مرکز آموزش عالی جهاد دانشگاهی
شعبه صنعتی اصفهان

# مسیریابی

## پروژه دوره کارشناسی
## در رشته کامپیوتر گرایش نرم افزار

توسط:

محسن زوله

استاد راهنما:

مهندس محمدرضا مصلحی

تیر ماه 89

## پیشگفتار:

از بررسی و قضاوت در مورد تحقیقاتی که هم اکنون صورت می پذیرد می توان بـه ایـن نتیجـه رسـید کـه مسیریابی در اینترنت جزء اکثر مواردی است که رغبت بدان هم چنان تنزل نیافته اسـت .مخصوصـا مسـیریابی مبتنی بر کیفیت سرویس (QOS) در سالهای اخیرگواه صحت این ادعاست.

در طول دهه اخیر،اینترنت از پروژه های تحقیقاتی ارتباطات که دنیای ما را برای همیشه دچار تحول ساخته اند،فراتر رفته است.پیام های فوری،تلفنی ip،فیلم و موسقی های درخواستی،بانکداری؛تنها بخشی از کاربرد هـای فراوانی هستند که زندگی ما را راحتر کرده اند.اما تکنولوژی و فناوری که ما را قادر به اسـتفاده از ایـن امکانـات می کند شبکه های کامپیوتری و نحوه ی ارتباط بین این شبکه ها می باشد.اینترنت که بزرگترین ابزار برای ارائه خدمات فوق می باشد از چندین هزار شبکه کوچک تشکیل شده است که برای برقراری ارتباط و تبادل اطلاعـت بین این شبکه ها به یک شبکه گسترده دیگر نیاز دارد که backbone نامیده می شود، و دارای device هـای مختلف از جمله router است ،نحوه ی رد و بدل شدن پیام ها بین router ها اساس کار این backbone مـی باشد،ما به دلیل اهمیتی که این تکنیک ارسال و دریافت پیام از یک نتقطه به نقطه دیگر دارد روش های مختلف انجام این کار را بررسی می کنیم و در نهایت بهترین و مناسب ترین روش انجام کار را به صـورت کامـل بررسـی می کنیم.

اساس آغاز یک پروژه نظریه فکر یا خواسته ای است که توسط شخص یا اشـخاص یـا سـازمانی مطـرح مـی شود.هدف از انجام این پروژه تحلیل و چگونگی کار پروتکل های مسیر یـابی و مقایسـه آنهـا و بررسـی پروتکـل OSPF به طور کامل و ارائه تکنیک های هوش مصنوعی برای بهبود کارایی این پروتکل است.

توضیحات ذیل درباره فصل های این پروژه است و ایده کلی از این پروژه را در اختیار شما قرار خواهد داد.

- فصل اول، تعریف کلی از مسیریاب و کاربرد آن در شبکه های کامپیوتری و معیار های مختلف برای یک الگوریتم مسیریابی ونحوه مسیریابی پروتکل IP به صورت ایستا را ارائه می دهد.
- فصل دوم، پروتکل مسیریابی OSPF و مزایای آن و چگونگی اجرای این الگوریتم در مسیریاب های سیسکو را بیان می کند.

- فصل سوم، طراحی و پیاده سازی مدل فازی الگوریتم OSPF و تجزیه و تحلیل این الگوریتم را بیان می کند.
- فصل چهارم،مسیریابی چند منظوره وچگونگی مسیریابی چند منظوره OSPF را توضیح می دهد.

تقدیم به ساحت مقدس یوسف زهرا (عج)

که چشم ها برای زیارت صبحش بیدارند...

وقتی که دانش و اطلاعات شخصی منظم نباشد هر چه که بیشتر بداند آشفته تر می شود.

**(اسپنسر)**

دانش محصول تحقیق تحقیق حاصل تلاش انسانهایی مصمم و با اراده است که بر این باورند بایستی وظیفه خود را به جامعه بشری ادا نمایند.و بدون شک بزرگان تحقیق و پژوهش در هر دانش همچو چراغی فروزان و راهنمایی دلسوز آیندگان جامعه خود را در کمال آرامش به سوی اهداف متعالی رهنمون می سازند.بنابراین بر خود می دانم بعنوان شاگردی بی ادعا اما علاقمند نهایت قدردانی و سپاسگذاری از همه پویندگان دانش کامپیوتر داشته باشم . و به ویژه دستان گرم و سخاوتمند استادان گرانقدر جناب آقای مهندس مصلحی وجناب آقای مهندس مطیعی را به گرمی بفشارم که در این راه از هیچ کمک و تلاشی دریغ ننمودند.

با این امید که در نقدی منصفانه قوت کار را محصول تلاش بزرگان این دانش تا به امروز،و ضعف آنرا حاصل تجربه اندک و بضاعت ناچیز علمی پژوهشگر بدانیم و از نظرات و پیشنهادات سازنده خود او را بی بهره نسازیم.

در پایان دست شما خواننده گرامی را بعنوان دوستی جدید می فشارم و بدین دوستی افتخار خواهم کرد.

**یا رب از ابر هدایت برسان بارانی**

**پیشتر زآنکه چوگردی زمیان برخیزم**

# فهرست مطالب

**عنوان** **صفحه**

# فهرست اشکال

**عنوان** **صفحه**

## چکیده:

امروزه علم کامپیوتر به حدی پیشرفت کرده که بسیاری از علوم دیگر پیشرفتشان وابسته به علم کامپیوتر می باشد.شبکه های کامپیوتری به حدی پیشرفت کرده اند که توانسته اند جهان را به یک دهکده علمی کوچک تبدیل نمایند.برای برقراری ارتباط بین این شبکه ها نیازمند به یک ستون فقرات می باشیم، این شبکه زیر بنایی که از تعداد زیادی مسیریاب تشکیل شده است وظیفه انتقال اطلاعات را دارد. بر روی این مسیریاب ها باید الگوریتم هایی اجرا شوند تا بتوانند بهترین مسیر را برای انتقال اطلاعات در این دهکده را انتخاب کنند.

مجموعه مطالبی که در اختیار شما خواننده گرامی است پژوهشی در رابطه با مسیریابی در شبکه های جهانی اینترنت و بررسی الگوریتم های مسیریابی متفاوت ،تجزیه و تحلیل،نحوه پیاده سازی این الگوریتم ها به صورت کاربردی می باشد.

# فصل اول
# مسيريابي بسته هاي IP

## 1-1مسیر یاب(ROUTER):

محیط‌های شبکه پیچیده می‌توانند از چندین قسمت که از پروتکل‌های مختلف با معماری‌های متفاوت هستند، تشکیل شده باشند. در این حالت ممکن است استفاده از پل برای حفظ سرعت ارتباطات بین قسمت‌های شبکه مناسب نباشد. در این محیط های شبکه‌ای پیچیده و گسترده به دستگاهی نیاز خواهد بود تا علاوه بر دارا بودن خواص پل و قابلیت‌های تفکیک یک شبکه به بخش‌های کوچکتر، قادر به تعیین بهترین مسیر ارسال داده از میان قسمت‌ها نیز باشد. چنین دستگاهی Router یا مسیریاب نام دارد.

مسیریاب‌ها در لایه شبکه مدل OSI عمل می‌کنند. مسیریاب‌ها به اطلاعات مربوط به آدرس‌دهی شبکه دسترسی دارند و در نتیجه قابلیت هدایت بسته‌های داده را از میان چندین شبکه دسترسی دارا هستند. این عمل از طریق تعویض اطلاعات مربوط به پروتکل‌ها بین شبکه‌های مجزا در مسیریاب ها انجام می‌شود. در مسیریاب از یک جدول مسیریابی برای تعیین آدرس‌های داده‌های ورودی استفاده می‌شود.

در لایه های مختلف سویچینگ داریم ،که سویچینگ لایه سوم را مسیر یابی گویند.فرآیند مسیر یابی همانند فرآیند انتقال نامه در دفاتر پستی می باشد.

مسیریاب‌ها بر اساس اطلاعات موجود در جداول مسیریابی، بهترین مسیر عبور بسته‌های داده را تعیین می‌کنند. به این ترتیب ارتباط میان کامپیوترهای فرستنده و گیرنده مدیریت می‌شود مسیریاب‌ها فقط نسبت به

عبور حجم زیادی از بسته‌های داده‌ای معروف به پدیده طوفان انتشار یا Broadcaste Storm را به شبکه نمی‌دهند.

مسیریاب‌ها بر خلاف پل‌ها می توانند چند مسیر را بین قسمت‌های شبکه LAN انتخاب کنند. به علاوه قابلیت اتصال قسمت‌هایی که از شکل‌های بسته‌بندی داده‌ها متفاوت استفاده می‌کنند، را نیز دارند.

مسیریاب‌ها می‌توانند بخش‌هایی از شبکه را که دارای ترافیک سنگین هستند، شناسایی کرده و از این اطلاعات برای تعیین مسیر مناسب بسته‌ها استفاده کنند. انتخاب مسیر مناسب بر اساس تعداد پرش‌هایی که یک بسته داده باید انجام دهد تا به مقصد برسد و مقایسه تعداد پرش‌ها، انجام می‌گیرد. پرش (اخح) به حرکت داده از یک مسیریاب بعدی اطلاق می‌شود.

مسیریاب‌ها بر خلاف پل‌هادر لایه شبکه (مدل OSI) کار می‌کنند و در نتیجه قادر به هدایت بسته‌های داده به شکل مؤثری هستند. آنها قابلیت هدایت بسته‌های داده را به مسیریاب‌های دیگر که ادرس آن‌ها خود شناسایی می‌کنند، نیز دارند. همچنین مسیریاب‌ها برخلاف پل‌ها که فقط از یک مسیر برای هدایت داده استفاده می‌کنند، می توانند بهترین مسیر را از بین چند مسیر موجود انتخاب کنند.

Brouler دستگاهی است که خواص پل و مسیریاب را با هم ترکیب کرده است Brouler در برابر پروتکل‌های با قابلیت مسیریابی به صورت یک مسیریاب عمل می‌کند و در دیگر موارد در نقش یک پل ظاهر می‌شود.

فرآیند دریافت یک واحد داده دارای هویت ،از یکی از کانال های ورودی و هدایت آن بر روی کانال خروجی مناسب ،بنحوی که بسوی مقصد نهایی خود نزدیک و رهنمون شود را سویچینگ گویند.

## 2-1تفاوت يك سوييچ لايه ۳ با يك مسيرياب معمولي:

سوییچینگ لایه ۳ (L3 Switching) و مسیریابی (Routing) هر دو به یک مضمون اشاره دارند : هدایت هوشمند بسته ها بر روی خروجی مناسب براساس آدرسهای جهانی و سرآیندی که در لایه ۳ به داده ها اضافه شده است. منظور از هدایت هوشمند نیز آن است که الگوریتمی بکار گرفته می شود تا کوتاهترین و بهینه ترین مسیرها محاسبه شده و براساس آن مسیر خروج بسته ها انتخاب گردد.

اگر چه مضمون این دو عبارت یکی است ولی هرگز در کلام یک متخصص شبکه سوییچ لایه ۳ و مسیریاب Routerیکسان تلقی نمی شود و با هم فرق اساسی دارند .مسیریاب چیز دیگری است و سوییچ لایه ۳ چیزی دیگر، هرچند هر دو یک کار مشابه انجام می دهند.!! حال به تفاوتها می پردازیم:

- مسیریاب بر خلاف سوییچ لایه ۳ تعداد کانال ورودی/خروجی محدودی دارد ولی در عوض قادر است از انواع و اقسام پروتکل های مسیریابی ساده و پیچیده حمایت کرده و خود را با انواع متنوع خطوط WAN مثل ISDN , Frame Relay,ATM, SONET, یا X.25تطبیق داده و از پروتکل های متعدد نقطه به نقطه پشتیبانی کند. لذا مسیریاب یک ابزار کاملا پیچیده و در عین حال بسیار منعطف و قابل پیکربندی در شرایط مختلف است. در ضمن یک مسیریاب میتواند با پروتکل های مختلف لایه ۳ مثل IP,IPX و یا نظایر آن کارکند.

- سوییچ لایه ۳ عموما یک سوییچ با تعداد زیادی پورت همنوع (عموما پورت اترنت) است که ضمن آنکه می تواند داده ها را در لایه ۲ و بر اساس آدرس MAC بین پورتها هدایت کند می تواند همین کار را نیز براساس آدرس های جهانی درج شده در سرآیند بسته ها در لایه ۳ انجام بدهد. ولی در عوض از خطوط متنوع WANحمایت چندانی نمی کنند و انعطاف زیادی در پیکربندی آن در محیطهای مختلف با توپولوژی پیچیده و پروتکل های قدرتمند ندارد.
- سوییچ لایه ۳ عموما فقط یک سوییچ اترنت است که از فرآیند مسیریابی برای ایجاد ارتباط بین VLANها و تفکیک حوزه پخش فراگیر (Broadcast Domain) و افزایش سطح کنترل و نظارت بر دسترسی و فیلترینگ بسته ، استفاده می کند و فضا و توپولوژی شبکه ای که در آن مسیریابی صورت می گیرد چندان گسترده و غیرهمگن نیست.
- یک سوییچ لایه ۳ در مقایسه با تعداد پورت و سرعتی که دارد بسیار ارزانتر از یک مسیریاب تمام می شود. به عنوان مثال یک سوییچ catalyst 3550-24 دارای ۲۴ پورت اترنت ۱۰۰ Mbps است و می تواند در هر ثانیه ۶.۶ میلیون بسته را بین پورتها هدایت نماید و ضمن حمایت از , VLAN بین آن ها مسیریابی انجام دهد .چنین سوییچی را امروزه می توان با قیمتی حدود دو میلیون تومان خرید (قیمت جهت مقایسه است و مربوط به تاریخ خاصی نمی باشد) درحالیکه یک مسیریاب نمونه مثل cisco 7300 با ظرفیت هدایت ۳.۵ میلیون بسته در ثانیه که تنها دو پورت اترنت گیگابیت دارد به قیمتی حدود ۱۰ میلیون تمام می شود. یعنی با ظرفیتی حدود نصف ظرفیت هدایت یک سوییچ ۳۵۵۰ قیمتی حدود پنج برابر آن دارد ولی درعوض می تواند از خطوط WANو پروتکل های بسیار متنوع و پیچیده حمایت کند.
- نظر به آنکه عملیات مسیریابی در یک سوییچ در سطح بسیار ساده و عموما برای مسیریابی بین VLANها انجام میگیرد لذا می توان در یک سوییچ لایه ۳ با استفاده از مدارات مجتمع (ASIC (Application Specific Integrated Circuitsکه صرفا برای عمل مسیریابی در سطح سخت افزار طراحی و ساخته می شود سرعت هدایت بسته ها را تا حد بسیار بالایی افزایش داد. در حالی که در یک مسیریاب با پروتکل های پیشرفته و بسیار وسیعی که پشتیبانی میکند نمی توان به سادگی و با طراحی مدارات مجتمع ساده و ارزان به یک سوییچ لایه ۳ با سرعت هدایت بالا دست یافت. سطح عملیات قابل انجام توسط یک مسیریاب و انواع واسط های شبکه درآن به قدری وسیعند که یک سخت افزار واحد ASICو پیش برنامه ریزی شده (Preprogrammed)نمی تواند این عملیات را به تنهایی انجام بدهد. پس یک مسیریاب باید بخش بزرگی از عملیات سطح نرم افزار و به کمک پردازنده های همه منظوره انجام گیرد که سرعت کمتری نسبت به پردازنده های خاص منظوره ASIC دارند. برای بالا بردن سرعت هدایت یک مسیریاب باید از پردازش موازی در محیطی چند پردازنده بهره گرفته شود که همین موضوع قیمت مسیریاب را بشدت افزایش خواهد داد.
- یک مسیریاب را می توان در طراحی ستون فقرات شبکه های WAN بکارگرفت ولی سوییچ لایه ۳ عموما زیرساخت شبکه های محلی پردیس( Campus LAN) به کار می آید.

- به دلیل تنوع و تفرق زیاد در خطوط ارتباطی یک مسیریاب ، عموما نمی توان یک مسیریاب را برای سوییچینگ لایه ۲ پیکربندی کرد.

مسیر یابی فرآیندی مبتنی بر یکسری قواعد منطقی و سیاست هاست که پیچیدگی آن به سطوح و لایه ی امنیت،امکان پشتیبانی همزمان از دو یا سه پروتکل و پیچیدگی ساختار و توپولوژی شبکه دارد.انتقال داده ها از یک شبکه به شبکه دیگر وقتی که تنها یک مسیر واحد بین آن دو شبکه وجود دارد،ساده ترین فرآیند مسیر یابی است اما زمانی که بین دو شبکه چندین مسیر وجود دارد ،مکانیزم پیدا کردن بهترین مسیر و همچین اعمال معیار های بهینگی مسیر،به الگوریتم های پویا نیاز دارد.

## 3-1پروتکل هاي INTERIOR وEXTERIOR :

پروتکل هایی که در داخل یک سازمان فعالیت می کنند به نام پروتکل های Interior نامیده شده که شامل IS-IS،IGRP،EIGRP،OSPF،RIP می شوند.شبکه های خود مختار (AS) شبکه هایی هستند که تحت نظارت و سرپرستی یک مجموعه یا سازمان خاص پیاده و اداره میشود.مسیریابی بسته های IP درون یک شبک ۀ خود مختار بیشتر تابع پارامترهایی نظیر سرعت و قابل اعتماد بودن الگوریتم مسیریابی است.مسیریابی بسته های اطلاعاتی بر روی شاهراه هایی که شبکه های AS را بهم متصل کرده ، مسائلی کاملاً متفاوت با مسیریابی در درون یک شبک ۀ خودمختار دارد. در مسیریابی بین شبکه های AS مسائلی نظیر امنیت، پرداخت حقّ اشتراک و سیاست نیز میتواند در انتخاب بهترین مسیر دخیل باشد.هر کدام از AS ها را با یک شماره می شناسند این شماره asn نامیده می شود،که این شماره می تواند در دو نوع private وpublic باشد.شماره AS های متصل به اینترنت باید در تمامی محیط اینترنت منحصر به فرد بوده و بنابراین سازمان IANA اقدام به تخصیص شماره های فوق می نماید.

تعریف : Asn در محدوده ی 1 تا 65535 تعریف شده است بخشی از این محدوده یعنی از 64512 تا 65535 نیز برای استفاده ی اختصاصی کنار گذاشته شده است و قابل ثبت نیست .

پروتکل هایی که اطلاعات Routing مربوط به سازمان ها را در بین آنها منتقل می نماید،به نام پروتکل های Exterior خوانده شده و تنها نمونه موجود آن،پروتکل BGP 4 می باشد.

## 4-1شبکه هايي كه با مسيرياب BGP در ارتباطند:

شبکه های پایانی-Stub -: این نوع از شبکه ها فقط با یک مسیریاب نوع BGP در ارتباطند و بنابراین نمیتوانند در ستون فقرات اینترنت نقش ایفا کنند و کمکی به توزیع ترافیک بر روی شبک ۀ اینترنت نمی کنند .معمولاً برای وصل شبکه های پایانی به یکی از مسیریابهای BGP باید هزین ۀ قابل توجهی در هر ماه پرداخت شود .اکثر شبکه های متصل به اینترنت در ایران به خاطر عدم وجود ستون فقرات ارتباطی سریع بین شهرها و استانهای مختلف کشور ، از نوع شبکه های پایانی -Stub- بشمار میروند.

شبکه های چندارتباطی: این گونه از شبکه ها بین مسیریابهای نوع BGP واقعند و میتوانند برای توزیع و حمل ترافیک در شبکهٔ اینترنت مورد استفاده قرار بگیرند مگر آنکه بدلایل امنیتی ، تمایل به چنین کاری نداشته باشند.

شبکه های ترانزیت: این گونه شبکه ها که به نحوی به روی ستون فقرات شبکه اینترنت واقعند وظیفه عمده ای در حمل و توزیع بسته های IP بعهده دارند.(همانند شبکهٔ NSFNet در آمریکا)

## 1-5دو دیدگاه الگوریتم هاي مسیریابي:

الف) از دیدگاه روش تصمیم گیری و میزان هوشمندی الگوریتم

ب) از دیدگاه چگونگی جمع آوری و پردازش اطلاعاتِ زیرساخت ارتباطی شبکه

با دیدگاه اول الگوریتم های مسیریابی را میتوان به دو دستهٔ " ایستا "و" پویا " تقسیم بندی کرد .در الگوریتم های ایستا هیچ اعتنایی به شرایط توپولوژیکی و ترافیک لحظه ای شبکه نمی شود. معمولاً در این الگوریتم ها برای هدایت یک بسته ، هر مسیریاب از جداولی استفاده می کند که در هنگام برپایی شبکه تنظیم شده و در طول زمان ثابت است. در هنگام وقوع هرگونه تغییر در توپولوژی زیرساختِ شبکه ، این جداول باید توسط مسئول شبکه بصورت دستی مجدداً تنظیم شود .اگرچه این الگوریتم ها بسیار سریعند ولی چون ترافیک لحظه ای شبکه متغیر است ، نمی توانند بهترین مسیرها را انتخاب نمایند و هرگونه تغییر در توپولوژی زیرساخت ارتباطی شبکه ، یک مشکل عمده و جدی ایجاد خواهد کرد.

.در الگوریتم های پویا مسیریابی بر اساس آخرین وضعیت توپولوژیکی و ترافیک شبکه انجام می شود .جداول مسیریابی در این نوع الگوریتم ها هر T ثانیه یکبار به هنگام میشود.

این الگوریتمها بر اساس وضعیت فعلی شبکه تصمیم گیری مینمایند ولی ممکن است پیچیدگی این الگوریتمها به قدری زیاد باشد که زمان تصمیم گیری برای انتخاب بهترین مسیر ، طولانی شده و منجر به تاخیرهای بحرانی شده و نهایتاً به ازدحام بیانجامد؛ بهمین دلیل در مسیریابهای سریع از تکنیکهای چند پردازندهای و پردازش موازی استفاده میشود.

از دیدگاه دوم الگوریتمهای مسیریابی به دو دستهٔ " سراسری / متمرکز" و" غیرمتمرکز" تقسیم میشود.در" الگوریتمهای سراسری "هر مسیریاب باید اطلاعات کاملی از زیرساخت ارتباطی شبکه داشته باشد . یعنی هر مسیریاب باید تمامی مسیریابهای دیگر ، ارتباطات بین آنها و هزینهٔ هر خط را دقیقاً شناسایی نماید . سپس با جمع آوری این اطلاعات" ساختمان دادهٔ "مربوط به گراف زیرساخت شبکه را تشکیل بدهد .در چنین شرایطی برای یافتن بهترین مسیر بین هر دو مسیریاب ، از الگوریتمهای کوتاهترین مسیر نظیر" الگوریتم دایجکسترا"استفاده میشود .به چنین الگوریتمهایی که برای مسیریابی به اطلاعات کاملی از زیرساخت شبکه و هزینهٔ ارتباط بین هر دو مسیریاب نیازمندند ، اختصاراً الگوریتمهای LS گفته میشود و در مسیریابهای مدرن و جدید از آن استفاده میشود.

در الگوریتمهای" غیر متمرکز "، مسیریاب اطلاعات کاملی از زیرساخت شبکه ندارد بلکه فقط قادر است هـزین ۀ ارتباط با مسیریابهایی که بطور مستقیم و فیزیکی با آنها در ارتباط است محاسبه و ارزیابی نماید .سپس در فواصل زمانی منظم ، هر مسیریاب جدول مسیریابی خود را برای مسیریابهای مجاور ، ارسال مینماید .مسیریاب با دریافت این جداول و مقادیری که خودش مستقیماً اندازه گیری کرده ، با یک الگوریتم بسیار سـاده جـدول خـودش را بـه هنگام مینماید و برای هدایت هر بسته ، از آن استفاده میکند .در این الگوریتمها برای مسیریابی هر بسـته ، فقـط یک جستجو در جدول مسیریابی کافی است و در نتیجه پیچیدگی زمانی بسیار مناسبی دارد چراکه درگیر اجرای الگوریتمهای وقت گیری شبیه" دایجکِسترا "نخواهند شد .به این نوع الگوریتمها به اختصـار" الگوریتمهـای DV" گفته میشود.

