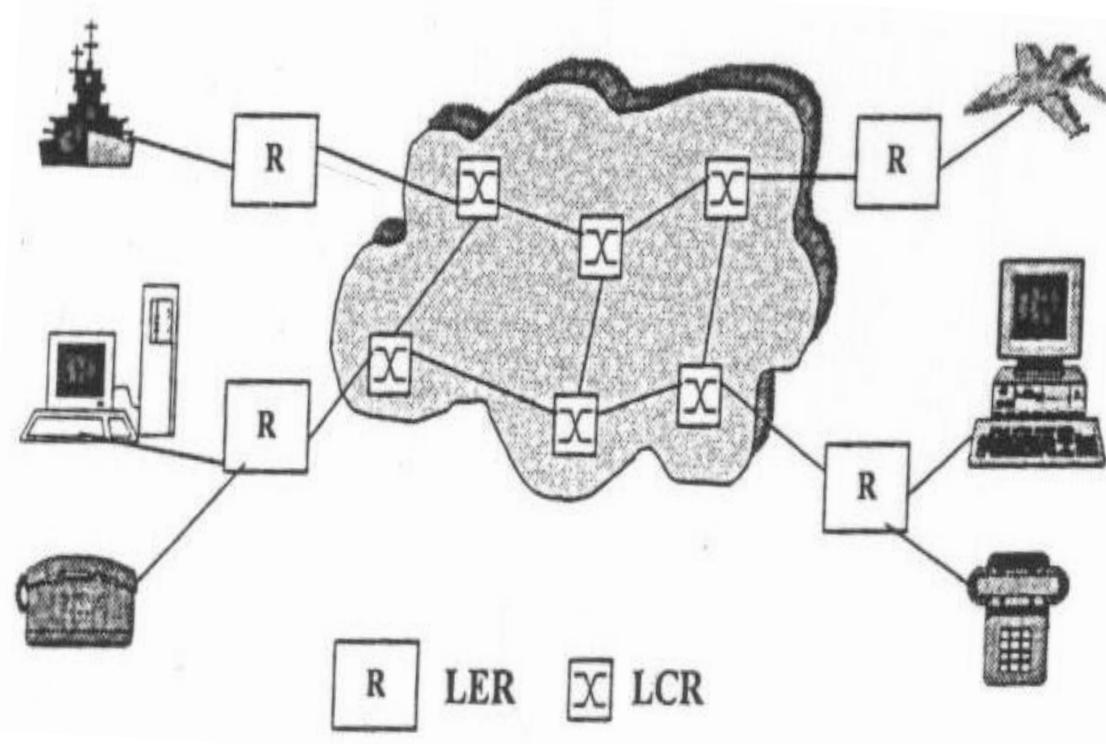




دانشگاه علم و صنعت ایران

شبکه های کامپیوتری پیشرفته



استاد : دکتر محمود فتحی

فهرست مطالب:

عنوان	صفحة
بخش ۱: مفاهیم پایه	۲
فصل ۱: مروری بر شبکه های کامپیوتروی	۳
بخش ۲: آدرس دهی	۲۴
فصل ۲: آدرس دهی در شبکه های کامپیوتروی	۲۵
فصل ۳: مسیریابی در مسیریابها	۳۸
فصل ۴: پروتکل های مسیریابی در شبکه	۴۵
فصل ۵: پروتکلهای مسیریابی Multicast و MultiCasting	۶۹
بخش ۳: سوئیچ داده	۸۰
فصل ۶: روشهای سوئیچ داده	۸۱
فصل ۷: شبکه های FrameRelay و ATM	۱۰۲
فصل ۸: MPLS و DiffServ , ISA	۱۳۴
بخش ۴: پروتکلهای شبکه	۱۵۷
فصل ۹: پروتکل IP	۱۵۸
فصل ۱۰: پروتکل های ICMP و IGMP	۱۷۱
فصل ۱۱: کنترل اتصالات در شبکه	۱۷۹
فصل ۱۲: پروتکل های TCP و UDP	۱۹۱
فصل ۱۳: پروتکلهای مدیریت شبکه	۲۰۱
بخش ۵: شبکه های بی سیم	۲۱۶
فصل ۱۴: شبکه های محلی بی سیم	۲۱۷
بخش ۶: امنیت در شبکه	۲۵۱
فصل ۱۵: امنیت در شبکه	۲۵۲
منابع	۲۶۰

بخش ا:

مفاتیح پایه شبکه

فصل ۱: مروری بر شبکه های کامپیوتری



www.samavi.info

فصل ا:

مژوی بز شبکه های کامپیوتری

استفاده از شبکه های کامپیوتری در چندین سال اخیر رشد فراوانی کرده و سازمانها و موسسات اقدام به برپایی شبکه نموده اند . هر شبکه کامپیوتری باید با توجه به شرایط و سیاست های هر سازمان ، طراحی و پیاده سازی گردد. در واقع شبکه های کامپیوتری زیر ساخت های لازم را برای به اشتراک گذاشتن منابع در سازمان فراهم می آورند؛ در صورتیکه این زیر ساختها به درستی طراحی نشوند، در زمان استفاده از شبکه مشکلات متفاوتی پیش آمده و باید هزینه های زیادی به منظور نگهداری شبکه و تطبیق آن با خواسته های مورد نظر صرف شود.

در زمان طراحی یک شبکه سوالات متعددی مطرح می شود:

- برای طراحی یک شبکه باید از کجا شروع کرد؟
- چه پارامترهایی را باید در نظر گرفت؟
- هدف از برپاسازی شبکه چیست؟
- انتظار کاربران از شبکه چیست؟
- آیا شبکه موجود ارتفاع می باید و یا یک شبکه از ابتدا طراحی می شود؟
- چه سرویس ها و خدماتی بروی شبکه ارائه خواهد شد؟

بطور کلی قبل از طراحی فیزیکی یک شبکه کامپیوتری ، ابتدا باید خواسته ها شناسایی و تحلیل شوند، مثلاً در یک کتابخانه چرا قصد ایجاد یک شبکه را داریم و این شبکه باید چه سرویس ها و خدماتی را ارائه نماید؛ برای تامین سرویس ها و خدمات مورد نظر اکثریت کاربران ، چه اقداماتی باید انجام داد ؛ مسائلی چون پروتکل مورد نظر برای استفاده از شبکه ، سرعت شبکه و از همه مهمتر مسائل امنیتی شبکه ، هریک از اینها باید به دقت مورد بررسی قرار گیرد. سعی شده است پس از ارائه تعاریف اولیه ، مطالبی پیرامون کاربردهای عملی آن نیز ارائه شود تا در تصمیم گیری بهتر یاری کند.

شبکه کامپیوتری چیست؟

اساساً یک شبکه کامپیوتری شامل دو یا بیش از دو کامپیوتر و ابزارهای جانبی مثل چاپگرهای اسکنرها و مانند آینها هستند که بطور مستقیم بمنظور استفاده مشترک از سخت افزار و نرم افزار، منابع اطلاعاتی ابزارهای متصل ایجاده شده است توجه داشته باشید که به تمامی تجهیزات سخت افزاری و نرم افزاری موجود در شبکه منبع گویند. در این تشریک مساعی با توجه به نوع پیکربندی کامپیوتر، هر کامپیوتر کاربر می تواند در آن واحد منابع خود را اعم از ابزارها و داده ها با کامپیوترهای دیگر همزمان بهره ببرد.

دلایل استفاده از شبکه را می توان موارد ذیل عنوان کرد :

- ۱ - استفاده مشترک از منابع :استفاده مشترک از یک منبع اطلاعاتی یا امکانات جانبی رایانه ، بدون توجه به محل جغرافیایی هریک از منابع را استفاده از منابع مشترک گویند.
- ۲ - کاهش هزینه :متمرکز نمودن منابع واستفاده مشترک از آنها و پرهیز از پخش آنها در واحدهای مختلف واستفاده اختصاصی هر کاربر در یک سازمان کاهش هزینه را در پی خواهد داشت .
- ۳ - قابلیت اطمینان :این ویژگی در شبکه ها بوجود سرویس دهنده های پشتیبان در شبکه اشاره می کند ، یعنی به این معنا که می توان از منابع گوناگون اطلاعاتی و سیستم ها در شبکه نسخه های دوم و پشتیبان تهیه کرد و در صورت عدم دسترسی به یک از منابع اطلاعاتی در شبکه " بعلت از کارافتادن سیستم " از نسخه های پشتیبان استفاده کرد. پشتیبان از سرویس دهنده ها در شبکه کارآیی، فعالیت و آمادگی دائمی سیستم را افزایش می دهد.
- ۴ - کاهش زمان : یکی دیگر از اهداف ایجاد شبکه های رایانه ای ، ایجاد ارتباط قوی بین کاربران از راه دور است ؛ یعنی بدون محدودیت جغرافیایی تبادل اطلاعات وجود داشته باشد. به این ترتیب زمان تبادل اطلاعات و استفاده از منابع خود بخود کاهش می یابد.

۵ - قابلیت توسعه : یک شبکه محلی می تواند بدون تغییر در ساختار سیستم توسعه یابد و تبدیل به یک شبکه بزرگتر شود. در اینجا هزینه توسعه سیستم هزینه امکانات و تجهیزات مورد نیاز برای گسترش شبکه مد نظر است.

۶ - ارتباطات: کاربران می توانند از طریق نوآوریهای موجود مانند پست الکترونیکی و یا دیگر سیستم های اطلاع رسانی پیغام هایشان را مبادله کنند؛ حتی امکان انتقال فایل نیز وجود دارد.

در طراحی شبکه مواردی که قبل از راه اندازی شبکه باید مد نظر قرار دهید شامل موارد ذیل هستند:

- ۱ - اندازه سازمان
- ۲ - سطح امنیت
- ۳ - نوع فعالیت
- ۴ - سطح مدیریت
- ۵ - مقدار ترافیک
- ۶ - بودجه

هرگاه شما کامپیوتری را به شبکه اضافه می کنید، این کامپیوتر به یک ایستگاه کاری^۱ یا گره^۲ تبدیل می شود. یک ایستگاه کاری؛ کامپیوتری است که به شبکه الصاق شده است و در واقع اصطلاح ایستگاه کاری روش دیگری است برای اینکه بگوییم یک کامپیوتر متصل به شبکه است. یک گره چگونگی و ارتباط شبکه یا ایستگاه کاری و یا هر نوع ابزار دیگری است که به شبکه متصل است و بطور ساده تر هر چه را که به شبکه متصل و الحاق شده است یک گره گویند. برای شبکه جایگاه و آدرس یک ایستگاه کاری مترادف با هویت گره اش است.

مدل های شبکه:

در یک شبکه، یک کامپیوتر می تواند هم سرویس دهنده و هم سرویس گیرنده باشد. یک سرویس دهنده، کامپیوتری است که فایل های اشتراکی و همچنین سیستم عامل شبکه که مدیریت عملیات شبکه را بعهده دارد - را نگهداری می کند. برای آنکه سرویس گیرنده بتواند به سرویس دهنده دسترسی پیدا کند، ابتدا سرویس گیرنده باید اطلاعات مورد نیازش را از سرویس دهنده تقاضا کند. سپس سرویس دهنده اطلاعات در خواست شده را به سرویس گیرنده ارسال خواهد کرد. سه مدل از شبکه هایی که مورد استفاده قرار می گیرند، عبارتند از :

- ۱ - شبکه نظیر به نظیر^۳
- ۲ - شبکه مبتنی بر سرویس دهنده^۴
- ۳ - شبکه سرویس دهنده / سرویس گیرنده^۵

مدل شبکه نظیر به نظیر:

در این شبکه ایستگاه ویژه ای جهت نگهداری فایل های اشتراکی و سیستم عامل شبکه وجود ندارد. هر ایستگاه می تواند به منابع سایر ایستگاه ها در شبکه دسترسی پیدا کند. هر ایستگاه خاص می تواند هم عنوان سرویس دهنده و هم عنوان سرویس گیرنده عمل کند. در این مدل هر کاربر خود مسئولیت مدیریت و ارتقاء دادن

1 - WorkStation

2 - Node

3 - Peer to Peer

4 - Server Based

5 - Client Server

نرم افزارهای ایستگاه خود را بعده دارد. از آنجایی که یک ایستگاه مرکزی برای مدیریت عملیات شبکه وجود ندارد ، این مدل برای شبکه ای با کمتر از ۱۰ ایستگاه بکار می رود .

مدل شبکه مبتنی بر سرویس دهنده :

در این مدل شبکه ، یک کامپیوتر بعنوان سرویس دهنده کلیه فایل ها و نرم افزارهای اشتراکی نظیر واژه پرداز ها، کامپایلرها ، بانک های اطلاعاتی و سیستم عامل شبکه را در خود نگهداری می کند. یک کاربر می تواند به سرویس دهنده دسترسی پیدا کرده و فایل های اشتراکی را از روی آن به ایستگاه خود منتقل کند

مدل سرویس دهنده / سرویس گیرنده :

در این مدل یک ایستگاه در خواست انجام کارش را به سرویس دهنده ارائه می دهد و سرویس دهنده پس از اجرای وظیفه محوله ، نتایج حاصل را به ایستگاه در خواست کننده عوتد می دهد. در این مدل حجم اطلاعات مبادله شده شبکه ، در مقایسه با مدل مبتنی بر سرویس دهنده کمتر است و این مدل دارای کارایی بالاتری می باشد.

شبکه های فعال (Active Network) و غیر فعال (passive network). در شبکه های غیر فعال بسته ها فقط داده هستند اما در شبکه های فعال ، بسته ها می توانند برنامه هایی باشند که در مقصد اجرا می شود و شبکه های سلولی: شبکه ای را گویند که از سلول به عنوان واحد پایه در انتقال داده استفاده می کند. سلول عبارتست از بسته های کوچک و با طول ثابت اطلاعات.

هر شبکه اساساً از سه بخش ذیل تشکیل می شود:

ابزارهایی که به پیکربندی اصلی شبکه متصل می شوند بعنوان مثال : کامپیوتر ها ، چاپگرهای هاب ها، سیم ها ، کابل ها و سایر رسانه هایی که برای اتصال ابزارهای شبکه استفاده می شوند. سازگار کننده ها^۱، که بعنوان اتصال کابل ها به کامپیوتر هستند . اهمیت آنها در این است که بدون وجود آنها شبکه تنها شامل چند کامپیوتر بدون ارتباط موازی است که قادر به سهیم شدن منابع یکدیگر نیستند . عملکرد سازگار کننده در این است که به دریافت و ترجمه سیگنال های درون داد از شبکه از جانب یک ایستگاه کاری و ترجمه وارسال برون داد به کل شبکه می پردازد.

اجزاء شبکه :

اجزا اصلی یک شبکه کامپیوتري عبارتند از :

- ۱ - کارت شبکه(NIC)^۲ : برای استفاده از شبکه و برقراری ارتباط بین کامپیوتر ها از کارت شبکه ای استفاده می شود که در داخل یکی از شیارهای برد اصلی کامپیوتر های شبکه "اعم از سرویس دهنده و گیرنده بصورت سخت افزاری و برای کنترل ارسال و دریافت داده نصب می گردد.
- ۲ - رسانه انتقال^۳ : رسانه انتقال کامپیوتر ها را به یکدیگر متصل کرده و موجب برقراری ارتباط بین کامپیوتر های یک شبکه می شود . برخی از متداولترین رسانه های انتقال عبارتند از : کابل زوج سیم بهم تابیده، کابل کواکسیال و کابل فیبر نوری .

Adaptors - ^۱

Network Interface Card - ^۲

Transmission Medium - ^۳

۳ - سیستم عامل شبکه (NOS¹): سیستم عامل شبکه بر روی سرویس دهنده اجرا می شود و سرویس های مختلفی مانند: اجازه ورود به سیستم، رمز عبور، چاپ فایل ها، مدیریت شبکه را در اختیار کاربران می گذارد.

انواع شبکه از لحاظ جغرافیایی:

نوع شبکه توسط فاصله بین کامپیوتر های تشکیل دهنده آن شبکه مشخص می شود:

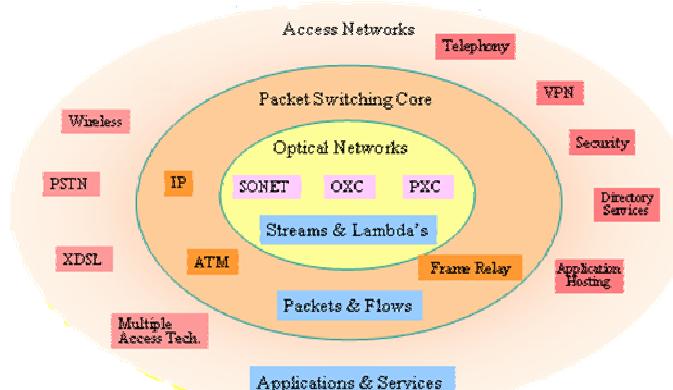
- شبکه محلی (LAN): ارتباط واتصال بیش از دو یا چند رایانه در فضای محدود یک سازمان از طریق کابل شبکه پروتکل بین رایانه ها و با مدیریت نرم افزاری موسوم به سیستم عامل شبکه را شبکه محلی گویند. کامپیوتر سرویس گیرنده باید از طریق کامپیوتر سرویس دهنده به اطلاعات و امکانات به اشتراک گذاشته دسترسی یابند. همچنین ارسال و دریافت پیام به یکدیگر از طریق رایانه سرویس دهنده انجام می گیرد. از خصوصیات شبکه های محلی می توان به موارد ذیل اشاره کرد:
 - ۱ - اساسا در محیط های کوچک کاری قابل اجرا و پیاده سازی می باشد.
 - ۲ - از سرعت نسبتا بالایی برخوردارند.

۳ - دارای یک ارتباط دائمی بین رایانه ها از طریق کابل شبکه می باشند.

اجزای یک شبکه محلی عبارتند از :

- سرویس دهنده
- سرویس گیرنده
- پروتکل
- کارت واسطه شبکه
- سیستم ارتباط دهنده

- شبکه گسترده (WAN): اتصال شبکه های محلی از طریق خطوط تلفنی، کابل های ارتباطی ماهواره و یا دیگر سیستم هایی مخابراتی چون خطوط استیجاری در یک منطقه بزرگتر را شبکه گسترده گویند. در این شبکه کاربران یا رایانه ها از مسافت های دور و از طریق خطوط مخابراتی به یکدیگر متصل می شوند. کاربران هر یک از این شبکه ها می توانند به اطلاعات و منابع به اشتراک گذاشته شده توسط شبکه های دیگر دسترسی یابند. از این فناوری با نام شبکه های راه دور² نیز نام برده می شود. در شبکه گسترده سرعت انتقال داده نسبت به شبکه های محلی خیلی کمتر است. بزرگترین و مهم ترین شبکه گسترده، شبکه جهانی اینترنت می باشد.



تصویر ۱-۱: ساختار لایه ای اینترنت

Network Operating System - ¹
Long Haul Network - ²

توبولوژی شبکه :

توبولوژی شبکه تشریح کننده نحوه اتصال کامپیوتر ها در یک شبکه به یکدیگر است. پارامترهای اصلی در طراحی یک شبکه ، قابل اعتماد بودن و مقرنون به صرفه بودن است. انواع متداول توبولوژی ها در شبکه کامپیوترا عبارتند از :

▪ توبولوژی ستاره ای(Star): در این توبولوژی ، کلیه کامپیوتر ها به یک کنترل کننده مرکزی با هاب متصل هستند. هرگاه کامپیوترا بخواهد با کامپیوترا دیگری تبادل اطلاعات نماید، کامپیوترا منبع ابتدا باید اطلاعات را به هاب ارسال نماید. سپس از طریق هاب آن اطلاعات به کامپیوترا مقصد منتقل شود. اگر کامپیوترا شماره یک بخواهد اطلاعاتی را به کامپیوترا شماره ۳ بفرستد ، باید اطلاعات را ابتدا به هاب ارسال کند، آنگاه هاب آن اطلاعات را به کامپیوترا شماره سه خواهد فرستاد.

نقاط ضعف این توبولوژی آن است که عملیات کل شبکه به هاب وابسته است. این بدان معناست که اگر هاب از کار بیفتند، کل شبکه از کار خواهد افتاد . نقاط قوت توبولوژی ستاره عبارتند از:

- نصب شبکه با این توبولوژی ساده است.
- توسعه شبکه با این توبولوژی به راحتی انجام می شود.
- اگر یکی از خطوط متصل به هاب قطع شود ، فقط یک کامپیوترا از شبکه خارج می شود.

▪ توبولوژی حلقوی(Ring): این توبولوژی توسط شرکت IBM اختراع شد و بهمین دلیل است که این توبولوژی بنام IBM Tokenring مشهور است. در این توبولوژی کلیه کامپیوترا ها به گونه ای به یکدیگر متصل هستند که مجموعه آنها یک حلقه را می سازد. کامپیوترا مبدا اطلاعات را به کامپیوترا بعدی در حلقه ارسال نموده و آن کامپیوترا آدرس اطلاعات را برای خود کپی می کند، آنگاه اطلاعات را به کامپیوترا بعدی در حلقه منتقل خواهد کرد و به همین ترتیب این روند ادامه پیدا می کند تا اطلاعات به کامپیوترا مبدا برسد. سپس کامپیوترا مبدا این اطلاعات را از روی حلقه حذف می کند. نقاط ضعف توبولوژی فوق عبارتند از:

- اگر یک کامپیوترا از کار بیفتند ، کل شبکه متوقف می شود.
- به سخت افزار پیچیده نیاز دارد ” کارت شبکه آن گران قیمت است ”.
- برای اضافه کردن یک ایستگاه به شبکه باید کل شبکه را متوقف کرد.

نقاط قوت توبولوژی فوق عبارتند از :

- نصب شبکه با این توبولوژی ساده است.
- توسعه شبکه با این توبولوژی به راحتی انجام می شود.
- در این توبولوژی از کابل فیبر نوری میتوان استفاده کرد.

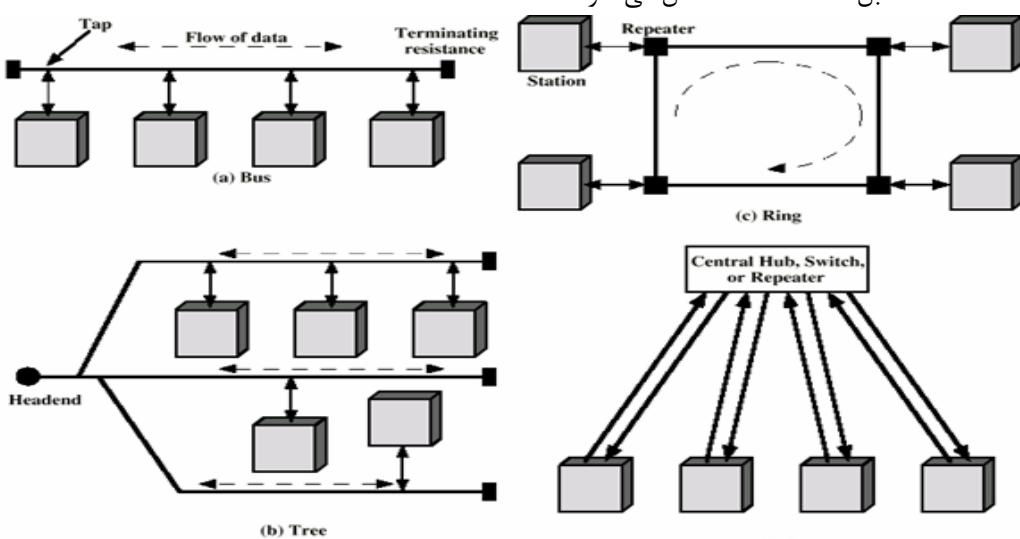
▪ توبولوژی BUS: در یک شبکه خطی چندین کامپیوترا به یک کابل به نام BUS متصل می شوند. در این توبولوژی ، رسانه انتقال بین کلیه کامپیوترا ها مشترک است. یکی از مشهورترین قوانین نظارت بر خطوط ارتباطی در شبکه های محلی اترنت است. توبولوژی BUS از متداولترین توبولوژی هایی است که در شبکه محلی مورد استفاده قرار می گیرد. سادگی ، کم هزینه بودن و توسعه آسان این شبکه ، از نقاط قوت توبولوژی BUS می باشد. نقطه ضعف عمدۀ این شبکه آن است که اگر کابل

اصلی که بعنوان پل ارتباطی بین کامپیوتر های شبکه می باشد قطع شود، کل شبکه از کار خواهد افتاد.

توبولوژی توری(Mesh): در این توبولوژی هر کامپیوتری مستقیما به کلیه کامپیوترهای شبکه متصل می شود. مزیت این توبولوژی آن است که هر کامپیوتر با سایر کامپیوتر ها ارتباطی مجزا دارد. بنابراین ، این توبولوژی دارای بالاترین درجه امنیت و اطمینان می باشد. اگر یک کابل ارتباطی در این توبولوژی قطع شود ، شبکه همچنان فعال باقی می ماند. از نقاط ضعف اساسی این توبولوژی آن است که از تعداد زیادی خطوط ارتباطی استفاده می کند، مخصوصا زمانیکه تعداد ایستگاه ها افزایش یابند. به همین جهت این توبولوژی از نظر اقتصادی مقرن به صرفه نیست. برای مثال ، در یک شبکه با صد ایستگاه کاری ، ایستگاه شماره یک نیازمند به نود و نه می باشد. تعداد کابل های مورد نیاز در این توبولوژی با رابطه $N(N-1)/2$ محاسبه می شود که در آن N تعداد ایستگاه های شبکه می باشد.

توبولوژی درختی(Tree): این توبولوژی از یک یا چند هاب فعال یا تکرار کننده برای اتصال ایستگاه ها به یکدیگر استفاده می کند. هاب مهمترین عنصر شبکه مبتنی بر توبولوژی درختی است؛ زیرا کلیه ایستگاه ها را به یکدیگر متصل می کند. وظیفه هاب دریافت اطلاعات از یک ایستگاه و تکرار و تقویت آن اطلاعات و سپس ارسال آنها به ایستگاه دیگر می باشد.

توبولوژی ترکیبی (Hybrid): این توبولوژی ترکیبی است از چند شبکه با توبولوژی متفاوت که توسط یک کابل اصلی بنام Back bone به یکدیگر مرتبط شده اند . هر شبکه توسط یک Bridg به کابل متصل می شود.



تصویر ۱-۲: برخی توبولوژی های رایج شبکه

مدل OSI^۱:

این مدل مبتنی بر قراردادی است که سازمان استانداردهای جهانی ایزو بعنوان مرحله ای از استاندارد سازی قراردادهای لایه های مختلف توسعه دارد . نام این مدل مرجع به این دلیل OSI است زیرا با اتصال سیستم های باز سروکار دارد و سیستم های باز سیستم هایی هستند که برای ارتباط با سیستم های دیگر باز هستند . این مدل هفت لایه دارد که اصولی که منجر به ایجاد این لایه ها شده اند عبارتند از :

▪ وقتی نیاز به سطوح مختلف از انتزاع است ، لایه ای باید ایجاد شود.

- هر لایه باید وظیفه مشخصی داشته باشد.
- وظیفه هر لایه باید با در نظر گرفتن قراردادهای استاندارد جهانی انتخاب گردد.
- مرزهای لایه باید برای کمینه کردن جریان اطلاعات از طریق رابط‌ها انتخاب شوند.

اکنون هفت لایه را به نوبت از لایه پایین مورد بحث قرار می‌دهیم:

- ۱ - لایه فیزیکی : به انتقال بیتهاي خام بروئی کانال ارتباطی مربوط می‌شود. در اینجا مدل طراحی با رابطهای مکانیکی ، الکتریکی ، و رسانه انتقال فیزیکی که زیر لایه فیزیکی قرار دارند سروکار دارد.
- ۲ - لایه پیوند داده : مبین نوع فرمت هاست مثلا شروع فریم ، پایان فریم ، اندازه فریم و روش انتقال فریم . وظایف این لایه شامل موارد زیر است : مدیریت فریم‌ها ، خطایابی و ارسال مجدد فریم‌ها ، ایجاد تمایز بین فریم‌ها داده و کنترل وایجاد هماهنگی بین کامپیوتر ارسال کننده و دریافت کننده داده‌ها . پروتکل‌های معروف برای این لایه عبارتند از :

- پروتکل **SDLC** که برای مبادله اطلاعات بین کامپیوتر‌ها بکار می‌رود و اطلاعات را به شکل فریم سازماندهی می‌کند.
- پروتکل **HDLC** که کنترل ارتباط داده‌ای سطح بالا زیر نظر آن است و هدف از طراحی آن این است که با هر نوع ایستگاهی کارکند از جمله ایستگاههای اولیه ، ثانویه و ترکیبی.

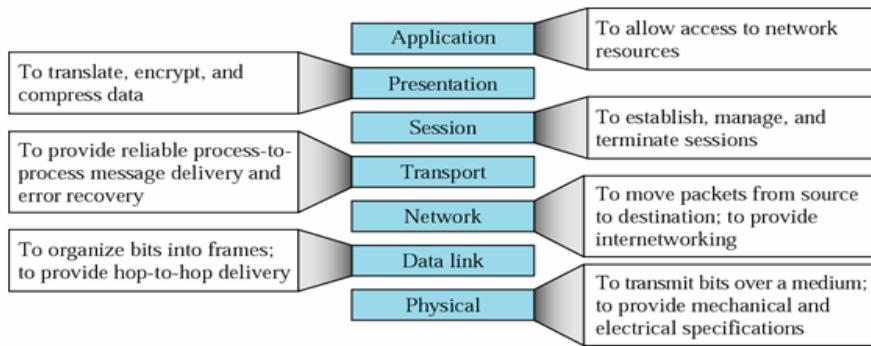
- ۳ - لایه شبکه : وظیفه این لایه ، مسیر یابی می‌باشد ، این مسیر یابی عبارتست از : تعیین مسیر مناسب برای انتقال اطلاعات . لایه شبکه آدرس منطقی هر فریم را بررسی می‌کند . و آن فریم را بر اساس جدول مسیر یابی به مسیر یاب بعدی می‌فرستد . لایه شبکه مسئولیت ترجمه هر آدرس منطقی به یک آدرس فیزیکی را بر عهده دارد . پس می‌توان گفت برقراری ارتباط یا قطع آن ، مولتی پلکس کردن از مهمترین وظایف این لایه است . از نمونه بارز خدمات این لایه ، پست الکترونیکی است.

- ۴ - لایه انتقال : وظیفه ارسال مطمئن یک فریم به مقصد را بر عهده دارد . لایه انتقال پس از ارسال یک فریم به مقصد ، منتظر می‌ماند تا سیگنالی از مقصد مبنی بر دریافت آن فریم دریافت کند . در صورتیکه لایه محل در منبع سیگنال مذکور را از مقصد دریافت نکند . مجدداً اقدام به ارسال همان فریم به مقصد خواهد کرد .

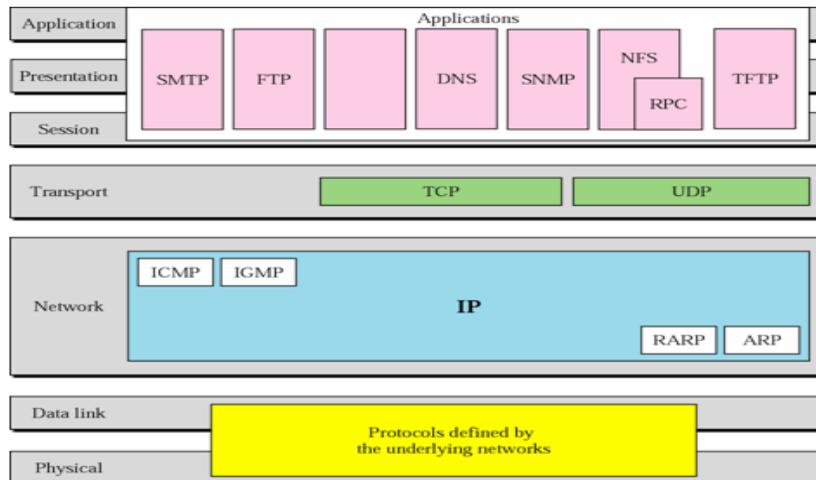
- ۵ - لایه اجلاس : وظیفه برقراری یک ارتباط منطقی بین نرم افزار‌های دو کامپیوتری که به یکدیگر متصل هستند به عهده این لایه است . وقتی که یک ایستگاه بخواهد به یک سرویس دهنده متصل شود ، سرویس دهنده فرایند برقراری ارتباط را بررسی می‌کند ، سپس از ایستگاه ، درخواست نام کاربر ، و رمز عبور را خواهد کرد . این فرایند نمونه‌ای از یک اجلاس می‌باشد .

- ۶ - لایه نمایش : این لایه اطلاعات را از لایه کاربرد دریافت نموده ، آنها را به شکل قابل فهم برای کامپیوتر مقصد تبدیل می‌کند . این لایه برای انجام این فرایند اطلاعات را به کدهای ASCII و یا Unicode تبدیل می‌کند .

- ۷ - لایه کاربرد : این لایه امکان دسترسی کاربران به شبکه را با استفاده از نرم افزارهایی چون E-mail ، FTP و ... فراهم می‌سازد .



TCP/IP and OSI model



تصویر ۱-۳: مدل ۷ لایه OSI و ۴ لایه TCP/IP

پروتکل های شبکه :

در این بخش تنها دو تا از مهمترین پروتکل های شبکه را معرفی می کنیم:

- پروتکل کنترل انتقال / پروتکل اینترنت(TCP/IP)^۱: از مهمترین و مشهورترین پروتکل های مورد استفاده در شبکه اینترنت است این بسته نرم افزاری به اشکال مختلف برای کامپیوتر ها و برنامه های مختلف ارائه می گردد. TCP/IP از مهمترین پروتکل های ارتباطی شبکه در جهان تلقی می شود و نه تنها برروی اینترنت و شبکه های گسترده گوناگون کاربرد دارد، بلکه در شبکه های محلی مختلف نیز مورد استفاده قرار می گیرد و در واقع این پروتکل زبان مشترک بین کامپیوتر ها به هنگام ارسال و دریافت اطلاعات یا داده می باشد. این پروتکل به دلیل سادگی مفاهیمی که در خود دارد اصطلاحا به سیستم باز مشهور است ، بر روی هر کامپیوتر و ابرایانه قابل طراحی و پیاده سازی است. پروتکل فوق شامل چهار سطح است که عبارتند از :

- الف - سطح لایه کاربرد
- سطح انتقال
- سطح اینترنت
- سطح شبکه

از فاکتورهای مهم که این پروتکل عنوان یک پروتکل ارتباطی جهانی مطرح می‌گردد، به موارد زیر می‌توان اشاره کرد:

- این پروتکل در چار چوب UNIX Operating System ساخته شده و توسط اینترنت بکار گرفته می‌شود.
- برروی هر کامپیوتر قابل پیاده‌سازی می‌باشد.
- بصورت حرف‌ای در شبکه‌های محلی و گسترده مورد استفاده قرار می‌گیرد.
- پشتیبانی از مجموعه برنامه‌ها و پروتکل‌های استاندارد دیگر چون پروتکل انتقال فایل، PPP، و پروتکل دو سویه FTP.

بنیاد و اساس پروتکل TCP/IP آن است که برای دریافت و ارسال داده‌ها یا پیام پروتکل مذکور؛ پیام‌ها و داده‌ها را به بسته‌های کوچکتر وقابل حمل تر تبدیل می‌کند، سپس این بسته‌ها به مقصد انتقال داده می‌شود و در نهایت پیوند این بسته‌ها به یکدیگر که شکل اولیه پیام‌ها و داده‌ها را بخود می‌گیرد، صورت می‌گیرد.

یکی دیگر از ویژگی‌های مهم این پروتکل قابلیت اطمینان آن در انتقال پیام‌هاست یعنی این قابلیت که به بررسی و بازبینی بسته‌ها و محاسبه بسته‌های دریافت شده دارد. در ضمن این پروتکل فقط برای استفاده در شبکه اینترنت نمی‌باشد. بسیاری از سازمان و شرکت‌ها برای ساخت وزیر بنای شبکه خصوصی خود که از اینترنت جدا می‌باشد نیز در این پروتکل استفاده می‌کنند.

پروتکل سیستم ورودی و خروجی پایه شبکه Net Bios. واسطه یا رابطی است که توسط IBM¹ عنوان استانداردی برای دسترسی به شبکه توسعه یافته. این پروتکل داده‌ها را از لایه بالاترین دریافت کرده و آنها را به شبکه منتقل می‌کند. سیستم عاملی که با این پروتکل ارتباط برقرار می‌کند سیستم عامل شبکه NOS، نامیده می‌شود کامپیوتر‌ها از طریق کارت شبکه خود به شبکه متصل می‌شوند. کارت شبکه به سیستم عامل ویژه‌ای برای ارسال اطلاعات نیاز دارد. این سیستم عامل ویژه را BIOS² نامند که در حافظه ROM³ کارت شبکه ذخیره شده است. این پروتکل همچنین روشنی را برای دسترسی به شبکه‌ها با پروتکل‌های مختلف مهیا می‌کند. این پروتکل از سخت افزار شبکه مستقل است. این پروتکل مجموعه‌ای از فرامین لازم برای در خواست خدمات شبکه‌ای سطح پایین را برای برنامه‌های کاربردی فراهم می‌کند تا جلسات لازم برای انتقال اطلاعات در بین گره‌های یک شبکه را هدایت کنند.

در حال حاضر وجود Net BEUI⁴ Net BIOS⁵ امتیازی جدید می‌دهد که این امتیاز درواقع ایجاد گزینه انتقال استاندارد است و Net BEUI⁶ در شبکه‌های محلی بسیار رایج است. همچنین قابلیت انتقال سریع داده‌ها را نیز دارد. اما چون یک پروتکل غیر قابل هدایت است به شبکه‌های محلی محدود شده است.

ابزارهای اتصال دهنده^۲:

ابزارهای اتصال به یک شبکه اضافه می‌گردد تا عملکرد و گستره شبکه و توانایی‌های سخت افزاری شبکه را ارتقاء دهد. گستره وسیعی از ابزارهای اتصال در شبکه وجود دارند اما شما احتمالاً برای کار خود به ابزارهای ذیل نیازمند خواهید بود:

¹ Net BIOS Enhanced User Interface -
² Connectivity Devices -

۱. تکرار کننده: تکرار کننده وسیله‌ای است که برای اتصال چندین سگمنت یک شبکه محلی بمنظور افزایش وسعت مجاز آن شبکه مورد استفاده قرار می‌گیرد. هر تکرار کننده از درگاه ورودی^۱ خود داده‌ها را پذیرفته و با تقویت آنها، داده‌ها را به درگاهی خروجی خود ارسال می‌کند. یک تکرار کننده در لایه فیزیکی مدل OSI عمل می‌کند. هر کابل یا سیم بکار رفته در شبکه که عنوان محلی برای عبور و مرور سیگنال هاست آستانه‌ای دارد که در آن آستانه سرعت انتقال سیگنال کاهش می‌یابد و در اینجا تکرار کننده عنوان ابزاری است که این سرعت عبور را در طول رسانه انتقال تقویت می‌کند.

۲. هاب: ابزاری هستند در شبکه که برای اتصال یک یا بیش از دو ایستگاه کاری به شبکه مورد استفاده قرار می‌گیرد و یک ابزار معمول برای اتصال ابزارهای شبکه است. هابها معمولاً برای اتصال سگمنت‌های شبکه محلی استفاده می‌شوند. یک هاب دارای درگاهی‌های چند گانه است. وقتی یک بسته در یک درگاهی وارد می‌شود به سایر درگاهی‌ها کپی می‌شود تا اینکه تمامی سگمنت‌های شبکه محلی بسته‌ها را ببینند. سه نوع هاب رایج وجود دارد:

- هاب فعال: که مانند آمپلی فایر عمل می‌کند و باعث تقویت مسیر عبور سیگنال‌ها می‌شود و از تصادم و برخورد سیگنال‌ها در مسیر جلوگیری بعمل می‌آورد. این هاب نسبتاً قیمت بالایی دارد.
- غیر فعال: که بر خلاف نوع اول که در مورد تقویت انتقال سیگنال‌ها فعال است این هاب منفعل است.
- آمیخته: که قادر به ترکیب انواع رسانه‌ها کابل کواکسیال نازک، ضخیم و... بوده و باعث تعامل درون خطی میان سایر هابها می‌شود.

۳. مسیریاب: در شبکه سازی فرایند انتقال بسته‌های اطلاعاتی از یک منبع به مقصد عمل مسیریابی است که تحت عنوان ابزاری تحت عنوان مسیریاب انجام می‌شود. مسیریابی یک شاخصه کلیدی در اینترنت است زیرا که باعث می‌شود پیام‌ها از یک کامپیوتر به کامپیوتر دیگر منتقل شوند. این عملکرد شامل تجزیه و تحلیل مسیر برای یافتن بهترین مسیر است. مسیریاب ابزاری است که شبکه‌های محلی را بهم متصل می‌کند یا به بیان بهتر بیش از دو شبکه را بهم متصل می‌کند. مسیریاب بر حسب عملکردش به دو نوع زیر تقسیم می‌شود:

- مسیریاب ایستا: که در این نوع، جدول مسیریابی توسط مدیر شبکه که تعیین کننده مسیر می‌باشد بطور دستی مقدار دهی می‌شود.
- مسیریاب پویا: که در این نوع، جدول مسیریابی خودش را، خود تنظیم می‌کند و بطور اتوماتیک جدول مسیریابی را روز آمد می‌کند.

۴. دروازه^۲: دروازه‌ها در لایه کاربرد مدل OSI عمل می‌کنند. کاربرد آن تبدیل یک پروتکل به پروتکل دیگر است. زمانیکه که در ساخت شبکه، هدف استفاده از خدمات اینترنت است، دروازه‌ها مقوله‌های مطرح در شبکه سازی خواهند بود.

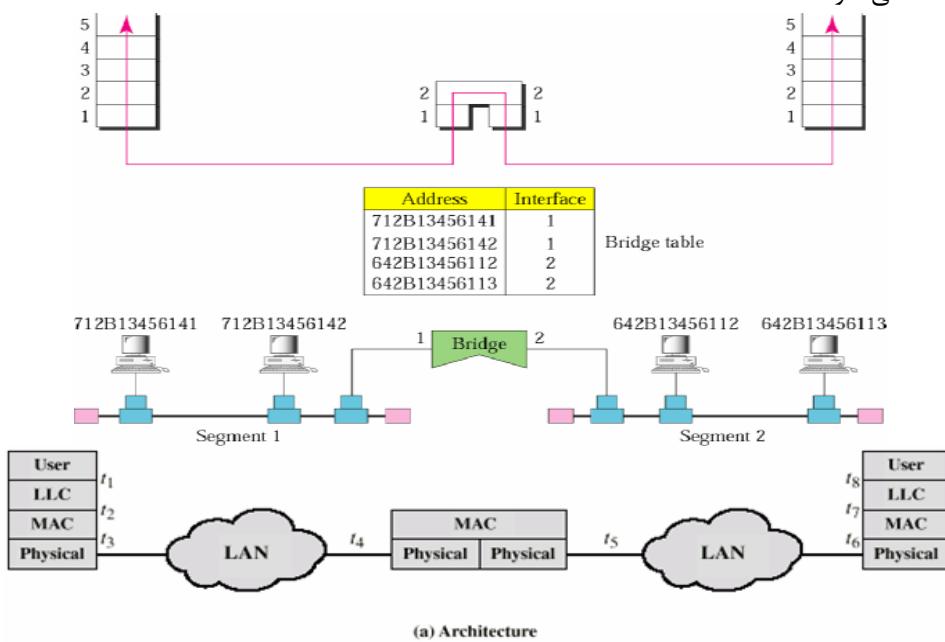
۵. پل: یک پل برای اتصال سگمنت‌های یک شبکه "همگن" به یکدیگر مورد استفاده قرار می‌گیرد. یک پل در لایه پیوند داده‌ها، عمل می‌کند. پل‌ها فریم‌ها را بر اساس آدرس مقصدشان ارسال می‌کنند. آنها همچنین می‌توانند جریان داده‌ها را کنترل نموده و خطاهایی را که در حین

۱ Port –

۲ Gateway –

ارسال داده ها رخ می دهد. عملکرد پل عبارتست از تجزیه و تحلیل آدرس مقصد یک فریم ورودی و اتخاذ تصمیم مناسب برای ارسال آن به ایستگاه مربوطه.

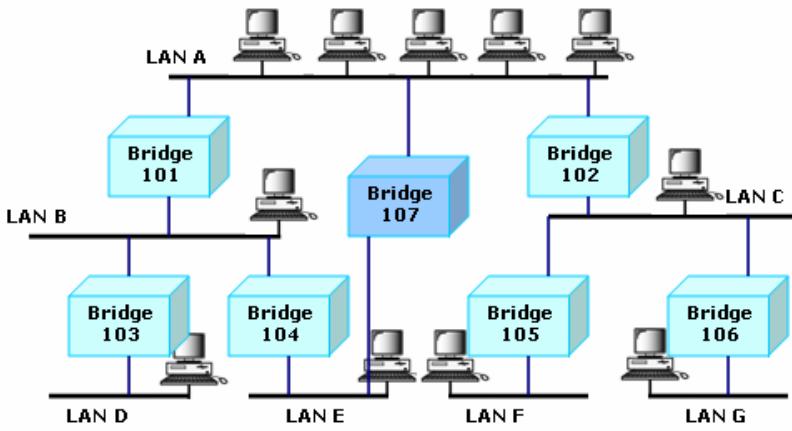
پل ها قادر به فیلتر کردن فریم ها می باشند. فیلتر کردن فریم برای حذف فریم های عمومی یا همگانی که غیر ضروری هستند مفید می باشد، پل ها قابل برنامه ریزی هستند و می توان آنها را به گونه ای برنامه ریزی کرد که فریم های ارسال شده از طرف منابع خاصی را حذف کنند. با تقسیم یک شبکه بزرگ به چندین سگمنت و استفاده از یک پل برای اتصال آنها به یکدیگر، توان عملیاتی شبکه افزایش خواهد یافت. اگر یک سگمنت شبکه از کار بیفت، سایر سگمنت های متصل به پل می توانند شبکه را فعال نگه دارند، پل ها موجب افزایش وسعت شبکه محلی می شوند.



تصویر ۱-۴: ساختار تبادل داده بین سگمنت های شبکه با استفاده از پل

موارد استفاده از پل:

- افزایش فاصله سگمنت های شبکه
- توانایی فیلتر کردن (لایه ۲) و دسته بندی بسته ها در بخش های مختلف شبکه
- اتصال دو LAN متفاوت به یکدیگر



تصویر ۱-۵: دستیابی چندگانه در شبکه

یکی از مسائلی که در LAN ها مورد توجه است این است که ممکن است از چند مسیر (از طریق چند پل) بتوان به یک LAN دسترسی پیدا کرد (مثل LAN E در شکل فوق). برای این کار باید از مسیریابی استفاده کرد. پل به دو نوع است: Transparent Source Routing یا Source Routing در آدرس پل مورد نظر را در بسته قرار می‌گیرد. در Source Routing خود پل ها اطلاعات با هم رد و بدل می‌کنند.

BPU(Bridge Protocol Data Unit)

در این روش از Spanning Tree استفاده می‌شود تا از دو مسیری یا چند مسیری جلو گیری شود. برای به وجود آوردن درخت Spanning سه مرحله وجود دارد:

- 1) Spanning Tree
- 2) Address Learning
- 3) Frame Forwarding

پل ها بسته هایی را با هم رد و بدل می‌کنند و تاخیر خود را از پلهای دیگر و همچنین هزینه مسیر را اندازه گیری می‌کنند. بدین ترتیب درخت Spanning ساخته می‌شود.

۶. سوئیچ: سوئیچ نوع دیگری از ابزارهایی است که برای اتصال چند شبکه محلی به یکدیگر مورد استفاده قرار می‌گیرد که باعث افزایش توان عملیاتی شبکه می‌شود. سوئیچ وسیله‌ای است که دارای درگاه‌های متعدد است که بسته ها را از یک درگاه می‌پذیرد، آدرس مقصد را بررسی می‌کند و سپس بسته ها را به درگاه مورد نظر که متعلق به ایستگاه میزبان با همان آدرس مقصد می‌باشد، ارسال می‌کند. اغلب سوئیچ‌های شبکه محلی در لایه پیوند داده‌های مدل OSI عمل می‌کند.

سوئیچ‌ها بر اساس کاربردشان به متقارن^۱ و نامتقارن^۲ تقسیم می‌شوند. در نوع متقارن، عمل سوئیچینگ بین سگمنت‌هایی که دارای پهنهای باند یکسان هستند انجام می‌دهد یعنی ۱۰ Mbps به ۱۰ Mbps سوئیچ خواهد شد. اما در نوع نامتقارن این عملکرد بین سگمنت‌هایی با پهنهای باند متفاوت انجام می‌شود. دو نوع سوئیچ وجود دارد که عبارتند از :

¹Symmetric
²Asymmetric

▪ سوئیچ Cut-through : این نوع سه یا چهار بایت اول یک بسته را می خواند تا آدرس مقصد آنرا بدست آورد ، آنگاه آن بسته را به سگمنت دارای آدرس مقصد مذکور ارسال می کند این در حالی است که قسمت باقی مانده بسته را از نظر خطایابی مورد بررسی قرار نمی دهد.

▪ سوئیچ Store-and-forward : این نوع ابتدا کل بسته را ذخیره کرده سپس آن را خطایابی می کند ، اگر بسته ای دارای خطایابی بود آن بسته را حذف می کند ، در غیر اینصورت آن بسته را به مقصد مربوطه ارسال خواهد کرد. این نوع برای شبکه محلی بسیار مناسبتر از نوع اول است زیرا بسته های اطلاعاتی خراب شده را پاکسازی می کند و بهمین دلیل این سوئیچ باعث کاهش بروز عمل تصادف خواهد شد.

، تکرار کننده و پل، بخش‌های مختلف یک LAN را به هم‌دیگر متصل می کند، اما مسیریاب، LAN ها و WAN های مختلف را به هم‌دیگر پیوند می دهد (Internetworking).

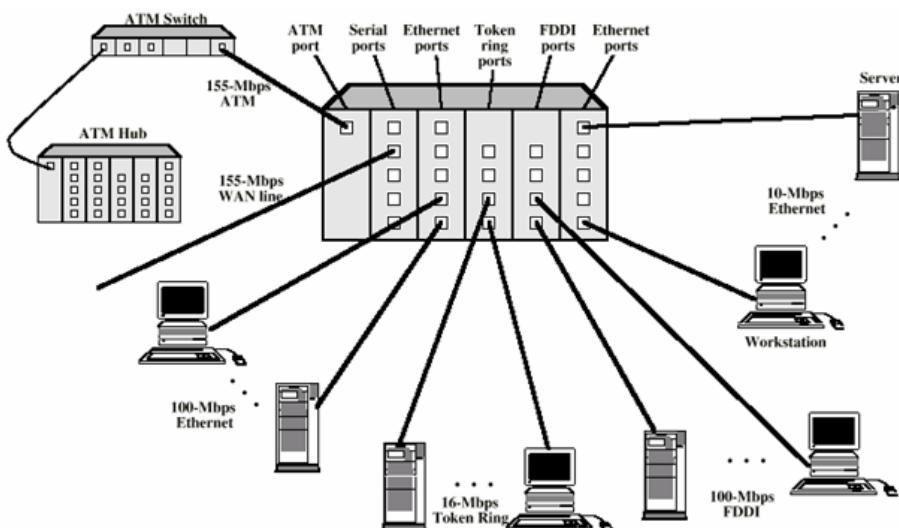
نسل های مختلف LAN :

• نسل اول : CSMA/CD که برای شبکه های اترنت و اترنوت سریع می باشد .

• نسل دوم : شبکه های FDDI .

• نسل سوم : ATM LAN .

یک هاب به صورت چند پروتکلی می باشد؛ یعنی پورتهای برای اترنوت CSMA/CD ، پورتهای برای FDDI و ... دارد .



تصویر ۱-۶: هاب ATM LAN

به خاطر نرخ داده بسیار بالای ATM ، این شبکه ها روبه رو رشد هستند . پورتهای مختلف می توانند نرخ داده های مختلف داشته باشند . برای افزایش سرعت و کاهش پهنای باند از MLT استفاده می شود . یعنی تغییرات جزئی در نظر گرفته نمی شود و تغییر سیگنالهای بزرگ در نظر گرفته می شود. شبکه های محلی ATM سه نوع دارند:

1. شبکه های ATM محلی خالص : هر نود مستقیماً به سوئیچ ATM متصل است.
2. شبکه های مرسوم ATM : شبکه های غیر ATM از طریق مبدلها بی به سوئیچ ATM متصل می باشند.

