگرام IPv6 را مسیر یابی می کنند،دقیقا همان طور که اگر دیتاگرام IPv6 را از ارتباط مستقیم در مجاور (همسایه) IPv6 دریافت کرده باشد.

ما این بخش را تمام می کنیم با توجه به پذیرش این موضوع که IPv6 در ابتدا به آرامی خود را مطرح کرد[Lawton 2001] ، که اخیرا با سرعت بیشتری ساخته می شوند. اداره مدیریت و بودجه (OMB) ایالات متحده در ژوئن 2008 درخواست تغییر و تحول IPv6 را داد. گسترش دستگاه هایی همانند تلفن های فراهم کننده IP (IP-enabled Phones) و دیگر دستگاه های قابل حمل فشار مضاعف برای گسترش گسترده IPv6 بودند.در نسل سوم پروژه مشارکت اروپا [3GPP 2007] IPv6 به عنوان طرح آدرس یابی استاندارد برای برنامه های چند رسانه ای(Multimedia) موبایل تعیین شد. حتی اگر IPv6 در ۱۰ سال اول عمر کوتاه خود به صورت گسترده گسترش نیافته بودند در دراز مدت این موضوع به صورت واضح مشاهده می شد.

www.it98.ir

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

سیستم شماره تلفن امروزی چند دهه را در بر دارند ، اما امروزه تقریبا بعد از گذشت نیم قرن بدون هیچ نشانه ای از دور افتادگی به کار خود ادامه می دهند.به همین نحو IPv6 نیز برای رسیدن به این جایگاه به زمان نیاز دارد، اما ممکن است این زمان بیش از حد طولانی شود. برایان کارپنتر (Brian Carpenter) رئیس سابق کمیته معماری اینترنت [IAB 2007] و نویسنده چندین نظر خواهی مربوط به IPv6 گفته "من همیشه نگاهی به عملکرد و پیشرفت این ۱۵ سال که از سال ۱۹۹۵ شروع شد داشته ام" [Lawton 2001] .

یک درس مهم که ما می توانیم از تجربه IPv6 فرا بگیریم این است که تغییر پروتکل های لایه شبکه کاری فوق العاده دشوار است. در اوایل دهه 1990 ، پروتکل های بیشماری در لایه شبکه تشکیل شدند که انقلاب بزرگی برای اینترنت به شمار می رفت،اما بسیاری از این پروتکل ها در گذشت زمان محدود شدند. این پروتکل ها شامل IPv6 ، پروتکل های چند پخشی (فرستادن اطلاعات به چند شبکه به طور همزمان) (بخش ۴,۷) و پروتکل های ذخیره (بخش ۷) نیز می شوند. به راستی معرفی پروتکل های جدید در لایه شبکه همانند جابجایی پی یک ساختمان است- این عمل خیلی سخت است که بدون ریزش کل ساختمان یا بدون جابجایی ساکنین خانه انجام شود- از سوی دیگر، اینترنت گسترش سریعی در پروتکل های جدید لایه برنامه کاربردی(Application Layer) به خود دیده است. نمونه های کلاسیک آن البته وب ، پیام رسانی فوری و اشتراک گذاری P2P است. نمونه های دیگر شامل جریان های صدا و تصویر و بازی های توزیع شده است. معرفی پروتکل های جدید لایه برنامه کاربردی همانند رنگ آمیزی دوباره یک ساختمان است – این کاری نسبتا آسان می باشد که در صورت انتخاب رنگ تاثیر گذار دیگر همسایه ها نیز از کار شما تقلید می کنند- خلاصه ، در آینده ما می توانیم تغییراتی در لایه شبکه اینترنت پیش بینی کنیم ، اما این تغییرات در مقایسه با لایه برنامه کاربدی احتمالا بسیار آهسته تر اتفاق خواهد افتاد.

۴,۴,۵ خلاصه ای از تهاجم به امنیت IP

در بخش ۴,۴,۳ توضیحاتی در مورد IPv4 که شامل سرویس هایی که باعث بهبودی آن و چگونگی اجرای این سیستم ها بود بحث شد. زمانی که این بخش را کاملا مطالعه کنید ، ممکن است شما متوجه شوید که هیچ گونه تذکری در مورد سرویس های امنیتی وجود ندارد.IPv4 در دوره زمانی (دهه ۱۹۷۰) ، زمانی که اینترنت اصولا برای یک ارتباط شبکه ای تحقیقاتی قابل اعتماد استفاده می شد ، طراحی شده بود. ساخت یک شبکه کامپیوتری آن هم با استفاده از انبوهی از تکنولوژی های لایه رابط (Link-Layer) بدون نگرانی در مورد امنیت آن خود به اندازه کافی به چالش کشیده شده است.

اما امنیت امروزه اهمیت زیادی به خود گرفته است .محققان اینترنت در حال طراحی جدید پروتکل های لایه شبکه هستند که تنوع زیادی در سرویس های امنیتی فراهم می کنند. یکی از این پروتکل ها IPsec است که یکی از محبوب ترین پروتکل های امن لایه شبکه می باشد و همچنین در بسیاری از موارد در شبکه های خصوصی مجازی (VPN) مورد استفاده قرار می گیرد. اگر چه IPsec و زیربند پنهانی آن را در فصل ۸ مورد بحث قرار می دهیم ، ولی در این بخش به مقدمه ای در مورد سرویس IPsec می پردازیم.

www.it98.ir

IPsec به نوعی طراحی شده که با IPv4 و IPv6 سازگاره است .به خصوص به منظور جمع آوری مزایای IPsec ، ما نیازی به جابجا کردن یا جایگزین کردن بسته های پروتکلی در تمامی روتر ها و میزبان (Host) ها در اینترنت نداریم. برای مثال استفاده از حالت حمل و نقل (Transport mode) (یکی از دو حالت IPsec) ، اگر دو میزبان بخواهند به صورت مطمئن ارتباط داشته باشند، کافی است IPsec فقط در این دو میزبان در دسترس باشد. تمام روترها و میزبان های دیگر میتوانند برای ادامه از IPv4 بدون IPsec استفاده کنند.

به منظور فهم بیشتر ، ما به حالت حمل و نقل IPsec توجه می کنیم ، دو میزبان ابتدا قابلیت IPsec را بین خودشان بر قرار می کنند. (بنابر این IPsec ارتباط گراست!) با این قابلیت ، تمام قطعه ها (بخش ها)ی TCP و UDP بین این دو میزبان با برخورداری از سرویس های امنیتی که توسط IPsec فراهم شده ارسال می شوند. در قسمت ارسال ، لایه حمل و نقل قطعات را به IPsec صادر می کند. سپس IPsec قطعات را رمز دار کرده و فیلد افزودنی امنیتی را به قطعات پیوست می کند ، و آنها را به صورت کپسول در آورده و نتیجه را به صورت مقرون به صرفه برای حمل و نقل به دیتاگرام IP ارسال می کند. (در واقع این کار قدری پیچیده تر است که آن را در فصل 8 خواهیم دید.) سپس میزبان ارسال کننده دیتاگرام را به اینترنت ارسال می کند ، جایی که بسته حمل و نقل به میزبان مقصد (گیرنده) می رسد. در میزبان گیرنده IPsec قطعات را رمز گشایی می کند و آنها را به قطعات بدون رمز تبدیل کرده و به لایه حمل و نقل تحویل می دهد.

توافق نامه سرویس هایی که از قابلیت IPsec استفاده می کنند شامل موارد زیر می باشد :

- *توافق پنهانی* . مکانیزم هایی که به دو میزبان در حال ارتباط اجازه می دهد تا با الگوریتم ها و کلید های پنهانی سازش کنند.

- *رمز دار کردن دیتاگرام قابل حمل IP* . زمانی که میزبان ارسال کننده یک قطعه از لایه حمل و نقل دریافت می کند ، IPsec بسته قابل حمل را رمز دار می کند. بسته قابل حمل فقط می تواند توسط IPsec موجود در میزبان گیرنده رمزگشایی شود.

- *یکپارچگی داده* . IPsec به میزبان گیرنده اجازه می دهد که فیلد سرپیام(Header) دیتاگرام و بسته قابل حمل رمزدار شده را تا زمانی که دیتاگرام در مسیر مبدا به مقصد است را وارسی کند.

- *قانون منبع* . زمانی که میزبان از IPsec دیتاگرامی از مبدا قابل اعتماد دریافت می کند (همراه با کلید اطمینان- به فصل ۸ مراجعه کنید) میزبان مطمئن است که IP آدرس مبدا ای که در دیتاگرام وجود دارد ، مبدا واقعی دیتاگرام است.

www.it98.ir

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

زمانی که دو میزبان قابلیت IPsec را برقرار کنند ، تمام قطعات TCP و UDP به صورت رمزدار و قانون مند شده بین آنها ارسال می شود. از این رو IPsec نوعی پوشش دفاعی و امنیتی را در ارتباط بین دو میزبان برای تمامی برنامه های شبکه فراهم می کند.

یک شرکت می تواند از IPsec برای ارتباط مطمئن میان شبکه اینترنت عمومی غیر مطمئن استفاده کند.برای روشن شدن مفهوم ، ما به یک مثال ساده اشاره می کنیم. شرکتی که تعداد زیادی از فروشندگان را داراست در نظر بگیرید ، که هر کدام دارای یک کامپیوتر لپ تاپ هستند. فرض کنید که فروشندگان بارها نیاز به مشاوره محرمانه با اطلاعات شرکت دارند (به طور مثال ، اطلاعات قیمت و تولید) که این اطلاعات روی سرور (Server) شرکت اصلی ذخیره شده اند. به علاوه تصور کنید که فروشندگان همواره نیاز به ارسال مدارک محرمانه به یکدیگر دارند. چگونه این ارتباط به وسیله IPsec برقرار می شود؟ ممکن است شما حدس زده باشید ، ما IPsec را روی سرور اصلی و لپ تاپ های فروشندگان نصب می کنیم. با نصب IPsec رو این میزبان ها ، هر موقع که فروشنده نیاز به ارتباط با سرور اصلی و یا فروشنده دیگری داشته باشد ، ارتباط مذکور کاملا امن خواهد بود.

4.5 الگوریتم های مسیر یابی

تا اینجا در این فصل ما بیشتر در مورد کارایی ارسال لایه شبکه شبکه بحث کردیم. آموختیم یک بسته چه موقع به روتر می رسد و اندکس های روتر چگونه جداول و واسط های ارتباطی بسته را هدایت می کنند. همچنین آموختیم که الگوریتم های مسیر یابی، که در روتر های شبکه به کار گرفته شده اند، چگونه اطلاعات را که در جداول ارسال شکل بندی شده اند، مبادله و محاسبه می کنند. تاثیرات بین الگوریتم های مسیر یابی و جداول ارسال در تصویر 4.2 نمایش داده شده است. عمق بحث ما در مورد ارسال بود که اکنون توجه خود را روی مبحث مهم دیگری در این فصل یعنی ، کارایی حیاتی مسیر یابی لایه شبکه جلب می کنیم. خواه زمانی که لایه شبکه یک سرویس دیتاگرام فراهم می کند (که در این صورت بسته های مختلفی بین مبدا و مقصد رد و بدل می شوند که می تواند از چندین روتر عبور کنند) یا زمانی که یک سرویس مجازی کامپیوتر (VC) داشته باشیم (که در این صورت بسته ها بین مبدا و مقصد از یک مسیر مشابه رد و بدل می شوند). با این وجود لایه شبکه میبایست بهترین مسیر را برای ارسال بسته ها از فرستنده به گیرنده تعیین کند. خواهیم دید که کار مسیر یابی تعیین بهترین مسیر ها از فرستنده ها به گیرنده ها از میان روترهای شبکه است (به طور هم ارز یا چند مسیری).

به طور نمونه میزبان به طورت مستقیم به یک روتر به نام روتر پیش فرض (Default Router) متصل شده است (همچنین به آن روتر First-hop نیز می گویند). هر وقت میزبان بسته ای ارسال می کند ، بسته ابتدا به روتر پیش فرض ارسال می شود. ما به روتر پیش فرض مبدا به عنوان روتر مبدا و به همین ترتیب به روتر پیش فرض مقصد به عنوان روتر مقصد مراجعه می کنیم. مشکل مسیر یابی یک بسته از میزبان مبدا به میزبان مقصد به مشکل مسیر یابی یک بسته از روتر مبدا به روتر مقصد قابل حل تر شده است. تمرکز ما در این بخش به همین موضوع است.

www.it98.ir

هدف از الگوریتم های مسیر یابی بسیار ساده است : گروهی از روتر ها را به همراه پیوند (Link) های ارتباطی در نظر بگیرید ، الگوریتم مسیر یاب "بهترین" مسیر را از روتر مبدا به روتر مقصد تعیین می کند. برای نمونه ، یک مسیر خوب ، مسیری است که حداقل هزینه را در بر داشته باشد. خواهیم دید ، هرچند این کار ، یک کار تکنیکی باشد ، دنیای واقعی نگرانی هایی از قبیل مسائل سیاست گذاری (برای مثال، یک اداره را مثل روتر x در نظر بگیرید که وابسته به سازمان Y است این اداره نباید هر بسته رسیده از طریق شبکه متعلق به سازمان Z را ارسال کند) و همچنین پیچیده شدن مفهوم ساده و زیبای الگوریتم ها به نظریه های اولیه مسیر یابی شبکه های امروزی دارد.

یک نمودار برای فرمول بندی کردن مشکلات مسیر یابی استفاده می شود. فراخوانی این نمودار به صورت G=(N,E) است ، که N گروه گره ها و E مجموعه دوره هاست ، جایی که دوره یک مسیر بسته بین گره هاست. مفهوم مسیر یابی لایه شبکه به این شکل است که، گره ها در این نمدار نمایشی ، روتر ها – نقاط مکان هایی هستند که تصمیماتی برای بسته های ارسالی گرفته می شود– و دروه های متصل شده به این گره ها پیوند بین روتر ها را نمایش می دهند. مثل نمودار نمایش داده شده از یک شبکه کامپیوتری که در تصویر 4.27 نمایش داده شده است. برای دیدن نمودارهای بیشتری از نقشه های واقعی شبکه به [Dodge 2007,Cheswick 2000] مراجعه کنید; برای بحث در مورد چگونگی تفاوت مدل های بر اساس نمودار (Graph-based) اینترنت به [Zegura 1997, Faloutsos 1999, Li 2004] مراجعه کنید.

همان طور که در تصویر 4.27 نمایش داده شده همواره یک دوره یک مقدار به تابعیت از ارزش خود دارد. به طور نمونه ، ارزش یک دوره می تواند بازتابی از طول فیزیکی رابط آن (برای مثال ، رابط عبوری از اقیانوس دارای ارزش (قیمت) بیشتری از یک رابط کوچک زمینی است) ، سرعت رابط ، و یا مقدار پولی پیوند با رابط باشد. برای فهم بیشتر ، ما بسادگی قیمت دوره ها را به عنوان داده می گیریم و هیچ نگرانی در مورد چگونگی تصمیم گیری آن نداریم. برای هر دوره (x,y) در E ، ما c(x,y) را به عنوان قیمت بین دو گره x و y مشخص می کنیم. اگر هر دوی (x,y) به E تعلق نداشتند ، قرار می دهیم c(x,y)=∞ . همواره ما تفکر می کنیم فقط روی نمودار های هدایت نشده (یعنی ، نمودار هایی که دوره های آن سمت و جهتی ندارند) بنابر این دوره (x,y) همانند دوره (y,x) است و داریم c(x,y) =c(y,x). همچنین گفته می شود گره y همسایه گره x است اگر (x,y) متعلق به E باشد.

با توجه به اینکه هزینه های اختصاص داده شده به دوره های مختلف در نمودار انتزاعی ، یکی از اهداف الگوریتم های مسیر یاب شناسایی مسیر های کم خرج بین مبدا و مقصد است. برای اینکه این مسئله را به طور دقیق مورد بررسی قرار دهیم ، یک مسیر از نمودار G=(N,E) را فراخوانی می کنیم که دارای رشته ای از گره ها (x_1 , x_2 x_p , ... ,) که هر کدام دو به دو مثل (x_1,x_2) , (x_2,x_3), . . . , (x_{p-1},x_p) دوره هایی در E هستند. قیمت مسیر (x_1 , x_2 , ... , x_p) به سادگی جمع تمام دوره های موجود در این مسیر می شود ، یعنی c(x_1,x_2) + c(x_2,x_3) + ... + c(x_{p-1},x_p) . با توجه به دو گره x و y ، به طور مثال بین این دو گره چندین مسیر وجود دارد. هر کدام از این مسیر ها قیمتی دارد. یک یا چند کدام از این مسیر ، مسیر کم هزینه می باشد. مسئله کم هزینه بودن از این رو روشن می شود : پیدا کردن یک مسیر بین مبدا و مقصد با کم ترین هزینه. در

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

تصویر 4.27 ، برای مثال ، مسیر کم هزینه بین گره مبدا u و گره مقصد w مسیر (u,x,y,w) می باشد که هزینه آن در نهایت ۳ می شود.

Figure 4.27

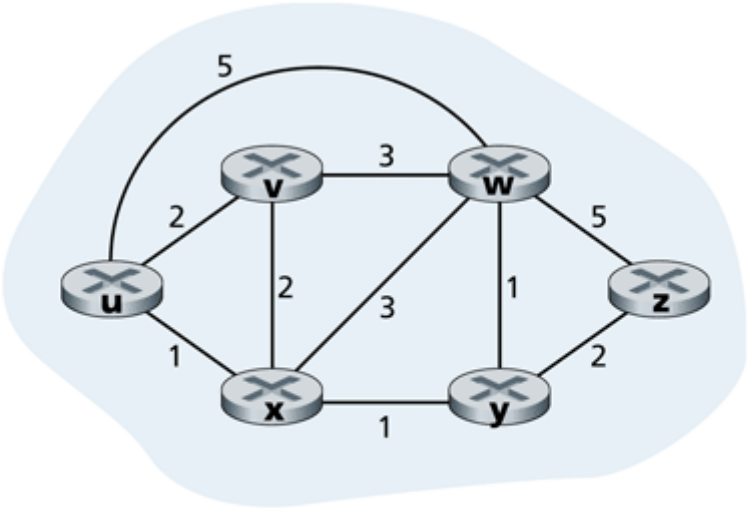


Figure 4.27 ♦ Abstract graph model of a computer network

توجه داشته باشید که اگر تمام دوره ها در نمودار قیمت مشابهی داشته باشند ، مسیر کم هزینه همواره کوتاه ترین مسیر نیز می باشد (یعنی مسیری با کوچک ترین مقدار عددی رابط بین مبدا و مقصد).

به عنوان یک تمرین ساده ، کم هزینه ترین مسیر را بین دو گره u و z در تصویر ۴,۲۷ پیدا کنید و به چگونگی محاسبه این مسیر فکر کنید. شما نیز مثل اکثر افراد مسیر بین دو گره u و z را با بررسی تصویر ۴,۲۷ انتخاب می کنید، برای این کار چند مسیر بین دو گره را دنبال می کنید ، در نهایت به طریقی خود را متقاعد می کنید ، مسیری را که انتخاب کردید در تمام مسیر های ممکن کم هزینه ترین است. (آیا شما ۱۷ مسیر ممکن بین دو گره u و z را بررسی کردید؟ احتمالا خیر!) یکی از اهداف الگوریتم های مسیر یابی محاسبه مسیر هاست- الگوریتم های مسیر یاب در یک منطقه با اطلاعات کامل در مورد شبکه اجرا می شوند- به طور کلی ، یک راه برای دسته بندی الگوریتم های مسیر یاب ، قرار دادن آنها در گروه های کلی و غیر متمرکز است.

- یک *الگوریتم مسیر یابی کلی (سراسری)* کم هزینه ترین مسیر را بین مبدا و مقصد با استفاده از شناسایی کلی شبکه ، محاسبه می کنند. به این صورت که الگوریتم اتصال بین تمام گره ها و ارزش (قیمت) های آنها را به عنوان ورودی دریافت می کند ، سپس الگوریتم قبل از تعیین محاسبه این اطلاعات را درخواست می کند. بنابراین الگوریتم محاسبه در یک سایت (که از الگوریتم مسیر یاب کلی استفاده میکند) یا چندین سایت اجرا می شود. در اینجا کلید تشخیص دهنده عمل می کند ، هر چند ، الگوریتم کلی اطلاعات کاملی درباره اتصال و ارزش مسیر ها دارد. الگوریتم

www.it98.ir

هایی دارای اطلاعات کلی معمولا به الگوریتم های *Link-State(LC)* معروف هستند. الگوریتم های این چنین اطلاعات مربوط به ارزش هر لینک را در شبکه معین می کنند. در مورد الگوریتم های *LS* در بخش ۴,۵,۱ مطالعه خواهیم کرد.

- در *الگوریتم مسیر یابی غیر متمرکز* کم هزینه ترین مسیر را در صورت تکرار از وضعیت توزیع محاسبه می کند. در این الگوریتم هیچ گره ای اطلاعات کامل درباره ارزش لینک های شبکه ندارد. در عوض هر کدام از این گره های فقط با شناسه ای از ارزش خودشان که در لینک های آنها مستقیما پیوست شده شروع می شوند.پس یک گره از طریق تکرار ، فرآیند محاسبه و مبادله اطلاعات کم هزینه ترین مسیر به مقصد یا مجموعه ای از مقصد ها را با گرهای مجاورش (یعنی گره هایی دیگر در قسمت پایانی لینکی که خودشان پیوست شده اند) به تدریج محاسبه می کند. ما در مورد الگوریتم مسیر یابی غیر متمرکز که به آن الگوریتم بردار مسافت *Distance-Vector(DV)* نیز می گویند بیشتر مطالعه خواهیم کرد. به این دلیل به آنها الگوریتم بردار مسافت می گویند ، که هر گره بردار تخمینی را در مورد ارزش (مسافت) بین تمام گره های شبکه را تخمین می زند.

دومین روش دسته بندی الگوریتم های مسیر یاب مطابق دسته بندی آنها به دو دسته ایستایی (static) یا پویایی (Dynamic) است. در الگوریتم های مسیر یاب استایی ، ارسال ها در نتیجه دخالت انسان ، از لحاظ زمانی خیلی آهسته تغییر می کنند (برای مثال، تغییر دستی جدول ارسال یک مسیر توسط انسان). الگوریتم مسیر یاب پویایی مسیر های ارسال را به ترافیک بارگذاری شبکه ای یا جغرافیایی تغییر می دهند . یک الگوریتم پویا می تواند به صورت دوه ای یا مستقیما تغییرات مقداری (ارزشی) یا جغرافیایی لینک (رابط) ها را دریافت کند. تا زمانی که الگوریتم های پویا دارای عکس العمل سریع به تغییرات شبکه باشند ، در معرض مشکلاتی همچون حلقه های ارسال و نوسانات ارسال هستند.

سومین روش برای دسته بندی الگوریتم های مسیریاب ، دسته بندی آنها به حساس به بارگذاری (Load-sensitive) یا غیر حساس به بارگذاری (Load-insensitive)می باشد. در الگویتم حساس به بارگذاری ، ارزش لینک ها نوسانات پویایی به ازدحام جریان لینک اصلی دارند. اگر یک ارزش بالا به یک لینک پر ازدحام پیوند داده شده باشد ، الگوریتم مسیر یاب متمایل به انتخاب مسیر لینک پر ازدحام خواهد بود. در زمان پروژه اولیه *ARPAnet* که الگوریتم های مسیر یاب حساس به بارگذاری بودند [McQuillan 1980] به سختی ارسال ها صورت می گرفت [Huitema 1998]. امروزه الگوریتم های مسیر یاب اینترنت (مثل RIP OSPF , و BGP) غیر حساس به بارگذاری هستند ، در ارزش لینک ها درصد ازدحام به طور قطع ازدحام جریان پیدا نمی شود (اخیرا پایان یافته).

۴,۵,۱ الگوریتم مسیر یابی *Link-State (LS)*

در یک الگوریتم *Link-State* فراخوانی شبکه جغرافیایی و ارزش تمام لینک ها شناخته شده است. یعنی به عنوان ورودی برای الگوریتم *LS* در دسترس است. در واقع این عمل با داشتن بسته های *LS* انتشار یافته هر گره به تمام گره های دیگر شبکه ، که هر کدام از این بسته های *LS* شامل شناسه ها و ارزش های پیوست شده به لینک

wWw.it98.ir

www.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

هستند ، انجام شده است. در واقع (برای مثال ، پروتکل مسیر یابی OSPF اینترنت ، که در بخش ۴,۶,۱ مورد بحث قرار خواهد گرفت) با الگوریتم *Link-State Broadcast* شناخته شده است [Perlman 1999] . ما در مورد الگوریتم های قابل انتشار (Broadcast) در بخش ۴,۷ مطالعه خواهیم کرد. نتیجه انتشار گره ها این است که تمام گره ها نمایش یکسان و کاملی در شبکه دارند. هر گره می تواند الگوریتم *LS* را اجرا کند و مجموعه مشابه مسیر های کم هزینه از هر گره دیگر را محاسبه کند. الگوریتم *Link-state* که ما اکنون به این نام می شناسیم در قبل به نام *Dijkstra's algorithm* شناخته می شد ، بعد از اختراعش به این اسم لقب گرفت. شرح دیگر الگوریتم ، الگوریتم *Prim* است *:* برای بحث کامل تر در مورد انواع الگوریتم ها به [Cormen2001] مراجعه کنید. الگوریتم *Dijkstra* کم هزینه ترین مسیر را از یک گره (مبدا ، جایی که ما به گره u اشاره کردیم) به تمام گره های دیگر در شبکه محاسبه می کند. الگوریتم *Dijkstra* یک ویژگی تکرار دارد و ویژگی تکرار را تا k بار در الگوریتم اجرا می کند، این کار برای تعیین کردن کم هزینه ترین مسیر k گره های مقصد و میان تمام مسیر های کم هزینه گره های مقصد ،که k مسیر کم ارزش خواهیم داشت انجام می دهد. اجازه دهید با نماد گذاری توضیح دهیم :

- *D(v)* : ارزش ، کم ارزش ترین مسیر از مبدا به مقصد v به عنوان تکرار الگوریتم.
- *P(v)* : گره قبلی (مجاور v) در امتداد جریان مسیر کم ارزش از مبدا به v.
- *N′* : زیر مجموعه گره ها ; v در مجموعه N′ است اگر مسیر کم ارزش از مبدا به v که مقصد شناخته شده است.

الگوریتم مسیر یاب سراسری شامل ارزش دهی به مرحله بعد توسط حلقه می باشد. تعداد دفعاتی که حلقه اجرا می شود برابر است با تعداد گره های موجود در شبکه . به محض پایان یافتن حلقه الگوریتم کوتاه ترین مسیر ار مبدا u به هر گره دیگر در شبکه را محاسبه می کند.