ساختار مسیریاب‌های دینامیـک بـه دلیـل آن کـه از فاکتورهـای زیـادی نظیـر انـدازه Port Queue و مقـدار در دسترس بودن آن در عملیات مسیریابی استفاده می‌کنند، پیچیده می‌باشد.

## 6-1انواع پروتکل:

در لایــه network دو نــوع پروتکــل یکــی Routed Protocol و دیگــری Routing Protocol وجــود دارد.پروتکل های Routed در واقع یک پروتکل لایه سومی می باشد که اطلاعـات را از یـک نقطـه بـه نقطـه ای دیگر انتقال می دهد.بسته های مربوط به پروتکل های Routed شامل خود دیتا به همراه اطلاعات پروتکل هـای لایه سوم می باشد.اما پروتکل های Routing باعث انتقال اطلاعات بین روترهای همسایه می شود.در نتیجه ایـن عمل،تمامی روترها درباره تمامی شبکه های موجود اطلاعت لازم را دریافت کرده و بنـابراین بهتـرین مسـیرهای ممکن برای دسترسی به مقصد را تعیین می کنند.

### 1-6-1انواع پروتکل Routed:

IP-4،DECnet-3،IPX-2، APPLETALK-1

همه پروتکل‌ها از مسیریابی پشتیبانی نمی‌کنند. پروتکل‌هایی که قابلیـت مسـیریابی دارنـد عبارتنـد از IP، IPX، سیستم شبکه زیراکس XNS و Apple Talk. نمونه‌های از پروتکل‌هایی کـه از مسـیریابی پشـتیبانی نمـی‌کننـد عبارتند از Local Area Transport (LAT) و NetBEUI.

### 2-6-1انواع پروتکل Routing :

با اینکه هدف تمامی پروتکل ها انتخاب بهترین مسیر منتهی به مقصـدی خـاص مـی باشـد،اما مکانیسـم عمل آن ها تفاوت های زیادی نسبت به همدیگر دارد.هر یک از پروتکل های Routing در واقع یک نرم افـزار در روی روترها بوده که هدف آنها،تبادل اطلاعات بین روترهای موجود در شبکه می باشد.روترها بـا اسـتفاده از ایـن رطلاعات اقدام به انتخاب مسیرهای منتهی به مقاصد مورد نظر مینمایند.

پروتکل های روتینگ را می توان از لحاظ پارامترهای مختلف در گروه های جداگانه قرار داد.یکی از تفاوت ها در ماسک مربوط به آدرس ها در داخل پیام های ارسالی می باشد.بدین صورت که برخی از آن ها ماسک مربوطه را نیز در داخل پیام ارسالی گنجانده ولی برخی دیگر این کار را نمی کنند.به ترتیب پروتکل های دسته اول را classless وپروتکل های دسته دوم را Classful گویند.

## :CLASSFUL ROUTING7-1

مشخصات کلی مربوط به این گروه آدرس های IP:

1)عمل Summarization در مرز بین شبکه ها بصورت خود به خود انجام می گیرد.

2)عملیات Summarization در مورد route هایی که بین شبکه های ناشناخته منتقل می شوند انجام شده و به صورت آدرس های با کلاس استاندارد در خواهند آمد.

3)پیام هایی که بین Subnetهای یک شبکه کلاس استاندارد منتقل می شوند،دارای ماسک مربوط به آدرس ها نیستند.

4)پروتکل های Classful فرض را بر این می گیرند که Interfaceهای مربوط به تمامی روترها به شبکه هایی با ماسک یکسان متصل گشته اند ودلیل نگنجاندن ماسک مربوطه در داخل پیام های ارسالی نیز همین مسئله است.

5)شامل پروتکل های RIPv1 و IGRP می باشد.

طرز هدایت پیام ها توسط پروتکل های Classful ،وابسته به قانون های مربوط به آنهاست.بدین صورت که اگر مورد متناظری در داخل جدول routing وجود داشته باشد،پیام دریافت شده به طرف همان مقصد هدایت خواهد شد.اگر هیچ مورد متناظری در داخل جدول وجود نداشته باشد،پیام از بین خواهد رفت.حتی اگر از یک Default Route نیز استفاده شود،تنها در صورتی استفاده از آن مجاز خواهد بود که هیچ نوع مورد متناظری در داخل جدول وجود نداشته باشد.بدین معنی حتی در صورت وجود شبکه اصلی در داخل جدول route پیام ها از بین رفته و به سمت Default Route نیز ارسال نخواهند شد.

محدودیت های مربوط به این دسته پروتکل ها:

1-پروتکل های Classful باعث از دست رفتن آدرس های بیشتری می شوند.

2-استفاده از ویژگی VLSM در داخل شبکه مجاز نیست.

3-بدون استفاده از VLSM اندازه جدول روتینگ بیش از حد نرمال افزایش یافته و بنابراین پیام های Update انتقالی بین روتر ها نیز دارای سایزی بزرگتر خواهند بود.

## :CLASSLESS ROUTING8-1

پروتکل های فوق برای حل محدودیت های موجود در پروتکل های Classful مورد استفاده قرار می گیرند.

مشخصات کلی این دسته از آدرس های Ip:

1)Interfaceهای متصل به یک شبکه لایه سوم می توانند از ماسک های متفاوتی استفاده نمایند.

2)شامل پروتکل های BGP،RIPV2،IS-IS،EIGRP،OSPF می شوند.

3)استفاده از ویژگی CIDR در داخل شبکه مجاز می باشد.

4)استفاده از هر نوع Summarization دستی و اتوماتیک در مورد Routeهای موجود در جدول Routing مجاز می باشد.

برای اینکه پروتکل های Classful نیز از برخی مزایای موجود در پروتکل های Classless برخوردار گردند،دستور IP CLASSLESS را می توان اجرا نمود.البته بصورت Default،دستور مزبور در نسخه های اخیر IOS فعال گشته است.

## 9-1پروتکل هاي IP Distance Vector :

پروتکل های Distance Vector که در اوایل مورد استفاده قرار می گرفتند مناسب شبکه های کوچک بوده و از نوع Classful بودند.این پروتکل ها شامل RIPv1 وIGRP می گردند که در طول زمان و با اصلاحات انجام شده،پروتکل های RIPv2 وEIGRP معرفی گشته اند.با اینکه مکانیسم عمل پروتکل های جدید بر پایه نسخه های قدیمی تر بنا شده است،اما نسخه های جدید از نوع Classless می باشند.البته با وجود اینکه پروتکل های IGRP وEIGRP توسط سیسکو به عنوان پروتکل های Distance Vector معرفی گشته اند،اما برای مثال پروتکل EIGRP از برخی از خصوصیات مربوط به هر دو دسته از پروتکل ها برخوردار است .از این رو می توان آنها را از نوع Hybrid دانست.

## 10-1عملکرد پروتکل هاي Distance Vector :

این دسته از پروتکل ها محتویات مربوط به جدول Routing را به صورت متناوب و در قالب پیام های broadcast برای روتر های همسایه که به صورت مستقیم با روتر در تماس می باشند ارسال می کنند.

فاصله زمانی بین ارسال پیام های مزبور بستگی به نوع پروتکل مورد استفاده دارد.هر کدام از این پروتکل ها دارای یک تایمر می باشند که بعد از سپری شدن در زمان تعیین شده،اقدام به ارسال پیام های Update که شامل تمامی محتویات جدول Routing می باشد خواهند نمود.این تایمر بلافاصله بعد از ارسال پیام دوباره از صفر شروع خواهد شد.هر کدام از روترها بعد از دریافت پیام Update روتر همسایه،اقدام به اصلاح جدول Route خود کرده و تغییرات را از طریق پیام های Update دیگر برای بقیه روترها نیز ارسال می نمایند.بنا به اینکه روترها در این شرایط فقط با تکیه بر اطلاعات دریافت شده از طریق روترهای همسایه خود اقدام به ایجاد جدول Riuting خود می کنند،به چنین عملکردی در اصطلاح،Routing By Rumer گفته می شود.

پروتکل های DV از نوع Classful می باشند.هدف اجرای پروتکل های DV ،ایجاد یک شبکه بدون چرخه یا loopهای لایه سوم می باشد.تکنیک هایی که پروتکل های DV برای جلوگیری از بروز چرخه های لایه سوم به کار می گیرند عبارتند از:

1)Split Horizon

2)Poison Revers

3)Holddown

4)Triggerd Updates

5)تخصیص یک زمان عمر برای هر کدام از Routeهای موجود در جدول

پروتکل های فوق از hop count به عنوان metric استفاده می کنند که عبارتست از تعداد روترهای موجود در بین راه منتهی به مقصد.سیسکو پروتکل های IGRP وEIGRP را به عنوان پروتکل های DV طبقه بندی می کند.اما پروتکل های فوق از hop count به عنوان metric استفاده نکرده و به جای آن از مجموعه ای از پارامترهای مختلف بهره می گیرند.پروتکل های DV برای یافتن بهترین مسیر منتهی به مقصد از الگوریتمی به نام Bellman Ford استفاده کرده که بر اساس hop countهای مربوط به انواع Routeها می باشد.اما پروتکل EIGRP از الگوریتمی دیگر به نام DUAL برای یافتن بهترین مسیر منتهی به مقصد استفاده می نمایید.

## 11-1پروتکل هاي IP Link State:

پروتکل های Link State نوع دیگری از پروتکل ها بوده که برای انجام عملیات Routing دارای امکانات پیشرفته تری می باشند.پروتکل های مزبور به جای ارسال تمامی محتویات جداول Routing در قالب پیام های broadcast،اقدام به فرستادن پیام های افزایشی یا Incremental به صورت پیام های multicast خواهند کرد.البته برخی از پروتکل ها در کنار پیام های Incremental همچنان اقدام به ارسال پیام های Update متناوب نیز مینمایند.البته این کار در هر 30 دقیقه یکبار انجام گرفته و از پیام های multicast بهره خواهند گرفت.

## 12-1آگاهي از وضعيت شبکه:

پروتکل های Link State در همان ابتدای کار اقدام به ارسال پیام های hello برای دیگر روترهای موجود کرده و در نتیجه روترهای همسایه خود و نیز شبکه های متصل به آنها را شناسایی می نمایند.این عملیات به صورت مطمئن انجام می گیرد.بدین صورت که روترها دریافت کردن یا نکردن پیام ها را به اطلاع روتر ارسال کننده می رسانند.به این ویژگی در اصطلاح،connection-oriented گفته می شود.تا زمانی که روترها پیام های hello مربوط یه روترهای همسایه دیگر را دریافت می نمایند،ارتباط مجاورت یاadjacecy بین روترها به صورت

فعال باقی خواهد ماند.از این روست که هر گونه تغییری در وضعیت اتصالات شبکه سریعاً به اطلاع تمامی روترها خواهد رسید.اما به محض معیوب بودن یک روتر،پیام های hello آن برای روترهای همسایه ارسال نشده و بنابراین،روتر مزبور به نام روتر از رده خارج و یا dead در نظر گرفته میشود.برای موفقیت آمیز بودن این عمل،دو روتر باید دارای زمان های یکسان hello timer و ماسک های برابر باشند.

بلافاصله بعد از بروز هر گونه تغییر در شبکه ،روترها بجای این که منتظر فرا رسیدن زمان ارسال پیام های Update بمانند،اقدام به ارسال تغییرات انجام گرفته برای روترهای دیگر می نمایند که به نام Tiggered Update نامیده می شوند.این ویژگی باعث کاهش پهنای باند مصرفی شبکه شده و نیز زمان همگرایی شبکه را نیز کاهش می دهد.بدلیل اینکه پروتکل های Link State باعث مصرف کمتر منابع شبکه می گردند،دلایلی که می توان برای این کار مطرح کرد عبارتند از:

1)استفاده از پیام های multicast

2)استفاده از پیام های Triggered Update

3)ارسال پیام های Summary

4)ارسال پیام های hello برای برقرار نگهداشتن رابط مجاورت بین روترها به جای ارسال تمامی محتویات جدول Routing

یک پروتکل Link State اطلاعات مربوط به وضعیت شبکه،شامل تمامی روترها وشبکه های متصل به آنها را در خود ذخیره نمایند.این اطلاعات توسط الگوریتم مشخصی به نام Dijkstra باعث ایجاد جدول Routing می گردند.زمانی که روترها پیام های Update ارسالی را دریافت نماید،جدول توپولوژی خود را اصلاح کرده و مسیرهای احتمالی جدید برای دستیابی به مقاصد مختلف را شناسایی می نماید.انتخاب بهترین مسیر منتهی به مقصد،از طریق metric پیام ها انجام می پذیرد.

جدول زیر انواع پروتکل ها بر اساس دیدگاه های مختلف نشان می دهد:

جدول 1-1

| | | | |
|---|---|---|---|
| ROUTED | Appletalk-Ipx-Decnet Iv-Ip | | |
| ROUTING | IN AS | DV | IGP-RIP-IGRP |
| | | LS | IS_IS-OSPF |
| | BETWEEN AS | BGP | |

## 13-1نحوه ي مسيريابي بصورت استاتيک:

مسیریابی غیرمستقیم وقتی اتفاق می‌افتد که میزبانهای مبدا و مقصد روی یک قسمت از شبکه نیستند و بسته‌ها باید از طریق مسیریابی منتقل شوند. یک مسیریاب در ساده‌ترین حالتش یک پیوند فیزیکی بین دو شبکه ایجاد می‌کند. مسیریابها ابزارهای بی اعتنایی Passive هستند که توجهی به ترافیک عمومی شبکه ندارند.

بسته‌هایی که برای شبکه‌ی دیگر مقدر شده‌اند می‌بایست به منظور انتقال به یک مسیریاب ارسال شوند. عملاً شما می‌توانید یک مسیریاب را کامپیوتری با دو یا چند کارت شبکه روی آن بدانید. هر یک از این کارتها به یک قسمت جدا از شبکه صول شده‌اند و بدین ترتیب یک کامپیوتر می‌تواند پیامها را از یک قسمت به قسمت دیگر بفرستد. کامپیوترهایی که به عنوان مسیریاب پیکربندی شده‌اند، دروازه Gateway نیز نامیده می‌شوند.

یک مسیریاب ابزار فیزیکی است که برای اتصال دو یا چند شبکه استفاده می‌شود وقتی یک مسیریاب یک بسته را از میزبان فرستنده می‌گیرد، آن دو یا چند کار را انجام می‌دهد. اگر مسیریاب مستقیماً به شبکه مقصد وصل باشد آن می‌تواند بسته را مستقیماص به میزبان مقصد تحویل دهد. اگر مسیریاب مستقیماً به شبکه مقصد وصل نباشد باید آنها را به مسیریاب مستقیماً به شبکه مقصد وصل نباشد باید آنها را به مسیریاب دیگری برای گرفتن تصمیم مشابهی ارسال کند.

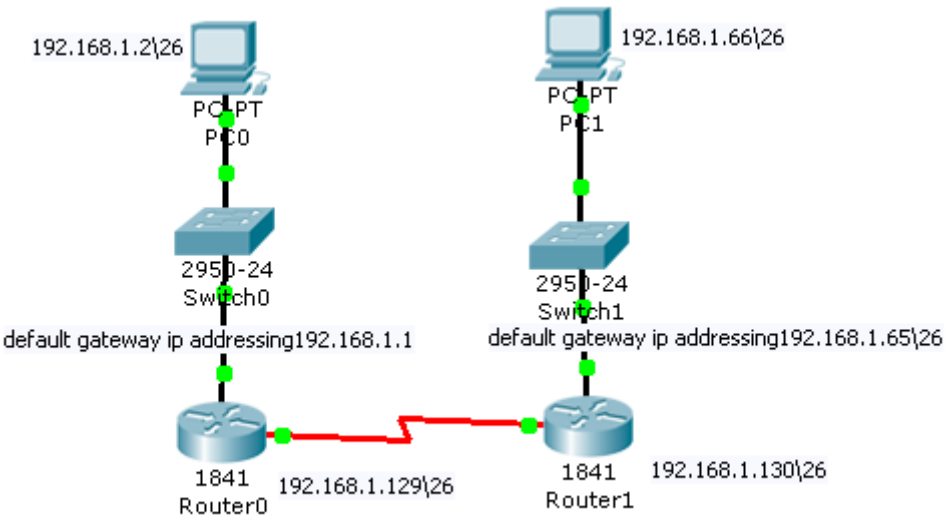
روی یک مسیریاب ایستا، جداول مسیریابی باید بصورت دستی وارد شوند. اگر شما یک مدیر شبکه باشید، این بدان معنی است که شما از این که بدانید که چه کسی این کار را انجام می‌دهد خوشحال خواهید شد. یک مسیریاب ایستا فقط شبکه‌هایی که مستقیماً به آن وصل شده است یا شبکه‌هایی که شما اطلاعاتی درباره آنها به آن مسیریاب داده‌اید را می‌شناسد. جداول مسیریابی ایستا باید بطور دستی پیکربندی شوند و باید شامل همه‌ی شبکه‌های شناخته شده روی internetwork به منظور کارایی بهتر باشند.

یک مسیر یاب قبل از انجام هر گونه مسیر یابی، باید برنامه ریزی و پیکربندی (CONFIG) شود.هر رابطی (Interface) که بر روی مسیر یاب استفاده می شود باید با یک آدرس IP و ماسک شبکه پیکر بندی شود.آدرس IP باید از آدرس های متعلق به شبکه ای باشد که با مسیر یاب در ارتباط است.با یک مثال نحوه ی انجام این کار را نشان می دهیم.

ما یک آدرس IP از کلاس C داریم و می خواهیم دو شبکه راه اندازی کنیم و بین این دو تا شبکه ارتباط برقرار کنیم تا بتوانند از هم PING بگیرند.ابتدا ما عملیات subneting را روی این آدرس ip انجام می دهیم ما برای راه اندازی این کار نیاز به 3 شبکه متفاوت داریم یعنی بین دو تا روتر نیز ما به یک شبکه نیاز داریم.

IP ADDRESS:192.168.1.0
SUBNET MUSK:255.255.255.192
RANGE ADDRESS IP SUBNET ONE:192.168.1.0\26 192.168.1.63\26
RANGE ADDRESS IP SUBNET TWO: 192.168.1.64\26 192.168.1.127\26
RANGE ADDRESS IP SUBNET THREE:192.168.1.128\26 192.168.1.191\26

همانند شکل زیر:




شکل 1-1

تذکر:تمامی مثال های حل شده توسط نرم افزار packet tracer که مختص تجهیزات شرکت سیسکو می باشد انجام می شود.

دستورات وارد شده در سیستم عامل IOS روترصفر برای برقراری ارتباط بین این دو شبکه:

Router> زمانی که ابتدا روتر روشن می شود وارد user mode می شویم

Router>Enable با وارد کردن دستور Enable وارد privilege mode می شویم

Router#conf t سپس با وارد کردن configuration terminal وارد global mode می شویم

Router(config)#interface fastEhternet0 حال به interfaceهای روتر آدرس ip می دهیم

Router(config-if)#ip address 192.168.1.1 255.255.255.192
Router(config-if)#no shut down

LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up.

LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up.

Router(config-if)#exit

حال به همین ترتیب وارد تمامی اینترفیس های روتر صفر و روتر یک شده و به همه آنها آدرس ip می دهیم و آنها را با دستور no shut down فعال می کنیم.

حال با وارد شدن به global mode روتر صفر دستورات زیر را جهت مسیر یابی به صورت استاتیک وارد می کنیم.

Router(config)#ip route 192.168.1.64 255.255.255.192 192.168.1.130
Router(config)#interface Serial0/0/0
Router(config-if)#clock rate 9600

بهمین ترتیب روتر یک را پیکربندی می کنیم:

Router(config)#ip route 192.168.1.0 255.255.255.192 192.168.1.129

```
Router(config)#interface Serial0/0/0
Router(config-if)#clock rate 9600
```

در شبکه های بزرگتر مسیرهای ثابت تنها زمانی مفید هستند که شما فرض کنید هیچ چیز تغییر نخواهد کرد.هیچ شبکه یا مسیر یابی خراب نخواهد شد.رابط های شبکه هرگز خراب نمی شوند و هیچ شبکه جدیدی نیز اضافه نخواهد شد.اگر همه این فرضیات درست باشند،می توان کار را با مسیرهای ثابت ادامه داد.اما اگر به یاد بیاورید که هیچ چیز به این شکل نخواهد ماند،در این صورت استفاده از مسیرهای ثابت به تنهایی تصمیم چندان درستی به نظر نمی رسد.شما نیاز به یک پروتکل مسیریابی پویا دارید که بطور خودکار جابجایی مسیرهای بین مسیریاب ها را انجام دهد و نیازی به انجام این کار بصورت دستی با مسیرهای ثابت نباشد.

نکته: نکته‌ی مهمی که باید درباره‌ی مسیریابهای پویا و ایستا بدانید این است که مسیریابهای ایستا نیاز به نگهداری بیشتری دارند اما ترافیک نامربوط در شبکه کمتر تولید می‌شود. مسیریابهای پویا نگهداری کمتری نیاز دارند اما ترافیک شبکه را به مقدار زیادی افزایش می‌دهند.

# فصل دوم
# پروتکل OSPF

## 2-1پروتکل OSPF:

بکارگیری پروتکل RIP در شبکه های کامپیوتری بیشتر به دلیل شرایط زمان بـوده اسـت .در ده هفتـاد و هشتاد حافظه و پردازندههای سریع ، گران قیمت بودند و پیاده سازی الگوریتمهای مسیریابی مبتنی بر روشـهایی نظیر LS که هم به حافظه و هم به پردازندهٔ سریع نیاز دارند ، مقرون به صرفه نبود .از طرفی شبکه ها نیز آنقـدر توسعه نیافته بودند که نیاز به الگوریتم های بهینه تر احساس شود .با گسترش اینترنـت و توسـعهٔ شـبکه هـای خودمختار در اواخر دههٔ هشتاد ، کاستی های پروتکل RIP نمود بیشتری پیدا کرد و با سریع شدن پردازنده ها و ارزان شدن سخت افزار ، نیاز به طراحی یک پروتکل بهینه ،IETF را واداشت تا در سال1990 ،OSPF را به عنوان یک پروتکل استاندارد ارائه نماید .مسیریابهای زیادی مبتنی بر این پروتکل به بازار عرضه شده انـد و احتمـال مـی رود که در آینده تبدیل به مهمترین پروتکل مسیریابی درونی در شبکه های AS شود.

## 2-2مقایسه پروتکلOSPF با پروتکل RIP:

- بر خلاف پروتکل RIP، این پروتکل از الگوریتمLS برای محاسـبهٔ بهتـرین مسـیر اسـتفاده میشـود و بنابراین مشکل" شمارش تا بینهایت "وجود ندارد.
- بر خلاف پروتکل RIP، در این پروتکل معیار هزینه فقط" تعداد گام "نیست بلکه میتواند چندین معیـار هزینه را در انتخاب بهترین مسیر در نظر بگیرد.

- بر خلاف پروتکل RIP، در این پروتکل حجم بار و ترافیک یک مسیریاب در محاسبهٔ بهترین مسیر دخالت داده میشود و در ضمن در هنگام خرابی یک مسیریاب ، جداول مسیریابی سریعاً همگرا میشود.
- بر خلاف پروتکل RIP، در این پروتکل ، فیلد Type of Service در بستهٔ IP میتواند در نظر گرفته شود و بر اساس نوع سرویس درخواستی ، برای یک بسته مسیر مناسب انتخاب گردد.
- بر خلاف پروتکل RIP، در پروتکل OSPF تمام بسته های ارسالی برای یک مقصد خاص ، روی بهترین مسیر هدایت نمی شود بلکه درصدی از بسته ها روی مسیرهایی که از لحاظ حداقل هزینه در رتبهٔ 2 ، 3و ... قرار دارند ارسال میشود تا پدیدهٔ "نوسان "که قبلاً به آن اشاره شد رخ ندهد .به این کار" موازنهٔ بار"گفته میشود.
- بر خلاف پروتکل RIP، در این پروتکل از مسیریابی سلسله مراتبی پشتیبانی میشود.
- بر خلاف پروتکل RIP، در این پروتکل مسیریابها جداول مسیریابی را از دیگر مسیریابها قبول نمیکنند مگر آنکه هویت ارسال کنندهٔ آن احراز شود .به همین دلیل مسئول شبکه برای هر مسیریاب یک" کلمهٔ عبور " تعیین میکند تا کاربران اخلالگر نتوانند با برنامه نویسی ، جداول مسیریابی مصنوعی تولید کرده و با ارسال آنها ، مسیریابی در شبکه را با مشکل مواجه کنند.