۳. شبکه های ATM با ساختار ترکیبی : شبکه های متصل به سوئیچ ATM بصورت ترکیبی از دو نوع بالا هستند.

مفاهیم مربوط به ارسال سیگنال و پهنهای باند:

پهنهای باند^۱ ، به تفاوت بین بالاترین و پایین ترین فرکانس هایی که یک سیستم ارتباطی می تواند ارسال کند گفته می شود. به عبارت دیگر منظور از پهنهای باند مقدار اطلاعاتی است که می تواند در یک مدت زمان معین ارسال شود. برای وسائل دیجیتال، پهنهای باند بحسب بیت در ثانیه و یا بایت در ثانیه بیان می شود. برای وسائل آنالوگ، پهنهای باند، بحسب سیکل در ثانیه بیان می شود. دو روش برای ارسال اطلاعات از طریق رسانه های انتقالی وجود دارد که عبارتند از: روش ارسال مبتنی بر باند^۲ و روش ارسال باند پهن^۳.

در یک شبکه LAN، کابلی که کامپیوترها را به هم وصل می کند، فقط می تواند در یک زمان یک سیگنال را از خود عبور دهد، به این شبکه یک شبکه مبتنی بر باند می گوئیم. به منظور عملی ساختن این روش و امکان استفاده از آن برای همه کامپیوترها، داده ای که توسط هر سیستم انتقال می یابد، به واحد های جداگانه ای به نام بسته^۴، شکسته می شود. در واقع در کابل یک شبکه LAN، توالی بسته های تولید شده توسط سیستم های مختلف را شاهد هستیم که به سوی مقاصد گوناگونی در حرکت اند.

برای مثال وقتی کامپیوتر شما یک پیام پست الکترونیکی را انتقال می دهد، این پیام به بسته های متعددی شکسته می شود و کامپیوتر هر بسته را جداگانه انتقال می دهد. کامپیوتر دیگری در شبکه که بخواهد به انتقال داده بپردازد نیز در یک زمان یک بسته را ارسال می کند. وقتی تمام بسته هایی که بر روی هم یک انتقال خاص را تشکیل می دهند، به مقصد خود می رستند، کامپیوتر دریافت کننده آنها را به شکل پیام الکترونیکی اولیه بر روی هم می چیند. این روش پایه و اساس شبکه های سوئیچ بسته ای می باشد که در فصل ۴ در مورد آن بیشتر توضیح داده می شود.

در مقابل روش مبتنی بر باند، روش ارسال باند پهن قرار دارد. در روش اخیر، در یک زمان و در یک کابل، چندین سیگنال حمل می شوند. از مثالهای شبکه ارسال باند پهن که ما هر روز از آن استفاده می کنیم، شبکه تلویزیون است. در این حالت فقط یک کابل به منزل کاربران کشیده می شود، اما همان یک کابل، سیگنالهای مربوط به کانالهای متعدد تلویزیون را بطور همزمان حمل می نماید. از روش ارسال باند پهن به طور روز افزونی در شبکه های WAN استفاده می شود.

از آنجاییکه در شبکه های LAN در یک زمان از یک سیگنال پشتیبانی می شود، در یک لحظه داده ها تنها در یک جهت حرکت می کنند. به این ارتباط Half-Duplex گفته می شود. در مقابل به سیستم هایی که می توانند بطور همزمان در دو جهت با هم ارتباط برقرار کننده Full-Duplex گفته می شود. مثالی از این نوع ارتباط شبکه تلفن می باشد. شبکه های LAN با داشتن تجهیزاتی خاص بصورت Full-Duplex عمل کنند.

کابل شبکه:

پیش از اینکه در مورد انواع کابل ها و پهنهای باند مربوط به آنها، به بحث بپردازیم، ذکر این نکته ضروری است که نوع کابل انتخابی شما بطور مستقیم به تپیلوژی شبکه تان وابسته است. در این قسمت سعی گردیده تپیلوژی مناسب با هر نوع کابل ذکر شود. کابل شبکه، رسانه ای است که از طریق آن، اطلاعات از یک دستگاه موجود در شبکه به دستگاه دیگر انتقال می یابد. انواع مختلفی از کابلها بطور معمول در شبکه های LAN استفاده می شوند. در برخی موارد شبکه تنها از یک نوع کابل استفاده می کند، اما گاه انواعی از کابلها در شبکه به کار گرفته می شود. غیر

BandWitdh - ^۱

Baseband - ^۲

Broadband - ^۳

Packet - ^۴

از عامل توپولوژی، پروتکل و اندازه شبکه نیز در انتخاب کابل شبکه مؤثرند. آگاهی از ویژگیهای انواع مختلف کابلها و ارتباط آنها با دیگر جنبه های شبکه برای توسعه یک شبکه موفق ضروری است. امروزه سه گروه از کابلها، در ایجاد شبکه مطرح هستند:

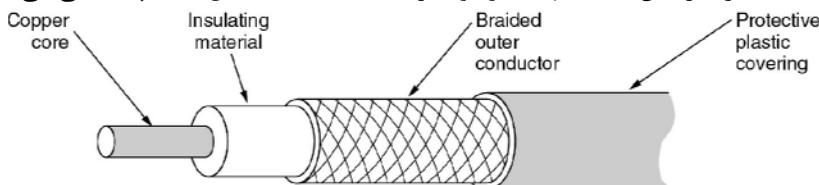
کابلهای کواکسیال زمانی بیشترین مصرف را در میان کابلهای موجود در شبکه داشت. چند دلیل اصلی برای استفاده زیاد از این نوع کابل وجود دارد:

- قیمت ارزان آن.

- سبکی و انعطاف‌پذیری.

- این نوع کابل به نسبت زیادی در برابر سیگنالهای مداخله‌گر مقاومت می‌نماید.

- مسافت بیشتری را بین دستگاههای موجود در شبکه، نسبت به کابل UTP پشتیبانی می‌نماید.



تصویر ۱-۷: کابل کواکسیال

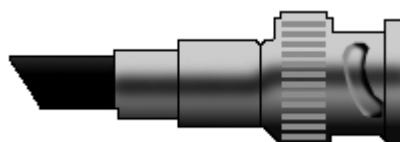
اجزای کابل کواکسیال بشرح زیر می‌باشد:

- Conducting Core یا هسته مرکزی که معمولاً از یک رشته سیم جامد مسی تشکیل می‌گردد.
- Insulation یا عایق که معمولاً از جنس PVC یا تفلون است.
- Copper Wire Mesh که از سیم‌های بافته شده تشکیل می‌شود و کار آن جمع‌آوری امواج الکترومغناطیسی است.
- Jacket که جنس آن اغلب از پلاستیک بوده و نگهدارنده خارجی سیم در برابر خطرات فیزیکی است.

کابل کواکسیال به دو دسته تقسیم می‌شود:

- Thin net: کابلی است بسیار سبک، انعطاف‌پذیر و ارزان قیمت، قطر سیم در آن ۶ میلیمتر معادل ۰/۲۵ اینچ است. مقدار مسیری که توسط آن پشتیبانی می‌شود ۱۸۵ متر است.
- Thick net: این کابل قطری تقریباً ۲ برابر Thin net دارد. کابل مذکور، پوشش محافظی را (علاوه بر محافظ خود) داراست که از جنس پلاستیک بوده و بخار را از هسته مرکزی دور می‌سازد.

raig ترین نوع اتصال دهنده مورد استفاده در کابل کواکسیال، BNC^۱ می‌باشد. انواع مختلفی از سازگار کننده‌ها برای BNC‌ها وجود دارند شامل: Terminator, Tconnector, Barrel connector.



تصویر ۱-۸: اتصال دهنده BNC

در شبکه هایی با توپولوژی Bus از کابل کواکسیال استفاده می‌شود.

¹ Bayonet-Neill-Concelman -

باید دانست که از عبارتهایی مانند Base 10 برای توضیح اینکه چه کابلی در ساخت شبکه بکار رفته استفاده می‌گردد. عبارت مذکور بدان معناست که از کابل کواکسیال و از نوع Thick net استفاده شده، علاوه بر آن روش انتقال در این شبکه، روش ارسال باند پهن است و نیز سرعت انتقال ۱۰ مگابیت در ثانیه می‌باشد. همچنین Base 2 ۱۰ یعنی اینکه از کابل Thin net استفاده شده، روش انتقال مبتنی بر باند و سرعت انتقال ۱۰ مگابیت در ثانیه است.

در طراحی جدید شبکه معمولاً از کابل‌های زوج سیم به هم تابیده شده^۱، استفاده می‌گردد. قیمت آن ارزان بوده و از نمونه‌های آن می‌توان به کابل تلفن اشاره کرد. این نوع کابل که از چهار جفت سیم بهم تابیده تشکیل می‌گردد، خود به دو دسته تقسیم می‌شود:

- UTP^۲: کابل ارزان قیمتی است که نصب آسانی دارد و برای شبکه‌های LAN سیم بسیار مناسبی است، همچنین نسبت به نوع دوم کم وزن‌تر و انعطاف‌پذیرتر است. مقدار سرعت دیتای عبوری از آن ۴ مگابیت در ثانیه تا ۱۰۰ مگابیت در ثانیه می‌باشد. این کابل می‌تواند تا مسافت حدوداً ۱۰۰ متر یا ۳۲۸ فوت را بدون افت سیگنال انتقال دهد. کابل مذکور نسبت به تداخل امواج الکترومغناطیس حساسیت بسیار بالایی دارد و در نتیجه در مکانهای دارای امواج الکترومغناطیس، امکان استفاده از آن وجود ندارد.

در سیم تلفن که خود نوعی از این کابل است از اتصال دهنده RJ11 استفاده می‌شود، اما در کابل شبکه اتصال دهنده‌ای با شماره RJ45 بکار می‌رود که دارای هشت مکان برای هشت رشته سیم است.



تصویر ۹-۱: اتصال دهنده RJ45

کابل UTP دارای هفت طبقه مختلف است. CAT1 یا نوع اول کابل UTP برای انتقال صدا بکار می‌رود، اما CAT2 تا CAT5 برای انتقال دیتا در شبکه‌های کامپیوتری مورد استفاده قرار می‌گیرند و سرعت انتقال دیتا در آنها به ترتیب عبارتست از: ۴ مگابیت در ثانیه، ۱۰ مگابیت در ثانیه، ۱۶ مگابیت در ثانیه و ۱۰۰ مگابیت در ثانیه. برای شبکه‌های کوچک و خانگی استفاده از کابل CAT3 توصیه می‌شود.



(a)



(b)

تصویر ۱۰-۱: کابل UTP نوع (a)^۳ و نوع (b)^۴

- در این کابل سیم‌های انتقال دیتا مانند UTP هشت سیم و یا چهار جفت دوتایی هستند. باید دانست که تفاوت آن با UTP در این است که پوسته‌ای به دور آن پیچیده شده که از اثربداری امواج بر روی دیتا جلوگیری می‌کند. از لحاظ قیمت، این کابل از UTP گرانتر و از فیبر نوری ارزان‌تر است. مقدار مسافتی که کابل

¹ Twisted Pair -	² Unshielded Twisted Pair -
³ Shielded Twisted Pair -	

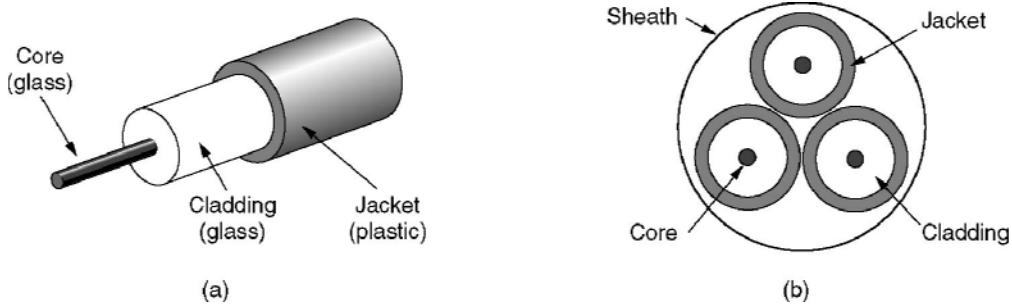
مذکور بدون افت سیگنال طی می کند برابر با ۵۰۰ متر معادل ۱۶۴۰ فوت است. در شبکه هایی با توپولوژی اتو بوسی و حلقه ای از دو نوع اخیر استفاده می شود. گفته شد که در این نوع کابل، ۴ جفت سیم بهم تابیده بکار می رود که از دو جفت آن یکی برای فرستادن اطلاعات و دیگری برای دریافت اطلاعات عمل می کنند.

در شبکه هایی با نام اترنت سریع دو نوع کابل به چشم می خورد:

- ۱۰۰ Base TX: یعنی شبکه ای که در آن از کابل UTP نوع CAT5 استفاده شده و عملاً دو زوج سیم در انتقال دیتا دخالت دارند (دو زوج دیگر بیکار می مانند)، سرعت در آن ۱۰۰ مگابیت در ثانیه و روش انتقال مبتنی بر باند است.
- ۱۰۰ Base T4: تنها تفاوت آن با نوع بالا این است که هر چهار جفت سیم در آن بکار گرفته می شوند.

کابل فیبر نوری کاملاً متفاوت از نوع کواکسیال و زوج سیم بهم تابیده شده، عمل می کند. به جای اینکه سیگنال الکتریکی در داخل سیم انتقال یابد، پالسهایی از نور در میان پلاستیک یا شیشه انتقال می یابد. این کابل در برابر امواج الکترومغناطیس کاملاً مقاومت می کند و نیز تأثیر افت سیگنال بر اثر انتقال در مسافت زیاد را بسیار کم در آن می توان دید. برخی از انواع کابل فیبر نوری می توانند تا ۱۲۰ کیلومتر انتقال داده انجام دهند. همچنین امکان به تله انداختن اطلاعات در کابل فیبر نوری بسیار کم است. کابل مذکور دو نوع را در بر می گیرد:

- حالت تنها^۱: که در این کابل دیتا با کمک لیزر انتقال می یابد و بصورت ۱۲۵/۸,۳ نشان داده می شود که در آن ۸,۳ میکرون قطر فیبر نوری و ۱۲۵ میکرون مجموع قطر فیبر نوری و محافظ آن می باشد. این نوع انعطاف پذیری کم و قیمت بالایی دارد برای شبکه های تلویزیونی و تلفنی استفاده می گردد.
- حالت چندگانه^۲: که در آن دیتا بصورت پالس نوری انتقال می یابد و بصورت ۱۲۵/۶۲,۵ نشان داده می شود که در آن ۶۲,۵ میکرون قطر فیبر نوری و ۱۲۵ میکرون مجموع قطر فیبر نوری و محافظ آن می باشد. این نوع مسافت کوتاه تر را نسبت به حالت تنها طی می کند و قابلیت انعطاف پذیری بیشتری دارد. قیمت آن نیز ارزان تر است و در شبکه های کامپیوتری استفاده می شود. بطور کلی کابل فیبر نوری نسبت به دو نوع کواکسیال و زوج سیم بهم تابیده قیمت بالایی دارد و نیز نصب آن نیاز به افراد ماهری دارد. شبکه های ۱۰۰ Base FX، شبکه هایی هستند که در آنها از فیبر نوری استفاده می شود، سرعت انتقال در آنها ۱۰۰ مگابیت در ثانیه بوده و روش انتقال مبتنی بر باند می باشد. امروز، با پیشرفت تکنولوژی در شبکه های فیبر نوری می توان به سرعت ۱۰۰۰ مگابیت در ثانیه دست یافت. در شکل صفحه بعد یک کابل فیبر نوری مشاهده می شود.



تصویر ۱۱-۱: نمونه های غلاف تکی و سه تایی فیبر نوری

بطور کلی توصیه هایی در مورد نصب کابل شبکه وجود دارد:

Single Mode - ^۱

Multi Mode - ^۲

- همیشه بیشتر از مقدار مورد نیاز کابل تهیه کنید.
- هر بخشی از شبکه را که نصب می‌کنید، آزمایش نمایید. ممکن است بخشهایی در شبکه وجود داشته باشند که خارج ساختن آنها پس از مدتی دشوار باشد.
- اگر لازم است بر روی زمین کابل کشی نمایید، کابلها را بوسیله حفاظت‌کننده‌هایی بپوشانید.
- دو سر کابل را نشانه‌گذاری کنید.

کارت شبکه^۱:

کارت شبکه یا NIC، که عموماً در شیارهای گسترش^۲ کامپیوتر قرار می‌گیرد، وسیله‌ای است که بین کامپیوتر و شبکه‌ای که کامپیوتر جزئی از آن است، اتصال برقرار می‌نماید. هر کامپیوتر در شبکه می‌باشد یک کارت شبکه داشته باشد که به باس گسترش سیستم^۳ اتصال می‌باید و برای کابل شبکه به عنوان یک واسطه عمل می‌کند. در برخی کامپیوتراها، کارت شبکه با مادربرد یکی شده است، اما در بیشتر مواقع شکل یک کارت گسترش را به خود می‌گیرد که یا به ISA^۴ و یا به PCI^۵ متصل می‌گردد. کارت شبکه به همراه نرم‌افزار راه اندازی آن، مسئول اکثر کارکردهای لایه پیوند داده و لایه فیزیکی می‌باشد. کارت‌های شبکه، بسته به نوع کابلی که پشتیبانی می‌کنند، اتصال دهنده‌های خاصی را می‌طلبند (کابل شبکه از طریق یک اتصال دهنده به کارت شبکه وصل می‌شود). برخی کارت‌های شبکه بیش از یک نوع اتصال دهنده دارند که این شما را قادر می‌سازد که آنها را به انواع مختلفی از کابل‌های شبکه اتصال دهید.

عملکردهای اساسی کارت شبکه:

کارت شبکه عملکردهای گوناگونی را که برای دریافت و ارسال داده‌ها در شبکه حیاتی هستند، انجام می‌دهد که برخی از آنها عبارتند از:

- محصورسازی داده: کارت شبکه و درایور (راهانداز) آن، مسئول ایجاد فریم در اطراف داده تولید شده توسط لایه شبکه و آماده‌سازی آن برای انتقال هستند.
- کدگذاری و کد برداری سیگنال: در واقع کارت شبکه طرح کدگذاری لایه فیزیکی را پیاده می‌کند و داده‌های دودویی تولید شده توسط لایه شبکه را به سیگنال‌های الکترونیکی قابل انتقال بر روی کابل شبکه تبدیل می‌نمایند. همچنین سیگنال‌های دریافتی از روی کابل را برای استفاده لایه‌های بالاتر به داده‌های دودویی تبدیل می‌سازد.
- ارسال و دریافت داده: کارکرد اساسی کارت شبکه، تولید و انتقال سیگنال‌های مناسب در شبکه و دریافت سیگنال‌های ورودی است. طبیعت سیگنال‌ها به کابل شبکه و پروتکل لایه پیوند داده بستگی دارد. در یک LAN فرضی، هر کامپیوتر هم بسته‌های عبوری در شبکه را دریافت می‌کند و کارت شبکه آدرس مقصد لایه پیوند داده را بررسی می‌کند تا ببیند آیا بسته برای کامپیوتر مذکور فرستاده شده یا خیر. در صورت مثبت بودن پاسخ، کارت شبکه بسته را برای انجام پردازش توسط لایه بعدی از کامپیوتر عبور می‌دهد، در غیر اینصورت بسته را به دور می‌افکند.

Network Interface Adapter - ^۱

Expansion Slot - ^۲

Expansion Bus System's - ^۳

Industry Standard Architecture - ^۴

peripheral component interconnect - ^۵

کارت شبکه قابل نقل و انتقال^۱ :

بسیار احتمال دارد که در شبکه شما یک کامپیوتر کیفی و قابل حمل وجود داشته باشد. گستره وسیعی از کارت شبکه‌های مناسب این کامپیوترها قابل دستیابی است. نوعی از کارت شبکه که در کامپیوترهای کیفی استفاده می‌شود عبارتست از: کارت PCMCIA یا همان PC Card.

PC Card در یک شیار و یا در یک جفت شیار موجود در کناره کامپیوتر کیفی جای می‌گیرد. کابل شبکه با استفاده از ابزاری به نام Dongle به کارت PC متصل می‌شود. کارتهای PC جز ابزارهای Plug-and-Play هستند، و نیز می‌توان در حالیکه کامپیوتر روشن و در حال فعالیت است، آنها را نصب یا خارج نمود و پس از نصب آنها نیازی به Restart کردن کامپیوتر نیست.

شبکه خصوصی مجازی(VPN²):

شبکه خصوصی مجازی(VPN)، امکانی است برای انتقال ترافیک خصوصی بر روی شبکه عمومی. معمولاً از VPN برای اتصال دو شبکه خصوصی از طریق یک شبکه عمومی مانند اینترنت استفاده می‌شود. منظور از یک شبکه خصوصی شبکه‌ای است که بطور آزاد در اختیار و دسترس عموم نیست. VPN به این دلیل مجازی نامیده می‌شود که از نظر دو شبکه خصوصی، ارتباط از طریق یک ارتباط و شبکه خصوصی بین آنها برقرار است اما در واقع شبکه عمومی این کار را انجام می‌دهد. پیاده سازی VPN معمولاً اتصال دو یا چند شبکه خصوصی از طریق یک تونل رمزشده انجام می‌شود. در واقع به این وسیله اطلاعات در حال تبادل بر روی شبکه عمومی از دید سایر کاربران محفوظ می‌ماند. VPN را می‌توان بسته به شیوه پیاده سازی و اهداف پیاده سازی آن به انواع مختلفی تقسیم کرد.

VPN را می‌توان با توجه به استفاده یا عدم استفاده از رمزنگاری به دو گروه اصلی تقسیم کرد:

○ VPN رمزشده : های رمز شده از انواع مکانیزم‌های رمزنگاری برای انتقال امن اطلاعات بر روی

شبکه عمومی استفاده می‌کنند. یک نمونه خوب از این VPN ها، شبکه‌های خصوصی مجازی اجرا شده به کمک IPSec هستند.

○ VPN رمزشده : این نوع از VPN برای اتصال دو یا چند شبکه خصوصی با هدف استفاده از منابع

شبکه یکدیگر ایجاد می‌شود. اما امنیت اطلاعات در حال تبادل حائز اهمیت نیست یا این که این امنیت با روش دیگری غیر از رمزنگاری تأمین می‌شود. یکی از این روشها تفکیک مسیریابی است. منظور از تفکیک مسیریابی آن است که تنها اطلاعات در حال تبادل بین دو شبکه خصوصی به هر یک از آنها مسیر دهی می‌شوند. (MPLS VPN) در این موقع می‌توان در لایه‌های بالاتر از رمزنگاری مانند SSL استفاده کرد.

هر دو روش ذکر شده می‌توانند با توجه به سیاست امنیتی مورد نظر، امنیت مناسبی را برای مجموعه به ارمغان بیاورند، اما معمولاً VPN های رمز شده برای ایجاد VPN امن به کار می‌روند. سایر انواع VPN مانند MPLS VPN بستگی به امنیت و جامعیت عملیات مسیریابی دارند.

دسته بندی براساس لایه پیاده سازی:

VPN بر اساس لایه مدل OSI که در آن پیاده سازی شده اند نیز قابل دسته بندی هستند. این موضوع از اهمیت خاصی برخوردار است. برای مثال در VPN های رمز شده، لایه ای که در آن رمزنگاری انجام می‌شود در حجم ترافیک رمز شده تاثیر دارد. همچنین سطح شفافیت VPN برای کاربران آن نیز با توجه به لایه پیاده سازی مطرح می‌شود.

Portable Computer Network Adapters - ^۱
Network Virtual Private - ^۲

- لایه پیوند داده : با استفاده از VPN های لایه پیوند داده می توان دو شبکه خصوصی را در لایه ۲ مدل OSI با استفاده از پروتکلهای مانند ATM یا Frame Relay به هم متصل کرد. با وجودی که این مکانیزم راه حل مناسبی به نظر می رسد اما معمولاً روش ارزانی نیست چون نیاز به یک مسیر اختصاصی لایه ۲ دارد. پروتکلهای ATM و Frame Relay مکانیزمهای رمزنگاری را تامین نمی کنند. آنها فقط به ترافیک اجازه می دهند تا بسته به آن که به کدام اتصال لایه ۲ تعلق دارد، تفکیک شود. بنابراین اگر به امنیت بیشتری نیاز دارید باید مکانیزمهای رمزنگاری مناسبی را به کار بگیرید.
- لایه شبکه : این سری از VPN ها با استفاده از Tunneling لایه ۳ و/یا تکنیکهای رمزنگاری استفاده می کنند. برای مثال می توان به IPSec Tunneling و پروتکل رمزنگاری برای ایجاد VPN اشاره کرد. مثالهای دیگر پروتکلهای GRE و L2TP هستند. جالب است اشاره کنیم که L2TP در ترافیک لایه ۲ تونل می زند اما از لایه ۳ برای این کار استفاده می کند. بنابراین در VPN های لایه شبکه قرار می گیرد. این لایه برای انجام رمزنگاری نیز بسیار مناسب است. در بخش‌های بعدی این گزارش به این سری از VPN ها به طور مسروچ خواهیم پرداخت.
- لایه کاربرد : این VPN ها برای کار با برنامه های کاربردی خاص ایجاد شده اند. VPN های مبتنی بر SSL از مثالهای خوب برای این نوع از VPN هستند. SSL رمزنگاری را بین مرورگر وب و سروری که SSL را اجرا می کند، تامین می کند. SSH مثال دیگری برای این نوع از VPN ها است. SSH به عنوان یک مکانیزم امن و رمز شده برای login به اجزای مختلف شبکه شناخته می شود. مشکل VPN ها در این لایه آن است که هرچه خدمات و برنامه های جدیدی اضافه می شوند، پشتیبانی آنها در VPN نیز باید اضافه شود.

دسته بندی **VPN** براساس کارکرد تجاری

- VPN را برای رسیدن به اهداف تجاری خاصی ایجاد می شوند. این اهداف تجاری تقسیم بندی جدیدی را برای VPN بنا می کنند:
- اینترانتی : این سری از VPN ها دو یا چند شبکه خصوصی را در درون یک سازمان به هم متصل می کنند. این نوع از VPN زمانی معنا می کند که می خواهیم شعب یا دفاتر یک سازمان در نقاط دوردست را به مرکز آن متصل کنیم و یک شبکه امن بین آنها برقرار کنیم.
 - اکسٹرانتی : این سری از VPN ها برای اتصال دو یا چند شبکه خصوصی از دو یا چند سازمان به کار می روند. از این نوع VPN معمولاً برای سناریوهای B2B که در آن دو شرکت می خواهند به ارتباطات تجاری با یکدیگر بپردازنند، استفاده می شود.

بخش ۳: آدرس دهن

فصل ۲: آدرس دهی در شبکه های کامپیووتری

فصل ۳: مسیریابی در مسیریابها

فصل ۴: پروتکلهای مسیریابی در شبکه

فصل ۵: پروتکلهای Multicast و پروتکلهای Multicasting

فصل ۳:

آدرس دهنی در شبکه های کامپیووتری

آدرس در شبکه های کامپیوتری به سه نوع تقسیم می شود:

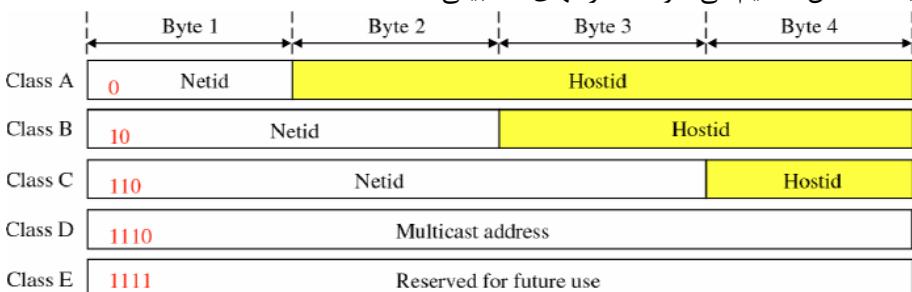
۱. آدرس فیزیکی (در لایه های فیزیکی و اتصال داده)

۲. آدرس IP (لایه شبکه)

۳. آدرس پورت (لایه حمل و نقل)

آدرسهای IP :

به ۵ کلاس تقسیم می شوند (آدرسهای ۳۲ بیتی هستند) :



IP Address Classes

کلاس A : در این کلاس ۱۲۷ شبکه می توان تعریف کرد که در هر شبکه ۱۶ میلیون HOST می تواند قرار بگیرد (این کلاس پر شده است) .

کلاس B : در این کلاس ۱۶۳۸۲ شبکه می توان تعریف کرد که هر شبکه ۲ به توان ۱۶ HOST می تواند داشته باشد.

کلاس C : در این کلاس ۲ میلیون شبکه می توان تعریف کرد که هر شبکه ۲ به توان ۸ HOST می تواند داشته باشد.

کلاس D : چهار بیت سمت چپ آن ۱۱۱۰ است ، این کلاس برای Multicast استفاده می شود . (یعنی می توان برای چند مقصد یک آدرس قرار داد و هر وقت بسته ای ارسال شود و آدرس Multicast در آن قرار داده شود ، همه مقصدها می توانند بسته را دریافت کنند)

آدرسهای گفته شده آدرسهای IP هستند که GLOBAL است. البته آدرس فیزیکی هم وجود دارد که آدرس ۴۸ بیتی کارت شبکه است .

برای راحتی و قابل حفظ بودن آدرسهای IP از DNS استفاده می شود . یعنی یک نام حوزه اختصاص داده می شود .

آدرسهای خاص:

• HostId=0 : آدرس شبکه.

• BroadcastHostId : آدرس تمام یک.

• 127.X.Y.Z : آدرس loop Back IP. بسته های با این آدرس از لایه IP برگردانده می شوند و به شبکه راه نمی یابند.

• 0.0.0.N : اگر دو Host در یک شبکه باشند و یکی از آنها بخواهد برای دیگری با آدرس

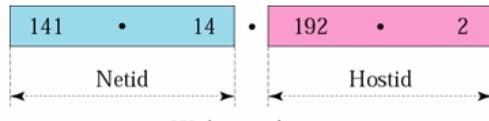
X.Y.Z.N پیامی را ارسال بکند می تواند از آدرس 0.0.0.N ۰.۰.۰.N جهت آدرس مقصد استفاده کند.

آدرس شبکه ، کلاس آدرس ، بلاک و دامنه آدرس در بلاک را مشخص می نماید. مثلاً 223.168.21.124 را در نظر بگیرید، بلاک آدرس شبکه آن 223.168.21.0 از کلاس C و دامنه آدرس آن 223.168.21.0 تا 223.168.21.225 می یابد.

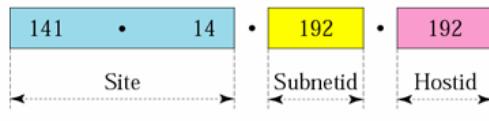
به Host یی که به دو شبکه متصل باشد ، Multihmode Device گفته می شود.

Broadcast مسقیم آدرس: پیامی است که توسط یک مسیریاب برای تمام Host های عضو شبکه محلی ارسال می گردد.

محدود آدرس: پیامی است که توسط یک Host داخل شبکه محلی برای سایر اعضای آن شبکه ارسال می‌گردد. این پیام فقط داخل همان شبکه است و مسیریابها در حین خروج از شبکه آن را بلاک می‌کنند. اگر بخواهیم از ساختار طبقاتی برای آدرس دهی در شبکه استفاده نمائیم باید از Subnet استفاده نمائیم:



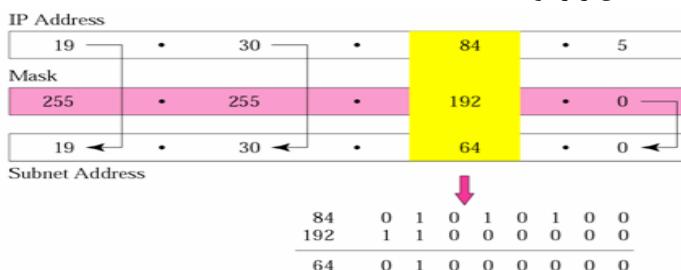
a. Without subnetting



b. With subnetting

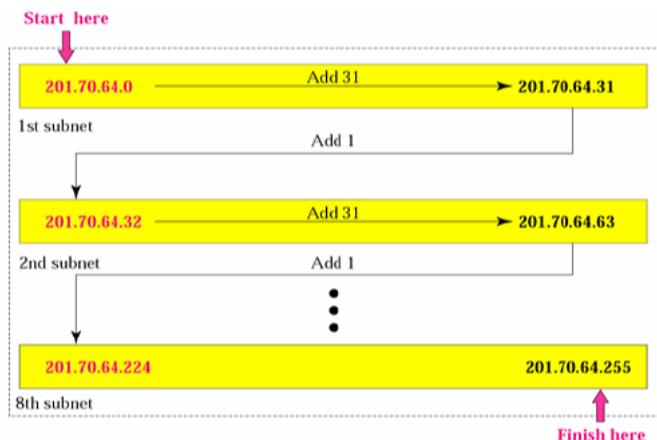
روشهای پیدا کردن Subnet

۱. صریح(Straight): آدرس IP را با آدرس Mask شبکه بیت به بیت AND می‌شود.
۲. میانبر(Shortcut): قسمتهایی از آدرس IP که مقدار معادل آن در Mask ۲۵۵ است را عیناً در Subnet کپی می‌کنیم. برای قسمتهایی از Mask که مقدار ۰ دارند، مقدار صفر را در Subnet موقعیت معادل آن کپی می‌کنیم. برای سایر قسمتها، مقدار IP را با Mask، بیت به بیت AND می‌کنیم. به مثال زیر توجه نمایید:



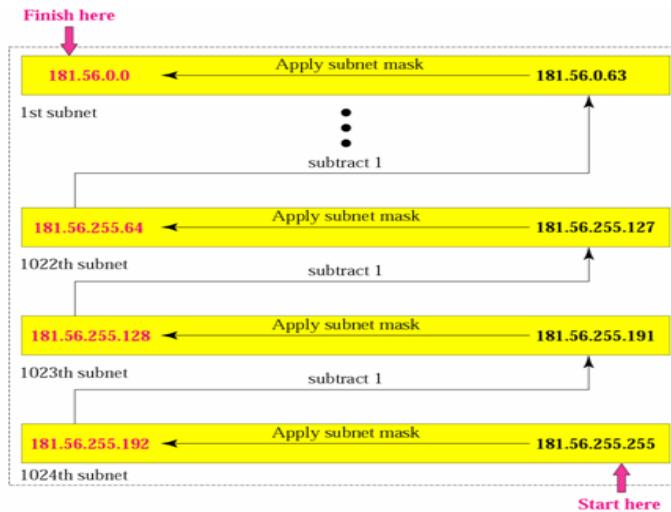
تعداد Subnet ها توانی از دو است و بنابراین تعداد یکهای نمایش دودویی Subnet برابر با مجموع تعداد یکهای نمایش دودویی Mask پیش فرض شبکه و تعداد یکهای نمایش دودویی Subnet می‌باشد. مثال: یک شرکت فضای آدرس 201.70.64.0 را دارد(کلاس C) و درخواست ۶ Subnet دارد. از آنجاییکه ۶ توانی از ۲ نیست، کوچکترین عدد توان ۲ که عدد ۸ است را در نظر می‌گیریم. تعداد یکهای Mask پیش فرض ۲۴ می‌باشد. بنابراین تعداد یکهای Mask ۲۴+۳=۲۷ Subnet می‌باشد و تعداد صفرها ۳۲-۲۷=۵ می‌باشد. بنابراین ۸ Subnet Mask هر کدام با $2^5=32$ آدرس خواهیم داشت. Subnet Mask در این حالت برابر است با:

255.255.255.224 11111111 11111111 11111111 11100000

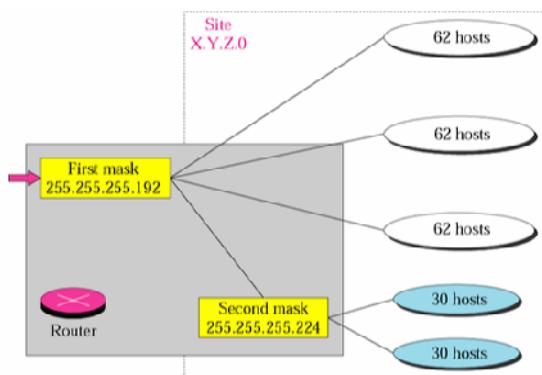


مثال: یک شرکت فضای آدرس 181.56.0.0 (کلاس B) را دارد. این شرکت نیازمند 1000 Subnet می باشد. این Subnet را طراحی کنید.

تعداد یکهای Mask پیش فرض 16 می باشد. 1000 توانی از 2 نیست. اولین عدد توان 2، 1024 است. بنابراین نیازمند 10 یک دیگر در Subnet Mask هستیم ($10 = 2^3 + 1 = 2^6 - 6$). تعداد صفرها نیز 6 است. بنابراین عبارتست از: 11111111 11111111 11111111 110000000 Subnet Mask 255.255.255.192 یا 192.168.1.11111111 11111111 11111111 110000000. تعداد Subnet ها 1024 هست، هر 2⁶ آدرس.



می توان Subnet هایی در Subnet هایی ایجاد شده بوجود آورد (Subnet با طول متغیر)



شرکتهای بسیاری وجود دارند که دارای تعداد زیادی آدرس شبکه متفاوت هستند. Supernetting تکنیکی است که می توان این فضاهای آدرس متفاوت را یکپارچه نمود. قوایین حاکم بر Supernet عبارتند از:

- تعداد بلاکها باید توانی از 2 باشد.
- فضای آدرس بلاکها باید پیوسته باشد.
- بایت سوم آدرس اول باید بر تعداد بلاکها، قابل تقسیم باشد.

مثال: یک شرکت نیازمند Supernet Mask از 16 آدرس کلاس C می باشد. آن را مشخص نمائید.

برای 16 کلاس نیازمند 4 بیت می باشیم. بنابراین Supernet Mask این فضا عبارتست از:

11111111 11111111 1111**0000** 00000000 یا 255.255.240

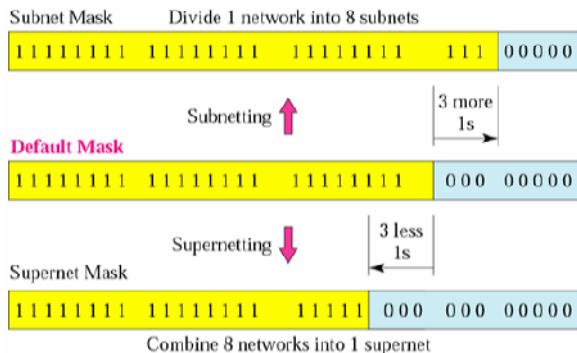
مثال: یک شرکت نیازمند 600 آدرس می باشد. کدامیک از فضاهای بلاکهای کلاس C زیر برای Supernet در این شرکت مناسب است.

198.47.32.0	198.47.33.0	198.47.34.0	
198.47.32.0	198.47.42.0	198.47.52.0	198.47.62.0
198.47.31.0	198.47.32.0	198.47.33.0	198.47.34.0

198.47.32.0 198.47.33.0 198.47.34.0 198.47.35.0

- ۱- نه. تنها سه بلاک وجود دارد.
- ۲- نه. فضای بلاکها پیوسته نیست.
- ۳- نه. ۳۱ در بلاک اول قابل تقسیم نیست.
- ۴- بله. هر سه شرط قابل برآورده است.

در تصویر زیر Subnet Mask و Supernet Mask عادی مقایسه شده است:



مثال: آدرس ابتدایی یک 255.255.248.0 ، Supernet Mask 205.16.32.0 می باشد و می باشد. یک مسیریاب سه بسته با آدرسهای زیر دریافت می کند.

205.16.37.44
205.16.42.56
205.17.33.76

کدامیک از این بسته ها مربوط به این شبکه است؟

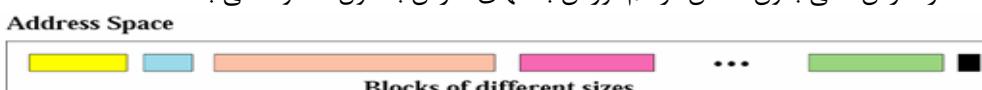
205.16.37.44 AND 255.255.248.0 --> 205.16.32.0
205.16.42.56 AND 255.255.248.0 --> 205.16.40.0
205.17.33.76 AND 255.255.248.0 --> 205.17.32.0

تنهای آدرس اول به این Supernet مربوط می شود.

مثال: یک Supernet دارای یک آدرس شروع 205.16.32.0 و یک Supernet Mask 255.255.248.0 می باشد. چند بلاک در این Supernet وجود دارد و دامنه آدرسهای آن چیست؟
SuperNet دارای ۲۱ عدد یک می باشد و Mask پیش فرض دارای ۲۴ یک می باشد. با توجه به اختلاف سه بیتی این دو می توان نتیجه گرفت که ۸ بلاک در این Supernet وجود دارد. این بلاکها عبارتند از ۲۰۵.۱۶.۳۹.۰ تا ۲۰۵.۱۶.۳۹.۰. آدرس ابتدایی عبارتست از ۲۰۵.۱۶.۳۲.۰ و آخرین آدرس عبارتست از ۲۰۵.۱۶.۳۹.۲۵۵.

آدرس دهی بدون کلاس^۱:

هدف از آدرس دهی بدون کلاس فراهم آوردن بلاکهای آدرس با طول متفاوت می باشد.



یک شبکه داخلی ممکن است تنها به ۲ آدرس نیاز داشته باشد؛ یک شرکت کوچک به ۱۶ آدرس و یک شرکت بزرگ به ۱۰۲۴ آدرس. در هر صورت تعداد آدرسها بلاک باید توانی از ۲ باشد (۲, ۴, ۸, ...). آدرس شروع بلاک باید بر تعداد آدرسها قابل تقسیم باشد. مثلاً اگر بلاک ۴ آدرس داشته باشیم، آدرس ابتدایی باید بر ۴ قابل تقسیم باشد. برای بلاک با کمتر از ۲۵۶ آدرس، تنها باید سمت راست ترین بایت آدرس چک شود و برای بلاکی با کمتر از ۶۵۵۳۶ آدرس ۲ بایت سمت راست چک می شود.

مثال: کدامیک از آدرسها زیر می تواند آدرس ابتدایی یک بلاک ۱۶ آدرس باشد؟

205.16.37.32
190.16.42.44
17.17.33.80
123.45.24.52

سمت راست ترین بایت آدرس اول ۳۲ است که بر ۱۶ قابل تقسیم است . همچنین سمت راست ترین بایت آدرس سوم نیز ۸۰ است که بر ۱۶ قابل تقسیم است. بنابراین تنها آدرس اول و آدرس سوم می توانند آدرس‌های معتبری برای این منظور باشند.

مثال: کدامیک از موارد زیر می تواند آدرس شروع یک بلاک با ۱۰۲۴ آدرس باشد؟

205.16.37.32
190.16.42.0
17.17.32.0
123.45.24.52

برای قابلیت تقسیم بر ۱۰۲۴، سمت راست ترین بایت صفر باشد و بایت دوم از سمت راست باید بر ۴ قابل تقسیم باشد. تنها آدرس ۱۷.۱۷.۳۲.۰ این شرایط را دارد.

نماد /^۱:

A.B.C.D/n یک نماد برای نشان دادن تعداد یکهای Mask یک آدرس می باشد. نماد / را نماد CIDR^۲ نیز می نامند.

مثال: یک سازمان کوچک یک بلاک با آدرس شروع و طول پیشوندی 29/24(در نماد /) را دارد . دامنه بلاک را تعیین کنید.

آدرس ابتدایی 205.16.37.24 است. برای پیدا کردن آدرس انتهایی، ما باید ۲۹ بیت اول را حفظ کرده و ۳ بیت انتهایی را با یک تعویض کنیم.

Beginning : **11001111 00010000 00100101 00011000**
Ending : **11001111 00010000 00100101 00011111**

در هر بلاک تنها ۸ آدرس وجود دارد. دامنه آدرس برای این مثال ۸ است. بنابراین می توان به شکل زیر نیز آدرس نهایی را محاسبه نمود:

$$24 + 7 = 31 \rightarrow 205.16.37.31$$

کلاس‌های A و B و C را براحتی می توان به کمک نماد / بشکل زیر نمایش داد:

Class A : A.B.C.D/8
Class B : A.B.C.D/16
Class C : A.B.C.D/24

مثال: آدرس شبکه را در صورتیکه یکی از آدرس‌های شبکه بصورت 167.199.170.82/27 باشد، را تعیین نمائید.

طول پیشوند ۲۷ است که به معنی آنست که باید اول را نگه داری کرده و بیت‌های باقیمانده(۵ بیت) را صفر کنیم. ۵ بیت تنها آخرین بایت را تحت تاثیر قرار می دهد. آخرین بیت ۰۱۰۱۰۰۱۰ است که با صفر کردن ۵ بیت آخر آن ۰۱۰۰۰۰۰۰ و یا ۶۴ را بدست می آوریم. آدرس شبکه برابر است با 167.199.170.64/27 .

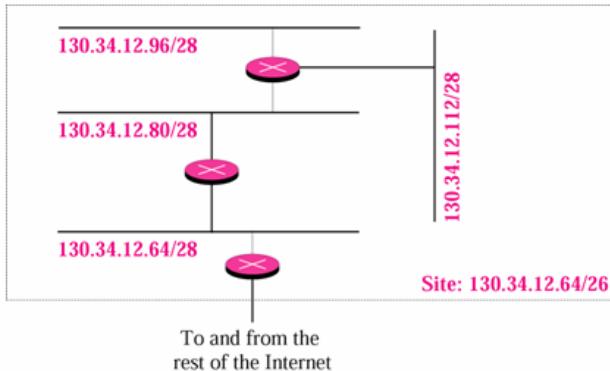
مثال: یک سازمان بلاک آدرس 130.34.12.64/26 را دارد. این سازمان نیازمند ۴ subnet است. ها و دامنه آدرس آنها را مشخص کنید.

طول پسوند ۶ است. به عبارت دیگر هر بلاک ۶۴ آدرس (۳^۶) دارد. بنابراین اگر ۴ subnet بخواهیم هر کدام ۱۶ آدرس خواهند داشت. بنابراین طول پیشوند در این حالت 26+2=28 می باشد.

Subnet 1: 130.34.12.64/28 to 130.34.12.79/28.
Subnet 2: 130.34.12.80/28 to 130.34.12.95/28.
Subnet 3: 130.34.12.96/28 to 130.34.12.111/28.

Slash notation - ^۱
Classless Inter Domain Routing - ^۲

Subnet 4: 130.34.12.112/28 to 130.34.12.127/28.



یک ISP یک بلاک آدرس با آدرس ابتدایی 190.100.0.0/16 دارد. این ISP نیازمند آنست که این فضای آدرس را بین سه گروه زیر توزیع کند:

گروه اول ۶۴ مشتری هر کدام نیازمند ۲۵۶ آدرس

گروه دوم ۱۲۸ مشتری هر کدام نیازمند ۱۲۸ آدرس

گروه سوم ۱۲۸ مشتری هر کدام نیازمند ۶۴ آدرس

زیر بلاکها را طراحی کرده و Slash notation هر کدام را بدست آورید. همچنین مشخص کنید چند آدرس بدون استفاده باقیمانده است.

گروه ۱: در این گروه هر مشتری نیازمند ۲۵۶ آدرس است. این به معنی طول ۸ ($2^8 = 256$) برای پیشوند است.
بنابراین طول پیشوند برابر است با $2^{32-8} = 2^24$

01: 190.100.0.0/24 → 190.100.0.255/24

02: 190.100.1.0/24 → 190.100.1.255/24

.....
64: 190.100.63.0/24 → 190.100.63.255/24

Total = $64 \times 256 = 16,384$

گروه دوم: در این گروه هر مشتری نیازمند ۱۲۸ آدرس است. این به معنی طول ۷ ($2^7 = 128$) برای پیشوند است.
بنابراین طول پیشوند برابر است با $2^{32-7} = 2^25$

01: 190.100.64.0/25 → 190.100.64.127/25

02: 190.100.64.128/25 → 190.100.64.255/25

.....
64: 190.100.127.128/25 → 190.100.127.255/25

Total = $64 \times 256 = 16,384$

گروه سوم: در این گروه هر مشتری نیازمند ۶۴ آدرس است. این به معنی طول ۶ ($2^6 = 64$) برای پیشوند است. بنابراین طول پیشوند برابر است با $2^{32-6} = 2^26$

001: 190.100.128.0/26 → 190.100.128.63/26

002: 190.100.128.64/26 → 190.100.128.127/26

.....
128: 190.100.159.192/26 → 190.100.159.255/26

Total = $128 \times 64 = 8,192$

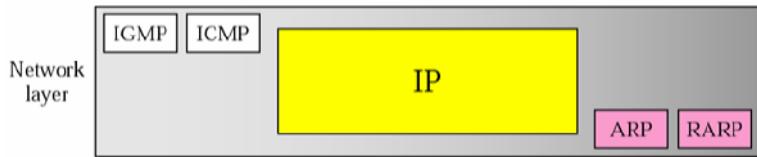
بنابراین مجموع آدرسهای موجود: ۶۵۵۳۵

مجموع آدرسهای تخصیصی: ۴۰۹۶۰

مجموع آدرسهای بدون استفاده: ۲۴۵۷۶

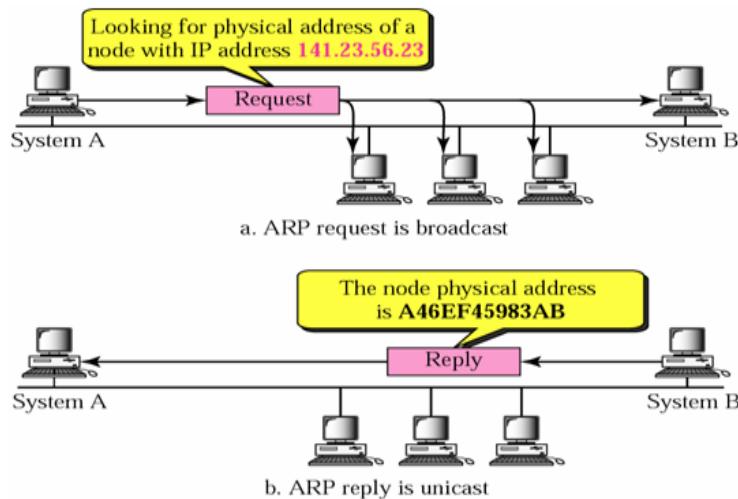
یافتن آدرس در شبکه:

در این بخش، به بررسی دو پروتکل IP می پردازیم ARP و RARP در لایه شبکه قرار دارند.

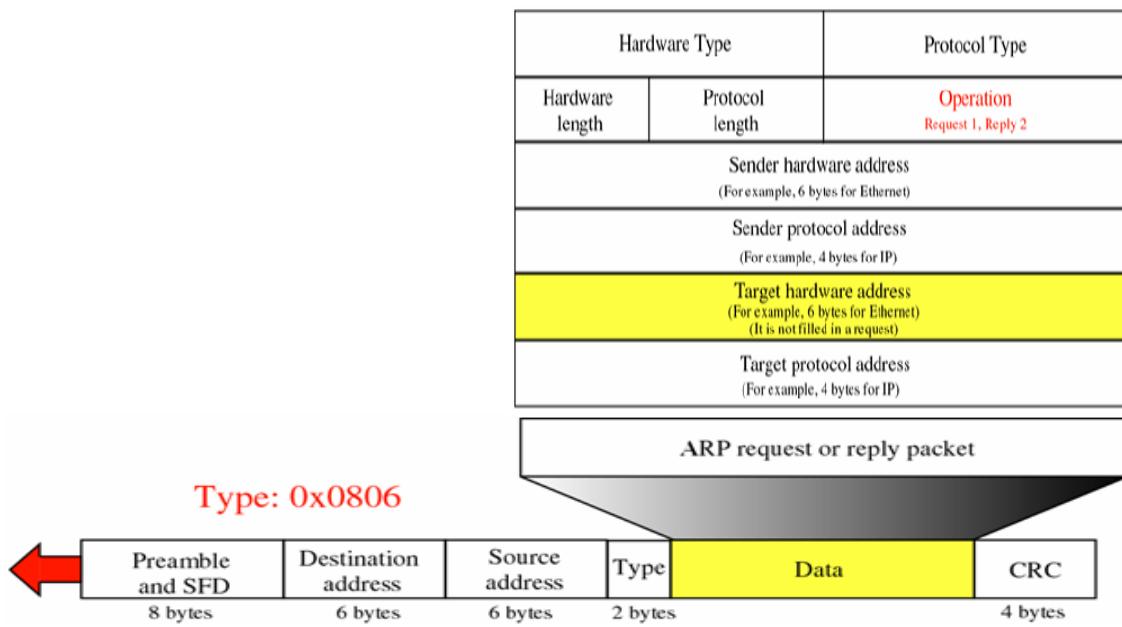


:¹ARP

پروتکلی است که آدرس فیزیکی (آدرس کارت شبکه) را بر می‌گرداند. وقتی بسته به مسیریاب رسید که باید این مسیریاب بسته را بر روی LAN بگذارد (برای یک کامپیوتر مشخص)، این مسیریاب باید آدرس فیزیکی (۴۸ بیتی) را داشته باشد. (زیرا در شبکه LAN آدرس IP معنی ندارد و باید آدرس بسته MAC استفاده شود) در غیر این صورت بسته نمی‌تواند در LAN حرکت کند. پروتکلی که آدرس فیزیکی را بدست می‌آورد ARP است.