شبه کد عکس شماره 372

به عنوان مثال ، شبکه ای را در تصویر ۴,۲۷ و همین طور محاسبه کم هزینه ترین مسیر از u به تمام مقاصد ممکن را تصور کنید. فهرستی خلاصه از محاسبات الگوریتم در جدول ۴,۳ نمایش داده شده است ، جایی که هر خط از این جدول ، مقدار متغیر های الگوریتم را در پایان تکرار می دهد. اجازه دهید جزئیات را در چند مرحله توضیح دهیم.

- در مرحله مقدار دهی ، به طور معمول مسیر های کم هزینه از u به پیوند های مستقیم مجاور یعنی x , v و w شناخته می شوند و به ترتیب ۲, ۱ و ۵ مقدار دهی می شوند. توجه خاص به این موضوع داشته باشید که ارزش (مقدار) w عدد ۵ تعریف شده است (اگر خواهیم دید که کم هزینه ترین مسیر در واقع وجود ندارد) به این دلیل که وقتی لینک u به w مقدار مستقیم است. مقدار های y و z بینهایت تعریف می شود زیرا آنها ارتباط مستقیم با u ندارند.
- در تکرار اول ، می بینیم که در میان گره ها هنوز هیچ کدام به مجموعه N′ اضافه نشده و هیچ گره کم هزینه ای در پایان تکرار قبلی پیدا نشده. گره x با مقدار ۱ کم مقدار ترین است پس به مجموعه N′ اضافه می شود. خط ۱۲ از الگوریتم LS به روز رسانی D(v) از همه گره های v را به عهده دارد و نتایج را در خط دوم (مرحله ۱) جدول ۴,۳

www.it98.ir

می ریزد. مقدار مسیر v غیر قابل تغییر است ، مقدار مسیر w (جایی که در پایان مقدار دهی ۵ بود) از طریق گره x مقدار ۴ را به خود می گیرد. از این رو مسیر دارای پایین ترین مقدار انتخاب شده و مقدار سابق w همراه کوتاه ترین مسیر از u به x پیدا می شود. به طور مشابه ، مقدار y (از طریق x) ۲ محاسبه می شود و در نتیجه جدول به روز می شود.

- در تکرار دوم ، گره های v و y به عنوان کم هزینه ترین مسیرها (۲) پیدا می شوند و ما رابطه را به دلخواه قطع می کنیم و y نیز به مجموعه N′ اضافه می شود ، اکنون مجموعه N′ شامل u , x و y است. مقادیر باقیمانده گره های هنوز در مجموعه N′ نیستند ، یعنی گره های v , w و z .

جدول ۴,۳

step	N′	D(v),p(v)	D(w),p(w)	D(x),p(x)	D(y),p(y)	D(z),p(z)
0	u	2,u	5,u	1,u	∞	∞
1	ux	2,u	4,x		2,x	∞
2	uxy	2,u	3,y			4,y
3	uxyv		3,y			4,y
4	uxyvw					4,y
5	uxyvwz					

Table 4.3 ♦ Running the link-state algorithm on the network in Figure 4.27

با به روز شدن در خط ۱۲ الگوریتم LS ، نتایج در ردیف سوم جدول ۴,۳ ریخته می شوند.

- و غیره ... .

وقتی که الگوریتم LS به پایان می رسد ، برای هر گره ، مسیر قدیمی اش را در امتداد مسیر کم هزینه گره مبدا ، خواهیم داشت. برای هر کدام از مسیر های قدیمی ، همواره مسیر قدیمی دیگری نیز وجود دارد ، بنابراین در این وضعیت ما می توانیم یک مسیر کامل از مبدا به تمامی مقصد ها ایجاد کنیم. جدول ارسال در یک گره ، مثل گره u ، می تواند توسط اطلاعات ذخیره شده اش برای هر مقصد ، لبه بعدی گره را از مسیر کم هزینه u به مقصد ایجاد کند. تصویر ۴,۲۸ فهرست نتایج مسیر های کم هزینه و جدول های ارسالی از گره u را در شبکه ی تصویر ۴,۲۷ نمایش می دهد.

پیچیدگی محاسباتی این الگوریتم چیست ؟ یعنی ، الگوریتم n گره می گیرد (بدون شمارش مبدا) چند محاسبه باید انجام شود که در بدترین حالت مسیرهای کم هزینه از مبدا به تمام مقصد ها پیدا شود ؟ در تکرار اول ،میان تمام n گره برای تعیین گره w که با وجود کمترین مقدار در مجموعه N′ نیست ، جستجو می کنیم. در تکرار دوم ، میان n-1 گره برای یافتن کمترین مقدار جستجو می کنیم. در تکرار سوم ، میان n-2 گره و به همین ترتیب...

wWw.it98.ir

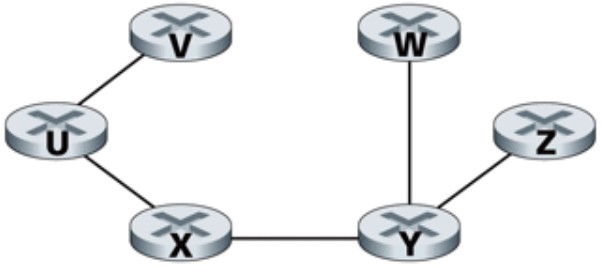
www.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

. در نهایت مقدار کل گره های که ما نیاز به جستجو در میان تمام تکرارها داریم برابر n(n+1)/2 می باشد ، بنابراین پیاده سازی الگوریتم LS در بدترین حالت ممکن ، دارای پیچیدگی مربع n یا $O(n^2)$ می باشد.(پیاده سازی پیچیده تر این الگوریتم ، استفاده از ساختار دادهای است ، که می تواند مقدار مینیمم را در خط ۹ به صورت الگوریتمی پیدا کند ، که این حالت سریع تر از دفعات خطی است، بنابراین پیچیدگی را کاهش می دهد.)

بعد از کامل شدن بحث ما در مورد الگوریتم LS ، اجازه دهید در مورد آسیب به وجود آمده توضیح دهیم.تصویر ۴,۲۹ نمایشی از یک شبکه ساده جغرافیایی است که تمام مسیر های آن دارای ارزش یکسان هستند ، برای مثال به صورت تاخیری بار گذاری می شوند. در این مثال ارزش لینک ها برابر نیست ؛ یعنی c(u,v) برابر است با c(v,u) فقط اگر هر دو لینک (u,v) به طور مشابه مستقیما بارگذاری شوند. در این مثال گره z واحد شروع مقصد گره w است،

Figure 4.28



Destination	Link
v	(u, v)
w	(u, x)
x	(u, x)
y	(u, x)
z	(u, x)

Figure 4.28 ♦ Least costs paths and forwarding table for nodule u

همچنین گره x نیز واحد شروع مقصد w می باشد ، گره y نیز مقداری برابر e وارد مسیر ترافیکی می کند که مقصد آن w می باشد. مسیر ابتدایی نمایش داده شده در تصویر 4.29(a) ارزش لینک ها بربر با مقدار ترافیک حمل شده است.

وقتی الگوریتم LS در اجرای بعدی ، گره y را محاسبه می کند (مستقر در ارزش لینک که در تصویر 4.29(a) نمایش داده شده)مسیر جهت عقربه ای ساعت به w مقدار ۱ به خود می گیرد ، به علاوه در مسیر مخالف عقربه ساعت مسیر w (در زمان استفاده) مقدار 1+e به خود می گیرد.از این رو مسیر کم هزینه از y به w در جهت عرقبه ساعت است. به طور مشابه گره x محاسبه می شود و کم هزینه ترین مسیرش به w در جهت عقربه ساعت است، نتیجتا ارزش ها در تصویر 4.29(b) نمایش داده شده. در اجرای بعدی الگوریتم LS گره های x , y و z به گره w ذر جهت مستقیم خلاف عقربه ساعت همه مسیر ارزش صفر را به خود می گیرند و تمام مسیر ترافیکی خود را به مسیر خلاف عقربه ساعت تبدیل می کنند. در اجرای بعدی الگوریتم LS گره های x , y و z مسیر ترافیکی خود را به جهت عقربه های ساعت تبدیل می کنند.

www.it98.ir

چگونه می توانیم برای جلوگیری از این گونه نوسانات انجام دهیم ؟ (این اتفاق در تمام الگوریتم ها موقع ازدحام یا تاخیر مسیر لینک رخ می دهد و مختص الگوریتم LS نیست.) یک چاره برای این مشکل می تواند این باشد که ارزش لینک ها به مقدار بار حمل شده ترافیکی آنها بستگی ندارد – این چاره غیر قابل قبول می شود زمانی که یکی از هدف های مسیر یابی برای اجتناب از تراکم بالای لینک ها (برای مثال ، تاخیر بالا) کنار گذاشته می شود- . چاره دیگر این مشکل ، اطمینان از اینکه تمامی روتر ها با هم در یک زمان مشابه الگوریتم LS را اجرا نکند. این راه حل به نظر منطقی تر می آید، زمانی که حتی اگر تمام روتر ها الگوریتم LS را در یک دوره تناوب اجرا کرده باشند، لحظه اجرا شدن الگوریتم در هر کدام از گره ها در یک زمان مشابه نباشد. به طور قابل توجهی ، محققان دریافتند که روترها می توانند خودهماهنگی بین خودشان ایجاد کنند [Floyd Synchronization 1994] . یعنی حتی با وجود اینکه الگوریتم در یک دوره زمانی مشابه اجرا می شود ولی در لحظه های مختلف این اجرا به عمل می آید ، لحظه اجرای الگوریتم می تواند در نهایت ، همزمان در روترها تبدیل و باقی بماند. یک راه برای جلوگیری از خود هماهنگ سازی روتر ها این است که برای هر روتر زمان فرستادن اطلاعات را تصادفی کنیم.

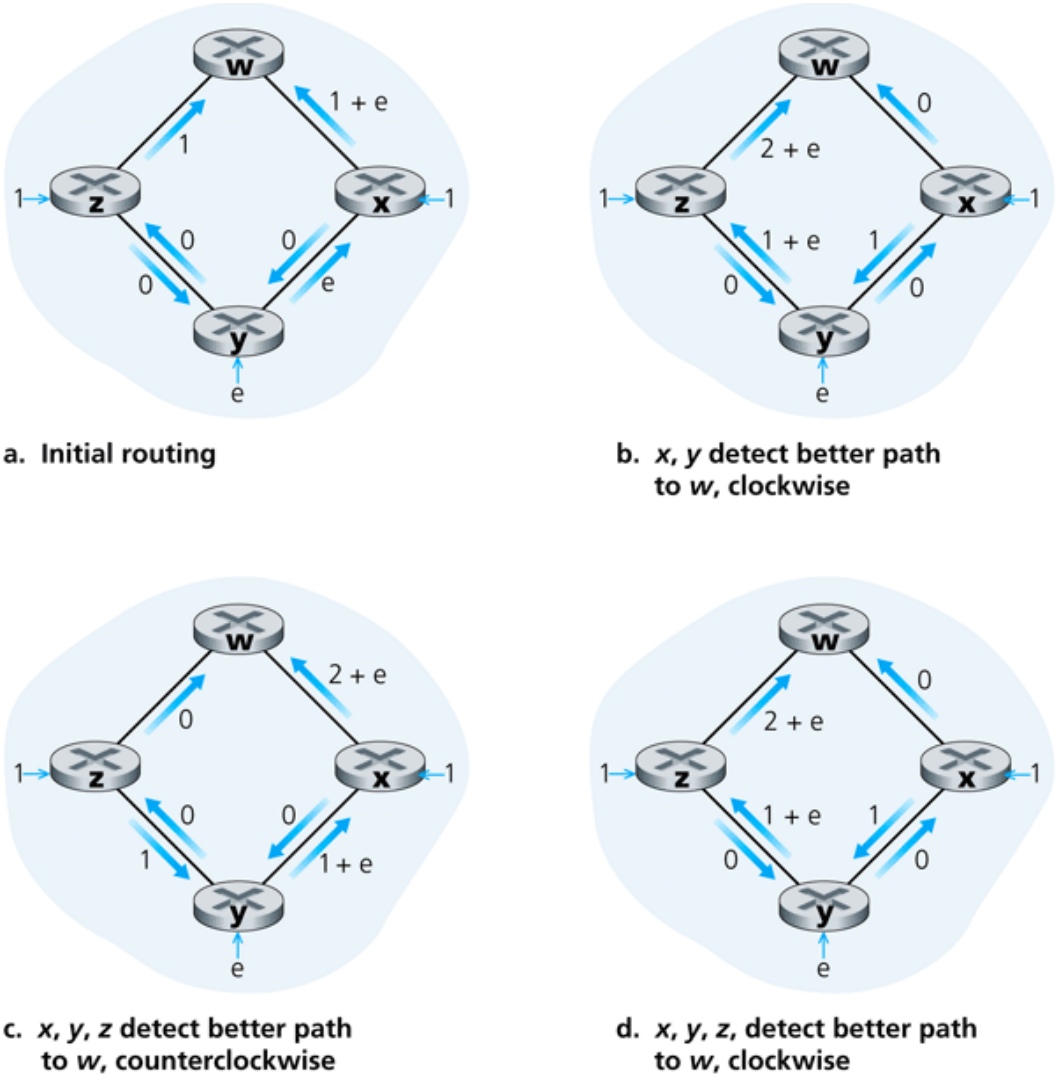
در مورد الگوریتم LS آموختیم ، اجازه دهید در مورد الگوریتم بزرگ دیگری که امروزه مورد استفاده قرار می گیرد توضیح دهیم – الگوریتم مسیر یابی بردار مسافت (Distance-Vector Routing Algorithm)

Figure 4.29

www.it98.ir

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir



a. Initial routing

b. *x, y* detect better path to *w*, clockwise

c. *x, y, z* detect better path to *w*, counterclockwise

d. *x, y, z*, detect better path to *w*, clockwise

Figure 4.29 ♦ Oscillations with congestion-sensitive routing

www.it98.ir

۴,۵,۲ الگوریتم مسیر یابی Distance-Vector(DV)

از آنجایی که الگوریتم LS الگوریتم استفاده کننده از اطلاعات سراسری بود ، الگوریتم DV لگوریتمی تکرار شونده ، ناهماهنگ و توزیع شده است. به این دلیل توزیع شده است که هر گره مقداری اطلاعات از یک یا چند پیوند مستقیم مجاورش دریافت می کند ، سپس محاسبه ای انجام می دهد و نتایج محاسبه شده اش را به مجاورینش تقسیم (توزیع) می کند. تکرار شونده است به این دلیل که ، فرآیند الگوریتم تا وقتی که هیچ اطلاعاتی بین مجاورین ردو بدل نشود ادامه پیدا می کند. (به طور قابل توجه ، الگوریتم همچنین خود پایان دهنده است – یعنی هیچ دستوری برای توقف محاسبات وجود ندارد ، خودش متوقف می شود-). ناهماهنگ است زیرا ، این الگوریتم از گره ها درخواست نمی کند که پشت سر هم ، به همدیگر متصل شوند. خواهیم دید که الگوریتم ناهماهنگ، تکرار شونده ، خود پایان پذیر و توزیع شده خیلی جالب تر و سرگرم کننده تر از الگوریتم متمرکز است !

قبل از معرفی الگوریتم DV ، ثابت خواهد شده که بحث درمورد یک رابطه مهم که میان ارزش های مسیر های کم هزینه وجود دارد ، سومند خواهد بود. $d_x(y)$ را برابر ارزش مسیر کم هزینه از گره x به y قرار می دهیم. بنابراین کم هزینه ترین مسیر از رابطه مشهور Bellman-Ford اینگونه تعریف می شود :

$$d_x(y) = min_v\{c(x,y)+ d_v(y)\} \qquad (4.1)$$

min_v در تساوی تمام مجاورین گره x را می گیرد. رابطه Bellman-Ford درک سریع تری دارد. در واقع بعد از ارسال از x به y ، اگر ما مسیر کم هزینه را از v به y در نظر بگیریم ، برای ارزش مسیر خواهیم داشت $c(x,y)+ d_v(y)$. بعد از این ، ما باید ارسال به چند مجاور v را شروع کنیم ، که کمترین ارزش از x به y کوچکترین مقدار $c(x,y)+ d_v(y)$ می باشد ، که برای تمام مجاورین به همین نحو عمل می شود.

اما برای آن دسته از کسانی که ممکن است در مورد صحت این رابطه تردید داشته باشند ، تصویر 4.27 را از گره مبدا u و گره مقصد z بررسی می کنیم. گره مبدا u سه مجاور دارد یعنی گره های v , x و w . با گردش در امتداد مسیر های مختلف در نمودار ، به راحتی می توان دریافت $d_v(z) = 5$, $d_x(z) = 3$ و $d_w(z) = 3$ است. این مقادیر را به رابطه 4.1 وارد می کنیم ، همین طور ارزش های c(u,v)=2 , c(u,x)=1 و c(u,w)=5 را به معادله می دهیم، که نتیجه می دهد $d_u(z) = min$ {2+5 , 5+3 , 1+3}=4 ، جوابی که بدیهی است که صحیح است و دقیقا همان جوابی را به ما می دهد که الگوریتم Dijskstra در شبکه ای مشابه به ما می دهد. این بازبینی ساده و سریع باید باعث شده باشد که هر تردید شما در رابطه با این معادله برطرف شده باشد.

معاذله Bellman-Ford فقط دارای یک کنجکاوی فکری نیست. بلکه دارای یک اهمیت عملی است. به خصوص ، رابطه Bellman-Ford راه حل جدول ارسال گره x را فراهم می کند. v* را به هر گره مجاورش که می رسد کمترین مقدار را در رابطه ۴,۱ می گذاریم. پس اگر گره x بخواهد بسته ای را به گره y در امتداد کم هزینه ترین مسیر ارسال کند ، ابتدا باید بسته را به گره v* ارسال کند. بنابراین جدول ارسالی گره x به عنوان مسیر بعدی گره v* برای رسیدن به مقصد نهایی y تعیین می شود. دیگر کاربرد مهم رابطه Bellman-Ford ، همکاری است ، به طوری که مجاور به مجاور درخواست برقراری ارتباط می دهد که این بخشی از الگوریتم DV است.

نظریه اساسی را مطرح می کنیم . هر گره x که با $D_x(y)$ شروع می شود ، ارزش های مسیر های کم هزینه از خودش به گره y را در تمام گره های موجود در N ارزیابی می کند. بردار مسافت گره x را مقدار D_x = [$D_x(y)$: y in N] می گذاریم ، جایی که بردار ارزش تمام گره ها از x به y در N ارزیابی شده است. با الگوریتم DV ، هر گره x اطلاعات مسیر ارسالی را نگهداری می کند :

- برای هر مجاور v ، ارزش c(x,y) از مجاور مستقیم پیوست شده از x به v قرار دارد
- بردار مسافت گره x ، یعنی D_x = [$D_x(y)$: y in N] ، شامل ارزیابی تمام ارزش ها از خودش به y در N است

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

- بردار مسافت هر کدام از مجاورین ، یعنی D_x[D_v(y): y in N] = ، برای هر کدام از مجاورین x به v است

در تقسیم ، الگوریتم ناهماهنگ ، هر دفعه ، هر گره کپی(نمونه) بردار مسافت خود به مجاورینش را ارسال می کند. وقتی که گره ط یک بردار مسافت جدید از هر کدام از مجاورین گره v دریافت می کند ، بردار مسافت را ذخیره کرده و پس از استفاده از رابطه Bellman-Ford بردار مسافت به روز شده خود را ارسال می کند :

برای هر گره y در N داریم $D_x(y) = min_v\{c(x,y)+ D_v(y)\}$

اگره بردار مسافت گره x در مرحله بروز رسانی تغییر کند ، گره x بردار مسافت بروز شده اش را به مجاورینش ارسال می کند ، و دوباره می تواند بردار مسافت خود را بروز کند. به اندازه کافی حیرت آورست ، اینکه تمام گره ها به مبادله بردارهای مسافت خود در یک روش ناهماهنگ ادامه می دهند، هر ارزش ارزیابی شده $D_x(y)$ به $d_x(y)$ ، ارزش واقی مسیر کم هزینه از گره x به گره y تفاوت پیدا می کند [Bertsekas 1991] !

شبه کد الگوریتم DV

در الگوریتم DV ، گره x بردار مسافت بروز شده اش را وقتی که ببیند ارزش یکی از لینک های مستقیم پیوند شده اش تغییر کرده یا از چند مجاورش بروز شده بردار مسافت دریافت کند ، ارزیابی می کند. اما برای بروز رسانی جدول ارسالی اش برای فرستادن به مقصد y ، گره x چه نیازی به دانستن مسافت کوتاه ترین مسیر به y است ، در عوض مجاورین گره v*(y) در امتداد روتر بعدی کوتاه ترین مسیر به y هستند. شاید پیش بینی کند که روتر بعدی v*(y) مجاور v است که در خط ۱۴ الگوریتم DV کمترین مقدار را بدست می آورد. (اگر چند مجاور v وجود داشته باشد همگی آنها کمترین مقدار به خود می گیرند ، بنابراین v*(y) متواند هر کدام از این مقادیر مجاور ها را به خود بگیرد.) پس در خط ۱۳ و ۱۴ ، برای هر مقصد y ، گره x همواره جدول ارسالی بروز شده v*(y) را برای مقصد y ارزیابی می کند.

فرخوانی در الگوریتم LS که یک الگوریتم سراسری است به این نحوه است که ابتدا قبل از شروع الگوریتم Dijkstra از هر گره بدست آوردن نقشه کامل شبکه را درخواست می کند. الگوریتم DV یک الگوریتم نا متمرکز است و از اطلاعات سراسری استفاده نمی کند. در وقاع تنها اطلاعات یک گره ارزش لینک های مستقیما پیوست شده اش به مجاورانش است و این اطلاعات را از مجاورانش بدست می آورد. هر گره منتظر بروز رسانی از هر مجاورش می شود (خط ۱۰-۱۱) ، بردار مسافت جدیدش را بعد از دریافت بروز رسانی، محاسبه می کند (خط ۱۴) و بردار مسافت جدیدش را بین مجاورانش توزیع می کند (خط ۱۶-۱۷) . شبه کد الگوریتم DV در بسیاری از پروتکل های مسیر یابی که شامل RIP و BGP اینترنت , ISO IDRP , Novell IPX و ARPAnet اصلی می شوند ، استفاده می شود.

www.it98.ir

تصویر ۴,۳۰ فرایند الگوریتم DV را برای یک شبکه ساده دارای سه گره که در تصویر مشخص شده ، شرح می دهد. فرایند الگوریتم یک وضعیت ناهماهنگ را نشان می دهد، جایی که تمام گره ها در یک زمان بردار مسافت را از مجاورینشان دریافت می کنند، بردار مسافت جدید را محاسبه می کنند و به مجاورینشان بردار مسافت جدیدشان را اطلاع می دهند. بعد از مطالعه این مثال شما باید خود را متقاعد کرده باشید که این الگوریتم دارای یک وضعیت ناهماهنگ است ، که هر گره افزایش/پذیرش درخواست را در هر لحظه محاسبه و بروز می کند.

سمت چپ ترین ستون تصویر جدول مسیر یابی ابتدایی برای هر کدام از سه گره را نمایش می دهد. برای مثال ، جدول گوشه سمت چپ بالا متعلق به جدول مسیر یابی ابتدایی گره x است. در داخل یک جدول مسیر یابی مشخص ، هر ردیف یک بردار مسافت است – به ویژه ، هر کدام از جدول های مسیر یابی گره ها شامل بردار مسافت آن گره و تعداد مجاورانش می شود – بنابر این اولین ردیف در جدول ابتدایی مسیر یابی گره x برابر است با مقدار D_x=[0,2,7]=$[D_x(x), D_x(y), D_x(z)]$. ردیف دوم و سوم این جدول به ترتیب ، جدیدترین بردار های مسافت دریافت شده از گره y و z است. به این دلیل که در مقدار دهی گره x هیچ چیزی از گره های y یا z دریافت نشده ، مقدار اولیه ردیف دوم و سوم بینهایت تعریف می شوند.

بعد از مقدار دهی ، هر گره بردار مسافت خود را به دو گره مجاور خود ارسال می کند. این حالت در تصویر ۴,۳۰ با پیکان (فلش) از ردیف اول جدول ها به ردیف دوم مشخص شده است. برای مثال ، گره x بردار مسافت خود را یعنی D_x=[0,2,7] به دو گره y و z ارسال می کند. بعد از دریافت بروز رسانی ، هر گره دوباره بردار مسافتش را محاسبه می کند. برای مثال ، گره x اینگونه محاسبه می کند :

$$= 0 D_x(x)$$
$$= \min \{c(x,y)+ D_y(y) , c(x,z)+ D_z(y)\} = \min \{2+0 , 7+1\}=2 D_x(y)$$
$$= \min \{c(x,y)+ D_y(z) , c(x,z)+ D_z(z)\} = \min \{2+1 , 7+3\}=3 D_x(z)$$

wWw.it98.ir

- امنیت . مبادلات بین روترهای OSPF (به عنوان مثال، به روز رسانی های state-link) می توانند تأیید گردند. با تأیید، تنها روترهای مورد اعتماد می توانند در پروتکل OSPF از طریق یک AS شرکت داده شوند، بنابراین جلوگیری از بدخواهان سرزده (یا دانشجویان شبکه که دانش نوظهور خود را می خواهند برای خوشگذرانی بکار گیرند!) از تزریق اطلاعات غلط به لیستهای روتر قابل انجام است. بصورت قراردادی، پکهای OSPF بین روترها تأیید نمی گردند و قابل جعل شدن هستند. دو نوع تأییدیه قابل تنظیم هستند—ساده و MD5 (فصل ۸ در رابطه با تاییدیه MD5 و تأیید به شکلی کلی بحث می کند). در تأیید ساده، رمز بر روی هر روتر تنظیم گردیده است. زمانی که یک روتر یک بسته OSPF می فرستد، این بسته شامل رمز می باشد که دستکاری نشده است. واضح است که تأیید از نوع ساده ی آن بسیار امن نیست. تأیید از نوع MD5 بر اساس یک سری از کلمات کلیدی محرمانه به اشتراک گذاشته شده است که در همه ی روتر ها تنظیم شده است. برای هر بسته ی OSPF که فرستاده می شود، روتر هش MD5 محتویات بسته ی OSPF که به کلید محرمانه اضافه شده است را محاسبه می کند. (مبحث کدهای تأیید پیغام در فصل ۷ را مطالعه فرمایید.) سپس روتر حاوی ارزش هش نهایی (resulting hash value) موجود در بسته ی OSPF می شود. روتر دریافتگر، که از کلید محرمانه پیش شکل یافته استفاده می کند، یک هش MD5 از بسته را محاسبه و آن را با ارزش هش که بسته به همراه دارد مقایسه می کند و بدین گونه تأییدیه ی بسته مورد پذیرش قرار می گیرد. شماره های متوالی همچنین با تأییدیه ی MD5 نیز مورد استفاده قرار می گیرند تا در برابر حملات (replay attacks) حمایت گردند.
- مسیرهای هم ارزش چندگانه (Multiple same-cost paths). زمانی که مسیرهای مختلف به یک مقصد، ارزش یکسانی داشته باشند، OSDF به چندین مسیر مختلف اجازه می دهد که مورد استفاده قرار گیرند (در زمانی که مسیرهای مختلف با ارزش یکسان موجود باشند یک مسیر به تنهایی نمی تواند انتخاب شود تا تمام ترافیک را حمل کند).
- پشتیبانی مجتمع برای مسیریابی یونیکست و مالتیکست (Integrated support for unicast and multicast routing). OSPF مالتی کست (MOSPF) [RFC 1584] پسوندهای ساده ای برای OSPF ایجاد می کند تا برای مسیریابی مالتی کست آماده گردد (موضوعی که ما بصورت عمیق تر در فصل 2.7.4 به آن می پردازیم). MOSPF از بانک داده لینک OSPF موجود استفاده می کند و یک نوع جدید از آگهی state-link به مکانیزم داده پراکنی OSPF اضافه می کند.
- پشتیبانی برای سلسله مراتب از راه یک دامین تک مسیریابی . شاید مهمترین پیشرفت در OSPF قابلیت این باشد که یک سیستم خودگردان را بصورت سلسه مراتبی پی ریزی کند. فصل 3.5.4 قبلا در مورد بسیاری از پیشرفتهای مربوط به ساختارهای مسیریابی (مسیریابی، routing) سلسله مراتبی نگاه کرده است. ما پیاده سازی مسیریابی سلسله مراتبی OSPF را در باقی این فصل پوشش خواهیم داد.