## 2-3سلسله مراتب تعیین شده برای نواحی در پروتکل OSPF:

- یک شبکهٔ خودمختار (AS) به تعدادی" ناحیه"تقسیم می شود .تمام مسیریابهای درون یک ناحیه باید مسیریابهای هم ناحیهٔ خود و هزینهٔ ارتباط بین آنها را بدانند و در جدولی ذخیره کنند .در لحظات به هنگام سازی ، این جداول برای تمام مسیریابهای هم ناحیه ارسال خواهد شد .مسیریاب هیچ اطلاعی از وضعیت مسیریابهای درون نواحی دیگر ندارد.
- درون هر ناحیه یک یا چند مسیریاب وجود دارند که ارتباط بین نواحی را برقرار میکنند؛ به آنها ، "مسیریابهای مرزی"گفته میشود .مجموعهٔ مسیریابهای مرزی و مسیریابهایی که در خارج از هر ناحیه نقش توزیع ترافیک بین نواحی را بر عهده دارند (بهمراه ساختار ارتباطی بین این مسیریابها)"ستون فقرات "شبکهٔ AS را تشکیل می دهد.
- درون ستون فقراتِ شبکهٔ AS ممکن است مسیریابهایی وجود داشته باشند که با دیگر شبکه های AS در ارتباط باشد .به این مسیریابها" دروازه های مرزی"یا BGP گفته میشود .

در پروتکل OSPF جداول زیر توسط مسیریابها" اعلان "میشود:

- جدول مسیریابی محلی درون یک ناحیه : این جداول ، محتوی اطلاعاتی در مورد گراف هزینهٔ ناحیه ای است که یک مسیریاب به آن متعلق است و توسط هر مسیریاب درون آن ناحیه، به تمام مسیریابها اعلان میشود.

- جدول مسیریابی شبکه درون یک ناحیه: این جداول که محتوی اطلاعاتی در مورد مسیریابها و کانالهای بین آنها در یک شبکه است ، توسط مسیریاب های درون یک ناحیه به تمامی مسیریابها اعلان میشود.
- جدول خلاص ۀ مسیریابی مسیریابهای مرزی: این جداول محتوی اطلاعاتی خلاصه ، در مورد مسیرهای موجود در خارج از نواحی است و توسط مسیریاب های مرزی به تمامی مسیریاب های نواحی مختلف اعلان میشود.
- جدول مسیریابی شبکه: این جداول محتوی اطلاعاتی در مورد مسیریاب ها و کانالهای بین آنها در خارج از شبک ۀ AS است و توسط مسیریاب های واقع بر ستون فقرات شبک ۀ AS به تمامی مسیریاب های نواحی مختلف اعلان میشود ولی فقط در مسیریاب های مرزی مورد استفاده قرار می گیرد.

در پروتکل های link-state که به آنها پروتکل های path first shortest نیز گفته می شود ، هر روتر سه جدول جداگانه را ایجاد می نماید . یکی از این جداول وضعیت همسایگانی را که مستقیماً به آن متصل شده اند در خود نگهداری می نماید . در جدول دیگر ، توپولوژی تمامی شبکه نگهداری می گردد و از جدول سوم برای نگهداری اطلاعات روتینگ استفاده می شود .

روترهای link-state نسبت به پروتکل های روتینگ distance-vector دارای اطلاعات بیشتری در ارتباط با شبکه و ارتباطات بین شبکه ای می باشند. پروتکل های link-state اطلاعات بهنگام خود را برای سایر روترهای موجود در شبکه ارسال می نمایند (وضعیت لینک) .

OSPF ( برگرفته شده از Open Shortest Path First ) یک پروتکل روتینگ IP است که دارای تمامی ویژگی های یک پروتکل link-state است .پروتکل فوق ، یک پروتکل روتینگ استاندارد باز است که توسط مجموعه ای از تولیدکنندگان شبکه از جمله شرکت سیسکو ایجاد شده است . در صورتی که در یک شبکه از روترهائی استفاده می گردد که تمامی آنها متعلق به شرکت سیسکو نمی باشند ، نمی توان از پروتکل EIGRP استفاده کرد . در چنین مواردی می توان از گزینه هائی دیگر نظیر RIP ، RIPv2 و یا OSPF استفاده نمود . در صورتی که ابعاد یک شبکه بسیار بزرگ باشد ، تنها گزینه موجود پروتکل OSPF و یا استفاده از route redistribution است ( یک سرویس ترجمه بین پروتکل های روتینگ ) .

OSPF ، با استفاده از الگوریتم Dijkstra کار می کند . در ابتدا ، اولین درخت کوتاهترین مسیر ایجاد می گردد و در ادامه جدول روتینگ از طریق بهترین مسیرها توزیع می گردد . این پروتکل دارای سرعت همگرائی بالائی است ( شاید به اندازه سرعت همگرائی EIGRP نباشد ) و از چندین مسیر با cost یکسان به مقصد مشابه حمایت می نماید . برخلاف EIGRP ، پروتکل OSPF صرفاً از روتینگ IP حمایت می نماید.

## 4-2انواع Area:

1) Stub Area: این ناحیه به اطلاعات External LSA (type 5) نیازی ندارد زیرا به هر حال برای خروج از ناحیه دست به دامان ABR خود میشود. پس مسیر همیشه بدین گونه است و از طریق یک روتر خارج میشود. نکته و هدف از استفاده از این Area، Performance است. از آنجا که LSA 5 را قبول نمیکند پس LSA 4 نیز

در این ناحیه بی معنی است و توسط ABR، Filter می شود. هدف صرفه جوئی در Resource ها و Memory است. که البته Stub area محدودیت های خود را نیز دارد:

- هیچ ASBR ی در ناحیه نمی توان داشت. (و مسلما هیچ Redistribution و External Route)
- Virtual Link در این Area مجاز نیست (نه در ناحیه و نه بصورت Transit)
- می توان چند ABR در این ناحیه داشت اما از آنجا که بهترین مسیر به ASBR را نمیتوان در این ناحیه فهمید، تفاوتی در انتخاب ABR برای رسیدن به ASBR وجود ندارد.
- تمام روتر ها (در Hello Message) بیت E خود را صفر ست میکنند (علامت Stub) و با روتری با E Flag برابر با یک، ارتباطی برقرار نمی کنند.

2) Totally Stubby Area: اگر فیلتر کردن LSA 5 موجب بهبود کارایی روتر میشود، در این نوع از ناحیه حتی LSA 3 نیز Block میشود. این نوع Area توسط Cisco ارائه شده تا تنها با تزریق یک Default Route توسط ABR روتر ها تمام بسته هایی که مقصدشان داخل ناحیه نیست را به ABR بفرستند.

3) Not So Stubby Area: یک ناحیه Stub است که بنا به دلایلی اقدام به Redistribution میکند. (مثلا ارتباط با ISP) LSA 7 در داخل ناحیه منتشر میکند. برای اعلام به نواحی دیگر به ABR میرسد. توسط ABR، اگر P bit آن LSA صفر باشد، Block میشود و اگر P Bit آن یک باشد به صورت مبدل شده به LSA 5 به بیرون از ناحیه اعلام میگردد.

4) Backbone Area: این ناحیه بنام Area 0 مطرح میگردد و تمام نواحی از طریق این ناحیه به هم متصل میگردند. تمام LSA ها در این ناحیه مجازند غیر از نوع 7.

5. Standard Ordinary Area: این Area به Backbone وصل است و Stub نیست.

## 2-5وضعیت هاي اتصال:

OSPF مسیرها را همانند پروتکل های بردار مسافت معرفی نمی کند، بلکه با استفاده از اعلان وضعیت اتصال (Link Advertisements-LSA) مسیرها را معرفی مینماید. یک اتصال (Link) فقط یک رابط (Interface) مانند اترنت (Ethernet)، ویا سریال است. هر اتصال دارای ویژگی هایی شامل ناحیه OSPF که برای اتصال آن تنظیم شده، پهنای باند اتصال و پیشوند (Perfix) و ماسک زیر شبکه ثبت شده برای آن اتصال می باشد.وضعیت اتصال (Link-state) یعنی اینکه اتصال فعال یا غیر فعال است.

## 2-6خصوصیات یک شبکه OSPF :

- نواحی یک یا چندگانه OSPF
- اگر از بیش از یک ناحیه استفاده شود، یک ناحیه پشتیبان (Backbone) یا 0 باید تنظیم شود.
- تمام نواحی غیر 0 باید به ناحیه 0 وصل باشند.

- مسیریاب OSPF برای هر ناحیه ای که بر روی آن تنظیم می شود، یک پایگاه اطلاعـاتی OSPF ایجـاد می کند.
- آگهی های وضعیت اتصال (LSAs)، اطلاعات مربوط بـه رابـط هـای (Interface) یـک مسـیریاب را در سراسر ناحیه OSPF سرریز می سازند.
- پایگاه اطلاعاتی OSPF درون یک ناحیه باید قبل از اینکه یـک مسـیریاب ، مسـیرهای نصـب شـده در جدول مسیریابی IP را جمع بندی و محاسبه کند، هماهنگ شوند.
- الگـوریتم کوتـاهترین مسـیر اول (Shortest Path First-SPF) در تمـام پایگـاه هـای اطلاعـاتی یـک مسیریاب لستفاده شده است و مسیرهای نصب شده در جدول مسیریابی IP را تعیین میکند.
- مسیرها را می توان به نواحی خلاصه کرد، نه درون نواحی.

## ID7-2 مسیریاب OSPF:

بسیاری از عملکردهـا در OSPF وابسـته بـه ID مسـیریاب (Router ID) OSPF هسـتند. ID مسـیریاب OSPF یک عدد 32 بیتی است که یـک مسـیریاب OSPF را مشـخص مـی کنـد.آموختن چگـونگی تعیـین ID مسیریاب بسیار با اهمیت است.

اگر فقط رابط های فیزیکی موجود بر روی یک مسـیریاب تنظـیم شـده باشـند، ID مسـیریاب OSPF بـالاترین آدرس IP ثبت شده بر روی یک رابط فیزیکی فعال، خواهد بود.اگر ID مسیریاب از بین برود یا غیـر فعـال شـود آنگاه دوباره مسیریاب جهت گرفتن ID به رابط ها رجوع میکند و از بین آنها بزرگتـرین شـماره IP را بعنـوان ID انتخاب می کند، اما به دلیل ایجاد ثبات و پایداری در شبکه ، نباید امکان تغییر ID مسـیریاب OSPF را بـدهیم .پس یک راه بهتر، استفاده از یک رابط مجازی (Virtual Inteface) و یا حلقه برگشتی (LoopBack) است. یـک رابط حلقه برگشتی رابطی غیر فیزیکی و یا مجازی است که بر روی مسیریاب تنظیم و پیکربندی می شود.اگر از یک رابط حلقه برگشتی (Loopback) استفاده شود، در این صورت OSPF از آدرس IP ثبت شده بر روی حلقـه برگشتی ( Loopback Interface) استفاده خواهد کرد، حتی اگر این آدرس بـالاترین آدرس IP هـم نباشـد. بـه منظور تثبیت ID مسیریاب OSPF، بهترین روش استفاده از دستور route-id ip-address در پیکربندی پردازش OSPF است.متغیر ip-address می تواند هر آدرسی باشد البته تا زمانی که آن آدرس در شبکه شما منحصـر بـه فرد (Unique) است.

## 8-2همسایه یابي OSPF:

زمانی که OSPF بر روی یک رابط فعال می شود، مسیریاب یـک بسـته سـلام (Hello Packet) بـر روی شبکه ارسال می کند تا همسایگان خود را بیابد.در یک شبکه با چندین دسترسی (Multi-Access) بسـته سـلام هر ده ثانیه یکبار فرستاده می شود.در روتر وضعیت خاموش نشان دهنده ایـن اسـت کـه مسـیریاب هـیچ بسـته سلامی (Hello Packet) را ارسال نمی کند.زمانی که OSPF بر روی یک رابط فعال شـود، مسـیریاب بـه حالـت

Init و یا آغازین (Initialization) تغییر وضعیت می دهد و شروع به ارسال بسته های سلام می کند.وضعیت آغازین ،همسایه های OSPF را بر روی یک اتصال (Link) شناسایی میکند.درون بسته سلام ، ID مسیریاب OSPF (Router ID) نیز قرار دارد.زمانی که یک مسیریاب،بسته سلامی را از یک همسایه دریافت می کند، ID مسیریاب خود را درون بسته قرار می دهد و بر روی شبکه ارسال می کند.زمانی که مسیریاب ، ID مسیریاب خود را داخل بسته سلام همسایه مشاهده کند، همسایه ها در وضعیت دو طرفه (2-Way) قرار می گیرند.

در یک شبکه با چندین دسترسی (Multi-Access)،یک مسیریاب (Designated Router-DR) و یک مسیریاب به عنوان پشتیبان مسیریاب اختصاصی (Backup Designated Router-BDR) انتخاب شده است.معمولا مسیریابی که بالاترین ID مسیریاب را دارد، DR و مسیریابی که پس از آن بالاترین ID را داراست،BDR محسوب می شود.با توجه به انتخاب DR وBDR مهمترین مسئله تنظیم وقت است.زمانی که یک مسیریاب به عنوان DR انتخاب شد تا وقتی که از بین نرفته است DR باقی خواهد ماند.به تمام مسیریاب های یک شبکه با چندین دسترسی (Multi-Access) که DR وDBR نیستند، DROTHER گفته می شود.

تمام مسیریاب های OSPF باید با همسایه های خود تبادل اطلاعات کنند و از همسانی اطلاعات تمام مسیریاب های یک ناحیه مشخص اطمینان یابند. لزومی ندارد هر مسیریاب موجود در شبکه با چندین دسترسی اطلاعات خود را برای تمام مسیریاب های دیگر موجود در شبکه بفرستد.بنابراین هر مسیریاب، یک مسیریاب و یا LSA نوع 1 بوجود می آورد، که وضعیت رابط های متصل به مسیریاب را مشخص می کند.تمام مسیریاب ها ، LSA مسیریاب خود را به DR و BDR ارسال می کنند.DR و BDR یک شبکه یا LSA نوع 2 را بوجود می آورد و آنرا به تمام مسیریاب های موجود در شبکه با چندین دسترسی (Multi-Access) می فرستد.در این حالت تمام مسیریاب ها به همجواری (Adjacency) کامل با DR و BDR می رسند. همجواری با DR و BDR به این معناست که هر مسیریاب بداند LSAهای خود را باید به آنجا ارسال کند.

در شبکه های نقطه به نقطه (Point to Point) مفاهیم DR و BDR وجود ندارد. زیرا در آنجا فقط دو همسایه و یک اتصال نقطه به نقطه وجود دارد.مسیریاب ها در یک اتصال نقطه به نقطه یک همجواری کامل برای تبادل آگهی های وضعیت اتصال OSPF بوجود می آورند.

بررسی همجواری oSPF با استفاده از دستور show ip ospf neighbor صورت می گیرد.

## 9-2بررسي عملكرد OSPF:

برای بررسی صحت عملکرد OSPF می توان انواع دستورات show را مورد استفاده قرار داد، که عبارتند از:

- دستور show ip protocols نشان دهنده انواع مختلف پارامترهای OSPF مانند تایمرها ، فیلترها، metricها، شبکه ها و اطلاعات مفید دیگر مربوط روتر مورد نظر می باشد.
- دستور show ip route ospfنشان دهنده ospf routeهای شناخته شده توسط روتر است.استفاده از این دستور یکی از بهترین روش های تشخیص امکان برقراری ارتباط بین روتر مورد نظر و بقیه شبکه می

باشد.البته پارامترهای دیگری مانند OSPF process id را می توان در کنار دستور به کار برده و اطلاعات دلخواه را مورد بررسی قرار داد.

- دستور show ip ospf interface:نشان دهنده areaهای مربوط به interface های روتر می باشد.همچنین اطلاعات دیگری مانند تایمرها (مانند hello interval ) و روابط مجاورت بین روترها نیز توسط دستور فوق نمایش داده خواهند شد.
- دستور show ip ospf:این دستور نشان دهنده ospf router id، انواع تایمرها، تعداد دفعات اجرای الگوریتم spf و اطلاعات مربوط به lsaها می باشد.
- دستور show ip ospf neighbor:نشان دهنده لیست روترهای همسایه،id مربوط به روترهای DR/BDR در کنار id و priority مربوط به روترها و وضعیت رابطه مجاورت (init,Exstart,Full) آنها با این روتر خواهد بود.

## 10-2تایمرهاي OSPF:

در شبکه های Multi-Access تایمر سلام OSPF (OSPF Hello Timer) به طور پیش فرض در 10 ثانیه تنظیم شده است.تمام مسیریاب های OSPF که به یک شبکه عمومی نقطه به نقطه (Point To Point) یا (Multi-Access) متصل هستند، تا وقتی که دارای زمان سلام برابر نباشند، نمی توانند به همجواری (Adjacency) برسند.دست است که بسته های سلام جهت تشخیص همسایه یابی به کار می روند، اما کاربرد دیگر آنها بقای عمر می باشد!اگر 4 برابر زمان سلام ، بسته سلامی از یک هخمسایه دریافت نشود، از آن همسایه صرفه نظر خواهد شد.از این زمان به عنوان زمان مرگ (Dead Time) یاد می شود.

پس از اینکه OSPF به همجواری کامل با همسایه های مورد نظر دست پیدا کرد و پایگا های اطلاعاتی هماهنگ شدند، اگر تغییری در شبکه ایجاد شود یا بعد از 30 دقیقه OSPF تنها اطلاعات مربوط به پایگاه اطلاعاتی را ارسال می کند.بنابراین در یک شبکه ثابت OSPF پروتکلی آرام است.

بعد از تبادلات اولیه و همسانی پایگاه های اطلاعاتی ، OSPF با استفاده از الگوریتم SPF به محاسبه کوتاهترین مسیر به هر مقصد می پردازد.الگوریتم OSPF تنها در صورتی دوباره فعال خواهد شد که تغییری در شبکه دوباره رخ داده باشد. وسعت محاسبات الگوریتم OSPF بستگی به تعداد مسیریاب ها و پیشوند شبکه های موجود در یک ناحیه دارد.اگر یک شبکه نوسانی دارای تغییرات زیاد (Flapping) باشد(دائم شبکه از حالت بالا به پایین ،پایین به بالا و الی آخر باشد) با هر تغییر وضعیت شبکه، OSPF یک بروزرسانی ارسال می کند و تمام مسیریاب های ناحیه باید کوتاهترین مسیر را دوباره محاسبه کنند.به منظور جلوگیری از محاسبات بی پایان الگوریتم SPF توسط مسیریاب ها ، از یک تایمر SPF جهت تعیین حداقل زمان سپری شده پیش از محاسبه مجدد SPF استفاده می شود.به طور پیش فرض تایمر SPF در 10 ثانیه تنظیم شده است.

## 11-2انواع LSA در OSPF:

مسیریاب های OSPF برای معرفی شبکه هایشان از بسته هـای LSAهـا اسـتفاده مـی کننـد.جهت درک عملکرد OSPF نیازی به دانستن جزیئات و یا ساختار LSAها ندارید.اما دانستن انواع LSAها یی کـه در OSPF به کار می روند و اطلاعات موجود در آنها، برای شما مفید خواهد بود.

هر یک از انواع LSA ها به شرح زیر می باشند:

- LSA مسیریاب (Router LSA):برای ناحیه ای که مسیریاب به آن متصل است بوجود می آیـد. ارزش و حالت اتصالات مسیریاب را در یک ناحیه توضیح مـی دهـد.یک مسـیریاب LSA تنهـا در ناحیـه OSPF خـود سرریز خواهد شد.
- LSA شبکه (Network LSA):توسط DR بر روی یک شبکه با چند دسترسی (Multi-Access) بوجود آمده است و شامل اطلاعات مورد نیاز تمام مسیریاب های متصل به شبکه Multi-Access می باشد.
- LSA خلاصه شبکه (Network Summary LSA):توسط ABRها تولید شده اسـت و شـامل اطلاعـاتی درباره پیشوندهای OSPF بین ناحیه ای است. یک خلاصه شبکه LSA درون ناحیه OSPF غیر 0 سر ریز خواهد شد.
- LSA خلاصه ASBR (ASBR Summary LSA ):توسط ABRهـا بـه وجـود آمـده و دارای سـاختاری مشابه LSAهای خلاصه شبکه می باشد.اما به جای اطلاعات پیشوند IP ویژه، شامل موقعیت مکانی یک ABSR خواهد بود.
- LSA AS External:توسط ABSRها بوجود می آید و شامل اطلاعات مربوط به پیشوندهایی اسـت کـه در محدوده OSPF خارجی هستند(مسیرهای خارجی (External Route) نوع 1و2).
- LSA پیغام چند منظوره (Multicast LSA):OSPF با استفاده از این LSA بـرای پشـتیبانی از IPهـای چند منظوره اصلاح شده است ، اما از OSPF چند منظوره استفاده نمی شود.
- LSA خارجی NSSA (NSSA External LSA):در زمان تنظـیم بـه عنـوان یـک NSSA ،بـه وسـیله ASBRها بوجود می آید.اینها مسیرهای خارجی هسـتند کـه بـا N1 یـا N2 مشـخص شـده و فقـط در NSSA سرریز(Flooded) می شوند. مسیریاب ABR مسیرهای N1 وN2 را پیش از معرفی آنها درون محدوده OSPF به E1 وE2 تبدیل می کند.

## 12-2انواع شبکه هاي تعريف شده در OSPF:

درک این که هر کدام از OSPF AREA از انـواع مختلفـی از اتصـالات شـبکه ای ترکیـب شـده اسـت از اهمیت بسیاری برخوردار است. زیرا برقراری رابطه مجاورت در هر کدام از انواع شبکه ها متفاوت از دیگری بـوده و پیکربندی OSPF نیز باید به گونه ای انجام گیرد که عملیات routing شبکه با صحت تمام انجام گیرد.

عملکرد OSPF در انواع مختلف شبکه ها، مانند شبکه های Point-to-Point و broadcast نسبت به هم متفاوت بوده و در برخی از مواقع، تنظیمات پیش فرض آن جوابگو شرایط حاضر نمی باشد.OSPF شبکه ها را بر اساس نوع اتصالات فیزیکی مابین آنها تقسیم بندی می نماید.عملکرد OSPF در روی هر کدام از شبکه های مختلف نسبت به هم متفاوت بوده و نوع ونحوه برقراری رابطه مجاورت در هر کدام نسبت به بقیه دارای تفاوت محسوسی است.

انواع شبکه های تعریف شده در OSPF عبارتند از:

- Point-to-point :شبکه ای که متصل کننده یک جفت از روترهاست.
- Broadcast
- Nonbroadcast multi-access (NBMA) :در این نوع شبکه ها با اینکه تعداد زیادی از روترها با هم در تماس می باشند،امکان استفاده از پیام های broadcast وجود ندارد.برای مثال می توان به اتصالات x.25،ATM،Frame Relay اشاره کرد.

برقراری رابطه مجاورت در اتصالات point-to-point :

در این نوع اتصال ، دو روتر به صورت مستقیم با همدیگر در ارتباط می باشند.برای مثال می توان یک ارتباط T1 را که با استفاده از پروتکل های لایه دوم مانند PPP یا HDLC ایجاد شده اند نام برد.