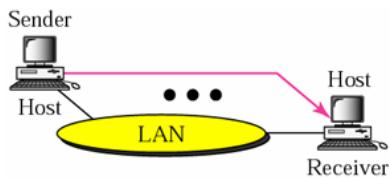


فرمت خاص خود را دارد و با یکی از بسته های خود آدرس IP مقصد را قرار داده و بسته را به LAN می‌فرستد. اندازه بسته ARP و RARP ۲۸ بایت می‌باشد.

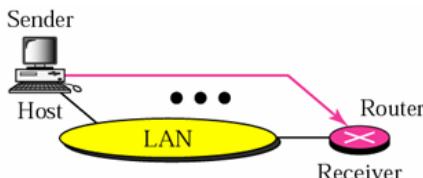


به چهار شکل مورد استفاده قرار می‌گیرد:

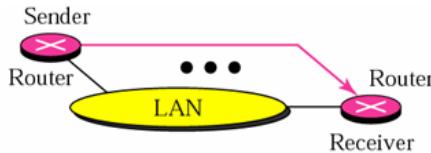
۱. تبادل بسته بین دو میزبان در یک شبکه. آدرس IP مقصد همان آدرس مقصد در بسته داده می باشد.



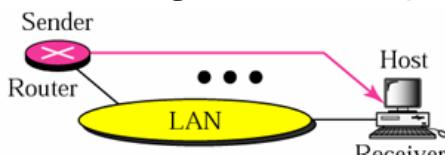
۲. یک میزبان می خواهد بسته ای را به میزبانی در شبکه دیگر بفرستد. بنابراین باید ابتدا بسته به مسیریاب شبکه تحويل داده شود. آدرس IP مقصد آدرس مسیریاب می باشد.



۳. یک مسیریاب بسته ای را دریافت نموده که باید به میزبانی در شبکه دیگری تحويل داده شود. بنابراین مسیریاب باید ابتدا بسته را به مسیریاب دیگری تحويل دهد. آدرس IP مقصد آدرس مسیریاب مناسبی است که براساس جدول مسیریابی باید بسته به آن تحويل گردد.

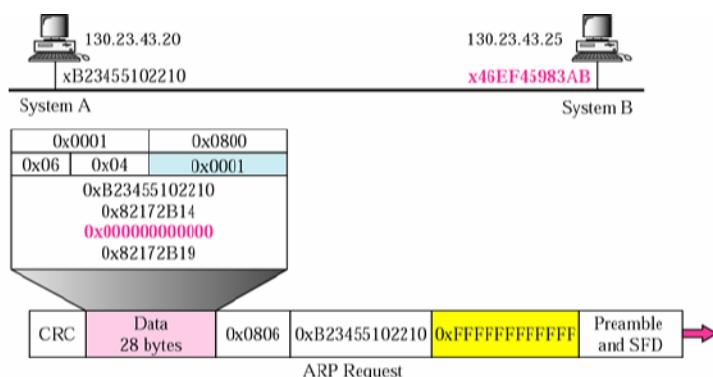


۴. مسیریاب بسته ای را دریافت کرده که باید به میزبانی در شبکه خودش تحويل داده شود. آدرس IP مقصد همان آدرس مقصد در بسته داده می باشد.

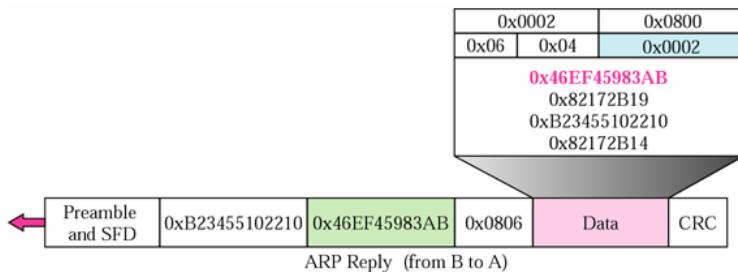


پیام ARP بصورت Broadcast ارسال می گردد، در حالیکه پاسخ آن بصورت Unicast می باشد. میزبانهای مقصد به آدرس IP بسته ARP نگاه می کنند. اگر آدرس موجود در بسته با آدرس IP خود یکی باشد، به بسته جواب می دهند یعنی آدرس فیزیکی خود را در بسته ARP قرار می دهند و ارسال می کنند. حال مسیریاب مقصد با دانستن آدرس فیزیکی میزبان مقصد می تواند بسته مورد نظر خود را با فریم لایه MAC به مقصد برساند (جداول ARP در پریودهای زمانی مشخص Update می شود).

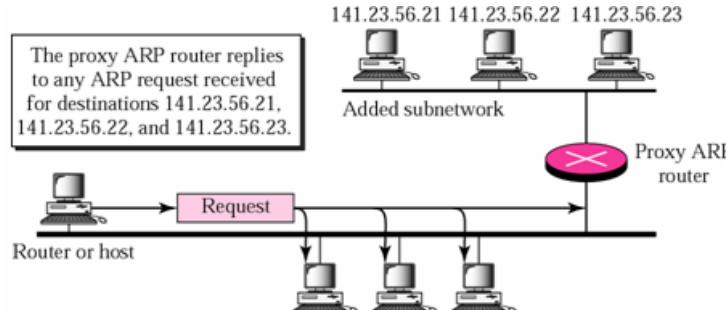
مثال: سیستم A از طریق یک پیام ARP درخواست خود را برای کسب آدرس فیزیکی سیستم B در شبکه منتشر می کند. فیلد Operation یک است (درخواست) و آدرس فیزیکی ماشین مقصد تمام یک است (آدرس Broadcast).



سیستم B در جواب پیام دریافتی، آدرس فیزیکی خود را ارسال می کند. مقدار فیلد Operation ۲ است(پاسخ) و آدرس فیزیکی B در قسمت آدرس فیزیکی سیستم ارسال کننده بسته قرار می گیرد.

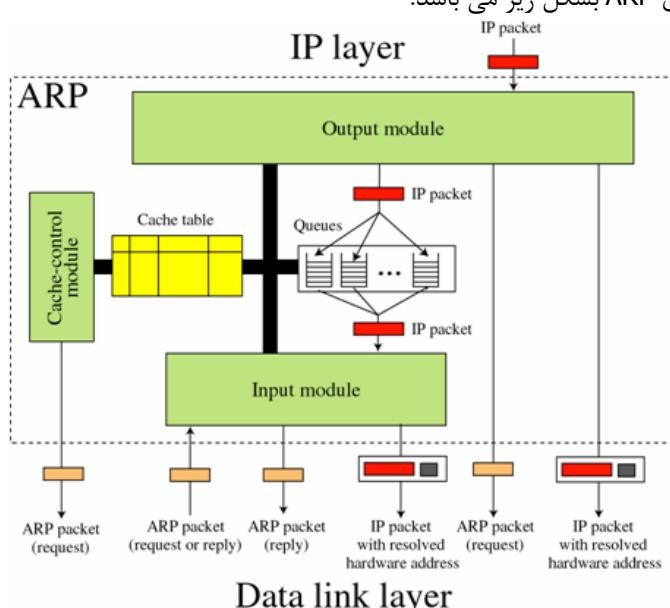


مسیریاب ARP مسیریابی در شبکه است که به پیامهای ARP بخش‌های مختلف شبکه در خصوص آدرس‌های فیزیکی میزبانهای واقع در سایر بخش‌های شبکه پاسخ می دهد. حسن این روش جلوگیری از انتشار بیهوده پیام ARP در کل شبکه و درنتیجه کاهش بار ترافیکی شبکه و همچنین افزایش سرعت پاسخ گویی به درخواستها می باشد. دلیل افزایش سرعت پاسخ گویی ، نگهداری پاسخ های دریافتی در مورد آدرس‌های فیزیکی میزبانهای سایر بخش‌های شبکه ، در بازه زمانی خاص، در مسیریاب می باشد. درنتیجه بجای آنکه بسته مسیر طولانی را تا میزبانی در بخش دیگری از شبکه طی نماید، فقط کافی است تا مسیریاب Proxy ARP برود.



در صورتیکه آدرس فیزیکی مورد نظر در جدول مسیریاب نباشد، درخواستی جهت محاسبه آن در شبکه منتشر می گردد.

ساختار درونی اجزای ARP بشكل زير می باشد:



ساختار اطلاعاتی موجود در جدول کش (Cache) و نحوه عملکرد مازولهای این ساختار در ادامه با یک مثال مورد بررسی قرار گرفته است. جدول کش (Cache) زیر را در نظر بگیرید:

<i>State</i>	<i>Queue</i>	<i>Attempt</i>	<i>Time-out</i>	<i>Protocol Addr.</i>	<i>Hardware Addr.</i>
R	5		900	180.3.6.1	ACAE32457342
P	2	2		129.34.4.8	
P	14	5		201.11.56.7	
R	8		450	114.5.7.89	457342ACAE32
P	12	1		220.55.5.7	
F					
R	9		60	19.1.7.82	4573E3242ACA
P	18	3		188.11.8.71	

ماژول خروجی ARP یک بسته IP Datagram (از لایه IP) با آدرس مقصد 114.5.7.89 را دریافت می نماید. ماژول خروجی جدول کش را چک کرده و یک مدخل برای این آدرس با حالت R (Resolved) پیدا می کند. ماژول خروجی آدرس فیزیکی را استخراج کرده (457342ACAE32) و بسته و آدرس را به لایه پیوند داده برای انتقال می فرستد. جدول کش بدون تغییر باقی میماند.

۲۰ ثانیه بعد، ماژول خروجی ARP یک بسته IP Datagram (از لایه IP) با آدرس مقصد 116.1.7.77 را دریافت می نماید. ماژول خروجی جدول کش را چک کرده و مدخلی برای آن در جدول پیدا نمی کند. ماژول یک مدخل با حالت P (Pending) و با مقدار یک برای فیلد Attempt به جدول اضافه می کند. سپس ماژول یک صف جدید برای این مقصد ایجاد نموده و بسته را در آن قرار می دهد. سپس ماژول یک درخواست ARP به لایه پیوند داده برای این مقصد، ارسال می نماید.

<i>State</i>	<i>Queue</i>	<i>Attempt</i>	<i>Time-out</i>	<i>Protocol Addr.</i>	<i>Hardware Addr.</i>
R	5		900	180.3.6.1	ACAE32457342
P	2	2		129.34.4.8	
P	14	5		201.11.56.7	
R	8		450	114.5.7.89	457342ACAE32
P	12	1		220.55.5.7	
P	23	1		116.1.7.22	
R	9		60	19.1.7.82	4573E3242ACA
P	18	3		188.11.8.71	

۱۵ ثانیه بعد، ماژول ورودی ARP یک بسته ARP با آدرس IP مقصد 188.11.8.71 را دریافت می نماید. ماژول جدول را چک کرده و این مدخل آدرس را پیدا می کند. ماژول ورودی فیلد حالت مدخل را به تغییر داده و مقدار ۹۰۰ را به فیلد Time-out (Resolved) R تخصیص می دهد و آدرس فیزیکی هدف (E34573242ACA) را نیز به مدخل می افزاید. در ادامه ماژول به صفت ۱۸ رفته و بسته هایی موجود در آن را یکی کی به لایه پیوند داده ارسال می کند.

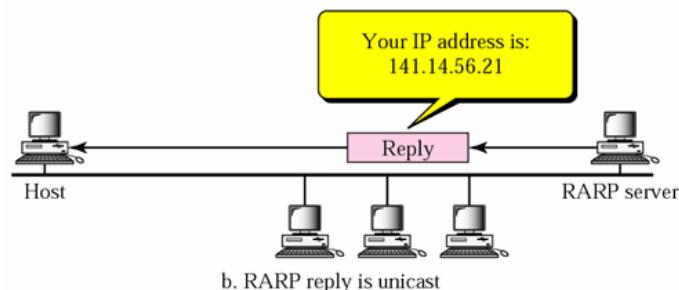
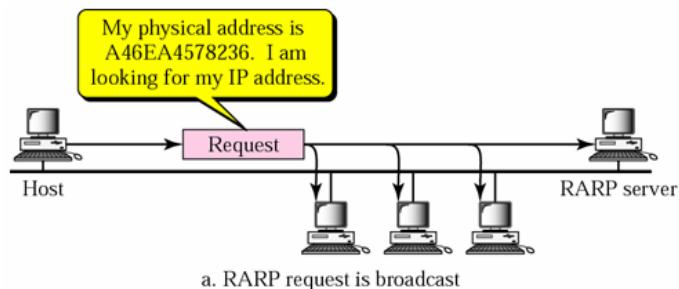
<i>State</i>	<i>Queue</i>	<i>Attempt</i>	<i>Time-out</i>	<i>Protocol Addr.</i>	<i>Hardware Addr.</i>
R	5		900	180.3.6.1	ACAE32457342
P	2	2		129.34.4.8	
P	14	5		201.11.56.7	
R	8		450	114.5.7.89	457342ACAE32
P	12	1		220.55.5.7	
P	23	1		116.1.7.22	
R	9		60	19.1.7.82	4573E3242ACA
R	18		900	188.11.8.71	E34573242ACA

۲۵ ثانیه بعد، مازول کنترل کش(Cache)، مدخلهای جدول را بروز می کند. مقدار Time-out برای سه مدخل Resolved شده ابتدایی به اندازه ۶۰ کاهش می یابد و برای مدخل انتهایی Resolved به اندازه ۲۵ کاهش می یابد. حالت مدخل ماقبل آخر بدلیل صفر شدن Time-out آن، به F(T) تغییر می کند. برای سه مدخل با حالت P، مقدار فیلد Attempt یکی افزایش می یابد. پس از این افزایش یک واحدی، اندازه فیلد Attempt برای پروتکل آدرس IP 201.11.56.7 از حد مجاز بیشتر شده و بنابراین حالت مدخل این آدرس نیز به F تغییر می یابد و صفحه آن حذف می گردد.

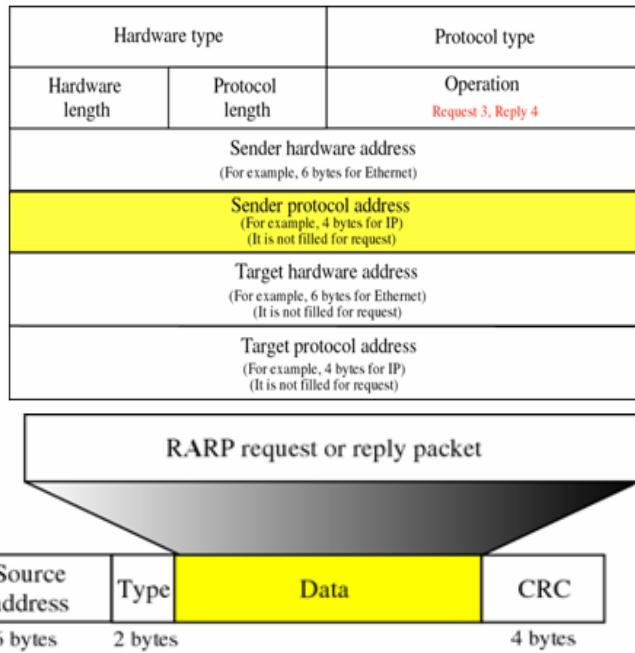
<i>State</i>	<i>Queue</i>	<i>Attempt</i>	<i>Time-out</i>	<i>Protocol Addr.</i>	<i>Hardware Addr.</i>
R	5		840	180.3.6.1	ACAE32457342
P	2	3		129.34.4.8	
F					
R	8		390	114.5.7.89	457342ACAE32
P	12	2		220.55.5.7	
P	23	2		116.1.7.22	
F					
R	18		874	188.11.8.71	E34573242ACA

:^۱RARP

این پروتکل زمانی مورد استفاده است که آدرس MAC موجود باشد و سیستم بخواهد آدرس IP خود را بدست آورد (خصوصاً برای جاهایی که میزبانها آدرس IP را نگه نمی دارند).



فرمت بسته های RARP بصورت زیر است:



مقدار فیلد operation برای این بسته ها ۳ برای درخواست و ۴ برای پاسخ است. همانند ARP، بسته های درخواست Broadcast.RARP شده و پاسخ آن Unicast می گردد.
در کامپیوترهای بدون دیسک متصل به شبکه، RARP نمی تواند اطلاعاتی همچون اطلاعاتی همچون Subnet Mask، آدرس IP مسیریاب و آدرس IP سرور را فراهم کند. برای همین از پروتکل های DHCL و BootP استفاده شود.

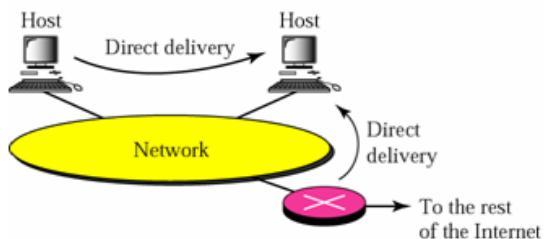
فصل ۳:

مسیریابی در مسیریابها

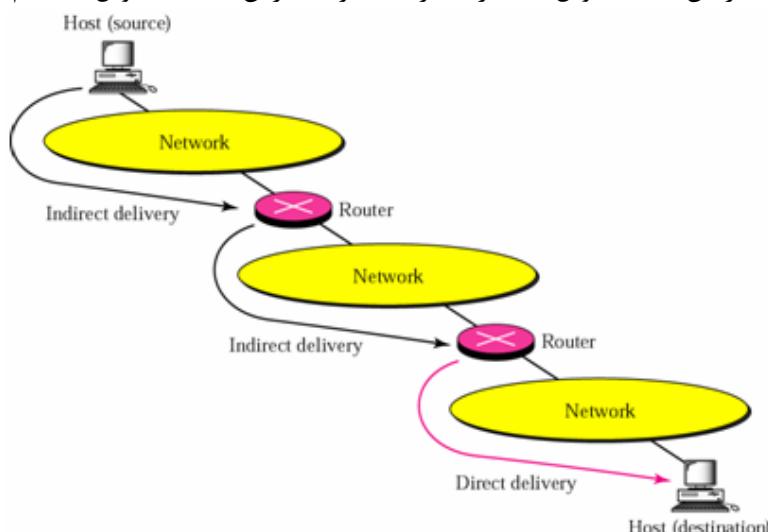
در ارتباطات مبتنی بر اتصال^۱، پروتکل لایه شبکه ابتدا یک اتصال را برقار می کند در حالیکه در ارتباط بدون اتصال^۲، پروتکل لایه شبکه برای هر بسته بصورت جداگانه عمل کرده و عملیات انجام گرفته برای هر بسته ارتباطی با سایر بسته ندارد.

تحویل بسته ها در شبکه به دو شکل انجام می پذیرد:

۱. تحویل مستقیم: ارسال و تحویل بسته از یک میزبان در یک شبکه به میزبانی در همان شبکه.



۲. تحویل غیر مستقیم: ارسال و تحویل بسته از میزبان در یک شبکه به میزبانی در شبکه دیگر. توجه کنید که در این حالت تحویل بسته از مسیریاب آخر به میزبان مقصد ، تحویل مستقیم می باشد.



متدهای مسیریابی در شبکه عبارتند از:

۱ - مسیریابی پرش بعدی(Next-hop Routing)

- بر پایه مسیر: آدرس‌های مسیر کامل تا مقصد در جدول مسیریابی وجود دارد.
- بر پایه فقط پرش بعدی: فقط آدرس پرش بعدی در جدول مسیریابی وجود دارد.

^۱ Connection Oriented –

^۲ Connectionless –

Routing table for host A		Routing table for R1		Routing table for R2	
Destination	Route	Destination	Route	Destination	Route
Host B	R1, R2, Host B	Host B	R2, Host B	Host B	Host B

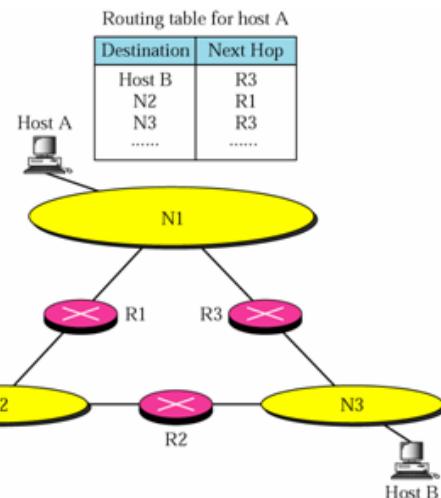
a. Routing tables based on route



Routing table for host A		Routing table for R1		Routing table for R2	
Destination	Next Hop	Destination	Next Hop	Destination	Next Hop
Host B	R1	Host B	R2	Host B	—

b. Routing tables based on next hop

۲- مسیریابی شبکه مشخص (Network-specific Routing): تعیین آدرس پرش بعدی براساس شبکه های مقصد.



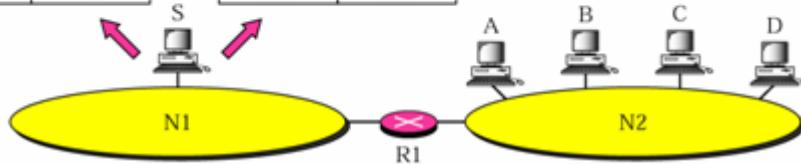
۳- مسیریابی میزبان مشخص (Host-specific Routing): تعیین آدرس پرش بعدی بر اساس میزبان مقصد.

Routing table for host S based on host-specific routing

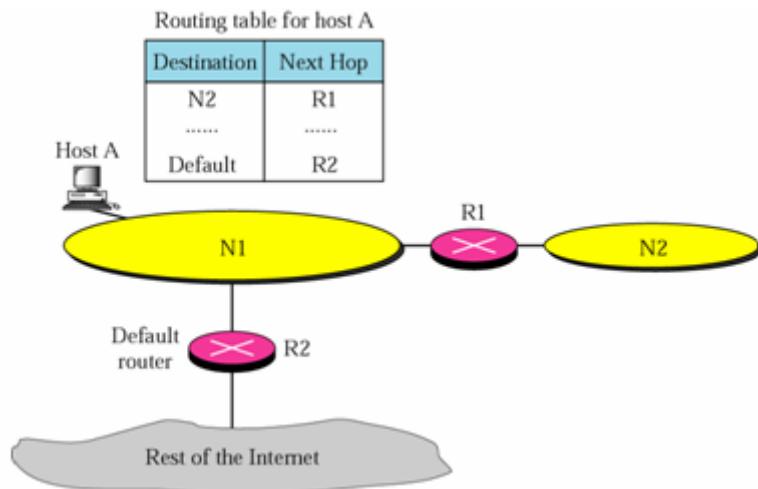
Destination	Next Hop
A	R1
B	R1
C	R1
D	R1

Routing table for host S based on network-specific routing

Destination	Next Hop
N2	R1



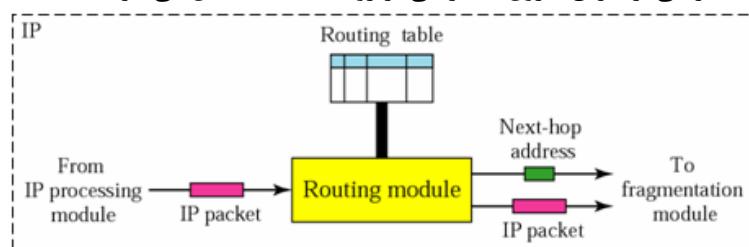
۴- مسیریابی پیش فرض (Default Routing): تخصیص یک مسیر پیش فرض برای مسیریابی آدرسهایی که در جدول دارای سطر مشخص، نیستند.



جداول مسیریابی به دو صورت هستند:

- ۱ جداول ایستا: اطلاعات این جداول بصورت دستی وارد می شود.
- ۲ جداول پویا: اطلاعات این جداول بصورت دوره ای بوسیله پروتکلهای OSPF، RIP و یا BGP بروز می گردد.

اطلاعات جدول مسیریابی از طریق ماذول مسیریابی بر روی بسته ها اعمال می گردد.



طرح یک جدول مسیریابی بصورت زیر می باشد:

Mask	Destination address	Next-hop address	Flags	Reference count	Use	Interface
255.0.0.0	124.0.0.0	145.6.7.23	UG	4	20	m2

فلگهای مورد استفاده در جداول مسیریابی عبارتند از:

- U: مسیریاب فعال است.
- G: مقصد در شبکه دیگری قرار دارد.
- H: آدرس بصورت میزبان مشخص می باشد.
- D: افروده شده بوسیله تعیین مسیر مجدد.
- M: تصحیح شده بوسیله تعیین مسیر مجدد.

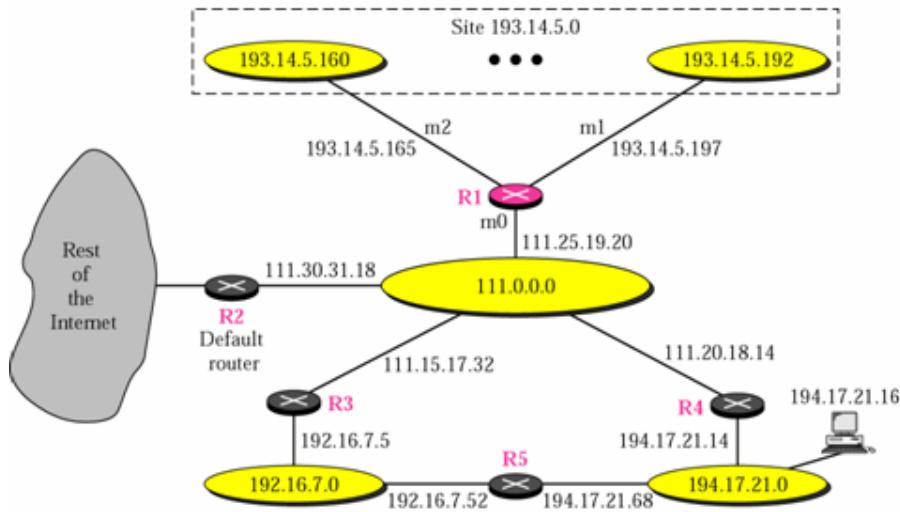
ترتیب قرار گرفتن سطرهای جدول مسیریابی بصورت زیر است:

- آدرس تحويل مستقيم
- آدرس میزبان مشخص

۳- آدرس شبکه مشخص

۴- آدرس پیش فرض

مثال: جدول مسیریابی شبکه زیر برای مسیریاب R1 را طراحی کنید.



Mask	Dest	Next Hop	I
255.0.0.0	111.0.0.0	--	m0
255.255.255.224	193.14.5.160	-	m2
255.255.255.224	193.14.5.192	-	m1
255.255.255.255	194.17.21.16	111.20.18.14	m0
255.255.255.0	192.16.7.0	111.15.17.32	m0
255.255.255.0	194.17.21.0	111.20.18.14	m0
0.0.0.0	0.0.0.0	111.30.31.18	m0

ماژول مسیریابی جهت پیدا کردن مسیر بسته، آدرس مقصد آن را تک به تک با اعمال Mask هر سطر با آدرس مقصد در آن سطر مقایسه کرده و در صورت تطابق، آدرس ارسال بسته را از آن سطر استخراج می کند. برای مثال اگر مسیریاب R1 بسته هایی برای آدرس 192.16.7.14 را دریافت نماید، سطر صحیح در جدول بصورت زیر مشخص می گردد:

Direct delivery

192.16.7.14 & 255.0.0.0 → 192.0.0.0 no match
192.16.7.14 & 255.255.255.224 → 192.16.7.0 no match
192.16.7.14 & 255.255.255.224 → 192.16.7.0 no match

Host-specific

192.16.7.14 & 255.255.255.255 → 192.16.7.14 no match

Network-specific

192.16.7.14 & 255.255.255.0 → 192.16.7.0 match

عملکرد همین مسیریاب برای بسته های با آدرس 193.14.5.176 به شکل زیر می باشد:

Direct delivery

193.14.5.176 & 255.0.0.0 → 193.0.0.0 no match

193.14.5.176 & 255.255.255.224 → 193.14.5.160

match

و برای بسته های با آدرس 200.34.12.34

Direct delivery

200.34.12.34 & 255.0.0.0	→ 200.0.0.0	no match
200.34.12.34 & 255.255.255.224	→ 200.34.12.32	no match
200.34.12.34 & 255.255.255.224	→ 200.34.12.32	no match

Host-specific

200.34.12.34 & 255.255.255.255	→ 200.34.12.34	no match
--------------------------------	----------------	----------

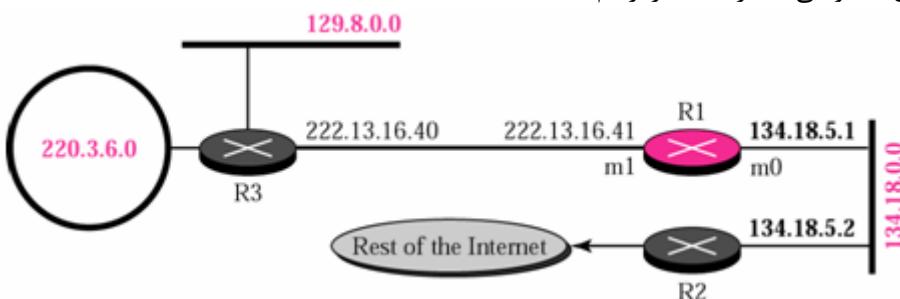
Network-specific

200.34.12.34 & 255.255.255.0	→ 200.34.12.0	no match
200.34.12.34 & 255.255.255.0	→ 200.34.12.0	no match

Default

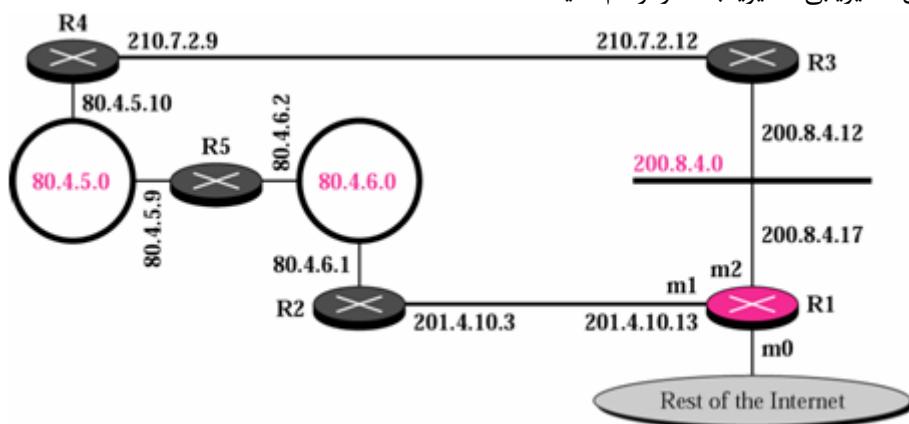
200.34.12.34 & 0.0.0.0	→ 0.0.0.0	match
------------------------	-----------	--------------

مثال: جدول مسیریابی مسیریاب R1 را رسم کنید.



Mask	Destination	Next Hop	I.
255.255.0.0	134.18.0.0	--	m0
255.255.0.0	129.8.0.0	222.13.16.40	m1
255.255.255.0	220.3.6.0	222.13.16.40	m1
0.0.0.0	0.0.0.0	134.18.5.2	m0

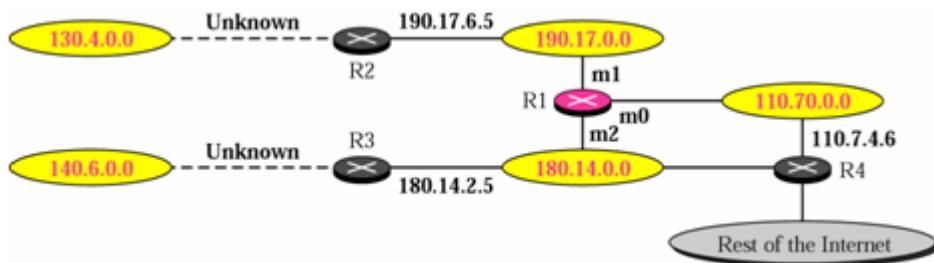
مثال: جدول مسیریابی مسیریاب R1 را رسم کنید.



Mask	Destination	Next Hop	I
255.255.255.0	200.8.4.0	----	m2
255.255.255.0	80.4.5.0	201.4.10.3 or 200.8.4.12	m1 or m2
255.255.255.0	80.4.6.0	201.4.10.3 or 200.4.8.12	m1 or m2
0.0.0.0	0.0.0.0	?????????????	m0

مثال: جدول مسیریابی مسیریاب R1 داده شده است. توبولوژی شبکه آن را رسم نماید.

Mask	Destination	Next Hop	I
255.255.0.0	110.70.0.0	-	m0
255.255.0.0	180.14.0.0	-	m2
255.255.0.0	190.17.0.0	-	m1
255.255.0.0	130.4.0.0	190.17.6.5	m1
255.255.0.0	140.6.0.0	180.14.2.5	m2
0.0.0.0	0.0.0.0	110.70.4.6	m0



در CIDR و یا آدرس دهی بدون کلاس موارد زیر قابل تأمل می باشند:

- اندازه جدول مسیریابی
- مسیریابی طبقاتی
- مسیریابی جغرافیایی
- الگوریتم جستجوی جدول مسیریابی

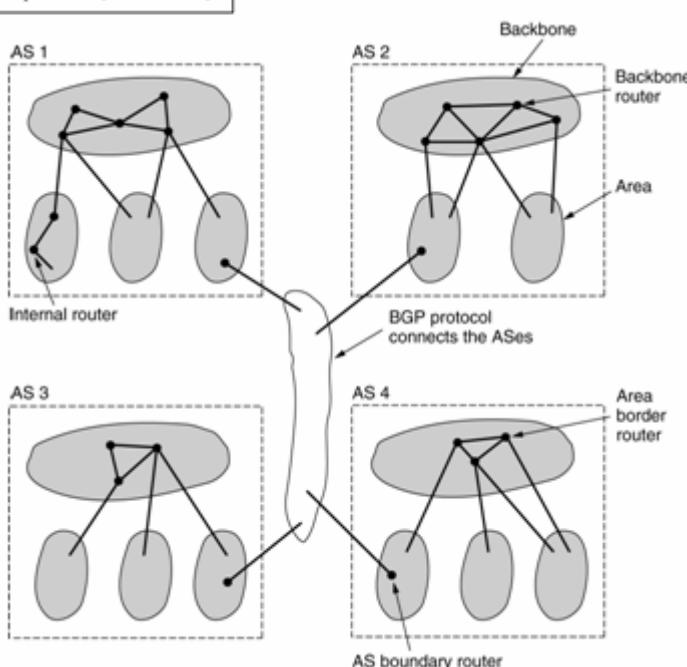
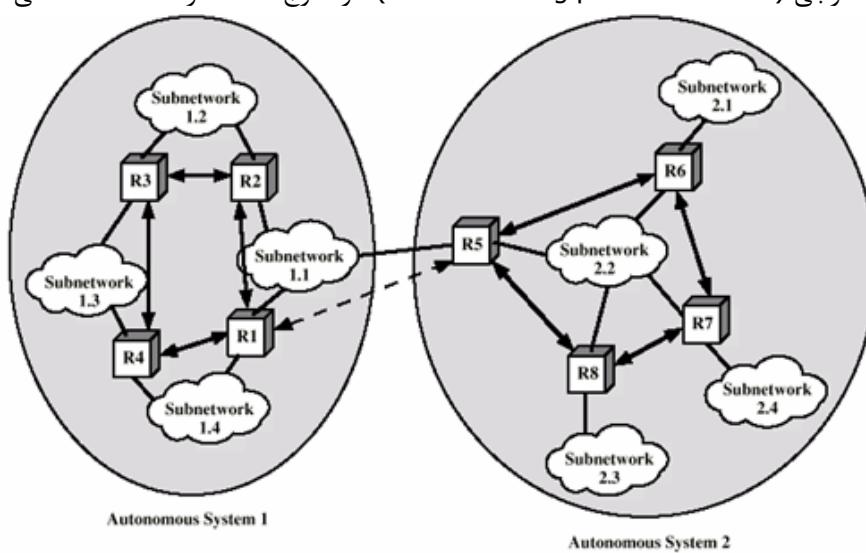
در آدرس دهی کلاسی، هر آدرس خودش حاوی اطلاعاتی است که جستجو در جدول مسیریابی را آسان می کند؛ اما در مورد آدرس دهی بدون کلاس اینگونه نیست.

فصل ۴:

پروتکل های مسیریابی در شبکه

اینترنت شبکه بزرگی است که بخش‌هایی از آن ممکن است توسط یک سازمان نگهداری شود که به آن Autonomous system (سیستم) می‌گویند (Autonomous system). سپس این AS‌ها به هم وصل می‌شوند و شبکه اینترنت را بوجود می‌آورند. بنابراین دو نوع مسیریابی داریم: مسیریابی داخلی AS و مسیریابی بین AS.

- مسیریابی داخلی (Interior routing Protocol or IRP): در داخل AS‌ها از OSPF و RIP استفاده می‌شود.
- مسیریابی خارجی (Exterior routing protocol or ERP): در خارج AS‌ها از BGP استفاده می‌شود.



The relation between ASes, backbones, and areas in OSPF

در واقع شبکه‌های WAN به صورت Store & Forward کار می‌کنند. یعنی بسته از مدا به سوئیچ منتقل می‌شود. بسته در Switch ذخیره می‌شود، آدرس‌ها را استخراج می‌کند و سپس اگر خط خروجی اشغال نباشد (آزاد باشد)، بسته را Forward می‌کند.

Next Hop Forwarding: هر سوئیچ فقط موظف است سوئیچ بعدی که بسته را می‌تواند دریافت کند، مشخص کند؛ یعنی مهم نیست که بسته چه زمانی به مقصد می‌رسد.

استقلال از مبدأ : در تصمیم گیری Routing مبدأ مهم نیست بلکه براساس مقصد تصمیم گیری صورت می گیرد. (در مداری مجازی ، کانال مجازی این وظیفه را بر عهده می گیرد). مسیریابی در سوئیچینگ بسته ای:

- این نوع مسیریابی باید توانایی های زیر را داشته باشد :
 - صحیح کار کردن، ساده بودن ، مقاوم بودن ، پایداری ، عدالت، بهینه بودن ، راندمان
 - معیار های کارآیی :
- تعداد Node های میانی (باید MIN باشد)، هزینه ، تأخیر ، گذردگی.
- زمان تصمیم گیری:
 - 1. هر بسته (در DataGRAM)
 - 2. هر ارتباط (در Virtual Circuit)
- محل تصمیم گیری (مسئول پیدا کردن مسیر) :
 - Node.1
 - Node.2 مرکزی
 - Node.3 آغاز کننده (Source Routing)
- منبع جمع آوری اطلاعات :
 - 1. هیچ (استاتیک)
 - 2. در مسیریابی DYNAMIC باید برای یافتن مسیر اطلاعاتی جمع آوری شود.
- محلی (مسیریابی LOCAL است نه GLOBAL)
 - 3. محلی (مسیریابی LOCAL است نه GLOBAL)
 - 4. Node های مسیر
 - 5. کل Node ها
 - 6. Node های همسایه
- زمان بهنگام سازی(زمان چک کردن هزینه تعویض مسیر)
 - 1. پیوسته
 - 2. پریودیک
 - 3. تغییربار زیاد
 - 4. تغییر توپولوژی

مسیریابی:

مسیریابی یا به صورت استاتیک است یا دینامیک. مسیریابی استاتیک ممکن است به صورت Source Routing باشد یا مسیریابی ثابت.

مسیریابی ثابت:

در مسیریابی ثابت، یک مسیر ثابت و یکتا برای هر زوج مبدأ و مقصد در شبکه، پیکربندی می شود. مسیرها ثابت هستند و یا حداقل تنها با تغییر ساختار شبکه، تغییر می یابند. بنابراین هزینه اتصال مورد استفاده در مسیریابهای هوشمند^۱، نمی تواند برپایه تغییرات پویا همانند ترافیک، قرار بگیرد. در شکل زیر نشان داده شده است که چگونه یک مسیریابی ثابت می تواند پیاده سازی گردد. یک ماتریس مسیریابی مرکزی، ایجاد شده است که

¹ Designing router –

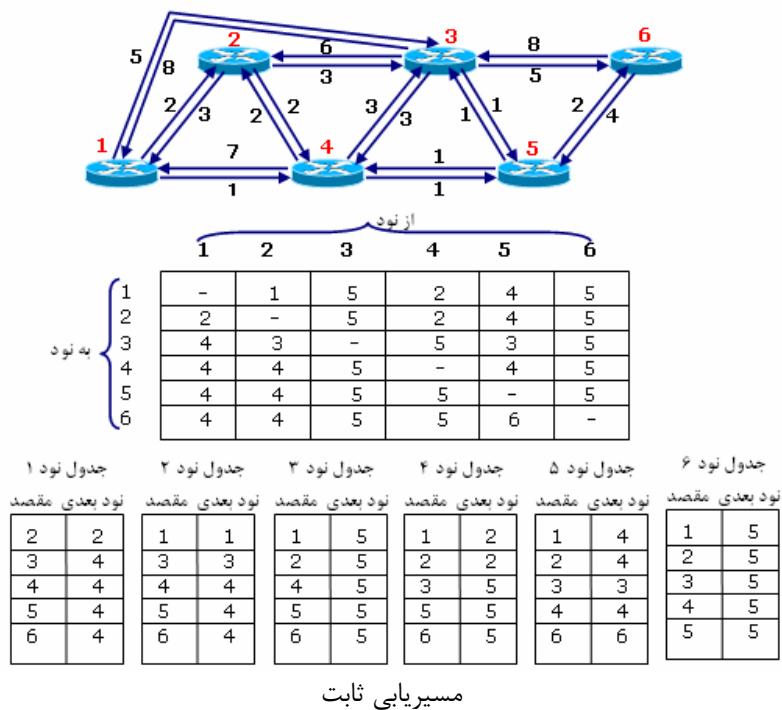
ممکن است در یک مرکز کنترل شبکه قرار گرفته باشد. ماتریس برای هر زوج مبدأ و مقصد، گره بعدی را مشخص می‌نماید.

توجه داشته باشید که لازم نیست که مسیر کامل برای هر زوج از گره‌های ممکن، ذخیره گردد. علاوه‌انکه، تعیین اولین گره مسیر، برای هر زوج گره، کافی است. برای دیدن این موضوع، فرض کنید که مسیر کمترین هزینه از X به Y با اتصال X-A-Y آغاز می‌شود. تنها برقراری تماس با باقیمانده مسیر R_1 که بخشی از مسیر A به Y است، لازم است. R_2 به عنوان کم‌هزینه‌ترین مسیر از A به Y تعریف می‌گردد. اگر هزینه R_1 بیشتر از هزینه R2 بود، مسیر X-Y می‌تواند با استفاده از مسیر R2 بهبود یابد. اگر هزینه R_1 از R2 کمتر بود، R2، کم‌هزینه‌ترین مسیر از A به Y نخواهد بود و بنابراین $R_1=R_2$. بنابراین در هر نقطه از مسیر، تنها کافی است گره بعدی و نه کل مسیر مشخص گردد. در مثال ما، مسیر از گره 1 به گره 6 با استفاده از گره 4، آغاز می‌گردد. دوباره با محاسبه در ماتریس، مسیر گره 4 به گره 6 از گره 5 می‌گذرد. سرانجام، مسیر از گره 5 به گره 6، یک اتصال مستقیم به گره 6 است. بنابراین مسیر کامل از گره 1 به گره 6، ۱-۴-۵-۶ می‌باشد.

با این ماتریس سراسری، جداول مسیریابی می‌توانند در هر گره توسعه داده شده و در هر گره ذخیره گردند. با توجه به استدلال پاراگراف قبلی هر گره تنها نیاز به ذخیره یک ستون از دایرکتوری مسیریابی را دارد. دایرکتوری گره، گره بعدی برای دسترسی به هر مقصد را مشخص می‌کند.

با مسیریابی ثابت، تفاوتی بین مسیریابی برای داده گرام و مدارات مجازی وجود ندارد. همه بسته‌ها از یک مبدأ داده شده به یک مقصد داده شده، از یک مسیر یکسان جریان می‌یابند. مزیت مسیریابی ثابت، سادگی و کارکرد خوب آن در شبکه‌های مطمئن با بارگذاری پایدار، می‌باشد. ضعف این روش فقدان انعطاف پذیری می‌باشد. این روش توانایی مقابله و سازش خود با شرایط ترافیکی و یا نقص در شبکه را ندارد.

یکی از مزایای مسیریابی ثابت آنست که اتصالات تطبیق پذیر هستند و گره‌های خارج از دسترس، یک گره بعدی ثانویه برای هر مقصد را فراهم می‌نماید. برای مثال گره‌های بعدی ثانویه در دایرکتوری گره 1 ممکن است ۳،۲،۳،۴ باشد.



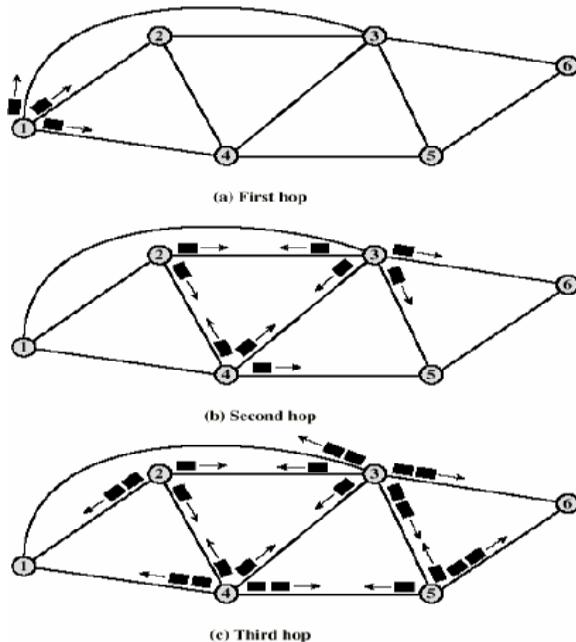
مسیریابی سیل آسا:

روش مسیریابی آسان دیگر، سیل آسا می باشد. این روش نیازمند اطلاعات شبکه نمی باشد و به صورت زیر کار می کند. یک بسته از یک گره مبداء به تمام همسایه هایش ارسال می گردد. در هر گره، یک بسته دریافتی به تمام اتصالات خارجی، بجز اتصالی که بسته از آن دریافت شده، ارسال می گردد. برای مثال، اگر گره ۱ بخواهد به گره ۶ بسته ای را ارسال کند، کپی بسته با آدرس مقصد ۶ را به گره های ۲، ۳ و ۴، ارسال می کند. گره ۲، کپی آن را به گره های ۳ و ۴ ارسال می کند. گره ۴ نیز کپی های را به گره های ۲، ۳ و ۵، ارسال می کند و این عمل همینطور ادامه می یابد. عاقبت تعدادی از بسته ها به گره ۶ می رستند. این بسته ها باید شناسه یکتاوی داشته باشند، همانند شماره مبداء و شماره توالی یا شماره مدار مجازی و شماره توالی، ت گره ۶ بتواند بقیه را بجز اولی، دور بریزد.

بدون وجود عاملی که انتقال پیاپی بسته ها را متوقف نماید، تعداد بسته ها در حلقه ای بدون حد و مرز که از یک بسته ابتدایی در منبع بود، رشد می یابد. یک راه برای جلوگیری از این موضوع آنست که هر گره مقدار شماره شناسایی هر بسته دوباره ارسال شده از خودش را بداند. زمانیکه نسخه دیگری از همان بسته را دریافت نمود، آن را دور بریزد. یک راه ساده تر آنست که یک فیلد تعداد پرش در هر بسته قرار گیرد. این مقدار می تواند با یک مقدارحداکثر ممکن همانند قطر شبکه (طول بزرگترین مسیر با کمترین پرش بین زوج گره های یک شبکه)، تنظیم گردد. هر زمان که یک گره قصد عبور یک بسته را دارد، یکی از مقدار این فیلد کم می شود. اگر این مقدار صفر شود، بسته دور ریخت می شود. مثالی از این موضوع در تصویر زیر آمده است. یک بسته از گره ۱ به ۶، ارسال می گردد و مقدار ۳ به فیلد پرش آن تخصیص می یابد. در اولین پرش، سه کپی از این بسته ایجاد می گردد. برای پرش دوم این کپی ها، مجموعاً ۹ کپی ایجاد می شود. کپی هایی که به گره ۶ می رستند، بدليل رسیدن به مقصد، دوباره ارسال نخواهند شد. اگرچه ۲۲ کپی جدیداً ایجاد شده، در آخرین پرش (سومین پرش) خود قرار دارند. توجه کنید که اگر یک گره، شناسه بسته ها را ردیابی نکند، ممکن است چندین کپی در سومین مرحله ایجاد شود. همه بسته های دریافتی در سومین پرش که به مقصد نرسیده اند، دور ریخته می شوند و گره ۶ نیز ۴ کپی اضافی از بسته را دریافت می نماید.

روش سیل آسا سه خاصیت مهم دارد:

- همه مسیرهای ممکن بین مبداء و مقصد، آزموده می شوند. بنابراین اهمیتی ندارد که یک اتصال و یا گره خروجی، معیوب باشد. یک بسته تولید شده در مبداء، همواره حداقل یک مسیر موجود بین مبداء و مقصد را طی خواهد نمود.
- بدليل آزمایش تمام مسیریابها، حداقل یک کپی از بسته به مقصد می رسد که می تواند عنوان یک مسیر با کمترین پرش، مورد استفاده قرار گیرد.
- همه گره های با اتصال مستقیم یا غیر مستقیم به مبداء، ملاقات می شوند.



نمونه مسیر یابی سیل آسا (تعداد پرش = ۳)

بدلیل اولین خاصیت، شیوه سیل آسا بسیار قوی است و می‌تواند جهت ارسال پیام‌های اضطراری مورد استفاده قرار بگیرد. یک مثال از این قبیل کاربردها در یک شبکه نظامی می‌باشد که هدف مهمی برای تخریب گستردگی، می‌باشد. بدلیل خاصیت دوم، روش سیل آسا ممکن است جهت برپاسازی اولیه یک مدار مجازی، بکار رود. خاصیت سوم بیان می‌کند که روش سیل آسا می‌تواند برای انتشار داده‌های مهم به همه گره‌ها، مفید باشد. همچنین چنین طرح‌هایی جهت انتشار اطلاعات مسیریابی نیز بکار می‌رود. ضعف این روش، یار ترافیکی بالایست که تولید می‌شود که رابطه مستقیم با تعداد اتصالات شبکه دارد.

روش اصلاح شده مسیریابی سیل آسا به صورت Selective Flooding است. یعنی در مسیرهای انتخابی Flooding صورت می‌گیرد.

مسیریابی اتفاقی:

مسیریاب اتفاقی یک روش سیل آسای ساده و قوی، با دوری جستن تا حد ممکن از یار ترافیکی، می‌باشد. با مسیریابی اتفاقی، یک گره تنها یکی از مسیرهای خروجی خود را برای ارسال دوباره یک بسته دریافتی، انتخاب می‌کند. اتصال خروجی بصورت اتفاقی انتخاب می‌شود، به استثنای اتصالی که بسته از آن رسیده است. اگر همه اتصالات بصورت یکسان و مشابه انتخاب شوند، یک گره می‌تواند اتصالات خروجی را به شیوه Round Robin، موردن بردازی قرار می‌دهد.