یک سیستم خودگردان OSPF می تواند در نواحی مختلفی قابل تنظیم باشد. هر ناحیه الگوریتم مسیریابی مخصوص به خود را اجرا می کند، همراه با هر روتر در یک ناحیه که link state خود را به تمام روترهای دیگر در آن ناحیه منتشر می کند. جزئیات داخلی یک ناحیه اینگونه برای تمام روترهای خارجی ناحیه مخفی می ماند. مسیریابی داخلی (Intra-area routing) تنها شامل آن روترهایی که در محدوده ی آن ناحیه هستند می باشد.

wWw.it98.ir

در داخل هر ناحیه، یک یا تعدادی روترهای مرزی ناحیه مسئول مسیریابی بسته های خارج از محدوده می باشند. نقش اولیه ناحیه ی backbone این است که ترافیک بین نواحی دیگر در سیستم خودگردان (AS) را مسیر دهی کند. Backbone همیشه حاوی تمامی روترهای مرزی ناحیه ای در سیستم خودگردان می باشد و بعلاوه می تواند حاوی روترهای غیرمرزی ناحیه ای هم باشد. مسیریابی بین ناحیه ای (area routing-Inter) در داخل سیستم خودگردان نیاز به این دارد که بسته ابتدا به یک روتر مرزی ناحیه ای (area routing-intra)، سپس در میان backbone به روتر مرزی که در ناحیه ی مقصد قرار دارد، و سپس به مقصد نهایی مسیر دهی گردد.

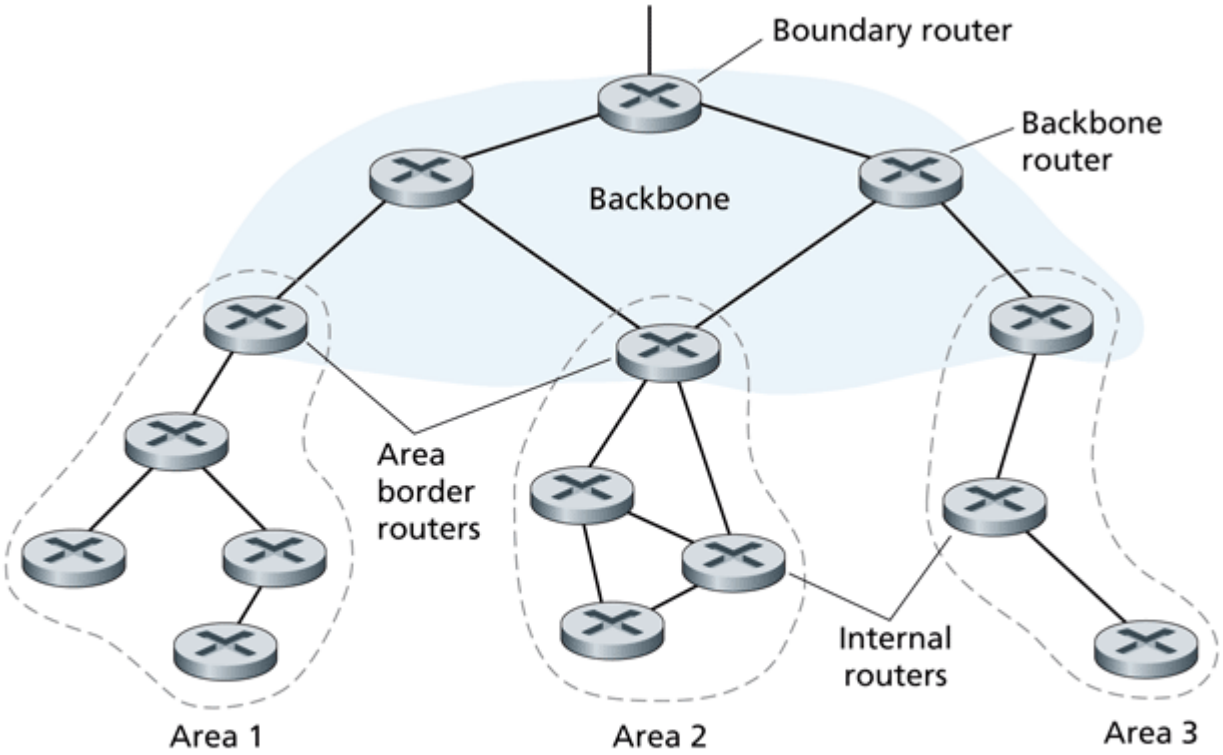


Figure 4.40 ♦ Hierarchically structured OSPF AS with four areas

تصویر ۴,۴۰: ساختار سلسله مراتبی سیستم خودگردان OSPF با چهار ناحیه

نموداری از یک ساختار سلسله مراتبی شبکه ی OSPF در تصویر 40.4 نشان داده شده است. ما می توانیم چهار نوع روتر OSPF در این تصویر مشخص کنیم:

- روترهای داخلی (Internal routers). این روترهای در نواحی backbone قرار دارند و فقط مسیریابی داخلی سیستم خودگردان را انجام می دهند.
- روترهای مرزی ناحیه ای. این روترها هم به ناحیه و هم به backbone تعلق دارند.
- روترهای Backbone (روترهای غیرمرزی). این روترها مسیریابی درون backbone را انجام می دهند اما خود روترهای مرزی نیستند. در میان یک ناحیه ی غیر backbone، روترهای داخلی ///
- روترهای کرانه ای (Boundary routers). یک روتر کرانه ای اطلاعات مسیریابی را با روترهایی که به

www.it98.ir

سیستمهای خودگردان دیگر تعلق دارند مبادله می کند. این روتر ممکن است بعنوان مثال از BGP برای انجام مسیریابیهای AS های داخلی استفاده کند. در واقع از طریق یک چنین روتر کرانه ای است که دیگر روترها از مسیرهای مربوط به شبکه های خارجی اطلاع می یابند.

OSPF یک پروتکل نسبتا پیچیده ای است و مطالب گفته شده در اینجا ضرورتاً مختصر است؛
منابع زیر شامل جزئیات اضافی تری می باشند:
[Huitema 1998; Moy 1998; RFC 2328]

اصول در عمل (PRINCIPLES IN PRACTICE)

چینش وزنهای لینک OSPF

بحث ما درباره ی مسیریابی state-link بطور ضمنی فرض می کرد که وزنهای لینک چیده شده اند، یک الگوریتم مسیریابی (مسیریابی) همانند OSPF در حال اجراست، و ترافیک بر اساس جداول مسیریابی محاسبه شده توسط الگوریتم LS گردش می کند. در شرایط کنش و واکنش، وزنهای لینک تعیین می گردند (مثلا آنها ابتدا می آیند) و نتیجه (از طریق الگوریتم Dijkstra) در مسیرهای مسیریابی حاصل این می شود که هزینه ی کل کاهش یابد.

عملاً رابطه ی کنش و واکنش بین وزنهای لینک و مسیرهای مسیریابی ممکن است معکوس گردد، بوسیله ی گردانندگان شبکه می توان وزنهای لینک را تنظیم کرد تا مسیرهای مسیریابی که اهداف مهندسی ترافیک خاصی را بدست می دهند، را بدست آورد [Fortz 2000, Fortz 2002]. بعنوان مثال، یک مدیر شبکه را در نظر بگیرید که تخمینی از کشش ترافیک وارد شونده به شبکه در هر نقطه ی ورود و مقصد برای هر نقطه ی خروج را دارد. مدیر سپس ممکن است در جایی یک روتر مشخص جریان ورود و خروج که حداکثر بکارگیری کلی از تمام لینکهای شبکه را به حداقل می رساند، قرار دهد. اما با یک الگوریتم مسیریابی همانند OSPF، knobهای اصلی اپراتور برای میزان سازی مسیریابی جریانها در شبکه وزنهای لینک هستند. بنابراین، برای اینکه به این هدف برسد که بکارگیری حداکثری لینک را محدود کند، باید جهت وزنهای لینک که او را به این هدف می رساند را بیابد. این یک واژگونی رابطه علت و معلولی است – مسیریابی (مسیریابی) مطلوب جریانها معلوم است و وزنهای لینک OSPF باید پیدا شوند که الگوریتم مسیریابی OSPF در این مسیریابی مطلوب جریانها نتیجه گردد.

4.6.3 مسیریابی Inter-AS : BGP

تا کنون فقط یاد گرفتیم که چگونه ISPها از OSPF و RIP برای تشخیص مسیرهای مطلوب برای جفتهای مقصد که نسبت به AS مشابه داخلی هستند، استفاده می کنند. اجازه دهید امتحان کنیم که چگونه مسیرها برای جفت های مقصد منبع (Source-destination) که چندین ASرا وصل می کنند، تعیین می شوند.

پروتکل دروازه ای مرزی نسخه ی ۴ که در RFC 4271 تعریف شده است (همچنین ببینید [RFC 1772;

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

[RFC 1773) در اینترنت امروزی بعنوان پروتکل مسیریابی inter-AS استاندارد فعال می باشد. BGPبعنوان یک پروتکل مسیریابی inter-AS (بخش 4.5.3 را ببینید)، هر AS را برای اهداف زیر بکار می گیرد:

۱- دریافت اطلاعات دسترسی زیرشبکه ای از ASها مجاور
۲- ابلاغ اطلاعات دسترسی به همه ی روترهای داخلی AS
۳- شناسایی روترهای "خوب" ("good") به زیرشبکه بر اساس اطلاعات دسترسی و سیاست AS.

مهمتر از همهBGP به هر شبکه این اجازه را می دهد تا به بقیه ی اینترنت وجود خود را ابلاغ کند. یک زیرشبکه فریاد می زند که "من وجود دارم و همین جا هستم!" و BGP اطمینان حاصل می کند که همه ی ASها در اینترنت از وجود زیرشبکه اطلاعا دارند و می دانند که چگونه به آن دسترسی پیدا کنند. اگر این وظیفه بر عهده ی BGP نبود هر شبکه باید ایزوله می ماند -- تنها و ناشناخته از بقیه ی اینترنت.

مبانی BGP

BGP بسیار پیچیده است؛ تمامی کتابهای اختصاص داده شده به موضوع و بسیاری نشریات هنوز هم بخوبی قابل فهم نیستند [Yannuzzi 2005]. بعلاوه بعنوان یک طراح یا مدیر یک ISP از نوع upper-tier حتی با خواندن کتابها و منابع (RFCها) ممکن است برای شما سخت باشد که بر BGP بدون ماه ها تمرین کردن مسلط شوید. با این وجود به دلیل اینکه BGP یک پروتکل حیاتی برای اینترنت است -- در اصل این پروتکلی است که همه چیز را با هم می چسباند-- ما نیاز داریم که حداقل یک درک ابتدایی در مورد اینکه این پروتکل چگونه کار می کند داشته باشیم. ابتدا به شرح چگونگی کارکرد BGP در شبکه ی مثال ساده ی ما در مباحث قبل که در تصویر 4.32 موجود است می پردازیم. در این مبحث ما بحث خود را بر اساس مسیریابی سلسله مراتبی بنا نهادیم، در بخش 4.5.3 شما را به خواندن دوباره ی مطلب تشویق می کنیم.

در BGP، جفت روترها اطلاعات مسیریابی را از طریق کانکشن های نیمه دائم TCP با استفاده از پورت 179 مبادله می کنند. کانکشنها ی نیمه دائم TCP برای شبکه ی تصویر 4.32 در تصویر 4.41 نشان داده شده اند. کانکشن BGP TCP از این نوع معمولا در هر لینک که مستقیماً دو روتر را در هر ASمتفاوت متصل می کند وجود دارد؛ بنابراین در تصویر 4.41 یک کانکشن TCP بین روترهای دروازه ای 3a و 1c و یک کانکشن TCP دیگری بین روترهای دروازه ای 1b و 2a وجود دارد. همچنین در داخل ASبین روترها کانکشن های BGP TCP نیمه دائم وجود دارند. در حالت خاص تصویر 4.41 تنظیمات معمولی یک کانکشن TCP برای هر جفت روتر داخلی یک AS را نشان می دهد که یک بافت از کانکشن های TCPدر هر AS ایجاد کرده اند. برای کانکشن TCP دو روتری که در انتهای کانکشن هستند همتاهای BGP (BGP peers) و کانکشن TCP بهمراه همه ی پیامهای BGP فرستاده شده از کانکشن یک جلسه ی BGP (BGP session) می گویند.

www.it98.ir

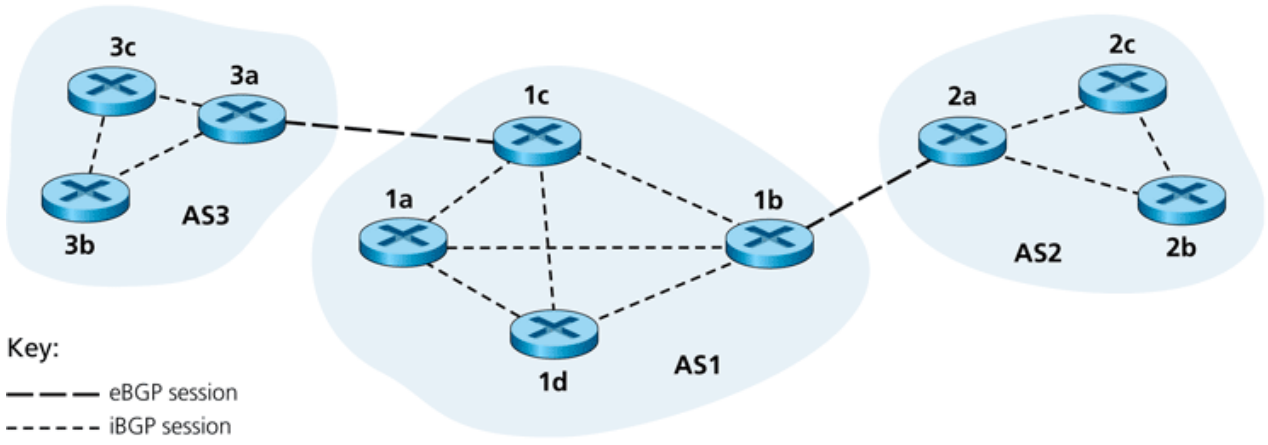


Figure 4.41 ♦ eBGP and iBGP sessions

----> تصویر 4.41 ، جلسه های eBGP و iBGP <-------

علاوه بر این، یک جلسه ی BGP که دو AS را بهم می پیوندد، یک جلسه ی BGP خارجی (eBGP session) نامیده می شود، و یک جلسه ی BGP بین روترهای همان AS یک جلسه ی BGP داخلی (iBGP session) نامیده می شود. در تصویر 4.41، جلسه های BGP خارجی با نقطه چین پررنگ نشان داده شده اند؛ جلسات BGP داخلی نیز با نقطه چینهای کم رنگ نشان داده شده اند. توجه داشته باشید که خطوط جلسه ی BGP در تصویر 4.41 همیشه متناظر با لینکهای فیزیکی در تصویر 4.32 نمی باشند.

BGP به هر AS اجازه می دهد تا آگاهی یابد که کدام مقصدها از طریق ASهای مجاورش قابل دسترس هستند. در BGP، مقصدها هاست نیستند ولی در عوض پیشوندهای CIDRized هستند، با هر پیشوند نشان دهنده ی یک زیرشبکه یا یک مجموعه از زیرشبکه ها. بنابراین به عنوان مثال، در نظر بگیرید که چهار زیر شبکه متصل به AS2 موجود می باشند: 138.16.64/24، 138.16.65/24، 138.16.66/24 و 138.16.67/24. سپس AS2 می توانسته است که پیشوند ها را برای این چهار زیرشبکه متراکم کند و از BGP استفاده کند تا پیشوند واحد 138.16.64/22 را به AS1 آگهی دهد. بعنوان مثالی دیگر فرض کنید که تنها سه تای اول از آن چهار زیرشبکه ی در AS2 هستند و چهارمین زیرشبکه، 138.16.67/24، در AS3 قرار دارد. سپس همانطور که در مقدمات و تمرین در بخش 4.4.2 توصیف کردیم، بدلیل اینکه روترها قدیمی ترین پیشوند مطابق را برای فرستادن دیتاگرامها مورد استفاده قرار می دهند، AS3 می تواند به AS1 مشخصترین پیشوند 138.16.67/24 را آگهی دهد و AS2 هنوز هم می تواند به AS1 پیشوند متراکم 138.16.64/22 را آگهی دهد.

اکنون اجازه دهید امتحان کنیم که چگونه BGP اطلاعات دسترسی به پیشوند را از طریق جلسه ی BGP نشان داده شده در تصویر 4.41 منتشر کند. همانطور که ممکن است انتظار داشته باشید، با استفاده از جلسه ی eBGP بین روترهای دروازه ای 3a و 1c، AS3 به AS1 لیست پیشوندهایی که از AS3 قابل دسترس هستند را می فرستد؛ و AS1 به AS3 لیست پیشوندهایی که از AS1 قابل دسترس هستند را می فرستد. بطور مشابه، AS1 و AS2 اطلاعات دسترسی به پیشوند را از طریق روترهای دروازه ای خود یعنی 1b و 2a مبادله می کنند. همچنین همانطور که ممکن شما نیز انتظار داشته باشید، زماین که یک روتر دروازه ای (در هر AS) پیشوندهای آگهی یافته eBGP را دریافت می کند، روتر دروازه ای جلسه های iBGP خود را مورد استفاده قرار می دهد تا پیشوندها را به روترهای دیگر

www.it98.ir

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

در AS منتشر کند. بنابراین همه ی روترها در AS1 از پیشوندهای AS3 آگاهی پیدا می کنند که شامل روتر دروازه ای 1b نیز می گردد. بنابراین روتر دروازه ای 1b (در AS1) می تواند پیشوندهای AS3 را به AS2 دوباره آگهی دهد. زمانی که یک روتر (دروازه ای یا غیر دروازه ای) از یک پیشوند جدید آگاهی می یابد، یک مدخل برای پیشوند و جدول ارسالش ایجاد می کند، همانطور که در بخش 4.5.3 توضیح داده شد.

روترهای BGP و خواص مسیر

اجازه دهید که اکنون با داشتن یک فهم پایه ای از BGP بر روی آن عمیق تر شویم (البته تا زمانی که برخی جزئیات کم اهمیت را به زیر فرش جارو می کنیم!). در BGP یک سیستم خودمختار (AS) توسط شماره ی جهانی سیستم خودمختار خود (ASN) شناخته می شود که شماره ای منحصر به فرد است [RFC 1930]. از لحاظ فنی یک AS دارای یک ASN نمی باشد. به ویژه، یک به اصطلاح AS ریشه (stub AS) که تنها ترافیک برای هر آنکه یک منبع یا مقصد باشد را حمل می کند، بطور معمول دارای یک ASN نخواهد بود؛ ما از این نکته ی فنی در بحث خود چشم پوشی می کنیم تا بخاطر درختان جنگل را بهتر ببینیم.) اعضای AS، مانند آدرس IP توسط ثبتهای ICANN منطقه ای تعیین شده اند، [ICANN 2007].

زمانی که یک روتر یک پیشوند در در سرتاسر یک جلسه ی BGP آگهی می دهد، این شامل پیشوند و یک شماره ی خاصیتهای BGP (BGP attributes) می باشد. در اصطلاحات BGP، یک پیشوند همراه با خواص خود یک مسیر (route) نامیده می شود.

بنابراین جفتهای BGP (BGP peers) روترها را به همدیگر آگهی می دهند. دوتا از مهمترین خاصیتهای AS-PATH و NEXT-HOP از قرار زیر می باشند:

- AS-PATH: این خاصیت حاوی ASهایی که در آنها آگهی برای پیشوندها انجام شده است، می باشد. زمانی که یک پیشوند به یک AS گذر کرده باشد، AS شماره ی (ASN) آن را به خاصیت AS-PATH اضافه می کند. بعنوان مثال، تصویر 4.41 را درنظر بگیرید و فرض کنید که پیشوند 138.16.64/24 در ابتدا از AS2 به AS1 آگهی داده شده است؛ اگر پس از آن AS1 پیشوند را به AS3 آگهی دهد، AS-PATH به شکل AS2 AS1 خواهد شد. روترها از خاصیت (attribute) AS-PATH استفاده می کنند تا آگهی های تکراری را شناسایی و از آنها جلوگیری کنند؛ خصوصا اگر یک روتر ببیند که AS او در لیست مسیر موجود است، آگهی را رد خواهد کرد. همانطور که بزودی بحث خواهیم کرد، روترها همچنین از خاصیت AS-PATH برای انتخاب از میان چندین مسیر به پیشوند استفاده می کنند.
- در ایجاد لینک حیاتی بین پروتکلهای مسیریابی inter-AS و intra-AS، خاصیت NEXT-HOP یک استفاده ی مهم و دقیقی دارد. *NEXT-HOP رابط روتری است که AS-PATH را شروع می کند.* برای بدست آوردن دانش لازم در خصوص این خاصیت (attribute)، اجازه دهید که دوباره به تصویر 4.41 اشاره ای کنیم. مشاهده که چه اتفاقی می افتد زمانی که روتر دروازه ای 3a در AS3 با استفاده از eBGP یک مسیر به روتر دروازه ای 1c در AS1 آگهی می دهد. مسیر شامل پیشوند آگهی داده شده است که ما نام آن را x می گذاریم، و یک AS-PATH به پیشوند.

www.it98.ir

آگهی همچنین حاوی NEXT-HOP می باشد که آدرس IP اینترفیس روتر 3a که به 1c هدایت می کند، می باشد. (یادآوری می کنیم که یک روتر چندین آدرس IP دارد که هر یک برای هر کدام از اینترفیسهایش می باشد.) اکنون مشاهده کنید که چه اتفاقی می افتد زمانی که روتر 1d در مورد این مسیر از iBGP آگاهی پیدا می کند. پس از آگاهی یافتن در مورد این مسیر به x، روتر 1d ممکن است بخواهد بسته هایی را به x در تمام طول مسیر بفرستد، به عبارت دیگر روتر 1d ممکن است بخواهد ورودی (x, l) را در جدول ارسال خود بگنجاند که l اینترفیس آن می باشد که کم ارزشترین مسیر را از 1d به روتر دروازه ای 1c شروع می کند. برای تعیین l، 1d آدرس IP را در خاصیت NEXT-HOP برای ماژول مسیریابی intra-AS خود ایجاد می کند. توجه داشته باشید که الگوریتم مسیریابی intra-AS کم ارزشترین مسیر را به همه ی زیرشبکه های متصل به روترهای AS1، شامل زیرشبکه هایی به لینک بین 1c و 3a تعیین کرده است. از این کم ارزشترین مسیر از 1d به زیرشبکه ی 1c-3a، 1d اینترفیس روتر l خود که این مسیر را شروع، سپس ورودی (x, l) را به جدول ارسال خود اضافه می کند، را تعیین می کند. واو! (در اینجا نویسنده هیجان زده شده است!) بطور خلاصه خاصیت AS-PATH توسط روترها مورد استفاده قرار می گیرد تا بشکلی صحیح جدول ارسال آنها را تنظیم کند.

تصویر 4.42 حالت دیگری را نشان می دهد که در آن AS-PATH مورد نیاز است. در این تصویر، AS1 و AS2 توسط دو لینک همتا متصل هستند. یک روتر در AS1 می تواند از دو مسیر مختلف به همان پیشوند x آگاهی یابد. این دو مسیر می توانند AS-PATH مشابه را به x داشته باشند، اما می توانند ارزش NEXT-HOP مختلفی را متناظر با لینکهای همتای مختلف داشته باشند. با استفاده از ارزش AS-PATH و الگوریتم مسیریابی intra-AS، مسیریابی می تواند ارزش مسیر را به هر کدام از لینکهای همتا تعیین کند، و سپس مسیریابی hot-potato (بخش 4.5.3) را برای شناسایی اینترفیس مناسب بکار بندد.

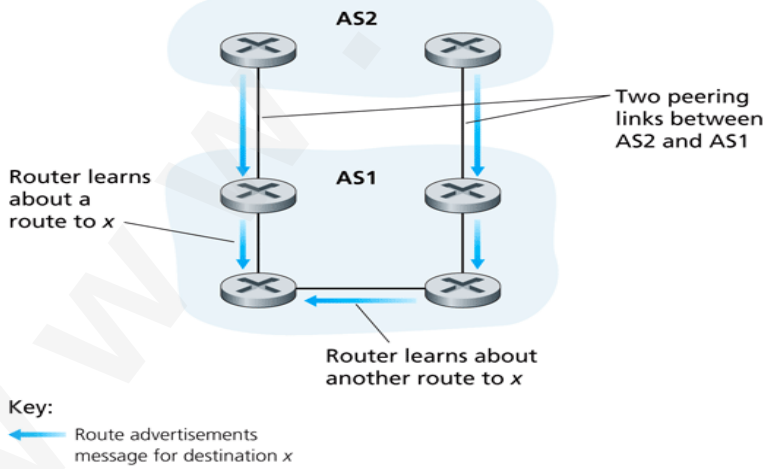


Figure 4.42 ♦ NEXT-HOP attributes in advertisements are used to determine which peering link to use.