در این نوع شبکه ها، یک روتر با ارسال پیام های multicast با آدرس 224.0.0.5 برای روترهای OSPF اقدام به شناسایی اتوماتیک روترهای همسایه خواهد کرد.به دلیل اینکه فقط دو روتر در یک شبکه point-to-point وجود دارد، نیازی به انتخاب روترهای DR/BDR نیست.آدرس فرستنده مربوط به یک پیام ارسالی معمولا برابر با آدرس interface ارسال کننده پیام قرار می گیرد.البته با استفاده از ویژگی ip unnumbered interface می توان آدرس مزبور را برابر با آدرس یک interface دیگری قرار دارد.در یک اتصال point-to-point مدت زمان پیش فرض بین ارسال پیام های hello یا hello interval برابر با 10 ثانیه و مدت زمان dead interval نیز برابر با 40 ثانیه می باشد.

برقراری رابطه مجاورت در اتصالات Broadcast:

برقراری رابطه مجاورت بین روترهای OSPF در شبکه های broadcast مانند Ethernet نیاز به انتخاب روترهای DR/BDR دارد.بدین صورت که هر کدام از روترها اقدام به برقراری رابطه مجاورت فقط با روترهای BR/BDR نموده و محتویات جدول LSDB خود را فقط با روترهای مزبور به اشتراک می گذارند.زمانی که یک روتر به عنوان DR ایفای نقش می نماید، روتر BDR در حالت غیر فعال قرار خواهد داشت.یعنی BDR پیام های رسیده به DR را عینا دریافت کرده اما عملیات ارسال پیام ها برای روترهای DROTHER و نیز برقراری رابطه مجاورت با آنها از وظایف روتر DR می باشد.به محض اینکه روتر DR معیوب گشته و یا به هر دلیلی قابل دسترسی نباشد، روتر BDR به عنوان DR قرار داده شده و رئتر دیگری برای در اختیار گرفتن نقش BDR انتخاب خواهد شد.به دلایل زیر، استفاده از روترهای DR/BDR عملکرد شبکه را بهبود خواهد بخشید:

- کاهش ترافیک شبکه با کاهش میزان Updateهای ارسالی.یک روتر BR/BDR به عنوان روتـر مرکـزی بوده و بقیه روترهای رابطه مجاورت خود را فقط با روترهای DR/BDR برقرار خواهند ساخت.به جای اینکه یـک روتر OSPF اقدام به ارسال پیام Update خود برای تک تک روترهای واقع در یک شبکه broadcast نماید، پیـام ها فقط برای روتر DR/BDR ارسال خواهد شد واین روترهای DR/BDR می باشند که وظیفه پخـش پیـام را در بین روترهای دیگر بر عهده دارند.این ویژگی باعث کاهش محسوس ترفیک شبکه می گردد.
- مدیریت پخش محتویات جدول LSDB:بـه دلیـل اینکـه روترهـای DR/BDR وظیفـه یکسـان سـازی اطلاعات روتینگ شبکه را در روی همه روترها بـر عهـده دارنـد، از ایـن رو اخـتلالات پـیش آمـده در عملیـات routing ، به دلیل یکسان نبودن LSDB در روی روترهای شبکه، به حداقل خواهد رسید.

## 13-2برقراري رابطه مجاورت در شبکه هاي NBMA:

زمانی که یک روتر از روی یک interface خود به سایت های مختلفی از طریق اتصالات NBMA متصـل گردد،نبود امکان استفاده از پیام های broadcast باعث بروز مشـکلات عـدم دسترسـی در شـرایط فـوق خواهـد گردید.همانطور که گفته شد، دتر یک شبکه NBMA چندین روتر بـدون اسـتفاده از پیـام هـای broadcast بـا همدیگر در تماس خواهند بود.به عنوان مثال زمانی که یک شـبکه NBMA بـه صـورت fully-meshed طراحـی نشده باشد، پیام های multicast وbroadcast ارسالی از یک روتر توانایی دسترسی به برخی از روترها را نخواهند داشت.

یک روتر در شبکه NBMA برای شبیه سـازی یـک پیـام broadcast یـا multicast عـین پیـام را مجـددا بـرای دریافت کننده بعدی ارسال خواهد کرد.این کار باعث بالا رفتن پردازشی روتر شده و مصرف پهنای باند شـبکه را نیز افزایش می دهد.

مدت زمان پیش فرض بین ارسال پیام های hello یا hello interval در شبکه های NBMA برابر با 30 ثانیـه و زمان dead interval برابر با 120 ثانیه می باشد.

پروتکل OSPF فرض را بر این می گذارد که شبکه های NBMA دارای عملکردی شبیه شبکه هـای broadcast می باشند.با وجود این ،توپولوژی NBMA بر پایه hub-and-spoke عمل می نماید.بـدین معنـی کـه توپولـوژی hub-and-spoke به صورت fully-meshed طراحی نمی گردد.در چنین شرایطی انتخاب روترهای DR/BDR نیز با مشکل مواجه خواهد شد.زیرا برای عملکرد روترهای DR/BDR نیاز به وجود یک رابـط فیزیکـی بـین تمـامی روترهای شبکه داریم.همچنین روترهای DR/BDR برای برقراری رابطه مجاورت با روترهای دیگـر بایـد لیسـت تمامی روترهای شبکه را در اختیار داشته باشد.در نتیجه ،OSPF قادر به برقراری اتوماتیـک رابطـه مجـاورت بـا روترهای همسایه در شبکه های NBMA نخواهد بود.

## 14-2پیکربندي OSPF در شبکه هاي Frame Relay:

بسته به نوع توپولوژی Frame Relay، گزینه های متفاوتی را می توان در پیکربندی OSPF به کار برد.روش برقراری ارتباط روترهای remote با یکدیگر در یک اتصال frame relay می تواند متفاوت از هم باشد.به صورت پیش فرض، نوع interface مورد استفاده در اتصال frame relay به صورت multipoint قرار داده می شود.انواع مختلف توپولوژی frame relay عبارتند از:

1. توپولوژی STAR:

این نوع توپولوژی که به نام hub-and-spoke نیز نامیده می شود، یکی از معمول ترین نوع توپولوژی بکار رفته در اتصالات frame relay می باشد.در چنین مواردی، روترهای remote به یک روتر مرکزی که ارائه دهنده سرویس می باشد متصل می شوند.به دلیل اینکه تعداد PVCهای مورد نیاز در این توپولوژی کم می باشد، از این رو اجرای آن نسبت به بقیه اتصالات frame relay دارای هزینه کمتری است. همچنین روتر مرکزی معمولا با استفاده از یک multipoint interface اقدام به برقراری ارتباط با روترهای remote مینماید.

2. توپولوژی full-mesh:

در این توپولوژی، تمامی روترها دارای یک VC به سمت روترهای دیگر می باشند.با اینکه هزینه برقراری چنین توپولوژی زیادتر خواهد بود، ولی به دلیل وجود ارتباط مستقیم بین تمامی روترها مزیت هایی را نیز در اختیار خواهیم داشت.برای محاسبه تعداد VCها ی مورد نیاز از فرمول n(n-1)/2 استفاده می شود که n نشان دهنده تعداد روترهای موجود در شبکه می باشد.

3. توپولوژی partial-mesh:

در این توپولوژی بر خلاف نوع قبلی ، همه روترها دارای اتصال مستقیمی با یکدیگر نمی باشند. بلکه VCها فقط در بین روترهای مورد نیاز ایجاد گشته اند. این روش هزینه نسبتا کمتری را نسبت به توپولوژی قبلی در بر خواهد داشت.

طبق استاندارد RFC 2328، پروتکل OSPF به یکی از دو طرق زیر در شبکه های NBMA اجرا می گردد:

1)Nonbroadcast:در این متد، پروتکل OSPF شبیه به شبکه های broadcast عمل می نماید.پیکربندی روترهای همسایه باید به روش دستی انجام گرفته و انتخاب روترهای DR/BDR نیز ضروری است.این روش معمولا در شبکه های fully-meshed اجرا می گردد.

2)point-to-point:در این روش، شبکه NBMA به صورت مجموعه ای از اتصالات point-to-point در نظر گرفته می شود.شناسایی روترهای همسایه به صورت اتوماتیک انجام شده ولی نیازی به انتخاب روترهای DR/BDR وجود ندارد.این روش معمولا در شبکه های partially-meshed اجرا می شود.

با نتخاب یکی از گزینه های فوق در واقع نوع ارسال پیام های hello و چگونگی انتشار پیام ها را مشخص می کنیم.مزیت روش اول در هزینه کمتر آن و مزیت متد دوم در پیکربندی آسانتر آن می باشد.علاوه بر موارد فوق سیسکو سه روش دیگر نیز تعریف نموده است که عبارتند از:

1)point-to-point nonbroadcast

2)broadcast

3)point-to-point

نکته: دستوری که شبکه را در پروتکل OSPF پیکربندی می کند به صورت

Router(config-if)#ip ospf network [{broadcast |non-broadcast |point-to-multipoint }]

کاربرد OSPF در شبکه های non-broadcast(NBMA):

با تعیین نوع non-broadcast، عملکرد OSPF در شبکه های broadcast شبیه سازی می گردد.انتخاب روترهای DR/BDR ضروری بوده و روتر DR وظیفه برقراری رابطه مجاورت با بقیه روترهای شبکه و نیز ارسال پیام های LSA Update برای آنها را به عهده دارد.در چنین شرایطی، طراحی شبکه معمولا به صورت fully-mesh صورت می گیرد تا ایجاد رابطه مجاورت بین روترهای شبکه آسان تر انجام بگیرد.زمانی که طراحی به صورت fully-mesh انجام نگرفته باشد، روترهای DR/BDR را باید به صورت دستی پیکربندی کرده تا از اینکه آنها توانایی برقراری ارتباط مستقیم با بقیه روترهای شبکه را دارند اطمینان حاصل نمود.در هنگام استفاده از این نوع، تمامی interface های دخیل باید در یک شبکه IP قرار داشته باشند.

هر کدام از interfaceهای non-broadcast در هنگام ارسال پیام LSU، آن را از طریق VCها برای هر کدام از روترهای همسایه مشخص شده در جدول Neighbor ارسال می نمایند.

در شرایطی که تعداد روترهای واقع در یک شبکه کم باشد، به کارگیری non-broadcast نسبت به استفاده از point-to-multipoint باعث صرفه جویی در هزینه های برقراری ارتباط خواهد شد.بطور پیش فرض پروتکل OSPF در اتصالات X.25، ATM و frame relay در نوع non-broadcast اجرا می گردد.

## 15-2کاربرد OSPF در شبکه frame relay point-to-multipoint:

برای اجرای سناریو فوق نیاز به در اختیلر داشتن توپولوژی partial-mesh یا star داریم.در این نوع، نیازی به انتخاب روترهای DR/BDR نداشته و همچنین پیام های LSA نوع 2 نیز برای روترهای مجاور ارسال نمی شود.در چنین حالتی، روترها اقدام به تبادل پیام های LSU مخصوص کرده و در نتیجه روترهای همسایه خود را شناسایی می نمایند.

به دلیل این که در point-to-multipoint نیازی به طراحی full-mesh شبکه نداریم، هزینه های مازاد برای ایجاد VCها صرفه جویی شده و مخارج کلی طرح کاهش خواهد یافت. علاوه بر آن،جداول routing روتر در شبکه های partial-mesh دارای روترهای کمتری بوده و به این ترتیب بار پردازشی روتر و مصرف پهنای باند شبکه نیز کاهش می یابد.ویژگی های point-to-multipoint به شرح زیر است:

1)نیازی به طراحی full-mesh شبکه ندارد.در این نوع ،عملیات routing بین دو روتر که نه به صورت مستقیم،بلکه از طریق یا روترهای واسط که توسط VCها با دو روتر در تماس می باشند،انجام گیرد.

2)نیاز به تعیین دستی روترهای همسایه وجود ندارد.

3)از یک آدرس IP استفاده می شود.

در point-to-multipoint نیازی به انتخاب روترهای DR/BDR وجود نداشته و بنابراین تعیین priority نیز دارای اهمیت خاصی نخواهد بود.

برای بررسی از صحت کار می توان از دستور show ip ospf interface بهره گرفت که عملکرد ospf را با ازای تک تک interfaceها نمایش می دهد.در خروجی دستور فوق می توان نوع شبکه ospf ،شماره area، مقدار پارامتر cost و وضعیت interface مورد نظر را مشاهده نمود.باید در نظر داشت که مقدار زمان hello interval در این نوع برابر با 30 ثانیه و زمان dead interval نیز برابر با 120 ثانیه می باشد.مقدار این دو زمان باید در روی دو روتر همسایه یکسان باشد.در غیر اینصورت، روترها قادر به برقراری رابطه مجاورت با همدیگر نخواهد بود.شناسایی روترهای همسایه نیز به صورت اتوماتیک انجام گرفته و نیازی به مشخص کردن دستی آن ها با دستور neighbor نیست.

سیسکو یک نوع دیگر برای روش point-to-multipoint معرفی کرده است که مخصوص خود بوده و به نام point-to-multipoint nonbroadcast نامیده می شود.در این روش،مشخص کردن روترهای همسایه به صورت دستی انجام گرفته و در این حین می توان cost مربوط به اتصال یک روتر همسایه با این روتر را نیز تعیین نمود.نسخه RFC این روش،نیاز به استفاده از پیام های broadcast و یا multicast دارد.بنابراین زمانی که اجازه ارسال چنین پیام هایی در روی یک VC صادر نشده باشد،نمی توان point-to-multipoint را به کار گرفت.در چنین شرایطی است که استفاده از point-to-multipoint nonbroadcast سیسکو توصیه می شود.

## 16-2انواع روترهاي OSPF:

به دلیل اینکه سایز جداول OSPF LSDB معمولا زیاد است،بنابرابین طراحی شبکه باید به صورت درختی یا hierarchical انجام گیرد.یکی از راه حل های موجود تقسیم بندی شبکه به مناطق کوچکتر و استفاده از انواع روترها با نقش های مختلف می باشد.

پروتکل OSPF معمولا در شبکه های دارای یک area مورد استفاده قرار می گیرد.اما در صورتی که area مزبور شامل تعداد زیادی شبکه باشد،بهعث بروز مشکلات زیر خواهد شد:

- اجرای متناوب الگوریتم SPF: شبکه های بزرگ معمولا دچار تغییرات زیادی می شوند.در نتیجه روترها نیاز به اجرای چندین باره الگوریتم SPF و به روز کردن جدول routing خود خواهند داشت.
- جداول routing حجیم:پروتکل OSPF به صورت پش فرض عمل summarization را انجام نمی دهد. در این شرایط،سایز جدول routing می تواند به طور چشمگیری افزایش یابد.

- جداول LSDB حجیم:به دلیل اینکه OSPF اطلاعات مربوط به تمامی شبکه های موجود را در داخل جدول توپولوژی یا LSDB خود نگهداری می کند،بنابراین در صورت افزایش تعداد شبکه ها موجود در داخل یک area اندازه جدول فوق نیز افزایش پیدا خواهد کرد.

در این موقعیت،می توان پروتکل PSPF را به مناطق مدیریتی کوچکتر تقسیم کرده و مشکلات فوق را برطرف نمود.هر کدام از این مناطق به نام area نامیده می شود.در شرایطی که یک شبکه بزرگ را به areaهای کوچکتری تقسیم می کنیم.عملیات routing در بین areaها مختلف رخ داده اما اجرای الگوریتم SPF محدود به داخل یک area خواهد شد.

در هنگام استفاده از areaهای متعدد،انواع مختلفی از روترها را در اختیار خواهیم داشت که عبارتند از:

1)روترهای داخلی یا internal:

روترهایی که تمامی interfaceهای آن ها در داخل یک area قرار داشته و دارای محتویات یکسان در داخل جدول LSDB خود باشند به نام روترهای داخلی یا internal نامیده می شوند.

2)روترهای backbone:

روترهایی که حداقل از طریق یکی از interfaceهای خود به area 0 متصل می باشند.به نام روترهای backbone نامیده می شوند.مکانیسم اجرای الگوریتم SPF در این روترها شبیه به روترهای داخلی می باشد.

3)روترهای ABR:

روترهایی که به چند area مختلف متصل شده اند،حاوی جداول LSDB جداگانه برای هر کدام از areaهای متصل می باشند.روترهای ABR به عنوان تنها نقطه اتصال یک area به areaهای دیگر بوده و بنابراین ترافیک های به مقصد areaهای دیگر تحویل روترهای ABR خواهد شد.همچنین می توان عملیات summarization را در هنگام ارسال اطلاعات از یک area به area دیگر انجام داد.اطلاعات فرستاده شده توسط یک area و روتر ABR آن،برای area 0 فرستاده شده که آن نیط به نوبه خود پیام ها را برای area مقصد ارسال خواهد کرد.البته به یاد داشته باشید که هر کدام از areaها می توانند دارای چندین روتر ABR باشند.

4)روترهای ASBR:

روترهایی که حداقل یکی از interfaceهای آ«ها متصل به یک AS خارجی یا شبکه ای غیر از OSPF می باشد،به نام روترهای ASBR نامیده می شوند.این روترها وظیفه انتقال اطلاعات routing به داخل یک OSPF domain و بالعکس را دارند.این پروسه به نام Route Redistribution نامیده میشود.

## 17-2انواع پیام در پروتکل OSPF:

- پیام سلام :وقتی یک مسیریاب روشن و بوت میشود موظف است به تمام مسیریابهایی که مستقیماً به آنها متصل است یک پیام" سلام "بفرستد تا آنها از حضور این مسیریاب درشبکه مطلع شوند.
- پیام Link State Update: هر مسیریاب موظف است که در بازههای زمانی مشخص ،جدول مسیریابی خودش را به روش سیلآسا به اطلاع دیگر مسیریابهای همناحیه برساند .این کار را با ارسال این پیام انجام میدهد؛

در ضمن هر مسیریاب وقتی هزینهٔ یکی از خطوط مستقیم او تغییر کرد یا مسیریاب مجاورش از شبکه بیرون رفت ( یا به شبکه برگشت ) سریعاً با این پیام آنرا به اطلاع دیگران میرساند.

- پیام Database Description : هر مسیریاب به ازای تکتک رکوردهای هزینه که در یک بانک اطلاعاتی درون حافظهٔ اصلی ذخیره کرده ، یک فیلد شمارهٔ ترتیب در نظر میگیرد. مسیریابِ ارسال کننده این پیام ، شمارهٔ ترتیب و تمام رکوردهایی را که در بانک اطلاعاتی خود ذخیره کرده است ، ارسال مینماید .گیرندهٔ این پیام با مقایسهٔ شمارههای ترتیب رکوردها با رکوردهایی که در بانک اطلاعاتی خود دارد میتواند رکوردهای قدیمیتر را با رکوردهای جدید جایگزین نماید.
- پیام Link State Request : با این پیام هر مسیریاب میتواند اطلاعات جدول مسیریابی را از از یک مسیریاب خاص تقاضا نماید .با این کار مسیریاب میتواند ضمن درخواست جدول مسیریابی همسایههای خود و مقایسهٔ شمارهٔ ترتیب رکوردهای آن اقدام به تازهسازی جدول خود نماید.
- پیام Link State Ack : این پیام توسط گیرندهٔ پیام Link State Update برای ارسال کنندهٔ آن ارسال میشود و به منظور تصدیق دریافت جدول مسیریابی میباشد.

با استفاده از ویژگی authentication، روترهای OSPF قادر به شناسایی روترهای همسایه می باشند.بدین معنی که با به کارگیری authentication می توان روترهای شرکت کننده در پروسه های routing را مشخص کرد.

انواع OSPF authentication:

دو متد برای پیکربندی مکانیسم شناسایی هویت در OSPF وجود دارد که عبارتند از :

1) Simple یا plain

2) MD5

در صورت پیکربندی یک متد برای شناسایی هویت روترها در OSPF ،زمانی که یک روتر اقدام به دریافت پیام Update ارسال شده از روتری دیگر می نماید، هویت روتر ارسال کننده را با استفاده از یک پسورد بررسی کرده و در صورت یکسان بودن آن با پسورد تعیین شده در روی خود،پیام دریافت شده را خواهد پذیرفت.به صورت پیش فرض هیچ نوع مکانیسمی برای شناسایی هویت روترهای ارسال کننده پیام Update در پروتکل OSPF مورد استفاده قرار نمی گیرد.

## 18-2کاربرد Ipv6 در پروتکل OSPF:

استاندارد RFC 2740 کاربرد پروتکل OSPF در پروتکل IPv6 را تعریف می کند.

نسخه های جدید پروتکل های routing قادر به پشتیبانی از آدرس های با طول زیاد مانند آدرس های IPv6 و همچنین ساختار header مربوط به آن می باشند.

مکانیسم استفاده از routeهای استاتیک در IPv6 نیز شبیه به IPv4 می باشد.استاندارد RFC 2461 در مورد IPv6 چنین می گوید:هر کدام از روترها باید از آدرس link-local مربوط به تمامی روترهای همسایه خود با

اطلاع بوده؛ به صورتی که پیام های ارسالی قادر به تشخیص روترهای مقصد با استفاده از آدرس های link-local باشند.

گفته فوق بدین معناست که استفاده از آدرس های global unicast به عنوان آدرس next-hop توصیه نمی گردد.قبل از اینکه هر کدام از پروتکل های مختلف قادر به استفاده از IPv6 باشند،باید با استفاده از دستور زیر اقدام به فعال سازی IPv6 در روی روتر نماییم.

Router(config)#ipv6 unicast-routing

## 19-2عملکرد OSPF در شبکه هاي IPv6:

پروتکل OSPF از گروه link state بوده و از پارامترcost به عنوان metric استفاده می کند.

پروتکل OSPF اطلاعات مربوط به interface مانند ipv6 prefix ،ماسک مربوطه،نوع شبکه متصل،روترهای متصل به شبکه فوق و...را بین روترهای همسایه منتقل می نماید. اطلاعات مربوطه از طریق پیام های LSA منتقل شده و هر روتر نیز تمامی اطلاعات کسب شده از طریق مبادله پیام های LSA را در داخل جدول LSDB خود ذخیره می نماید.سپس الگوریتم dijkstra رجرا شده و بهترین مسیرهای منتهی به مقاصد مختلف در داخل جدول routing قرار داده می شود.

تفاوتی که بین جدول routing و جدول LSDB وجود دارد، در آنجاست که جدول LSDB حاوی اطلاعات مربوطه به تمامی مقاصد و مسیرهای منتهی به آنها بوده اما جدول routing فقط شامل بهترین مسیرهای برگزیده شده به سمت مقاصد مختلف می باشد.

جدیدترین نسخه OSPF ،نسخه سوم آن بوده و در استاندارد RFC 2740 تعریف می گردد.

## 20-2مقایسه OSPF V2 و OSPF V3:

با اینکه مکانیسم عملکرد دو نسخه OSPF بسیار شبیه به هم می باشد،اما برخی از تغییرات اعمال شده در OSPF V3 باعث گردیده است تا این پروتکل قادر به حمل آدرس های طولانی IPv6 بوده و نیز توانایی اجرای مستقیم بر روی IP را داشته باشد.برخی از شباهت های موجود بین این دو نسخه عبارتست از:

- هر دو پروتکل از پیام های یکسانی برای انجام فعالیت خود بهره می گیرند. این پیام ها شامل hello ،dbd،lsr،lsu،lsa می شوند.
- مکانیسم شناسایی روترهای همسایه و نیز چگونگی برقراری رابطه مجاورت با روترهای همسایه نیز شبیه هم می باشد.
- هر دو پروتکل از شبکه های یکسانی پشتیبانی می کنند که لیست آنها عبارتند از point-to-point،point-to-multipoint،broadcast،nbma.
- مکانیسم انتشار پیام های LSA و نیز تعیین مدت زمان عمر هر کدام از LSAها در روی هر پروتکل یکسان می باشد.