یک انتشار با این شیوه، با اختصاص یک احتمال به هر اتصال خروجی، جهت انتخاب اتصال برپایه این احتمال، می‌باشد. این احتمال می‌تواند برپایه فرمول زیر باشد:

$$P_i = \frac{R_i}{\sum_j R_j}$$

P_i: احتمال انتخاب اتصال α
R_i: نرخ انتقال داده در اتصال α

جمع بر روی همه اتصالات خروجی نامزد، انجام می‌گیرد. این طرح باید توزیع ترافیکی خوبی را فراهم آورد. توجه کنید که احتمال می‌تواند برپایه هزینه‌های ثابت اتصال نیز باشد.

همانند روش سیل آسا، مسیریابی اتفاقی نیز نیازمند استفاده از اطلاعات شبکه نیست. بدلیل انتخاب مسیر اتفاقی، مسیر واقعی نمی تواند حتماً کم هزینه ترین و یا کم پرش ترین مسیر باشد. بنابراین، شبکه باید یک بار ترافیکی بالاتر از بار ترافیکی بهینه را تحمل کند؛ اگرچه در حد روش سیل آسا نیست.

مسیریابی تطبیقی:

در شبکه های سوئیچ بسته ای تمام مجازی، برخی روشهای مسیریابی تطبیقی، بکار می روند. این به این معناست که تصمیمات مسیریابی با تغییر شرایط شبکه، تغییر می یابند. شرایطی که بر مسیریابی شبکه تاثیر می گذارند، عبارتند از:

- خرابی: زمانیکه یک گره خراب می شود و دیگر نمی توان از آن بعنوان بخشی از یک مسیر استفاده کرد.
- تراکم: زمانیکه بخش معینی از شبکه، شدیداً دچار تراکم شده باشد، مسیریابها باید بسته ها را از ناحیه تراکم دور کنند.

برای مسیریابی تطبیقی، اطلاعات وضعیت شبکه باید بین گره ها مبادله شوند. چند مشکل راه حل های مورد استفاده در مسیریابی تطبیقی، در مقایسه با مسیریابی ثابت، در زیر آمده اند:

- تصمیم مسیریابی بسیار پیچیده است، بنابراین پردازش در گره های شبکه افزایش می یابد.
- در اغلب موارد، استراتژیهای تطبیقی به اطلاعات وضعیت که در یک محل گردآوری شده اند، اما در محل دیگری مورد استفاده قرار می گیرند، وابسته می باشند. این تعاملی بین کیفیت اطلاعات و حجم سربار می باشد. اطلاعات بیشتر که مبادله می شود و فرکانس های بیشتری که تبادل انجام می گیرد، زمینه تصمیم گیری بهتر در زمینه مسیریابی در هر گره را فراهم می آورد. از سوی دیگر، این اطلاعات خود یک بار بروی اجزای اصلی شبکه ها می باشد که باعث کاهش کارایی می گردد.
- یک استراتژی تطبیقی ممکن است بدلیل ایجاد تراکم، بسرعت تغییر شرایط را اعمال نماید و یا آنکه بکندي اين کار انجام بدهد.

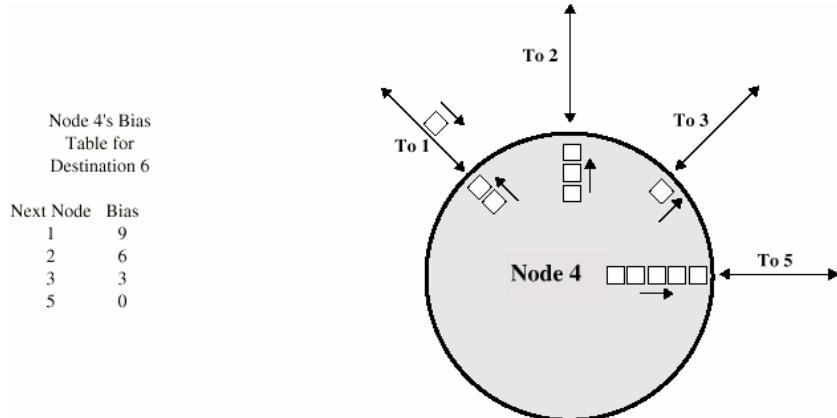
با وجود این مخاطرات جدی، مسیریابیهای تطبیقی به دو دلیل بسیار شایع می باشند:

- از دیدگاه کاربران شبکه، یک استراتژی مسیریابی تطبیقی می تواند کارایی را بهبود ببخشد.
- یک استراتژی مسیریابی تطبیقی می تواند به کنترل تراکم کمک کند. بدلیل آنکه یک استراتژی مسیریابی تطبیقی، تمایل به بارگذاریهای متوازن دارد، می تواند شروع تراکم های گوناگون را به تاخیر بیندازد.

برپایه درستی طراحی و طبیعت بارگذاری، این مزایا ممکن است و یا ممکن نیست که واقعی باشند. با رشد آن، مسیریابی تطبیقی، کار فوق العاده مشکلی جهت انجام صحیح می باشد. برای توضیح این مطلب باید گفت که شبکه های سوئیچ بسته ای همانند ARPANET و پس از آن TYMNET و نمونه های توسعه داده شده توسط IBM و DEC حداقل یک بازدید سراسری عمده از استراتژی مسیریابیشان را، تحمل می نمایند.

یک شیوه متدال جهت طبقه بندی استراتژیهای مسیریابی تطبیقی، مبتنی بر اطلاعات مبدأ می باشد: محلی، گره های مجاور، همه گره ها. یک مثال از استراتژی مسیریابی تطبیقی که تنها اطلاعات محلی را مورد استفاده قرار می دهد آنست که ، یک گره هر بسته را به اتصال خروجی با کمترین طول صف، Q، هدایت کند. این موضوع می تواند در متوازن سازی بار اتصالات خروجی، موثر باشد. اگرچه برخی ار اتصالات خروجی ممکن است در

مسیر مناسب قرار نداشته باشد. همچنین می توانیم این مسئله را با محاسبه کردن جهت برتر، منطبق با مسیریابی اتفاقی، بهبود ببخشیم. در این حالت هر اتصال از هر گره باید یک مقدار تمایل⁽¹⁾ برای هر مقصد I داشته باشد. برای هر بسته ورودی رسیده برای گره آ، گره، اتصال خروجی با حداقل $Q+B_i$ را انتخاب می کند. بنابراین یک گره مراقب ارسال بسته ها در مسیر صحیح می باشد و یک امتیاز انحصاری نیز جهت تاخیر ترافیکهای جاری ایجاد می نماید.



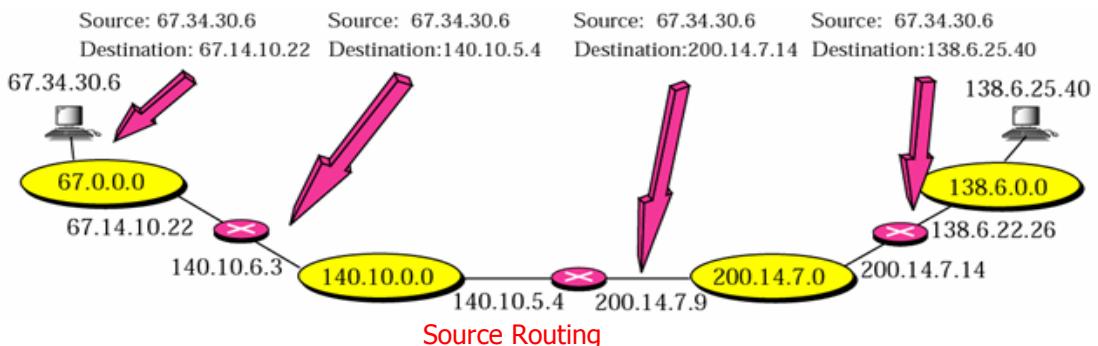
نمونه ای از مسیردهی تطبیقی مجزا

به عنوان یک مثال، تصویر بالا نشانگر وضعیت گره ۴ تصاویر قبلی در یک زمان خاص می باشد. گره ۴ به ۴ گره دیگر، اتصالاتی را دارد. تعدادی بسته دریافت شده و یک ابلاشت در یک صف برای بسته های منتظر خروج، در هر اتصال خروجی، ایجاد شده است. یک بسته از گره ۱ به مقصد گره ۶، دریافت می شود. بسته باید به کدام اتصال خروجی هدایت شود. برای این طول کوتی اصفها و مقادیر تمایل B_6 برای اتصالات خروجی، حداقل مقدار $Q+B_6$ است که بر روی اتصال گره ۳، قرار دارد. بنابراین گره ۴، بسته را به سمت گره ۳ هدایت می کند.

طرح های تطبیقی که تنها برای اطلاعات محلی هستند، به ندرت مورد استفاده قرار می گیرند؛ زیرا آنها اطلاعات موجود را بخوبی بکار نمی بند. استراتژیهای مبتنی بر گره های همسایه و یا همه گره ها، بصورت متداول و عمومی مورد استفاده قرار می گیرند. هر دو روش از مزایای اطلاعات موجود در هر گره در مورد تاخیرها و خروجیهای تجربه شده، بهره می برد. اینچنین استراتژیهای تطبیقی می توانند بصورت توزیع شده و یا مرکزی باشند. در حالت توزیع شده، هر گره اطلاعات تاخیر را با سایر گره ها معاوضه می نماید. برای اطلاعات ورودی، یک گره سعی در برآورد بازده شبکه کرده و الگوریتم مسیریابی کمترین هزینه را اعمال می نماید. در حالت مرکزی، هر گره وضعیت تاخیر انتشارش را به یک گره مرکزی، گزارش می دهد. این گره مسیرها را برای این اطلاعات ورودی، طراحی نموده و اطلاعات مسیریابی را به گره ها، باز می گرداند.

در WAN Source Routing کمتر استفاده می شود و بیشتر برای اتصال Bridge ها استفاده می شود (در شبکه های محلی LAN). در شبکه های TOKEN RING از Source Routing استفاده می شود.

¹ Bias -



در لایه ۲ استفاده می شود. برای هنگامی مفید است که بخواهیم دو یا چند LAN را به هم متصل کنیم ولی برای WAN مناسب نیست در صورتی که مسیریاب در لایه ۳ است. مسیریابی در پلهای به شکل‌های زیر می باشد:

- Source Routing
- Transparent Bridge

در این روش از protocl BPDU استفاده می شود. در این روش از spanning tree استفاده می شود. در این روش بین مقصد و مبدأ یک مسیر وجود دارد بنابراین یک بسته از مقصد به مبدأ می رسد. پروتکل BPDU (رد و بدل اطلاعات) در پلهای، ریشه و سایر گره ها وجود دارد، پس از رد و بدل شدن اطلاعات، مسیریابی مربوط مشخص می شود، یعنی مسیرهای را که جز درخت نیست، پیدا می کند.



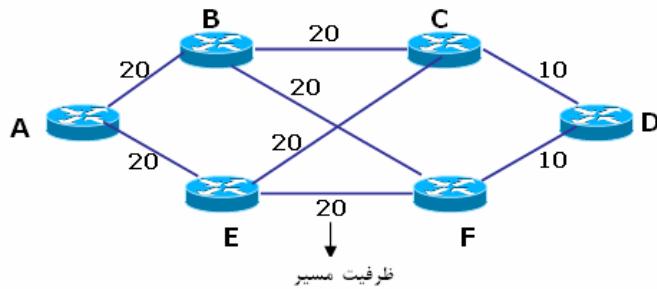
Spanning Tree

: FLOW BASED Routing

یک سری ROUTER و Node به هم متصل شده اند و یک توپولوژی را ایجاد کرده اند . به هر مسیر یک هزینه افزوده می شود که معمولا طول صف یا تاخیر است سپس یک الگوریتم کوتاهترین مسیر اعمال می شود (مانند دیکسترا) و مسیر مینیم هزینه را بین مبدأ و مقصد پیدا می کند، برای هزینه علاوه بر تاخیر، بار (Load) را هم باید در نظر گرفت. روش flow based routing روشنی است که علاوه بر تاخیر، بار را هم در نظر می گیرد.

FLOW در شبکه کامپیوتری دو معنی دارد . یکی بار، یعنی میزان انتقال اطلاعات است (که هدف ما همین است) و دیگری دسته ای از بسته که خصوصیت مشترکی دارند. (یعنی برای مسیریابی بسته ها، به جای اینکه برای هر بسته مسیریابی انجام شود، بسته ها را کلاسه بندی می کنند (PACKET CLASSIFICATION)) و سپس برای FLOW (دسته مشترک) مسیریابی انجام می شود . (برای اینکار از TCAM در مسیریاب ها استفاده می شود)

١. توپولوژی شبکه (مسیریاب ها چگونه به هم متصل شده اند)
٢. ماتریس ترافیک
٣. ماتریس ظرفیت که ظرفیت هر مسیر را بر حسب Xbps مشخص می کند .



ظرفیت مسیر

از به	A	B	C	D	E	F
A		9 AB	4 ABC	1 ABFD	7 AE	4 AEF
B	9 BA		8 CB	3 BFD	2 BFE	4 BF
C	4 CBA	8 CB		3 CD	3 CE	2 CEF
D	1 DFBA	3 DFB	3 DC		3 DCE	4 DF
E	7 EA	2 EFB	3 FC	3 ECD		5 EF
F	4 FEA	4 FB	2 FEC	4 FD	5 FE	

ماتریس ترافیک (ترافیک
برحسب بسته بر ثانیه).
یعنی در یک مقطع زمانی
وضعیت مسیرها اینگونه
بوده است.

ماتریس ظرفیت

i	خط	λ_i	$C_i(\text{kbps})$	$\mu C(\text{PK/S})$	T_i	وزن
1	AB	14	20	25	91	0.171
2	BC	12	20	25	77	0.146
3	CD	6	10	12.5	154	0.073
4	AE	11	20	25	71	0.134

Flow Based Routing

اگر در ماتریس ترافیک بسته های مسیر AB را حساب کنیم (نه BA را) می بینیم که 14 تا بسته وجود دارد ($9+4+1$) که λ را در جدول فوق نشان می دهد. در مدل سازی شبکه از مدل توزیع پواسن استفاده می شود.



$$T = 1/(\mu * C - \lambda)$$

μ : نرخ سرویس (نرخ خروج)

$\lambda = 1/\mu$: طول متوسط بسته ها بر حسب بیت.

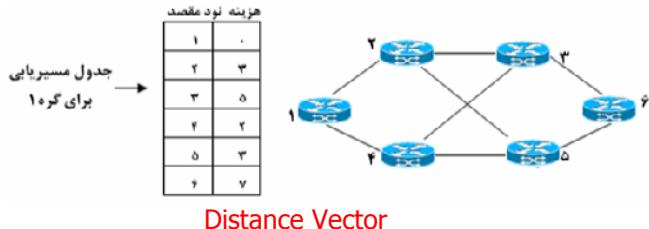
λ : از جدول ترافیک محاسبه می شود(به کمک نمونه برداری نحوه انتقال بسته ها از مسیرهای مختلف) برای محاسبه وزن هر مسیر T آن را بر مجموع T_i تقسیم می کنیم. مثلاً برای AB داریم $W_{AB} = T_1 / (T_1 + T_2 + \dots) = 0.171$

نکته ای که باید در نظر گرفت آنست که در محل فوق فرض کردیم که تاخیر بسیار ناچیز است و بسته ها (بیت ها) پشت سر هم می آیند که توانستیم بگوییم $1/\text{bps}$ = اندازه. الگوریتم های مسیریابی در اینترنت :

• اینترنت اولیه در شبکه های ناول و DEC هم پیاده سازی شده است (RIP).

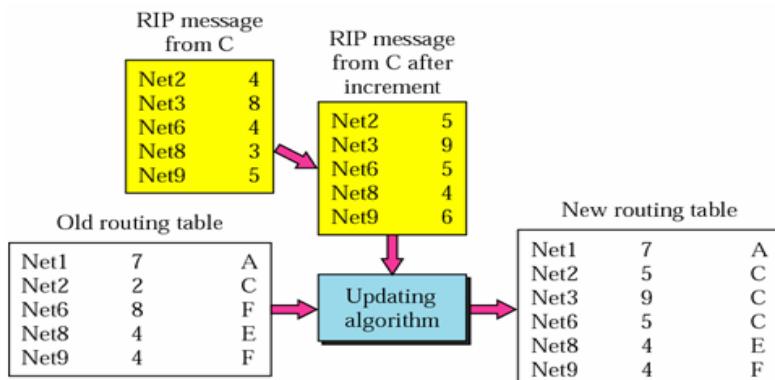
• اخیراً (ده سال است) از این روش استفاده می شود (OSPF).

در روش ROUTER ها یک بردار تاخیر دارند که تاخیر MIN به هر Node را دارد البته بعدی را هم به نحوی مشخص می کند. هر مسیریاب در یک پریود زمانی بردار تاخیر خود را به همسایه های خود می فرستد. هر Node با توجه به بردارهای دریافتی، بردار جدیدی ایجاد می کند و Min تاخیر را برای هر مسیر پیدا می کند.



محاسبه تأخیر چگونه انجام می شود؟

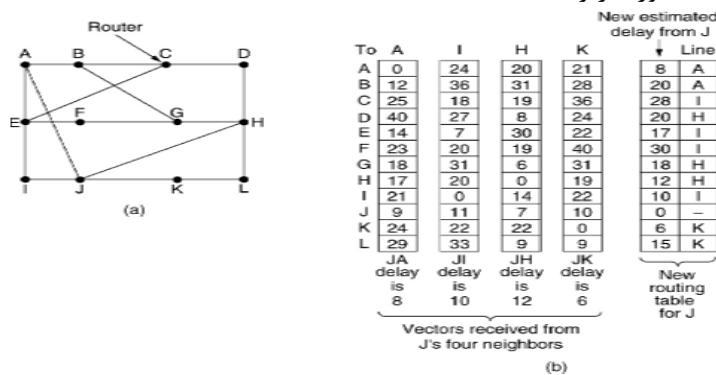
هر ROUTER یک بسته آزمایشی به نام ECHO را برای همسایه می فرستد و مسیریاب دیگر جواب می دهد و متوسط زمان رفت و برگشت، زمان تأخیر خواهد بود.



- Net1: No news, do not change
- Net2: Same next hop, replace
- Net3: A new router, add
- Net6: Different next hop, new hop count smaller, replace
- Net8: Different next hop, new hop count the same, do not change
- Net9: Different next hop, new hop count larger, do not change

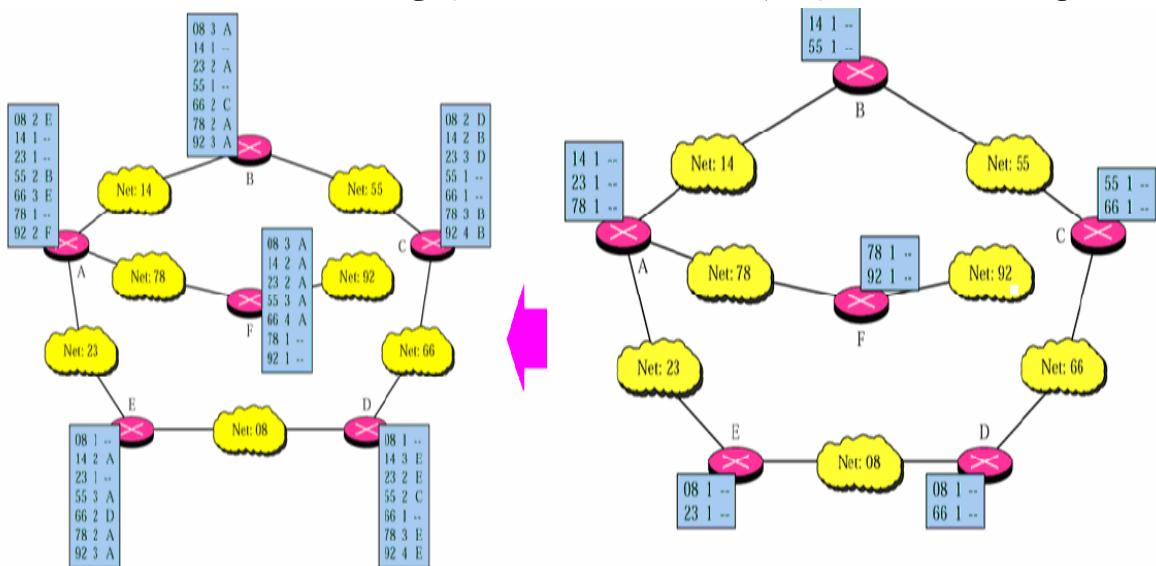
Updating Vector Table

مثال: در زیر ابتدا مسیریاب C جدول مسیریابی خود را بروز نموده است و در ادامه جدول جدید را برای همسایه خود می فرستد. نحوه بروز رسانی جدول مسیریابی مسیریاب همسایه C در شبکه پس از ورود جدول جدید مسیریابی از مسیریاب C بصورت زیر است:

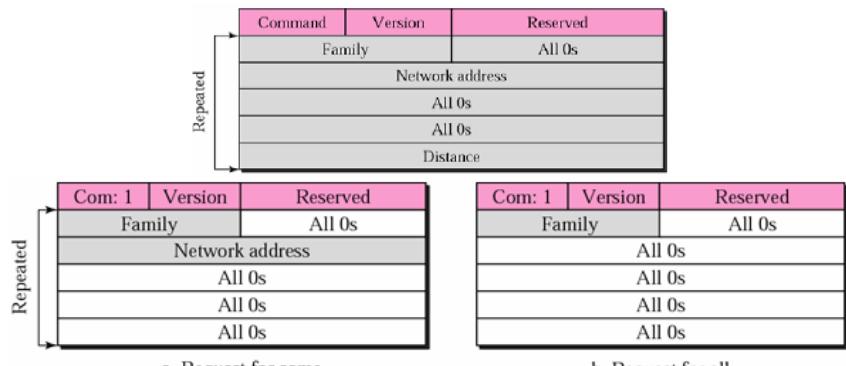


Updating Vector Table Example

طرح های زیر نحوه بروز شدن تمام مسیریابهای یک شبکه را نمایش می دهد:



فرمت بسته های RIP و پاسخ آنها بصورت زیر می باشد:



مثال: فرض کنید مسیریاب R1 تمام AS را می شناسد. پاسخ دوره ای فرستاده شده بوسیله مسیریاب R1 چیست؟



مسیریاب R1 می تواند سه شبکه 144.2.7.0 و 144.2.9.0 و 144.2.12.0 را اعلان کند. پاسخ دوره ای بسته بروز رسانی (RIP message) بصورت زیر است:

RIP message		
2	1	Reserved
2	All 0s	
144.2.7.0	All 0s	
All 0s	All 0s	
**	All 0s	
2	All 0s	
144.2.9.0	All 0s	
All 0s	All 0s	
**	All 0s	
2	All 0s	
144.2.12.0	All 0s	
All 0s	All 0s	
1		

تایمراهای RIP شامل موارد زیر می باشد:

۱. دوره ای(Periodic): ۳۵-۲۵ ثانیه

۲. انقضای(Expiration): ۱۸۰ ثانیه

۳. مجموعه زباله(Garbage Collection): ۱۲۰ ثانیه

مثال: یک جدول مسیریابی ۲۰ مدخل دارد. این جدول اطلاعات ۵ مسیریاب را برای زمان ۲۰۰ ثانیه دریافت نمی کند. چند تا از این تایمراهها در این زمان درحال اجرا می باشد.

تایمراه ای: ۱

تایمراه انقضای: $200 - 5 = 195$

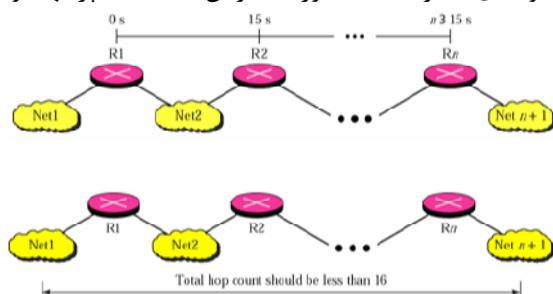
تایمراه مجموعه زباله: ۵

RIP مشکلات:

۱- یکی از مشکلات این روش این است که ظرفیت را در نظر نمی گیرد .

۲- اشکال دیگر این است که برای محاسبه تأخیرها ، زمان زیادی لازم است .

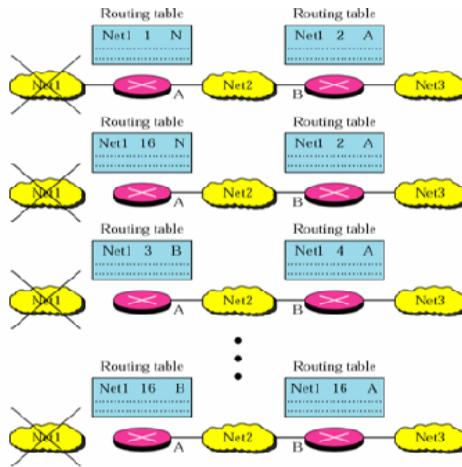
۳- یکی دیگر از عیوب این روش کند بودن است (Slow convergence). چون باید هر نود و تأخیرش را با کلیه نودهای دیگر به دست آورد. بنابراین باید تعداد پرسشها موجود کمتر از ۱۶ باشد.



۴- از طرفی چون همه نودها بسته ECHO می فرستند مشکل ترافیک هم به وجود می آید (حجم محاسبات بالاست).

۵- یکی از مشکلاتی که در Update کردن جدول مسیریابها وجود دارد این است که دقیقاً سنکرون نیستند یعنی کلاک وجود ندارد که همه با هم Update شوند. که در روش Distance Vector هم این مشکل وجود دارد و باعث می شود که تأخیر کاملاً بهینه نباشد ولی در روش State چون از TIME استفاده می شود به نوعی (تا حدودی) مشکل را حل کرده است .

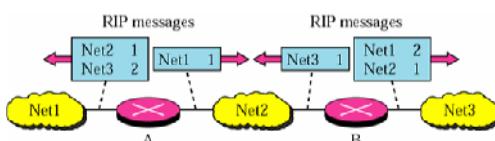
۶- بی ثباتی(Instability) از دیگر مشکلات RIP می باشد. برای درک این مفهوم تصویر زیر را در نظر بگیرید.



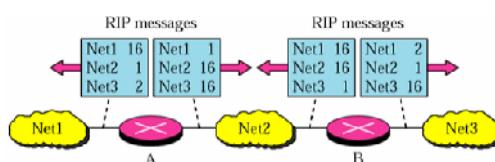
مسیریاب A به شبکه Net1 متصل است و مسیریاب B از طریق مسیریاب A به این شبکه متصل است. با قطع اتصال مسیریاب A با شبکه A، مقدار هزینه تا این شبکه را به حداقل (۱۶) می‌رساند تا عدم اتصال با آن را نشان می‌دهد. اما این قطع اتصال هنوز به مسیریاب B گزارش نشده است. قبل از اعلام این وضعیت به مسیریاب B، مسیریاب B جدول بروز شده جدید خود را برای مسیریاب A می‌فرستد. مسیریاب A به تصور اینکه مسیریاب B با این شبکه ارتباط دارد، جدول خود را با اطلاعات جدید، بروز می‌کند. جدول مسیریاب B نیز با اطلاعات اشتباہ مسیریاب A بروز می‌شود. این چرخه تا آنجا ادامه می‌یابد تا هزینه هر دو جدول برای این شبکه به ۱۶ برسد.

برای رفع این مشکلات ۲ راه پیش‌بینی شده است:

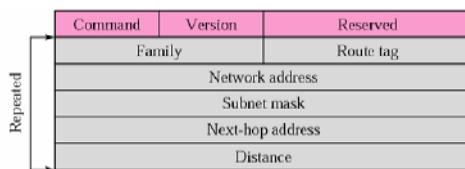
۱. **Split Horizon**: در این روش اطلاعات مسیرهایی از یک رابط مسیریاب ارسال می‌گردد که از آن رابط دریافت نشده است.



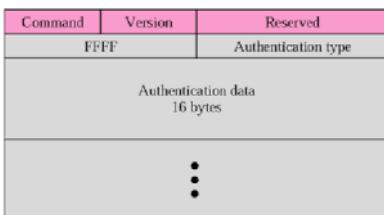
۲. **Poison Reverse**: در این حالت اطلاعات کامل جدول مسیریابی بر روی تمام رابط‌ها پخش می‌شود. اما اگر اطلاعات شبکه‌ای از یک رابط بدست آید، اطلاعات ارسالی آن شبکه از همان رابط، مقدار ۱۶ خواهد داشت.



نسخه دوم RIP از CIDR پشتیبانی می‌کند. فرمت این RIP بصورت زیر می‌باشد:



از RIP می‌توان برای Authentication نیز استفاده کرد. فرمت این بسته بصورت زیر است:



از پورت ۵۲۰ UDP استفاده می کند.

Link State

در این روش چند مرحله وجود دارد :

- ۱) یادگیری همسایه ها
- ۲) اندازه گیری هزینه هر خط
- ۳) ساخت بسته های Link State
- ۴) توزیع بسته های Link State
- ۵) محاسبه تأخیر

این روش ظرفیت را نیز علاوه بر تأخیر در نظر می گیرد و برای شبکه های جدید مناسب است . اینترنت کنونی هم از Link State استفاده می کند .
یادگیری همسایه ها:

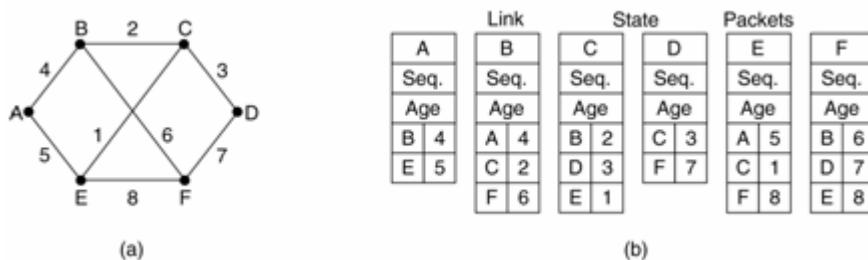
هر مسیریاب وقتی وارد شبکه می شود باید همسایه هایش را بشناسد و این کار باید به صورت خودکار صورت گیرد . هر مسیریاب آدرس خودش را می فرستد و خودش را معرفی می کند (آدرس هر مسیریاب یکتا است).

اندازه گیری هزینه هر خط:

هر مسیریاب به همسایه هایش یک بسته ECHO می فرستد و همسایه ها جواب می دهند و با متوسط گیری زمان رفت و برگشت ، هزینه خط به دست می آید . (ECHO هم می تواند در صف قرار گیرد تا LOAD (بار) هم محاسبه گردد)

ساخت بسته های Link State :

این بسته ها یا به صورت پریودیک ایجاد می شوند یا اینکه تحول خاصی رخ داده باشد ،



Link State Model

پس برای هر بسته یک SEQUENCE NUMBER درنظر گرفته می شود همچنین یک فیلد به نام age که طول عمر بسته را در نظر می گیرد که هم به صورت زمانی از آن کم می شود و هم اینکه از هر مسیریابی که بگذرد از آن کم می شود .

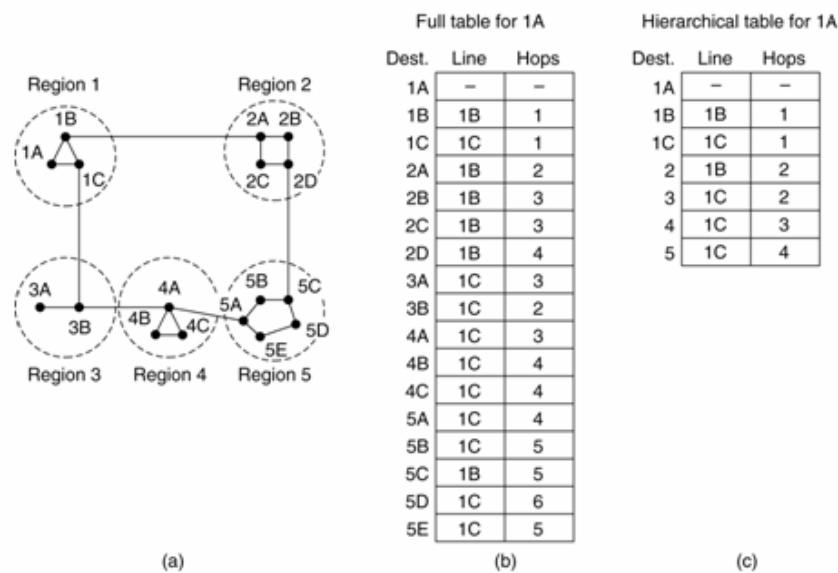
توزیع بسته های Link State

روشی که برای توزیع استفاده می شود روش Flooding است هر مسیریاب وقتی بسته ای را در نظر می گیرد به NO SEQ آن نگاه می کند اگر شماره بیشتری نسبت به قبل داشته باشد آن را منتشر می کند و بسته قبلى را دور می ریزد و اگر بسته جدید دارای SEQ NO کمتری نسبت به قبلى باشد دور ریخته می شود و از انتشار روبه جلوی آن خودداری می کند ، پس AGE Number به همراه فیلد SEQUENCE به این دلیل اضافه شده اند که از ترافیک بیهوده جلوگیری شود .
بسته های ACK هم Link State می شوند .

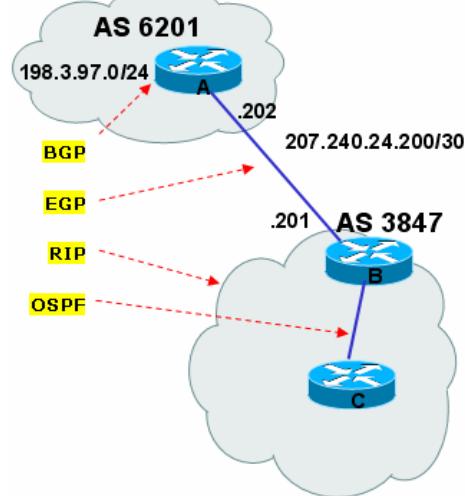
Source	Seq.	Age	Send flags			ACK flags			Data
			A	C	F	A	C	F	
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	

Link State Propagation

برای مثال در شکل قبل ، فرض می شود که بسته هایی را از A , C , F دریافت می کند . چگونه ها منتشر می شوند؟ بسته ارسالی از E از طریق A,F به B می رسد. بنابراین فقط به طرف C منتشر می شود. بسته ارسالی از C از طریق خود C دریافت شده و بنابراین به دو مسیر دیگر ارسال می گردد. یکی از مشکلات این است که اگر مسیریاب های زیادی در شبکه وجود داشته باشد پس از مدتی اندازه جدول بسیار بزرگ می شود . یکی از راه حل های این مشکل این است که مسیریابی را به صورت سلسه مراتبی انجام دهیم و نه به صورت کلاستر بندی.



(a) (b) (c)



Multilevel Link State

به صورت INTERIOR ROUTER OSPF, RIP و EXTERIOR EGP و BGP به صورت HOSTEND یعنی فقط با ناحیه داخلی خود ارتباط دارند ولی است.

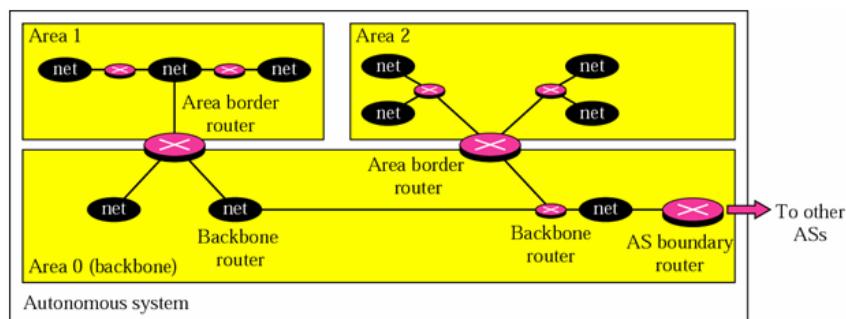
محاسبه تأخیر :

وقتی بسته ها رسید هر مسیریاب با توجه به زمان رفت و برگشت و با استفاده از الگوریتم هایی مانند دیکسترا ، کوتاهترین مسیر و تأخیر را محاسبه می کند یعنی تأخیر هم با استفاده از بسته های Link State و به دست آوردن گراف شبکه محاسبه می شود . (مانند Link State)

:¹OSPF

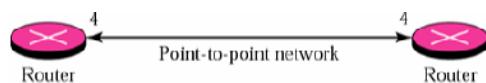
مسیریابهای AS به چهار دسته تقسیم می شود:

- مسیریابهای داخل نواحی
- مسیریابهای لبه های نواحی
- مسیریابهای Back Bone
- مسیریابهای مرزی AS

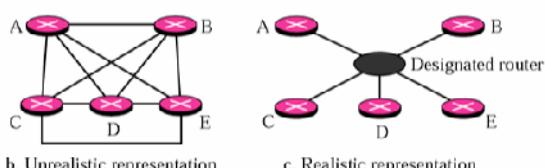
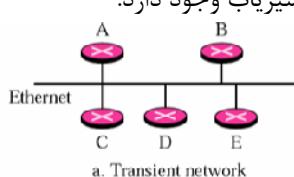


:AS ا نوع اتصالات در

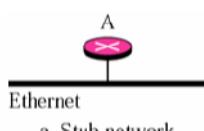
در این ورث دو مسیریاب مستقیماً با شماره پورت یکسان به همدیگر متصل هستند.



در این روش یک مسیریاب به نام Designated Router وظیفه ارائه اطلاعات شبکه را برعهده دارد. در شبکه چند مسیریاب وجود دارد.



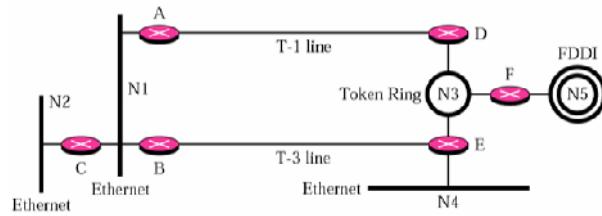
فقط یک مسیریاب به شبکه متصل است.



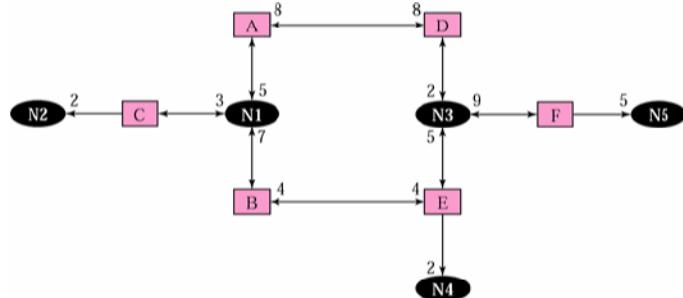
b. Representation

Open Shortest Path First - ¹

مثال: طرح شبکه زیر را با انواع اتصالات بازسازی نماید.

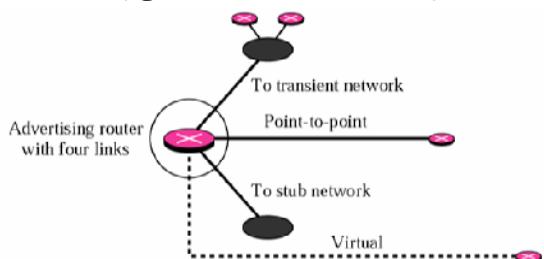


دقت کنید که مسیریابهای با اتصال نقطه به نقطه فقط نیازمند شماره پورت برای ارتباط با هم هستند.

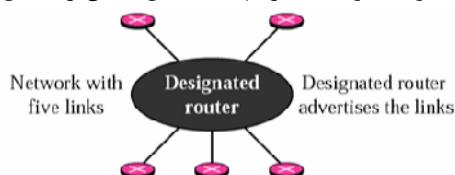


انواع اعلان وضعیت اتصال:

• Router Link: مسیریاب اعلان کننده لینکهای مختلف را می‌پذیرد.

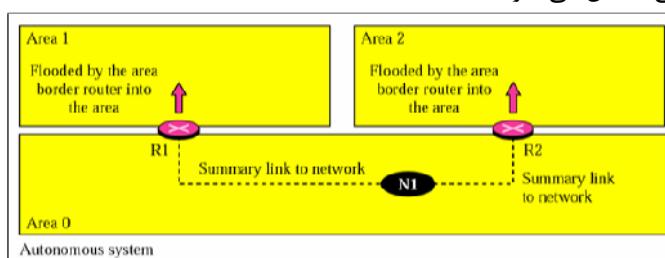


• Network Link: یک شبکه و مجموعه مسیریابهای متصل به آن را شامل می‌شود.



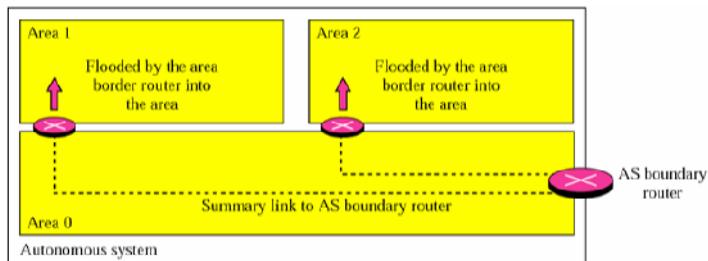
• Summery Link to Network: اطلاعات شبکه‌های داخل نواحی توسط مسیریابهای لبه نواحی

به سایر نواحی منتقل می‌شود.

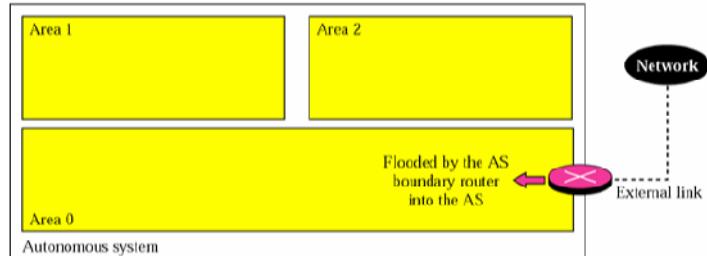


• Summery Link to AS Boundary Router: انتقال اطلاعات داخل AS از مسیریاب مرزی AS

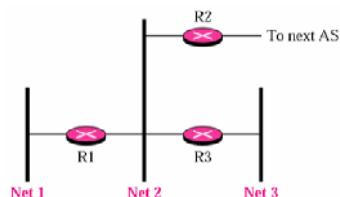
به سایر نواحی



AS: انتقال داده های خارج از AS به داخل AS از طریق مسیریاب مرزی •



مثال: در تصویر زیر معین کنید هر مسیریاب چه Router Link LSA هایی را ارسال می کند.



همه مسیریابها Router Link LSA ها را اعلان می کنند.

.Net1 و Net2 دو اتصال دارد: R1

.Net2 و R2 یک اتصال دارد:

.Net3 و Net2 دو اتصال دارد: R3

کدام مسیریاب اطلاعات Network Link LAS را به خارج ارسال می کند؟

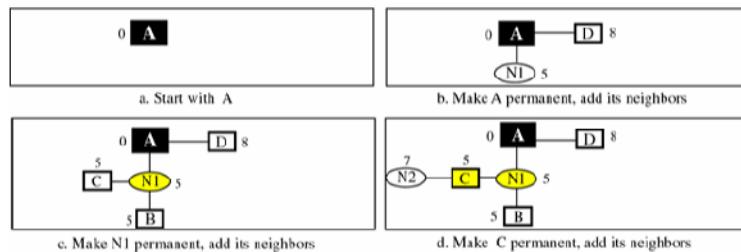
همه سه شبکه باید Network Link LSA ها را اعلان نمایند.

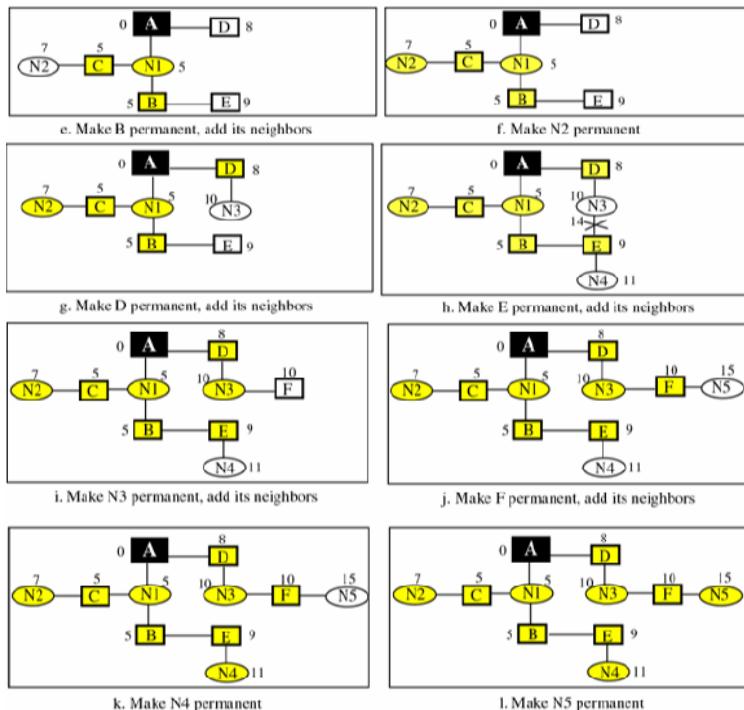
اعلان Net1 بوسیله R1 انجام می گیرد، زیرا تنها مسیریاب متصل به آن است و بنابراین Designated Router می باشد.

اعلان Net2 بوسیله R1 یا R2 و یا R3، براساس اینکه کدامیک از آنها به عنوان Designated Router شود، می تواند انجام گیرد.

اعلان Net3 بوسیله R3 انجام می گیرد، زیرا تنها مسیریاب متصل به آن است و بنابراین Designated Router می باشد.

در OSPF، همه مسیریابها پایگاه Link State یکسان دارند. نحوه محاسبه کوتاهترین مسیر در تصاویر زیر نمایش داده شده است:



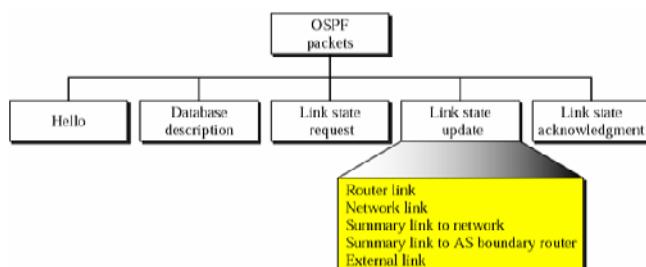


هزینه هر گره از گره قبلی در کنار آن درج شده است. در هر بار اجرای الگوریتم کوتاهترین مسیر، مسیر با کمترین هزینه انتخاب می شود و توسعه داده می شود. چنانچه با توسعه یک مسیر یک حلقه بوجود آید باید با انتخاب کوتاهترین مسیر تا گره جدید، حلقه بوجود آمده را حذف کرد.

سرآیند بسته های OSPF شامل دو قسمت می شود. فرمت قسمت عمومی این سرآیند به شکل زیر می باشد:

Version	Type	Message length
Source router IP address		
Checksum		Authentication type
	Authentication	

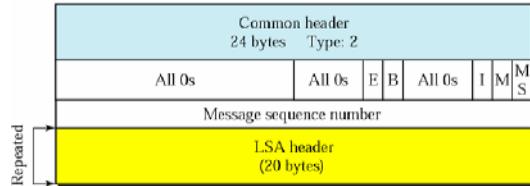
أنواع بسته های OSPF



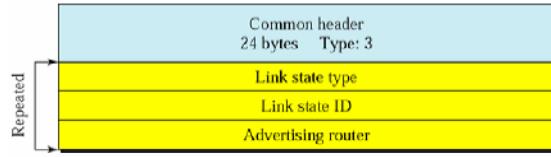
فرمت بسته Hello بصورت زیر می باشد:

Common header 24 bytes	Type: 1			
Network mask				
Hello interval	All 0s	E	T	Priority
Dead interval				
Designated router IP address				
Backup designated router IP address				
Neighbor IP address				
Repeated				

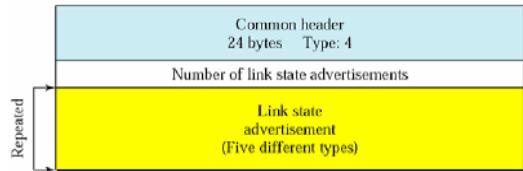
فرمت بسته Database Description



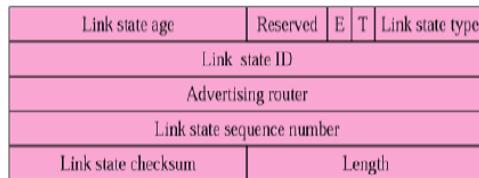
فرمت بسته درخواست Link State



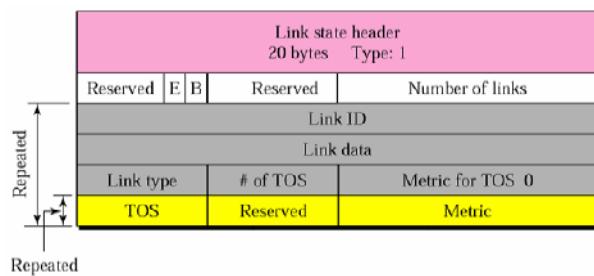
فرمت بسته بروز رسانی Link State



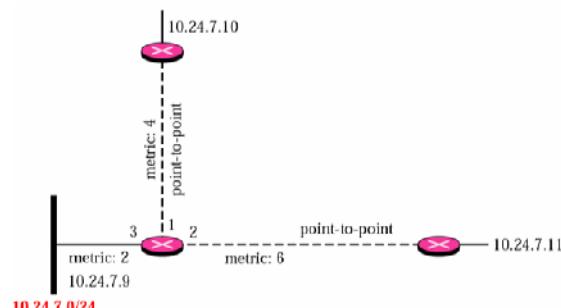
فرمت سرآیند بسته LSA



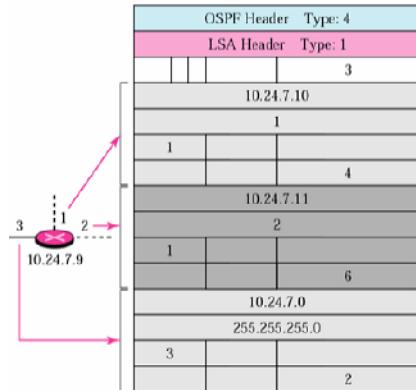
فرمت بسته Router Link LSA



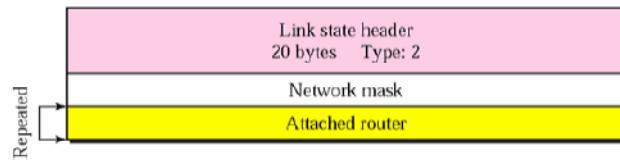
مثال: Router Link LSA ارائه شده توسط مسیریاب 10.24.7.9 چیست؟



این مسیریاب سه پیوند دارد: ۲ تا از نوع ۱ (Point to Point) و یکی از نوع ۳ (Stub). طرح بسته Router Link LSA این مسیریاب به شکل زیر می باشد:

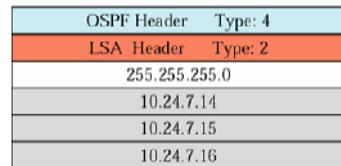


فرمت اعلان Network Link

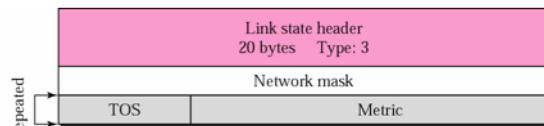


مثال: Network Link LSA طرح رو برو چیست؟

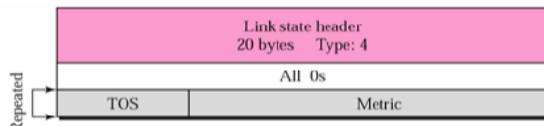
این شبکه دارای سه مسیریاب اتصالی می باشد. LSA آدرس Mask و آدرس مسیریابها را ارائه می دهد. دقیق تر نهایاً یک مسیریاب به عنوان Designated Router را اعلان می کند.