تصویر 4.42 خواص NEXT-HOP در آگهی دادن برای تشخیص اینکه کدام لینک همتا مورد استفاده قرار بگیرد، مورد استفاده قرار می گیرند.

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

BGP همچنین حاوی خواصی است که به روترها اجازه می دهند تا متریکهای برتری را به روترها اختصاص دهند، و یک خاصیت که نشان می دهد که چگونه پیشوند در BGP در AS مبدأ قرار داده شده است. برای یک بحث کامل در مورد خواص مسیر، مراجعه کنید به [Griffin 2002; Stewart 1999; Halabi 2000; Feamster 2004; RFC 4271].

زمانی که یک روتر دروازه ای یک آگهی روتر دریافت می کند، آن روتر از سیاست ورود خود استفاده می کند تا تصمیم بگیرد که آیا قبول کند یا مسیر را فیلتر کند و اینکه آیا خواص خاصی همچون متریکهای برتری روتر را قرار دهد یا خیر. سیاست مهم ممکن است یک مسیر را فیلتر کند زیرا AS ممکن است نخواهد ترافیک را بطرف یکی از ASها در AS-PATH مسیر بفرستد. همچنین ممکن است که روتر دروازه ای یک مسیر را فیلتر کند زیرا از قبل از یک مسیر بهتر به همان پیشوند اطلاع دارد.

انتخاب مسیر BGP

همانطور که قبلا در این بخش توضیح دادیم، BGP از eBGP و iBGP استفاده می کند تا مسیرها را به همه ی روترها در داخل ASها توزیع کند. از این توزیع ممکن است یک روتر از بیش از یک مسیر به هر یک پیشوند آگاهی یابد که در این حالت روتر باید فقط یک مسیر ممکن را برگزیند. ورودیها (inputs) به این فرآیند انتخاب مسیر مجموعه ای از تمام مسیرهایی است که روتر آنها را شناخته و قبول کرده است. اگر دو و یا مسیرهای بیشتری به همان پیشوند وجود داشتند، BGP تا زمانی که تنها یک مسیر باقی بماند، پی در پی قواعد زدودگی (elimination rules) زیر را فراخوانی می کند:

•مسیرها به عنوان یکی از خواص (attributes) خود بعنوان یک ارزش اولویت محلی (local preference value) تعیین شده اند. اولویت محلی یک مسیر می توانسته توسط روتر انجام شده باشد یا می توانسته توسط روتری دیگر در همان ASمورد آگاهی واقع شده باشد. این یک تعیین سیاست است که بدست مدیر شبکه ی AS گذاشته شده است. ما به زودی در مورد مسائل مربوط به سیاست BGP با کمی جزئیات بحث خواهیم کرد.) مسیرها با بیشترین ارزش اولویت محلی انتخاب می شوند.

•از مسیرهای باقی مانده (همه با ارزش اولویت محلی یکسان)، مسیر با کمترین AS-PATH انتخاب می شود. اگر این قاعده تنها قاعده برای انتخاب مسیر بود، بنابراین BGP می بایست از یک الگوریتم DV برای تشخیص مسیر استفاده می نمود، که متریک فاصله از تعداد هاپهای AS بجای تعداد هاپهای روتر استفاده می کند.

•از مسیرهای باقی مانده (همه با ارزش اولویت محلی و طول AS-PATH یکسان)، مسیر با نزدیکترین روتر NEXT-HOP انتخاب می شود. در اینجا، نزدیکترین به این معناست که روتر برای هر قیمت کم ارزشترین مسیر، که توسط الگوریتم intra-AS مشخص گردیده، نزدیکترین می باشد. همانطور که در بخش 4.5.3 توضیح داده شد این فرآیند مسیریابی hot-potato نامیده می شود.

•اگر بیش از یک مسیر هنوز باقی مانده است، روتر تشخیص دهنده های BGP را مورد استفاده قرار می دهد تا

www.it98.ir

مسیر را انتخاب کند؛ مراجعه کنید به [Stewart 1999].

قواعد زدودگی (eliminatio rules) حتی از آنکه در بالا توضیح دادیم نیز پیچیده تر هستند. برای دوری کردن از کابوسهای شبانه! در مورد BGP بهترین راه یادگیری بیشتر در مورد قواعد انتخاب BGPدر بخشهای کوچک است.

سیاست مسیریابی

اجازه دهید مقداری از مفاهیم پایه ای سیاست مسیریابی BGP را با یک مثال ساده توضیح دهیم. تصویر 4.43 شش سیستم خودمختار بهم پیوسته را نشان می دهد: A، B، C، W، X و Y. مهم است که به این توجه کنید که A، B، C، W، X و Yسیستم خودمختار (AS) هستند نه روتر. فرض کنیم که سیستمهای W، X و Y شبکه هایی خرد هستند و اینکه A، B، و C شبکه های ارائه دهنده ی ستون فقرات (backbone) هستند. همچنین فرض می کنیم که A، B و C همه باهمدیگر همکاری می کنند و اطلاعات BGP کاملی به شبکه های مشتری خود ارائه می دهند. همه ترافیک وارد شونده به یک شبکه ی خرد (stub network) باید برای آن شبکه از قبل تعیین شده باشد، و همه ی ترافیک خارج شونده از یک شبکه ی خرد باید از آن شبکه آغاز شده باشد. واضح است که W و Y شبکه هایی خرد هستند. X تا زمانی که به بقیه ی شبکه از طریق دو ارائه دهنده ی مختلف وصل می باشد، شبکه ی خرد چند خانه ای (multi-homed stub network) است (یک سناریو که بطور فزاینده به شکلی عملی در حال عمومی شدن است). بهرحال همانند W و Y، X خود باید منبع/مقصد تمام ترافیک ورودی/خروجی به خود باشد. اما چگونه رفتار این شبکه ی خرد قابل پیاده سازی و اجرا خواهد بود؟ چگونه از X در مقابل ترافیک فرستاده شده بین B و C حمایت خواهد شد؟ اینکار با کنترل کردن رفتاری که در آن روترهای BGP آگهی می شوند، براحتی قابل اجراست. بویژه اگر X آگهی دهد (به همسایه های خود B و C) که هیچ مسیری به هیچ مقصدی جز خودش ندارد، در آنصورت بعنوان یک شبکه ی خرد عمل خواهد کرد. این به این معناست که حتی اگر X از مسیری اطلاع داشته باشد، مثلا XCY، که به شبکه ی Y می رسد، این مسیر را به B آگهی نخواهد داد. تا زمانی که B نا آگاه است که X یک مسیر به Y دارد، به هیچ وجه ترافیک معین شده به Y (یا C) را از طریق X نخواهد فرستاد. این مثال ساده توضیح می دهد که چگونه یک سیاست آگهی مسیر انتخابی می تواند برای پیاده سازی روابط مسیریابی مشتری/سرویس دهنده مورد استفاده قرار بگیرد.

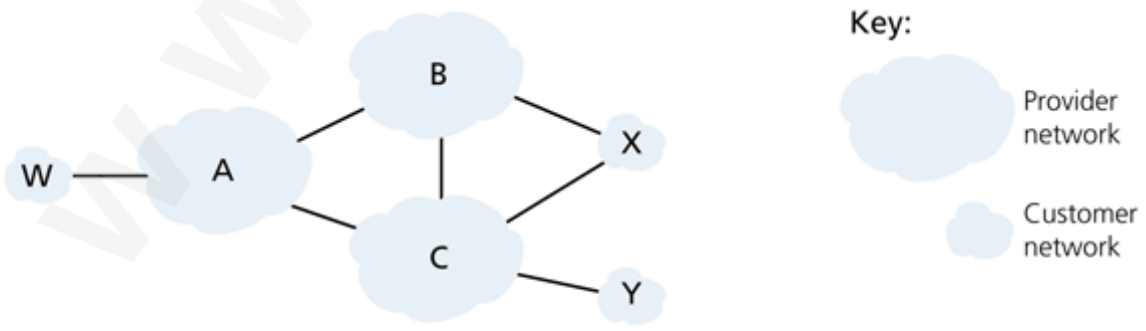


Figure 4.43 ♦ A simple BGP scenario

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

تصویر 4.43 یک سناریوی ساده ی BGP

اصول در عمل (PRINCIPLES IN PRACTICE)

چرا پروتکلهای مسیریابی INTRA-AS و INTER-AS مختلفی وجود دارند؟

اجازه دهید سپس بر یک شبکه ی ارائه دهنده تمرکز کنیم، مثلا AS B. فرض کنید که B (از A) آگاهی یافته است که A یک مسیر AW به W دارد. بنابراین Bمی تواند مسیر BAW را در مرکز اطلاعات مسیریابی خود نصب کند. واضح است که B همچنین می خواهد که مسر BAW را به مشتری خود X آگهی دهد تا اینکه X بداند که می تواند به W از طریق B مسیردهی کند اما آیا B باید مسیر BAW را به C آگهی دهد؟ اگر بله، پس Cمی تواند ترافیک را به W از طریق CBAW مسیر دهی کند. اگر A، B و C همه ارائه دهندگان ستون فقرات هستند، نسبت به B باید بطور صحیح احساس کنند که نباید بار (و هزینه!) حمل ترافیک انتقالی بین A و C را بر روی دوش کشید. B ممکن است بطور صحیح احساس کند که این کار A و C می باشد (و همینطور هزینه ی آنهاست!) که اطمینان حاصل کنند که C می تواند به/از مشتریان A از طریق یک کانکشن مستقیم بین A و C مسیر دهی کند. بطور رسمی هیچ استاندارد رسمی وجود ندارد که چگونه مسیر ISPهای ستون فقرات را فرمان دهد. بهرحال یک قاعده سرانگشتی که توسط ISPهای تجاری دنبال می گردد اینست که هر ترافیک در حال جریان در یک شبکه ی ستون فقرات ISP باید یک منبع یا یک مقصد (یا هر دو آنها) را در یک شبکه که یک شبکه مشتری آن ISP است داشته باشد؛ وگرنه ترافیک باید بشکلی آزاد در شبکه ی ISP جریان پیدا کند. توافق نامه های همتاسازی فردی (Individual peering agreements) (که باید به سوالاتی که در بالا گفته شدند پاسخ دهد) بطور معمول بین جفت ISPها و اغلب بصورت محرمانه مذاکره می گردند؛ [Huston 1999a] یک بحث جالب در مورد توافقنامه های همتاسازی (peering agreements) ایجاد می کنند. برای یک بحث مشروح در مورد اینکه سیاست مسیریابی چگونه روابط تجاری را در میان ISPها بازتاب می دهد، مراجعه کنید به [Gao 2001]. برای یک بحث متأخر در مورد سیاستهای مسیریابی BGP از نقطه نظر یک ISP، مراجعه کنید به [Caesar 2005].

همانطور که در بالا اشاره شد، BGP یک استاندارد بالفعل برای مسیریابی inter-AS برای اینترنت عمومی است. برای دیدن محتویات جداول مسیریابی BGP مختلف که از روترهای ISPهای tier-1 استخراج شده اند، مراجعه کنید به http://www.routeviews.org. جداول مسیریابی BGPاغلب حاوی دهها هزار پیشوند و خاصیت متناظرند. آمار درمورد سایز و مشخصات جداول مسیریابی BGP در منابعی همچون [Huston 2001; Meng 2005] نشان داده شده اند.

این مقدمه ی ما را در مورد BGP کامل می کند. درک BGP مهم است زیرا نقش مرکزی را در اینترنت بازی می

www.it98.ir

کند. ما شما را تشویق می کنیم که مرجعهایی از قبیل [Griffin 2002; Stewart 1999; Labovitz 1997; Halabi 2000; Huitema 1998; Gao 2001; Feamster 2004; Caesar 2005] را ببینید تا بیشتر در مورد BGP بدانید.

4.7مسیریابی Braodcast و Multicast

تا کنون در این فصل تمرکز ما پروتکل های مسیریابی بود که ارتباط unicast (همچون point-to-point) را پستیبانی می کردند، که در آن یک گره ی منبع یک بسته را به یک گره ی مقصد می فرستد. در این قسمت ما تمرکز خود را به پروتکلهای مسیریابی broadcastو multicast معطوف می کنیم. در مسیریابی broadcast، لایه ی شبکه یک سرویس برای فرستادن یک بسته ی فرستاده شده از یک گره ی منبع به همه ی گره ها در شبکه ایجاد می کند؛ مسیریابی broadcast یک گره ی منبع واحد را قادر می سازد تا یک کپی از یک بسته را به یک زیرشبکه از گره های شبکه های دیگر بفرستد. در بخش 4.7.1 ما الگورتیمهای مسیریابی broadcast و تجسم آنها در پروتکلهای مسیریابی را در نظر خواهیم گرفت. ما مسیریابی multicast را در بخش 4.7.2 امتحان خواهیم کرد.

4.7.1 الگوریتمهای مسیریابی Broadcast

شاید آسانترین راه برای انجام ارتباط broadcast برای گره ی فرستنده برای فرستادن یک کپی مجزا از بسته به هر مقصد باشد، همانطور که در تصویر 4.44(a) نشان داده شده است. با N گره ی مقصد داده شده، گره ی منبع بشکلی ساده انتقال را برای N کپی به Nمقصد با استفاده از مسیریابی unicast انجام می دهد. این رویکر N-way-unicast به نشر ساده است -- هیچ پروتکل مسیریابی لایه ی شبکه ی جدید، چندبرابر سازی بسته، یا عملکردهای ارسال مورد نیاز نیستند. بهرحال چندین اشکال به این رویکرد وجود دارند. اولین اشکال عدم کارایی آن است. اگر گره ی منبع به بقیه ی شبکه از طریق یک لینک واحد متصل باشد بنابراین N کپی مجزا از همان بسته آن لینک خواهند پیمود. واضح است کارایی بهتر خواهد بود اگر اولین گره اولین کپی را انجام دهد و از طریق لینک فرستاده شود و سپس گره ی بعدی عمل کپی و فرستادن را انجام دهد. این به این معناست که برای خود گره های شبکه کاراتر خواهد بود اگر بخواهند کپی از یک بسته را انجام دهند (بجای اینکه فقط گره ی منبع انجام دهد). بعنوان مثال در تصویر 4.44(b) تنها یک کپی مجزا از لینک R1-R2 عبور می کند. آن بسته در R2 تکثیر شده و با یک کپی از لینکهای R2-R3 و R2-R4 فرستاده شده است.

اشکالات دیگر مربوط به این رویکرد شاید دقیق تر باشند اما اهمین کمتری دارند. فرض ضمنی دیگر در مورد N-way-unicast این است که گیرندگان پخش، و آدرسشان توسط فرستنده شناخته شده است. اما این اطلاعات چگونه بدست آمده اند؟ به احتمال زیاد مکانیزمهای پروتکل اضافی (همچون یک عضویت broadcast یا پروتکل ثبت مقصد) مورد نیاز باشند. اینکار سربالایی و اهمین و پیچیدگی بیشتری را به یک پروتکل که در ابتدا بسیار ساده بنظر می رسیده، اضافه می کند. آخرین اشکال N-way-unicast مربوط می شود به اهدافی که بخاطر آنها broadcast استفاده می گردد. در بخش 4.5 ما یاد گرفتیم که پروتکلهای مسیریابی link-state از broadcast برای انتشار اطلاعات link-state که برای محاسبه ی مسیرهای unicast مورد استفاده قرار می

www.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

گیرند، استفاده می شد. واضح است که در شرایطی که broadcast مورد استفاده قرار می گیرد تا مسیرهای unicast را ساخته و بروزرسانی کند، این واقعا غیرهوشمندانه خواهد بود که بر ساختار مسیریابی unicast برای دریاف broadcast اطمینان کنیم.

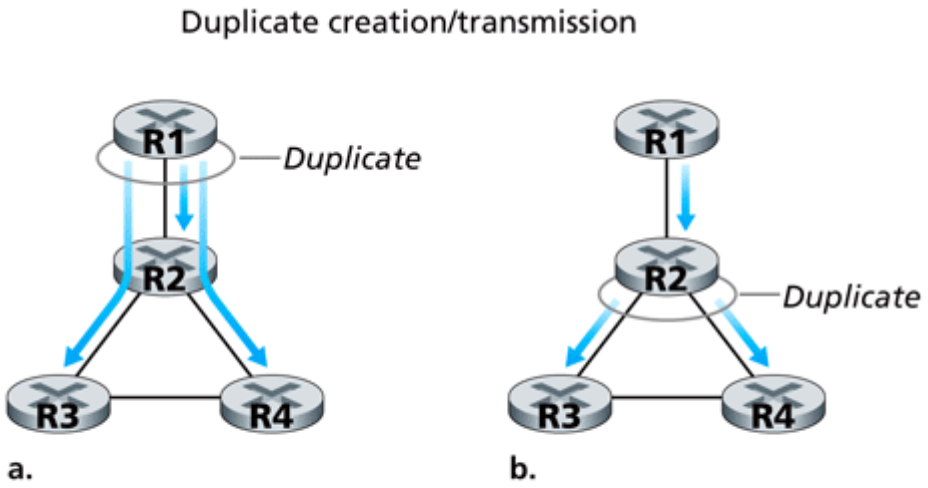


Figure 4.44 ♦ Source-duplication versus in-network duplication

تصویر 4.44 تکثیر منبع در مقابل تکثیر درون شبکه ای

با توجه به چندین اشکالی که از پخش N-way-unicast گرفتیم، رویکردهایی که در آنها گره های شبکه خود نقش فعال در تکثیر، ارسال بسته و محاسبه مسیرهای پخش بسته بازی می کنند، از موضوعات مورد علاقه است. ما چندین رویکرد زیر را امتحان خواهیم کرد و دوباره نماد گراف معرفی شده در بخش 4.5 را برمی گزینیم. ما دوباره شبکه را بعنوان یه گراف، G=(N,E) مدلسازی می کنیم، که N مجموعه ای از گره ها و یک مجموعه ی E از لبه هاست، که هر لبه یک جفت گره است از N. ما درمورد گزینش خود و استفاده از N برای مراجعه به هردو مجموعه از گره ها کمی سردر گم خواهیم بود و همچنین در مورد کاردینالیته (|N|) سایز آن مجموعه زمانی که هیچگونه سردرگمی وجود نخواهد داشت.

سیلاب کنترل نشده

واضح ترین تکنیک برای انجام پخش یک روش سیلابی است که در آن گره ی منبع یک کپی از بسته به همه ی مجاورهایش می فرستد. زمانی که یک گره یک بسته ی broadcast را دریافت می کند، بسته را تکثیر می کند و آن را به همه ی مجاورهایش (به جز مجاوری که بسته را از آن دریافت نمود) می فرستد. واضح است که اگر گراف متصل باشد، این طرح سرانجام یک کپی از بسته ی پخش (broadcast packet) به همه ی گره ها در گراف خواهد فرستاد. اگرچه این طرح ساده و ظریف است، یک جریان مهلک دارد (قبل از ادامه ی خواند، ببینید که آیا می توانید این جریان مهلک را شناسایی کنید یا خیر.): اگر گراف چرخه هایی دارد، بنابراین یک یا کپی های بیشتری از هر بسته ی پخش بشکلی نامحدود گردش خواهد کرد. بعنوان مثال در تصویر 4.44، R2 به R4یک سیلاب ایجاد می کند، و

www.it98.ir

به همین ترتیب R4به R2 و R2 دوباره به R3 و الی آخر! این سناریوی ساده منجر به چرخه ای نامحدود از دو بسته ی پخش می شود، یکی ساعتگرد و دیگری پادساعتگرد. اما حتی جریان مهلک فجیع بیشتری هم می تواند وجود داشته باشد: زمانی که یک گره به بیش از دو گره ی دیگر متصل است، چندین کپی از بسته ی پخش را خواهد ساخت و خواهد فرستاد که هر کدام چندین کپی را ساخته و می فرستند (البته با گره های دیگر با بیش از دو مجاور) و ... . این طوفان پخش (broadcast storm) نتجه شده از کپی های بی اندازه از بسته های پخش، قطعا بسیاری بسته ها بوجود خواهند آمد که شبکه آنها را بی فایده خواهد خواند. (سوالات مربوط به تکالیف که در پایان فصل در مورد تجزیه و تحلیل مسئله ی نرخ افزایش طوفان پخش می باشند را مطالعه کنید.)

سیلاب کنترل شده (Controlled Flooding)

کلید جلوگیری از طوفان پخش این است که یک گره بطور قضاوتمندانه انتخاب کند که چه زمانی یک بسته را به سیل بکشاند (مثلا زمانی که یک کپی و سیل پیش از موعد از یک بسته دریافت کرده باشد) و چه زمانی این کار را نکند. در عمل، اینکار از یکی از چندین راه امکانپذیر خواهد بود.

در سیل شماره ی ترتیبی کنترل شده (sequence-number-controlled flooding) یک گره ی منبع آدرس خود (یا هر تشخیص دهنده ی دیگری را) و همچنین یک شماره ی ترتیبی پخش را در یک بسته ی پخش قرار می دهد، سپس بسته را به همه ی مجاورهایش می فرستد. هر گره یک لیست از آدرس منبع و شماره ی ترتیبی هر بسته ی پخشی که دریافت کرده، تکثیر کرده و پخش کرده است را نگه می دارد.

زمانی که یک گره یک بسته ی پخش را دریافت می کند، در ابتدا چک می کند که آیا بسته در لیست قرار دارد یا نه. اگر بله بنابراین بسته حذف خواهد شد؛ وگرنه بسته تکثیر و به همه ی گره های مجاور (بجز گره ی مجاوری که بسته از آنجا دریافت شده باشد) فرستاده می شود. پروتکل Gnutella، که در فصل ۲ بحث می شود، از سیل کنترل شده با شماره ی ترتیبی استفاده می کند تا را سوالات خود را در پوشش شبکه ی خود پخش کند. (در Gnutella، تکثیر پیام و فرستادن آن در لایه ی درخواست بجای لایه ی شبکه انجام می گیرد.)

دومین رویکرد به سیل کنترل شده با عنوان انتقال مسیر معکوس (Reverse Path Forwarding - RPF) شناخته می شود [Dalal 1978]، همچنین بعضی اوقات با عنوان پخش مسیر معکوس (RPB) به آن اشاره می شود. ایده ی پشت RPF ساده و در عین حال ظریف است. زمانی که روتر یک بسته ی پخش را همراه با آدرس منبع دریافت می کند، بسته را بر روی همهی لینکهای خارج شونده ی خود (بجز لینکی که بسته را از آن دریافت کرده) انتقال می دهد جز بسته ای که بر روی لینکی که بر روی کوتاهترین مسیر unicast خود به منبع بر می گردد قرار دارد. در غیر اینصورت، روتر بشکلی ساده بسته ی ورودی را بدون فرستادن آن به هیچ یک از لینکهای خروجی خود به دور می اندازد. چنین بسته ای می تواند از بین برود زیرا روتر آن را می شناسد یا یک کپی از بسته را بر روی لینکی که بر روی کوتاهترین مسیر خود به فرستنده قرار دارد دریافت می کند یا دریافت کرده است. (شما ممکن است بخواهید خود را متقاعد کنید که در این در حقیقت اتفاق خواهد افتاد و اینکه چرخه و طوفانهای پخش به هیچ وجه اتفاق نخواهند افتاد.) توجه داشته باشید که RPF از مسیریابی unicast تا واقعا یک بسته را به مقصدی بفرستد استفاده نمی کند و نه حتی نیاز دارد که یک روتر تمام کوتاهترین مسیر را از خود به منبع بشناسد. RPF تنها نیاز به این دارد که مجاور را بر مسیر کوتاهترین unicast خود به فرستنده بشناسد؛ و در واقع از شناسه ی مجاور خود تنها برای تشخیص اینکه

www.it98.ir

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

آیا یک بسته ی رسیده را به سیل بکشاند یا خیر، استفاده می کند.

تصویر RPF 4.45 را شرح می دهد. فرض کنید که لینکهای رسم شده با خطوط نازک نشان دهنده ی کم ارزشترین مسیرها از دریافتگر به منبع (A) باشند. گره ی A در ابتدا یک بسته ی منبع A به گره های C و B پخش می کند. گره ی B بسته ی منبع A دریافت شده از A را (تا زمانی که A بر روی کم هزینه ترین مسیر به A باشد) به هردو گره ی C و D می فرستد. Bاز هر بسته ی منبع A که از هر گره ای (مثلا C یا D) دریافت کرده چشم پوشی خواهد کرد.

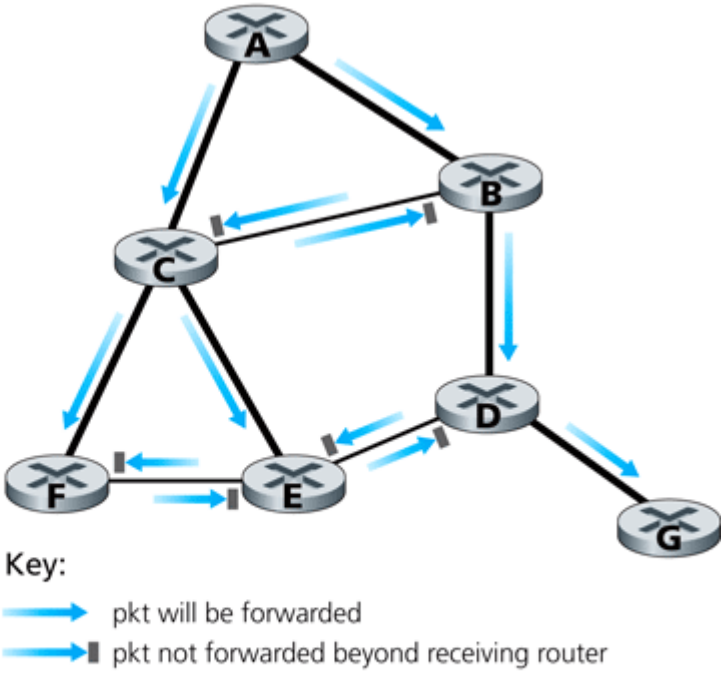


Figure 4.45 ♦ Reverse path forwarding

تصویر 4.45 حمل مسیر معکوس

اجازه دهید اکنون گره ی C را در نظر بگیریم که علاوه بر B یک بسته ی منبع A را مستقیما از A دریافت خواهد کرد. تا زمانی که B بر کوتاهترین مسیر برگش به A مربوط به C قرار ندارد، C هر بسته ی منبع A که از B دریافت می کند را رد خواهد کرد. از طرف دیگر، زمانی که C یک بسته ی منبع A را مستقیماً از A دریافت می کند، بسته را به گره های B، E و F خواهد فرستاد.