به دلیل اینکه پروتکل OSPF v2 بر پایه IPv4 بنا شده است ،بیشترین تغییرات اعمال شده در OSPF v3 برای پشتیبانی پروتکل OSPF از IPv6 صورت گرفته است.برخی دیگر از تغییرات اعمال شده عبارتند از:غیر وابسته بودن آن به پلتفرمی خاص،انجام عملیات routing بر اساس هر یک از پیوندها(پروتکل OSPF v2 عملیات routing را بر پایه هر کدام از دستگاه ها انجام می دهد)،اجرای چندین پروسه مختلف در روی یک اتصال،تغییرات در ساختار پیام ها ودر مکانیسم authentication.

هم اکنون OSPF،IPv6 به عنوان یک استاندارد توسط سازمان IETF پذیرفته شده و مانند RIPng از پروتکل IPv6 برای حمل اطلاعات و نیز از آدرس های link-local به عنوان آدرس فرستنده بهره می گیرد.همچنین بقیه پارامترهای اختیاری در OSPF v2 مانند NSSA،MOSPF نیز به همان صورت در OSPF v3 پشتیبانی می گردد.

پروتکل OSPF v2 وابسته به شبکه ای است که در داخل آن اجرا می گردد.اما پروتکل OSPF v3 وابسته به اتصالاتی است که متصل به یک روتر می باشد.

پروتکل OSPF اجازه پیکربندی بیش از یک پروسه OSPF را در روی یک interface نمی دهد.اما این کار در OSPF v3 قابل اجرا است.

در پروتکل OSPF v3 انجام عمل authentication دیگر بر عهده OSPF نبوده و وظیفه آن را خود IPv6 بر عهده دارد.

تفاوت های عمده پروتکل های OSPF v2 و OSPF v3 به شرح زیر است:

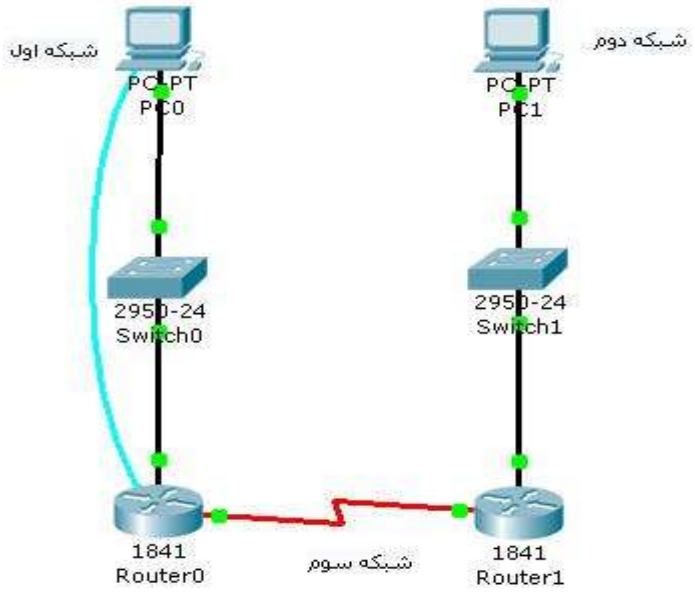
- اجرای OSPF v3 در روی روتر اتصال مورد نظر:دستور network مورد استفاده در پروتکل OSPF v2 با دستور دیگری در OSPF v3 جایگزین شده است.پیکربندی چندین پروسه مجزای OSPF در روی یک اتصال واحد در نسخه جدید پروتکل لمکان پذیر شده است.
- روترها در OSPF v3 از آدرس های IPv6 link-local برای شناسایی همدیگر و برقراری رابطه مجاورت استفاده می نمایند.
- استفاده OSPF v3 از آدرس multicast برابر با FF02::5 برای نشان دادن تمامی روترهای OSPF داخل شبکه.(معادل آدرس 224.0.0.5 در پروتکل OSPF v2).
- استاده OSPF v3 از آدرس multicast برابر با FF02::6 برای نشان دادن تمامی روترهای DR داخل شبکه.(معادل آدرس 224.0.0.6 در پروتکل OSPF v2)
- آدرس های IPv6 جزئی از قسمت OSPF header نبوده ،بلکه در داخل پاکت ها قرار می گیرند.
- سایز مربوط به link state id،area id،router id برابر با 32 بیت می باشد.
- شناسایی روترهای DR/BDR توسط شناسه یا id آنها انجام می گیرد و نه با آدرس ip مربوط به آنها

## 2-21نحوه مسیریابی با پروتکل OSPF:

در پایان این فصل یک توپولوژی ساده را با نرم افزار شبیه سازی packet tracer پیاده سازی می کنیم :

ابتدا دو شبکه ایجاد می کنیم .شبکه اول یا آدرس شبکه 192.168.1.0 با ماسک 255.255.255.192 و شبکه دوم با آدرس شبکه 192.168.1.64 با ماسک 255.255.255.192 را ایجاد می کنیم .اما چون این دو شبکه از هم مجزا هستند برای برقراری ارتباط این دو شبکه به Deviceهایی مانند روتر نیاز داریم .اما نکته ای که نباید فراموش شود این است که بین این دو روتر نیز باید یک شبکه بوجود آوریم .آدرس شبکه بین روترهایمان 192.168.1.128 با ماسک 255.255.255.192 می باشد.ما روترهایمان را جهت اینکه بتوانند ارتباط برقرار کنند باید config کنیم و بر خلاف مثال فصل اول از مسیریابی داینامیک اسفاده می کنیم پروتکلی که این مسیریابی را انجام می دهد OSPF نام دارد و ما در اینجا نحوه ی بکار اندازی پروتکل OSPF درون سیستم عامل IOS روتر تشریح می کنیم.

همانند شکل زیر :




شکل 2-1

دستورات زیر جهت config روترهای صفر و یک بکار میروند:

```
Router0(config)#router ospf 1
Router0(config-router)#network 192.168.1.0 0.0.0.63 area 0
Router0(config-router)#network 192.168.1.128 0.0.0.63 area 0
Router0(config-router)#end

Router0(config)#router ospf 1
Router0(config-router)#log-adjacency-changes
Router0(config-router)#end
Router1(config)#router ospf 1
```

```
Router1(config-router)#network 192.168.1.64 0.0.0.63 area 0
Router1(config-router)#network 192.168.1.128 0.0.0.63 area 0
Router1(config-router)#end

Router1(config)#router ospf 1
Router1(config-router)#log-adjacency-changes
Router1(config-router)#end
```

# فصل سوم
# طراحي و پياده سازي مدل فازي OSPF

## 3-1مسير يابي مبتني بر كيفيت سرويس(QOS):

منظور از مسیریابی مبتنی بر کیفیت سرویس درشکل پایه ای آن مبتنی بر قید کیفیت سرویس می باشد.مسئله ای که مسیریابی کیفیت سرویس سعی در حل آن دارد اثبات بهبود سطح سرویس کاربران به منظور پشتیبانی از نیازمندیهای چند رسانه ای در دنیای امروز اینترنت است. مسیریابی کیفیت سرویس یک امکان برای کارگذار و مدیر شبکه در افزایش کارایی آنان برای اداره کردن ترافیک موجود در شبکه براساس خصوصیات و ویژگی های آن ترافیک می باشد.OSPF به کمک فیلدی از هدر خود به نام TOS( نوع سرویس ) امکاناتی را برای مسیریابی بر اساس حداقل تاخیر (TOS =16) و یا حداکثر گذردهی (TOS =8) را فراهم نموده است .اما موردی که هست چون در این پروتکل مسیریابی هر کدام از این2 وضعیت، از پارامتر های مجزا از هم جهت در بر آوردن این خصوصیات استفاده می نماید، لذا نه تنها قابل پیگیری از طریق هم نمی باشند که امکان بهره مندی توامان از هر دو وجود نخواهد داشت اما درباره طول صف روتر و تاخیر لینک سعی بر آن شده است که با کمک یک الگوریتم فازی از ترکیب این 2 معیار و تولید یک معیار واحد نتایج مطلوبتری در انتخاب مسیرها ودرنتیجه پشتیبانی بهتر از کیفیت سرویس بدست آید.البته هر کدام از این 2 معیار دارای محدودیت های مخصوص به خود می باشند .مثلا تاخیر لینک پارامتری است که از مجموع آن برای تمامی لینک های یک مسیر،تاخیر آن مسیر (ROUTE DELAY) بدست می آید.لذا تاخیر یک پارامتر جمعی بوده است .اما آنچه که باید در نظر گرفت این موضوع است که پایین بودن تاخیر یک مسیر به معنای وجود پهنای باند کافی در آن مسیر نمی باشد .لذا مشخص و بارز خواهد بود که تاخیر برای بیان وضعیت شبکه کافی نیست و یا بعنوان مثالی دیگر اگر از طول صف مربوط به آن لینک ومسیر نیز کمک بگیریم ، مشکلات اندازه صف هم با موارد مشابه تاخیر،آشکار خواهد شد که به تنهایی قابل اعتماد نیست . چرا که محدودیتهایی برای بیان رفتار شبکه خواهد داشت . مواردی نظیر انفجارهای ترافیکی

و احتمال وجود بافرینگ در مسیرها باعث می شودکه پارامتر اندازه صف محدودیتهایی را برای صحت بیان ازدحام واعلام آن بر خود وارد بداند.چرا که با مواردی که توضیح داده شد رخداد صف بندی در زمانی که جریان ترافیکی حاضر کمتر از ظرفیت لینک باشد نیز وجود خواهد داشت .ضمنا پارامتر تاخیر برای یک لینک از 2 پارامتر تاخیر صف بندی به علاوه تاخیر لینک که از مشخصه های فیزیکی آن است ، تشکیل می شود.که در این بین سهم تاخیر صف بندی را باید بزرگتر در نظر گرفت چرا که عکس این مورد را در نظر بگیریم از آنجا که سیگنال های الکتریکی ویا نوری با سرعتی معادل نور درون لینک در حرکتند، این فرض غیر منطقی به نظر خواهد رسید.حال در ادامه مقاله در مورد گزینش پارامترها و نحوه ترکیب آنها توضیحات کاملتریارائه خواهد شد.

## 3-2اهداف مسیریابي کیفیت سرویس:

پروتکل های فعلی مسیریابی در اینترنت از قبیل BGP,RIP,OSPF پروتکل های مسیر یابی بهترین تلاش نام دارند که فقط کوتاهترین مسیر به مقصد را مشخص می کنند .به عبارت دیگر از الگوریتم های بهینه سازی تک منظوره بهره می گیرندکه در این الگوریتم ها تنها یک پارامتر(یا پهنای باند یا تعداد پرش و یا هزینه) لحاظ می گردد .لذا تمام ترافیک ها به کوتاهترین مسیر مسیر یابی می شوند .حتی اگر مسیر های دیگری نیز وجود داشته باشند ،مادامی که کوتاهترین مسیر نباشند مورد استفاده قرار نخواهند گرفت. باید توجه شود که کوتاهترین مسیر در اینجا لزوما به معنی مسیری با کوتاهترین فاصله فیزیکی نمی باشد . مثلا ممکن است به معنی مسیری با حداقل هزینه یا کمترین تعداد پرش ها باشد.عیب عمده این طرح این است که موجب ازدحام در برخی لینک ها می شود در حالیکه برخی از لینک های دیگر کاملا و یا حتی اصلا مورد استفاده قرار نگرفته اند واین همان مشکلی است که مهندسی ترافیک برای حل آن بکار گرفته می شود.عیب دیگر آن این است که مسیر یابی بهترین تلاش فعلی ، وقتی که مسیر بهتری یافت شود ، ترافیک را به آن منتقل می نماید، حتی اگر مسیر فعلی نیز نیازهای کیفیت سرویس آن ترافیک را تامین کند . این امر سبب ناپایداری در مسیر یابی می گردد .چرا که چنین شاخص هایی به سرعت تغییر می کنندو باعث می شوند که ترافیک دائما

به عقب برگردد وبه مسیردیگری ارسال شود.در بدترین حالت،این ناپایداری می تواند تاخیر و تغییرات تاخیر را به شدت افزایش دهد.مسیریابی مبتنی بر کیفیت سرویس برای رفع این معایب طراحی شده است که اهداف عمده آن عبارتند:تامین نیازهای کیفیت سرویس کاربر پایانی،یافتن مسیری که نیازهای پهنای باند ،تاخیر،تغییرات تاخیر ،احتمال از دست دادن بسته و .... کاربر را تامین نمایدو بهینه سازی در استفاده از منابع شبکه .مسیر یابی مبتنی بر کیفیت سرویس بایدترافیک را به گونه ای مسیر یابی وجهت دهی کند که بتواند میزان گذردهی کلی شبکه را به حداکثر برساند .یافتن کوتاهترین مسیر به این مسئله کمک می کند زیرا که مسیر طولانی تر ،منابع بیشتری از شبکه را مصرف می نماید.مسیر یابی مبتنی بر کیفیت سرویس باید به خصوص در حالتی که حجم بار ترافیکی سنگین است، کارایی بهتری را نسبت به مسیر یابی بهترین تلاش از خود نشان دهد(مثلا میزان گذردهی بهتری داشته باشد.)

## 3-3پروتکل LINK STATEوOSPF :

الگوریتم مسیریابی که ما به کمک آن این بهبود را نشان می دهیم ،پروتکل مسیریابی OSPF مـی باشـد، که پروتکل مسیر یابی گسترش یافته ای در اینترنت می باشد به طوری که هم اکنون OSPF نسخه 3 در آسـتانه ورود به اینترنت می باشد. OSPF یک ساختاری بهینه از پروتکل مسیر یابی وضعیت لینک (LINK STATE) می باشد.در شبیه ساز شبکه نسخه2 (NS-2) هم اکنون یک پیاده سازی از پروتکل OSPF بـا نـام LINK STATE ROUTING موجود می باشد . ساختار اصلی OSPF همان LINK STATE( وضعیت لینک)می باشـد. وضـعیت لینک بلوک هایی هستند که جهت کامل کردن نقشه توپولوژی شبکه که توسط هر نـود درشـبکه نگهـداری مـی شوند . این نقشه توسط پایگاه داده وضعیت لینک نمایش داده می شوند جهـت توزیـع ایـن پایگـاه داده هـر نـود ضرورتا هزینه تمام اتصالات خود را بدست می آورد و سپس این اطلاعات را به همسایگان خود ارسال می نمایـد . معمولا این هزینه یا مقداری است که مدیر شبکه با تناسبات مالی بدان اتصال اختصـاص مـی دهـد و یـا معمـولا تاخیر آن لینک را به عنوان هزینه آن در نظر می گیریم .اطلاعات ارسالی به همسایگان از طریق بسته های اعـلان وضعیت لینـک (LSA)LINK STATE ADVERTISEMENT و بـه کمـک پروتکـل طوفـانی (FLOODING PROTOCOL) صورت می پذیرد .نود دریافت کننده برای هر LSA آن را تکرار و به همه خروجی های خـود بـه جز خروجی نودی که LSA را از طریق آن در یافت کرده است ، ارسال می نماید . پروتکل OSPF برای محاسـبه کوتاهترین مسیر ممکن براساس هزینه تمام لینک ها ازالگوریتم دایجسترا DIJKSTRA بهره می گیرد

.

## 3-4سیستم فازي پیشنهادي:

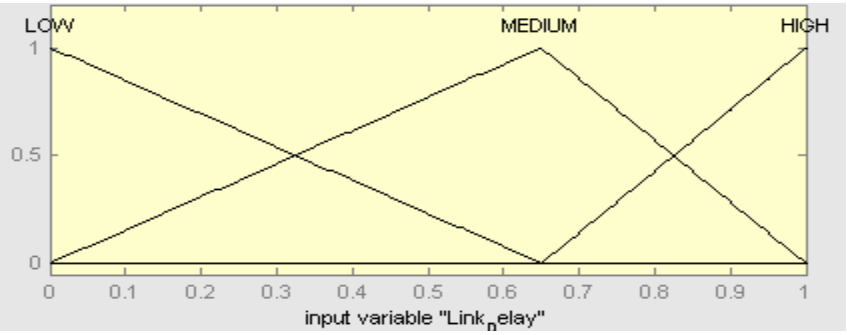
تاخیر، تغییرات تاخیر ، صف بندی ، پهنای باند و احتمال از بین رفتن بسته ها و .... از میـان پارامترهـای شبکه جهت استفاده در محاسبه یک پارامترتنها ، در مسیریابی شبکه ای بیشتر مورد اسـتفاده قـرار مـی گیرنـد . امکان استفاده از تمامی این پارامترها نیزهست اما نه تنها از نظر محاسباتی زمان زیـادی از دسـت خواهـد رفـت ، بلکه افزونگی اطلاعات بین این چند پارامتر وجود دارد که نیازی به استفاده از آنهـا نیسـت. تـاخیر یـک پـارامتر حیاتی در مبحث کیفیت سرویس (QOS) برای اکثربرنامه های کاربردی مـی باشـد ، مخصوصـا در برنامـه هـای محاوره ای چرا که این برنامه ها به حداقل تاخیر جهت ارتباط مناسب با کاربران احتیـاج دارنـد . البتـه برخـی از برنامه های کاربردی مانند Voice over IP(VOIP) و video conferencing در یـک محدودخاصـی تـاخیر را مـی تواند تحمل نمایند . با در نظر گرفتن این شرایط ، تاخیر به عنوان نقطه شروعی از پارامترها ، پـارامتر مهمـی کـه باید در نظر گرفته شود . تاخیر یک پارامتر جمعی است یعنی تاخیر یک مسیر را می توان از مجموع تاخیر لینک های تشکیل دهنده آن مسیر بدست آورد . اما پایین بودن تـاخیر یـک مسـیر لزومـا بـه معنـای بهتـر بـودن آن مسیرنیست و به معنای این نیست که این مسیر لزوما پهنای باند بهتری داشته باشد و یا بهروری لینک پـایین تـر داشته باشد . تاخیر اندازه گیری شده معمولا به صورت میانگین می باشد یعنی دراتصال با تاخیر برابر لزوما دارای فراز و نشیب ترافیکی یکسانی نیستند . صرف نظراز این مطالب اگردر مواقعی یـک اتصـال دارای تـاخیر بیشـتری

باشد ممکن است بدلیل داشتن پهنای باند باقیمانده ی بیشتری نسبت به سایر اتصالات،از آن استفاد گردد . و آن لینک بهتری محسوب گردد .چرا که ممکن است آن تاخیرمربوط به یک قله ترافیکی باشد( در مدت زمان اندازه گیری تاخیر)در حالیکه سایر لینک ها در آن مدت زمان در دره ترافیکی خود بوده باشند . لذا دقیق نبودن تاخیر اندازه گیری شده ممکن است بصورت سلسله مراتبی در محاسبه مسیر بهینه نیزتاثیر گذار شود و مسیر صحیحی را محاسبه ننماییم . پس لازم جهت دقیق تر شدن معیار وزن دهی به لینک خاص از یک پارامتر دیگر جهت این امر استفاده نماییم به این منظور باید این پارامتر با (SINGLE) پارامتر تاخیر جهت تولید یک معیار توام اما تنها استفاده شود . متوسط طول صف و تاخیر در آن از مهمترین خصوصیات یک روتر در مرز ازدحام و درنتیجه از بین بردن بسته ها می باشد بطوریکه در لحظات قبل از رخداد ازدحام ، هم زمانی که صرف صف بندی می شود افزایش می یابد و هم طول صف) طول لحظه ای آن (به مقدار ماکزیمم طول صف نزدیک می گردد. ضمنا از بین رفتن بسته ها دقیقا زمانی رخ میدهد که صف مربوط به آن روتردچار شلوغی و سریزمی گردد بگونه ای که اگر یک لینک دارای تاخیر کمتر و طول صف کوتاهتر باشد دارای وزن کمتر می باشد یعنی از نظر الگوریتم مسیر یابی کیفیت سرویس لینک برجسته تر و بهتری خواهد بود. زمانی که بیش ازیک پارامتربرای وزن دهی به لینک ها وجود دارد راههای متفاوتی نیز برای ترکیب این 2 پارامترو تشکیل یک پارامتر منفرد جهت مقداردهی به آن لینک وجود دارد : از راههای ساده ای همچون از آنها ضرب ، می نیمم گرفتن تا محاسبات هوشمندانه از نوع حتی مصنوعی آن .اما آنچه که مهم است این است که این محاسبات والگوریتم باید ساده ، آسان و در حداقل زمان صورت پذیرد تا امکان استفاده و پیاده سازی آن به راحتی در یک پروتکل مسیر یابی وجود داشته باشد. سربار ناشی از پیاده سازی الگوریتم باید در حداقل امکان قرار بگیرد البته دقت معیار خروجی با آنچه که از آن پارامترهای اولیه انتظار داریم نیز نباید متفاوت باشد الگوریتم باید به گونه ای باشد تا برتری هایی نیز نسبت به تک تک ان پارامترها داشته باشد . لذا از میان روشهای موجود ، با استقبالی که امروزه از متدهای فازی (Fuzzy) صورت می پذیرد ، تصمیم گرفتم که این روش ترکیب در منطق فازی انجام گیرد و آن هم ترجیحا به خاطر سادگی روش آن در حل مسایل می باشد . چرا که در این روش ترکیب پرامترهای ورودی به سادگی و سهولت میباشد و قابل درک نیز هست و با کمک قوانین فازی به راحتی می توان پارامترها ی خروجی و نیز بازدهی را کنترل و تنظیم نمود که در مقایسه با سایر روشها بهتر عمل می نماید.

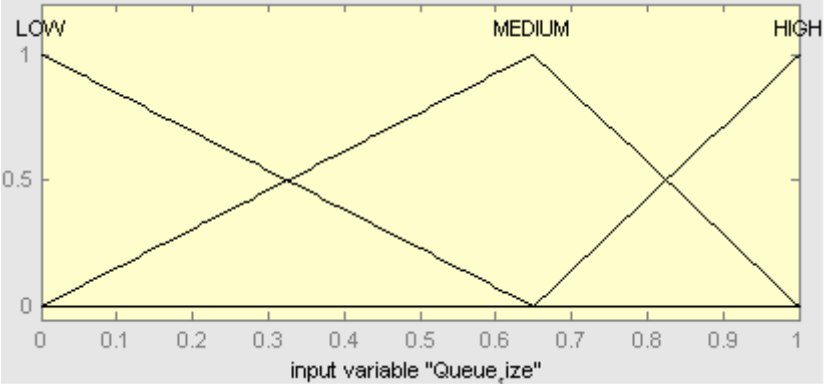
## 3-5توابع عضویت و بانک قوانین:

منطق فازی یک مجموعه خاص از منطق بولی است که جهت تبیین و توضیح مفهوم صحت جزئی و مقادیر بین دو کران" کاملا صحیح" و" کاملا غلط "توسعه داده شده است این منطق توسط آقای لطفی زاده در دهه 1960 میلادی معرفی گردید.استفاده از منطق فازی در بیان رفتار شبکه ، در حقیقت روشی است که در آن یک شخص است که رفتار لینک را و در کل رفتار کل مسیر را تعیین می کند،با این تفاوت که این تصمیم گیری بسیار سریع و در حقیقت با سرعت CPU انجام پذیر می شود. منطق فازی یک روش ساده مبتنی بر یک سری قوانین به فرم IF X AND Y THEN Z می باشد منطقی که در آن یک فرد ، درباره رفتار شبکه تصمیم می گیرد

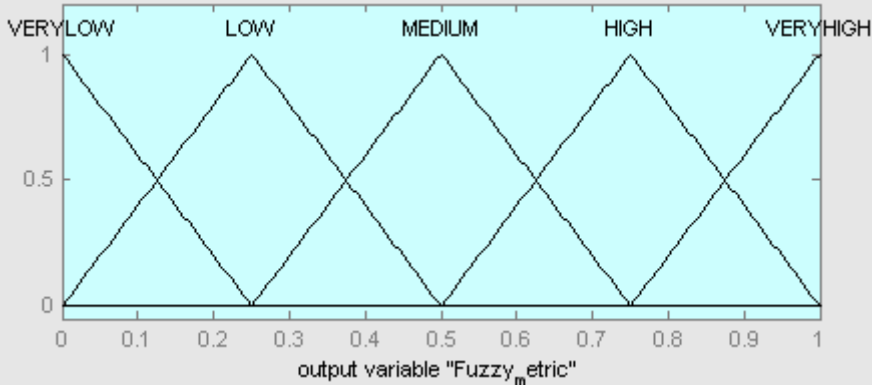
و به روشهای ریاضی و مدل کردن ریاضی ترجیح داده می شود،روشی مبتنی بر مشاهده و از روی تجربیات شـبکه است تا درک خصوصیات ترافیک. شکل1 چگونگی به کار گیری الگوریتم فازی را نمایش می دهد:



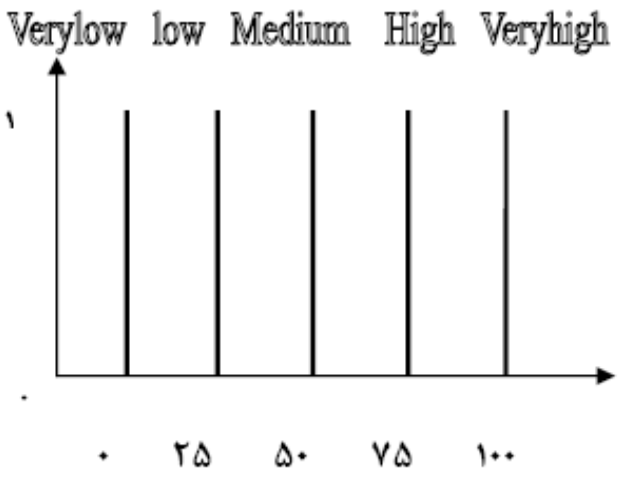

شکل3-1:نمودارتابع عضویت فازی ورودی تاخیر لینک




شکل :3-2نمودار تابع عضویت فازی ورودی اندازه صف




شکل:3-3 نمودار تابع عضویت فازی خروجی معیار فازی ( FM )




شکلD-۱ : غیرفازی ساز از نوع میانگین مراکز

ماتریس قوانین فازی را در شکل 2 ملاحظه مینمایید.