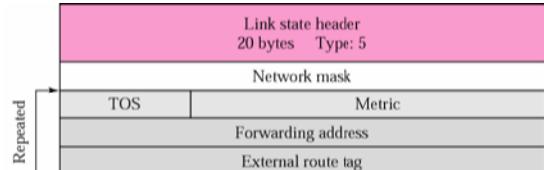
فرمت بسته Summary Link to Network LSA



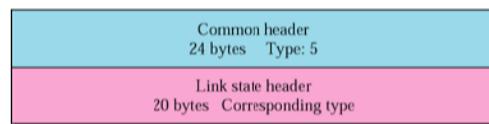
فرمت بسته Summary Link to AS boundary LSA



فرمت بسته External Link



فرمت بسته Link State Acknowledgment



بسته های OSPF در بسته های IP Datagram قرار می گیرند.

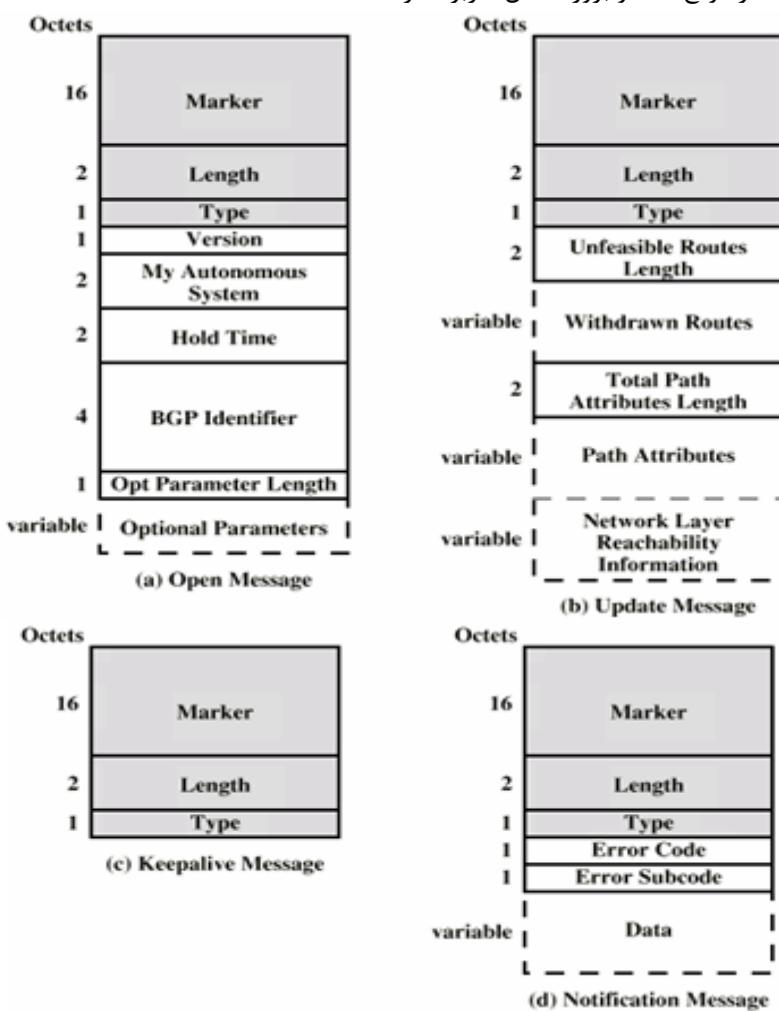
^۱BGP

اینترنت مجموعه ای از AS ها می باشد . هر AS می تواند از وصل شدن چند شبکه مختلف به هم تشکیل شده باشد . چهار پیغام برای BGP تعریف شده است که توسط این چهار پیغام مسیریابی که BGP را اجرا می کنند یکدیگر را شناخته و ردوبدل اطلاعات می کنند .
پیغامهای BGP :

۱. **Open** : یعنی یک مسیریاب دریک AS می خواهد با مسیریاب دیگر در AS دیگر ارتباط برقرار کند (رابطه همسایگی) .

۲. **Update** : انتقال اطلاعات در رابطه با شبکه های فرعی و یا چند hop دسترسی دارد که یک مسیریاب به آن متصل است و بهنگام کردن اتصالات .

۳. **Keepalive** : در پاسخ open وقتی یک مسیریاب می خواهد ارتباط همسایگی را برقرار کند (Ack) .
۴. **Notification** : در موقع خطأ و بروز اشکال کاربرد دارد .



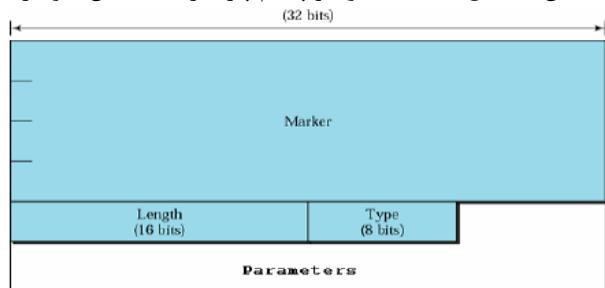
AS Messages

با توجه به پیغامهای فوق سه procedure BGP توسط انجام می شود :

۱. **Neighbour acquisition** : وقتی دو مسیریاب که در همسایگی هم هستند بخواهند رابطه همسایگی برقرار کنند از این procedure استفاده می کنند . ممکن است این درخواست از طرف مسیریاب همسایه قبول نشود (فعلاً) . زمانی که دو مسیریاب آماده بودند با پیغامهای **Keepalive**, **open** این رابطه برقرار می شود .

بعد از برقراری ارتباط ، این procedure توسط ردو بدل کردن اطلاعات به صورت پیامهای Keepalive رابطه همسایگی را بصورت دائم برقرار می کند .
Network reachability.۳ : توسط رد و بدل کردن پیامهای update صورت می گیرد یعنی هر مسیریاب اطلاعات زیر شبکه خود را به مسیریاب دیگر ارسال می کند (یعنی به چند شبکه فرعی و چگونه متصل شده است).

وقتی که تغییراتی در زیر شبکه به وجود آید ، این تغییرها توسط پیامها به مسیریابهای دیگر منعکس می شود . پیامهای BGP از سه بخش تشکیل شده است و هر پیغام پارامترهای خاص خود را دارد .



AS Messages Header Format

سرآیند هر پیغام حداقل ۱۹ بایت است .

طول : طول پیغام

نوع : نوع پیغام

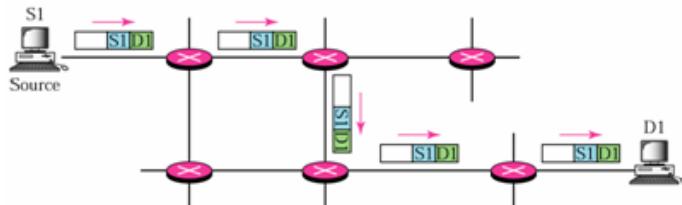
فقط سه بخش بالائی را دارد و پارامتر ندارد . Keepalive

فصل ۷

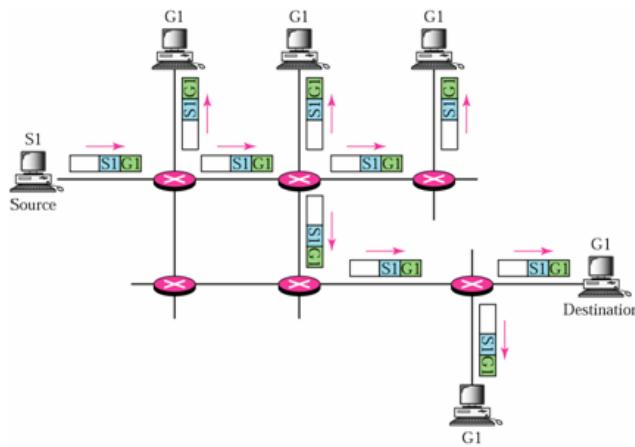
میزبانی Multicast و پروتکل های MultiCasting

ارسال بسته ها در شبکه، به سه صورت انجام می شود:

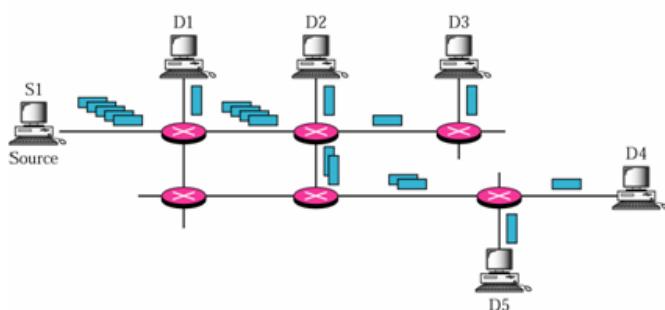
۱. **Unicast** : مسیریاب بسته دریافتی را تنها از یک رابط خود ارسال می کند. در این حالت گروهی از دریافت کننده ها وجود ندارد.



۲. **Multicast** : مسیریاب بسته دریافتی را ممکن است از چند رابط خود ارسال کند. بسته های با آدرس Multicast جهت اعضا یک گروه ارسال می گردد.



تلاش جهت تقلید Multicast بوسیله چند Unicast، نه تنها کارا نیست بلکه باعث ایجاد تاخیر های طولانی ، بخصوص برای گروه های بزرگ، می گردد. عبارت دیگر، کاربرد ارسال Multicast ، جهت ایجاد تبادل موثرتر بین گروه هایی از دستگاه ها ، بوجود آمده است. داده ها در این حالت با یک آدرس Multicast IP ارسال می گردد و بوسیله هر دستگاه با این آدرس، دریافت می گردد.



ابزارهای Multicast از آدرس IP کلاس D، جهت گفتگو استفاده می کند. این آدرس ها در دامنه ای از ۰.۰.۰.۰ تا ۲۳۹.۲۵۵.۲۵۵.۲۵۵ قرار دارد. برای هر آدرس Multicast، یک مجموعه بین صفر تا تعداد زیادی میزبان وجود دارد که به بسته های منتقل شده برای آدرس، گوش می دهند. به این مجموعه از دستگاه ها، یک گروه میزبان، می نامند. میزبانی که به یک

گروه مشخص، بسته هایی را ارسال می نماید، لازم نیست تا عضو آن گروه باشد. میزبان حتی ممکن است اعضای گروه را نداند. دو نوع گروه میزبان وجود دارد.

- ثبت: کاربردهای متعلق به این نوع گروه از یک آدرس IP ثابت تخصیصی بوسیله IANA

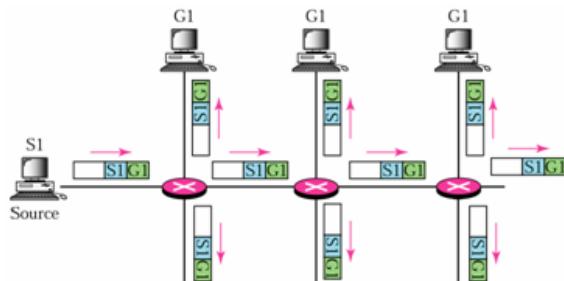
استفاده می نمایند. عضویت در این نوع از گروه ها، ثابت نیست و یک میزبان، بر حسب نیاز، می تواند به یک گروه به پیوندد و یا از آن جدا گردد. یک گروه ثابت، حتی در صورت عدم وجود عضو برای آن، همچنان باقی می ماند. لیست آدرس های IP تخصیصی به گروه های میزبان ثابت، در RFC 1700 آمده است. این آدرس های رزرو شده بشرح زیر می باشند:

- آدرس رزرو شده پایه.
- همه سیستم ها در این زیر شبکه.
- همه مسیریابهای این زیر شبکه.
- RIP2
- OSPF
- OSPF Designated مسیریابی

یک کاربرد می تواند از DNS جهت بدست آوردن آدرس IP تخصیص یافته به یک گروه میزبان ثابت، می تواند استفاده نماید. می توان گروه ثابت از یک آدرس را به کمک یک اشاره گر پرسو جو، مشخص نماید.

- موقع: هر گروهی که ثابت نباشد، موقع خواهد بود. گروه جهت تخصیص پویا در صورت نیاز، موجود می باشد. گروه های موقع در زمان صفر شدن تعداد اعضاء، متوقف می گردند.

۳. Broadcast: مسیریاب بسته دریافتی را از تمام رابطه های خود (بجز رابط ورودی)، ارسال می کند.



در یک شبکه فیزیکی:

این پردازش، آسان می باشد. پردازش ارسال کننده، یک آدرس Multicast IP مقصد را مشخص می نماید. درایور دستگاه این آدرس را به آدرس فیزیکی منطبق با آن تبدیل می نماید و بسته ها را به مقصد ارسال می نماید. پردازش های مقصد نیز با چک کردن درایورهای خود، از دریافت بسته های داده گرام با آدرس Multicast مطلع می گردند.

همانطور که قبلاً نیز گفته شد، جهت نگاشت آدرس IP کلاس D به آدرس فیزیکی مرتبط، تنها از ۲۳ بیت سمت راست آدرس IP استفاده می گردد. بدلیل چشم پوشی از ۵ بیت از آدرس IP در این حالت، بیتهاي ۵ تا ۹ از سمت چپ، این وضع می تواند باعث نکاشت ۳۲ آدرس غیر-یکتا، در یک آدرس فیزیکی گردد. این موضوع نیاز به

فیلتر شدن بسته ها در درایورهای دستگاه را بوجود می آورد. این فرایند بواسیله چک کردن آدرس IP مقصد در سرآیند، قبل از ارسال بسته به لایه IP، انجام می شود. این کار، اطمینان می دهد تا پردازشگاهی دریافت کننده، داده گرامهای نادرست را دریافت ننمایند. ۲ دلیل دیگر جهت نیاز به فیلترگذاری نیز وجود دارد:

- برخی از آدپتورهای LAN، تعداد محدودی آدرس همزمان Multicast را دارند. زمانیکه این محدودیت نقض شود، آنها تمام بسته های Multicast را دریافت می نمایند.
- فیلترها در برخی آدپتورهای LAN، از مقادیر جدول درهم ساز^۱، بجای تمام آدرس Multicast، استفاده می نمایند. اگر ۲ آدرس با مقدار درهم سازی یکسان در یک زمان مورد استفاده قرار بگیرد، فیلتر ممکن است بسته های نقض کننده محدودیت را عبور دهد.

با وجود نیاز برای این نرم افزار فیلتر گذاری، انتقلات Multicast، هنوز هم سربارهای کمی را برای میزانهای شرکت نکرده در نشست خاصی را، باعث می گردد. بویژه، میزانهایی که عضو یک گروه نیستند، به آدرسهای گوش نمی دهند. در چنین موقعیتهایی، بسته های Multicast بواسیله سخت افزار رابط شبکه لایه پایین، فیلتر می گردد.

در بین چند شبکه: Multicast

ترافیک Multicast، به یک شبکه فیزیکی مجزا، محدود نمی گردد. اگرچه، مخاطرات ذاتی در Multicast بین شبکه ای وجود دارد. اگر محیط شامل چندین مسیریاب باشد، باید اطمینان حاصل شود که بسته های Multicast در یک حلقه بینهایت در شبکه گرفتار نیامده اند. ایجاد حلقه مسیردهی Multicast بسیار ساده می باشد. برای چنین آدرسی، پروتکلهای مسیردهی Multicast، جهت تحويل بسته ها، در زمان اجتناب از مسیردهی های حلقه و انتقالات ناقص، توسعه داده شده اند.

دو نیازمندی برای Multicast داده بروی چند شبکه، وجود دارد:

- تعیین مشترکین Multicast: یک مکانیزم جهت تعیین اینکه آیا لازم است بسته داده گرام به شبکه ای خاص ارسال گردد، یا نه. این مکانیزم بواسیله RFC 2236 IGMP برای TTL=0 تعريف می گردد.
- تعیین قلمرو Multicast: مکانیزمی جهت تعیین میدان یک انتقال. برخلاف آدرسهای Unicast، آدرسهای Multicast می توانند در سرتاسر اینترنت، گسترش یابند. برای این منظور از فیلد TTL استفاده می شود.
 - : داده گرام TTL=0 Multicast، با این مقدار، محدود به خود میزان منبع می گردد.
 - : چنین داده گرام هایی، به تمام میزانهای دورن یک شبکه، که عضو گروه هستند، می رسد.
 - : TTL=2 و یا مقدار بیشتر: یک داده گرام Multicast اینچنینی، بواسیله تمام میزانهای روی یک SubNet، که عضو گروه هستند، دریافت می گردد. این عملیات در مسیریابهای Multicast براساس آدرسهای گروه مشخص، انجام می گیرد.
- : 224.0.0.0-224.0.0.255: این دامنه از آدرس، برای کاربردهای Multicast تک پرشی، نامزد می باشد. مسیریابهای Multicast، بسته های داده گرام با آدرس مقصود در این محدوده را ارسال نمی نمایند. از این آدرسها می توان جهت ارسال پیام عضویت در یک گروه، توسط یک میزان، استفاده نمود.

سایرین: داده گرامهای با سایر آدرسهای مقصد D، بصورت نرمال بوسیله مسیریابهای Multicast، ارسال می گردند. مقدار فیلد TTL در هر پرش، یکی کم می شود. این موضوع زمینه ایجاد توسعه حلقه جستجو جهت قرار دادن Multicast نزدیکترین سرویس دهنده سرور گوش دهنده به یک آدرس Multicast مشخص را فراهم می آورد. جهت یافتن این سرور، بسته های داده گرام با مقادیر TTL افزایش یافته در هر مرحله، با شروع از TTL=1، ارسال می گردد، تا زمانیکه نزدیکترین سرویس دهنده پیدا شود.

جهت ارسال بسته های Multicast، به کمک الگوریتمهای ارسال Multicast^۱ و IGMP، مسیر ارسال بصورت یک درخت تشکیل می گردد. این درختها دارای انواع زیر می باشد:

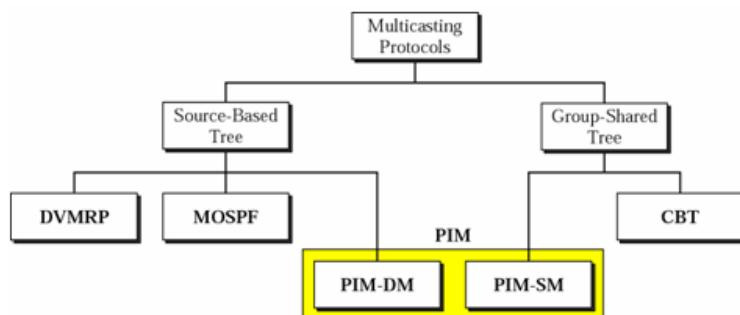
- ۱- درخت مبتنی بر مبدأ^۲: ترکیب مبدأ و گروه ، درخت را مشخص می نماید.
- ۲- درخت مشترک در گروه^۳: گروه طرح درخت را مشخص می کند.

الگوریتمهای ارسال Multicast

این الگوریتمها جهت برپاسازی مسیرهایی در شبکه ، بکار می روند. این مسیرها زمینه دریافت موثر ترافیک Multicast به تمام اعضای گروه را فراهم می آورند. هر الگوریتم باید مجموعه نیازمندیهای زیر را برآورده سازد:

- ارسال داده تنها به اعضای گروه
- بهینه سازی مسیر مبدأ تا مقصد
- ایجاد مسیرهای بدون حلقه
- فراهم آوردن توابع سیگنال دهی قابل توسعه، مورد استفاده در ایجاد و حفظ اعضای گروه
- عدم ایجاد ترافیک متمرکز برروی بخشی از اتصالات شبکه

بر این اساس چندین پروتکل شکل گرفته و مورد استفاده قرار گرفته اند. این الگوریتمها سطوح دسترسی متفاوت به اهداف بالا را فراهم می آورند. ترکیب پروتکل های مسیریابی Multicast بصورت زیر می باشد:



^۴DVMRP انواع

Multicast Forwarding Algorithms - ^۱

Source based - ^۲

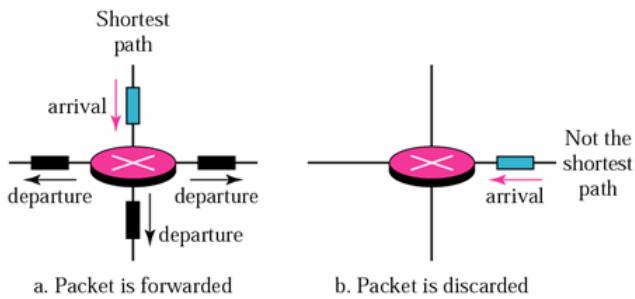
Group Shared - ^۳

Distance Vector Multicast Routing Protocol - ^۴

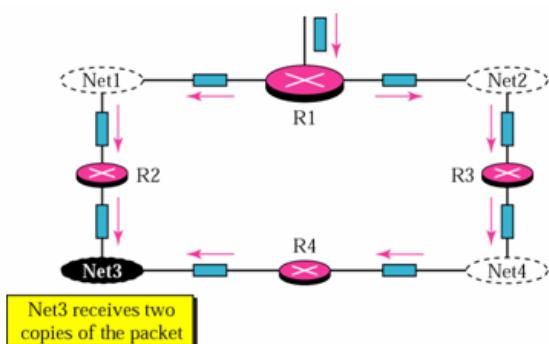
یک پروتکل مسیردهی Multicast برپا شده، می باشد(RFC 1075). این استاندارد در ابتدا برای پردازش mroute در برخی از سیستمهای یونیکس، ایجاد گردید. DVMRP یک پروتکل درونی می باشد و جهت ایجاد درختهای برای هر منبع، برای هر گروه^۱ در درختهای تحويل Multicast در AS بکار می رود.

DVMRP داده گرامهای Unicast را پشتیبانی نمی کند و مسیریابهای پشتیبانی کننده از Unicast توام با Multicast، باید با دو الگوریتم مسیردهی متفاوت، پیکربندی شوند. بدليل وجود این پردازشها جدأگانه، ترافیکهای Multicast و Unicast، الزاماً مسیر یکسانی را در شبکه طی نخواهند کرد.

- ارسال مسیر معکوس(RPF²): مسیریاب بسته های رسیده با کوتاهترین از مبدأ به مسیریاب را به سایر رابطهایش ارسال می کند؛ در غیر این صورت بسته دور ریخته می شود. این مکانیزم با استفاده از جدول مسیر معکوس، محقق می گردد.

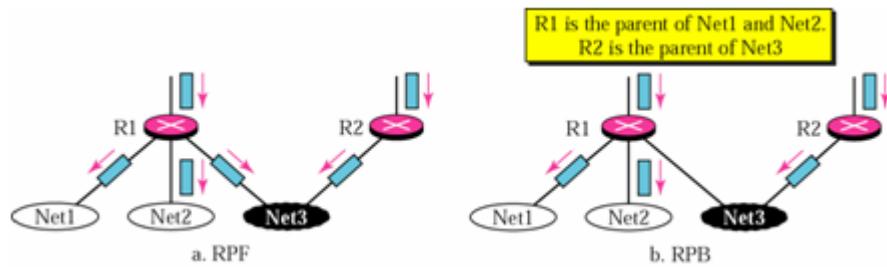


از مزایای این روش می توان به تحويل سریع بسته، بدليل استفاده از کوتاه ترین مسیر ممکن بین مبدأ و مقصد، اشاره نمود. همچنین با این روش بدليل ایجاد درختهای جدأگانه در گره، استفاده کاراتر از منابع شبکه را باعث می گردد، هر بسته تحويلی بر روی چند اتصال شبکه منتشر می گردد. با این روش جلوی حلقه ها گرفته می شود؛ اما ممکن است از چند مسیر مختلف، بسته های مشابه به یک شبکه برسد.

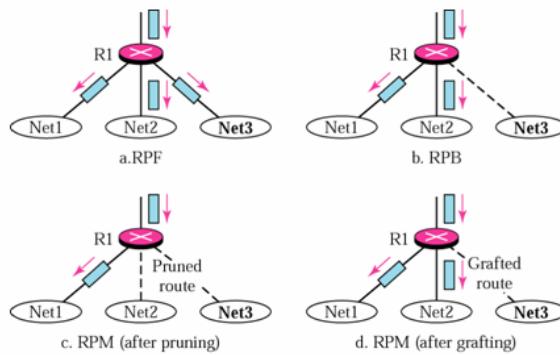


- مسیر معکوس (RPB): در این روش جهت حل مشکل روش قبلی، از درخت کوتاهترین مسیر Broadcast از مبدأ به هر مقصد استفاده می شود. به این ترتیب تضمین می گردد که هر مقصد تنها یک بسته را دریافت نماید. در درخت فوق هر شبکه به یک مسیریاب منتنسب می شود و مسیریاب نقش والد آن شبکه را بازی می کند.

Per-Source Per-Group - ¹
Reverse Path Forwarding - ²



مسیر معکوس (RPM): در این روش امکان تغییرات پویای عضویت (هرس شدن و یا پیوند خوردن اعضاء) به RPB افزورده شده و به این ترتیب بجای درخت کوتاهترین مسیر Broadcast، درخت کوتاهترین مسیر Multicast ایجاد می‌گردد.



ایجاد درخت تحويل :Multicast

یک مسیریاب Multicast بسته‌ها را به دو دسته از ابزارها، منتقل می‌کند: مسیریابها و میزبانهای پایین رو که اعضای یک گروه Multicast معین، می‌باشند. اگر یک مسیریاب Multicast وابستگی به همسایه‌های پایین رو خود، از طریق یک رابط خاص، ندارد، شبکه یک شبکه برگ می‌باشد. درخت تحويل، با اطلاعات مسیریابی تشریح کننده این انواع مختلف مقصد، ساخته می‌شود.

اگر رابط جریان پایین رو، به یک شبکه برگ متصل باشد، بسته‌ها تنها به میزبانهایی که اعضای گروه Multicast خاصی هستند، ارسال می‌گردد. مسیریاب این اطلاعات را از پایگاه داده محلی گروه IGMP بدست می‌آورد. اگر آدرس گروه در پایگاه داده لیست شده باشد و مسیریاب نیز ارسال کننده نامزد جهت منبع باشد، رابط در درخت تحويل Multicast، گنجانده می‌شود. اگر اعضای گروه، وجود نداشته باشند، رابط مستثنی می‌گردد.

در آغاز، همه شبکه‌های غیر برگ، در درخت تحويل Multicast، گنجانده شده‌اند. این به هر مسیریاب پایین رو، امکان سهیم شدن در ترافیکهای ارسالی برای هر گروه را می‌دهد.

مسیریابهای متصل به یک شبکه برگ، یک رابط را در صورتیکه اعضای مرتبط با یک رابط، دیگر در فعالیتهای گروه Multicast خاص، فعال نباشند، حذف می‌نماید. با انجام این کار، بسته‌های Multicast، دیگر از طریق آن رابط ارسال نمی‌شوند. اگر یک مسیریاب قادر به حذف تمام رابطهای جریان پایین رو خود، برای گروه خاصی باشد، همسایه بالاتر خود را آگاه می‌سازد که نیازی به ترافیک برای زوج منبع و گروه خاص، ندارد. این اطلاع دهنده ارسال یک پیام هرس شدن¹ به همسایه بالاتر، صورت می‌پذیرد. اگر یک همسایه بالاتر، چنین پیامی را از هریک از مسیریاب‌های پایین رو در یک رابط، دریافت نمود، این مسیریاب می‌تواند براحتی رابطش را از درخت تحويل Multicast، حذف نماید. این روش در مورد مسیریابهای سطوح بالاتر نیز عیناً اتفاق می‌افتد و به این وسیله شاخه‌های اضافی درخت تحويل، حذف می‌گردد.

¹ Prune Message –

جهت حذف اطلاعات هرس خارج از رده، هر پیام هرس، شامل یک زمانبند دوره حیات هرس می باشد. این زمان، دوره زمانیست که هرس تاثیر گذار می باشد. اگر یک رابط در پایان دوره هرس و انقضای زمانبند آن، همچنان هرس شده باشد، آن رابط دوباره به درخت تحويل Multicast، متصل می گردد. درصورت اشتباه بودن این عمل و عدم نیاز به ارسال داده از طریق آن رابط، مجدداً مکانیزم هرس بکار می افتد.

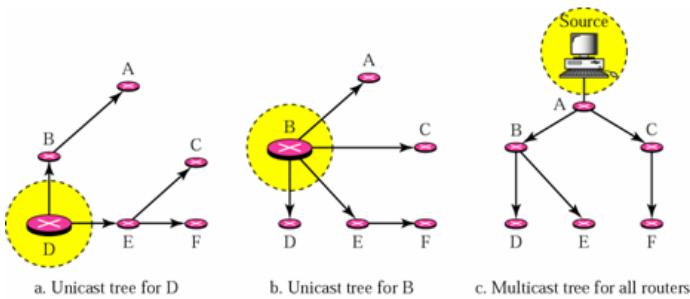
از آنجا که IP از عضویت پویا در گروه، حمایت می کند، میزبانها ممکن است در هر زمانی به عضویت یک گروه Multicast درآیند. زمانی که این امر اتفاق افتاد، مسیریابهای DVMRP، از پیام های پیوند¹، جهت اتصال مجدد شبکه به درخت تحويل Multicast، استفاده می نماید. یک پیام پیوند، به عنوان نتیجه دریافت یک گزارش عضویت IGMP برای یک گروه، که قبلاً هرس شده بود، ارسال می گردد. پیامهای پیوند مجزا، برای هر منبع شبکه که هرس شده بود، به همسایه های بالاتر ارسال می گردد.

دریافت یک پیام پیوند بوسیله یک پیام تایید، تصدیق می گردد. این امر به فرستنده اجازه می دهد تا بین یک بسته پیوند مفقود شده و یک ابزار غیر فعال، تفاوت قائل گردد. اگر یک پیام تایید، در دوره زمانی مشخص آن، دریافت نگردید، درخواست مجدد ارسال می گردد. هدف پیام تایید، تایید دریافت یک پیام پیوند می باشد. بنابراین، همه پیامهای درخواست پیوند، حتی درصورتیکه باعث انجام عملی، توسط مسیریاب دریافت کننده نگردد، تایید می گردد.

برخی از مسیریابهای IP، ممکن است جهت پشتیبانی از مسیردهی های Multicast محلی، پیکربندی نشده باشند. DVMRP توانایی تولن سازی داده گرامهای IP Multicast را در مسیرهایی از شبکه که چنین مسیریابهایی را دارند، را فراهم می آورد. در چنین مواردی داده گرامهای در بسته های IP Unicast قرار می دهند و این بسته ها را در شبکه ارسال می کنند. وقتی بسته به نقطه انتهایی دیگر تولن می رسدند، بسته Multicast استخراج شده و با اعمال Multicast استاندارد DVMRP، در زیر شبکه ها ارسال می نماید.

:۳MOSPF

در این روش هر مسیریاب درخت Unicast خودش از شبکه را دارد؛ اما با درنظر گرفتن یک مبدأ(یک ایستگاه کاری)، می توان یک درخت Multicast برای تمام مسیریابهای شبکه ایجاد نمود. در این روش از درخت مبدأ-پایه استفاده شده است.



:۴CBT

الگوریتم CBT، روش دیگری را جهت تعیین مسیرهای بهینه بین اعضای یک گروه Multicast، توصیف می نماید. در این روش از یک مسیریاب مرکزی به نام مسیریاب میعادگاه² استفاده می شود. مبدأ، بدلیل آنکه

Graft Message – ¹

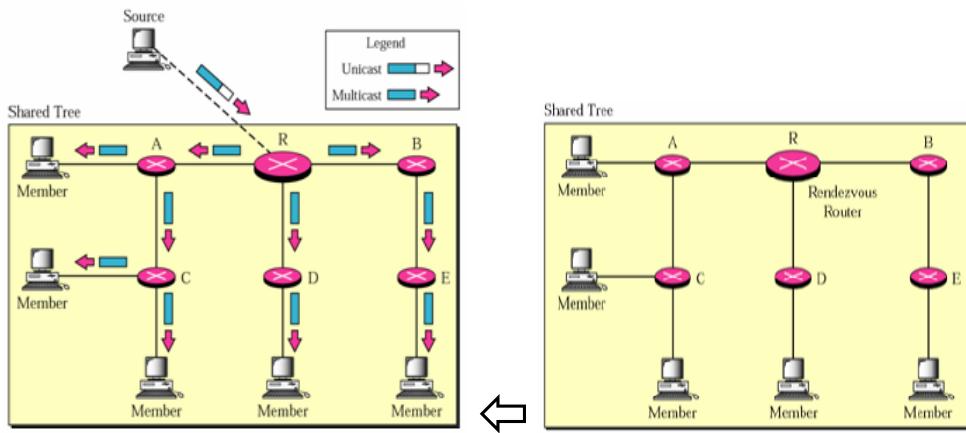
Multicast OSPF – ²

Center Based Tree – ³

Rendezvous – ⁴

می تواند جزء گروه نباشد، بسته های Unicast را در بسته های Multicast مخصوص کرده و این بسته های را به مسیریاب میعادگاه می فرستد. این مسیریاب جزئی از درخت گروه می باشد. مسیریاب میعادگاه این بسته های Multicast را بازیابی نموده و برای اعضای گروه، Multicast می نماید.

در این روش از درخت مشترک در گروه، استفاده شده است. هر مسیریابی یک درخت واحد را برای کل گروه حفظ می نماید که مغایر با RPF و روش های مشابه می باشد. در RPF، هر ارسال کننده در یک گروه درخت خودش را دارد. مشکل این روش، ایجاد مسیر های احتمالی کمتر بهینه برای برخی منابع و دریافت کنندگان، می باشد.



:PIM

پیچیدگی MOSPF باعث جلب توجه به PIM گردید. PIM یک پروتکل مسیردهی Multicast دیگر می باشد. برخلاف MOSPF، PIM از هرگونه پروتکل مسیردهی Unicast، جدا می باشد. با این وجود با همه پروتکلهای مسیردهی Unicast، کار می کند. PIM دو شیوه و یا عمل کرد را معرفی می کند:

- شیوه متراکم (PIM-DM)^۲
- شیوه پراکنده (PIM-SM)^۳، RFC 2362

شیوه متراکم و شیوه پراکنده، به تراکم اعضای گروه در یک ناحیه، ارجاع می دهد. یک گروه به عنوان متراکم شناخته می شود، اگر احتمال یافتن حداقل یک عضو گروه، بالا باشد. این موضوع حتی در مورد اندازه های کوچک نیز صادق است. اگر احتمال یافتن یک عضو گروه، کم باشد، یک گروه، پراکنده شناخته می شود. PIM توانایی سوئیچ بین شیوه پراکنده و متراکم را فراهم می نماید. همچنین اجازه استفاده از هر دو شیوه در یک گروه یکسان را می دهد.

:PIM-DM

ابزار PIM-DM، یک بسته را دریافت می کند؛ این ابزار، تایید اعتبار ورودیها را با استفاده از جدول مسیردهی Unicast موجود، انجام می دهد. اگر ورودیها، بهترین مسیر به منبع را منعکس نمایند، مسیریاب بسته های Multicast را منتشر می کند. بسته به همه رابطهایی که از درخت تحویل Multicast حذف نشده اند، ارسال می گردد.

¹ Protocol Independent Multicast -

² Protocol Independent Multicast-Dense Multicast -

³ Protocol Independent Multicast-Sparse Multicast -

برخلاف PIM-DM، DVMRP تلاشی جهت محاسبه مسیریابهای مشخص Multicast، انجام نمی‌دهد. بلکه فرض می‌کند که مسیریابهای جدول مسیردهی Unicast، متقارن هستند. همانند عملیات در یک محیط PIM-DM، یک ابزار Multicast دریافتی می‌باشد. مسیریابها دیتاگرامها را به همه نواحی شبکه، ارسال می‌کند. اگر برخی از نواحی، دریافت کننده‌هایی برای گروه Multicast خاصی را نداشته باشند، PIM-DM، این شاخه‌ها را از درخت تحویل، حذف می‌نماید. فرایند حذف بدلیل آنکه PIM-DM اطلاعات دریافت کننده‌های پایین را از جدول مسیردهی Unicast بدست نمی‌آورد، فعال می‌شود. PIM-DM پیاده‌سازی راحتی دارد. تنها فرض لازم آنست که یک مسیریاب قادر باشد تا لیستی از درخواستهای هرس را حفظ نماید. با شیوه‌های جریان دهی و هرس بکار رفته در PIM-DM، این پروتکل باید در محیط‌های که اکثر میزبانهای یک دامنه نیازمند دریافت داده‌های Multicast باشند، بکار می‌رود. در چنین محیط‌هایی، اکثربیت شبکه‌ها از درخت تحویل حذف نخواهند شد. سربار جریان دهی نیز کم می‌باشد. این پیکربندی در موارد زیر نیز مناسب می‌باشد:

- فرستنده‌ها و گیرنده‌ها در فاصله کمی از یکدیگر قرار دارند.
- تعداد فرستنده‌ها کم و تعداد دریافت کننده‌ها زیاد باشد.
- حجم ترافیک Multicast زیاد است.
- جریان ترافیک Multicast ثابت است.

برخلاف PIM-DM، DVMRP از تونلها، جهت انتقال ترافیک Multicast در شبکه‌های غیر Multicast حمایت نمی‌کند. بنابراین، مدیر شبکه باید مطمئن باشد که ابزارهای متصل به مسیرهای انتهایی، توانایی Multicast را دارند.

:PIM-SM

از این روش در محیط‌های پراکنده همانند WAN، استفاده می‌شود. این روش همانند CBT است اما از روش‌های ساده‌تری استفاده می‌کند.

:MBONE

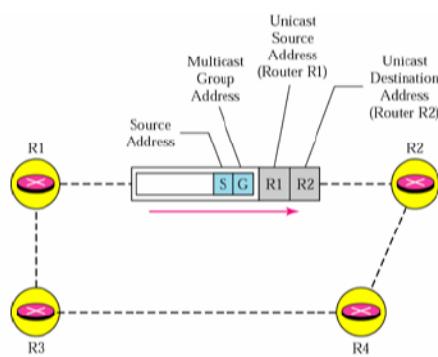
MBONE در مارس ۱۹۹۲ پیاده سازی گردید. این شبکه اساساً جهت پروتکلهای Multicast، توسعه یافته است. اولین کاربرد این شبکه در نشست صوتی IETF Multicast بود. در آن زمان ۲۰ سایت به این شبکه متصل بود. دو سال بعد، انتقالات صوتی و تصویری مشابه، در بیش از ۵۰۰ نقطه در ۱۵ کشور، توزیع شده بود. از آن پس، MBONE برای Broadcast ماموریت‌های شاتل فضایی ناسا، کنسرت‌های راک و تعداد زیادی از کنفرانس‌های علمی، بکار رفته است. کاربردهای تجاری و خصوصی از MBONE هنوز هم در حال استفاده است.

Multicast Backbone به عنوان یک شبکه پوشش مجازی، با استفاده از ساختار فیزیکی اینترنت، شروع شد. در آن زمان، مسیردهی Multicast، در ابزارهای مسیردهی استاندارد، پشتیبانی نمی‌شد. اولین نقاط MBONE، در سیستمهای یونیکس مجهز به پردازنش مسیردهی mroute، شکل گرفت. امروزه MBONE هنوز هم عملیاتی است، اما دیگر اتصالات Multicast بصورت محلی در بسیاری از مسیریابهای اینترنت، انجام می‌گیرد. تلاشهایی جهت یکپارچه کردن مستقیم MBONE با ساختار اینترنت، در حال انجام می‌باشد.

ترافیکهای Multicast بروی همه قسمتهای اینترنت، جریان نمی‌یابند. بدلیل این محدودیت، بصورت مجموعه‌ای از نواحی شبکه‌های Multicast می‌باشد. این نواحی از طریق تونلهای مجازی به یکدیگر متصل شده‌اند. تونل‌ها نقش پل را بر روی نواحی که از ترافیک Multicast حمایت نمی‌کنند، بازی می‌کنند.

یک مسیریاب که نیازمند ارسال بسته‌های Multicast به نواحی Multicast دیگر است، این بسته‌ها را در بسته‌های Unicast قرار می‌دهد. این بسته‌های مخصوص شده، از طریق مسیریابهای استاندارد اینترنت، منتقل می‌گردند. آدرس مقصد در بسته Unicast، نقطه انتهایی تونل می‌باشد. مسیریاب انتهایی دیگر تونل، سرآیند را برداشت و بسته‌های Multicast را به گیرنده‌ها، ارسال می‌دارد.

تونلهای MBONE دارای پارامترهای اندازه‌ای و سطح اندازه‌ای باشد. پارامترهای اندازه‌ای، به عنوان یک هزینه در الگوریتمهای مسیردهی Multicast، بکار می‌رود. الگوریتمهای مسیردهی، این مقادیر را برای انتخاب بهترین مسیر در شبکه، بکار می‌برند. تونلهای از مقادیر اندازه‌ای متفاوت، جهت انتقال ترافیک نامتوازن در شبکه، استفاده می‌کند.



بخش ۳:

سوئیچ داده

فصل ۶: روش‌های سوئیچ داده

فصل ۷: شبکه‌های ATM و FrameRelay

فصل ۸: MPLS، ISA و DiffServ

فصل ۶:

روش‌های سوئیچ داده

در سال ۱۹۷۰، سوئیچ بسته ای به عنوان معماری جهت انتقال داده دیجیتال فواصل دور معرفی گردید. این فناوری در طول زمان تغییراتی یافته است، اما باید در نظر داشت که:

۱- پایه های فناوری سوئیچ بسته ای امروزی همانهایی است که در شبکه های اولیه ۱۹۷۰، وجود داشته است.

۲- سوئیچ بسته ای هنوز هم یکی از فناوریهای موثر در انتقال داده فواصل دور می باشد.

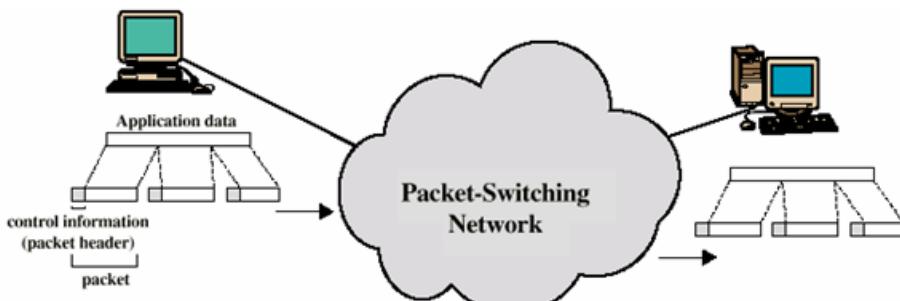
این فصل مروری دارد بر فناوری سوئیچ بسته ای و بسیاری از مزایای سوئیچ بسته ای (انعطاف پذیری، اشتراک منابع، قوی بودن، حساسیت) را به همراه هزینه خواهیم دید. یک شبکه سوئیچ بسته ای، مجموعه توزیع شده ای از گره های سوئیچ بسته ای است. بصورت ایده آل، تمام گره های سوئیچ بسته ای همیشه از وضعیت کل شبکه آگاهند. متاسفانه، بدلیل توزیع شده بودن گره ها، یک تاخیر زمانی بین تعویض وضعیت در بخش هایی از شبکه وجود دارد و دانش آن تغییرات در جای دیگری هستند. بعلاوه تبادل اطلاعات، خود شامل سربارهایی می باشد. عنوان یک نتیجه می توان گفت که یک شبکه سوئیچ بسته ای، هیچگاه بصورت کامل عمل نمی کند و از الگوریتمهای دیگری جهت کاهش تاخیر زمانی و جبران سربار عملیات شبکه ای استفاده می شود.

مفاهیم سوئیچ بسته ای:

شبکه های ارتباطی سوئیچ مداری دوربرد، بطور خاص جهت مدیریت ترافیک صوت طراحی شده اند و ترافیک عمده در آنها صوت می باشد. یک خصوصیت کلیدی در شبکه سوئیچ مداری، تخصیص منابع شبکه به تماسهای خاص می باشد. برای اتصالات صوتی، مدار حاصل بهره وری بالایی دارد، زیرا در اغلب زمان اتصال، حداقل یکی از طرفین اتصال در حال گفتگو است. با این وجود زمانیکه شروع به استفاده از شبکه های مداری جهت انتقال داده شد، دو کمبود نمود یافت:

۱- در یک اتصال داده کاربر/میزبان خاص (همانند Login کامپیوتر های شخصی به یک سرور پایگاه داده)، در اکثر اوقات خط بیکار است. بنابراین در اتصالات داده ای، سوئیچ مداری ناکاراست.

۲- در یک شبکه سوئیچ مداری، اتصالات، نرخ داده ارسالی ثابتی را فراهم می آورند. بنابراین هر کدام از دو طرف اتصال باید دریافت و ارسال داده با نرخ یکسان به یکدیگر داشته باشند. این موضوع سبب محدودیت بهره وری شبکه در اتصال تعداد متغیری از کامپیوترهای میزبان و ایستگاه کاری می گردد.



تصویر ۶-۱: استفاده از بسته ها

جهت درک برخورد سوئیچ بسته ای با این مشکلات، اجازه بدھید مختصری در مورد عملکرد سوئیچ بسته ای، توضیح بدهیم. داده ها در بسته های کوچک منتقل می شوند. یک سقف بالای خاص برای طول بسته ها، ۱۰۰۰ بایت می باشد. اگر یک منبع، پیام طولانی تری جهت ارسال داشته باشد، پیام به مجموعه ای از بسته تقسیم شده و هر بسته شامل بخشی از (و یا تمام یک پیام کوتاه) داده های کاربر، بعلاوه برخی داده های کنترلی می باشد.

داده های کنترلی، حداقل شامل نیازمندیهای شبکه جهت مسیریابی بسته در طول شبکه و تحويل آن به مقصد مورد نظر، می باشد. در هر گره مسیر، بسته دریافت شده مدت کوتاهی ذخیره شده و سپس به گره بعدی ارسال می گردد. این روش مزایایی را بر سوئیچ مداری دارد که عبارتست از:

- ۱- کارایی خط بیشتر می شود، زیرا یک پیوند گره به گره می تواند بین بسته های زیادی در طول زمان به اشتراک گذاشته شود. بسته های رسیده از صف برداشته شده و با سرعترين حد ممکن از طریق پیوند، ارسال می شوند. در مقایسه با سوئیچ مداری، زمان پیوند گره به گره از قبل توسط مالتی پلکس تقسیم زمانی همزمان^۱، تخصیص می یابد. در بسیاری از زمانها، اتصال ممکن است بدليل خالی بودن بخشی از زمان تخصیصی به یک پیوند، خالی باشد.
- ۲- یک شبکه سوئیچ بسته ای می تواند بصورت نرخ داده متغیر عمل کند. دو ایستگاه با نرخ داده متفاوت می توانند به تبادل داده پردازنند؛ زیرا هر اتصال نرخ داده مختص خود را دارد.
- ۳- زمانیکه ترافیک در یک شبکه سوئیچ بسته ای، سنگین شد، برخی اتصالات مسدود می شوند و شبکه در خواستهای اتصال اضافی را تا زمان کاهش بار شبکه، رد می کند. در یک شبکه سوئیچ بسته ای، بسته ها همچنان پذیرفته می شوند، اما تاخیر تحويل بسته، افزایش می یابد.
- ۴- اولویت قابل استفاده است. از آنجاییکه یک گره دارای تعدادی بسته قرار گرفته در صف، جهت انتقال می باشد، می تواند ابتدا بسته های با اولویت بالا را ارسال کند. بنابراین، این بسته ها در برابر بسته های با اولویت پایین، تاخیر کمتری را تجربه می کنند.

تکنیک سوئیچ:

اگر یک ایستگاه پیامی را جهت ارسال از طریق یک شبکه سوئیچ بسته ای داشته باشد که طول آن از حد اکثر طول مجاز بسته بزرگتر باشد، آن را به بسته های کوچکتر تقسیم نموده و یکی یکی این بسته ها را به شبکه ارسال می نماید. سوالی که می تواند مطرح شود آنست که شبکه چگونه این جریان بسته ها را جهت مسیریابی در شبکه و تحويل به مقصد مورد نظر، مدیریت می کند. دو راه برای این موضوع در شبکه های کنونی وجود دارد: داده گرام و مداری مجازی.

در داده گرام، هر بسته بصورت مجزا عمل کرده و ارجاعی از قبل برای بسته ها وجود ندارد. در مداری مجازی، یک مسیر از قبل طرح شده، قبل از ارسال هرگونه بسته ای، برپا می گردد. در هر زمان هر ایستگاه می تواند بیش از یک مدار مجازی به سایر ایستگاه ها داشته باشد و مدارات مجازی می توانند برای بیش از یک ایستگاه مورد استفاده قرار گیرند.

بنابراین اصل مهمترین ویژگی در روش مدار مجازی، ایجاد یک مسیر، قبل از انتقال داده است. توجه کنید که این به این معنا نیست که این مسیر، یک مسیر تخصیص یافته همانند سوئیچ مداری می باشد. هر بسته هنوز هم در هر گره بافر می شود و جهت خروج از یک خط، در صف قرار می گیرد و این در حالیست که همزمان، بسته های دیگری بر روی کانالهای مجازی دیگر نیز، ممکن است بصورت اشتراکی از همان خط استفاده کنند. تفاوت این روش با داده گرام در آنست که گره نیازی به تصمیم گیری در هر مسیر هر بسته ندارد و مسیر فقط یک بار برای همه بسته ها با استفاده از مدار مجازی، ایجاد می گردد.

اگر دو ایستگاه از قبل قصد تبادل داده بر روی یک بازه زمانی گستردۀ را داشته باشند، مزایای مشخصی از مدارات مجازی مشخص می گردد: اول اینکه شبکه ممکن است سرویسهای مرتبط با مدار مجازی شامل توالی و کنترل خط، را فراهم کند. توالی به این حقیقت اشاره می کند که بدليل جریان یافتن همه بسته ها از یک مسیر، آنها با همان ترتیب اولیه دریافت می گردند. کنترل خط سرویسی است که اطمینان می دهد که نه تنها همه

^۱ Synchronous Time-Division Multiplexing –

بسته ها با توالی درست دریافت می گردد، که همه بسته ها دریافتی صحیح نیز باشند. برای مثال اگر یک بسته در یک توالی از گره A به گره B نرسد و یا با خطأ برسد، گره B می تواند درخواست ارسال مجدد آن را از گره A داشته باشد. مزیت دیگر آنست که بسته با یک مدار مجازی، سریعتر در شبکه منتقل می شود؛ زیرا نیازی به تصمیم گیری در مورد هر بسته در گره وجود ندارد.

یکی از مزایای داده گرام، اختناب از فاز برپاسازی اتصال می باشد. اگر یک ایستگاه بخواهد تنها یک یا تعداد کمی بسته را ارسال کند، تحويل داده گرامی سریعتر خواهد بود. مزیت دیگر داده گرام آنست که بدليل ابتدایی بودن بیشتر آن، قابل انعطافتر می باشد. برای مثال اگر تراکم در بخشی از شبکه اتفاق بیافتد، داده گرام های ورودی می توانند در مسیری خارج از تراکم، مسیردهی گرددند. با استفاده از کاتال مجازی، بسته ها از یک مسیر از پیش تعیین شده عبور می نمایند و بنابراین برای شبکه مشکل است تا خود را با شرایط تراکم، وفق دهد. مزیت سوم داده گرام، تحويل ذاتاً قابل اعتمادتر آنست. با استفاده از مدارات مجازی، اگر یک گره از مدار خراب شود. همه مسیرهای مجازی عبوری از آن گره، از دست می رود. با تحويل داده گرامی، اگر یکی از گره ها از دست بروند، بسته های بعدی ممکن است بتوانند مسیر جایگزین را بیابند و از آن گره بگذرند.