پخش از نوع درخت پوشا

تا زمانی که سیل کنترل شده با شماره ی ترتیبی و RPF از طوفانهای پخش (broadcast storms) جلوگیری می کنند، در واقع کاملا از انتقال بسته های پخش زائد جلوگیری نمی کنند. بعنوان مثال، در تصویر 4.46، گره های B، C، D، E و F یکی از یک یا دو بسته ی زائد را دریافت می کنند. بطور ایده آل، هر گره باید فقط یک کپی از بسته

www.it98.ir

ی پخش دریافت کند. با بررسی درخت شامل گره های متصل توسط خطوط نازک در تصویر 4.46(a)، می توانید ببینید که اگر بسته های پخش فقط همراه لینکهای داخل این درخت فرستاده شده بودند، هر گره ی شبکه می بایست دقیقا یک کپی بسته ی پخش دریافت کند--دقیقا راه حلی که ما بدنبال آن بودیم! این درخت یک مثال از یک درخت پوشا است--درختی که حاوی هر گره در یک گراف است. به شکلی رسمی تر، یک درخت پوشا از یک گراف G=(N,E) یک گراف G'=(N,E') می باشد بطوری که E' یک زیرشبکه از E است، G' متصل است، G' حاوی هیچ چرخه ای نیست و G' حاوی تمام گره های اصلی در G می باشد. اگر هر لینک یک هزینه ی همراه داشته باشد و هزینه ی یک درخت مجموع هزینه ی لینکها باشد، پس یک درخت پوشا که هزینه ی آن مینیمم تمام درختهای پوشای گراف باشد، (بدون تعجب!) یک درخت پوشای مینیمم نامیده می شود.

بنابراین رویکرد دیگری به ارائه ی پخش (broadcast) برای گره های شبکه است تا در ابتدا یک درخت پوشا بسازند. زمانی که یک گره ی منبع می خواهد یک بسته ی پخش را بفرستد، بسته را بر روی همه ی لینکهای تصادفی که متعلق به درخت پوشا هستند می فرستد. یک گره گیرنده ی یک بسته ی پخش (broadcast packet) سپس بسته را به تمامی مجاورهایش در درخت پوشا (بجز مجاوری که بسته را از آن دریافت می کند) می فرستد.

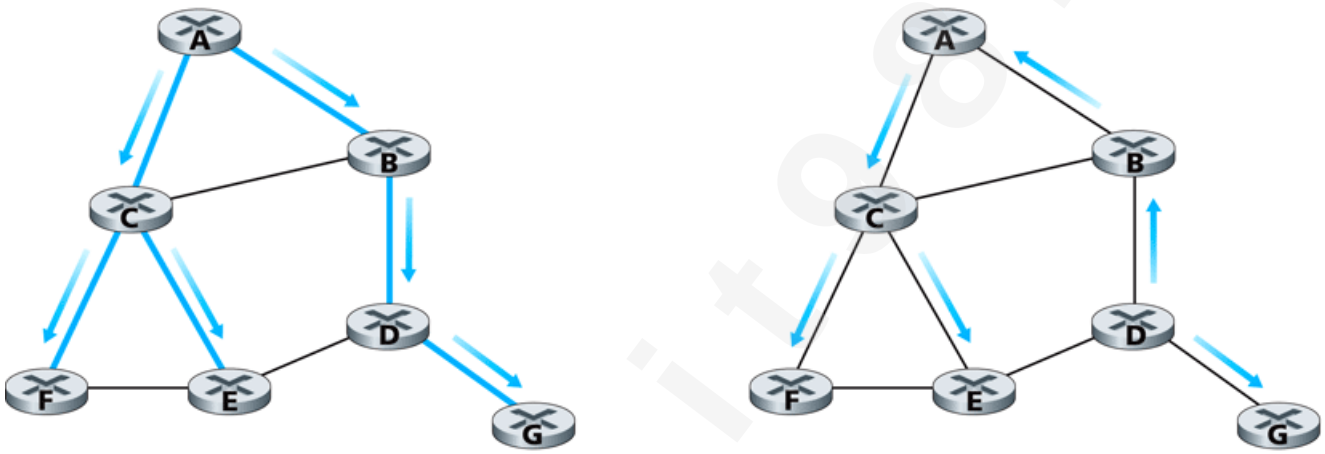


Figure 4.46 ♦ Broadcast along a spanning tree

تصویر 4.46 پخش در طول یک درخت پوشا

مشکل اصلی در مورد روش درخت پوشا ، ایجاد و حفظ درخت پوشاست . الگویتم های درخت پوشای بسیار زیادی تا کنون درست شده است (گالاگر ۱۹۸۳ ، گارتز۲۰۰۳) ما فقط در اینجا یک الگوریتم ساده را در نظر می گیریم در روش متمرکز برای ساختن یک درخت پوشا ، یک گره مرکزی (که به نام مرکز و نقطه وعده گاه هم نامیده می شود.) تعریف می شود . پس گره ها پیام های متصل به درخت که در مرکز نشان داده شد ، یک شکل می شوند . یک پیام متصل به درخت با استفاده از چرخش یک شکل شده به سمت مرکز می شود تا اینکه به گره ای می رسد که قبلا متعلق به درخت پوشا بوده یا به مرکزی دیگری می رسد در هر دو صورت ، مسیری که پیام متصل به درخت دنبال کرده ، شاخه

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

درخت پوشا ، بین گره حاشیه ای است که پیام متصل به درخت و مرکز آغاز کرده است . می توان این مسیر را به عنوان پیوندی روی درخت پوشای موجود دانست . شکل ۴۷-۴ ساختار یک درخت پوشا که بر روی مرکز متمرکز شده نشان می دهد . فرض کنید که گره یا منحنی E به عنوان مرکز درخت انتخاب می شود . فرض کنید که گره F ابتدا به درخت وصل می شود و یک پیام متصل به درخت را به سمت E می فرستد . یک اتصال مجزای EF اولین درخت پوشا می شود . سپس گره B با ارسال پیام متصل به درختش به سمت E به درخت پوشا می چسبد . فرض می گیریم که مسیر یکی شده به سمت E و از B ولی به وسیله D می چرخد . در این صورت ، پیام متصل به درخت باعث می شود مسیر BDE روی درخت پوشا پیوند بخورد سپس گره A ، گروه پوشا را با ارسال پیام متصل به درختش به سمت E وصل می کند . اگر مسیر A به سمت E از طریق B باشد پس چون B قبلا به درخت پوشا وصل شده بود ، رسیدن پیام A در B باعث اتصال AB خواهد شد که فورا به درخت پوشا پیوند می خورد . سپس گره C درخت پوشا را با ارسال پیام متصل متصل به درختش پیوند می خورد . سپس گره C درخت پوشا را با ارسال پیام متصل به درختش مستقیما به E وصل می کند .

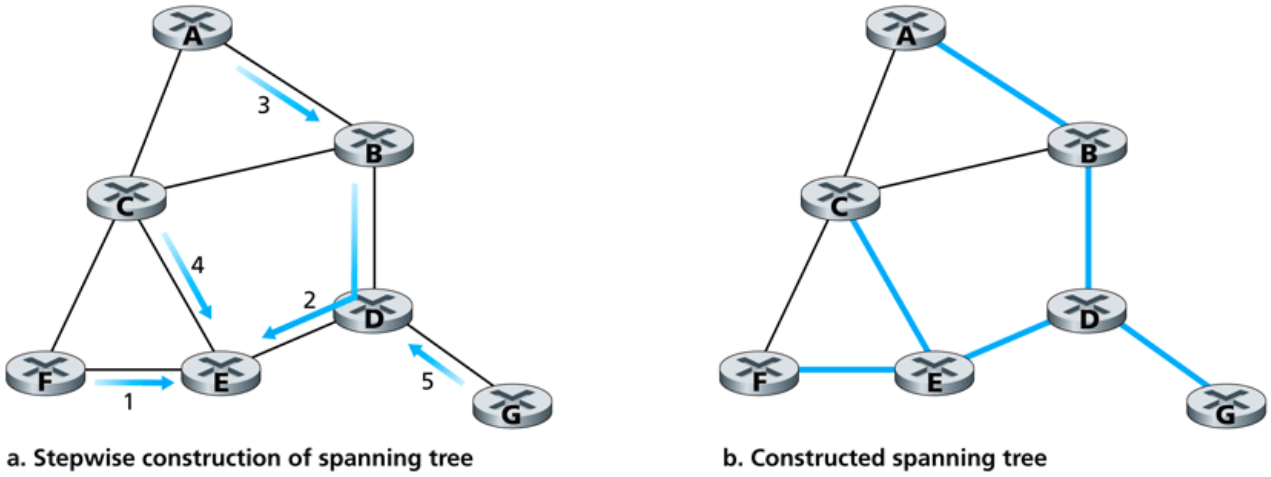


Figure 4.47 ♦ Center-based construction of a spanning tree

نهایتا چون چرخش کلی از G به E باید از طریق گره D باشد ، وقتی D پیام متصل در درختش را به E بفرستد ، اتصال CD به درخت پوشا در گره D پیوند می خورد .

الگوریتم های پراکنی در عمل (بطور عملیاتی)

پروتکل های پراکنی ، عملا در هر دو لایه شبکه و کاربرد بکار برده می شوند . همانطور که در بخش ۲,۶ گفتیم گنوتلا (گنوتلا ۲۰۰۷) از توزیع یا پراکنی در سطح – کاربردی به منظور انتشار (بخش) پرسش های برای محتوا در میان همتایان گنوتلا استفاده می شود . در اینجا یک ارتباط بین دو فرایند توزیع شده در سطح کاربردی در شبکه ی گنوتلا در واقع یک اتصال TCP است . گنوتلا از یک فرم شناور با کنترل تعداد توالی استفاده می شود که یک شناسه ی ۱۶

www.it98.ir

بیت و یک توصیف گر با ظرفیت حمل ۱۶ بیتی (که ۹ پیام گنوتلا را شناسایی می کند.) برای مشخص کردن اینکه آیا یک پرسش انتشار شده ی دریافتی قبلا دریافت شده ، نسخه برداری یا مجددا ارسال شده است یا نه بکار می برند . همانطور که در بخش ۶-۲ هم بحث شد گنوتلا همچنین از یک میدان مدت زمان برای زندگی (TTL) برای محدود کردن تعداد دفعاتی که یک سیل مولات به جاهای دیگر ارسال خواهد استفاده می کنند وقتی فرایند گنوتلا یک پرسش را دریافت و تکثیر می کند حوزه ی TTL را قبل از ارسال مجدد سوال کاهش می دهد بنابراین یک خیل عظیم پرسش گنوتلا فقط به آنهایی می رسد که در تعداد داده شده (مقدار اولیه TTL) از جهش های مربوط به سطح کاربری از آغازگر پرسش باشد ، بنابراین مکانیسم به راه اندازی گنوتلا گاهی اوقات بعنوان به راه انداز حوزه ی محدود نامیده می شود .

یک فرم از سان سیل با تعداد توالی های کنترل شده برای انتشار آگهی های بازرگانی مربوط به ایالتی (LSA) در الگوریتم چرخشی OSPF (RFC2328 per man 1999) و در سیستم متوسط به سیستم میانی (IS-IS) که الگوریتم چرخشی ست (RFC 1142,perman 1999) بکار می رود . OSPF از یک توالی عددی ۳۲ بیت و یک میدان به اندازه ی ۱۶ بیت برای شناسایی LSA استفاده می کنند . بیاد داشته باشید که یک گره LSA،OSPF را برای لینک های اتصالی اش بصورت دوره ای منتشر می کنند ، مخصوصا وقتی که ارزش لینک نسبت به آن نوع مجاورش تغییر می کند یا وقتی که لینک بالا و پایین می رود ، اعداد یا تعداد توالی های LSA برایب نمایان سازی تکثیر LSA بکار می روند ولی برای نقش مهم و ثانویه اش در OSPF هم هست . با انتشار و با اندازه ی برای یک LSA تولید شده بوسیله ی منبع در زمان t احتمال دارد که پس از یک LSA جدیدتر که خود از همین منبع و در زمان t برسد . اعداد توالی بکار رفته از سوی گره منبع باعث می شود یک LSA قدیمی تر از یک LSA جدیدتر تشخیص داده شود . حوزه و میدان سنی به منوری مثل مقدار TTL بکار می رود . مقدار عمر این حوزه صفر تعیین می شود در هر پرسش که راه اندازی صورت می گیرد ، زیاد می شود و همچنین آنگاه که روی یک حافظه ی چرخشی و منتظر برای راه اندازی می نشینید افزایش داده می شود . با اینکه ما فقط بطور مختصر الگوریتم راه اندازی LSA را در ایجا توضیح داده ایم ولی می گوییم که در واقع طراحی پروتکل های انتشار LSA می تواند یک کار بسیار با مهارت باشد . (RFC 789,perman1999) نمونه ای را توضیح می دهد که بطور نادرست LSA ها را با دو چرخش اشتباه انتقال داده و باعث شدند تا نسخه اولیه ی یک الگوریتم راه اندازی LSA کلا خراب شود . (ARPA net)

۲-۷-۴ Multicast

ما در بخش قبل دیده ایم که با سرویس انتشاری بسته ها به هر یک از گره ها در شبکه می رسند در این بخش ما توجه خود را به سرویس چندگانه ی انتشاراتی معطوف کرده ایم که یک بسته ی چندگانه فقط به زیر مجموعه های گره های شبکه می رسد و توسط آنها دریافت می شود . چندین کاربری شبکه ای نیاز به دریافت بسته ها از یک یا چند فرستنده به گروهی از گیرنده ها دارند . این کارها شامل انتقالات پرحجم (مثلا انتقال یک نرم افزار پیشرفته از

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

سازنده ی نرم افزار به کاربرانی که به ارتقا نیاز دارند) یک سری رسانه ی پیوسته (مثل انتقال متن ، ویدئو و صدای یک سخنرانی زنده برای یک مجموعه از شرکت کنندگان در سخنرانی) کاربری های اطلاعات مشترک (مثل کارهای وایت برد یا تله کنفرانس که در میان بسیاری از شرکت کنندگان تقسیم می شود) تغذیه اطلاعات ، مثلا مخازن ذخیره ای به روز رسانی مخازن وب ، و بازیهای مقابله ای (مثل محیطهای مجازی یا بازیهایی که نیاز به چندین بازیکن دارند) هستند .

در ارتباطات چند انتشاری ما فورا با دو مسئله مواجه می شویم یکی اینکه چطور گیرندگان یک بسته ی چند انتشاری را شناسایی کنیم و دوم اینکه چطور یک بسته ی ارسال شده را به این گیرنده ها نشان دهیم . در مورد ارتباطاتی که یک انتشار واحد داشتند آدرس FP گیرنده (مقصد) در هر نمودار اطلاعاتی TP آن منتقل شده و یک گیرنده ی مجزا را شناسایی می کند در مورد انتشار تمام گره ها لازم است که بسته ی انتشاراتی را دریافت کنند بنابراین به آدرس مقصد نیازی نیست ولی در مورد چند انتشاری ها دیگر چندین گیرنده داریم آیا برای هر بسته ی چند انتشاری خوب است که آدرسهای IP تمام گیرنده های چندگانه را منتقل کنیم ؟ در حالیکه این روش با تعداد کمی از گیرنده ها ممکن است کارآمد باشد ولی در مورد صدها یا هزاران گیرنده به درد نمی خورد ؛ میزان اطلاعات نشان داده شده در بخش اطلاعات سنج باید میزان اطلاعات که عملا در حوزه ی ظرفیتی و بسته ها منتقل می شود باید محافظ کنند شناسایی ساده ی گیرنده ها از سوی فرستنده همچنین نیاز دارد به اینکه فرستنده هویت ها و آدرس های تمام گیرندگان را بداند . ما خواهیم دید که در آنها نیازی به این کار نیست .

به این دلایل در طراحی اینترنت و دیگر شبکه ها مثل ATM (بلاک ۱۹۹۵) یک بسته ی چند انتشاری با استفاده از شناسایی آدرس نشان داده می شود و یک شناسه ی مجزا ثابت برای گروهی از گیرنده ها بکار می رود و یک نسخه از بسته ای که به گروه نشان داده می شود که از این شناسه واحد استفاده می کند برای تمام گیرنده های چند انتشاری مرتبط با آن گروه دریافت می شود در اینترنت شناسه ی واحدی که گروهی از گیرندگان را نشان می دهد یک آدرس IP چند انتشاری D است . گروهی از گیرندگان مرتبط با یک کلاس آدرس D بعنوان یک گروه چند انتشاری یاد می شود . انتزاع گروه چند رسانه ای در شکل ۴۸-۴ نشان داده می شود در اینجا ۴ میزبان که با رنگ تیره نشان داده شده اند مربوط به آدرس گروه چند رسانه ای ۱۹۷/۳۰/۱۷/۲۲۶ هستند و تمام نمودار های اطلاعاتی نشان داده شده برای آن آدرس چند انتشاری را دریافت خواهند کرد مشکلی که ما هنوز باید بگوییم این واقعیت است که هر میزبان یک آدرس انتشاراتی IP منحصر به فرد دارد که کاملا مستقل از آدرس گروه چند رسانه ای است که در آن شرکت می کنند .

در حالیکه انتزاع گروه چند انتشاری ساده است ولی باعث افزایش سوالات می شود چطور یک گروه شروع می شود و چطور به پایان می رسد ؟ چطور آدرس گروه انتخاب می شود ؟ میزبانهای جدید چطور به گروه اضافه می شوند (فرستنده ها یا گیرنده ها) ؟ آیا کسی می تواند به گروه بپیوندد (و از آن گروه چیزی دریافت کند یا برایشان بفرستد) یا عضویت در گروه محدود است ، اگر چنین است توسط چه کسی ؟ آیا اعضای گروه هویت سایر اعضا را بعنوان بخشی از

www.it98.ir

پروتکل لایه ی شبکه می شناسند یا نه ؟ چطور گره های شبکه با یکدیگر برای دریافت یک نمودار اطلاعاتی چند انتشاری برای تمام اعضای گروه کار می کنند ؟

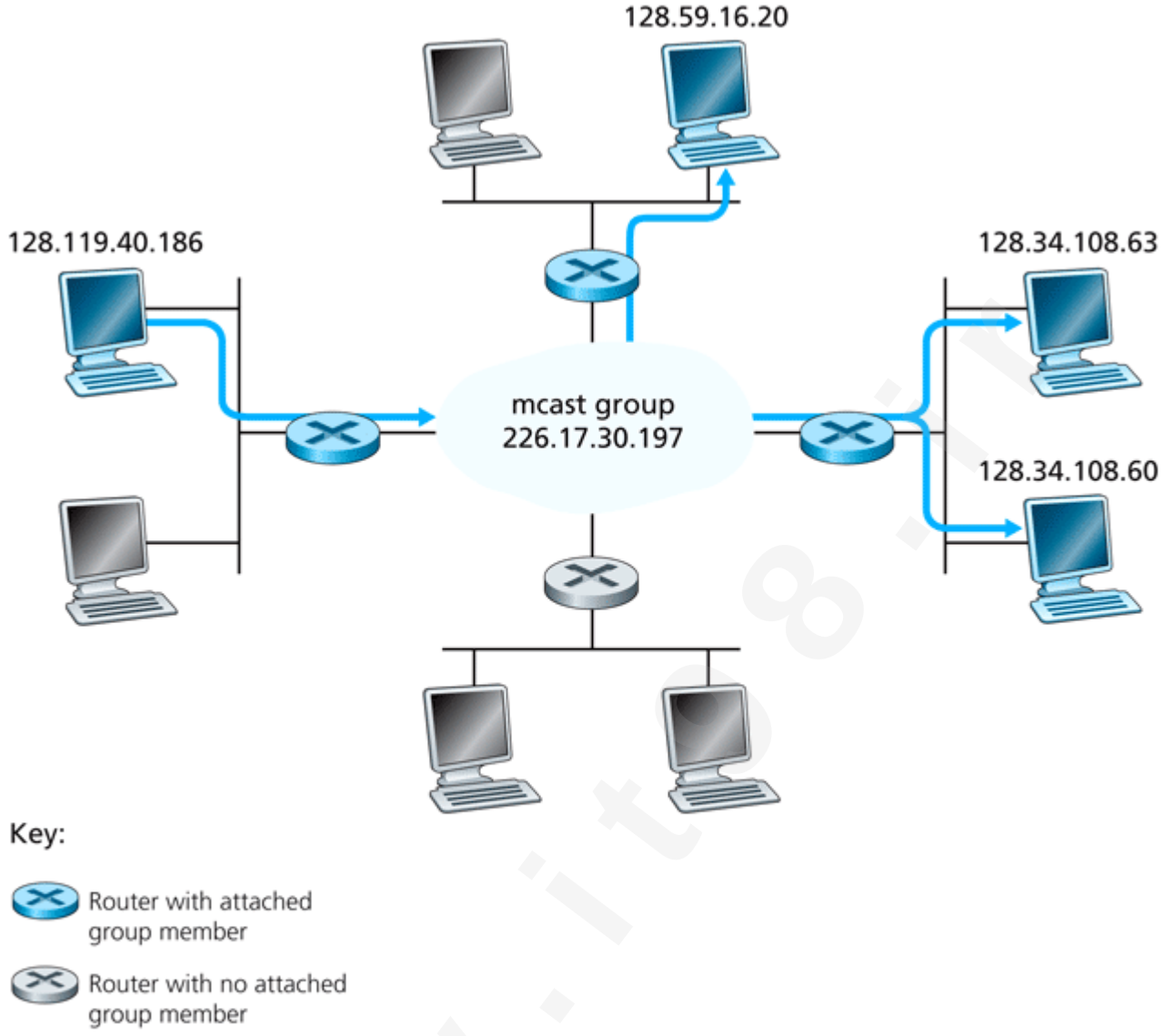


Figure 4.48 ♦ The multicast group: A datagram addressed to the group is delivered to all members of the multicast group.

برای اینترنت پاسخ به تمام این سوالات شامل پروتوکل مدیریت گروه اینترنت (RFC337) می شوند پس اجازه دهید که در اینجا بطور خلاصه IGMP را در نظر گرفته و سپس به این سوالات گسترده تر بپردازیم .

پروتکل مدیریت گروه اینترنت

مرژن (نسخه ۳) پروتکل IGMP (RFC3376) همانطور که در شکل ۴۹-۴ نشان داده شده بین یک میزبان و یک مسیر صاف کن که مستقیما به آن وصل است عمل می کند (خصوصا ما فکر می کنیم در مورد مسیر صاف کن که

www.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

مستقیما متصل است به عنوان اولین عمل کننده است تا یک میزبان در یک مسیر هر آنچه میزبان در خارج از شبکه محلی خودش می باشد را هم ببیند .) شکل ۴۹-۴ اولین ۳ حرکت مسیر صاف کن را نشان می دهد که هر کدام از طریق یک واسط خروجی محلی متصل به میزبان های متصل به خودش می باشد . این واسط در این مثال به LAN وصل شده ولی هر LAN میزبان چندگانه دارد که تقریبا تعداد کمی از آنها در هر زمان مشخص متعلق به گروه چند انتشاری داده شده هستند .

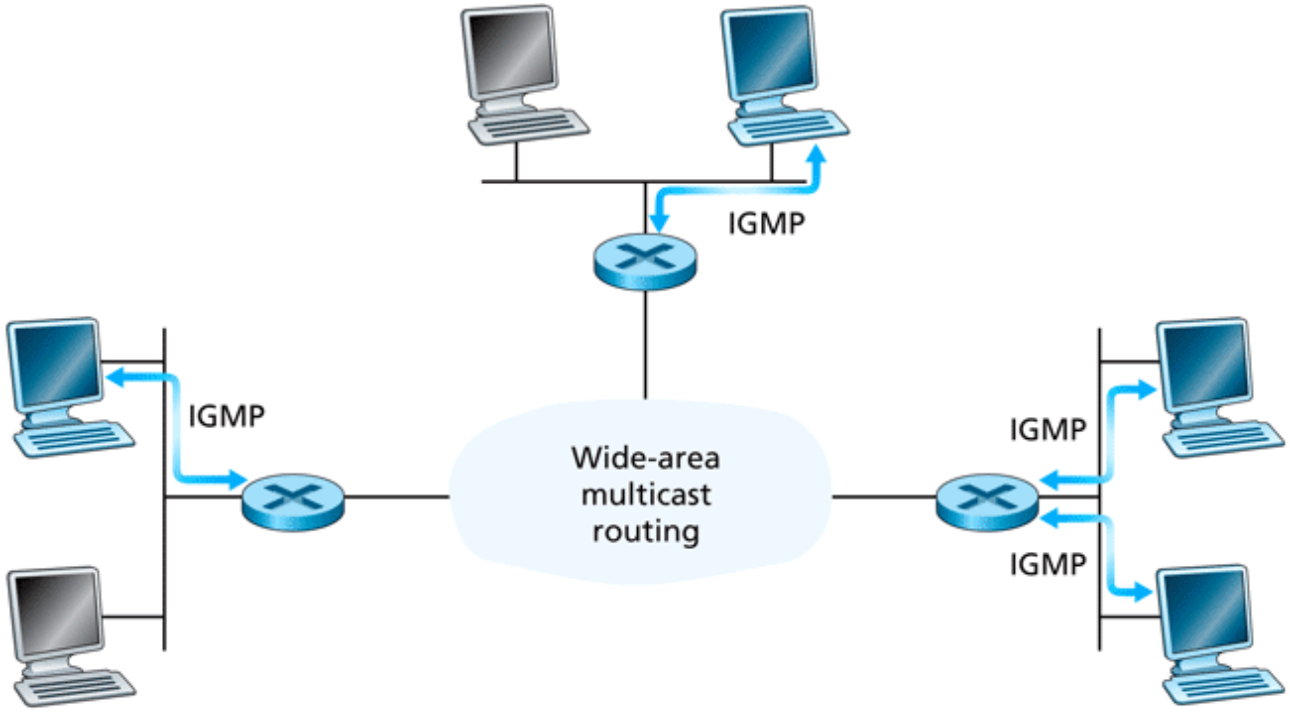


Figure 4.49 ♦ The two components of network-layer multicast in the Internet: IGMP and multicast routing protocols

IGMP ابزارهایی برای یک میزبان ارائه می کند تا به او اطلاع دهد که مسیر صاف کن متصل به او که روی آن کاربردی بوده ، میخواسته گروه چند انتشاری خاصی را وصل کند . فرض می شود که میزان رفتار IGMP محدود به میزان و مسیر صاف کن متصل به آن می باشد ، پروتکل دیگر برای هماهنگ کردن مسیر صاف کن های دیگر از طریق اینترنت لازم می شود تا اینکه اطلاعات چند جانبه به مقصد نهایی شان برسند . این کار توسط الگوریتم های مسیر صاف کن چند انتشاری لایه شبکه مثل همانهایی که مات میخواهیم راجع به آنها صحبت کنیم انجام می گیرد . بنابراین ، چند انتشار لایه – شبکه در اینترنت شامل دو مولفه متممی است : IGPM و پروتکل های مسیر صاف کن با انتشار چندگانه .