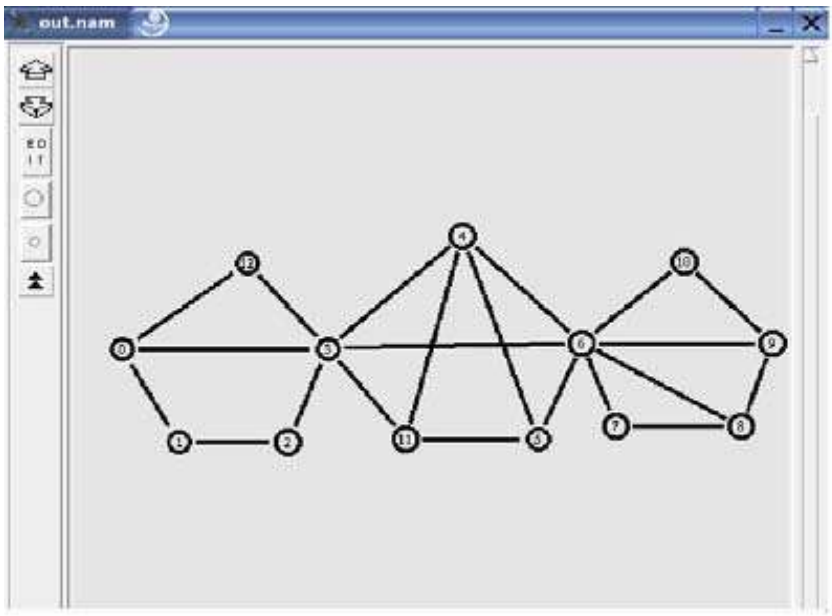
اندازه صف(QUEUE SIZE)

| تاخیر (Delay) | LOW | MEDIUM | HIGH |
|---|---|---|---|
| LOW | VERYLOW | LOW | MEDIUM |
| MEDIUM | LOW | MEDIUM | HIGH |
| HIGH | MEDIUM | HIGH | VERYHIGH |

شکل ۲ : ماتریس قوانین فازی

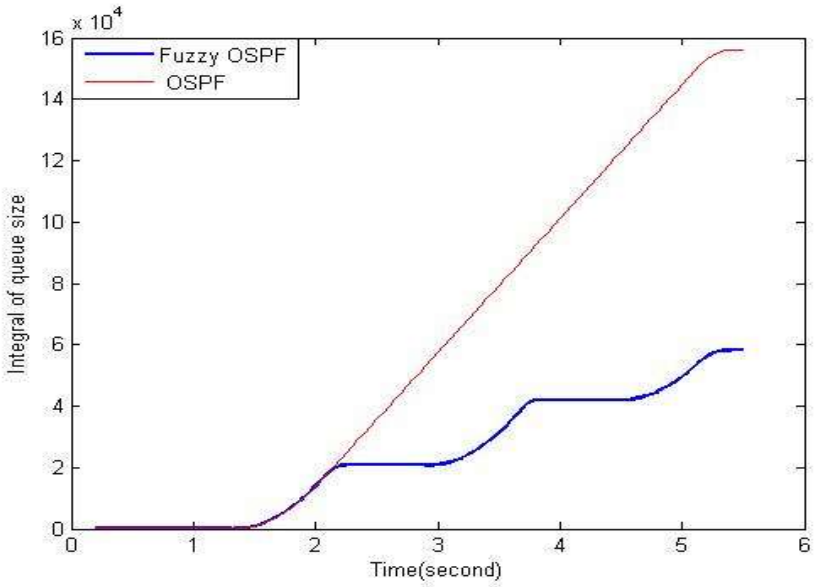
## 3-6شبیه سازی و ارزیابی عملکرد:

در این آزمایش از یک توپولوژی حلقه استفاده شد که در آن مبدا به مقصد بیش از یک مسیر وجود دارد .نمـایی از توپولوژی مورد استفاده در شکل 3 مشاهده می شود.

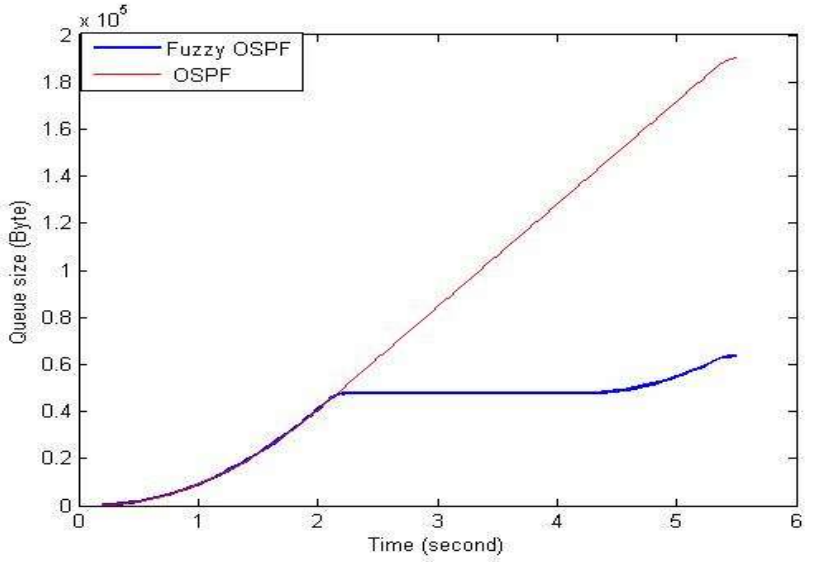



شکل3-4: توپولوژی مورد استفاده

در حالت نرمال OSPF با انتخاب مسیری با کمترین هزینه بـه مقصـد و ارسـال ترافیـک کـار خـود را بـه سرانجام می رساند از آنجاکه OSPF، پارامتر تاخیر(هزینه) را به تنهایی جهت تخمین هزینه استفاده مـی نمایـد ،اگر ترافیک ارسالی بیش از بافر طول صف نودهای میانی باشد وسرریز رخ دهد برایش تفاوتی احساس نمی شود و مقداری از بسته ها ممکن است بسته به شدت جریان از دست برود . اما در الگوریتم فازی با احساس افزایش تاخیر وافزایش طول صف روتر سعی در اختصاص وزن متناسب با آن به لینک متصل به روتر می نمایـد . لـذا بـا تغییـر مسیر از اتلاف بسته ها جلوگیری به عمل می آورد.اولین نموداری که بررسی شده است نمودارشـکل 4 اسـت کـه صحت عملکرد الگوریتم فازی راتایید می نماید. با مونیتور کردن لینکی در مسیراولیه در هنگام رخداد تغییر مسیر ملاحظه می شود که در نمودار آزمایش روش فازی، انتگرال)مجموع های جزئی( طول صف در مسیر سـابق ثابـت می ماند چرا که با تغییر مسیر، طول صف به سمت صفر میل می نماید و مقدار صفر با مقدار قبلی جمع می گردد و مجموع آن ثابت می ماند .در حالیکه در نمودار روش معمول OSPF ، به علت ادامه ازدحام بسته ها و آنکه طول صف همچنان در میزان حداکثر خود باقی مانده است لذا این مقدار ماکزیمم به مجمـوع قبلـی افـزوده و نمـودار مذکور به صعود خود ادامه خواهد داد. اولین رخداد این سناریو در لحظاتی پس از ثانیه دوم آزمایش می باشد.



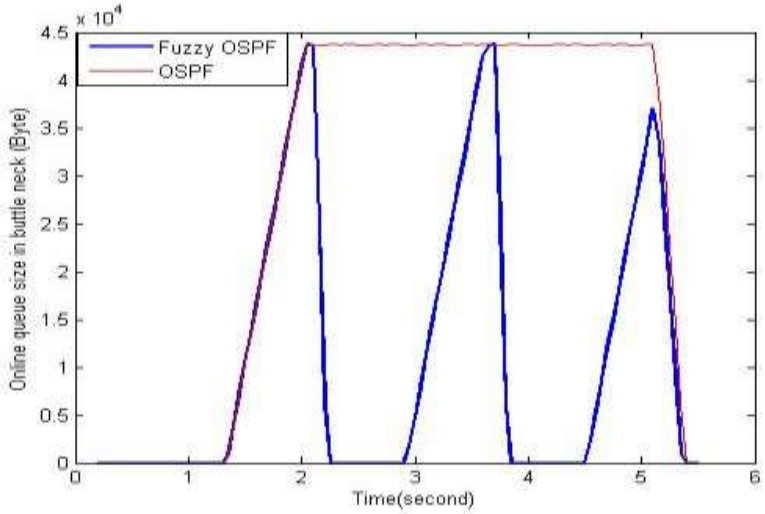

شکل 3-5: نمودار مجموع جزیی طول صف بر حسب Byte یک روتر میانی با منبع ترافیکی EXPONENTIAL با زمان on/off 5 ,3,0




شکل3-6: نمودار مجموع جزیی طول صف بر حسب Byte یک روتر میانی با منبع ترافیکیCBR با فاصله زمانی 0,005

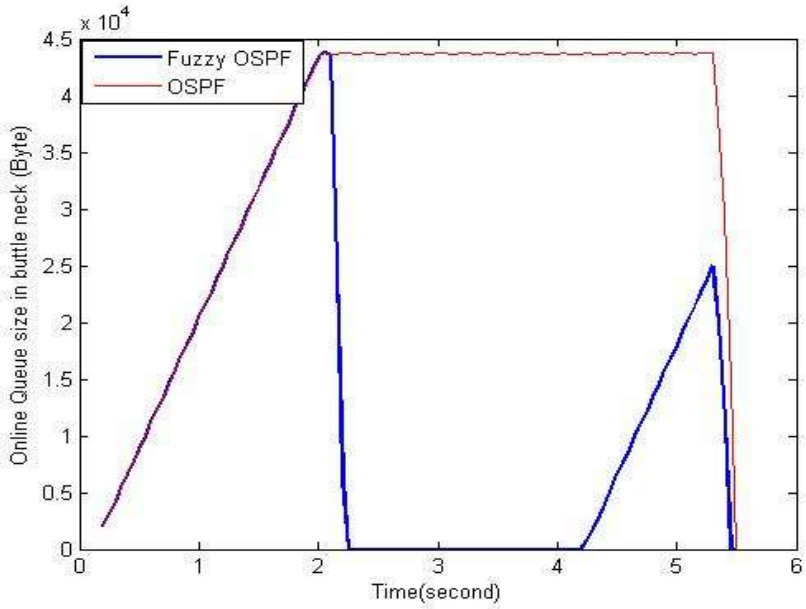
اگر باز به پارامتر طول صف پرداخته شود، با توجه به توضیحات فوق که چگونگی رخداد طول صف ماکزیمم قبل از رخداد حذف بسته مورد بررسی قرار گرفت ، نمودار شکل 5 حاصل می شود . دراین نمودارها طول لحظه به لحظه صف یک روتر میانی به نمایش گذاشته شده است . پس از رسیدن طول صف به مقدار ماکزیمم خود ( در حدود43و5) در روش مسیریابی فازی جریان ترافیکی ازKB مسیر دیگری ارسال می شود و لذا بار ورودی صف کاهش یافته و طول صف رو به افول می گذارد اما روش معمول با اصرار بر طی مسیر قبلی

باعث سر ریز صف روتر مذکور می گردد و بخاطر آن طول صف در بازه ای نزدیک به مقدار ماکزیمم نوسان می نماید.




شکل 3-7: نمودار طول لحظه ای صف بر حسب Byte یک روتر میانی

با منبع ترافیکی EXPONENTIAL با زمان on/off،0,5 ,3,0

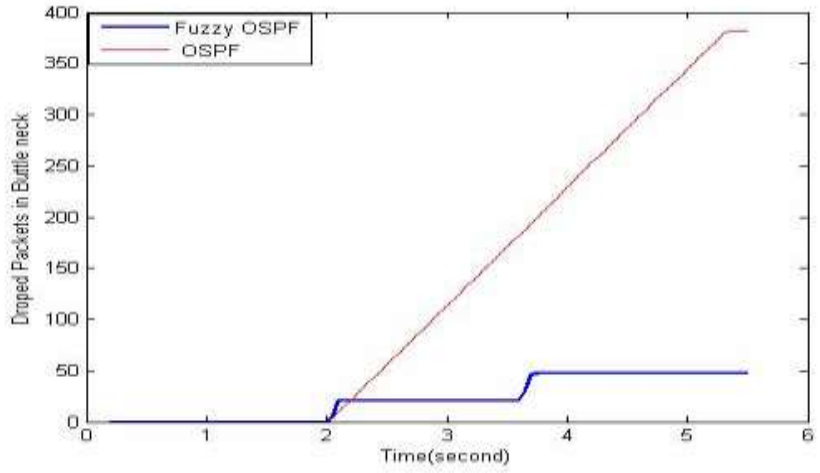



شکل 3-8: نمودار طول لحظه ای صف بر حسب Byte یک روتر میانی

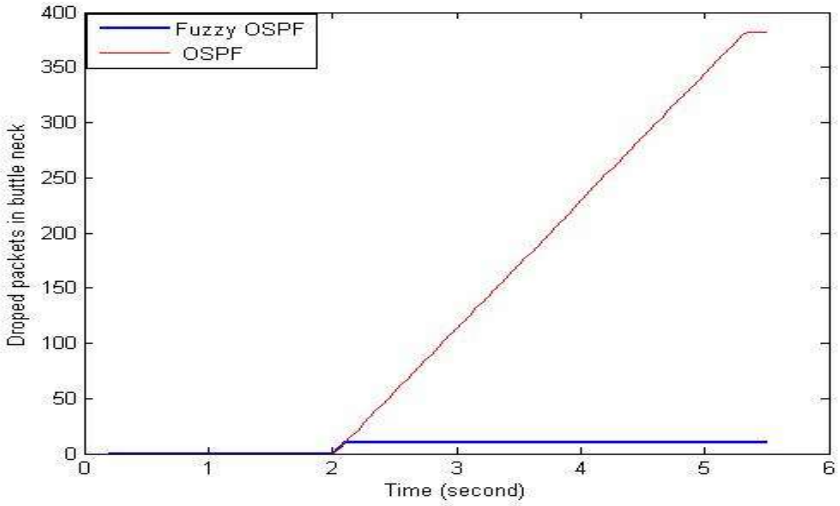
با منبع ترافیکی CBR با فاصله زمانی 0,005

در نمودار شکل 6 با عنوان تعداد بسته های حذف شده در لینکی از مسیر اولیه نیز مواردی یافت می شود که موید توضیحات قبلی است ، در روی نموادار در لحظاتی پس از ثانیه دوم آزمایش مشاهده می شود که در حالت نرمال در این لحظه که صف ظرفیت خود را تکمیل شده می بیند شروع به حذف بسته های تازه رسیده می نماید در حالیکه با کمی پیروی از این رویه ، در روش فازی چون مسیر ترافیکی تغییر یافته است ، لذا نمودار در یک مقدار ثابت در طول زمان به مسیر خود ادامه می دهد . زیرا ترافیکی جدید به این لینک وارد نمی شود پس از

ازدحام طول صف روتر تقلیل یافته و دیگر بسته ای حذف نمی شود . پس در این 2 نمودار اثبات می شود که الگوریتم روش فازی عملکردی بهتر در انتخاب مسیر در شبکه خواهد داشت.



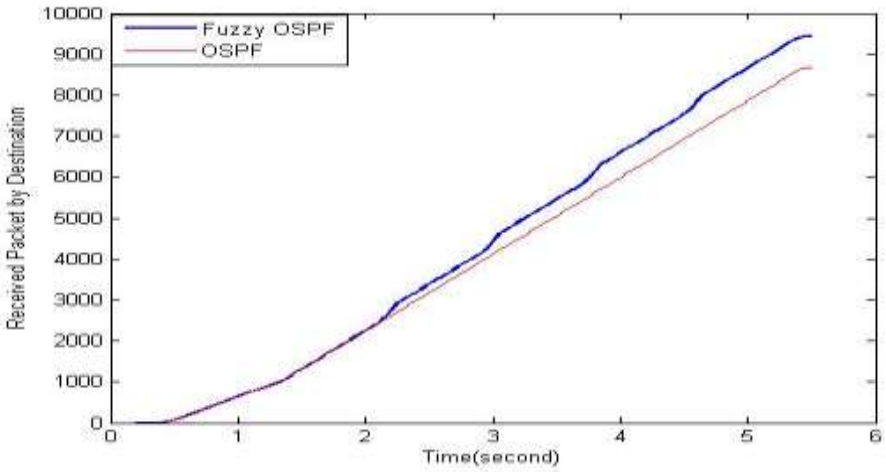

شکل 3-9: نمودار تعداد بسته های حذف شده در صف یک روترمیانی با منبع ترافیکی EXPONENTIAL با زمان on/off،0,5 ,3,0




شکل 3-10: نمودار تعداد بسته های حذف شده در صف یک روترمیانی با منبع ترافیکی CBR با فاصله زمانی0,005

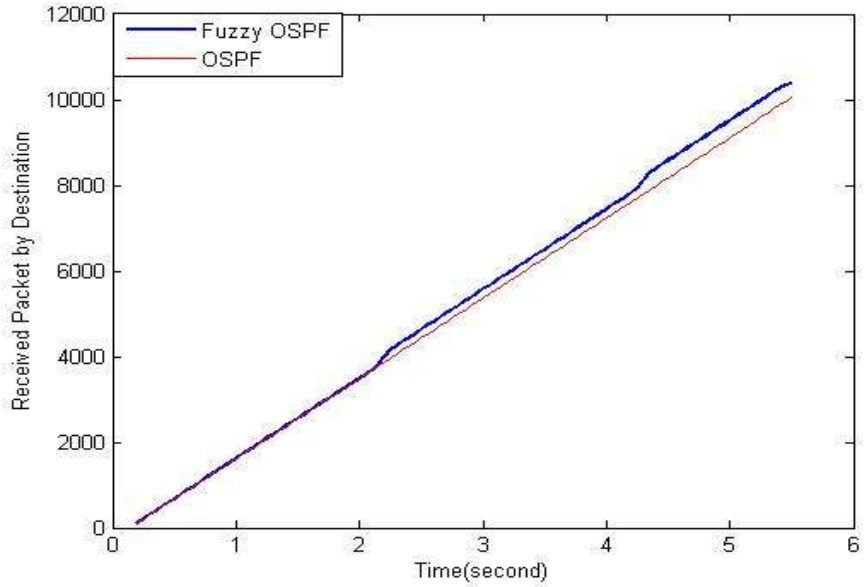
در نمودار شکل 7 حجم بسته های دریافتی در مقصد مشاهده می شود که در لحظاتی صعودهایی داشته است. علت آن است که در لحظه ای که به علت تراکم در صف روتر و افزایش تاخیر که منجر به حذف شدن بسته ها در مسیر اولیه می شود مسیر جدید برای ارسال ترافیک انتخاب می شود، مقداری از بسته ها ترافیکی که در روتر های میانی و بافرهای صف آنان باقی مانده است به مقصد ارسال می گردند وباعث افزایش حجم بسته های دریافتی مقصد می شود .پس می توان به تصریح کرد که این افزایش از نظر تداوم زمانی خود ، بسته به میزان

بافری است که در روترهای میانی برای صف ورودی اختصاص داده می شودو از نظـر مقـدار افـزایش بسـته هـای دریافتی به پهنای باند گلوگاه مسیر، وابسته خواهد بود.




شکل 3-11: نمودار تعداد بسته های دریافت شده در مقصد منبع ترافیکی

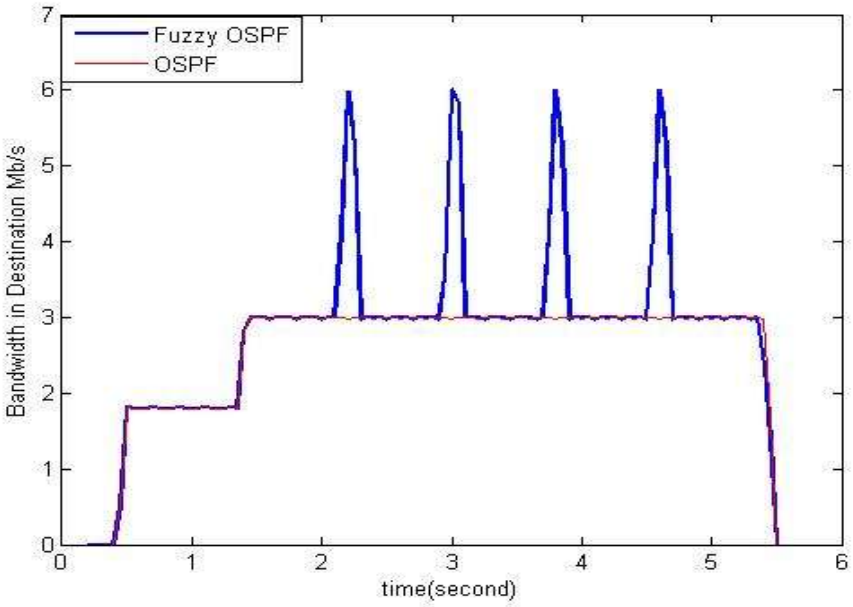
EXPONENTIAL با زمان on/off،0,5 ,3,0




شکل3-12: نمودار تعداد بسته های دریافت شده در مقصد منبع ترافیکی

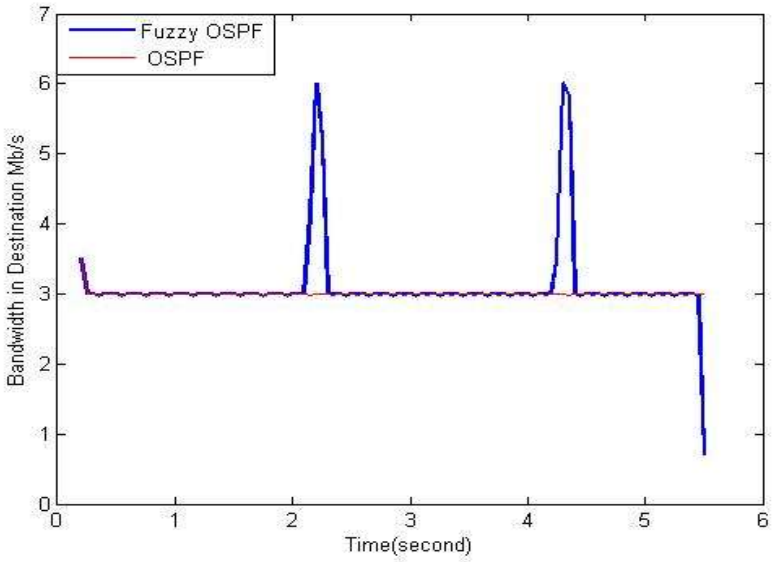
CBR با فاصله زمانی 0,005

با توجه به تعریف پهنای باند که میزان داده ای که در واحد زمان دریافت می شود نمودار پهنای بانـد نیـز از نظـر رفتاری مشابه نمودار حجم بسته های دریافتی است که در شکل8 مشاهده می شود .مقصد در لحظاتی تقریبـا 2 برابر متوسط پهنای باند لینک های متصل به خود ، پهنای باند در یافتی خواهد داشت.