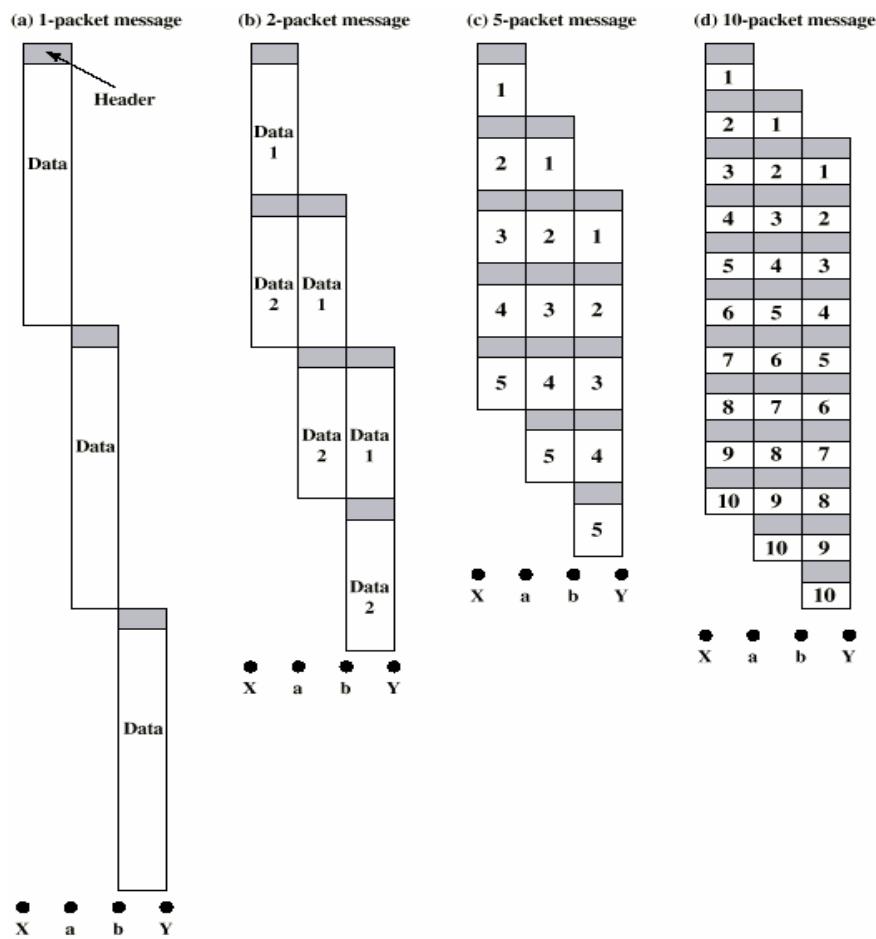
اکثر شبکه های سوئیچ بسته ای موجود، از مدارات مجازی برای اعمال داخلیشان استفاده می کند. این موضوع جهت گیری تاریخی برای ایجاد شبکه ای که بتواند در توالی، سرویسهای مطمئن همانند یک شبکه سوئیچ مداری، ارائه دهد را نمایان می سازد. با این وجود، برخی از تهیه کنندگان شبکه های سوئیچ بسته ای خصوصی از عملکرد داده گرامی استفاده می کنند. از دیدگاه کاربران باید تفاوت اندکی بین رفتار خارجی در استفاده از داده گرام و مدار مجازی، وجود داشته باشد.

طول بسته:

همانطور که در تصویر ۶-۲ مشاهده می شود، بین طول بسته و زمان انتقال، رابطه مهمی وجود دارد. در این مثال، ما فرض کرده ایم که یک مدار مجازی از ایستگاه X، از طریق گره های a و b، به ایستگاه Z، وجود دارد. پیام ارسالی ۴۰ بایت است و هر بسته ۳ بایت اطلاعات کنترلی دارد که در ابتدای بسته قرار گرفته و عنوان سرآیند عمل می کند. اگر کل پیام بصورت یک بسته ۴۳ بایتی (۳ بایت سرآیند بعلاوه ۴۰ بایت داده) فرستاده شود و بسته از ایستگاه X به گره a ارسال شود؛ زمانیکه بسته در a دریافت گردد، می تواند از a به b ارسال گردد. و زمانیکه b آن را کامل دریافت نماید، می تواند آن را به Z ارسال کند. با درنظر نگرفتن زمان سوئیچ، زمان کل انتقال به اندازه زمان انتقال ۱۲۹ بایت (۳×۴۳ بسته انتقال یافته) می باشد. فرض کنید که پیام را به دو بسته، هر کدام ۲۰ بایت، تقسیم نموده ایم و البته هر کدام ۳ بایت سرآیند یا اطلاعات کنترلی دارند. در این حالت گره a، بلافصله پس از دریافت اولین بسته از X، بدون آنکه بخواهد منتظر دریافت بسته دوم شود، می تواند آن را ارسال نماید. بدليل این همپوشانی زمان انتقال، کل زمان انتقال به زمان انتقال ۹۲ بایت، تقلیل می یابد. با تقسیم پیام به ۵ بسته، هر گره میانی می تواند سریعتر انتقال را شروع نماید و در نتیجه زمان صرفه جویی شده بیشتر می شود (زمان انتقال ۷۷ بایت برای انتقال). اگرچه اگر از بسته های بیشتر و کوچکتر استفاده کنیم، عاقبت نتیجه، افزایش تاخیر، بجائی کاهش آن، می باشد. این بدليل آنست که هر بسته شامل یک سرآیند با طول ثابت است و بسته های بیشتر به معنی سرآیندهای بیشتر می باشد. بعلاوه این مثال تاخیرهای پردازش و صف گذاری را نشان نداده است. این تاخیرها در زمان مدیریت بسته های بیشتر برای یک پیام، بزرگتر هستند. با این وجود خواهیم دید که بسته های کوچک ۵۳ بایتی ATM می توانند در طراحی یک شبکه کارامد، بکار روند.

مقایسه سوئیچ مداری با سوئیچ بسته ای:

با نگاهی به عملکرد داخلی یک سوئیچ بسته ای، می توانیم به مقایسه این روش با سوئیچ مداری، بپردازیم. ابتدا به موضوع مهم کارایی نگاه کرده و سپس سایر خواص را می آزمائیم.



تصویر ۲-۶: تاثیر اندازه بسته بر فریم انتقال

کارایی^۱:

یک مقایسه ساده از سوئیچ مداری و ۲ طرح سوئیچ بسته ای در تصویر ۳-۶ آمده است. تصویر، انتقال پیام در بین ۴ گره را در بردارد؛ یک منبع در گره یک و یک مقصد در گره ۴ واقع است. در این تصویر ما با سه نوع تاخیر مواجه هستیم:

- **تاخیر انتشار:** فاصله زمانیکه یک سیگنال از یک گره به گره دیگری منتشر می شود را گویند. این زمان، بطور کلی ناچیز می باشد. برای مثال، سرعت سیگنال الکترومغناطیسی در یک محیط سیمی $2 \times 10^8 \text{ m/s}$ می باشد.
- **زمان انتقال:** فاصله زمانیکه یک انتقال دهنده، جهت انتقال یک بلاک داده صرف می کند. برای مثال جهت انتقال بلاک ۱۰,۰۰۰ بیتی داده با یک خط ۱۰ kbps، این زمان یک ثانیه می باشد.
- **تاخیر گره:** فاصله زمانیکه یک گره جهت انجام پردازش لازم، جهت سوئیچ داده لازم دارد.

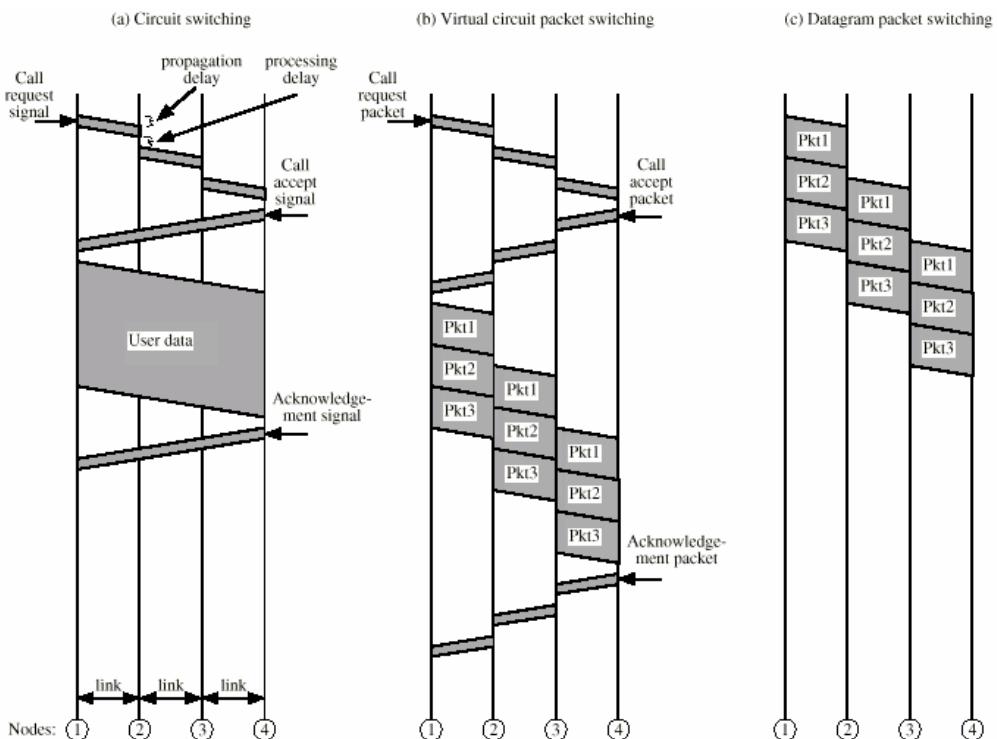
برای سوئیچ مداری، حجم تاخیر مشخصی قبل از ارسال پیام وجود دارد. ابتدا یک سیگنال درخواست تماس از طریق شبکه ارسال می گردد تا اتصال تا مقصد بربا گردد. اگر ایستگاه مقصد شلوغ نباشد، یک سیگنال پذیرش تماس، باز می گرداند. توجه کنید که یک تاخیر پردازش در هر گره، در طی درخواست تماس، تحمیل می گردد که این زمان در هر گره صرف برپا سازی اتصال می شود. در بازگشت این پردازش دیگر مورد نیاز نیست، زیرا دیگر

¹ Performance-

اتصال برپا شده است. پس از برپاسازی اتصال، پیام بصورت یک بلاک واحد و بدون تاخیر قابل توجه در سوئیچ کردن گره ها، ارسال می گردد.

سوئیچ بسته مدار مجازی، بسیار شبیه به سوئیچ مداری است. یک مدار مجازی بوسیله یک بسته درخواست تماس، درخواست می گردد که در هر گره تاخیری را متحمل می شود. مدار مجازی با یک بسته قبول تماس ، مورد پذیرش واقع می شود. در مقایسه با حالت سوئیچ مداری، تماس هنوز هم تاخیر گره ها را متحمل می شود؛ حتی در مسیرهای مجازی که اکنون برپا شده اند. دلیل این آنست که بسته در هرگره در صف قرار گرفته و باید زمانی را برای انتقال، صرف کند. زمانیکه مدار مجازی برپا گردید، پیام بصورت بسته هایی ارسال می گردد. باید دقت شود که این فاز نمی تواند سریعتر از سوئیچ مداری در شبکه های مشابه و قابل مقایسه، باشد. دلیل این امر آنست که سوئیچ مداری یک پردازش ذاتاً شفاف است و یک نرخ داده ثابت را در امتداد شبکه ایجاد می نماید. سوئیچ بسته ای شامل برخی تاخیرها در هر گره از مسیر می شود. بدتر آنکه این تاخیر متغیر است و با افزایش بارگذاری شبکه، افزایش می یابد.

سوئیچ بسته ای داده گرام نیازمند برپاسازی یک تماس نمی باشد. بنابراین برای پیامهای کوتاه می تواند از سوئیچ بسته ای مدار مجازی و حتی سوئیچ مداری ، سریعتر باشد. با این وجود، بدليل مسیردهی جداگانه هر داده گرام، پردازش هر داده گرا م در هر گره ممکن است طولانی تر از بسته های مدار مجازی باشد. بنابراین برای پیامهای طولانی، روش مدار مجازی بهتر خواهد بود. تصویر زیر تنها به منظور ارائه یک طرح از کارایی نسبی هر روش ، ارائه شده است و کارایی واقعی به ضرایبی از میزان همانند اندازه شبکه، ساختار شبکه، الگوی بارگذاری و خصوصیات تبادلات خاص آن، بستگی دارد.



تصویر ۶-۳: زمان رویدادها برای سوئیچ مداری و سوئیچ بسته ای

سایر خواص:

در کنار کارایی، تعداد کمی از خواص دیگر نیز می باشند که ممکن است جهت مقایسه روشها مورد بحث قرار بگیرند. جدول زیر مهمترین آنها را بطور خلاصه نشان می دهد. اغلب این خصوصیات توضیح داده شده اند و توضیحات مختصری نیز در ادامه آمده است.

همانطور که ذکر شد سوئیچ مداری بطور ذاتی یک سرویس شفاف است. یک بار که یک اتصال برقرار شد، یک نرخ داده ثابت برای ایستگاه ها فراهم می گردد. این حالت در سوئیچهای بسته ای وجود ندارد که در آنها تأخیر متغیر تعریف شده تا داده ها بصورت متغیر دریافت گرددن. بعلاوه در سوئیچ بسته ای داده گرام، داده ها با ترتیبی متفاوت از ترتیب انتقال آنها ممکن است دریافت گرددن.

علاوه بر شفافیت، هیچ سرباری برای تطبیق سوئیچ مداری، وجود ندارد. یک بار که یک اتصال برقرار شد، داده های آنالوگ یا دیجیتال از طریق آن از مبدأ به مقصد منتقل می شوند. برای سوئیچ بسته ای، داده آنالوگ باید قبل از انتقال به دیجیتال تبدیل گردد و بعلاوه هر بسته نیازمند بیتها سربار همانند آدرس مقصد نیز می باشد.

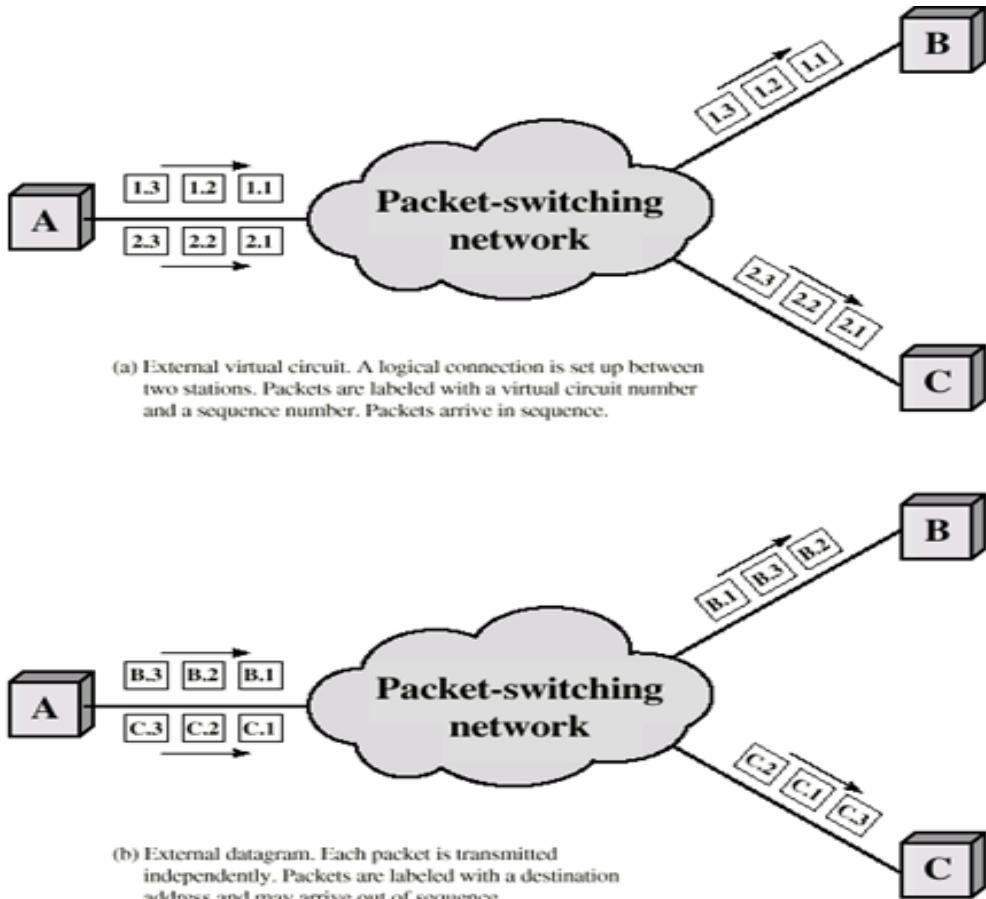
سوئیچ بسته مدار مجازی	سوئیچ بسته ای داده گرام	سوئیچ مداری
عدم اختصاص مسیر انتقال	عدم اختصاص مسیر انتقال	اختصاص مسیر انتقال
انتقال بسته ها	انتقال بسته ها	انتقال پیوسته داده
سرعت کافی جهت تعامل	سرعت کافی جهت تعامل	سرعت کافی جهت تعامل
بسته ها ممکن است تا زمان تحويل ذخیره می شوند	بسته ها ممکن است تا زمان تحويل ذخیره می شوند	پیامها ذخیره نمی شوند
مسیر برای تمام گفتگو برپا می شود	مسیر برای هر بسته برپا می شود	مسیر برای تمام گفتگو برپا می شود
تاخیر برپاسازی تماس، تاخیر انتقال بسته	تاخیر انتقال بسته	تاخیر انتقال تماس، تاخیر انتقال ناچیز
فرستنده ممکن است از عدم تحويل بسته است	فرستنده ممکن است از عدم تحويل بسته آگاه شود	در صورت مشغول بودن تماس گرفته شده سیگنال اشغال
بارگذاری اضافه ممکن است برپاسازی را مسدود کند، تاخیری برای تماسهای برپاسازی وجود ندارد	بارگذاری اضافی تاخیر تحويل بسته را افزایش می دهد	بارگذاری اضافه ممکن است برپاسازی را مسدود کند، تاخیری برای تماسهای برپاسازی وجود ندارد
گره های سوئیچ کوچک	گره های سوئیچ کوچک	سوئیچ الکترومکانیکی یا کامپیوتري
شبکه ممکن است مسئول بسته های متواالی باشد	شبکه ممکن است مسئول بسته های جداگانه باشد	کاربر مسئول حفظ در برابر فقدان بسته است
تبدیل سرعت و کد	تبدیل سرعت و کد	معمولًا تبدیل سرعت یا کد ندارد
استفاده پویا از پهنای باند	استفاده پویا از پهنای باند	پهنای باند ثابت
بیتها سربار در هر بسته	بیتها سربار در هر بسته	بیتها سربار پس از برپاسازی تماس وجود ندارد

جدول ۱-۶: مقایسه روشهای ارتباط سوئیچی

اعمال داخلی و خارجی:

یکی از مهمترین خصوصیت یک شبکه سوئیچ بسته ای آنست که از داده گرام و یا مدارات مجازی استفاده می کند. در واقع دو بعد از این خصوصیات وجود دارد که در تصاویر ۴-۵ و ۵-۶ تشریح شده اند. در رابط بین یک ایستگاه و یک گره شبکه، یک شبکه ممکن است هم سرویس اتصال گرا و هم بدون اتصال را فرهم آورد. با یک سرویس اتصال گرا، یک ایستگاه یک درخواست تماس را برای ایجاد یک اتصال منطقی با ایستگاه دیگر، ارائه می دهد. همه بسته های ارائه شده به شبکه مشخص شده هستند که عضو یک اتصال منطقی مشخص می باشند و بصورت پیاپی شماره گذاری شده اند. شبکه بسته ها را بصورت پیاپی تحويل می گیرد. اتصال منطقی اغلب با عنوان "مدار مجازی" مورد ارجاع قرار می گیرد و سرویس اتصال گرا به عنوان سرویس مدار مجازی خارجی، مورد ارجاع

قرار می‌گیرد. این سرویس خارجی با مفهوم عملکرد مدار مجازی داخلی متفاوت است. یک نمونه مهم از سرویس مجازی خارجی، X.25 می‌باشد که در ادامه مورد بررسی قرار می‌گیرد.

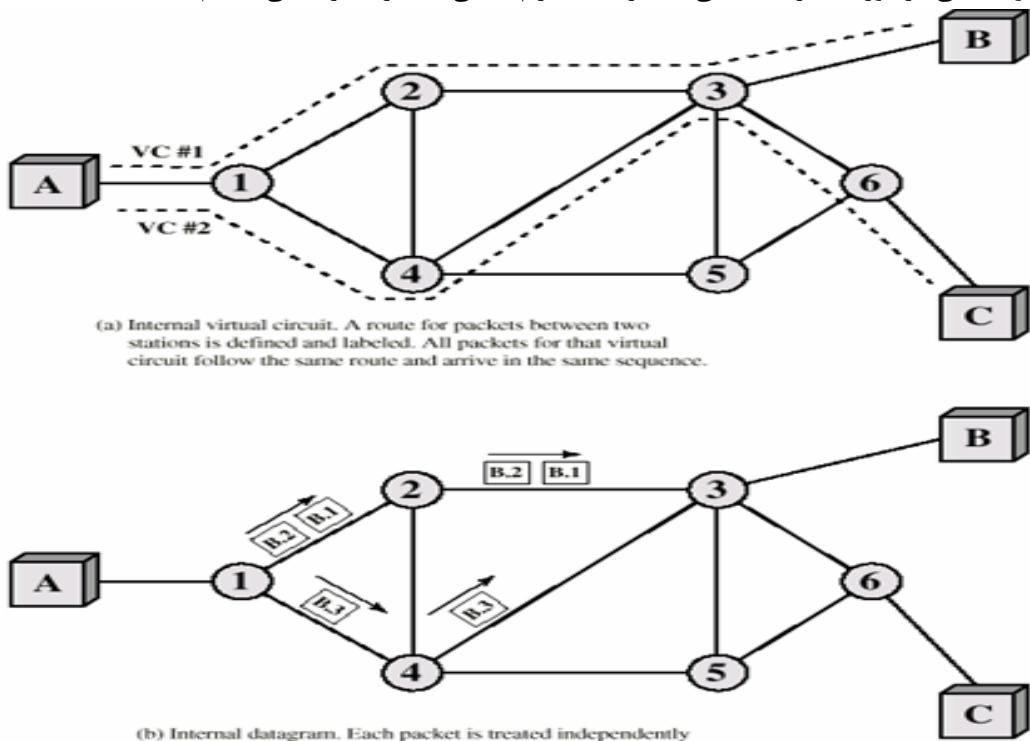


تصویر ۴-۶: عملیات مدار مجازی و داده گرام خارجی

با سرویس بدون اتصال، شبکه بسته‌ها را جداگانه مدیریت می‌کند و ممکن است آنها را به ترتیب یا مطمئن تحویل نگیرد. این نوع سرویس، گاهی اوقات بنام سرویس داده گرام خارجی شناخته می‌شود و این نیز با مفهوم عملکرد داده گرام داخلی متفاوت است. در داخل، هر شبکه ممکن است یک مسیر ثابت بین نقاط انتهایی ایجاد کند (مداری مجازی) و یا نکند (داده گرام). لازم نیست تا این نیاز طراحی داخلی و خارجی همزمان و منطبق باشد.

- مدار مجازی خارجی، داده گرام داخلی: شبکه هر بسته را جداگانه مدیریت می‌کند. بنابراین بسته‌های متفاوت برای مدار مجازی خارجی یکسان، ممکن است مسیرهای متفاوتی داشته باشند. اگرچه، در صورت نیاز، شبکه داده‌ها را در مقصد بافر می‌کند تا آنها با ترتیب اولیه در حین ایجاد شدن به ایستگاه مقصد تحویل داده شوند.
- داده گرام خارجی، داده گرام داخلی: هر بسته از نقطه نظر کاربر و شبکه، بصورت جداگانه رفتار می‌کند.
- داده گرام خارجی، مدار مجازی داخلی: هرچند شبکه یک اتصال منطقی را بین ایستگاه‌ها برای تحویل بسته برپا می‌کند، کاربر خارجی هیچ اتصالی را نمی‌بیند و بسادگی، بسته‌ها را یکی یکی دریافت می‌نماید. شبکه ممکن است اینچنان اتصالاتی را برای دوره‌های زمانی گسترده، برای ارضاء نیازهای آتی مورد انتظار، بصورت برپا شده رها کند.

سئوالی که مطرح می شود این است که انتخاب مدارات مجازی و یا داده گرام هردو داخلی و یا خارجی، چگونه است. این موضوع به اهداف خاص طراحی برای تماسهای شبکه و ضرایب هزینه بستگی دارد. در ادامه، اقدام به ارائه توضیحاتی در مورد معیارهای نسبی عملکرد داده گرام داخلی با مدار مجازی، می نمائیم.



تصویر ۶-۵: عملیات درونی مدار مجازی و داده گرام

با توجه به سرویسهای خارجی، می توانیم مشاهدات زیر را داشته باشیم. سرویس داده گرام زوج شده پوسیله داده گرام داخلی، اجازه استفاده کارا از شبکه را می دهد. این روش نیازمند برقراری تماس و نگه داری بسته ها جهت ارسال مجدد آنها در زمان خطای نمی باشد. ویژگی آخر، در برخی از کاربردهای زمان واقعی مطرح می گردد. سرویس مدار مجازی می تواند توالی انتها به انتهای و کنترل خطای را فراهم آورد. این سرویس جهت پشتیبانی از کاربردهای اتصال گرا همانند انتقال فایل و دسترسی از راه دور به پایانه، جذاب می باشد. در عمل، سرویس مدار مجازی متداولتر از سرویس داده گرام می باشد. اطمینان و سهولت یک سرویس اتصال گرا، جذابتر از مزایای داده گرام می باشد.

مسیر یابی:

یکی از پیچیده ترین و حیاتی ترین جنبه های طراحی شبکه های سوئیچ بسته ای، مسیر یابی می باشد. این بخش خواص کلیدی مورد استفاده در استراتژیهای مسیر یابی می باشد. مسیر یابی از استراتژیهای مسیر یابی خاص را مورد بررسی قرار می دهد. مفاهیم توضیحی در این بخش، در مسیر یابی بین شبکه ای نیز کاربرد دارد.

خصوصیات:

وظیفه مندی اولیه یک شبکه سوئیچ بسته ای، پذیرش بسته از ایستگاه مبدأ و تحويل آن به یک ایستگاه مقصد می باشد. برای انجام این کار، یک مسیر در طول شبکه باید مشخص باشد. در حالت کلی، ممکن است بیش از یک مسیر وجود داشته باشد. بنابراین یک تابع مسیر یابی باید اجرا شود. نیازمندیهای اولیه این تابع عبارتند از:

صحیح بودن	•
садگی	•
قوی بودن	•
پایداری	•
انصاف	•
بهینه بودن	•
موثر بودن	•

دو گزینه اول، خودشان خود توصیف هستند. قوی بودن به معنی آنست که شبکه توانایی تحويل بسته ها را با وجود خرابیها و سربارهای محلی، داشته باشد. بصورت ایده آل، شبکه می تواند با چنین تغییراتی با دور ریختن بسته ها و یا شکستن مدارات مجازی، برخورد کنند. طراحانی که بدبانی قوی بودن هستند، باید از عهده نیازمندیهای پایداری نیز برآیند. شیوه های تغییر شرایط، یک تاثیر نامطلوب، چه به جهت تلاشهای آهسته مجدد رویدادها و چه به جهت تجربه نوسان ناپایدار یک نقطه دور دست به نقطه دیگر را دارد.

برای مثال، یک شبکه ممکن است بدليل ترافیک در یک ناحیه، اقدام به شیفت قسمت بزرگی از بار به ناحیه دوم، بکند. اکنون ناحیه دوم دارای بارگذاری بیش از اندازه شده و اولی زیر حد بهره وری قرار گرفته است، که خود باعث شیفت دوم می گردد. در طی این شیفتها، بسته ها ممکن است در شبکه، در داخل یک حلقه، گرفتار شوند. همچنین یک تعامل نیز بین انصاف و بهینه بودن، وجود دارد. برخی کارایی ها ممکن است به تبادل بسته ها بین ایستگاه های نزدیک، نسبت به تبادل بسته بین ایستگاه های دور از هم، اولویت بالاتری بدتهند. این سیاست ممکن است میانگین بازدهی بالایی داشته باشد؛ اما در مورد ایستگاه های نیازمند به تبادل اطلاعات با ایستگاه های دور، منصفانه نخواهد بود.

سرانجام، هر روش مسیردهی شامل یکسری سربار در گره می باشد و گاهی سربار انتقال نیز دارد. هر دوی اینها تاثیر منفی بر کارایی شبکه دارند. جریمه چنین سربارهایی کاهش مزایای حاصل از سایر معیارهای معقول همانند افزایش قوی بودن و یا انصاف، می باشد.

مبنی اطلاعات شبکه	معیارهای کارایی
هیچ	تعداد پرس
محلي	هزینه
گره همسایه	تأخیر
گره های موجود در طول مسیر	بازد
همه گره ها	

زمان تصمیم گیری
بسته(داده گرام)
نشست(مدار مجازی)

محل تصمیم
در هر گره(توزیع شده)
گره مرکزی(متبرکز)
گره آغاز کننده(منبع)

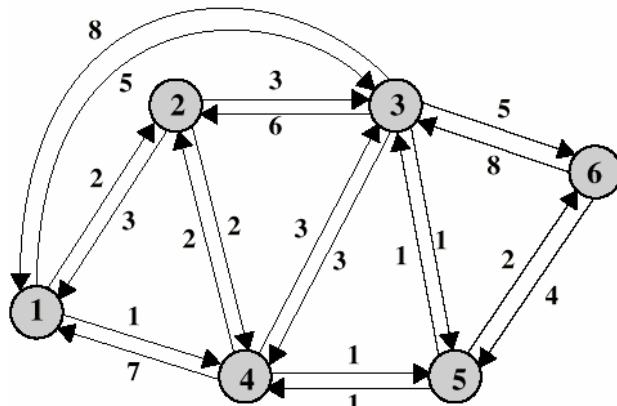
جدول ۲-۶: عناصر روش‌های مسیردهی برای شبکه های سوئیچ بسته ای

با نیازمندیهای ذکر شده، ما در موقعیتی هستیم که عناصر مختلف طراحی را که در یک استراتژی مسیردهی، سهم دارند را تشخیص دهیم. جدول بالا این عناصر را لیست کرده است. برخی از این طبقات همپوشانی داشته و یا به سایرین وابسته هستند. با وجود بررسی این لیست باعث توضیح و دسته بندی مفاهیم مسیریابی می‌گردد.

معیارهای کارایی:

بطور کلی انتخاب یک مسیر برپایه برخی جنبه‌های معیارهای کارایی می‌باشد. یکی از ساده‌ترین ملاک‌ها، انتخاب مسیر با کمترین پرش (پرش از روی کمترین تعداد گره) در طول شبکه، می‌باشد. این یک معیار ساده است و در آن باید مصرف منابع شبکه به حداقل برسد. هدف کلی ملاک کمترین تعداد پرش، کمترین هزینه مسیریابی می‌باشد. در این حالت، به هر پیوند یک هزینه تخصیص داده می‌شود و از این طریق برای هر زوج از ایستگاه‌های متصل، مسیر دورن شبکه با کمترین هزینه، براحتی محاسبه می‌گردد. برای مثال تصویر زیر یک شبکه را با دو خط ارتباطی بین گره‌های شبکه به معنی اتصال آنها و مقادیر متناسب که هزینه پیوند جاری را نشان می‌دهد، را توصیف می‌کند.

کوتاهترین مسیر از گره ۱ به ۶، ۶-۳-۶ با هزینه $1+5=6$ می‌باشد؛ اما مسیر با حداقل هزینه ۱-۴-۵-۶ با هزینه $1+2=4$ می‌باشد. هزینه تخصیصی به هر پیوند جهت پشتیبانی یک یا چند هدف، طراحی می‌باشد. برای مثال، هزینه می‌تواند بصورت عکس نرخ انتقال داده باشد (نرخ داده بالاتر در یک پیوند = هزینه تخصیص پایینتر در پیوند) و یا نمایانگر تاخیر صفحه‌گذاری جاری در پیوند باشد. در حالت اول، مسیر با حداقل هزینه باید بالاترین بازده را داشته باشد. حالت دوم، مسیر با حداقل هزینه باید تاخیر را حداقل کند.



تصویر ۶-۶: مثالی از شبکه سوئیچ بسته ای

در حداقل پرش و یا حداقل هزینه، الگوریتم تشخیص مسیر بهینه برای هر زوج از ایستگاه‌ها، نسبتاً سر راست بوده و زمان پردازش باید در حد محاسبات باشد. بدلیل انعطاف پذیری بیشتر معیار حداقل هزینه، این روش متدائلتر از ملاک حداقل پرش می‌باشد. در حال حاضر، الگوریتمهای مسیریابی کمترین هزینه متفاوتی، استفاده می‌شوند.

زمان و مکان تصمیم گیری:

دو ملاک مهم دیگر از معیارهای کارایی، زمان و مکان تصمیم گیری است. زمان تصمیم گیری بوسیله اینکه آیا تصمیم مسیریابی برروی یک بسته و یا مدار مجازی، گرفته شود، مشخص می‌گردد. زمانیکه عملکرد داخلی یک شبکه داده گرام است، تصمیم مسیریابی جداگانه برای هر بسته اتخاذ می‌شود. در ساده‌ترین حالت، همه بسته‌های

آتی از مدار مجازی با مسیر یکسان، استفاده می کنند. در طراحی شبکه های پیچیده تر، شبکه ممکن است مسیر تخصیص یافته به یک مدار مجازی را بحسب تغییر شرایط (همانند سرریز ترافیک و یا نقص در بخشی از شبکه) تغییر دهد.

عبارت " محل تصمیم گیری" مبین آنست که کدام گره و یا گره های شبکه، مسئول اتخاذ تصمیم مسیریابی هستند. عده ترین حالت، مسیریابی توزیع شده است که در آن هر گره مسئول انتخاب یک اتصال خروجی برای مسیریابی بسته های ورودی می باشد. برای مسیریابی مرکز، تصمیم بوسیله برخی گره های طراحی شده همانند یک مرکز کنترل شبکه، اخذ می گردد. خطر روش آخر در آنست که فقدان مرکز کنترل شبکه ممکن است باعث مسدود شدن عملکرد شبکه گردد. روش توزیع شده، شاید پیچیده تر باشد، اما قویتر است. روش سوم که در برخی از شبکه ها مورد استفاده قرار می گیرد، استفاده از مسیریابی مبداء می باشد. در این حالت تصمیم مسیریابی بوسیله مبداء و نه یک گره شبکه، اخذ می شود و سپس اتصال با شبکه برقرار می گردد. این روش به کاربر امکان می دهد تا با تعیین مسیر در شبکه ها، به ملاکهای محلی آن دستیابی بیابد.

زمان و مکان تصمیم، متغیرهای طراحی مستقل هستند. برای مثال در شکل ۶-۶ فرض کنید محل تصمیم گیری، هر گره است و هزینه های داده شده، زمان هستند. هزینه ممکن است تغییریابند. اگر بسته ای از گره ۱ به گره ۶، تحويل داده شود، ممکن است از مسیر ۱-۴-۵-۶ حرکت نماید. مقادیر هر مسیر بوسیله گره ارسال کننده بصورت محلی، مشخص می شوند. اکنون فرض کنید که مقادیر تغییر یافته اند، بگونه ایکه دیگر ۱-۴-۶، مسیر بهینه نیست. در یک شبکه داده گرام، بسته بعدی ممکن است مسیر متفاوتی را دنبال کند که در هر گره مسیر مشخص می شود. یک شبکه مداری مجازی، هر گونه تصمیم مسیریابی که در طول برپاسازی مدار مجازی، شکل گرفته است را بخاطر خواهد داشت و بسادگی و بدون ایجاد تصمیم جدید، بسته ها را عبور می دهد.

منبع و زمان بروزرسانی اطلاعات شبکه:

اکثر استراتژیهای مسیریابی نیازمند آنند که برپایه دانش ساختار شبکه، بارگذاری ترافیک و هزینه اتصال، تصمیم گیری نمایند. با کمال تعجب شاهد آنیم که برخی از استراتژیها، از این اطلاعات استفاده نکرده و هنوز بسته ها را از طریق استراتژیهای سیل آسا^۱ و یا اتفاقی، مدیریت می کنند.

با مسیریابی توزیع شده که در آن تصمیم مسیریابی بوسیله هر گره اتخاذ می شود، گره های مجزا ممکن است تنها برای اطلاعات محلی مورد استفاده قرار بگیرند (همانند هزینه اتصال خروجی). هر گره همچنین ممکن است اطلاعاتی همانند حجم تراکم تجربه شده در هر گره را از گره های مجاور خود تهیه کند (گره های با اتصال مستقیم)، سرانجام ، الگوریتمهایی وجود دارند که اجازه می دهند تا گره، اطلاعات را از همه گره ها در هر مسیر بالقوه دلخواه، بدست آورد. در حالت مسیریابی مرکزی، گره مرکزی، اطلاعات تمام گره ها را جمع آوری می کند.

یک مفهوم مرتبط، زمان بروزرسانی می باشد که تابعیست از اطلاعات منبع و استراتژیهای مسیریابی.

مشخصاً، اگر اطلاعاتی مورد استفاده قرار نگیرد (همانند روش سیل آسا)، اطلاعاتی نیز برای بروزرسانی وجود ندارد. اگر تنها اطلاعات محلی مورد استفاده قرار بگیرد، بروزرسانی پیوسته خواهد بود، زیرا هر گره همیشه از وضعیت محلی خود مطلع است. برای سایر روشهای منبع اطلاعات (گره های همسایه، همه گره ها)، زمان بروزرسانی به استراتژی مسیریابی وابسته است. با یک استراتژی ثابت، اطلاعات هرگز بروز نمی شوند. برای یک استراتژی وفقی^۲، جهت وفق تصمیم مسیریابی با شرایط تغییر یافته، اطلاعات بصورت لحظه به لحظه، بروز می شوند.

¹ Flooding

² Adaptive

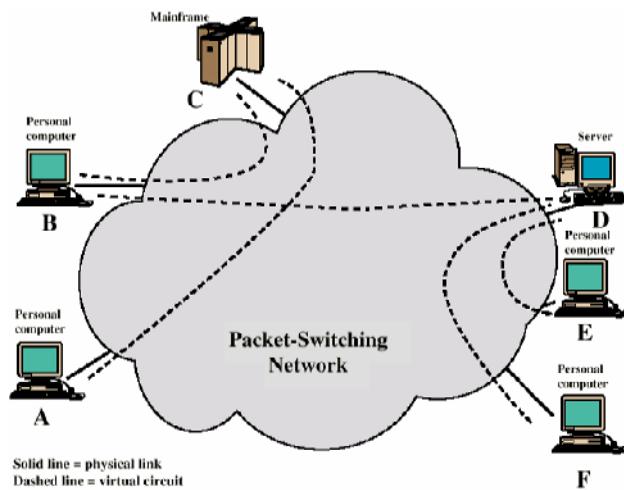
همانطور که ممکن است انتظار داشته باشید، زمانیکه اطلاعات زیادی وجود دارند و فرکانس‌های بروزرسانی نیز بالا می باشد، شبکه می تواند تصمیمات مسیریابی خوبی بگیرد. از سوی دیگر، انتقال اطلاعات، منابع شبکه را مصرف می کنند.

تعداد زیادی از استراتژیهای مسیریابی وجود دارند که بر روی نیازمندیهای مسیریابی شبکه های سوئیچ بسته ای، بحث می کنند. بسیاری از این استراتژی ها بر روی مسیریابی های بین شبکه ای نیز اعمال شده اند.^۴ استراتژی کلیدی مطرح در این شبکه ها عبارتند از: ثابت، سیل آسا، اتفاقی و تطبیقی. این استراتژیها قبلاً در فصل ۴ مورد بررسی قرار گرفته اند.

X.25

یکی از پروتکلهای پر استفاده X.25 می باشد که در سال ۱۹۷۶، ارائه شده است و از آن زمان تا کنون تغییرات زیادی یافته است. این استاندارد یک رابط را بین یک سیستم میزبان و یک شبکه سوئیچ بسته ای، مشخص می نماید. این استاندارد همچنین بصورت جهانی جهت رابط شبکه های سوئیچ بسته ای بکار رفته و در سوئیچ بسته ای ISDN نیز پیاده شده است. این استاندارد سه سطح پروتکل را دارا می باشد:

- سطح فیزیکی
- سطح پیوند
- سطح بسته



تصویر ۶-۷: استفاده از مدارات مجازی

این سه سطح بر سه لایه پایین مدل OSI، منطبق می باشند. سطح فیزیکی، یک رابط فیزیکی بین یک ایستگاه الحاقی (کامپیوتر، پایانه) و یک اتصال که ایستگاه را به گره سوئیچ بسته ای، متصل می سازد، را معرفی می نماید. در این استاندارد به ماشین های کاربران به عنوان ابزار پایانه^۱ (DTE) و به گره های سوئیچ بسته ای که DTE به آنها متصل است را ابزار مدار پایان دار داده^۲ (DCE) می گویند. X.25 از لایه فیزیکی با استاندارد X.21 استفاده می نماید، اما استانداردهای دیگری همانند EIA-232 به عنوان جانشین نیز وجود دارند. سطح پیوند، جهت انتقال مطمئن داده در طول اتصال فیزیکی، بوسیله ارسال داده بصورت یک توالی از فریمهای، ایجاد شده است.

¹ Data Terminal Equipment -

² Data Circuit-terminating Equipment -

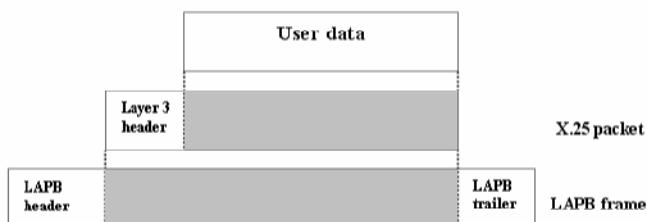
استاندارد سطح پیوند با عنوان LAPB^۱(پروتکل دسترسی به پیوند متوازن)، شناخته می شود. LAPB زیر مجموعه ای از HDLC^۲ می باشد.

سطح بسته یک سرویس مدار مجازی خارجی را فراهم می آورد. این سرویس هر مشترکی را در شبکه، برای برپاسازی اتصالات منطقی بنام **مدارات مجازی**، به سایر مشترکین، توانا می سازد. یک مثال در تصویر ۷-۶ ارائه شده است. در این مثال، ایستگاه A یک اتصال مدار مجازی به C، دارد. ایستگاه B دو مدار مجازی برقرار نموده است؛ یکی به C و دیگری به D، و E و F نیز هر کدام یک اتصال مدار مجازی به D، دارند.

تصویر ۷-۶، رابطه بین سطوح X.25 را نشان می دهد. داده های کاربر به سمت پایین و سطح ۳ X.25 عبور داده می شوند، که در این مسیر به آنها اطلاعات کنترلی بنام سرآیند، افزوده می شود و یک بسته ایجاد می گردد. در حالت دیگر، داده کاربر ممکن است به چند بسته تقسیم گردد. اطلاعات کنترلی بسته، اهداف مختلفی را سرویس می دهد که عبارتند از:

- مشخص کردن شماره یک مدار مجازی مشخص ، که داده ها با آن در ارتباط هستند.
- ایجاد شماره توالي^۳ که می تواند جهت کنترل جریان^۴ و خطای پایه مدار مجازی، بکار می رود.

سپس کل بسته X.25 به موجودیت LAPB در پایین تحويل می گردد که در آنجا اطلاعات کنترلی به ابتداء و انتهای بسته افزوده شده و یک فریم LAPB را تشکیل می دهد. اطلاعات کنترلی برای اعمال پروتکل LAPB، مورد نیاز می باشد.



تصویر ۷-۶: داده های کاربر و اطلاعات کنترلی پروتکل X.25

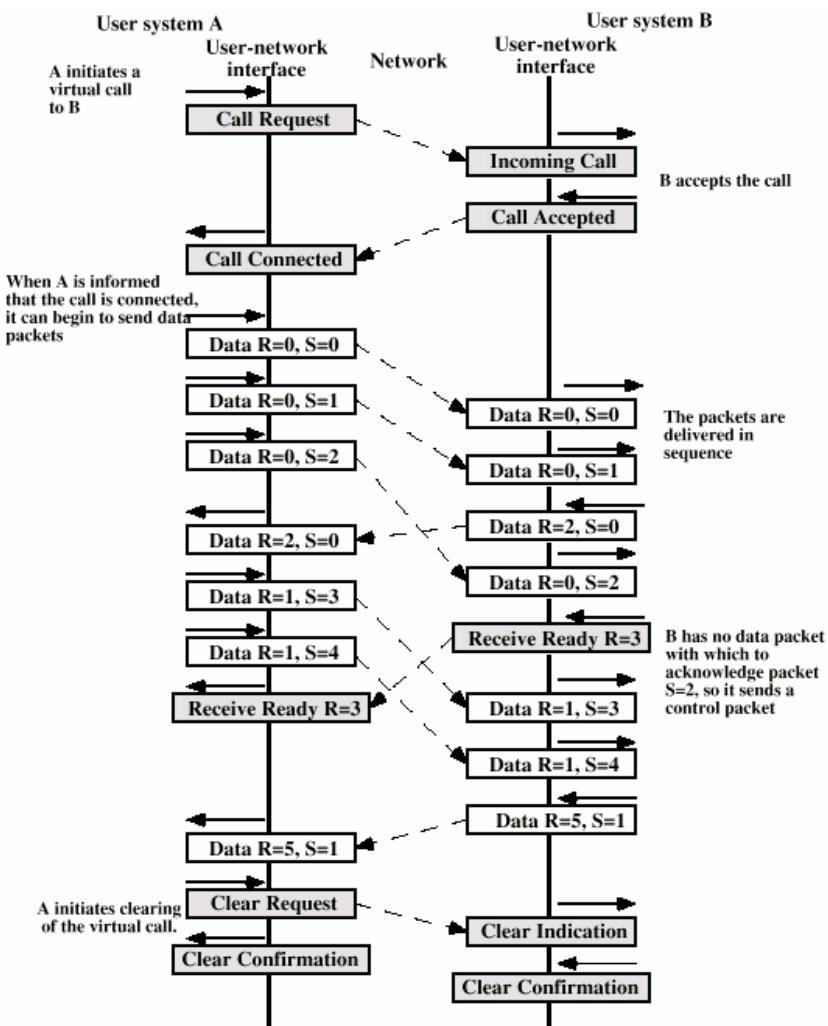
سرویس مدار مجازی:

سرویس مدار مجازی X.25 برای دو نوع مدار مجازی، تهیه شده است. تماس مجازی^۵ و مدار مجازی ثابت^۶. یک تماس مجازی، یک مدار مجازی برپا شده با استفاده از یک برپاسازی تماس و روای تماس خاتمه^۷، می باشد. یک مدار مجازی ثابت، یک مدار مجازی ثابت و تخصیص یافته توسط شبکه، می باشد. انتقال داده ها با تماسهای مجازی می باشد، اما نیازی به تماس برپاسازی و تماس خاتمه، وجود ندارد.

تصویر ۹-۶، یک توالی رویداد خاص در یک تماس مجازی را نمایش می دهد. بخش سمت چپ تصویر، مبادله بسته ها بین ماشین کاربر A و گره سوئیچ بسته ای که به آن متصل شده است، را نشان می دهد. بخش سمت راست، مبادله بسته بین ماشین کاربر B و گره اش را نشان می دهد. مسیردهی بسته در داخل شبکه برای کاربر، آشکار نیست.

توالی رویدادها بصورت زیر می باشد:

Link Access Protocol Balanced -	^۱
High Level Data Link Control -	^۲
Sequence Number -	^۳
Flow -	^۴
Virtual Call -	^۵
Permanent Virtual Circuit -	^۶
Call Clearing Procedure -	^۷



تصویر ۶-۹: توالی رویدادها: پروتکل X.25

- ۱ درخواست یک مدار مجازی را از B، با ارسال یک بسته درخواست تماس به DCE، اعلام می نماید. بسته شامل آدرس‌های مبدأ و مقصد، همچنین شماره مدار مجازی مورد استفاده برای این مدار مجازی جدید، می باشد. انتقالهای به داخل و بیرون بعدی، بوسیله شماره مدار مجازی مشخص می گردد.
- ۲ شبکه این درخواست تماس را به DCE، هدایت می کند.
- ۳ DCE، درخواست تماس را دریافت نموده و یک بسته تماس ورودی به B. می فرستد. این بسته فرمتی همانند بسته درخواستهای تماس را دارد، اما شماره مدار مجازی متفاوتی دارد که بوسیله B، از میان شماره های تخصیص نیافته محلی، انتخاب می گردد.
- ۴ B پذیرش برای تماس را با ارسال یک بسته پذیرش تماس به A، که همان شماره مدار مجازی بسته تماس ورودی را دارد؛ نشان می دهد.
- ۵ DCE، یک پذیرش تماس را دریافت نموده و یک بسته تماس برقرار شده به A می فرستد. این بسته فرمتی همانند بسته پذیرش تماس، فقط با این تفاوت که شماره مدار مجازی همانند بسته درخواست تماس اصلی دارد، را دارا می باشد.
- ۶ A و B داده و بسته های کنترل را به یکدیگر، با استفاده از شماره مدارات مجازی به ترتیب مخصوص خود، ارسال می کنند.

-۷ A (یا B)، یک بسته درخواست خاتمه را برای خاتمه مدار مجازی، ارسال می کند و یک

بسته تایید خاتمه را دریافت می نماید.

-۸ B (یا A)، یک بسته شاخص خاتمه را دریافت نموده و یک بسته تایید خاتمه را ارسال

می نماید.

فرمت بسته:

تصویر ۶-۱۰، فرمت بسته پایه مورد استفاده در X.25 را نشان می دهد. برای داده های کاربر، داده ها به بلاکهایی با اندازه طول حداقل، تقسیم شده و یک سرآیند ۳۲، ۲۴ و یا ۵۶ بیتی به هر بلاک داده از یک بسته داده افزوده می شود. برای مدارات مجازی، که از شماره توالی ۱۵ بیتی استفاده می کنند، سرآیند با یک شناسه پروتکل با مقدار ۰۰۱۱۰۰۰. آغاز می شود. سرآیند شامل یک شماره مدار مجازی ۱۲ بیتی (شامل ۴ بیت شماره گره و ۸ بیت شماره کانال)، می باشد. فیلدهای P(S) و P(R)، توابع کنترل جریان و خط را در پایه های مدار مجازی، پشتیبانی می کنند. بیت Q، در استاندارد تعريف نشده است، اما به کاربر توانایی تشخیص دو نوع داده را می دهد. بعلاوه جهت انتقال داده کاربر، ۲۵ X. باید اطلاعات کنترل مرتبط با برپاسازی، نگهداری و خاتمه مدارات مجازی را نیز منتقل نماید. اطلاعات کنترلی در یک بسته کنترل منتقل می شوند. هر بسته کنترل شامل شماره مدار مجازی، نوع بسته که تابع کنترل خاصی را مشخص می نماید و اطلاعات کنترلی اضافه مرتبط با تابع، می باشد. برای مثال، یک بسته درخواست تماس شامل فیلدهای زیر می باشد:

Q	D	0	1	Group Number
Channel Number				
P(R)	M	P(S)	0	
User Data				

(a) Data packet with 3-bit sequence numbers

X	0	0	1	Group Number			
Channel Number							
Packet Type	1						
Additional Information							

(b) Control packet for virtual calls with 3-bit sequence numbers

0	0	0	1	Group Number			
Channel Number							
P(R)	Packet Type			1			
Additional Information							

(c) RR, RNR, and REJ packets with 3-bit sequence numbers

Q	D	1	0	Group Number			
Channel Number							
P(S)	0						
P(R)	M						
User Data							

(d) Data packet with 7-bit sequence numbers

X	0	1	0	Group Number			
Channel Number							
Packet Type	1						
Additional Information							

(e) Control packet for virtual calls with 7-bit sequence numbers

0	0	1	0	Group Number			
Channel Number							
P(R)	1						
Additional Information							

(f) RR, RNR, and REJ packets with 7-bit sequence numbers

0	0	1	1	0	0	0	0			
Group Number										
Channel Number										
P(S) - low order	0									
P(S) - high order										
P(R) - low order	M									
P(R) - high order										
User Data										

(g) Data packet with 15-bit sequence numbers

0	0	1	1	0	0	0	0			
Group Number										
Channel Number										
Packet Type	1									
Additional Information										

(h) Control packet for virtual calls with 15-bit sequence numbers

0	0	1	1	0	0	0	0
Group Number							
Channel Number							
Packet Type	1						
P(R) - low order	0						
P(R) - high order							

(i) RR, RNR, and REJ packets with 15-bit sequence numbers

تصویر ۶-۱۰: فرمت بسته های X.25

- طول آدرس DTE تماس گیرنده(۴ بایت): طول فیلد آدرس متناظر در واحدهای ۴ بیتی.
- طول آدرس DTE تماس گرفته شده(۴ بایت): طول فیلد آدرس متناظر در واحدهای ۴ بیتی.
- آدرس DTE(متغیر): آدرس گیرنده و تماس گرفته شده.