IGPM فقط دارای ۳ نوع پیام است . مثل IGMP ، پیام های IGMP درون یک بسته اطلاعاتی IP با تعداد ۲ پروتکل IP منتقل می شوند . پیام membership query (یا تحقیق - عضویت) توسط یک مسیر صاف کن به

www.it98.ir

تمام میزبان ها روی یک واصل چسبیده یا الحاقی فرستاده می شود (مثلا برای تمام میزبان ها روی یک شبکه محلی) تا مجموع تمام گروههایی چند انتشاری را که به وسیله میزبان ها روی آن واسط قرار گرفته اند را تعیین و مشخص کند . میزبان ها به این پیام با IGMP member ship-report پاسخ می دهند . پیام های گزارشی همچنین میتوانند توسط یک میزبان تولید شوند که زمانی که یک کاربری اول بدون منتظر ماندن برای پیام تحقیقی از مسیر صاف کن ، یک گروه چندگانه انتشاراتی را وصل می کند . آخرین نوع پیام leave-group است . جالب است که بدانید این پیام اختیاری و انتخابی است .

ولی اگر انتخابی است یک مسیر صاف کن ، وقتی یک میزبان گروه چند انتشاری را ترک می کند ، چطور متوجه اش می شود ؟ پاسخ به سوال این است که مسیر صاف کن ، فرض می گیرد که میزبان بیشتر در گروه چند انتشاری نمی ماند ، مخصوصا اگر بیشتر پاسخ به پیام تحقیقی ندهد (با همان آدرس گروه داده شده) این نمونه همان چیزی است کهنگاهی اوقات در پروتکل اینترنت به آن حالت نرم هم می گویند . در یک پروتوکول حالت نرم یا ساده حالت از طریق یک رخداد با وقفه (مثل یک پیام دوره ای تحقیقی) برداشته می شود مخصوصا اگر به سادگی به حالت اولش برنگردد (در این مورد با یک پیام گزارشی از یک میزبان الحاقی) چنین استدلال شده است که پروتکل های حالت نرم و ساده باعث کنترل ساده تری نسبت به پروتوکول های حالت سخت دارند که نه تنها به ساده شدن نیاز دارند و آسان برداشته شوند بلکه نیاز به مکانیزم هایی برای دریافت از وضعیتی ست که مقدار مسئول برداشتن یا تعویض حالتی ست که سیستم دچار اشکال شده است در قسمت (Lui2004,Ji2003,Raman1999) دارای بحث هایی درباره ی این حالت می باشند .

الگوریتم های مسیر انتشار چندگانه

مسئله ی مسیر با انتشار چندگانه در شکل ۵۰-۴ نشان داده شده است میزبانهای متصل به گروه دارای چند انتشاری با رنگ تیره تر نشان داده شده اند که البته مسیر صاف کن که بلافاصله به آنها وصل می شود هم با رنگ سایه ی تیره نشان داده می شود . همانطور که از این شکل می بینید فقط یک مجموعه از این مسیر صاف کن ها نیاز واقعی به دریافت ترافیک چند انتشاری دارند . در شکل ۵۰-۴ فقط مسیرهای چند انتشاری ABE,F از این نوعند . چون هیچ یک از میزبانهای متصل به مسیر صاف کن به گروه چند انتشاری وصل نیستند و چون C هم هیچ اتصالی به میزبانها ندارد نه C و نه D نیازی به دریافت ترافیک گروه چند انتشاری ندارند . پس هدف از چرخش چند انتشاری یافتن درخت اتصالات است که تمام مسیر صاف کن ها را به هم متصل سازد که به میزبانهای مرتبط با گروه چند انتشاری الحاق شده اند . سپس بسته های چند انتشاری در امتداد این درخت از فرستنده به تمام میزبانهای مرتبط با درخت چند انتشاری خواهند رفت البته درخت ممکن است شامل مسیر صاف کن هایی باشد که میزبانهای الحاقی نداشته باشد تا آنرا به گروه چند انتشاری مربوط سازد برای مثال در شکل ۵۰-۴ اتصال مسیر صاف کن های A,B,E,F در یک درخت بودن در لحاظ کردن C یا D غیره ممکن است .

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

در عمل برای این بحث از روش از قبل مورد بررسی قرار گرفته و بنابراین ما فقط بصورت گذرا در اینجا آنها را عنوان می کنیم . این دو روش از لحاظ اینکه آیا یک درخت با گروه مشترک واحد برای توزیع ترافیک جهت تمام فرستنده ها در گروه استفاده می شود یا نه و آیا یک درخت با منبع خاص برای هر یک از فرستنده ها بصورت جداگانه ساخته می شود یا نه با هم فرق دارند .

- مسیر با انتشار چندگانه با استفاده از یک درخت دارای گروه مشترک . همانگونه که در مورد انتشار درخت پوشا گفتیم چرخش و مسیرهای چند انتشاری در یک درخت با گروه مشترک هم بر اساس درختی ست که شامل تمام مسیر صافکن های حاشیه ای با میزبانهای الحاقی و مرتبط با گروه چند انتشاری هستند . در عمل یک روش متمرکز بکار می رود تا درخت چند انتشاری با مسیر صاف کنهای حاشیه ای و میزبانهای الحاقی مرتبط با ارسال گروه چند انتشاری از طریق پیامهای متصل که به گره مرکز نشان داده می شوند ، بسازد در مورد انتشار یک پیام متصل با استفاده از مسیر یک انتشاری برای مرکز فرستاده می شود تا اینکه یا به مسیری برسد که از قبل مربوط به درخت چند انتشاری بوده یا به مرکز می رسد .

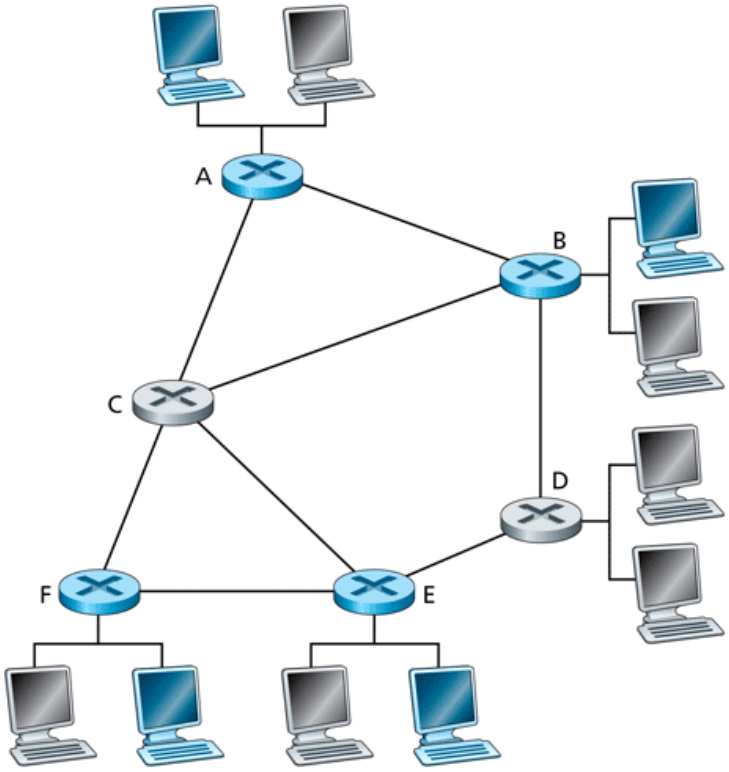


Figure 4.50 ♦ Multicast hosts, their attached routers, and other routers

تمام مسیرهای موجود که پیام از آنها می آید باید بسته های دریلفتی را به مسیر صاف کن های حاشیه ای برسانند که اتصال چند انتشاری را آغاز کرده اند یک سوال اساسی برای درخت دارای مرکز و مسیر چند انتشاری فرایند بکار رفته برای اتخاب مرکز است . الگوریتم های انتخاب مرکز در
Strim 1997,thaler 1997,wall 1980 بحث شده اند .

www.it98.ir

- مسیر چند انتشاری با استفاده از یک درخت دارای منبع در حالیکه درخت گروه مشترک چرخشی و چند اشتراکی یک درخت مجزا و دارای مسیر مشترک را می سازد تا بسته ها را برای تمام فرستنده ها صاف کند ، روش دوم یک درخت چرخشی چند انتشاری را برای هر منبع در گروه چند انتشاری می سازد در شرایط عملی یک الگوریتم RPF با گره منبع x بکار می رود تا یک درخت چند انتشاری ارسالی را برای t اطلاعات چندگانه ای که از منبع x می آید بسازد . الگوریتم انتشاری RPF که ما قبلا بررسی کردیم به t ضعیف جهت انتشار چند مسیری نیاز دارد . میخواهیم ببینیم چرا مسیر صاف کن D را در شکل ۵۱-۴ بررسی می کنیم . برای انتشار RPF باید بسته ها را به G بفرستد حتی اگر G به میزبانی وصل نباشد که به نوبه خود آنهم وصل به گروه چند انتشاری باشد در حالیکه برای این مورد خیلی بد نیست که D فقط یک مسیر مجزا داشته باشد (G) تصور کنید چه می شود اگر هزاران مسیر مستقیم و مجزا هز D وجود داشته باشد هر یک از این هزاران مسیر باید بسته های چند انتشاری ناخواسته را دریافت کند (این مبحث خیلی هم نسبت به آنچه که به نظر می رسد بعید نیست MBone اولیه (کاسنر ۱۹۹۲،ماکدونی۱۹۹۴)اولین شبکه چند انتشاری جهانی است که در ابتدا از این موضوع دچار نقص بود) راه حل مسئله دریافت بسته های ناخواسته چند انتشاری با RPF معروف به هرس می باشد . یک مسیر صاف کن که بسته های چند تایی را دریافت می کند و میزبان الحاقی با آن گروه ندارد ، یک پیام هرس به مسیر صاف کن بالایی اش می فرستد ، اگر یک مسیر صاف کن پیامی را از هر یک از مسیر صاف کنهای پایینی اش بگیرد پس می تواند یک پیام هرس را بالاتر ی هم بفرستد .

مسیرهای چند انتشاری در اینترنت

اولین پروتکل صاف کننده چند انتشاری بکار رفته در اینترنت پروتکل صاف کنند چند انتشاری بردار فاصله ای (DVMRP) می باشد (RFC1075) . DVMRP درخت های گرفته شده از منبع را با مسیر برعکس فرستادن و هرس کردن بکار می برد . DVMRP از الگوریتم RPF با هرس بکار می رود که در بالا هم گفته شد . احتمالا پرکاربردترین پرتکل از این نوع پروتکل صافی چند انتشاری مستقل از پروتکل (PIM) می باشند که به راحتی دو متن توضیعی را تشخیص می دهد در روش متراکم (RFC3973) اعضای گروه چند انتشاری به صورت فشرده واقع شده اند که بسیاری از مسیر صاف کن ها در آنجا باید در ساختار اطلاعات لحاظ شده باشند . روش PIM متراکم یک مسیر معکوس جریان و هرس تکنیکی مثل روح برای DVMPR می باشد .

در روش پراکنده یا تنک (RFC4601) تعداد مسیر صاف کن ها با اعضای گروه الحاقی از لحاظ تعداد کل کم است و اعضای تعداد گروه تا حدود زیادی پراکنده اند. حالت کم پشت pim از نقاط ایستگاهی استفاده می کند تا درخت توزیعی را تنظیم نماید در انتشار چندگانه از منبع خاص(SSM) (RFC3569.94607) فقط به یک فرستنده اجازه داده می شود تا تعدادی را به درخت چند انتشاری بفرستد که بسیار شبیه به روشی باشد که پروتکل هائی مثل rip-is-is و ospf می تواند پیکربندی کند .

wWw.it98.ir

www.it98.ir

وقتی pim و dvmp در یک حوزه استفاده می شوند اپراتور شبکه می تواند مسیر صاف کن های ip را در حوزه ترکیب بندی نماید. ولی اگر بین حوزه های مختلف مسیرهای چند گانه لازم شود چه اتفاقی می افتد؟ آیا معادل انتشار چندگانه ای از پروتکل bgp درون شبکه ای وجود دارد؟ پاسخ (از لحاظ ادبی) بله است (rfc4271) تعمیمی چند پروتکلی به bgp را تعریف می کند تا اجازه دهد اطلاعات برای دیگر پروتکل ها مخصوصا اطلاعات انتشار چندگانه منتقل شود پروتکل کشف منبع و با انتشار چندگانه (msdp) (rfc3678و ۴۶۱۱) می تواند بکار رود تا نقاط ایستگاهی در حوزه های pim متفرقه را بتواند با هم وصل کند در اینجا بحث خود را راجع به انتشار چندگانه ip با ذکر این نکته که هنوز باید بررسی بیشتری روی آن صورت پذیرد به پایان می رسانیم برای بحث های جالب در این زمینه دابوت ۲۰۰۰ و شارم ۲۰۰۳ را ببینید بر خلاف کمبود پراکندگی انتشار چندگانه در سطح شبکه با زوال فاصله زیادی دارد. ترافیک با انتشار چندگانه به مدت چند سال اینترنت ۲ و شبکه همراه با کاربران استفاده شده است(اینترنت ۲، ۲۰۰۷) در بریتانیا ، bbc در مورد آزمایش توزیع خبر از طریق انتشار چندگانه ip کارهائی صورت گرفته می شود (انتشار چندگانه bbc) به طور همزمان انتشار چندگانه در حد کاربردی که در بخش ۲ هم دیدید در سیستم هائی مثل (esm2007) توزیع چندگانه خبر در میان شنونده ها با استفاده از پروتکل های انتشاری لایه کاربری به جای لایه شبکه ارائه می کنند.

www.it98.ir

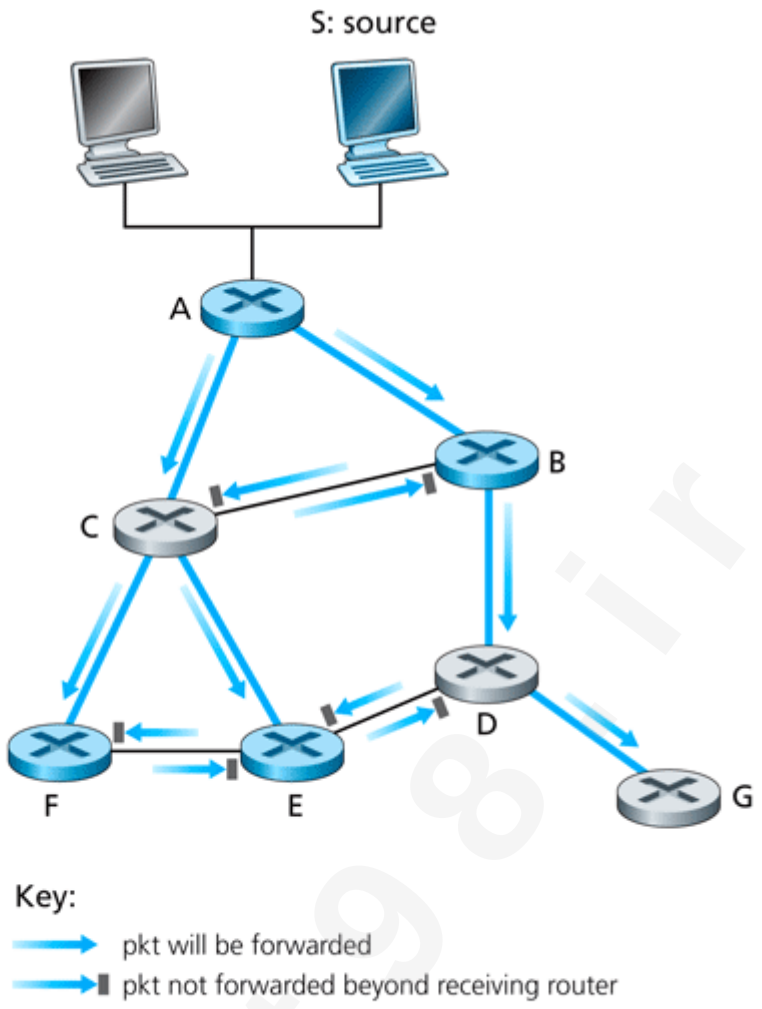


Figure 4.51 ♦ Reverse path forwarding, the multicast case

آیا خدمات انتشارات چندگانه آینده می تواند در لایه شبکه بکار رفته یا در لایه کاربری (در حاشیه شبکه) ؟ در حالیکه شکاف فعلی برای توزیع اصلی از طریق روشهای هم درجه کردن توازن را به نفع انتشار لایه کاربری در آینده نزدیک پیش می برد پیشرفتها باید ادامه یابد تا انتشار چندگانه ip ساخته شود و نهایتا به سمت پیشرفت گراید.

۸-۴ خلاصه

در این بخش ما سفر خود را به درون هسته شبکه آغاز کرده ایم ما آموختیم که لایه شبکه شامل هر یا تمام میزبانها و مسیر صاف کن ها در شبکه می باشد به همین دلیل پروتکل های لایه شبکه در بسته پروتکل ها بیشترین مشکل را بوجود می آورند.

ما فرا گرفتیم که یک مسیر صاف کن ممکن است تا نیاز داشته باشد میلیونها بسته را بین جفت مقصد- مبدا بطور همزمان پرداش کند. برای اجازه دادن به یک مسیر صاف کن برای پردازش یک چنین تعداد زیادی طراحان شبکه به مرور زمان یاد گرفته اند که کارهای مسیر صاف کن باید تا حد امکان ساده باشد معیارهای بسیار یرا می توان بکار برد

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

تا وظیفه مسیر صاف کن آسانتر شود مثل استفاده از لایه شبکه اطلاعات بجای لایه شبکه ای که منحصرا و مدار مجازی باشند استفاده از یک پیشرو به سمت مستقیم و با اندازه ثابت مثل ipv6 حذف یا کاهش قطعه سازی(مثل آنچه که در ipv6 انجام شد) و ارائه بهترین خدمات می باشند . شاید مهمترین کار در اینجا این نباشد که جریانات جداگانه را لحاظ کند بلکه بر ساختار سلسله مراتبی در نمودار اطلاعاتی تاکید کند. جالب است بگوئیم که خدمات پستی سالهاست که از این روش استفاده می کند.

در این بخش ها همچنین به اصول اساسی الگوریتم های بازگشائی ،نگاهی انداختیم. ما یاد گرفتیم که چطور این الگوریتم ها شبکه کامپیوتری را به یک نمودار با گره ها و اتصالات بسیار تجزیه می کند با اینکار می توانیم تئوری قدرتمند کوتاهترین مسیر اصلاحی در مدارها را استخراج کرده که بیش از ۴۰ سال می باشد .

که در عملیات تحقیق الگوریتم ها کاربد دارند.ما دیدیم که دو روش گستره وجود دارد. یک روش جهانی(متمرکز) که هر گره نقشه کاملی از شبکه را بدست آورده و بطور مستقل الگوریتم مربوط به مسیر کوتاه را بکار می برد و دیگری روش تمرکز زدا است که گره های جداگانه فقط تصویری نسبی از شبکه کامل را دارند در حالیکه گره ها با یکدیگر کار می کنند تا بسته ها را در کوتاهترین مسیر ها دریافت نمایند . ما همچنین بررسی کردیم

که سلسله مراتبی چطور به مساله مقیاس از طریق تقسیم شبکه های بزرگ به حوزه های اجرائی مستقل بنام سیستم های مستقل یا خود گردان(AS) می پردازد.هر AS به طور مستقل نمودارهای اطلاعاتی را پیموده درست مثل اینکه هر کشور بطور مستقل نامه های پستی اش را در سرتاسر کشور پخش می کند و می رساند. ما می دانیم که چطور روش های متمرکز تمرکز زدا و سلسله مراتبی در پروتکل های اصلی در اینترنت جا داده می شود: RIP، BGP،OSPF. ما مطالعه خود را با الگوریتم های چرخشی و با پرداختن به مسیرهای انتشار و متعدد شدن آن به پایان رساندیم.

با رسیدن به اینجا، ما به پروتکلی می رسیم به نام لایه اتصال . همانند لایه شبکه ،لایه اتصالی هم بخشی از مرکز (هسته) شبکه است . ولی در بخش بعد خواهیم دید که لایه اتصالی ، کار بسیار (وظیفه) بیشتری برای جابجا نمودن بسته ها بین گره ها بر روی لینک مشابه یا LAN دارد. البته ، با اینکه این کار ممکن است از لحاظ ظاهری و در مقایسه با کارهای لایه شبکه، جزعی(کم) باشد ، ولی خواهیم دید که لایه لینک دارای موارد بسیار مهمی است که می تواند ما را برای مدتی طولانی به خود مشغول سازد.

مساله ، سوالات (تکالیف): سوالات مروری بخش ۴

بخش های ۱-۴ تا ۲-۴

R1. می خواهیم برخی از لغاتی را که در این کتابچه بکار برده ایم بررسی کنیم. به یاد داشته باشید که نام بسته لایه-انتقالی قطعه است و اسم بسته لایه – اتصال (لینک)، چارچوب است .

www.it98.ir

نام بسته لایه شبکه چیست؟

می دانید که سوئیچ های لایه اتصال (لینک) و مسیر صاف کن ها ، هر دو ، سوئیچ هـای بسـته ای نامیـده مـی شـوند. تفاوت بنیادی بین یک مسیر صاف کن و سوئیچ لایه – اتصال(لینک) چیست؟

بیاد آورید که ما از کلمه مسیر صاف کن برای شبکه های VC و شبکه های نمودار اطلاعات استفاده می کنیم.

R2. دو کار اصلی لایه شبکه در یک شبکه نمودار اطلاعاتی چیست؟ سه کار مهم لایه شـبکه در شـبکه مدارمـدارهای مجازی چیست.

R3 . تفاوت بین پیمودن مسیر و ارسال به دیگری چیست؟

R4 . آیا مسیر صاف کن ها در شبکه های نمودار اطلاعاتی و شبکه های با مدار مجازی از جدول های ارسالی اسـتفاده می کنند.؟ اگر چنین است جدول ها را برای هر دو شبکه توصیف کنید.

R5 . چند سرویس فرضی را که لایه شبکه می تواند برای یک بسته مجزا ارائه دهد توضیح دهید؟برای جریان بسته ها هم چنین کنید. آیا خدمات فرضی شما توسط لایه شبکه اینترنت تهیه شده اند ؟ آیا آنهـا بـا مـدل سـرویس CBR از ATM ارائه می شوند.؟ آیا سرویسی هستند که با ABR از مدل ATM گرفته شده باشد.

www.it98.ir

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

www.it98.ir

ب اگر هر VC مجاز به داشتن تعداد VC مختلف در لینک های مختلف در طول مسیر خود را (به طوری که جداول حمل و نقل باید VC ترجمه شماره) انجام چند ترکیب مختلف از ۴ تعداد 1) VC برای هر یک از ۴ لینک) می تواند مورد استفاده قرار گیرد؟

p5 در متن ما با استفاده از سرویس های کانکشن گرا برای توصیف لایه حمل و نقل خدمات و سرویس اتصال به لایه شبکه.

چرا مخفی کردن زیرکانه در اصطلاحات؟

P6. در بخش ۴,۳ ، ما اشاره کردیم که می توان بدون ورودی صف بندی وجود ندارد اگر پارچه سوئیچینگ است زمان محلی شما با نفر سریعتر از ورودی نرخ خط ، فرض نفر همه خطوط ورودی به خط نرخ مشابه دارد. توضیح دهید (در کلمه) که چرا این باید اتفاق بیفتد.

P7. در نظر بگیرید که یک روتر با سوئیچ ، ۲ پورت های ورودی (آ و ب) و ۲ پورت های خروجی (ج و د). فرض کنید سوئیچ عملیات را در ۱,۵ زمان شما با سرعت خط انجام می دهد.

آ. اگر ، برای برخی دلایل ، تمام بسته ها را از به توسعه به مقصد ، و تمام بستهها از ب به ج به مقصد ، می توانید پارچه روشن می شود به طوری که هیچ ورودی صف بندی پورت وجود دارد طراحی شده است؟ توضیح دهید که چرا و چرا نه در یک جمله.

ب فرض کنید در حال حاضر بسته ها از الف و ب به طور تصادفی انتخاب و به هر دو سی دی به مقصد می پارچه سوئیچ را طوری طراحی شده است که هیچ پورت ورودی صف بندی وجود دارد؟

توضیح دهید که چرا و چرا نه در یک جمله.

p8 در نظر بگیرید با استفاده از شبکه دادهای آدرس ۳۲ بیتی میزبان. فرض کنید تا به روتر ، ۴ لینک ، از ۰ تا ۳ شماره دار ، و بسته می شود به رابط لینک به عنوان فرستاده شرح زیر است :

آدرس لینک مقصد محدوده رابط

www.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

۰۰۰۰۰۰۰۰ ۰۰۰۰۰۰۰۰ ۰۰۰۰۰۰۰۰ ۱۱۱۰۰۰۰۰

میان	۰

۱۱۱۱۱۱۱۱ ۱۱۱۱۱۱۱۱ ۱۱۱۱۱۱۱۱ ۱۱۱۰۰۰۰۰

۰۰۰۰۰۰۰۰ ۰۰۰۰۰۰۰۰ ۰۰۰۰۰۰۰۰ ۱۱۱۰۰۰۰۱

میان	۱

۱۱۱۱۱۱۱۱ ۱۱۱۱۱۱۱۱ ۰۰۰۰۰۰۰۰ ۱۱۱۰۰۰۰۱

۰۰۰۰۰۰۰۰ ۰۰۰۰۰۰۰۰ ۰۰۰۰۰۰۰۱ ۱۱۱۰۰۰۰۱

میان	۲

۱۱۱۱۱۱۱۱ ۱۱۱۱۱۱۱۱ ۰۰۰۰۰۰۰۱ ۱۱۱۰۰۰۰۱

دیگر راهها	۳

www.it98.ir

آ. ارائه جدول حمل و نقل است که ۴ ورودی ، استفاده می کند مطابق طولانی ترین پیشوند ، و جلو بسته ها به واسطهای لینک درست باشد.