شکل 3-13: نمودار پهنای باند دریافت شده در مقصد بر حسب Mb/s

منبع ترافیکی EXPONENTIAL با زمان on/off،0,5 ,3,0

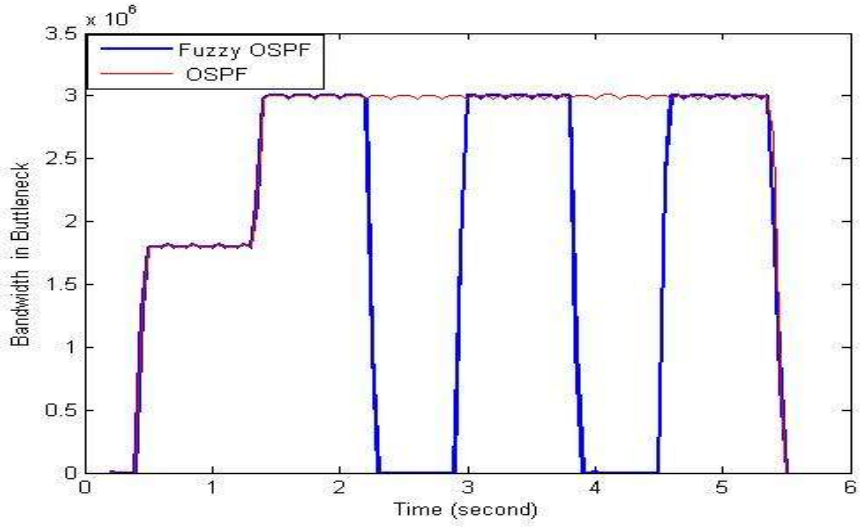



شکل 3-14: نمودار پهنای باند دریافت شده در مقصد بر حسب Mb/s

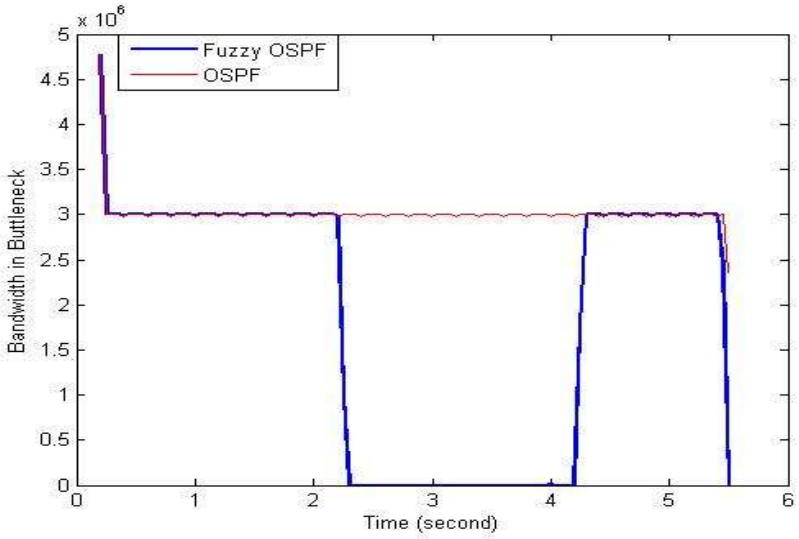
منبع ترافیکیCBR با فاصله زمانی0,005

درنمودارشکل 9 تحت عنوان پهنای باند لینک گلوگاه مسیر از آنجا کـه در ایـن سـناریو جریـان ترافیکـی جهت رخداد سرریز صف به نحوی تنظیم گردیده است که از حداکثر ظرفیت لینک بهربـرداری نمایـد ، نمیتـوان روش معمول را بر فازی صاحب برتری دانست . چرا که هرچندOSPF در لحظاتی روش فازی پهنای باند کمتـری را ارائه نموده است اما حقیقت آن است که در این زمان الگوریتم فازی از مسیر مستقل دیگری بسته های ترافیکی خود را به آدرس مقصد نهایی ارسال نموده و با محسوب کردن مقدار هر چند کم پهنای بانـد ایـن نمـودار ، روش

فازی در مجموع پهنای باند مطلوبتری را در مقصد به کاربر ارائه می نماید که در نمودار شکل 8 بـه ایـن موضـوع پرداخته شده است.



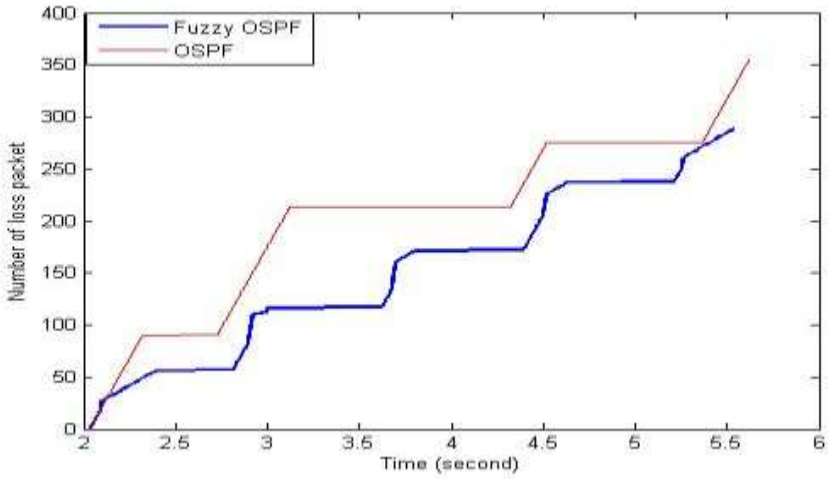

شکل3-15: نمودار پهنای باند لینکی میانی بر حسب Mb/s منبع ترافیکی EXPONENTIALبا زمان 0,5 ,3,0 on/off




شکل3-16: نمودار پهنای باند لینکی میانی بر حسب Mb/s

منبع ترافیکی CBR با فاصله زمانی 0,005

مهمترین نتیجه و نمودار حاصل از این روش که تفاوت معناداری را در مقایسه با روش معمـول مسـیریابی در ایجاد نموده است در شکل 10 ملاحظه می شود.OSPF مطلبی که در این نمودار بر آن تاکید شده است ، تعداد کل بسته هایی است که در طول سناریو حذف شده اند . برتری مسیریابی فازی ارائه شده روشن است و علـت آن تغییر مسیری است که الگوریتم فازی با افزایش طول صف و تاخیر در روترهای مسیر اولیه بر روند ارسال ترافیـک به مقصد به OSPF نهایی اعمال می نماید . اما روش مرسومی که کمک آن مسیریابی را انجام می دهـد قـادر بـه تشخیص دقیق وضعیت از بین رفتن بسته ها در روترهای میانی نبوده و معمولا اصرار بر پیمودن مسیر اولیه دارند .




شکل 3-17: نمودار تعداد کل بسته های حذف شده در شبکه منبع ترافیکی EXPONENTIAL با زمان on/off،0,5 ,3,0

# فصل چهارم
# مسير يابي چند منظوره

## 4-1مسير يابي چند منظوره:

در دنیای مسیر یابی IP می تران با تهیه کپی از یک بسته در طول راه،توسط مسیر یاب ها،آن را برای چندین دریافت کننده ارسال نمود.این فرآیند چند منظوره سازی(Multicasting) نام دارد.

در مسیر یابی IP تک منظوره،آدرس IP مقصد یکی از آدرس های کلاس C،B، A می باشد که یک میزبان مشخص را در اینترنت نشان می دهد.نقش پروتکل های مسیر یابی IP تک منظوره،مسیر یابی بسته های IP از یک مبدا ویژه IP به یک مقصد ویژه IP می باشد.فرض کنید که می خواهید چندین میزبان،بسته های IP را از یک میزبان دریافت کند.اگر کامپیوتر مبدا از آدرس IP تک منظوره میزبانان مقصد استفاده کند،باید یک بسته را برای هر یک از میزبانان مقصد ارسال کند.با افزایش تعداد میزبانان مقصد،تعداد بسته های IP تک منظوره ای که باید توسط مبدا ارسال شوند نیز افزایش می یابد و مدت زمان زیادی برای مبدا و شبکه طول می کشدتا این تعداد بسته معین را از مبدا به سمت هر یک از میزبانان مسیر یابی کنند.مشکل دیگر،تعیین این نکته است که مبدا چند منظوره (Multicast) چگونه آدس میزبانان خواستار دریافت بسته را مشخص می سازد.آدرس های چند منظوره جادویی،کلاس دیگری از آدرس های IP هستند و زمانی مورد استفاده قرار می گیرندکه بیش از یک دریافت کننده برای اطلاعات ارسالی از مبدا وجود داشته باشد.در واقع (Multicasting) یک راه حل مناسب جهت برقراری ارتباط با چندین میزبان می باشد.

## 4-2انتخاب مسیر چند منظوره:

بسته های IP تک منظوره با استفاده از آدرس سخت افزاری به میزبان منتقل می شوند.این آدرس سخت افزاری اساساً یک آدرس اترنت است.زمانی که یک مسیریاب بسته ای دریافت می کند،آدرس سخت افزاری را از آن جدا می کند و آدرس IP مقصد را جهت رابط مورد استفاده برای ارسال بسته به سمت میزبان بررسی مینماید.اگر مسیر یاب به شبکه در بر گیرنده میزبان متصل باشد،از پروتکل تجزیه و تحلیل آدرس ( Adderss Resolution Protocol-ARP) جهت درخواست آدرس اترنت میزبان دارای آدرس IP مقصد ذکر شده در بسته استفاده می کند.مسیر یاب،آدرس اترنت میزبان را به بسته اضافه کرده و آن را به سوئیچ ارسال می نماید.سوئیچ،یک جدول انتخاب مسیر دارد که شامل فهرستی از آدرس های اترنت است.این آدرس ها،به طور مستقیم میزبان و درگاه (port) سوئیچ را به یکدیگر متصل کرده اند.

جفت کردن آدرس های اترنت و IP میزبان،در IPهای تک منظوره صورت می گیرد.هر میزبان دارای یک IP تک منظوره منحصر به فرد و یک آدرس اترنت است و این جفت کردن در انتقال بسته های چند منظوره ممکن نیست،زیرا ممکن است چندین میزبان بر روی همان شبکه نیازمند دریافت بسته های چند منظوره یکسانی باشد.این بدین معنی است که آنها با همان آدرس گروهی مقصد چند منظوره به بسته های IP گوش می دهند.بنابراین،میزبانان دریافت کننده آدرس اترنت چند منظوره نیاز دارند که بوسیله مسیریاب برای انتقال بسته های IP چند منظوره به چندین میزبان استفاده می شود.

برای تعیین آدرس اترنت چند منظوره برای آدرس IP چند منظوره ،ابتدا IP مبنای 10 نقطه دار را به مبنای 16 و سپس مبنای 2 تبدیل نمایید.23 بیت آخر آدرس IP چند منظوره را به آدرس مبنای اترنت 00 00 00 01 5 E اضافه کنید ،این آدرسی است که مسیر یاب و سوئیچ جهت انتقال بسته های چند منظوره به یک میزبان از آن استفاده می کنند.

یک سوئیچ از طریق ملاحظه بسته های ارسالی توسط میزبانان،آدرس های اترنت میزبان های متصل را شناسایی می کنند.زمانی که سوئیچ یک پیام اترنت را از یک میزبان دریافت می کند،پیام بر روی یک درگاه خاص دریافت می شود.سوئیچ به آدرس اترنت مبدا نگاه کرده و آدرس اترنت میزبان متصل به آن درگاه را شناسایی می کند.از طرفی،سوئیچ تمام آدرس های اترنت تک منظوره میزبان متصل را می داند.در Multi casting متفاوت است،چرا که میزبانان بسته های چند منظوره را دریافت می کنند اما آنها را منتقل نمی سازند.سوئیچ چطور متوجه می شود که یک میزبان خواستار دریافت بسته چند منظوره از یک مبدا خاص است؟پاسخ در استفاده از پروتکل مدیریت گروهی اینترنت Internet Group Management Protocol(IGMP) است.

## 4-3پروتکل IGMP:

پروتکل مدیریت گروهی اینترنت بین میزبانان و مسیریابهای محلی آنها جهت ایجاد مسیریاب گروه های چند منظوره ای که باید بر روی شبکه محلی ارسال شوند،بکار می رود.

مسیر یاب ،گروه چند منظوره (Multicast Group) را به فهرست گروه هایی که باید بر روی شبکه محلی ارسال شوند اضفه می نماید.مسیریاب ها رابطه خود را با تمام میزبانان خواستار دریافت بسته از گروه های چند منظوره حفظ نمی کنند.برای یک مسیریاب دانستن اینکه حداقل یک میزبان خواستار دریافت بسته است،کفایت می کند.زمانی که میزبان دیگر متقاضی دریافت بسته چند منظوره نباشد،پیام ترک IGMP به مسیریاب ارسال می شود.مسیر یاب از میزبانان شبکه محلی سوال می کند که آیا هنوز متقاضی وجود دارد یا خیر.اگر هیچ متقاضی جهت دریافت بسته چند منظوره وجود نداشته باشد،کسیر یاب گروه را غاز فهرست گروه های ارسالی حذف می کند.

IGMP بین میزبانان و مسیریاب ها استفاده می شود و سوئیچ تنها برای انتقال بسته بین مسیریاب ها و میزبانان بکار می رود.زمانی که مسیر یاب یک بسته چند منظوره را دریافت می کند،اگر میزبان ها به آن گروه چند منظوره بخصوص پیوسته باشند،مسیریاب بسته را را به سوئیچ ارسال می نماید.سوئیچ با آن بسته مانند یک بسته انتشاری (Broadcast Packet) رفتار می کند و آن را به تمام میزبانان متصل به خود ارسال می دارد.

انتشار (Broadcasting) بسته چند منظوره،استفاده مناسبی از پهنای باند (Bandwidth) مورد استفاده نمی باشد.بهمین منظور،دو پروتکل مورد استفاده قرار می گیرند تا سوئیچ بسته چند منظوره را به میزبانان عضو گروه چند منظوره ارسال نماید:

- پروتکل مدیریت گروهی سیسکو (Cisco Group Management Protocol)
- جستجوی IGMP (IGMP Snooping)

پروتکل IGMP سه ورژن دارد.

## 4-4پروتکل CGMP:

Cgmp یک پروتکل اختصاصی سیسکو است که بین مسیریاب ها و سوئیچ های سیسکو از آن استفاده می شود.

اگر CGMP بر روی مسیریاب و سوئیچ تنظیم شده باشد ،زمانی که میطبان به گروه چند منظوره بخصوص می پیوندد،مسیریاب ها با استفاده از CGMP سوئیچ را مطلع می سازند.مسیریاب آدرس اترنت تک منظوره میزبان را می داند زیرا آدرس در بسته IGMP ارسالی به مسیریاب وجود دارد.مسیریاب آدرس اترنت تک منظوره میزبان و گروه چند منظوره ای را که میزبان به آن پیوسته است به اطلاع سوئیچ می رساند.آدرس اترنت چند منظوره در جدول انتخاب ثبت می شود.زمانی که مسیریاب بسته چند منظوره را به سوئیچ ارسال می کند ،سوئیچ بسته را به میزبانانی که دارای آدرس اترنت چند منظوره در جدول انتخاب مسیر هستند، می فرستد.این روش از ارسال بسته ها های چند منظوره به میزبانانی که عضو گروه نیستند ،جلوگیری می نماید.زمانی که میزبانان ،دیگر متقاضی دریافت بسته ها از آن گروه خاص نباشد،یک پیام ترک IGMP به

مسیریاب ارسال میکنند.مسیریاب با استفاده از IGMP به سوئیچ اطلاع می دهد که این گروه چند منظـوره را در جدول انتخاب مسیر برای آن میزبان حذف نماید.

## 5-4جستجوي IGMP:

جستجوی IGMP (IGMP Snooping) پروتکلی استاندارد است که همـان وظـایف CGMP را بـر عهـده دارد.زمانی که جستجوی IGMP بر روی سوئیچ فعال باشد،سوئیچ بسته های IGMP ارسالی به مسـیریاب هـای محلی را زیر نظر می گیرد.زمانی که میزبان با استفاده ازIGMP به یک گروه چند منظـوره مـی پیونـدد،سـوئیچ آدرس اترنت چند منظوره (Multicast ) را برای آن میزبان در جدول انتخاب مسیر اضافه می کنـد و زمـانی کـه میزبان گروه را ترک کند،سوئیچ ورودی چند منظوره را از جدول انتخاب مسیر حذف خواهد کرد.

ارسال چند منظوره:

بسته های IP تک منظوره براساس آدرس IP مقصد مسیریابی می شـوند.اما یـک بسـته چنـد منظـوره را نمی توان با استفاده از آدرس IP مقصد مسیریابی کرد،چرا که چندین مقصد برای آن وجود دارد.نحوه ی مسـیر یابی ،بستگی به تعداد میزبانان متقاضی دریافت بسته چند منظوره دارد. ارسال چند منظوره بر اسـاس آدرس IP مبدا با استفاده از روشی به نام برگشت مسیر ارسال (Reverse Path Forwarding-RPF) صورت می گیرد.

استفاده از روش RPF،یک درخچه انتقال (Delivery Tree) بدون حلقه،بر اساس مبدا و کوتاهترین مسیر ایجـاد می کند.

درخچه انتقال بر پایه مبدا،یک موقعیت مکانی بدون حلقه (Loop-Free) است از مبدا چند منظوره به سمت هـر مسیریاب انشعابی.یک مسیریاب انشعابی (Leaf Router) مسیر یابی است که به طور مستقیم بـه میزبانـان عضـو گروه چند منظوره متصل است.با توجه به پروتکـل مسـیریابی IP تـک منظـوره ای کـه در شـبکه اسـتفاده مـی شود،موقعیت مکانی درخچه ممکن است متفاوت باشد وبا توجه به اینکه پروتکل هـای مسـیریاب IP از متریـک های متفاوتی استفاده می کنند،مسیر برگشت به سمت مبدا ممکن است دچار تغییر شود.به عنوان مثـال RIP از جهش شمار(Hop Count) استفاده می کند در حالیکه OSPF از متریکـی بـر مبنـای سـرعت را بـط بهـره مـی گیرد.این موضوع نشان می دهد که می توانید برای پروتکل هـای مسـیریابی IP درخچـه هـای متفـاوتی داشـته باشید.

## 6-4پروتکل مستقل مسیریابي چند منظوره:

سیسکو از پروتکل چند منظوره مستقل (Protocol Independent Multicast-PIM) بعنوان یک پروتکـل مسیریابی چند منظوره استفاده می کند.عدم وابستگی به این پروتکل به این معنی است که شما در انتخاب یـک پروتکل مسیر یاب IP تک منظوره مانند RIP،IGRP،EIGRP،OSPF،IS-IS بعنوان پروتکـل مسـیریابی ورودی داخلی خود آزاد هستید.رابط RPF از روی جدول مسیریابی IP تک منظوره تعیین شده و جدول مسیریابی IP از پروتکل مسیریابی IP بوجود می آید.

دو نوع PIM وجود دارد سبک متراکم (Dense Mode) وسبک پراکنده (Sparse Mode).

## PIM7-4 سبک متراکم:

پروتکل چند منظوره مستقل سبک متراکم ( Protocol Independent Multicast Dense Mode-PIM DM) یک پروتکل مسیر یابی چند منظوره، انتشاری( Broadcast) و آراسته است که از درخچه های انتقال بر اساس مبدا استفاده می کند.PIM DM تمام همسایگان PIM را متقاضی دریافت تمام بسته های چند منظوره دریافتی بوسیله مسیریاب فرض مینماید.اگر یک مسیریاب انشعابی (Leaf Router)،میزبان متقاضی دریافت بسته چند منظوره از یک گروه چند منظوره خاص نداشته باشد،مسیریاب انشعابی یک پیام هرس (Prune) به مسیریاب فرستنده ارسال و تقاضا می کند که آن مسیریاب بسته های آن گروه را ارسال نکند.هرس (Prune) دارای طول عمری در حدود 3 دقیقه است، 3دقیقه بعد از زمانی که بسته چند منظوره دوباره به سمت مسیریاب های انشعابی ارسال می شود.

سه گامی که برای انجام پیکربندی مسیریاب جهت مسیریابی چند منظوره باید برداشته شود عبارتند از:

- پیکربندی پروتکل مسیریابی تک منظوره
- فعال سازی مسیریابی چند منظوره
- فعال سازی رابط ها برای Multicast

ابتدا باید مسیریابی داخلی را پیکربندی کنیم، برای ایجاد جدول مسیریابی IP تک منظوره، که پردازش RPF از آن استفاده می کند.

بعد از اینکه OSPF تنظیم شد و جدول مسیریابی IP تک منظوره ساخته شد، پیکربندی PIM DM آسان است.بر روی هر مسیریاب با دستور ip multicast-routing مسیریابی چند منظوره را فعال کنید. حال بر روی هر رابط PIM DM را فعال کنید با درستور ip pim dense-mode . حالا PIM DM بر روی شبکه تنظیم شده است. همسایه ها با استفاده از دستور show ip pim neighbor ، بررسی می شوند.

PIM DM از درخچه انتقال بر اساس مبدا (Source-Based) ، از هر مبدا چند منظوره به هر میزبانی که عضو گروه چند منظوره باشد، استفاده می کند. بنابراین، هر مسیریاب PIM DM بهمراه درخچه انتقال ، برای هر مبدا و گروهی یک موقعیت ایجاد می کند.

مسیریاب های چند منظوره PIM DM ، اطلاعات مربوط به هر مبدا و هر گروه چند منظوره ای را که یک میزبان عضو آن باشد، نگهداری می کند.علاوه براین مسیریاب های PIM DM، بسته های چند منظوره را چه همسایه متقاضی آن باشد یا نباشد، به همسایگان PIM DM ارسال می کنند.

## PIM8-4 سبک پراکنده:

در سبک پراکنده PIM (PIM Sparse Mode-PIM SM) از درخچه های انتقال اشتراکی ( Shared Delivery Tree) به جای درخچه های بر اساس مبدا (Source-Based Tree) استفاده می شود.در درخچه های انتقال اشتراکی ، یک بسته چند منظوره به یک نقطه مشترک به نام نقطه تلاقی (Rendezvous Point-RP) فرستاده می شود.RP، بسته را به میزبانان عضو گروه می فرستد.در این روش مسیریاب ها تنها اطلاعات مربوط به گروه های چند منظوره را نگهداری میکنند ونیازی به نگهداری اطلاعات منابع ندارد.در نتیجه در حجم یادگیری بر روی مسیریاب کم خواهد شد.

استفاده از درخچه انتقال اشتراکی به این معنی است که از کوتاهترین مسیر از هر مبدا به سمت هر دریافت کننده استفاده نمی شود، چرا که بسته ابتدا به RP ارسال می شود.کوتهترین مسیر از RP به دریافت کننده در نظر گرفته می شود.