- امکانات: یک توالی از مشخصات امکانات. هر مشخصه یک از یک کد امکانات ۸ بیتی و یا بیشتر و صفر یا بیشتر کدهای پارمتر، تشکیل شده است. یک مثال از امکانات، مطالبه هزینه معکوس^۱ می باشد.

جدول ۳-۶ بسته های ۲۵.X را لیست نموده است. اکثر آنها تا کنون مورد بررسی قرار گرفته اند و توضیحات مختصری از موارد باقیمانده، در ادامه آمده است:

یک DTE ممکن است یک بسته وقفه را ارسال نماید تا یک روال کنترل جریان برای بسته های داده را از مسیر فرعی عبور دهد. بسته وقفه، بوسیله شبکه، با اولویت بالاتر نسبت به بسته های داده، به DTE مقصد تحويل داده می شود. یک مثال از این توانایی، انتقال کرکترهای شکست یک پایانه می باشد.

بسته خطایاب، به عنوان ابزاری جهت اعلام شرایط خطای مشخص که مقداردهی اولیه را تضمین نمی کند، بکار می رود. بسته های ثبت برای درخواست و تایید امکانات ۲۵.X، بکار می روند.

پارامترها	سروریس		نوع بسته	
	PVC	VC	از DCE به DTE	از DTE به DCE
برپاسازی تماس و خاتمه آن				
آدرس DTE تماس گیرنده، آدرس DTE تماس گرفته شده، امکانات، داده کاربر تماس		X	دریافت تماس	درخواست تماس
آدرس DTE تماس گیرنده، آدرس DTE تماس گرفته شده، امکانات، داده کاربر تماس		X	تماس برقرارشده	تماس پذیرفته شده
دلیل خاتمه، کد خطأ، آدرس DTE تماس گیرنده، آدرس DTE تماس گرفته شده،		X	اعلام خاتمه	درخواست خاتمه
آدرس DTE تماس گیرنده، آدرس DTE تماس گرفته شده، امکانات		X	پذیرش خاتمه	پذیرش خاتمه
داده و وقفه				
-	X	X	داده	داده
وقفه داده کاربر	X	X	وقفه	وقفه
-	X	X	تایید وقفه	تایید وقفه
کنترل جریان و بازنشانی				
P(R)	X	X	RR	RR
P(R)	X	X	RNR	RNR
P(R)	X	X		REJ
دلیل بازنشانی، کد خطأ	X	X	اعلام بازنشانی	درخواست بازنشانی
-	X	X	تایید بازنشانی	تایید بازنشانی
آغاز دوباره				
دلیل آغاز مجدد، کد خطأ	X	X	اعلام شروع مجدد	درخواست شروع مجدد
-	X	X	تایید شروع مجدد	تایید شروع مجدد
خطایاب				
کد خطأ، توصیف خطأ	X	X	خطایاب	

جدول ۳-۶: انواع بسته ها و پارامترهای آنها

مالتی پلکس کردن^۲:

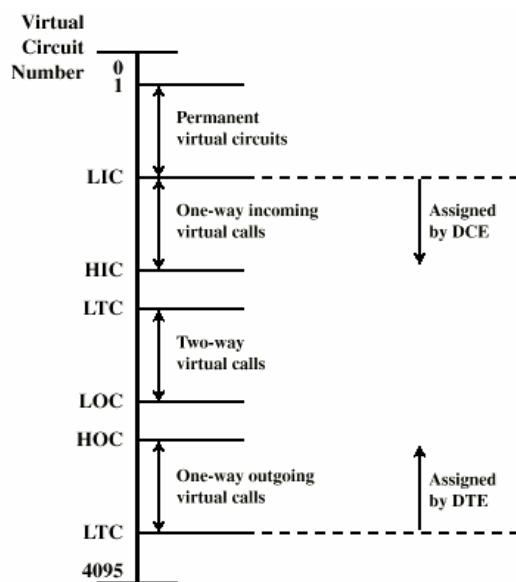
¹ Reverse Charging -

² Multiplexing -

شاید مهمترین سرویس ارائه شده در X.25 مالتی پلکس باشد. A DTE، اجازه برپاسازی ۴۰۹۶ مدار مجازی همانند با سایر DTE ها ببروی یک اتصال DTE-DCE فیزیکی، ممکن ساخته است. DTE می تواند بصورت دورنی این مدارات را به هر صورتیکه بخواهد، تخصیص دهد. مدارات مجازی مجزا، می توانند برای نمونه با کاربردها، پردازشها و یا پایانه ها، در تماس باشند. اتصال DTE-DCE، یک تقسیم و ارسال کاملاً دو رشته ای^۱ فراهم می آورند که در آن در هر زمان، در یک مدار مجازی، یک بسته می تواند در هر جهتی منتقل شود.

برای مرتب سازی و اینکه کدام بسته به کدام مدار مجازی متعلق است، هر بسته یک شماره مدار مجازی ۱۲ بیتی دارد. تخصیص شماره مدارات مجازی از طرح تصویر ۱۱-۶ تبعیت می کند. شماره صفر اغلب رزرو شده و جهت تشخیص بسته های عمومی برای همه مدارات مجازی، بکار می رود. شماره دامنه های متواالی به چهار گروه از مدارات مجازی، تخصیص یافته اند. مدارات مجازی ثابت با شماره هایی که با یک شروع می شوند، شماره گذاری شده اند. طبقه بعدی تماسهای مجازی ورودی یک طرفه می باشد. این به این معنی است که تنها تماسهای ورودی از شبکه می توانند این شماره را بخود تخصیص دهند. اگرچه مدارات مجازی دوطرفه هستند، زمانیکه یک درخواست تماس رسید، DCE یک شماره تخصیص نیافته از این گروه را انتخاب می نماید.

تماسهای خروجی یک جهته، آنهایی هستند که بوسیله DTE، مقداردهی می گردند. در این حالت شماره استفاده نشده از بین آنهاییکه به تماسها تخصیص یافته اند را انتخاب می نماید. این تفکیک گروه، جهت جلوگیری از انتخاب اعداد مشابه برای ۲ مدار مجازی مختلف بوسیله DCE و DTE می باشد. گروه تماس مجازی ۲ طرفه، یک سرریز را برای تخصیص مشترک بوسیله DTE و DCE، فراهم می آورند. این امر، تفاوت ضعیف در جریان ترافیک را مجاز می شمارد.



LIC = Lowest incoming channel HIC = Highest incoming channel Virtual circuit number = logical group number and logical channel number
 HOC = Highest outgoing channel LOC = Lowest outgoing channel
 LTC = Lowest two-way channel LTC = Highest two-way channel

تصویر ۱۱-۶: تخصیص شماره مدار مجازی

کنترل جریان و خطای:

کنترل جریان و خطای در سطح بسته X.25، به صورت مجازی با فرمت و رویه یکسان مورد استفاده برای HDLC، ارائه می شود و از یک پنجره لغزان، استفاده می شود. هر بسته داده، یک شماره توالی ارسال (P(S)) و یک

¹ Full Duplex -

شماره توالی دریافت($P(R)$) را دربردارد. به صورت پیش فرض، شماره توالی سه بیتی مورد استفاده قرار می گیرد. یک DTE می تواند بطور دلخواهانه، از طریق مکانیزم امکانات کاربر، درخواست شماره توالی ۷ یا ۱۵ بیتی را بنماید. DTE بوسیله $P(S)$ به بسته های خروجی در یک مدار مجازی پایه، تخصیص داده می شود. این کار به این صورت است که $P(S)$ ، هر بسته داده خروجی جدید بروی یک مدار مجازی، یکی بیشتر از مقدار بسته قبلی روی آن مدار می باشد(ماژول ۸، ۳۲۷۶۸ و یا ۱۲۸). $P(R)$ ، شامل شماره بسته بعدی است که از طرف دیگر یک مدار مجازی، انتظار دریافت آن وجود دارد. این روش جهت تایید سوار بر پشت^۱، بکار می رود. اگر یک سمت، داده ای جهت ارسال نداشته باشد، ممکن است ابتدا، بسته های ورودی را به شیوه HDLC، با بسته کنترلی آماده جهت دریافت(RR) و عدم آماده باش جهت دریافت(RNR) قبول نماید. اندازه پنجه پیش فرض ۲ است، اما با سه بیت شماره توالی آن ممکن است به رقم بالای ۷، تنظیم گردد(۱۲۷ برای ۷ بیت توالی و ۳۲۷۶۷ برای ۱۵ بیت توالی). قبول، به فرم فیلد (R) در بسته داده RR و یا RNR است و بنابراین کنترل جریان، ممکن است معنای محلی و یا انتهای بستهها برپایه تنظیمات بیت D ، را باشد. زمانیکه $D=0$ (حالت عمدی)، تایید بین DTE و شبکه، بکار می رود. وقتی $D=1$ است، تایید از DTE راه دور می رسد.

طرح کنترل خطاب برگشت ARQ می باشد. تایید منفی به معنی یک ردکردن^۲(REJ)، می باشد. اگر یک گره، یک تایید منفی دریافت نماید، باید آن بسته خاص و تمام بسته های ارسالی پس از آن را دوباره ارسال نماید.

توالی بسته ها:

X.25 توانایی تشخیص یک توالی پیاپی بسته های داده را فراهم می آورد که به آن **توالی بسته کامل^۳** می گویند. این خصیصه، چندین کاربرد دارد. یکی از مهمترین آنها بوسیله پروتکلهای بین شبکه ای مورد استفاده قرار می گیرد که در آن بسته های طولانی داده در امتداد شبکه با محدودیت اندازه بسته کوچکتر، بدون از دست دادن جامعیت بلاک، انتقال می یابند.

نمونه توالی های بسته						نمونه توالی بسته با تایید E-E میانی								
توالی اصلی			توالی ترکیبی											
نوع بسته	M	D	نوع بسته	M	D	نوع بسته	M	D						
A	1	0	A	1	0	A	1	0			*			
A	1	0				A	1	0						
A	1	0		1	0	A	1	0						
A	1	0				B	0	1						
A	1	0	B	0	1	A	1	0			*			
B	0	1				A	1	0						
توالی قطعات						B	0	1						
*: گروهی از قطعات که می تواند ترکیب گردد.						A	1	0			*			
						A	1	0						
						B	0	1						
پایان توالی														

جدول ۶-۴: توالی بسته X.25

Piggyback Acknowledgment - ^۱

Reject - ^۲

Complete Packet Sequence - ^۳

برای مشخص کردن این مکانیزم، ۲۵.X دو نوع بسته را معرفی می کند: بسته های A و بسته های B. یک بسته A، آنیست که بیت M آن، یک شده است، بیت D آن، صفر است و بسته طول کامل(برابر با حداکثر طول مجاز بسته) را دارد. یک بسته B، بسته ایست که از نوع A نباشد. یک توالی بسته کامل شامل صفر یا بیشتر بسته A است که بوسیله یک بسته B، دنبال می گردد. شبکه از ترکیب این توالی ممکن است یک بسته طولانی تر را ایجاد نماید. همچنین، شبکه ممکن است یک بسته B را به بسته های کوچکتر، تقسیم نماید تا یک توالی بسته کامل را ایجاد نماید.

شیوه مدیریت بسته B، به تنظیمات بیتها M و D، بستگی دارد. اگر $D=1$ ، یک تایید انتها به انتهای بوسیله DTE دریافت کننده به ارسال کننده، ارسال می شود. اگر $M=1$ ، توالی های بسته کامل اضافی، در ادامه وجود دارد. این ساختار، بسته های بعدی را به عنوان یک توالی بزرگتر، قرار می دهد که می تواند از تایید انتها به انتهای قبل از خاتمه توالی بزرگتر، استفاده نماید.

جدول ۴-۶، نمونه ای از این مفاهیم را نمایش می دهد. این وظیفه DCE هاست تا تغییرات شماره توالی، بوجود آمده در اثر تقسیم کردن و بازسازی، را تطبیق دهند.

بازنشاندن^۱ و آغاز دوباره^۲:

X.25، دو امکان را جهت بازیابی از خطأ، فراهم می کند. امکان بازنشاندن، جهت مقداردهی اولیه مجدد یک مدار مجازی بکار می رود. این به این معنی است که، شماره های توالی در هر دو انتها به صفر تنظیم می گردند. هر بسته داده یا وقفه در حالت انتقال، از دست می رود و این وظیفه یک پروتکل لایه بالاتر است تا بسته های مفقود شده را بازیابی نماید. یک بازنشاندن می تواند بوسیله تعدادی از شرایط خطأ شامل فقدان یک بسته، شماره توالی اشتباه، تراکم و یا فقدان مدار مجازی درونی شبکه، رخ دهد. در حالت آخر، هر دو DCE، باید مدار مجازی درونی را دوباره بسازند تا از مدار خارجی کماکان موجود DCE-DTE پشتیبانی نماید. DTE و یا می توانند یک بازنشانی را با یک شاخص درخواست یا بازنشانی، مقداردهی اولیه نمایند. گیرنده با یک تایید بازنشانی، پاسخ می دهد. صرفه نظر از چگونگی مقداردهی اولیه بازنشانی، DCE درگیر، مسئول اطلاع دهی به طرف مقابله باشد.

یکسری شرایط خطای جدی، درخواست یک آغاز مجدد را می کنند. انتشار یک بسته درخواست آغاز مجدد، معادل ارسال یک درخواست خاتمه در همه تماسهای مجازی و درخواست بازنشانی برروی همه مدارات مجازی ثابت می باشد. در اینجا نیز یک DCE و یا DTE ممکن است این حالت را بوجود آورد. یک نمونه از این شرایط هشدار آغاز مجدد، فقدان دسترسی موقت به شبکه، می باشد.

خلاصه فصل:

سوئیچ بسته ای جهت ایجاد سهولت و کارایی بیشتر نسبت به ترافیکهای انفجاری داده ، طراحی شده است. در سوئیچ بسته ای، یک ایستگاه داده را بصورت بلاکهایی کوچک بنام بسته ارسال می کند. هر بسته شامل بخشی از داده کاربر، بعلاوه اطلاعات کنترلی مورد نیاز جهت هدایت بسته در شبکه می باشد. یک عنصر اساسی مشخص در شبکه های سوئیچ بسته ای اینست که آیا عمل داخلی داده گرام است یا کanal مجازی. با کانالهای مجازی داخلی، یک مسیر بین دو نقطه انتهایی تشکیل می گردد و همه بسته ها برای آن کانال

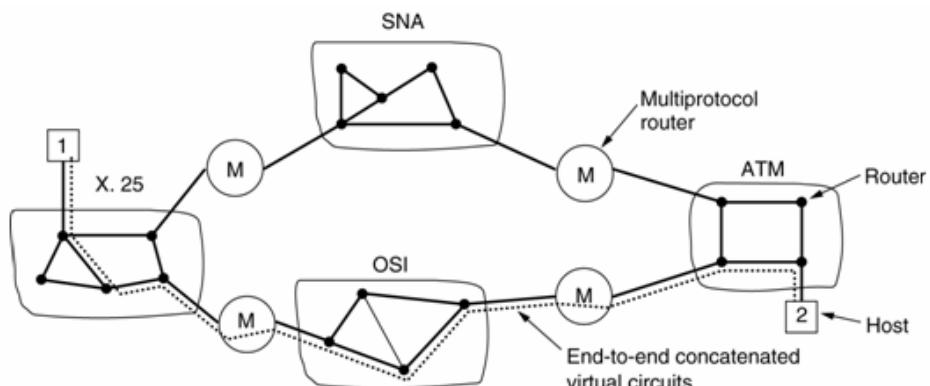
¹ Reset-
² Restart –

مجازی، از مسیر یکتایی عبور می نمایند. در داده گرام داخلی، هر بسته بصورت جداگانه عمل کرده و بسته های یک مقصد ممکن است از مسیرهای متفاوت عبور نمایند.

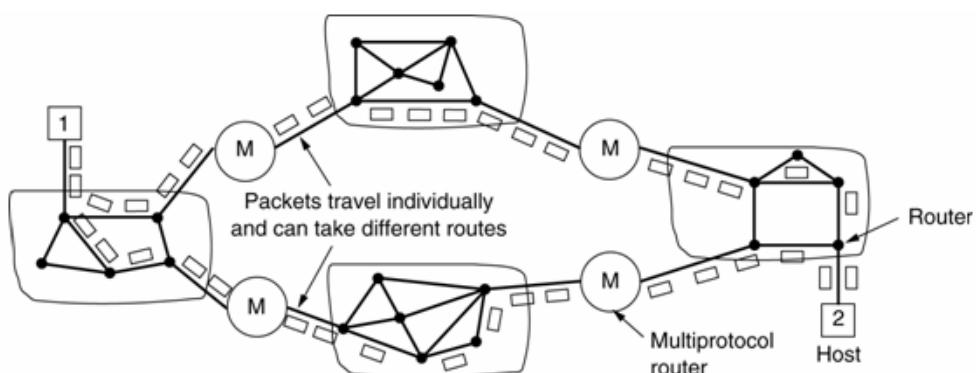
یک تابع مسیریابی در یک شبکه سوئیچ بسته ای، سعی در یافتن کم هزینه ترین مسیر در شبکه می کند که هزینه های آن شامل تعداد پرش، تاخیر مورد انتظار و سایر پارامترها می باشد. الگوریتمهای مسیریابی قابل تطبیق، براساس تبادل اطلاعات شرایط ترافیکی بین گره های شبکه عمل می کنند.

X.25 یک پروتکل استاندارد برای ارتباط یک سیستم نهایی و یک شبکه سوئیچ بسته ای، می باشد.

تصاویر زیر به درک بهتر تفاوت سوئیچ بسته ای مدار گرام کمک می کند. در تصویر ۱۲-۶ انتقال داده ها بین دو میزبان ۱ و ۲ از طریق شبکه های سوئیچ بسته ای مدار مجازی انجام شده است. مشاهده می شود که تمام داده ها از مسیر یکسانی عبور می کنند. در تصویر ۱۳-۶، انتقال داده ها بین میزبانهای ۱ و ۲، این بار با استفاده از شبکه های سوئیچ بسته ای داده گرام، انجام می گیرد. در این حالت بدليل مجزا بودن عملکرد بسته ها از یکدیگر، هر بسته می تواند مسیر متفاوتی از دیگران را جهت رسیدن به مقصد انتخاب و طی کند.



تصویر ۱۲-۶: انتقال داده ها با روش سوئیچ داده مدار مجازی



تصویر ۱۳-۶: انتقال داده ها با روش سوئیچ داده گرام

فصل ل:

شبکه های فریم FrameRelay

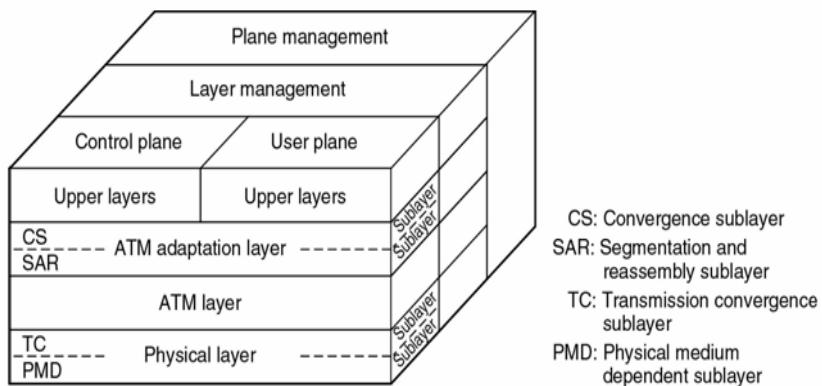
که با نام بازپخش سلول^۲ نیز شناخته می‌شود، از مزایای قابلیت اعتماد و وفاداری امکانات دیجیتال مدرن برای تهیه سوئیچ بسته ای سریعتر از ۰.۲۵X، استفاده نموده است. ATM در ابتدا به عنوان بخشی از کاربروی شبکه‌های باند گسترده ISDN، توسعه داده شد؛ اما پس از آن کاربردهایی را در محیط‌های غیر ISDN که نیازمند ارسال داده با نرخ بسیار بالا بودند، یافت.

ما با بحث در مورد جزئیات طرح ATM شروع کرده و سپس مفاهیم مهم لایه‌های تطبیق ATM^۳) را بررسی کرده و سرانجام مروری داریم بر یک طرح قدیمی‌تر، اما هنوز بر استفاده بنام FR، داریم.

۷-۱: معماری پروتکل:

ATM به شیوه ای مشابه با سوئیچ بسته ای ۰.۲۵X و FR، عمل می‌کند. همانند سوئیچ بسته ای و ATM داده‌ها را با قطعات بزرگ مجزا، منتقل می‌نماید. همچنین همانند سوئیچ بسته ای و ATM نیز اجازه ایجاد چندین اتصال منطقی را جهت مالتی پلکس داده‌ها برروی یک واسطه فیزیکی را مجاز می‌شمارد. در ATM جریان اطلاعات در هر اتصال منطقی در بسته‌های با طول ثابت بنام سلول، سازماندهی می‌گردد.

یک پروتکل ساده و موثر با حداقل قابلیتهای کنترل خط‌آ و جریان، می‌باشد. این امر باعث کاهش سربار پردازش سلولهای ATM شده و سربار تعداد بیتها مورد نیاز در هر سلول را نیز کاهش می‌دهد و بنابراین ATM با نرخهای داده بالا عمل می‌نماید. بعلاوه استفاده از سلول‌های با طول ثابت، پردازش مورد نیاز در هر گره ATM را ساده‌تر نموده است، که این خود جهت پشتیبانی از نرخ داده بالا در ATM بکار می‌رود.



تصویر ۱-۷: معماری پروتکل ATM

استاندارد ATM که بوسیله ITU-T ارائه شده است، برپایه ساختار معماري نشان داده شده در تصویر ۱-۷، می‌باشد که یک معماري پایه را برای یک رابط بین کاربر و شبکه تشریح می‌نماید. لایه فیزیکی شامل مشخصاتی از یک محیط انتقال و یک طرح رمزنگاری سیگنال، می‌باشد. دامنه نرخ داده در لایه فیزیکی بین ۲۵.۶ Mbps تا ۶۲۲.۰۸ Mbps می‌باشد. نرخ‌های داده دیگر، بالاتر یا پایین‌تر، نیز ممکن می‌باشند.

دو لایه از معماري پروتکل، به توابع ATM مربوط می‌گردند. یک لایه عمومي ATM جهت تمام سرويسها وجود دارد که تواناييهای انتقال بسته را فراهم می‌آورد و یک لایه تطبیق ATM که وابسته به سرويس می‌باشد. لایه ATM، انتقال داده در سلولهای با طول ثابت و استفاده از اتصالات منطقی را توصیف می‌نماید. استفاده از ATM، نیاز به یک لایه تطبیق برای پشتیبانی از پروتکلهای انتقال داده ای که برپایه ATM نیستند را بوجود می‌آورد. AAL

^۱ Asynchronous Transfer Mode -

^۲ Cell Relay -

^۳ ATM Adaption Layer -

اطلاعات لایه های بالاتر را جهت انتقال بر روی یک شبکه ATM را به سلولهای ATM نگاشت می کند و در پایان نیز اطلاعات سلولهای ATM را برای تحویل به لایه بالاتر، جمع آوری می نماید.

مدل مرجع پروتکل، شامل سه طرح متفاوت می باشد:

- طرح کاربر: زمینه انتقال اطلاعات کاربر را با کنترلهای مرتبط همانند کنترل خط و جریان، فراهم می آورد.
- طرح کنترل: کنترل تماس و سایر توابع کنترل اتصال را اعمال می نماید.
- طرح مدیریت: شامل مدیریت طرح، که توابع مدیریتی مرتبط را به یک سیستم بطور کامل اعمال می کند و هماهنگی را بین همه طرح ها و مدیریت لایه ایجاد می نماید، شامل توابع مدیریتی مرتبط با منابع و پارامترهای مقیم در موجودیتهای پروتکلهاش می شود.

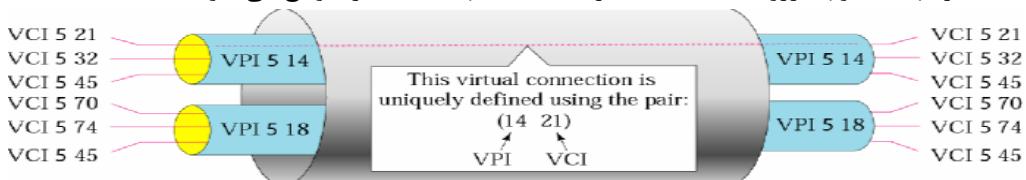
OSI layer	ATM layer	ATM sublayer	Functionality
3/4	AAL	CS	Providing the standard interface (convergence)
		SAR	Segmentation and reassembly
2/3	ATM		Flow control Cell header generation/extraction Virtual circuit/path management Cell multiplexing/demultiplexing
2	Physical	TC	Cell rate decoupling Header checksum generation and verification Cell generation Packing/unpacking cells from the enclosing envelope Frame generation
1		PMD	Bit timing Physical network access

جدول ۷-۱: تطبیق لایه های ATM مدل هفت لایه OSI

۲-۷: اتصالات منطقی ATM

اتصالات منطقی ATM به عنوان اتصالات کanal مجازی (VCC)^۱ نیز شناخته می شود. یک VCC، یک طرح قابل مقایسه با مدار مجازی در X.25 می باشد و واحد پایه سوئیچ در یک شبکه ATM می باشد. یک VCC، بین دو کاربر نهایی از طریق شبکه و یک نرخ متغیر جریان دو طرفه از سلولهای با طول ثابت که در طول شبکه مبادله می شوند، برپا می شود. VCC همچنین برای تبادلات کاربر-شبکه (سیگنالهای کنترلی) و تبادلات شبکه-شبکه (مدیریت و مسیردهی شبکه) نیز بکار می رود.

برای ATM، یک زیر لایه دوم پردازشی نیز تعریف شده است که مفاهیم مسیر مجازی را مطرح می نماید (تصویر ۷-۲). یک اتصال مسیر مجازی (VPC)^۲، یک مجموعه از VCC ها می باشد که نقاط انتهایی مشابه دارند. بنابراین همه جریانهای سلولها بر روی همه VCC ها در یک VPC تنها، با یکدیگر سوئیچ می شوند.



تصویر ۷-۲: روابط ATM

مفهوم مسیر مجازی جهت پاسخ به روند شبکه با سرعت بالا، توسعه داده شده که در آن، هزینه کنترل شبکه، رشد کمتری را در برابر رشد هزینه سراسری شبکه، فراهم می آورد. تکنیک مسیر مجازی با گره بندی اتصالات مشترک مسیر عمومی در شبکه، بصورت یک واحد یکه، به خودداری از هزینه کنترل کمک می کند. اعمال

¹ Virtual Channel Connection-
² Virtual Path Connection -

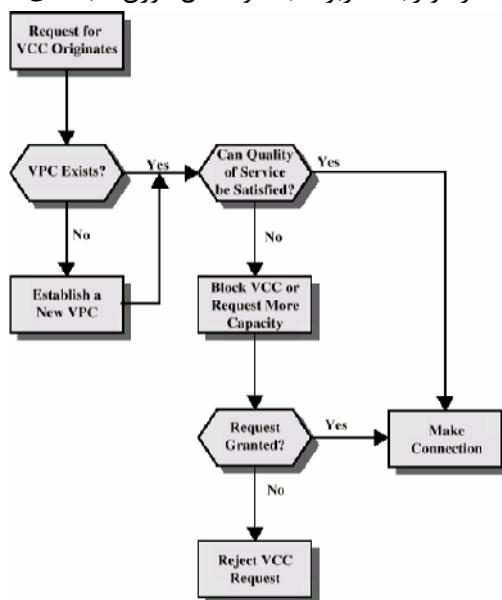
مدیریت شبکه می توانند تنها بروی تعداد کمی از گروه های اتصالات، بجای تعداد زیادی از اتصالات منفرد، اعمال شوند.

چند مزیت استفاده از مسیرهای مجازی در زیر لیست شده اند:

- توسعه کارابی و قابلیت اطمینان شبکه: شبکه با تعداد کمتری موجودیت سروکار دارد.
- کاهش پردازش و زمان برپاسازی اتصال کوتاه: بیشتر کار زمانی انجام می شود که مسیر مجازی برپا می گردد. با معکوس کردن ظرفیت یک اتصال مجازی در پیش بینی سایر تماسهای بعدی، اتصالات کanal مجازی جدید می توانند با اجرای توابع کنترلی ساده در نقاط انتهایی اتصال مسیر مجازی، برپا شوند و پردازش تماس در عبور از گره ها، مورد نیاز نیست. بنابراین افزودن کanalهای مجازی جدید شامل حداقل پردازش می گردد.
- توسعه سرویسهای شبکه: مسیر مجازی در درون شبکه بکار می رود، اما برای کاربر نهایی نیز قابل مشاهده است. بنابراین کاربر ممکن است گروه های کاربری بسته یا شبکه های بسته از مجموعه ای از کanalهای مجازی را تعریف نماید.

تصویر ۳-۷ یک مسیر کلی پردازش برپاسازی تماس، با استفاده از کanalها و مسیرهای مجازی را نشان می دهد. پردازش برپاسازی یک اتصال مسیر مجازی از طرف پردازش برپاسازی یک اتصال کanal مجازی منحصر بفرد ، مجزا شده است:

- مکانیزمهای کنترل مسیر مجازی شامل محاسبه مسیرها، تخصیص ظرفیت و ذخیره اطلاعات وضعیت اتصال می باشد.
- جهت برپاسازی یک کanal مجازی، ابتدا باید یک اتصال مسیر مجازی به گره مقصد مورد نظر با ظرفیت موجود به حد کافی، جهت پشتیبانی از کanal مجازی، با کیفیت سرویس مقتضی، وجود داشته باشد. یک کanal مجازی بوسیله ذخیره اطلاعات وضعیت مورد نیاز(نگاشت کanal مجازی/سرویس مجازی)، برپا می شود.
- واژه شناسی مسیر مجازی و کanalهای مجازی در جدول ۲-۷، بطور خلاصه آمده است. از آنجاییکه اکثر پروتکلهای لایه شبکه مورد بحث، تنها به رابط کاربر-شبکه مرتبط می باشد، مفاهیم مسیر مجازی و کanal مجازی معرفی شده در توصیه نامه ITU-T، به هر دو رابط کاربر-شبکه و اعمال دورن شبکه ای، اشاره دارد.



تصویر ۳-۷: برپاسازی تماس با استفاده مسیرهای مجازی

کاربرد اتصال کانال مجازی

- نقاط انتهایی یک VCC ممکن است کاربران نهایی، موجودیتهای شبکه و یا یک کاربر نهایی و یک موجودیت شبکه باشد. در همه موارد، جامعیت توالی سلول، در یک VCC، نگهداری می شود، که در آن، سلول‌ها با همان ترتیبی تحويل داده می شوند که ارسال شده اند. اجازه بدھید یک VCC را با مثال نشان دهیم:
- بین کاربران نهایی: می تواند جهت انتقال داده انتها به انتهای کاربران، بکار رود و همچنین می تواند جهت انتقال سیگنالهای کنترلی بین کاربران نهایی نیز بکار رود، که بعداً توضیح داده خواهد شد. یک VPC، بین کاربران نهایی فعال است و مجموعه ای از VCC‌ها را که از ظرفیت VPC تجاوز نمی کنند، را فراهم می کند.
 - بین یک کاربر نهایی و یک موجودیت شبکه: جهت سیگنالهای کنترلی کاربر به شبکه، بکار می رود. یک VPC کاربر به شبکه می تواند جهت تبادل توافق ترافیک از یک کاربر به یک شبکه یا سرور شبکه، مورد استفاده قرار بگیرد.
 - بین دو موجودیت شبکه: برای توابع مدیریت ترافیک شبکه و مسیردهی، بکار می رود. یک VPC شبکه به شبکه می تواند جهت تعریف یک مسیر عمومی برای تبادل اطلاعات مدیریت شبکه، بکار رود.

کانال مجازی (VC)	یک عبارت عام مورد استفاده جهت توصیف انتقال یک جهته سلول‌های ATM که با یک مقدار شناسه یکتا عمومی، پیوند خورده است.
اتصال کانال مجازی	یک ابزار جهت انتقال یک جهته سلولهای ATM بین یک نقطه که یک مقدار VCI به آن اختصاص یافته و نقطه ایکه مقدار به آن تفسیر یا ختم می گردد.
شناسه کانال مجازی (VCI)	یک برچسب عددی یکتا که یک اتصال VC مشخص برای یک VPC را مشخص می نماید.
اتصال کانال مجازی (VCC)	یک اتصال از پیوندهای VC که بین دو نقطه که کاربران سرویس ATM در آن به لایه ATM دسترسی دارند، گستردۀ شده است. VCC‌ها برای اهداف انتقال اطلاعات کاربر-کاربر، کاربر-شبکه و یا شبکه شبکه، فراهم می گردد. جامعیت توالی سلول برای سلولهای متعلق به VCC یکسان، پیش رزرو شده است.
مسیر مجازی	یک عبارت عام مورد استفاده جهت توصیف انتقال یک جهته سلولهای ATM متعلق به کانالهای مجازی که با یک مقدار شناسه یکتا عمومی، پیوند خورده است.
اتصال مسیر مجازی	یک گروه از پیوندهای VC، مشخص شده بوسیله یک مقدار عمومی VPI. بین یک نقطه که یک مقدار VCI به آن اختصاص یافته و نقطه ایکه مقدار به آن تفسیر یا ختم می گردد.
شناسه مسیر مجازی (VPI)	تعیین کننده یک پیوند VP منحصرفرد.
اتصال مسیر مجازی (VPC)	یک اتصال از پیوندهای VP گستردۀ شده بین دو نقطه که مقادیر VCI به آنها تخصیص یافته و نقطه ایکه مقدار به آن تفسیر یا ختم می گردد (همانند گسترش طول یک مرز پیوندهای VC که در یک VPI یکسان مشترک است). VPC‌ها برای اهداف انتقال اطلاعات کاربر-کاربر، کاربر-شبکه و یا شبکه شبکه، فراهم می گردد.

جدول ۷-۲: واژه شناسی کانال مجازی / مسیر مجازی

خواص مسیر مجازی / کانال مجازی:

- توصیه نامه I.150 ITU-T، خصوصیات زیر را برای اتصالات کانال مجازی ذکر می کند:
- کیفیت سرویس: یک کاربر یک VCC، بوسیله کیفیت سرویس تعیین شده بوسیله پارامترهایی همانند نرخ گم شدن سلول‌ها منتقل شده و بازه تغییرات تاخیر سلول، فراهم شده است.

• اتصالات کانال مجازی سوئیچ شده و دارای مدت محدود^۱: یک VCC سوئیچ شده، یک اتصال بدون تقاضا می باشد که نیازمند سیگنالهای کنترلی تماس برای برپاسازی و خاتمه دادن، می باشد. یک VCC دارای مدت محدود آنسیت که از دوره طولانی می باشد و بوسیله پیکربندی یا فعالیت مدیریت شبکه برپا می شود.

• جامعیت توالی سلول: توالی سلولهای ارسالی در یک VCC، نگه داشته می شود.
• محاوره پارامتر ترافیک و استفاده از نظارت^۲: پارامترهای ترافیکی می توانند بین یک کاربر و شبکه برای هر VCC، مورد بحث قرار گیرند. سلولهای ورودی به VCC بوسیله شبکه مورد نظر نظارت قرار می گیرند ، تا اطمینان حاصل شود که پارامترها نقض نشده باشند.

انواع پارامترهای ترافیکی که می توانند مورد بحث قرار گیرند شامل نرخ متوسط، نرخ حداکثر، انفجاری بودن و دوره اوج، می باشد. شبکه ممکن است به تعداد زیادی از استراتژیها جهت برخورد با تراکم و مدیریت VCC های موجود و درخواست شده، نیاز داشته باشد. در سطح بدترین حالت، شبکه ممکن است هر درخواست VCC جدید را جهت جلوگیری از تراکم، ندیده بگیرد. بعلاوه سلولها در صورت تخطی از پارامترهای مبادله شده و یا وقوع تراکم، ممکن است دور ریخته شوند.

I.150 خصوصیات VPC را نیز لیست نموده است. ^۴ خاصیت اولیه لیست شده، با موارد ذکر شده برای VCC ها، یکسان هستند کیفیت سرویس، VPC سوئیچ شده و دارای محدودیت زمانی، جامعیت توالی سلول و محاوره پارامترهای ترافیک و استفاده از نظارت، خصوصیاتی هستند که برای یک VPC نیز آمده اند. چند دلیل برای این تکرار وجود دارد: اول، ایجاد انعطاف پذیری در چگونگی اینکه سرویس شبکه اقدام به مدیریت درخواستهایی که بر پایه آن می باشد، می کند. دوم، شبکه باید با نیازمندیهای سراسری برای یک VPC مرتبط باشد و در یک VPC، ممکن است جهت برپاسازی کانالهای مجازی با خصوصیات داده شده، گفتگو کند. و مورد آخر آنکه، زمانیکه یک VPC برقرار شد، برای کاربران نهایی، این قابلیت وجود دارد که جهت ایجاد VCC های جدید، گفتگو کنند. خصوصیات VPC، یک سیاست برmbنای انتخابهای ممکن کاربران نهایی را تحمیل می نماید.

جدا از این موارد، خاصیت پنجمی نیز برای VPC، ذکر شده است:

• محدودیت شناسه کانال مجازی در یک VPC: یک یا چند شناسه کانال مجازی، ممکن است برای کاربر VPC، فراهم نباشد، اما ممکن است برای استفاده از شبکه رزرو شده باشد. نمونه ای از این حالت را می توان در نمونه ای از این حالت را می توان در VCC های مورد استفاده در مدیریت شبکه، مشاهده نمود.

سیگنال دهی کنترل^۳:

در ATM، مکانیزمی جهت برپاسازی و انتشار VPC ها و VCC ها مورد نیاز می باشد. تبادل اطلاعات در این پردازش با عنوان سیگنال دهی کنترل مطرح شده است و در اتصالاتی جدا از آنهاییکه مدیریت شده ند، رخ می دهد. برای VCC ها، I.150 روش برای ایجاد یک امکان برپاسازی انتشار، ارائه داده است. یک یا ترکیبی از این روشها می تواند در هر شبکه مشخص بکار رود:

۱ - VCC های دارای مدت محدود، ممکن است جهت تبادلات کاربر به کاربر، بکار رود. در این حالت به سیگنال دهی کنترلی، نیازی نمی باشد.

¹ Semipermanent -

² Monitoring -

³ Control Signaling -

- ۲ هیچ پیش برپاسازی کانال تماس سیگنال دهی کنترل، وجود ندارد و یکی باید ایجاد شود. برای این منظور یک تبادل سیگنال دهی کنترل باید بین کاربر و شبکه در برخی کانال‌ها، باید رخ دهد. بنابراین بدليل نیاز ما به یک کانال ثابت، شاید با نرخ پایین، می‌توان از آن جهت برپاسازی VCC‌های که می‌تواند جهت کنترل تماس بکار رود، استفاده کرد. چنین کانال‌هایی یک کانال Metasignaling نامیده می‌شود، که جهت برپاسازی کانال‌های سیگنال دهی مورد استفاده قرار می‌گیرد.
- ۳ کانال Metasignaling، می‌تواند جهت برپاسازی VCC‌ها بین کاربر و شبکه، برای سیگنال دهی کنترلی، بکار می‌رود. این کانال مجازی سیگنال دهی کاربر به شبکه، می‌تواند جهت برپاسازی VCC‌ها، جهت حمل داده‌های کاربر بکار رود.
- ۴ همچنین کانال Metasignaling، می‌تواند جهت برپاسازی کانال سیگنال دهی کاربر به کاربر نیز، بکار رود. اینچنین کانالی باید در یک VPC پیش برپاشده، برپا گردد. این موضوع می‌تواند جهت مجاز ساختن کاربران نهایی، بدون دخالت شبکه، جهت برپاسازی و انتشار VCC‌های کاربر به کاربر جهت حمل داده‌های کاربر، بکار رود.

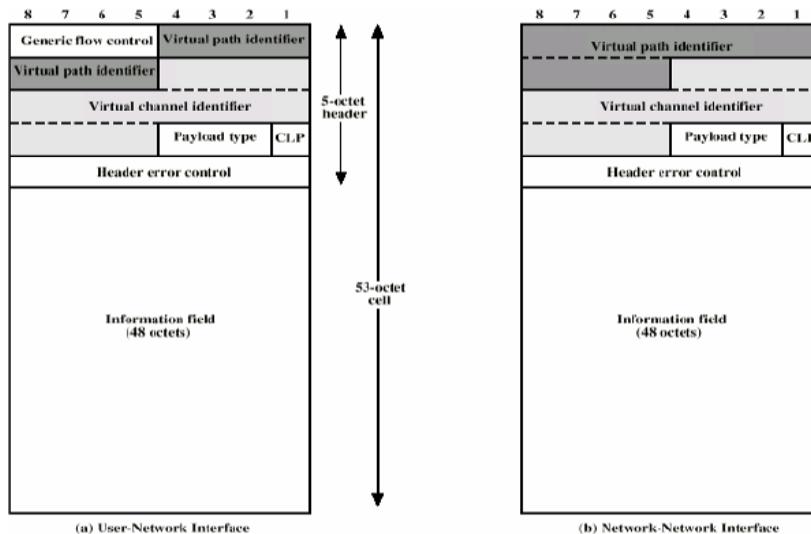
برای VPC‌ها، سه روش^۱ در I.150 تعریف شده است:

- ۱- یک VPC می‌تواند برمبنای یک مدت محدود، بوسیله توافق قبلی، برقرار گردد. در این حالت سیگنال دهی کنترلی وجود ندارد.
- ۲- برپاسازی/انتشار VPC، می‌تواند بصورت کنترل شده توسط مشتری باشد. در این حالت مشتری از یک سیگنال دهی VCC، برای درخواست VPC، استفاده می‌نماید.
- ۳- برپاسازی/انتشار VPC، ممکن است بصورت کنترل شده توسط شبکه باشد. در این حالت، یک VPC برای راحتی خودش برپا می‌کند. مسیر ممکن است شبکه به شبکه، کاربر به شبکه و یا کاربر به کاربر، باشد.

۳-۷ ATM سلولهای

ATM از سلولهایی با طول ثابت استفاده می‌کند که ۵ بایت آن سرآیند و ۴۸ بایت بخش داده آن می‌باشد. چندین مزیت در استفاده از سلولهای کوچک و با طول ثابت، وجود دارد. اول آنکه استفاده از سلوهای کوچک می‌تواند تاخیر صفت‌گذاری را برای سلوهای با اولویت بالا، کاهش دهد؛ زیرا چنین سلوی اگر با فاصله زمانی کوتاهی پس از یک سلول با اولویت پایین‌تر، از راه برشد، می‌تواند دستیابی به یک منبع، همانند انتقال دهنده را بدست آورد. دوم آنکه واضح است سلولهای با طول ثابت، با کارایی بالاتری می‌توانند سوئیچ شوند، که این برای نرخ داده بالای ATM، بسیار مهم است. با سلولهای با طول ثابت، پیاده سازی مکانیزم سوئیچ در سخت افزارها، ساده‌تر می‌گردد.

^۱ Method -



تصویر ۷-۴: فرمت سلول ATM

فرمت سرآیند:

تصویر ۷-۴، سمت چپ(a)، فرمت سرآیند سلول در یک رابط کاربر-شبکه را نشان می دهد. تصویر سمت راست (b) فرمت سرآیند سلول در یک رابط شبکه-شبکه را نشان می دهد.

فیلد کنترل جریان عمومی(GFC^۱)، در سرآیند سلول درون شبکه ای، دیده نمی شود و تنها در رابط کاربر-شبکه، وجود دارد. بنابراین، این فیلد تنها می تواند برای کنترل جریان ترافیک، برای کیفیت سرویس‌های متفاوت، بکار رود. در هر صورت، مکانیزم GFC برای کم کردن دوره های کوتاه بارگذاری اضافی در شبکه، مورد استفاده قرار می گیرد.

I.150، به عنوان یک نیاز مکانیزم GFC، عنوان می کند که همه پایانه ها باید قادر باشند تا به ظرفیتهای مطمئن خودشان، دسترسی داشته باشند. این شامل همه پایانه های نرخ بیتی ثابت(CBR^۲) و پایانه های نرخ بیتی متغیر(VBR^۳)، می گردد که یک عنصر ظرفیت تضمین شده، دارند CBR و VBR در بخش ۷-۵، توضیح داده شده اند. مکانیزم کنونی GFC در ادامه توضیح داده شده است.

کد PT	تفصیر
000	سلول داده کاربر بدون تراکم
001	سلول داده کاربر بدون تراکم
010	سلول داده کاربر با تراکم
011	سلول داده کاربر با تراکم
100	سلول OAM دار سگمنت
101	سلول OAM دار انتهای به انتهای
110	سلول مدیریت منابع
111	رزرو شده جهت توابعی آتی

OAM:Operation,Administration,Maintenance

SDU:Service Data Unit

جدول ۷-۳: تفسیر کدهای فیلد نوع Payload

Generic Flow Control - ^۱
Constant Bit Rate - ^۲
Variable Bit Rate - ^۳

شناسه مسیر مجازی(VPI)^۱، شامل یک فیلد مسیردهی برای شبکه می باشد. این فیلد در رابط کاربر-شبکه، ۸ بیتی و در رابط شبکه-شبکه، ۱۲ بیتی می باشد. حالت دوم اجازه پشتیبانی از شماره توسعه یافته VPC های درون شبکه ای، که جهت پشتیبانی از مشترکین و مدیریت شبکه مورد نیاز می باشد، را می دهد. شناسه کanal مجازی(VCI)^۲، برای مسیردهی از بجهه یک کاربر نهایی، مورد استفاده قرار می گیرد.

فیلد نوع Payload(PT)، نوع اطلاعات فیلد اطلاعات را مشخص می نماید. جدول ۷-۳، تفسیر بیتهای PT را نشان می دهد. مقدار صفر در اولین بیت، نشانگر اطلاعات کاربر می باشد(اطلاعات لایه بالایی بعدی). در این حالت بیتهای بعدی نشان دهنده وقوع تراکم می باشد و بیت سوم که بنام بیت نوع واحد داده سرویس(SDU)^۳، معروف است، یک فیلد تک بیتی است که می تواند جهت تشخیص دو نوع SDU در یک اتصال ATM، بکار رود. عبارت SDU، به Payload^۴ بایتی سلول اشاره دارد. یک مقدار یک در بیت اول فیلد Payload، نشان می دهد که این سلول حامل اطلاعات مدیریت یا ابقاء شبکه، می باشد. این شاخص، امکان افزودن سلولهای مدیریت شبکه به های کاربر را بدون تأثیر بر داده های کاربر، فراهم می آورد. بنابراین فیلد PT می تواند اطلاعات کنترلی درونی را فراهم آورد.

بیت اولویت فقدان سلول(CLIP)^۵، می تواند به عنوان راهنمایی برای شبکه در حین تراکم، مورد استفاده قرار بگیرد. مقدار صفر نشانگر آنست که سلول اولویت بالایی دارد و نباید دور ریخته شود، مگر آنکه چاره دیگری وجود نداشته باشد. مقدار یک نشانگر آنست که این بسته یک انتخاب مناسب، جهت دور ریختن در شبکه، می باشد. کاربر ممکن است از این فیلد استفاده نماید تا سلولهای اضافی(فراتر از ترخ توافق شده) را به شبکه وارد کند، با CLIP یک، تا درصورت عدم وجود تراکم در شبکه، به مقصد تحويل داده شوند. شبکه ممکن است این بیت را برای هر سلول داده یک بنماید، که این مغایر با پارامترهای ترافیکی توافق شده با کاربر، می باشد. در این حالت سوئیچ که تنظیمات را انجام می دهد متوجه می شود که سلولها از پارامترهای ترافیکی توافقی تخطی کرده اند، اما سوئیچ قادر به مدیریت سلول ها می باشد. اگر در نقطه جلوتری در شبکه، تراکم رخ بدده، این سلولها در برابر سلولهایی که از محدودیتهای ترافیکی توافقی تخطی ننموده اند، جهت دور ریخته شدن، انتخاب و علامت گذاری می شوند.

فیلد کنترل خطای سرآیند، برای کنترل خطای همزمانی، استفاده می شود که در ادامه بررسی می گردد.

کنترل جریان عمومی:

I.150، استفاده از فیلد GFC را برای کنترل جریان در رابط کاربر-شبکه (UNI^۶)، ارائه داده است تا زمینه کاهش بارگذاریهای بیش از حد کوتاه مدت را، فراهم آورد. مکانیزمهای کنترل جریان واقعی در I.361، تعریف شده است. کنترل جریان GFC، بخشی از یک توانایی انتقال سلول کنترل شده(CCT)^۷، در یک ATM WAN مخصوصاً CCT نامزد تهیه سرویس خوب برای ترافیک های انفجاری با حجم بالا با طول پیام متغیر، می باشد.

Virtual Path Identifier -	۱
Virtual Channel Identifier -	۲
Service Data Unit -	۳
Cell Loss Priority -	۴
User-Network Interface -	۵
Controlled Cell Transfer -	۶

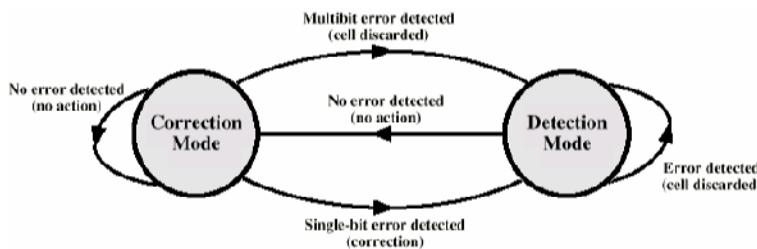
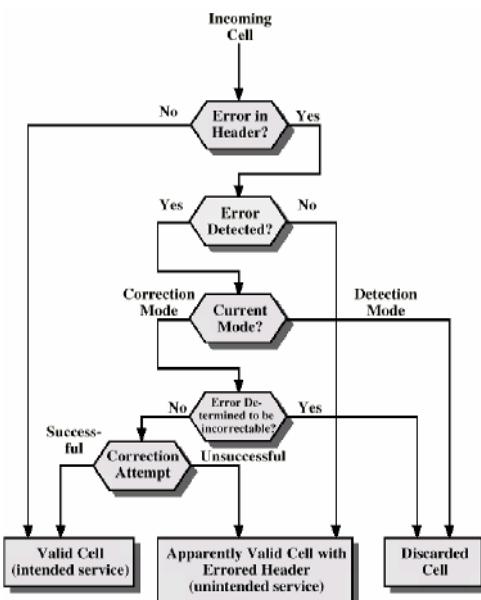


Figure 11.5 HEC Operation at Receiver

تصویر ۷-۵: عملکرد HEC در دریافت کننده

کنترل خطای سرآیند:

هر سلوی ATM شامل ۸ بیت کنترل خطای سرآیند(HEC^۱) می باشد که برایه ۳۲ بیت باقیمانده سرآیند، محاسبه می گردد. چند جمله ای مورد استفاده جهت تولید کد $X^8 + X^2 + X + 1$ می باشد. در اکثر پروتکلهای موجود که شامل فیلد کنترل خطا هستند، همانند HDCL، داده هایی که عنوان ورودی محاسبه در خطا بکار می روند، بسیار بزرگتر از اندازه کد خطای نتیجه می باشد. این امر تشخیص خطای ممکن می سازد. در ATM، ورودی محاسبه تنها ۳۲ بیت، در مقایسه با ۸ بیت برای کد، است. در حقیقت ورودیهای کوچکتر، نه تنها برای تشخیص خطا بکار می روند، بلکه حتی در برخی از موارد، برای تصحیح نیز بکار می روند؛ این موضوع بدليل وجود افزونگی کافی در کد، جهت بازیابی الگوهای خطای خاص، می باشد.