ب جدول چگونگی حمل و نقل خود را تعیین رابط مناسب برای ارتباط با datagrams آدرس های مقصد را پیدا کنید :

۱۱۰۰۱۰۰۰ ۱۰۰۱۰۰۰۱ ۰۱۰۱۰۰۰۱ ۰۱۰۱۰۱۰۱

۱۱۱۰۰۰۰۱ ۰۰۰۰۰۰۰۰ ۱۱۰۰۰۰۱۱ ۰۰۱۱۱۱۰۰

۱۱۱۰۰۰۰۱ ۱۰۰۰۰۰۰۰ ۰۰۰۱۰۰۰۱ ۰۱۱۱۰۱۱۱

p9 در نظر بگیرید با استفاده از آدرس های شبکه دادهای ۸ بیتی میزبان. فرض کنید یک روتر استفاده می کند مطابق طولانی ترین پیشوند است و جدول زیر حمل و نقل :

رابط	Prefix Match
۰	۰۰
۱	۰۱
۲	۱۰
۳	۱۱

برای هر یک از چهار رابط ، ارائه دامنه آدرس های مربوط به میزبان مقصد و تعداد آدرس های در محدوده می شود.

p10. در نظر بگیرید با استفاده از آدرس های شبکه دادهای ۸ بیتی میزبان. فرض کنید یک روتر استفاده می کند مطابق طولانی ترین پیشوند است و جدول زیر حمل و نقل :

رابط	
۰	۱
۱	۱۱

انجمن فناوری اطلاعات
www.it98.ir

۲ ۱۱۱

۳ راههای دیگر

برای هر یک از چهار رابط ، ارائه دامنه آدرس های مربوط به میزبان مقصد و تعداد آدرس های در محدوده می شود.

P11. روتر را در نظر بگیرید که interconnects 3 subnets : زیرشبکه ۱ ، زیرشبکه ۲ ، ۳ و زیر شبکه. فرض کنید همه رابط در هر یک از این ۳ subnets لازم به ۲۴/۲۲۳,۱,۱۷ پیشوند. همچنین فرض کنید که زیر شبکه ۱ مورد نیاز است برای حمایت از ۱۲۵ تا واسط ، و Subnets 2 و ۳ هر مورد نیاز برای حمایت از ۶۰ تا واسط. فراهم می کند که شبکه ۳ آدرس به صورت abcd / اکس) که برآوردن این محدودیتها.

P12. ۴,۲,۲ در بخش حمل و نقل به عنوان مثال جدول (با استفاده از طولانی ترین مطابق پیشوند) داده می شود. بازنویسی این جدول با استفاده از حمل و نقل abcd / نماد اکس به جای نماد رشته دودویی.

www.it98.ir

P13. مشکل در P7 از شما خواسته برای ارائه جدول حمل و نقل (با استفاده از طولانی ترین مطابق پیشوند). بازنویسی این جدول با استفاده از حمل و نقل abcd / نماد اکس به جای نماد رشته دودویی.

P14. در نظر بگیرید یک زیرشبکه با ۲۶/۱۰۱,۱۰۱,۱۰۱,۶۴ پیشوند. را نمونه ای از یک آی پی آدرس (از فرم xxx.xxx.xxx.xxx) است که می تواند به این شبکه قرار گرفتند.

فرض کنید صاحب ISP بلوک آدرس ۱۷/۱۰۱,۱۰۱,۱۲۸ فرم.

فرض کنید که میخواهد به ایجاد ۴ subnets از این بلوک با هر بلوک داشتن همان تعداد آدرس های آی پی. پیشوندهای (از فرم abcd چه هستند / ایکس) برای ۴ subnets؟

P15. در نظر بگیرید توپولوژی نشان داده شده در شکل ۴,۱۷. دلالت کردن 3 subnets با میزبان (در جهت عقربه های ساعت شروع ۰۰:۰۰) به عنوان شبکه های الف ، ب ، و ج) دلالت subnets بدون عنوان میزبان نمایش

مشخصات : د ، الکترونیکی ، و اف.

آ. آدرس شبکه اختصاص به هر یک از این ۶ subnets ، با محدودیت های زیر است : همه باید از آدرس ۲۳/۲۱۴,۹۷,۲۵۴ قرار گرفتند ؛ زیرشبکه باید آدرس به اندازه کافی برای حمایت از رابط ۲۵۰ ؛ اند باید آدرس زیر شبکه ب به اندازه کافی برای حمایت از ۱۲۰ واسطهای داشته باشد ؛ و آدرس زیر شبکه سی باید به اندازه کافی برای حمایت از ۱۲۰ رابط داشته باشد. البته ، subnets د ، الکترونیکی و اف باید هر یک قادر به پشتیبانی از رابط های ۲.

برای هر یک از زیر شبکه ، واگذاری باید به صورت abcd را / یا abcd ایکس / ایکس -- efgh / y.

ب با استفاده از پاسخ خود به بخش () ، ارائه جداول حمل و نقل (با استفاده از طولانی ترین مطابق پیشوند) برای هر یک از روترهای ۳.

P16. در نظر بگیرید ارسال دادهای ۳،۰۰۰ بایت به لینک است که MTU از ۵۰۰ کلمه در ادامه متن. فرض کنید دادهای اصلی با شماره شناسایی ۴۲۲ مهر. چگونه بسیاری از قطعات تولید شده؟ ویژگی های آنها چیست؟

P17. فرض کنید datagrams به ۱۵۰۰ کلمه در ادامه متن (از جمله هدر) بین منبع و مقصد میزبان هاست ب) با فرض ۲۰ بایت هدر آی چند datagrams خواهد بود ملزم به ارسال MP3 متشکل از ۴ میلیون کلمه در ادامه متن محدود؟

P18. راه اندازی شبکه را در نظر بگیرید که در شکل ۴,۲۲. فرض کنید که ISP به جای اختصاص روتر آدرس ۱۲۶,۱۳,۸۹,۶۷ که آدرس شبکه ای از شبکه خانگی است ۱۶/۱۹۲,۱۶۸.

آ. انتساب آدرس به تمامی واسط های شبکه ای در خانه.

ب فرض کنید هر میزبان دارای دو اتصال TCP مداوم ، همه به پورت ۸۰ در میزبان ۱۲۸,۱۱۹,۴۰,۸۶. فراهم می کند که ۶ مدخل متناظر در جدول ترجمه NAT.

P19. در این مساله خواهیم تاثیر NATs در برنامه های P2P اکتشاف.

فرض کنید همکار با نام کاربری آرنولد کشف از طریق پرس و جو که همکار با نام کاربری برنارد است فایل آن را می خواهد به خود دانلود کنید. همچنین فرض کنید که

www.it98.ir

wWw.it98.ir

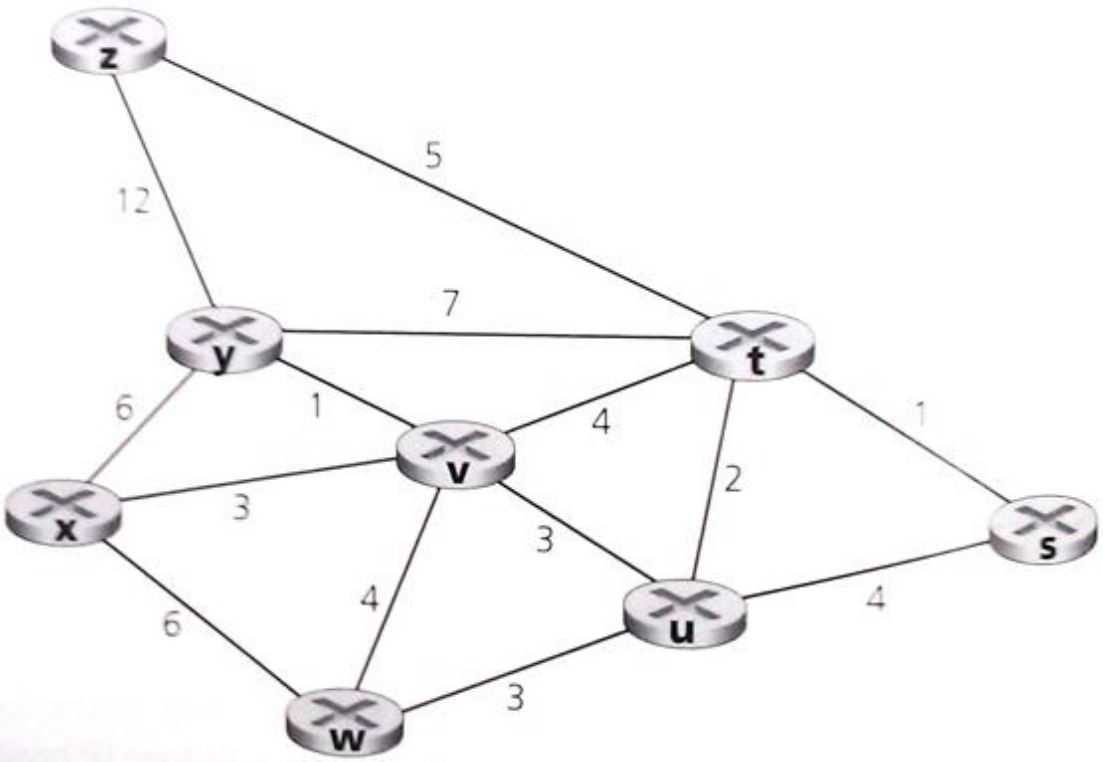
انجمن فناوری اطلاعات
www.it98.ir

برنارد آرنولد و هر دو در پشت NAT. سعی کنید که اجازه خواهد داد که روش آرنولد ارتباط TCP با برنارد پیکربندی NAT بدون برنامه خاص برای ایجاد را به تدبیر کردن. اگر شما مشکل دارند ابداع چنین تکنیک ، بحث چرا.

P20. نگاهی به شکل ۴,۲۷ ، شمردن از مسیرهای پنجم به y است که هیچ حلقه نیست.

P21. تکرار P20 مشکل برای مسیرهای از اکس وات ، وات به تو ، و الف به x.

P22. در نظر بگیرید شبکه زیر است. با لینک نشان داد هزینه ها ، استفاده از کوتاه ترین مسیر ، الگوریتم دیکسترا کوتاهترین مسیر برای محاسبه از اکس به تمام گره های شبکه. نشان دهد که چگونه الگوریتم آثار محاسبات جدول مشابه جدول ۴,۳.



P23. در نظر بگیرید شبکه نشان داده شده در P22 مشکل. با استفاده از الگوریتم دیکسترا.

www.it98.ir

و نشان دادن کار خود را با استفاده از جدول مشابه جدول ۴,۳ ، آیا به صورت زیر است :

آ. محاسبه کوتاه ترین مسیر از ثانیه به همه گره های شبکه.

ب محاسبه کوتاهترین مسیر از گره های شبکه تی به همه.

ج محاسبه کوتاه ترین مسیر از تو به تمام گره های شبکه.

د محاسبه کوتاهترین مسیر از گره های شبکه پنجم به همه.

ث محاسبه کوتاهترین مسیر از گره های شبکه به عرض همه.

اف. محاسبه کوتاهترین مسیر از گره های شبکه y به همه.

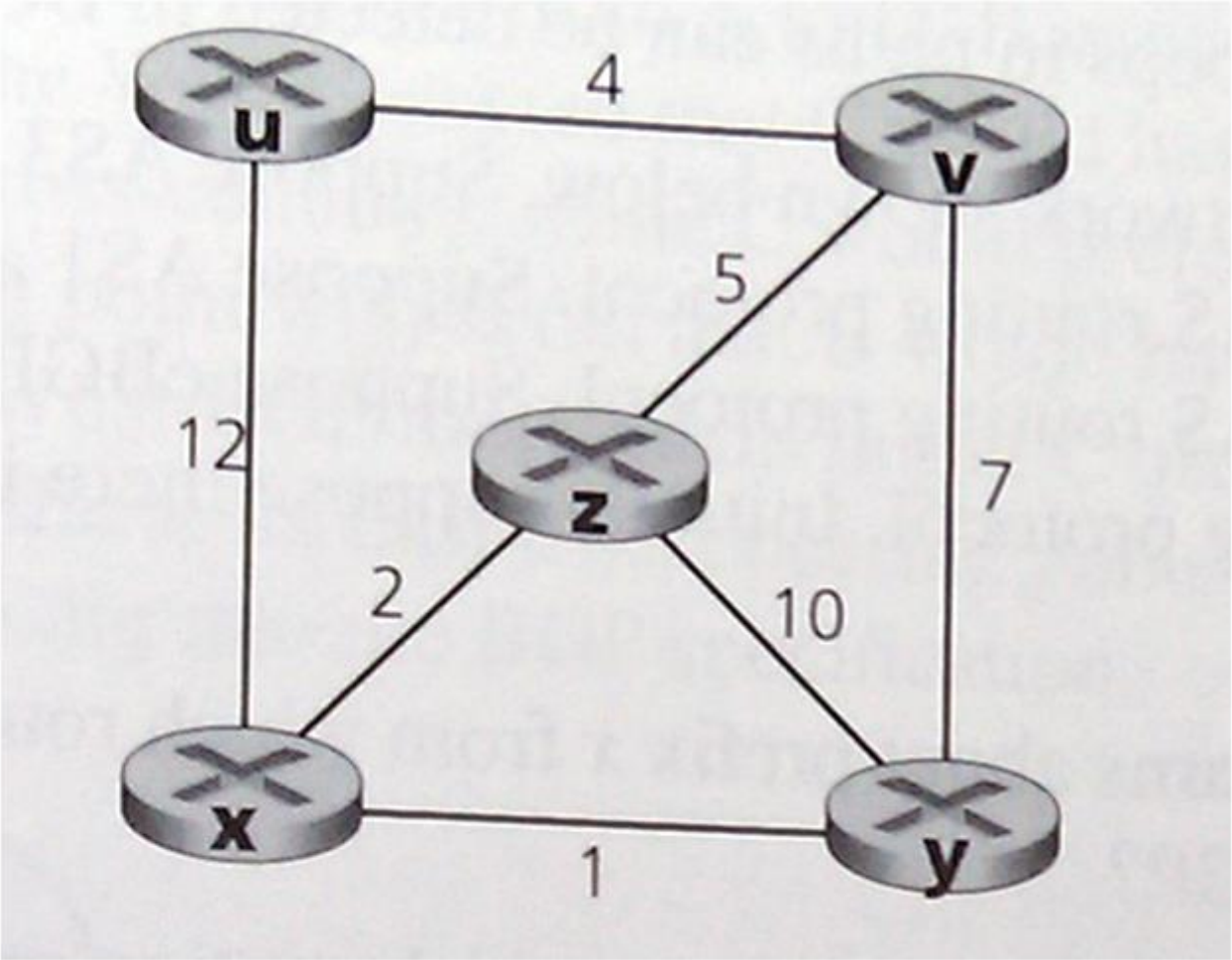
چ محاسبه کوتاه ترین مسیر از الف تا گره های شبکه ای همه.

www.it98.ir

p24. در نظر بگیرید شبکه زیر نشان داده شده ، و فرض کنیم که هر گره در ابتدا می داند به هزینه های هر یک از کشورهای همسایه است. در نظر بگیرید الگوریتم بردار فاصله ، را نشان دهد و در مدخل جدول فاصله گره از گره z.

wWw.it98.ir

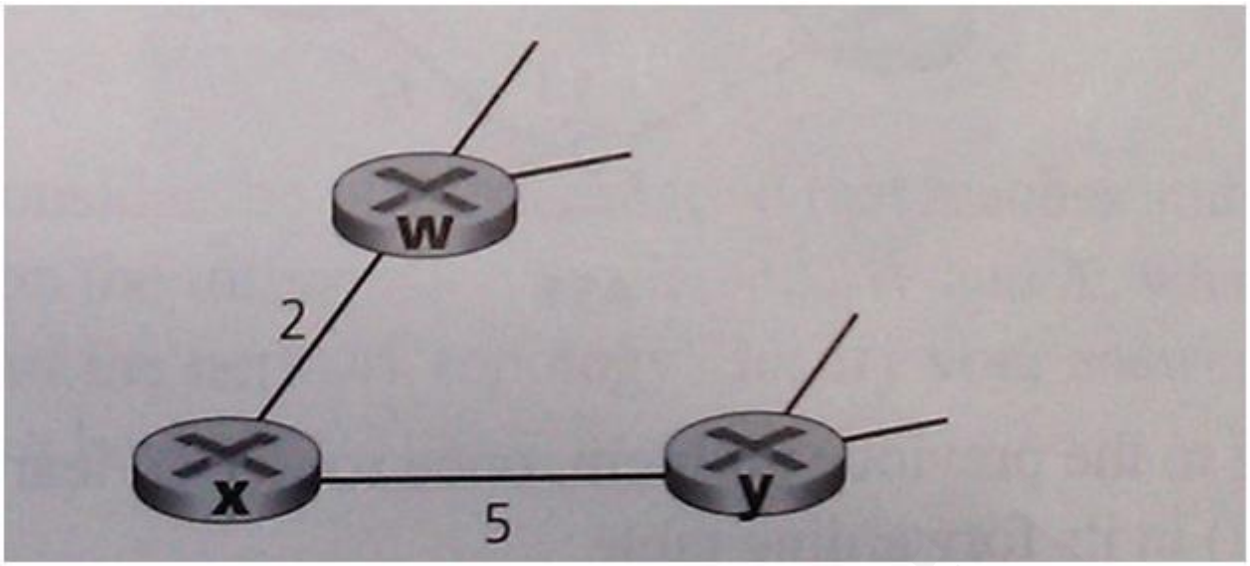
انجمن فناوری اطلاعات
www.it98.ir



P25. توپولوژی عمومی را در نظر بگیرید (یعنی ، شبکه خاصی در بالا نشان داده نمی شود) و نسخه همزمان از الگوریتم از راه دور ستونی است. فرض کنید که در هر تکرار ، مبادلات گره بردار فاصله خود را با همسایگان خود و دریافت از راه دور خود را بردار. با فرض این که الگوریتم آغاز می شود با هر گره دانستن تنها هزینه های فوری برای همسایگان خود ، حداکثر تعداد تکرار مورد نیاز قبل از همگرایی الگوریتم توزیع شده چیست؟ رنگ پس پاسخ خود را.

P26. در نظر بگیرید قطعه شبکه زیر نشان داده شده. اکس تنها ۲ همسایه وصل ، وات و y. وات تا مسیر حداقل هزینه به تو مقصد (نشان داده نمی شود) ۵ و y تا مسیر حداقل هزینه به تو ۶. مسیر کامل از وات و y به تو (و بین وات و y) نمایش داده می شود نیست. کلیه هزینه های پیوند را در شبکه به طور اکید مقادیر عدد صحیح مثبت است.

www.it98.ir



آ. اکس را در بردار فاصله برای عرض مقصد ، y ، و تو هستی.

ب لینک را هزینه تغییر برای هر ج (اکس ، وات) و یا ج (اکس ، y) به صورتی که ایکس خواهد شد همسایگان خود را از مسیر حداقل هزینه جدید را به تو اطلاع رسانی به عنوان یک نتیجه از اجرای الگوریتم از راه دور ستونی است.

ج - را لینک هزینه تغییر برای هر ج (اکس ، وات) و یا ج (اکس ، y) به صورتی که ایکس به همسایگان خود از راه حداقل هزینه جدید اطلاع به تو به عنوان یک نتیجه از اجرای الگوریتم بردار فاصله ، .

P27. در نظر بگیرید توپولوژی سه گره نشان داده شده در شکل ۴,۳۰. به جای داشتن هزینه های لینک نمایش داده شده در شکل ۴,۳۰ ، لینک هستند هزینه های ج (اکس ، y) = 5 ، ج (y ، الف) = ۶ ،

ج (الف ، ایکس) = ۲. محاسبه فاصله جداول پس از مرحله دهی اولیه و بعد از هر تکرار از نسخه تا همزمان از الگوریتم بردار فاصله ، (همانطور که در بحث قبلی ما را از شکل ۴,۳۰ بود).

P28. توصیف کنید که چگونه حلقه ها را در مسیر می توان در BGP شناسایی شده است.

www.it98.ir

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

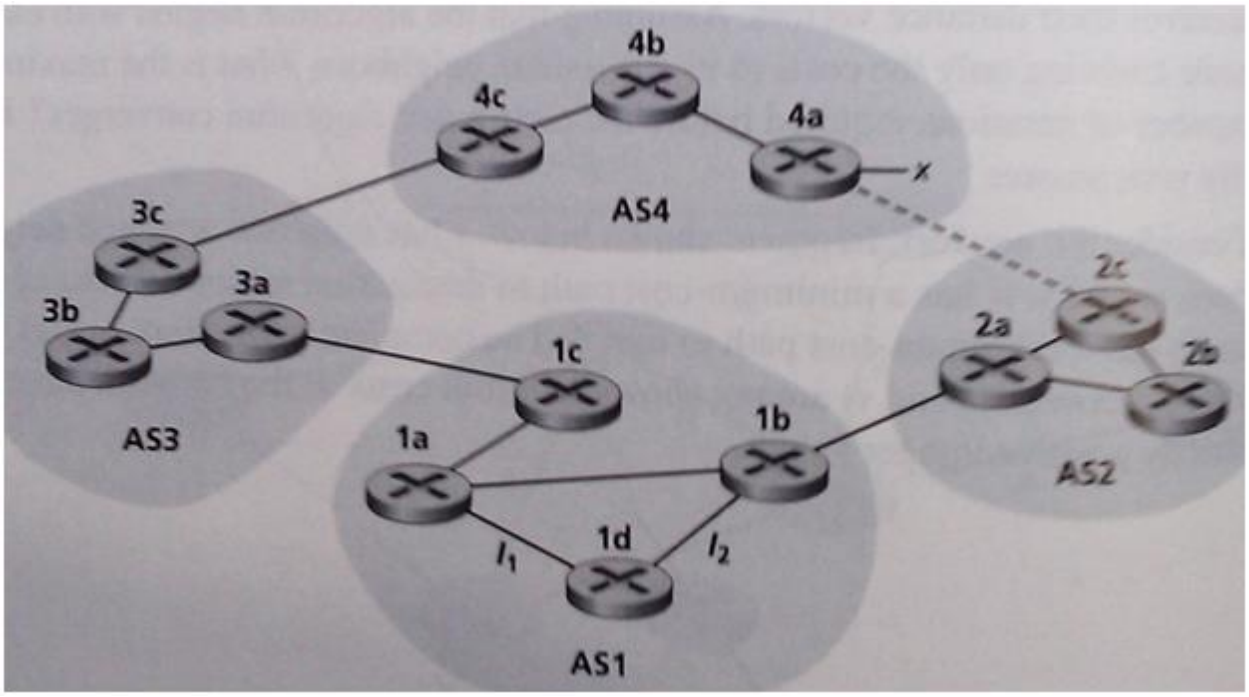
P29. در نظر بگیرید شبکه زیر نشان داده شده. فرض کنید AS2 AS3 و در حال اجرا هستند OSPF برای داخل خود را به عنوان پروتکل مسیریابی باشد. فرض کنید AS1 و AS4 در حال اجرا هستند را برای پاره کردن داخل خود را به عنوان پروتکل مسیریابی باشد. فرض کنید eBGV و iBGP برای بین پروتکل مسیریابی ع استفاده می شود ، در ابتدا فرض کنید هیچ پیوند فیزیکی بین AS2 و AS4 وجود دارد.

آ. از روتر C۳ یاد می گیرد در مورد پیشوند ایکس که از پروتکل مسیریابی : OSPF ، پاره کردن ، eBGP یا iBGP؟

ب. از روتر a۳ یاد می گیرد که در مورد ایکس از پروتکل مسیریابی؟

ج. از روتر 1c یاد می گیرد که در مورد ایکس از پروتکل مسیریابی؟

د. از روتر1d یاد می گیرد که در مورد ایکس از پروتکل مسیریابی؟



P30. با اشاره به مشکل قبلی ، یک بار D۱ روتر یاد می گیرد در مورد ایکس آن را در ورودی (اکس ، ۱) در جدول حمل و نقل است.

آ. آیا من می شود برابر با I1 I2 یا برای این مطلب؟ توضیح دهید که چرا در یک جمله.

ب حالا فرض کنید که یک لینک فیزیکی بین AS2 و AS4 ، نشان داده شده توسط خط نقطه چین وجود دارد.

www.it98.ir

فرض کنید D۱ روتر یاد می گیرد که اکس قابل دسترسی است از طریق AS2 و همچنین از طریق AS3 ، آیا من به I1 I2 یا تنظیم؟ توضیح دهید که چرا در یک جمله.

ج حالا فرض کنید یکی دیگر از ع ، به نام AS5 که دروغ در مسیر بین AS2 و AS4 (در نمودار نشان داده نشده است وجود دارد). فرض کنید D۱ روتر یاد می گیرد که اکس قابل دسترسی است از طریق AS2 الاغ AS4 و همچنین از طریق AS3 AS4. آیا من به مجموعه ای I1 یا L2؟ توضیح دهید که چرا در یک جمله.