چهار روش پیکربندی PIM SM بر روی مسیریاب های سیکو عبارتند از:

- RP ایستا(Static RP)
- RP خودکار(Auto RP)
- PIM SM نسخه دو
- RP همه منظوره (Anycast RP)

## RP9-4 ثابت (Static RP):

در RP ثابت یک مسیریاب بعنوان RP برای شبکه انتخاب شده است و تمام مسیریاب های چند منظوره با آدرس IP مربوط به RP تنظیم می شوند.زمانی که یک مسیریاب انشعابی (Leaf Router)، پیام پیوند (IGMP ) را برای گروه چند منظوره دریافت میکند ، یک پیام پیوند به RP می فرستد تا یک مسیر چند منظوره از RP به سمت مسیریاب انشعابی ساخته شود.

مسیریابی که دارای اتصال مستقیم با مبدا چند منظوره است ، بسته چند منظوره را از مبدا دریافت می کند و این بسته را در یک پیام ثبتی (Register Message) به RP ارسال مینماید.پیام ثبتی با استفاده از IP تک منظوره (Unicast) ارسال می شود و این پیام یک مسیر چند منظوره از مسیریاب متصل به مبدا به سمت RP می سازد.بعد از ایجاد مسیر ، RP یک پیام توقف ثبت برای مسیریاب ارسال میکند و مسیریاب ارسال بسته ها را از طریق تک منظوره متوقف کرده و شروع به ارسال آنها از طریق چند منظوره می نماید .در این روش هر مبدا ، ادارای یک کوتا ترین مسیر به سمت RP است و RP هم دارای یک کوتاهترین مسیر به سمت هر یک از دریافت کننده ها می باشد.

در تمام مسیریاب ها ،باید چند منظوره سازی IP فعال بوده و همچنین یک پروتکل مسیریابی داخلی تنظیم شده باشد.در سبک پراکنده (Sparse Mode) هر رابط از طریق دستور ip pim sparse-mode تنظیم می شود.

محدودیت استفاده از RP ثابت این است که در این حالت تنها یک RP وجود دارد.اگر RP از بین برود، سبک پراکنده دیگر عملی نخواهد بود.سایر روش های تنظیم چند منظوره سازی سبک پراکنده که بر این محدودیت غلبه می کنند، عبارتند از:Auto-RP،PIM SM نسخه 2 ، Anycast RP.

## :Auto-RP10-4

Auto-RP–میتوان چندین RP تنظیم کرد و هر RP می تواند برای تمام فضای آدرس چند منظوره و یا زیر مجموعه ای از آن ایفای نقش نماید.RPها خود را بعنوان یک RP داوطلب معرفی کرده و شامل دامنه آدرس های چند منظوره ای می شوند که برای آنها اعلام آمادگی نموده اند.ایستگاه (Entity) دیگری که مسئول نقشه برداری (Mapping Agent-MA) نام دارد، اطلاعیه داوطلبی را از RP داوطلب دریافت کرده است و تعیین می کند که کدام RP برای تمام و یا قسمتی از آدرس های چند منظوره فعالیت خواهد کرد.اگر چندین نقشه برداری (MA) وجود داشته باشند، یکی از آنها به عنوان MA فعال انتخاب خواهد شد.داشتن چندین RP و MAدر یک شبکه منجر به افزایش افزونگی (Redundancy) خواهد شد.

در تمام مسیریاب ها باید IP چند منظوره سازی فعال بوده و نیز یک پروتکل مسیریاب داخلی هم تنظیم شده باشد، در سبک پراکنده (Sparse Mode) هر رابط با استفاده از دستور ip pim sparse-dense-mode تنظیم می شود.Sparse-Dense به مسیریاب ها اجازه می دهد تا در صورت در دسترس نبودن RP از سبک متراکم (Dense Mode)استفاده کنند.

PIM SM نسخه 2:

PIM SM نسخه 2 شبیه Auto-RP است.یک یا چندین RP دوطلب تنظیم می شود.هر یک از RPهای داوطلب می توانند تمام فضای آدرس چند منظوره و یا زیر مجموعه ای از آن را پشتیبانی کنند.مسیریاب های خود راه انداز (Bootstrap Routers-BSRs) نقش MAها را در Auto-RP ایفا می کنند.خصوصیات یک BSR، مسیریاب انتخابی به عنوان BSR فعال را تعیین مینماید. اگر BSRهای داوطلب دارای خصوصیات یکسانی باشند،BSR دارای آدرس IP بالاتر به عنوان BSR فعال انتخاب خواهد شد.معمولا RPهای داوطلب و BSRها از آدرس IP رابط حلقه برگشتی خود برای تعیین هویت استفاده می کنند.

BSR فعال اعلامیه های RPها ی فعال را از RPها جمع آوری و گروه RPها را به مسیریاب های چند منظوره شبکه اعلام می نماید.مسیریاب های چند منظوره با استفاده از خصوصیات RP، RP مورد استفاده خود را انتخاب می کنند.

در تمام مسیریاب ها باید IP چند منظوره سازی فعال (IP Multicasting Enable) بوده و یک پروتکل مسیریابی داخلی نیز تنظیم شده باشد. در سبک پراکنده (Sparse Mode)، هر رابط با استفاده از دستور ip pim sparse-dense-mode تنظیم می شود. Sparse-Dense این اجازه را به مسیریاب ها می دهد، در زمانی که RP در دسترس نبود، از سبک متراکم (Dense Mode) استفاده کند.

### :Anycast- RP11-4

یکی از محدودیت های RP ثابت این است که آدرس RP ثابت است و اگر RP از بین برود، شبکه چند منظوره نیز از بین می رود.از آنجایی که RP ثابت است، مسیریاب های چند منظوره نمی توانند به سبک متراکم سوئیچ نمایند، زایرا به هیچ روشی از جریان از بین رفتن RP مطلع نمی شوند.

در Anycast RP، چندین RP با یک آدرس IP حلقه برگشتی(Loopback) تنظیم می شوند و تمام مسیریاب های چند منظوره با این آدرس حلقه برگشتی به طور ثابتی تنظیم شده اند. این آدرس حلقه برگشتی توسط پروتکل مسیریابی داخلی تک منظوره معرفی شده و هر مسیریاب چند منظوره نزدیکترین RP را انتخاب می نماید. اگر یکی از RPها از بین برود، پروتکل مسیریابی تک منظوره دیگر آدرس آن RP را معرفی نخواهد کرد.مسیریاب هایی که از RP از بین رفته استفاده می نمودند بعد از همگرایی پروتکل مسیریابی داخلی، بر روی یک RP دیگر سوئیچ خواهند کرد.

در تمام مسیریاب ها باید IP چند منظوره سازی فعال شود و یک پروتکل مسیریابی داخلی تنظیم شده باشد.در سبک پراکنده هر رابط با استفاده از دستور ip pim sparse-mode تنظیم می شود.از سبک پراکنده ( Sparse Dense) نمی توان استفاده کرد، زیرا RPها به طور ثابت تعیین شده اند و مسیریاب ها به هیچ روشی از جریان از بین رفتن RPها مطلع نمی شوند.

### 12-4آدرس هاي چند منظوره ذخيره :

جدول زیر برخی از آدرس های چند منظوره ذخیره شده برای مقاصد خاص را نشان می دهد.این آدرس ها نباید توسط کاربرد های چند منظوره استفاده شوند. به عنوان مثال ، آدرس چند منظوره 224.0.0.5 توسط OSPF جهت تبادل اطلاعات پروتکل بین مسیریاب های OSPF به کار می رود.

| آدرس های چند منظوره | توضیحات |
|---|---|
| 224.0.0.1 | تمام سیستم های یک زیر شبکه |
| 224.0.0.2 | تمام مسیریاب های یک زیر شبکه |
| 224.0.0.5 | تمام مسیریاب های OSPF |
| 224.0.0.6 | مسیریاب های اختصاصی OSPF |
| 224.0.0.9 | مسیریاب های RIP نسخه دو |
| 224.0.0.10 | مسیریاب های EIGRP |
| 224.0.0.13 | مسیریاب های PIM |

## 13-4مسیریابي هوشمند:

مسیریابی هوشمند آگاه از توان در شبکه های حسگر بیسیم به کمک روشهای هوش ازدحامی و شبکه های عصبی:

یک شبکه حسگر بی سیم متشکل از تعداد زیادی گره‌های حسگر است که در یک محیط به طور گسترده پخش شده و به جمع‌آوری اطلاعات از محیط می‌پردازند. مسئله مسیریابی در شبکه‌های حسگر بی سیم از جمله مهمترین مسائلی است که کارکرد بهینه یک شبکه حسگر را تضمین می‌کند. به دلیل محدویت میزان انرژی هر گره در یک شبکه حسگر، مسیریابی باید طوری صورت بگیرد که در مجموع طول عمر کلی شبکه بیشینه شود. هدف اصلی این روش مسیریابی که به صورت توزیع شده در یک شبکه حسگر بی سیم طراحی می شود، بهینه سازی طول عمر شبکه حسگر با توجه به میزان انرژی هر گره، هزینه مسیر ها و میزان اهمیت آن گره در فرآیند مسیریابی می باشد. این روش مسیریابی توزیع شده از عاملهای مورچه جهت جمع آوری اطلاعات، تجمیع آنها و تعلیم شبکهٔ عصبی گره ها استفاده می کند، که برگرفته از الگوریتم مورچگان شبکه است. در طول پروسه مسیر یابی اوزان شبکه عصبی طوری تعلیم می بینند که عدالت در مسیر یابی رعایت شده و طول عمر شبکه به بیشترین مقدار ممکن برسد. خاصیت وفق پذیری این روش مسیریابی، آن را قادر می کند تا تغییرات گوناگون توپولوژی شبکه را که در اثر حرکت گره ها یا اتمام باتری آنها به وجود می آید، در فرآیند مسیریابی بهینه لحاظ نماید. کاربرد عمده‌ی این نوع از شبکه های حسگر، شناسایی یک منطقه نظامی است که میان نیروهای خودی و نیروهای دشمن قرار گرفته است. شبکه ی حسگر بر روی یک منطقه مورد شناسایی به طور تصادفی توزیع شده است و ادوات نظامی دشمن بین گره های این شبکه حرکت می کنند. شبیه سازی انجام شده حاکی از افزایش قابل توجه طول عمر شبکه‌ی حسگر در فرآیند مسیریابی به کمک این روش نسبت به سایر روش های موجود می باشد. کلیه بخش های این روش از رابطه های خطی پیروی می کنند و لذا قابلیت پیاده سازی روی گره های حسگر با توان پردازشی پایین را دارند. با استفاده از این روش می توان نوعی هوشمندی توزیع شده در سرتاسر شبکه حسگر ایجاد نمود و از مجموعه همزمان پردازش های هوشمند در گره های حسگر، در حل سایر مسائل موجود در شبکه های حسگر نیز استفاده کرد.

## نتیجه گیری:

از آنجایی که الگوریتم های مسیریابی هر کدام نقاط ضعف و نقاط قوت خود را دارند ما بایدالگوریتمی را انتخاب کنیم که دارای خصوصیاتی از جمله :

عمومی باشد یعنی بر روی انواع مسیریاب بتوان آنرا اجرا کردسرعت همگرایی بالایی داشته باشد یعنی در کوتاهترین زمان اطلاعات به روز خود را برای بقیه مسیریاب ها ارسال کندز انواع پروتکل های routed پشتیبانی نمایدبتواند هوشمندانه عمل نماید و... باشد.

در بین تمامی الگوریتم ها ی مسیریابی چنانچه در این مجموعه ذکر شد الگوریتم OSPF تا حدودی توانسته است این انتظارات را برآورده کند.

از آنجا که تصمیم گیری در انتخاب مسیر در زمان استفاده از معیار فازی با استفاده از اطلاعات اضافی یک بعد دیگر(علاوه بر تاخیر،طول صف نیز هست) صورت می گیرد لذا خوشایندتر بوده وجلب نظر می نماید .

اما نقطه ضعف استفاده از پارامتر های ترکیبی از نوع فازی ، از بین رفتن اطلاعات مربوط به پارامترهای تنهایی هست که از ترکیب آنها این پارامتر فازی را ایجاد می شوند که در اینجا همان تاخیر و طول صف می باشند .

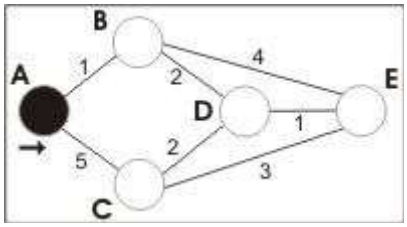
اما نباید نگران بود چراکه ،هر دوی این پارامترها از ارائه اطلاعات دقیق در باره کل شبکه عاجز بودند لذا استفاده از پارامتری فازی جهت مسیر یابی در شبکه به جای هر کدام از این2 پارامتر، نه تنها نگران کننده نیست ،بلکه راضی کننده هم خواهد بود. امید است که در آینده بتوان بهترین الگوریتم های ممکن را که بتوانند به صورت هوشمند عمل نمایند بر روی مسیریاب ها پیاده سازی کرد.

# پیوست 1

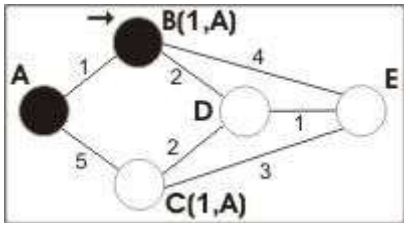
## الگوریتم Dijkstra:

در اینجا ما می خواهیم بهترین مسیر بین گره های A و E را پیدا کنیم همانطورکه میبینید 6 مسیر بین A و E وجود دارد. (ABE، ACE، ABDE، ACDE، ABDCE،ACDBE) و واضح است که ABDE بهترین مسیر میباشد زیرا کمترین وزن را دارد اما همیشه به این سادگی نیست و برخی موارد پیچیده وجود دارد که در آن ما مجبوریم از الگوریتم هایی برای یافتن بهترین مسیر استفاده کنیم.

همانطور که در تصویر ذیل مشاهده میکنید،گره منبع (A) بعنوان گرهT انتخواب شده و بنابراین برچسب آن Permanent، می باشد.(ما گره های Permanent را با دایره های تو پر و گره های T را با یک پیکان نشان میدهیم).

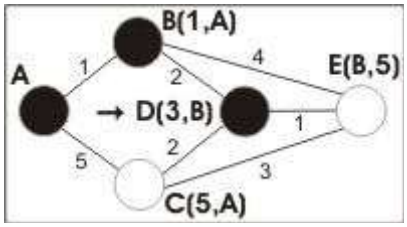



در این مرحله شما میبینید که مجموع برآورد وضعیت گره های Tentative که مستقیما به گره B ، T (C) متصل شده اند،تغییر یافته است.همچنین از آنجایی که گره B کمترین وزن را دارد،بعنوان گره T انتخاب شده و برچسب آن به حالت Permanent تغییر آرده است.

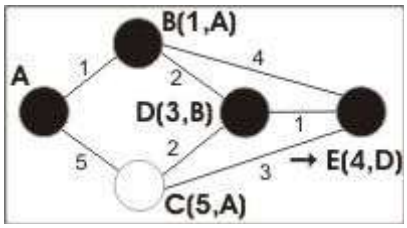



در این مرحله همانند مرحله قبل دو مجموعه برآورد وضعیت گره هایی که Tentativeدارای اتصال مستقیم به گره T میباشد. (E،D) تغییرکرده است.همچنین از آنجایی که گره D وزن کمتری دارد،بعنوان گره T انتخاب شده و برچسب آن به وضعیت Permanent تغییر کرده است. در این مرحله ما هیچ گره Tentative نداریم

بنابراین فقط گره T بعدی را شناسایی میکنیم.از آنجایی که میکنیم. E دارای کمترین وزن میباشد بعنوان گره T انتخاب میشود.




E گره مقصد بوده بنابر این کار ما در اینجا تمام میشود.اکنون ما کار شناسایی مسیر را به انتها رسانده ایم.گره قبلی E گره D ،گره B میباشد و گره قبلی B ،گره A میباشد.بنابراین بهترین مسیر ABDE است در این مورد وزن کل مسیر، 4(1+2+1) میباشد.




با وجودی که این الگوریتم بخوبی کار میکند اما آنقدر پیچیده است که زمان پردازش آن برای روتر طولانی بوده و راندمان شبکه را کاهش میدهد.همچنین اگر یک روتر اطلاعات غلطی را به روترهای دیگر بدهد،همه تصمیمات مسیر یابی نادرست خواهد بود.

## الگوریتم دایجکسترا برای پیدا کردن بهترین مسیر بین دو گره در یک گراف:

```
#define MAX_NODES /*گراف گرهای حد اکثر تعداد تعریف*/ 100
#define INFINITY /*هزینهٔ عنوان به بزرگ بسیار عدد یک تعریف
بینهایت */ 1000000000
int n, dist[MAX_NODES][ MAX_NODES]; /* /*همجواری ماتریس تعریف
میباشد گراف گرهای تعداد */ n */
void shortest_path(int s, int t, int path[])
{ struct state {
int predecessor; /* /*مسیر در قبلی گره
int length; /* /*مبدأ تا گره هزینهٔ
enum {permanent, tentative} label; /* /*گره حالت
```

```
} State[MAX_NODES]; /* /*یک درون گره هر برای حالت رکورد های تشکیل آرایه
int i, k, min;
struct state *p;
for(p = &State[0];p<&State[n];p++) { /* /*رکورد های به اولیه مقدار دهی حالت
p->predecessor=NULL;
p->length=INFINITY;
p->label=tentative;
}
State[t].length=0;
State[t].label=permanent;
k=t; /* میباشد شروع برای کار نقطهٔ گره k */
do {
for(i=0;i<n;i++)
if(dist[k][i]!=0 && State[i].label==tentative){
if(State[k].length+dist[k][i]<State[i].length){
/*دارد؟ وجود مبدا گره به فعلی گره از بهتری مسیر آیا*/
State[I].predecessor=k;
State[i].length= State[k].length+dist[k][i];
}
}
k=0; min=INFINITY; /* /*"موقتی" علامت با گرههای بین از گرهای یافتن دارد را هزینه کمترین که
for(i=0;i<n;i++)
if(State[i].label==tentative && State[i].length<min){



min= State[i].length;
k=i;
}
State[k].label=permanent;
} while (k!=s);
/* path[] /*آرایهٔ در اول به آخر از بهینه مسیر دادن قرار
i=0; k=s;
do {
path[i++]=k; k=State[k].predecessor;
} while (k>=0);
}
```

# پیوست 2

## دستورات پیکربندی اولیه روتر:

Router Modes:

| | |
|---|---|
| Router> | User mode |
| Router# | Privileged mode (also known as EXEC-level mode) |
| Router(config)# | Global configuration mode |
| Router(config-if)# | Interface mode |
| Router(config-subif)# | Subinterface mode |
| Router(config-line)# | Line mode |
| Router(config-router)# | Router configuration mode |

Entring Global Configuration Mode:

| | |
|---|---|
| Router> | Limited viewing of configuration. You cannot make changes in this mode. |
| Router# | You can see the configuration and move to make changes. |
| Router# | configure terminal |
| Router(config)# | Moves to global configuration mode. This prompt indicates that you can start making changes. |

Configuring a Router Name:

Router(config)# hostname Cisco The name can be any word you choose

Configuring Password:

| | |
|---|---|
| Router(config)# | enable password cisco Sets enable password |
| Router(config)# | enable secret class Sets enable secret password |
| Router(config)# | line console 0 Enters console line mode |
| Router(config-line)# | password console Sets console line mode password to console |
| Router(config-line)# | login Enables password checking at login |
| Router(config)# | line vty 0 4 Enters vty line mode for all five vty lines |
| Router(config-line)# | password telnet Sets vty password to telnet |
| Router(config-line)# | login Enables password checking at login |
| Router(config)# | line aux 0 Enters auxiliary line mode |

Router(config-line)# password backdoor Sets auxiliary line mode password to backdoor
Router(config-line)# login Enables password checking at login

Password Encryption:
Router(config)# service passwordencryption
Applies a weak encryption to passwords
Router(config)# enable password cisco Sets enable password to cisco
Router(config)# line console 0 Moves to console line mode
Router(config-line)# password Cisco Continue setting passwords as above
Router(config)# no service passwordencryption
Turns off password encryption
Configring a Serial Interface:
Router(config)# interface s0/0/0 Moves to serial interface 0/0/0 configuration mode
Router(config-if)# description Link to ISP Optional descriptor of the link is locally significant
Router(config-if)# ip address 192.168.10.1 255.255.255.0
Assigns address and subnet mask to interface
Router(config-if)# clock rate 56000 Assigns a clock rate for the interface
Router(config-if)# no shutdown Turns interface on

Configuring a Fast Ethernet Interface:
Router(config)# interface fastethernet 0/0 Moves to Fast Ethernet 0/0 interface configuration mode
Router(config-if)# description Accounting LAN
Optional descriptor of the
link is locally significant
Router(config-if)# ip address 192.168.20.1 255.255.255.0
Assigns address and subnet mask to interface
Router(config-if)# no shutdown Turns interface on
Saving Configuration:
Router# copy running-config startup-config
Saves the running configuration to local NVRAM
Router# copy running-config tftp
Saves the running configuration remotely to a TFTP server

Erasing Configuration:
Router# erase startup-config Deletes the startup configuration file from NVRAM

Show Commands:
Router# show ? Lists all show commands available.
Router# show interfaces Displays statistics for all interfaces.

| | |
|---|---|
| Router# | show interface serial 0/0/0 Displays statistics for a specific interface (in this case, serial 0/0/0). |
| Router# | show ip interface brief Displays a summary of all interfaces, including status and IP address assigned. |
| Router# | show controllers serial 0/0/0 Displays statistics for interface hardware. Statistics display if the clock rate is set and if the cable is DCE, DTE, or not attached. |
| Router# | show clock Displays time set on device. |
| Router# | show hosts Displays local host-to-IP address cache. These are the names and addresses of hosts on the network to which you can connect. |
| Router# | show users Displays all users connected to device. |
| Router# | show history Displays the history of commands used at this edit level. |
| Router# | show flash Displays info about flash memory. |
| Router# | show version Displays info about loaded software version. |
| Router# | show arp Displays the Address Resolution Protocol (ARP) table. |
| Router# | show protocols Displays status of configured Layer 3 protocols. |
| Router# | show startup-config Displays the configuration saved in NVRAM. |
| Router# | show running-config Displays the configuration currently running in RAM. |

# فهرست منابع


مقاله مربوط به همایش ها:

[1] حسین کاری ،طراحی و پیاده سازی مدل فازی پروتکل مسیر یابی ospf ،سومین کنفرانس فناوری اطلاعات و دانش، 6 آذر 1386، دانشگاه فردوسی مشهد، 1387

کتاب ها:

[1] احسان ملکیان، اصول مهندسی اینترنت،چاپ شانزدهم، انتشارات تهران:نص،1388

[2] براین استوارت،راهنمای جامع CCNA BSCI ،ترجمه دکتر حسین محسن زاده،چاپ اول،آریا پژوه و موسسه فرهنگی و اطلاع رسانی آموزگارمهر(انتشارات زوفا)،1387

[3] بیل پارکورست،مسیریابی گام اول،ترجمه علی مختار پور و نگار حمید سمیعی،چاپ اول ،انتشارات پندار پارس و با همکاری آریا پژوه،بهار 1387

[4] QOS Routing In Network With Inaccurate Information:Thepry and Alogrithms , Roch A_Gueerin and Ariel Orda, In Proceeding of Infocom,1997

وب سایت ها:

[1] وب سایت شرکت سیسکو ، www.cisco.com

[2] مقالات علمی و پژوهشی ، www.wikipedia.org

[3] جدیدترین آموزش های تجهیزات سیسکو، www.cisco.ded.ir

[4] آموزش سوئیچ و روتر، www.switch-routers.com

[5] آموزش دوره های تخصصی سیسکو www.cisco.parsfa.com