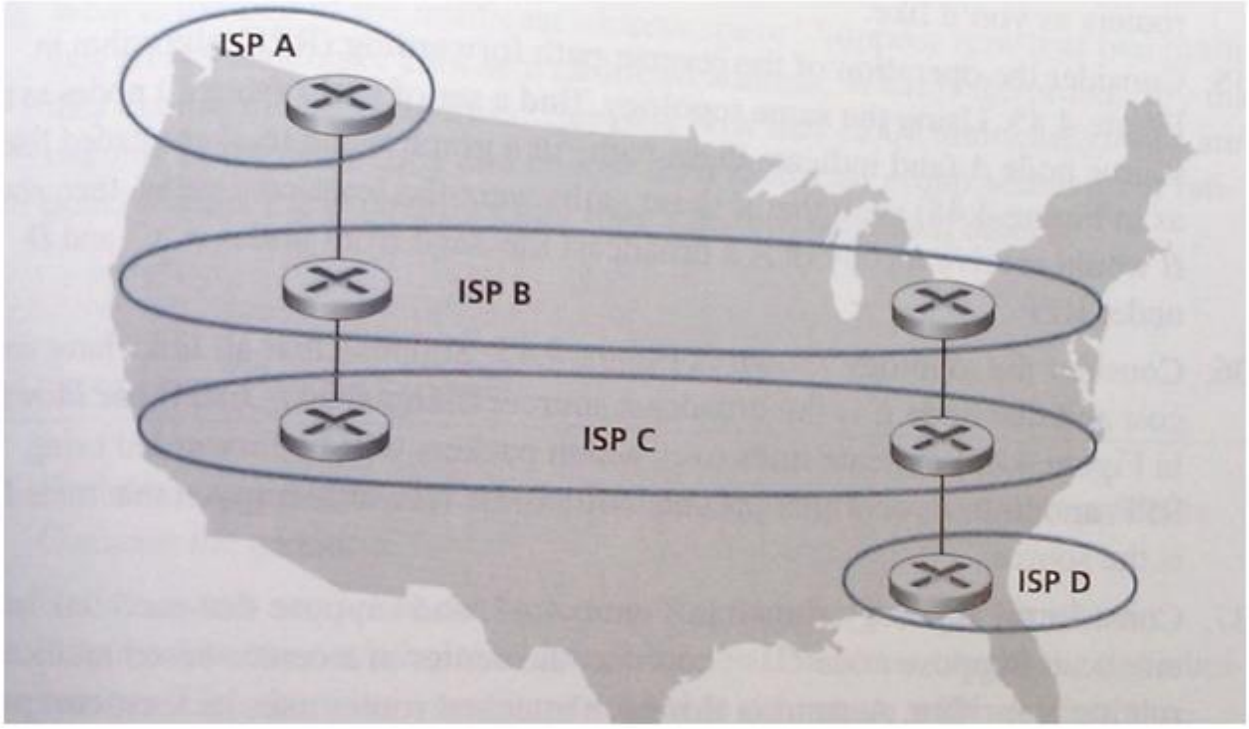
P31. در نظر بگیرید شبکه زیر است. ISP ارائه خدمات ب ستون فقرات ملی به منطقه ای ISP A. ISP سی فراهم می کند سرویس ستون فقرات ملی به منطقه ای ISP D.

هر ISP شامل ۱ ع. ب و ج با یکدیگر در دو محل با استفاده از BGP همکار. در نظر بگیرید رفتن از ترافیک به د ب ترجیح می دهید که ترافیک به بیش از سی به دست در ساحل غرب (به طوری که سی می توانست هزینه های حمل ترافیک های میدانی و صحرایی) به منظور جذب ، در حالی که سی ترجیح می دهید برای دریافت ترافیک از طریق آن ساحل شرق نقطه های مشابه با ب (به طوری که می توانست انجام ب ترافیک در سراسر کشور). چه ساز و ج ممکن است استفاده از BGP ، به طوری که ب را بیش از ترافیک به توسعه آن در شرق ساحل دست های مشابه نقطه؟ برای پاسخ به این سوال ، شما به حفاری به خصوصیات BGP نیاز دارند.

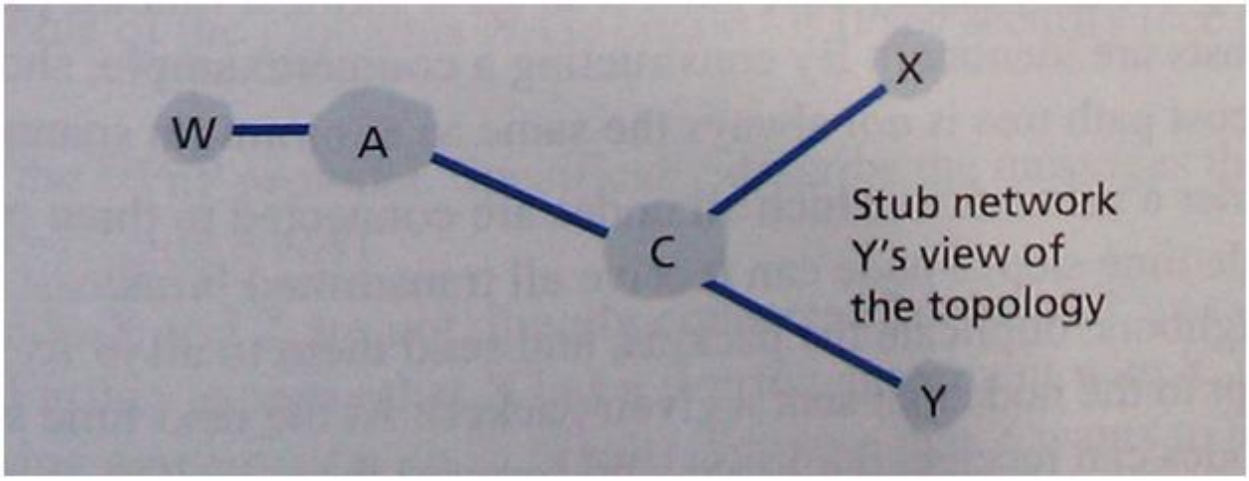
www.it98.ir

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir



P32. در شکل ۴,۴۳ را در نظر بگیرید که اطلاعات راه می رسد شبکه های خرد وات ، ایکس ، Y. در تاریخ و اطلاعات موجود در وات و اکس ، نظرات مربوطه می باشند از توپولوژی شبکه بر اساس چه؟ رنگ پس پاسخ خود را. مشاهده توپولوژی Y نشان داده شده است در زیر وارد نمایید.



• شبکه را در نظر بگیرید 8 - P33 گره (گره ها با برچسب به راست) ، در مسئله P22.

نمایش درخت حداقل هزینه در ریشه ها که شامل (به عنوان میزبان نهایی) گره تو ، پنجم ، عرض ، و y. غیررسمی چرا درخت درخت شما حداقل هزینه میکنند.

www.it98.ir

P34 . دور رویکرد اساسی مشخص برای دستیابی به پخش یعنی ، نمونه ساز یونی کاست (unicas Emulation) و لایه شبکه (مثل حمایت کننده مسیر یاب) ، و فرض کنید که درخت پوشای پخش کننده برای دستیابی به پخش لایه شبکه استفاده می شود. یک فرستنده و ۳۲ گیرنده را در نظر بگیرید. فرض کنید که فرستنده با یک درخت دودویی از مسیر یاب ها به گیرنده ها متصل شده است. ارزش ارسال بسته پخش شده در دو حالت نمونه سازی یونی کاست و پخش لایه شبکه در این وضعیت جغرافیایی چگونه خواهد بود ؟ هر زمانی که بسته (یا نومنه ای از بسته) به یک تک لینک فرستاده می شود ، موجب به وجود آمدن واحدی از ارزش می شود. چه وضعیت جغرافیایی ای برای بهم پیوستن فرستنده ، گیرنده ها و روتر ها موجب می شود که ارزش نمونه ساز یونی کاست و پخش لایه شبکه شما می توانید به دلخواه هر کدام از روتر ها را انتخاب کنید.

P35 . الگوریتم عملیات مسیر ارسالی معکوس (RPF) در تصویر ۴,۴۵ را در نظر بگیرید . از وضعیت جغرافیایی مشابه ای استفاده کنید ، مجموعه مسیر ها از تمام گره های به گره مبدا A (و مسیرهای نمایش داده شده در نمودار انبوه حبابی در تصویر ۴,۴۵) به طوری که اگر این مسیر ها کم ارزش ترین مسیر بودند را محاسبه کنید ، آنگاه گره B می تواند نمونه ای از پیام پخش شده A را از گره های A , C و D زیر پوشش RPF دریافت کند.

P36 . شکل جغرافیایی نمایش داده شده در تصویر ۴,۴۵ را در نظر بگیرید.فرض کنید تمام لینک ها واحد ارزشی دارند و گره E مبدا پخش کننده می باشد . همان طور که در تصویر ۴,۴۵ نشان داده شده از پیکان استفاده کنید . لینک های نمایش داده شده هر کدام از بسته هایی هستند که با استفاده از RPF هدایت شده اند، و لینک هایی که بسته های هدایت نشده را در گره مبدا E نشان می دهد.

P37 . شکل جغرافیایی نمایش داده شده در تصویر ۴,۴۷ را در نظر بگیرید ، فرض کنید هر کدام از لینک ها واحد ارزشی دارند. فرض کنید که گره C به عنوان مرکز در الگوریتم مسیر یابی چند منظوره مرکزی انتخاب شده است . هر کدام از روتر های پیوست شده به طور جداگانه از کم ارزش ترین مسیر به C برای ارسال پیام ها به C استفاده می کنند ، درخت مسیر یابی مبنا مرکز را رسم کنید . آیا درخت نتیجه ، کم مقدارترین درخت است ؟ پاسخ خود را توجیح کنید.

P38 . در بخش ۴,۵,۱ در مورد الگوریتم مسیر یابی LS Dijkstra آموختیم که مسیر های یونی کاست را که اختصاصا به مسیر های کم ارزش از مبدا به تمام مقصد ها اختصاص داشت ، محاسبه می کرد. اتصال بین این مسیر ها ممکن است شکلی از درخت مسیر کم ارزش یونی کاست را استدلال کند (یا درخت کوتاهترین مسیر یونی کاست ، اگر ارزش تمام لینک ها برابر باشد). با ساخت یک مثال شمارشگر نشان دهید که درخت مسیر کم ارزش همیشه شبیه به درخت پوشای مینیمم نیست.

www.it98.ir

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

P39 . شبکه ای که در آن هر گره با سه گره دیگر متصل است را در نظر بگیرید. در یک مرحله زمانی ، یک گره می تواند از مجاورانش تمام بسته های پخش شده را دریافت کند ، این بسته ها را تکثیر کند و به مجاورانش ارسال کند (به جز به گره ای که از آن بسته را دریافت کرده). در مرحله زمانی بعدی ، گره های مجاور میتوانند بسته ها را دریافت ، تکثیر و هدایت کنند و به همین ترتیب ادامه پیدا می کند. فرض کنید که سیل کنترل نشده ای پخش کننده در این شبکه استفاده شود. در مرحله زمانی بعدی ، چند تا از نمونه های بسته های پخش شده ارسال خواهند شد ، که هر کدام جداگانه در مرحله زمانی اول ، از یک بسته ارسال شده توسط گره مبدا به سه گره پخش شده است .

P40 . در بخش ۴,۷ دیدیم که هیچ گونه پروتکلی در لایه شبکه برای تعیین تعداد میزبان ها در یک گروه با چندین ماشین وجود ندارد. معین کنید که چگونه می توان برنامه های چند شبکه ای را برای شناسایی و تعیین میزبان های شرکت کننده در گروه چند شبکه ای ، توسعه داد ؟

P41 . پروتکل برنامه ای را طراحی کنید (شرحی از شبه کد) که آدرس های تمام میزبان های شرکت کننده در یک گروه چند شبکه ای نگهداری کند. مخصوصا معین کنید سرویس شبکه ای (چند شبکه ای یا یونی کاست) را که از این پروتکل استفاده می کنند ، و نشان دهید که پیامی را که پروتکل ارسال میکند به صورت نوار است یا خیر (راجع به داده های برنامه میان شرکت کننده های موجود در چند شبکه) و چرا .

P42 . اندازه فضای آدرس های چند شبکه ای چقدر است ؟ فرض کنید دو تا گروه شبکه ای به صورت تصادفی به عنوان آدرس چند شبکه ای انتخاب می شوند . احتمال این که در یک آدرس مشابه انتخاب شوند چقدر است ؟ فرض کنید ۱۰۰۰ گروه چند شبکه ای در یک زمان به صورت تصادفی آدرس های خود را انتخاب می کنند. احتمال اینکه با هم تداخل پیدا کنند چقدر است ؟

بحث و پرسش

D1 . سه شرکت پیدا کنید که محصولات روتر سرعت بالای خود را می فروشند.
محصولات را با هم مقایسه کنید.

D2 . از سیستم اینترنت که اطلاعات یک شخص را در شبکه از بانکهای اطلاعاتی ارائه می دهد (Whois Service) در شرکت ثبت شماره های اینترنت آمریکا برای تعیین قالب آدرس های IP برای سه دانشگاه استفاده کنید. آیا می توان از این سیستم برای تعیین قطی مکان جغرافیایی یک IP آدرس خاص استفاده کرد ؟

D3 . آیا امکان نوشتن برنامه Ping Client (استفاده از پیام های ICMP) در جاوا هست ؟ آری یا خیر ؟ چرا؟

D4 . در بخش ۴,۴ نشان دادیم که گسترش IPv6 بسیار آرام است. چرا این توسعه آرام انجام می شود ؟ چه چیزی نیاز است تا این گسترش تسریع یابد؟

D5 . در مورد چند مشکل NAT ساخته شده برای امنیت IPsec بحث کنید (مراجعه به [phifer 2000]).

D6 . در مورد پروتکل UPnP تحقیق کنید. مخصوصا در مورد میزبان هایی که از NAT استفاده میکنند توضیح دهید.

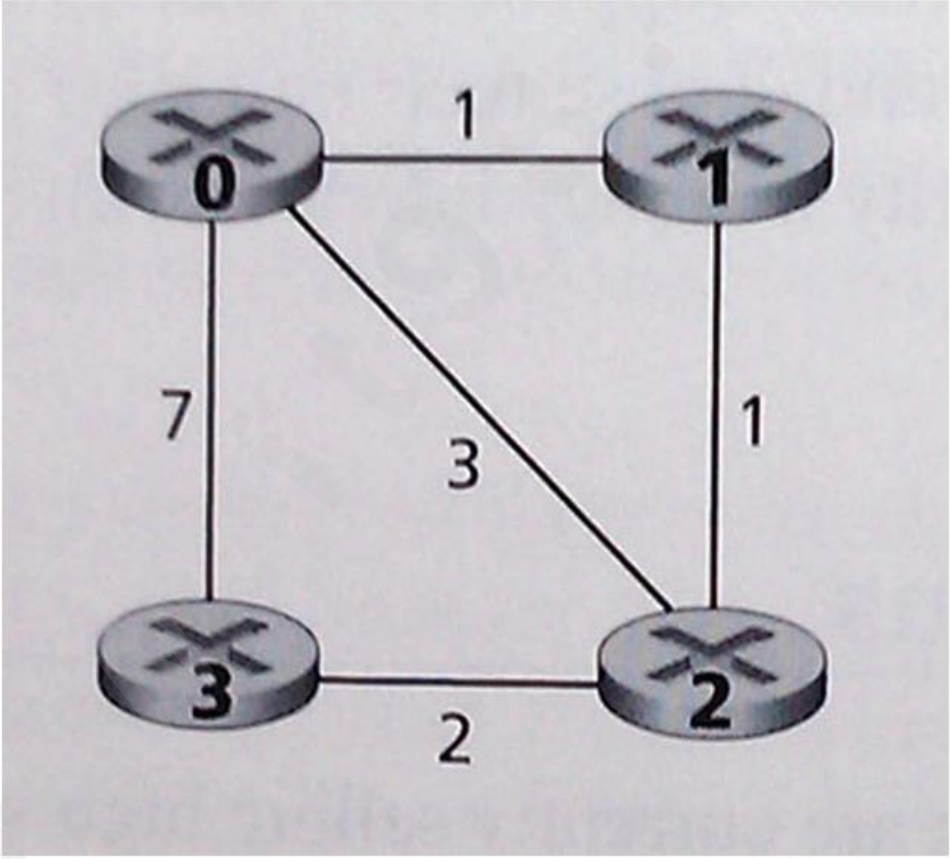
www.it98.ir

D7 . فرض کنید ASهای x و z به طور مستقیم به هم متصل نیستند در عوض به y AS متصل شده اند . بعلاوه فرض کنید x همتای y باشد ، و همچنین y همتای z باشد. در نهایت ، فرض کنید که z می خواهد از راه ترافیکی y گذر کند اما نمی خواهد از راه ترافیکی x عبور کند . آیا BGP اجازه می دهد به z که این سیاست را اجرا کند ؟

D8 . در بخش ۴,۷ ما تعداد برنامه های چند شبکه ای را نشان دادیم. کدامیک از این سرویس ها برای مدل سرویس چند شبکه ای کوچک اینترنت بهتر می باشد ؟ چرا ؟ کدامیک از این برنامه ها مخصوصا برای این مدل سرویس است ؟

در این مبحث برنامه نویسی ، شما باید مجموعه ای از شیوه های توزیع شده ناهماهنگ در مسیریابی DV برای شبکه ای که در پایین نمایش داده شده بنویسید.

شما باید برنامه ای عادی بنویسید که ناهماهنگی بین اجزای شبیه سازی شده در محیط تهیه شده برای این ماموریت محاسبه کند. برای گره 0 باید اینگونه بنویسید:



- rtinit0(). این جریان یکبار در شروع نمونه سازی صدا زده می شود. rtinit0() هیچ گونه استدلادی ندارد. کارش این است که جدول مسافت گره ۰ را ارزش دهی مستقیم ۱ ، ۳ و ۷ بترتیب به گره های ۱ ، ۲ و ۳ مقدار دهی اولیه کند. در تصویر نمایش داده شده بالا تمامی لینک ها دو طرفه و ارزش آنها در دو طرف برابر است. بعد از مقدار دهی اولیه جدول مسافت و هرگونه ساختار داده ای مورد نیاز برای جریان گره ۰ ، باید

www.it98.ir

wWw.it98.ir

اتصالی مستقیم به مسیر کمترین ارزش مجاورانش در تمام شبکه های دیگر ایجاد کند (یعنی ۱ ،۲ و ۳) . اطلاعات کمترین ارزش با صدا زدن جریان tolayer2() با بسته های بروز شده مسیر یابی به گره های مجاورش ارسال می کند. اینگونه از بسته های بروز شده مسیر یابی همواره در انتقالات کامل توصیف می شوند.

- .rtupdate0(struct rtpkt *rcvdpkt). این جریان موقعی صدا زده می شود که گره ۰ بسته های بروز شده مسیر یابی که ارسال کرده بود را از یکی از مجاورانش دریافت کند. پارامتر rcvdpkt* نشانه گری است برای بسته های دریافت شده rtupdate0() که به عنوان قلب الگوریتم DV معروف است. مقادیر در یافت شده در بسته های بروز شده مسیر یابی از گره i دارای ارزش کوتاه ترین مسیر i به تمام گره های شبکه ای دیگر است. rtupdate0() از این مقادیر دریافت شده برای بروز رسانی جدول مسافت خود استفاده می کند (که مخصوص الگوریتم DV است). اگر ارزش کمترین مقدار مسیر خود به گره های دیگر در بروز رسانی تغییری پیدا کند ، node() به مجاوران مستقیمش این تغییر را با فرستادن بسته مسیر یابی اطلاع می دهد. این را در الگوریتم DV بیاد بیاورید.

www.it98.ir

الگوریتم ، تنها به طور مستقیم گره های متصل خواهد تبادل مسیریابی بسته ها. بنابراین ، ۱ و ۲ با هم در ارتباط هستند ، اما گره های ۱ و ۳ نمی خواهند با یک دیگر ارتباط برقرار کند.

روال مشابه هستند برای گره های ۱ ، ۲ ، ۳ و تعریف شده است. بنابراین ، شما در تمام مراحل ۸ : rtinit0 () ، نوشتن rtinit1 () ، rtinit2 () ، rtinit3 () ، rtupdate0 () ، rtupdate1 () ، rtuplate2 () ، و rtupdate3 (). این روال با هم خواهد توزیع شده ، محاسبات ناهمزمان از جداول از راه دور برای توپولوژی و هزینه های نمایش داده شده در شکل را در صفحه قبل از اجرا.

شما می توانید جزئیات کامل ماموریت های برنامه نویسی ، پیدا کردن و همچنین کد سی که شما نیاز به سخت افزار شبیه سازی / محیط نرم افزاری ، در http://www.awl.com/kurose-ross ایجاد کنید. نسخه جاوا از واگذاری نیز موجود است.

آزمایشگاههای اتیری

به همراه وب سایت برای این کتاب درسی ، http://www.awl.com/kurose-ross ، شما ۲ اتیری تکالیف آزمایشگاه پیدا کنید. آزمایشگاه ۱ بررسی عملکرد پروتکل آی پی و آی پی با فرمت دادهای خاص. آزمایشگاه ۲ به بررسی استفاده از پروتکل مینویسد در پینگ و دستورات traceroute.

مصاحبه با...

Vinton G. Cerf

Vinton G. Cerf معاون رئیس جمهور و رئیس کشیش اینترنت برای گوگل است. او برای بیش از ۱۶ سال در همراه اول در سمت های مختلف خدمت کرده است ، تا پایان دوره تصدی خود را در آنجا به عنوان معاون ارشد رییس جمهور و فناوری برای استراتژی. او به طور گسترده به عنوان همکاری طراح تیسیپی / پروتکل آی پی و معماری از اینترنت شناخته شده است. در طی این مدت ۱۹۷۶ - ۱۹۸۲ در وزارت دفاع آمریکا طرح های پژوهشی پیشرفته آژانس (دارپا) او نقش کلیدی رهبری توسعه اینترنت و اینترنت مربوط به بسته اطلاعاتی داده ها و تکنیک های امنیتی است. او مدال ریاست جمهوری ایالات متحده از آزادی در سال ۲۰۰۵ و ایالات متحده مدال ملی فناوری در سال ۱۹۹۷ دریافت کرد. وی دارای لیسانس ریاضیات از دانشگاه استنفورد و کارشناسی ارشد و دکترا در رشته علوم رایانه ای را از UCLA.

www.it98.ir

wWw.it98.ir

انجمن فناوری اطلاعات
www.it98.ir

چه چیزی در شبکه به شما اختصاص دارد؟

من به عنوان برنامه نویس در UCLA در اواخر s۱۹۶۰ مشغول به کار بود. کار من شده توسط دفاع آمریکا آژانس پروژه های تحقیقاتی پیشرفته (آرپا نامیده می شود و سپس مورد حمایت قرار گرفت ، موسوم به دارپا در حال حاضر). من در آزمایشگاه پروفسور لئونارد Kleinrock در شبکه اندازه گیری مرکز ARPAnet به تازگی ایجاد شده مشغول به کار بود. گره ۱ از ARPAnet بود در UCLA در تاریخ ۱ سپتامبر نصب شد ، ۱۹۶۹. من مسئول برنامه های کامپیوتری که به هنگام ثبت نام اطلاعات مربوط به عملکرد ARPAnet و گزارش این اطلاعات را به عقب برای مقایسه با مدل های ریاضی و پیش بینی ها از عملکرد شبکه مورد استفاده قرار گرفت.

چندین نفر از دانشجویان فارغ التحصیل دیگر و من مسئول کار بر روی به اصطلاح میزبان پروتکل های سطح از ARPAnet ---- روش ها و فرمت های که انواع مختلفی از کامپیوترها در شبکه اجازه می دهد تا با یکدیگر ارتباط برقرار ساخته بودند. این اکتشافات شگفت انگیز به دنیای جدید (برای من بود) از توزیع محاسبات و ارتباطات.

آیا شما تصور کنید که آی پی را به عنوان فراگیر آن که امروز می توانید به طراحی پروتکل بپردازید وجود داشته است؟

هنگامی که باب کان و من برای اولین بار در تاریخ در سال ۱۹۷۳ این کار را می کردیم ، من فکر می کنم ما خیلی بیشتر بود در سوال مرکزی تمرکز : چگونه می توان شبکه های ناهمگن بسته میان عملیاتی آن با یکدیگر ایجاد می کنیم ، فرض کنیم در واقع نمی تواند تغییر شبکه های خود را دارند. ما امیدوار است که ما می تواند راه را برای مجوز مجموعه دلخواه بسته ، شبکه های تغییر در مد پیوسته پیدا شفاف شود ، به طوری که کامپیوتر میزبان می تواند پایان به انتها بدون نیاز به هیچ ترجمه ها را در بین ارتباط برقرار کند. من فکر می کنم ما می دانستیم که با تکنولوژی قدرتمند و قابل ارتقا خرید و فروش بودند ، اما من شک ما تا به حال تصویر روشنی از آنچه می خواهم دنیا را با صدها میلیون کامپیوتر می شود همه در اینترنت پیوسته.

شما چه هم اکنون برای آینده شبکه و اینترنت چه چیزی را پیش بینی می کنید؟ چه چالش عمده / موانع فکر میکنید دروغ در آستانه در توسعه خود را؟

به اعتقاد من اینترنت و شبکه خود را به طور کلی به تکثیر خود ادامه خواهد داد. در حال حاضر شواهد قانع کننده ای

www.it98.ir

وجود خواهد داشت که میلیاردها اینترنتی دستگاه موجود بر روی اینترنت فعال شود ، از جمله وسایل مانند تلفن های همراه ، یخچال ، دستیار شخصی دیجیتال ، سرور خانه ، تلویزیون ، و نیز آرایه معمول لپ تاپ ها وجود دارد ، سرویس دهنده ها ، و غیره . چالش های بزرگ شامل پشتیبانی برای تحرک ، عمر باتری ، ظرفیت لینک های دسترسی به شبکه ، و توانایی به مقیاس هسته نوری شبکه در مد نامحدود است. طراحی سیارات گسترش اینترنت پروژه که در آن من عمیقا درگیر در آزمایشگاه پیشرانش جت است. ما نیاز به کاهش بیش از از IPv4 [۳۲ بیتی آدرس] به IPv6 [128] بیت. لیست طولانی است!

چه کسی به شما الهام حرفه ای داد؟

من همکار باب کان ؛ مشاور پایان نامه من ، جرالد Estrin ؛ بهترین دوست من ، استیو کروکر (ما در دبیرستان ملاقات کرد و او به من معرفی کرد که به کامپیوتر در سال ۱۹۶۰!) ؛ و هزاران تن از مهندسان که در ادامه به تحول اینترنت امروز.

آیا شما هر گونه مشاوره برای دانش آموزان ورود به شبکه / حوزه اینترنت را درست می دانید؟

فکر کنید در خارج از محدودیت های موجود سیستم های - تصور آنچه ممکن است ممکن ؛ اما پس از آن انجام کار سخت بدانند چگونه می توان به آنجا برسیم از وضعیت فعلی امور. دره به رویا : همکاران دوازده و نیم من در آزمایشگاه پیشرانش جت کار کرده اند در طرح توسعه واقع در بین سیارات از اینترنت زمینی. ممکن است چند دهه به اجرای این ، ماموریت توسط ماموریت گرفتن ، بلکه برای ترجمه و تفسیر : "رسیدن به انسان باید درک او ، یا آسمان ها برای چه بیش از؟"

کاملترین مجموعه نمونه سوالات بهمراه پاسخنامه تستی و تشریحی، جزوه، اسلاید، حل تمرین، گزارش آزمایشگاه و کارآموزی، پروژه و... در سایت:
www.it98.ir
مرجع دانشجویان رشته کامپیوتر دانشگاه پیام نور