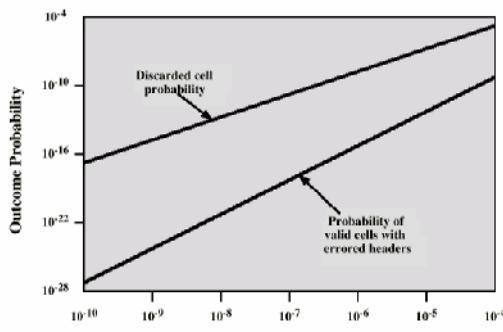
تصویر ۷-۶: تاثیر خطای بر سرآیند سلوی

تصویر ۷-۵، عملکرد الگوریتم HEC را در دریافت کننده، نشان می دهد. در ابتدا، الگوریتم تصحیح خطای دریافت کننده در حالت پیش فرض برای تصحیح یک بیت خطای می باشد. با ورود هر سلوی، محاسبه مقدار HEC، انجام می گیرد. مادامیکه خطای تشخیص داده نشود، دریافت کننده، در حالت تصحیح خطای باقی می ماند. زمانیکه یک خطای تشخیص داده شد، دریافت کننده، اگر یک بیت خطای وجود داشته باشد، آن را تصحیح می کند و اگر چند

بیت خطا وجود داشته باشد، آن را تشخیص می‌دهد. در این حالت دریافت کننده به حالت تشخیص می‌رود. در این حالت تلاشی در جهت تصحیح خطا انجام می‌گیرد. دلیل این تغییر آنست که یک اختلال انفجاری و یا رویداد دیگر، ممکن است باعث مجموعه متوالی از خطاها می‌باشد، حالتی که HEC، جهت تصحیح کد ناکافی می‌باشد. دریافت کننده مادامیکه سلولهای خطاطار دریافت می‌گردد، در حالت تشخیص باقی می‌ماند. زمانیکه یک سرآیند، آزموده شده و خطای در آن یافت نشد، دریافت کننده، دوباره به حالت تصحیح برمی‌گردد. فلوچارت تصویر ۷-۶، پی‌آمد خطاها را در سرآیند سلول، نمایش می‌دهد.

تابع حمایت در برابر خطا، بازیابی از خطاهای تک بیتی سرآیند و احتمال پایین تحویل بسته‌های با سرآیند معیوب، تحت شرایط خطاهای انفجاری را فراهم می‌آورد. خصوصیت خطا سیستم‌های انتقال فیری، ترکیبی از خطاهای تک بیتی و انفجاری بزرگ، می‌باشد و برای برخی سیستم‌های انتقال، توانایی تصحیح خطا، بدلیل وقتگیر بودن آن، ممکن است حذف شود.

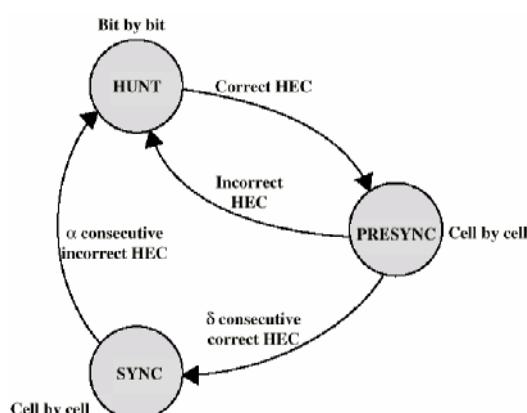
تصویر ۷-۷، برپایه I.432 ITU-T، می‌باشد و نشان می‌دهد که چگونه خطاهایی بیتی اتفاقی بر احتمال وقوع سلولهای دور ریخته شده و سلولهای معتبر با سرآیند معیوب، در زمان استفاده از HEC، تاثیر می‌گذارد.



تصویر ۷-۷: احتمال خطای بیتی

۷-۴: انتقال سلولهای ATM

I.432 بیان می‌کند که سلولهای ATM و یکی از چند نرخ داده 51.84، 155.52 Mbps، 622.08 Mbps و یا 25.6 Mbps، ممکن است منتقل شوند. ما نیازمند تعیین ساختار انتقال مورد استفاده جهت حمل Payload‌ها، می‌باشیم. دو روش در I.432 معرفی شده است: یک لایه فیزیکی سلول پایه و یک لایه فیزیکی SDH پایه.



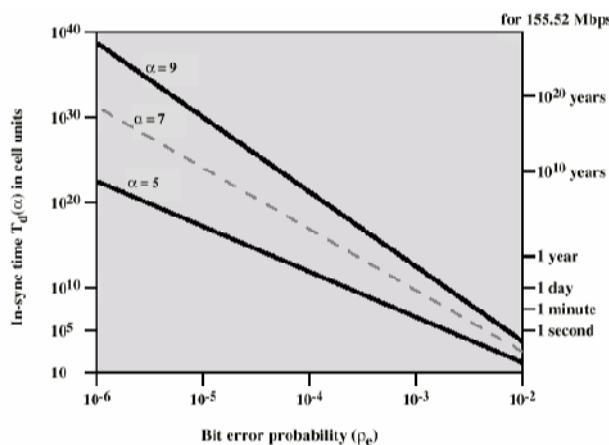
تصویر ۷-۸: نمودار توصیف حالات سلول

لایه فیزیکی مبتنی بر سلول:

برای لایه فیزیکی برپایه سلول هیچ چهارچوب گذاری، تحمیل نمی شود. ساختار رابط شامل جریان سلولهای ۵۳ بایتی است. بدلیل عدم وجود چهارچوب خارجی تحمیلی در روش مبتنی بر سلول، برخی از فرمهای همزمانی لازم می باشد. همزمانی بر مبنای فیلد کنترل خطای سرآیند(HEC)، در سرآیند سلول، بدست می آید. رووال این جریان به شکل زیر می باشد:

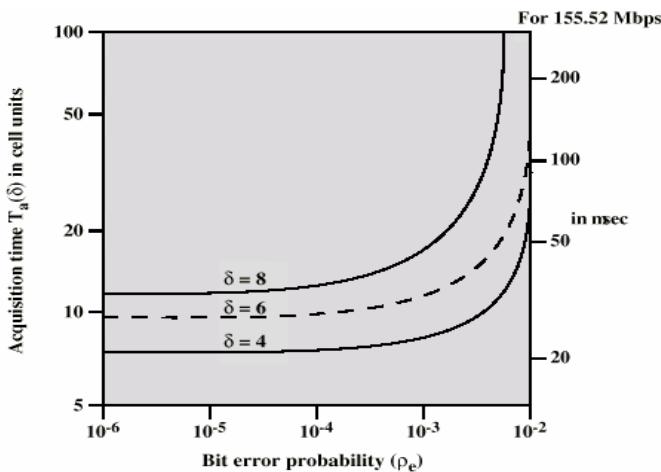
- ۱- در موقعیت HUNT، یک الگوریتم توصیف^۱، بصورت بیت به بیت، جهت تعیین کد HEC و مقایسه بین HEC دریافتی و HEC محاسبه شده، جهت تطبیق آنها، انجام می گیرد. زمانیکه یک تطبیق رخ دهد، فرض می شود که یک سرآیند پیدا شده و رویه به حالت PRESYNC، می رود.
- ۲- در حالت PRESYNC، یک ساختار سلول فرض می گردد. الگوریتم توصیف سلول ، بصورت سلول به سلول، تا زمان Δ ، بطور متواالی قانون رمزگذاری را تایید می نماید.
- ۳- در حالت SYNC، جهت تشخیص و تصحیح خطابکار می رود و سلول توصیف شده در صورت تشخیص α مرتبط خطای متواالی توسط HEC، از دست رفته تلقی می شود.

مقادیر Δ و α ، پارامترهای طراحی می باشند. مقادیر بزرگتر Δ ، باعث زمانهای تاخیر طولانیتر برپاسازی همزمان می باشند، اما قدرت بیشتری را در برابر توصیف اشتباه، پیدا می کند. مقادیر بزرگتر α ، تاخیر بیشتری را در تشخیص مرتب سازیهای اشتباه، باعث می گردد، اما قدرت بیشتری را در برابر مرتب سازیهای اشتباه غلط، ارائه می دهد. تصاویر ۹-۷ و ۱۰-۷ برپایه ۱.۴۳۲ تأثیر خطاهای بیتی اتفاقی بر روی کارایی سلول توصیف را برای مقادیر مختلف Δ و α ، نشان می دهد. تصویر اول نشان دهنده میانگین زمانی است که دریافت کننده همزمانی را در مواجه با خط، حفظ می نماید(با α ، بعنوان یک پارامتر). تصویر دوم نشان دهنده میانگین زمانی، برای بدست آوردن همزمانی، بعنوان تابعی از نرخ خط، می باشد(با Δ ، بعنوان یک پارامتر).



تصویر ۹-۷: تأثیر خطاهای بیتی اتفاقی بر روی توصیف کارایی سلول

Delineation – ^۱



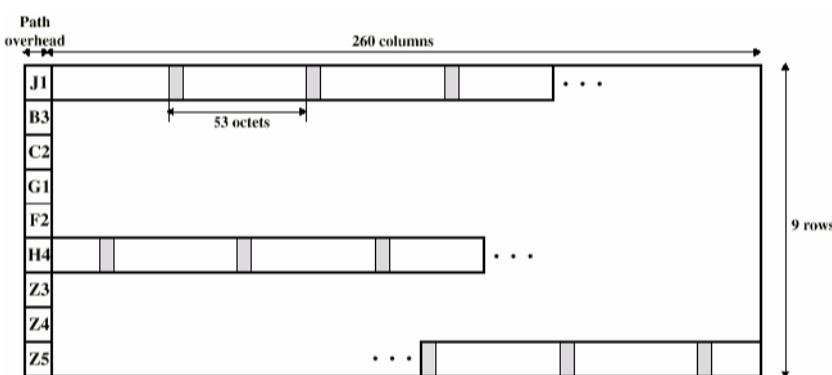
تصویر ۷-۱۰: زمان استفاده در برابر احتمال خطای بیتی

مزیت استفاده از طرح انتقال مبتنی بر سلول، سادگی رابطه می باشد که بواسطه آن هر دوتابع حالت ارسال^۱ و انتقال^۲، برپایه یک طرح عمومی قرار گرفته اند.

لایه فیزیکی مبتنی بر SDH

لایه فیزیکی مبتنی بر SDH یک ساختار را بر جریان سلول ATM تحمیل می نماید. در این بخش ما به I.432 برای سرعت 155.52 Mbps نگاه می کنیم. ساختارهای مشابهی برای سایر نرخ داده ها، مورد استفاده قرار می گیرند. برای لایه فیزیکی مبتنی بر SDH، چهارچوب گذاری، استفاده از چهارچوب (STS-3)STM1 را تحمیل ممکن است نماید. تصویر ۷-۱۱، بخش داده برای بخشی از یک چهارچوب STM1 را نشان می دهد. Payload ممکن است در ابتدای چهارچوب آفست گذاری شود، که بوسیله اشاره گری در بخش سربار چهارچوب، نمایش داده می شود. همانطور که مشاهده می شود، Payload شامل یک بخش سربار ۹ بایتی و باقیمانده که شامل سلولهای ATM است، می باشد. بدلیل اندازه ظرفیت Payload (۴۰۳۴۰ بایت)، که یک ضرب صحیح از طول سلول (۵۳ بایت) نیست، یک سلول ممکن است از مرزهای یک Payload، گذر کند.

بايت H4 در سربار مسیر، در سمت فرستنده، تنظیم می گردد تا موقع مرز سلول بعدی را مشخص نماید. مقدار فیلد H4، نشانگر تعداد بایتهای تا ابتدای مرز اولین سلول پس از بايت H4، می باشد. مقدار مجاز بین صفر تا ۵۲ می باشد.



تصویر ۷-۱۱: برای انتقال سلول ATM مبتنی بر SDH

^۱ Transmission –
^۲ Transfer –

مزایای روش مبتنی بر SDH بشرح زیر می باشد:

- می تواند جهت Payload های مبتنی بر ATM و یا STM¹، بکار می رود و این امکان را فراهم می آورد تا ظرفیت بالای انتقال مبتنی بر فیبر ساختاردار، برای یک سوئیچ مداری متغیر را گسترش داده و کاربردها را تخصیص داده و سپس به سهولت به سمت پشتیبانی از ATM بپرورد.
- برخی اتصالات خاص می توانند با استفاده از یک کانال SDH سوئیچ مداری باشند. برای مثال، یک اتصال حامل ترافیک ویدئویی نرخ بیتی ثابت می تواند به درون Payload انحصاری خود در پوشش سیگنال STM1، نگاشت گردد، که می تواند سوئیچ مداری باشد. این روش ممکن است از سوئیچ ATM موثرتر باشد.
- با استفاده از تکنیکهای مالتی پلکس همزمان SDH، چندین جریان ATM می توانند جهت ایجاد رابطهای با نرخ بیت بالاتر از حد پشتیبانی شده در لایه ATM در یک محل مشخص، با یکدیگر ترکیب گرددند. برای مثال، ۴ جریان ATM مجزا، هرکدام با یک نرخ بیت 155 Mbps (STM1)، می توانند با هم ترکیب شوند تا یک واسطه 622 Mbps (STM4) را بسازند. این کار به لحاظ هزینه موثرتر از جریان ATM 622 Mbps می باشد.

۷-۵: طبقات سرویس ATM

یک شبکه ATM طراحی شده است تا بتواند انواع متفاوتی از ترافیکهای مشابه را شامل جریانات زمان واقعی همانند صوت، تصویر و جریانات انفجاری TCP، را منتقل نماید. اگرچه هر کدام از چنین جریانات ترافیکی، بصورت جریان سلولهای ۵۳ بایتی از طریق یک کانال مجازی ارسال و مدیریت می گرددند. روشی که هر جریان داده می تواند با آن در شبکه مدیریت گردد، به خواص جریان ترافیک و نیازمندیهای کاربرد، بستگی دارد. برای مثال، ترافیک تصویری زمان واقعی باید با حداقل بازه تغییرات تاخیر، تحويل گردد. در این بخش، طبقه بندیهای سرویس ATM را که بوسیله یک سیستم نهایی برای تعیین نوع سرویس مورد نیاز، بکار می رود را خلاصه نموده ایم. طبقات سرویس زیر بوسیله انجمن ATM تعریف شده اند:

- سرویسهای زمان واقعی
 - نرخ بیت ثابت(CBR)
 - نرخ بیت متغیر زمان واقعی(rt-VBR)
- سرویسهای غیر زمان واقعی²
 - نرخ بیت متغیر غیر زمان واقعی(nrt-VBR)
 - نرخ بیت موجود³(ABR)
 - نرخ بیت نامعین⁴(UBR)

سرویسهای زمان واقعی:

مهمنترین تفاوت بین کاربردها، اندازه تاخیر و تغییرات تاخیری⁵ که کاربرد می تواند آن را تحمل نماید، مربوط می شود. کاربردهای زمان واقعی، نوعاً شامل یک جریان اطلاعات به یک کاربر است که به معنی باز تولید آن

Synchronous Transfer Module - ¹

Non Real Time - ²

Available Bit Rate - ³

Unspecified Bit Rate - ⁴

Jitter - ⁵

جريان در منبع می باشد. برای مثال، یک کاربر انتظار دارد یک جریان صوت و تصویر اطلاعات، بصورت پیوسته و نرم ، ارائه گردد. یک نقص در پیوستگی و یا فقدان بیش از اندازه، نتیجه اش از دست رفتن کیفیت سرویس می باشد. کاربردهایی که شامل تعامل در افراد هستند، محدودیتهای سختی در تاخیر دارند. مخصوصاً هر نوع تاخیر بیش از ۱۰۰ میلی ثانیه، می تواند قابل توجه و رنجش آور باشد. براین اساس درخواستها برای سوئیچ و تحويل داده های زمان واقعی در شبکه ATM بالا می باشد.

نحو بیت ثابت:

سرویسهای CBR، شاید ساده ترین سرویس جهت تعریف، می باشد. این سرویس بوسیله کاربردهایی که نیازمند یک نرخ داده ثابت هستند و باید بصورت پیوسته در طول زمان حیاتشان، اتصال موجود باشد و یک حد بالای محکم در تاخیر انتقال داشته باشند، مورد استفاده قرار می گیرد. CBR، بطور عمومی، جهت اطلاعات فشرده نشده صوت و تصویر ، بکار می رود. مثالهایی از CBR عبارتند از:

- ویدئوکنفرانس
- صوت تعاملی(مثل تلفن)
- توزیع صوت/تصویر(مثل تلویزیون، آموزش از راه دور)
- بازیابی صوت/تصویر(مثل تصویر مورد درخواست، کتابخانه صوتی)

نحو بیت متغیر زمان واقعی:

طبقه rt-VBR، برای کاربردهای حساس به زمان می باشد که نیازمند محدودیت تاخیر و تغییرات تاخیر سخت، می باشد. مهمترین تفاوت بین کاربردهای rt-VBR و CBR، آنست که کاربردهای rt-VBR انتقال با نرخ متغیر در طول زمان را دربر می گیرد. یک منبع rt-VBR می تواند تا حدی انفجاری نیز باشد. برای مثال، طرح استاندارد جهت فشرده سازی تصویر، باعث ایجاد فریهای تصویری با اندازه متفاوت می باشد. بدلیل نیاز تصویر زمان واقعی به یک نرخ انتقال فریم یکسان، نرخ داده واقعی متغیر می باشد.

سرویس rt-VBR، به شبکه انعطاف پذیری بیشتری را نسبت به CBR می دهد. شبکه قادر به مالتی پلکس ثابت تعدادی از اتصالات بر روی ظرفیت تخصیص داده شده است و هنوز هم سرویسهای مورد نیاز برای هر سرویس را فراهم می آورد.

سرویسهای غیر زمان واقعی:

سرویسهای غیر زمان واقعی برای کاربردهایی که خصوصیات ترافیک انفجاری داشته و محدودیتهای محکم بر روری تاخیر و تغییرات تاخیر، ندارد، نامزد می باشد. بر این اساس، شبکه انعطاف پذیری بیشتری در مدیریت چنین جریانات ترافیکی داشته و می تواند استفاده بیشتری از مالتی پلکس ثابت، برای افزایش کارایی شبکه را فراهم آورد.

نحو بیت متغیر غیر زمان واقعی:

برای برخی کاربردهای غیر زمان واقعی، ممکن است ترافیک مورد انتظار بگونه ای توصیف گردد که شبکه بتواند کیفیت سرویس را در مناطق فقدان و تاخیر، بهبود بخشد. چنین کاربردهایی می تواند از سرویسهای nrt-VBR استفاده نمایند. با این سرویس، سیستم نهایی یک نرخ سلول حداکثر، یک نرخ سلول قابل تحمل یا میانگین و یک اندازه از نحوه انفجاری یا انبوه بودن سلولها را مشخص نماید. با این اطلاعات، شبکه می تواند منابع را جهت تاخیر و فقدان سلول پایین و حداقل، تخصیص دهد.

سرویس **nrt-VBR**، می تواند برای انتقال داده که نیازمند زمان پاسخ بحرانی است، مورد استفاده قرار گیرد.
مثالهایی از این سرویس، رزرواسیون هواپیما، تراکنشهای بانکی و نظارت کردن بر پردازشها، می باشد.

نحو بیت نامعین:

در هر زمان، بخش معینی از ظرفیت یک شبکه ATM، جهت حمل انواع ترافیک CBR و VBR، صرف می گردد. ظرفیت اضافی برای یکی یا هر دو منظور زیر موجود می باشد:^۱ ۱) همه منابع به ترافیکهای CBR و VBR تخصیص نمی یابند و ۲) طبیعت انفجاری VBR به این معنیست که گاهی اوقات، ظرفیتی کمتر از ظرفیت تخصیصی، مورد استفاده قرار می گیرد. همه این ظرفیتهای بدون استفاده می تواند جهت سرویسهای VBR، موجود باشند. این سرویسها برای کاربردهایی که می توانند تغییرات تاخیر و برخی فقدان بسته ها را تحمل کنند، ترافیکهای مبتنی بر TCP، مناسب می باشند. با VBR، سلولها بصورت اولین ورود-اولین خروج^۱، با استفاده از ظرفیت بدون استفاده سایر سرویسها، ارسال می گرددند و هر دوی تاخیر و فقدان متغیر، ممکن است وجود داشته باشند. هیچ الزام اولیه ای برای منبع VBR ایجاد نمی گردد و هیچ بازخوردی نیز در باب تراکم ایجاد نمی گردد. به این سرویس، سرویس "بهترین تلاش"^۲ گفته می شود. مثالهایی از کاربردهای VBR در زیر آمده است:

- انتقال متن/داده/تصویری، پیغام دهی، توزیع، بازیابی
- پایانه راه دور (مثل ارتباط برقرار کردن راه دور^۳)

نحو داده موجود:

کاربردهای انفجاری که از یک پروتکل انتهای به انتهای مطمئن مانند TCP، استفاده می نمایند، می توانند تراکم در شبکه را بوسیله افزایش تاخیر رفت و برگشت و دور ریختن بسته ها، تشخیص دهنند. اگرچه TCP مکانیزمی جهت به اشتراک گذاشتن منصفانه منابع شبکه بین تعداد زیادی اتصالات TCP را ندارد. بعلاوه TCP نمی تواند تراکم را بصورت موثر، با استفاده از اطلاعات صریح گره های تحت تراکم شبکه، کم نماید. برای بهبود سرویس فراهم شده و برای منابع انفجاری که از UBR بشکل دیگر استفاده می کنند، سرویس ABR^۴ تعریف گشته است. کاربردهایی که از ABR استفاده می نمایند، یک نرخ سلول حداقل(PCR) را مشخص می کنند که از آن استفاده خواهند کرد و یک نرخ سلول حداقل(MCR)^۵ که به آن نیاز دارند. شبکه، منابع را بگونه ای تخصیص می دهد تا همه کاربردهای ABR حداقل ظرفیت MCR خود را دریافت نمایند. هر ظرفیت استفاده نشده، بصورت منصفانه و کنترل شده بین همه منابع ABR، به اشتراک گذاشته می شود. مکانیزم ABR از بازخورد صریح به مبدأ، استفاده می نماید تا اطمینان یابد که ظرفیت، منصفانه تخصیص یافته است. هیچ ظرفیت بدون استفاده ای توسط مبدأ های ABR، با ترافیک UBR باقی نمی ماند.

مثالهایی از کاربرد استفاده کننده از ABR، تماس بین LANها می باشد. در این حالت سیستمهای نهایی متصل به شبکه ATM مسیریابها می باشند. تصویر ۱۲-۷، چگونگی تخصیص منابع شبکه در طول یک دوره زمانی حالت دائمی(بدون حذف یا افزودن کانالهای مجازی) را تشریح می کند.

۷-۶: لایه تطبیق ATM

FIFO - ^۱

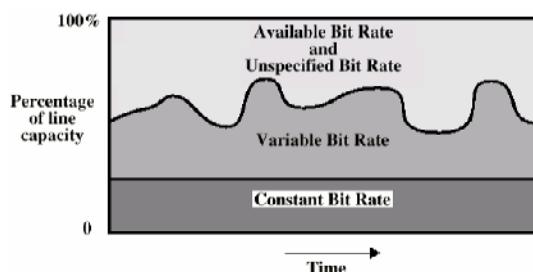
Best Effort - ^۲

Telecommuting - ^۳

Peak Cell Rate - ^۴

Minimum Cell Rate - ^۵

استفاده از ATM نیاز به یک لایه تطبیق جهت پشتیبانی از پروتکلهای انتقال اطلاعات که برپایه ATM نیستند، را ایجاد می‌نماید. دو نمونه از این پروتکلها PCM^۱ صوت و پروتکل اینترنت(IP)، می‌باشد. PCM صوت، یک کاربرد است که جریانی از بیتها را از یک سیگنال صوت، تولید می‌کند. جهت استفاده از این کاربرد بر روی ATM لازم است تا بیتهای PCM، در سلولها، جهت انتقال، قرار بگیرند و در مقصد بازخوانی گردند. در یک محیط ترکیبی که در آن شبکه‌های مبتنی بر IP به شبکه‌های ATM متصل هستند، یک راه ساده که یک جریان نرم و ثابت از بیتها به دریافت کننده، فراهم گردد، نگاشت بسته‌های IP به سلولهای ATM است. این امر عمدتاً به معنی قطعه قطعه کردن یک بسته IP و قراردادن آنها در درون سلولها جهت انتقال و بازسازی بسته از سلولها، در گیرنده می‌باشد. با مجاز شدن IP بر روی ATM، هر ساختار موجود IP می‌تواند بر روی شبکه ATM بکار رود.



تصویر ۱۲-۷: نرخ بیت سرویسهای ATM

سرویسهای AAL:

ITU-T I.362، مثالهای عمومی زیر را از سرویسهای تهیه شده بوسیله AAL، را لیست نموده است:

- مدیریت خطاهای انتقال
- قطعه قطعه کردن و بازسازی، جهت ایجاد توانایی انتقال بسته‌های بزرگ داده در فیلد اطلاعات سلوهای ATM
- مدیریت شرایط فقدان و الحاق اشتباه سلول
- کنترل جریان و زمان

جهت کم کردن تعداد پروتکلهای مختلف AAL که باید جهت رسیدن به نیازهای متغیر، مشخص شوند، ITU-T ۴، کلاس سرویس را که دامنه وسیعی از نیازمندیها را پوشش می‌دهد، تعریف نموده است. کلاس بندی برپایه آن بوده است که یک ارتباط زمانی باید بین مبدأ و مقصد حفظ گردد، چه اینکه کاربر نیازمند یک نرخ بیت ثابت باشد و چه اینکه انتقال ، اتصال گرا باشد یا بدون اتصال باشد. طبقه بندی سیستم، اکنون دیگر در اسناد ITU-T دیده نمی‌شود، اما مفهوم آن جهت توسعه پروتکل‌های AAL، مفید می‌باشد. بطور ذاتی، لایه AAL مکانیزمهایی جهت نگاشت کاربردهای متفاوت بسیاری به لایه ATM را فراهم نموده است و همچنین، پروتکلهایی را بر بالای تواناییهای مدیریت ترافیک لایه ATM، فراهم نموده است. بنابراین طراحی پروتکلهای AAL باید مرتبط با طبقات سرویس گفته شده در بخش‌های قبلی، باشد.

Network Architecture	Service Model	Guarantees ?			Congestion feedback
		Bandwidth	Loss	Order	
Internet	best effort	none	no	no	no (inferred via loss)
ATM	CBR	constant rate	yes	yes	no congestion
ATM	VBR	guaranteed rate	yes	yes	no congestion
ATM	ABR	guaranteed minimum	no	yes	yes
ATM	UBR	none	no	yes	no

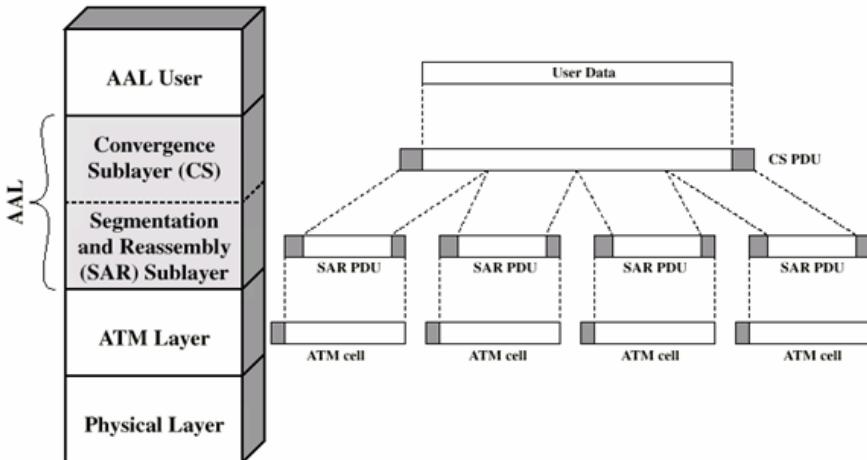
جدول ۴-۷: مقایسه سرویس‌های ATM با اینترنت

UBR	ABR	nrt-VBR	rt-VBR	CBR	
				تقلید مدار، ATM صوت برروی	AAL 1
			صوت و تصویر VBR		AAL 2
		سرвис داده عمومی			AAL 3/4
ATM برروی IP	LAN تقلید	Frame Relay, ATM LAN	صوت براساس نیاز، تقلید LAN	LAN تقلید	AAL 5

جدول ۵-۵: پروتکلها و سرویس‌های AAL

جدول ۵-۵، ۴ پروتکل AAL را با طبقات سرویس معرفی شده توسط انجمان ATM نمایش می‌دهد. موجودیت‌های جدول، نشانگر انواع کاربردهایی است که AAL و ATM می‌توانند با یکدیگر، آنها را پشتیبانی نمایند. آنها به شرح زیر می‌باشند:

- تقلید مدار: به پشتیبانی از ساختارهای انتقال TDM هم‌مان، همانند T1، بر روی یک شبکه ATM، اشاره می‌کند.
- صوت و تصویر VBR: اینها کاربردهای زمان واقعی هستند که بصورت فشرده منتقل می‌شوند. یکی از تاثیرات فشرده سازی، آنست که یک نرخ بیت متغیر می‌تواند کاربرد را حمایت نماید که نیازمند یک تحويل جریان بیتی پیوسته به مقصد می‌باشد.
- سرویس‌های داده عمومی: این شامل سرویس‌های پیام دهی و تراکنش می‌باشد که نیازمند پشتیبانی زمان واقعی نیستند.
- IP بر روی ATM انتقال بسته‌ها IP توسط سلولهای ATM.
- محصورسازی چند پروتکل بر روی MPOA(ATM)^۱: پشتیبانی گسترده متغیری از پروتکلهای جدا از IP(DECNET، Apple Talk، IPX، بر روی ATM) همانند
- تقلید LAN (LANE): پشتیبانی از ترافیک LAN به LAN از طریق شبکه‌های ATM، با شبیه سازی توانایی LAN Broadcast (انتقال از یک ایستگاه به تعداد زیادی ایستگاه)، جهت مجاز ساختن یک انتقال ساده از محیط یک LAN به محیط یک ATM می‌باشد.



تصویر ۱۳-۷: پروتکلهای AAL و PDU ها

پروتکلهای AAL^۱

لایه AAL به دو زیر لایه تقسیم می گردد: زیر لایه همگرایی (CS)^۲ و زیر لایه قطعه کردن و بازسازی (SAR)^۳. زیر لایه همگرایی، توابع مورد نیاز برای پشتیبانی از کاربردهای خاص استفاده کننده از AAL را فراهم می آورد. هر کاربر AAL در یک نقطه دسترسی سرویس (SAP)^۴ به AAL منتقل می گردد که به سادگی آدرس کاربرد می باشد. بنابراین این زیر لایه وابسته به کاربرد می باشد.

زیر لایه قطعه کردن و بازسازی، مسئول بسته بندی اطلاعات دریافتی از DS به درون سلوها جهت انتقال و خارج سازی اطلاعات از بسته ها در سمت دیگر، می باشد. همانطور که دیدیم، در لایه ATM هر سلول شامل ۵ بایت سرآیند و یک فیلد اطلاعات ۴۸ بایتی، می باشد. بنابراین SAR باید هر سرآیند و دنباله SAR و اطلاعات CS را درون بلاکهای ۴۸ بایتی، قرار دهد.

تصویر ۱۳-۷ عماری پروتکل عمومی برای ATM و AAL را نشان می دهد. یک بلاک داده لایه بالاتر در یک واحد داده پروتکل (PDU)^۵ یکتا، محصور شده است که شامل داده لایه های بالاتر و احتمالاً یک سرآیند و دنباله حاوی اطلاعات پروتکل در سطح CS، می باشد. سپس این PDU ای CS به لایه پایین SAR منتقل می گردد و به تعدادی بلاک تقسیم می شود. هر کدام از این بلاکها در یک PDU ای SAR ۴۸ بایتی منفرد، محصور می شود. که ممکن است شامل سرآیند و دنباله ای علاوه بر بلاک داده به پایین منتقل شده از CS، باشد سرانجام هر PDU ای SAR نقش Payload یک سلول منفرد ATM را می یابد.

بطور پایه، ITU-T چهار نوع پروتکل را تعریف نموده است، از نوع ۱ تا نوع ۴. در واقع هر پروتکل، حاوی ۲ پروتکل می باشد: یکی در زیر لایه CS و دیگری در زیر لایه SAR. اخیراً انواع ۳ و ۴ بصورت یک نوع ۴/۳ ادغام شده اند و یک نوع جدید، نوع ۵، تعریف شده است. در هر حالت بلاکی از داده ها از لایه بالاتر در یک واحد داده (PDU) پروتکل در زیر لایه CS، محصور شده است. در حقیقت این زیر لایه که به عنوان بخش عمومی زیر لایه همگرایی (CPCS)^۶، مورد ارجاع قرار می گیرد، احتمال اینکه تبع اضافی یا خاص بر روی سطح CS، اعمال گرددند، را باز گذاشته است. سپس PDU ای CPCS منتقل می شود که در آنجا به اندازه بلاکهای Payload، شکسته می شود. هر بلاک Payload، می تواند در یک PDU ای SAR قرار گیرد که طول کلی ۴۸ بایتی دارد. هر PDU ای SAR ۴۸ بایتی، می تواند در یک سلول ATM منفرد، قرار بگیرد.

^۱ Convergence Sublayer -

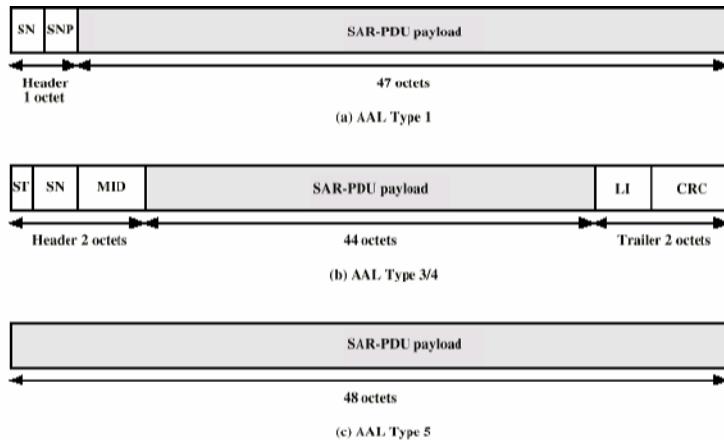
^۲ Segmentation And Reassembly -

^۳ Service Access Point -

^۴ Protocol Data Unit -

^۵ Common Part Convergence Sublayer -

تصویر ۱۴-۷، فرمت واحدهای داده پروتکل (PDU) را در سطح SAR بجز نوع ۲ که هنوز تعریف نشده است، را نشان می‌دهد.



SN = sequence number (4 bits)
SNP = sequence number protection (4 bits)
ST = segment type (2 bits)
MID = multiplexing identification (10 bits)
LI = length indication (6 bits)
CRC = cyclic redundancy check (10 bits)

تصویر ۱۴-۷: پروتکل تقسیم و بازسازی (SAR) واحد داده پروتکل (PDU)

نوع ۱: AAL

برای بررسی عملکرد نوع ۱، یک منبع نرخ ثبات را مورد بررسی قرار می‌دهیم. در این حالت، تنها وظیفه پروتکل SAR، قرار دادن بیتها به درون سلولها، جهت انتقال و استخراج آنها در مقصد، می‌باشد. هر بلاک، بوسیله یک شماره توالی (SN^۱)، همراهی می‌گردد تا PDU‌های معیوب، قابل ردیابی باشند. فیلد SN ۴ بیتی شامل یک بیت شناسه زیر لایه همگرایی (CSI^۲) و سه بیت شمارش توالی (SC^۳، می‌باشد. در انتقال، زیر لایه CS، جهت زیر لایه SAR، یک مقدار CSI، جهت قرار گرفتن در فیلد SN را فراهم می‌آورد. در گیرنده، زیر لایه SAR، این مقدار را به سمت بالا، جهت زیر لایه CS، ارسال می‌نماید. بیت CSI در مبادله اطلاعات به شیوه زیر مورد استفاده قرار می‌گیرد: سه بیت شمارش توالی یک ساختار چهارچوب، شامل ۸ سلول متوالی را شامل می‌گردد، شماره‌های صفر تا هفت. مقدار سلولهای ۱، ۳، ۵ و ۷، بعنوان یک مقدار زمانی ۴ بیتی، تعییه می‌گردد. این مقدار جهت اندازه گیری تفاوت اندازه فرکانس بین ساعت مرجع شبکه و ساعت انتقال دهنده، بکار می‌رود. در هر سلول با شماره زوج، CSI می‌تواند جهت پشتیبانی دسته بندی اطلاعات، از یک لایه بالاتر، بکار می‌رود. اگر بیت CSI در یک سلول با شماره زوج (۲، ۴، ۶)، به یک تنظیم گردد. اولین بیت Payload SAR PDU^۴ اشاره گری است که شروع دسته ساخت یافته بعدی در Payload این سلول و سلول بعدی را نشان می‌دهد. در این حالت، زوج سلولها (۰-۱، ۲-۳، ۴-۵، ۶-۷)، بعنوان دربردارنده یک اشاره گر یک بایتی و یک Payload ۹۳ بایتی عمل کرده و اشاره گر، محلی را بایت اول دسته بعدی قرار دارد را نشان می‌دهد. مقدار آفست ۹۳، جهت مشخص کردن پایان Payload ۹۳ بایتی، همزمان با خاتمه یک دسته ساخت یافته، مورد استفاده قرار می‌گیرد. مقدار آفست مجازی ۱۲۷، زمانیکه هیچ مرز ساختاری مشخص نشده باشد، بکار می‌رود.

فیلد ۳ بیتی SC، همانطور که دیدیم، یک ساختار چهارچوب ۸ سلولی را ایجاد می‌نماید. همچنین یک ابزار تشخیص سلولهای گم شده/ترتیب بهم ریخته را فراهم می‌آورد.

Sequence Number - ^۱
Convergence Sublayer Indication - ^۲
Sequence Count - ^۳

فیلد حمایت از شماره توالی(SNP)، یک کد خطا برای تشخیص خطا و احتمالاً تصحیح آن در فیلد شماره توالی، می باشد. این فیلد شامل یک بررسی افونگی دوره ای (CRC^۱) ۳ بیتی محاسبه شده بر مبنای فیلد ۴ بیتی و یک بیت توازن می باشد. بیت توازن بگونه ای تنظیم می گردد تا توازن سرآیند ۸ بیتی SAR را بسازد.

هیچ PDU CS براي نوع ۱ تعريف نشده است.تابع زير لايه CS براي نوع ۱، بوسيله ساعت و همزمانی ابتدائي ، عمل كرده و يك سرآيند CS جداگانه مورد نياز نمي باشد.

نوع AAL ۲

ساير انواع پروتکل، ۲، ۳/۴ و ۵، با اطلاعات نرخ بيت متغير ، سروکار دارند. نوع ۲ جهت کاربردهای آنالوگ همانند تصویر و صوت که نيازمند اطلاعات زمانی، بدون نياز به نرخ بيت ثابت هستند، نامزد می باشد. خصوصيات اوليه پروتکل ۲ (CS و SAR)، حذف شده اند و نسخه جاري I.363، سرويسها و توابع فراهم شده را ليست كرده است.

نوع AAL ۳/۴

خصوصيات پايه نوع ۳ و ۴ AAL در فرمت PDU و عملكرد، بسيار شبيه به هم بودند. براین اساس، ITU-T تصميم گرفت که اين دو را در يك پروتکل منفرد، در زير لايه هاي CS و SAR، ترکيب نماید، که به عنوان نوع ۳/۴ شناخته می شود.

انواع سرويس فراهم شده توسيط نوع AAL ۳/۴ می تواند در ۲ بعد توصيف گردد:

- ۱ - سرويس ممکن است اتصال گرا يا بدون اتصال باشد. در فرم اول، هر دسته داده ارائه شده به لايه SAR (واحد داده سرويس SAR و يا SDU^۲)، بطور مستقل عمل می کند. در حالت بعدی، امكان تعريف اتصالات منطقی SAR چندگانه بر روی يك اتصال ATM منفرد، وجود دارد.
- ۲ - سرويس ممکن است حالت پيام^۳ يا جريان^۴ داشته باشد. سرويس حالت پيام، داده دسته بندي شده را منتقل می نماید. بنابراین هر پروتکل OSI مرتبط و کاربردی، می خواهد در اين طبقه جا بگيرد. مخصوصاً LAPD^۵ يا Frame Relay^۶ تمایل به قرار گرفتن در حالت پيام دارند. يك بلاک دسته منفرد از لايه بالاي AAL در يك يا چند سلول، منتقل می گدد. سرويس حالت جريان، از انتقال داده پيوسته با سرعت پايان با نيازمنديهاي تاخير کم، پشتيباني می کند. ممکن است در كمترین حالت، تنها يك بيت در يك دسته با طول ثابت AAL، قرار گيرد. هر دسته در يك سلول منتقل می شود.

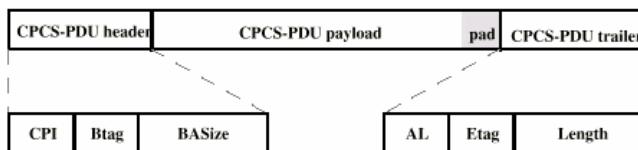
نوع AAL ۳/۴ سرويس انتقال داده خود را با پذيرش دستهای داده از لايه بالايي بعدی و ارسال هر کدام به يك کاربر AAL مقصد، فراهم می آورد. از آنجائیکه لايه ATM^۷ انتقال داده را به Payload های ۴۸ بايتي يك سلول، محدود می سازد، لايه AAL^۸ حداقل يك تابع قطعه قطعه کردن و بازسازی را باید فراهم آورد. عملكرد نوع AAL ۳/۴ بشرح زير می باشد. يك دسته داده از زير لايه بالاتر، همانند يك PDU^۹ در زير لايه CPCS^{۱۰}، محصور می گردد. سپس PDU^{۱۱} به زير لايه SAR^{۱۲} منتقل می گردد که به دسته های Payload^{۱۳} بايتي، تقسيم می گردد. هر دسته Payload^{۱۴} می تواند در يك PDU^{۱۵} قرار بگيرد که شامل يك سرآيند و يك دنباله برای طول کلي ۴۸ بايت می باشد. هر PDU^{۱۶} SAR ۴۸ بايتي در يك سلول منفرد، قرار می گيرد.

^۱ Cyclic Redundancy Check -

^۲ Service Data Unit -

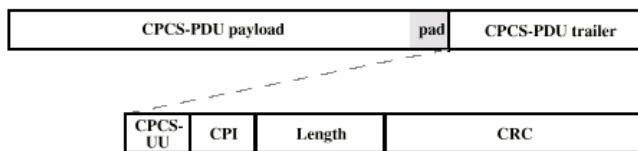
^۳ Message Mode -

^۴ Streaming Mode -



CPI = common part indicator (1 octet)
 Btag = beginning tag (1 octet)
 BASize = buffer allocation size (2 octets)
 AL = alignment (1 octet)
 Etag = end tag (1 octet)
 Length = length of CPCS-PDU payload (2 octets)

(a) AAL Type 3/4



CPCS-UU = CPCS user-to-user indication (1 octet)
 CPI = common part indicator (1 octet)
 Length = length of CPCS-PDU payload (2 octets)
 CRC = cyclic redundancy check (4 octets)

(b) AAL Type 5

تصویر ۷-۱۵: CPCS PDU

جهت درک عملکرد ۲ زیر لایه در نوع AAL ۳/۴، اجاز بدهید به PDU های مرتبط، نگاهی بیاندازیم. PDU^۱ در تصویر ۷-۱۵ نشان داده شده است. سرآیند، شامل سه فیلد می باشد:

- نشان دهنده بخش عمومی (۱ بایت): تغییر فیلدهای باقیمانده در سرآیند PDU را مشخص می نماید. در حال حاضر تنها یک تعبیر، تعریف گشته است: یک مقدار صفر CPI نشاندهنده آنست که فیلد ABSIZE، یک نیاز تخصیص بافر در بایتها را معرفی می نماید و فیلد طول نیز طول CPCS Payload را بر حسب بایت، مشخص می نماید.
- برچسب شروع^۱ (۱ بایت): عددیست که مرتبط با یک CPCS PDU معین می باشد. مقدار مشابهی در فیلد Btag، در سرآیند و فیلد Etag در دنباله، مشاهده می گردد. ارسال کننده، این مقدار را برای هر CPCS PDU پیاپی تغییر می دهد که براساس آن گیرنده قادر به تشخیص سرآیند و دنباله هر CPCS PDU مرتبط با هم ، گردد.
- اندازه تخصیص بافر (۲ بایت): نشاندهنده حداقل اندازه بافر مورد نیاز برای بازسازی SDU CPCS در موجودیت همتای دریافت کننده می باشد. برای حالت پیام، این مقدار برابر با طول CPCS Payload می باشد. برای حالت جریان، این مقدار، بزرگتر یا مساوی طول CPCS Payload می باشد.

- لایه بالایی بعدی با بیتهای غیر لازم کشیده می شود^۲ تا در یک حد ۳۲ بیتی قرار گیرد. دنباله CPCS PDU، شامل سه فیلد می گردد:
- تنظیم (۱ بایت): یک بایت پرکننده که تنها به منظور اینکه طول CPCS PDU، ۳۲ بیتی شود، مورد استفاده قرار می گیرد.

¹ Beginning Tag -

² Pad out -

- برچسب انتهای ۱ بایت): با فیلد Btag در سرآیند بکار می رود.
- طول ۲ بایت): طول فیلد Payload PDU

بنابراین هدف لایه CPCS، اعلام ورود یک دسته داده ، بصورت قطعات، به دریافت کننده می باشد و باید فضای بافر، جهت بازسازی آن تخصیص یابد. این موضوع تابع CPCS دریافت کننده را جهت بررسی پذیرش درست تمام PDU ای CPCS، توانا می سازد.

- تصویر b ۱۵-۷ ، فرمت SAR نوع ۳/۴ را نشان می دهد. اطلاعات از لایه بالایی بعدی ، CS، بصورت دسته هایی که بعنوان واحد داده سرویس SAR مطرح هستند، دریافت می گردد. هر SDU در یک یا بیشتر از یک PDU ای SAR منتقل می گردد. هر SAR در یک سلول ATM منفرد منتقل می شود. فیلدهای سرآیند SAR، جهت اهداف پردازش قطعات SDU در انتقال و بازسازی آنها در زمان پذیرش در مقصد، بکار می رود:
- نوع سگمنت: ۴ نوع PDU ای SAR وجود دارد. یک پیام متواالی منفرد (SSM)، یک SDU ای SAR کامل را شامل می گردد. اگر SDU ای SAR به دو یا چند SAR تقسیم شود، اولین PDU ای SAR آغاز پیام(BOM) و آخرین SAR پایان پیام(EOM) می باشد. و هر PDU ای SAR میانی، ادامه پیام COM^۱ می باشد.
- شماره توالی: در بازسازی یک PDU ای SAR، جهت اطمینان از دریافت تمام PDU های SAR و SAR الحاق صحیح آنها، بکار می رود. یک مقدار شماره توالی ، برای یک SDU ای SAR واحد، در BOM تنظیم شده و در هر COM و EOM، یکی به آن افزوده می شود.
- شناسایی مالتی پلکس(۱۰ بیت): این یک شناسه منفرد مرتبط با مجموعه ای از PDU های SAR می باشد که یک PDU ای SAR تنها را حمل می نمایند. این شماره نیز جهت اطمینان از بازسازی صحیح، مورد نیاز می باشد. در کاربردهای اتصال گرا، این فیلد اجازه مالتی پلکس چند اتصال SAR را در یک اتصال ATM می دهد.

دنباله PDU ای SAR، شامل فیلدهای زیر می باشد:

- نشانگر طول: تعداد بایتهایی از SDU ای SAR که واحد تقسیم سازی SAR را اشغال کرده اند، را نشان می دهد. این عدد مقداری بین ۴ تا ۴۴ (مضرب ۴) می باشد. این مقدار، همیشه برای PDU های BOM و COM SAR می باشد. این مقدار در یک SSM، اگر طول SDU ای SAR کمتر از ۴۴ باشد، مقدار کمتری خواهد بود. همچنین این مقدار در EOM نیز اگر طول SDU ای SAR مضربی از ۴۴ نباشد، مقداری کمتر از ۴۴ خواهد بود. در این حالت بدليل آنکه طول EOM نیز باید ۴۴ بایت گردد، ناگزیر هستیم باقیمانده Payload PDU ای SAR را با بیتهای غیرلازم، پر کنیم.
- CRC: یک CRC ۱۰ بیتی بر روی تمام PDU ای SAR، می باشد.

یک خصیصه مشخص از ۳/۴ AAL آنست که می تواند جریانهای متفاوت داده را ببرروی یک اتصال ATM مجازی یکسان (VPI/VCI)، مالتی پلکس کند. برای سرویسهای اتصال گرا، هر اتصال منطقی بین کاربران AAL متفاوت می تواند ببرروی یک اتصال واحد ATM، مالتی پلکس گردد. برای سرویسهای بدون اتصال می تواند جهت تبادل یک شناسه یکتا مرتبط با هر کاربر بدون اتصال، بکار رود و در این حالت نیز ترافیک کاربران AAL ممکن است مالتی پلکس گردد.

^۱Continuation of Message - ۱

AAL ۵ نوع

جدیدترین خصیصه افزوده شده به AAL، پروتکل نوع ۵ می باشد. این پروتکل جهت فراهم کردن یک امکان انتقال ساده و موثر برای پروتکلهای لایه بالاتر اتصال گرای معرفی شده است. اگر فرض شود که لایه بالاتر مراقب مدیریت اتصال می باشد و لایه ATM خطاهای کمی را باعث می گردد، بخش عمده ای از فیلدهای نوع $\frac{3}{4}$ SAR و VPI/VCI، PDU مورد نیاز نمی باشد. برای مثال، با سرویس‌های اتصال گرای، به فیلد MID، نیازی نیست، جهت مالتی پلکس سلول به سلول، موجود است و لایه بالاتر، مالتی پلکس پیام به پیام را پشتیبانی می کند. نوع ۵ برای اهداف زیر معرفی شده است:

- کاهش سربار پردازش پروتکل
- کاهش سربار انتقال
- اطمینان از تطبیق با پروتکلهای انتقال موجود

تصویر C ۱۴-۷ و b ۱۵-۷، فرمتهای PDU SAR و CPCS برای نوع ۵ را نشان می دهند. در مقایسه با نوع $\frac{3}{4}$ SAR، حجم سربار زیر وجود دارد:

نوع $\frac{3}{4}$	نوع ۵
۸ بایت برای SDU AAL	۸ بایت برای SDU AAL
چهار بایت برای سلول ATM	ATM

جهت درک عملکرد نوع ۵، اجازه بدھید با سطح CPCS، شروع نمائیم. U-PDU (تصویر ۱۱b-۱۵) دنباله ای با فیلدهای زیر دارد:

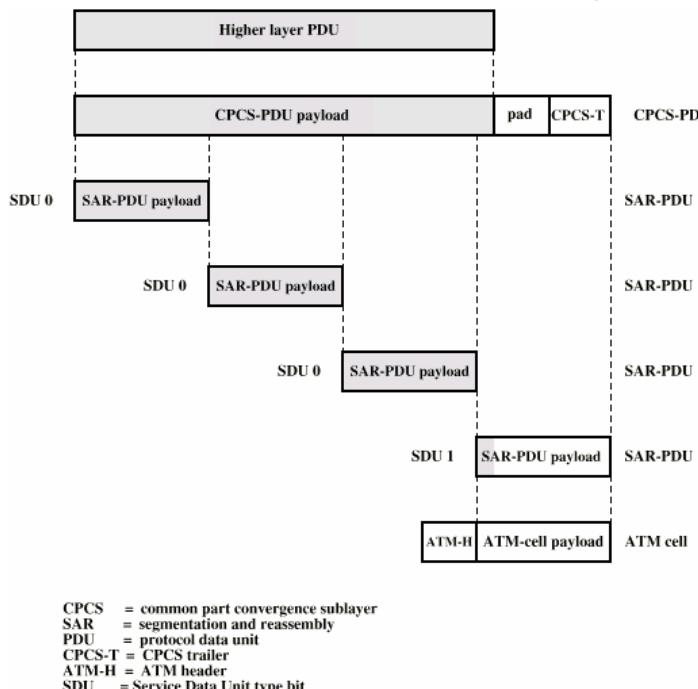
- نشانه کاربر به کاربر (CPCS ۱ بایت): جهت انتقال اطلاعات شفاف کاربر به کاربر بکار می رود.
- نشانه بخش عمومی (۱ بایت): جهت تفسیر فیلدهای باقیمانده در دنباله PDU CPCS، بکار می رود. در حال حاضر، تنها یک تفسیر وجود دارد.
- طول (۲ بایت): طول فیلد Payload PDU CPCS ای.
- ۴ بایت): جهت تشخیص خطاهای بیتی در PDU CRC CPCS بکار می رود.

توجه کنید که امکان ABSIZE تقلید شده است. اگر احیاناً دریافت کننده نیاز به پیش تخصیص یک بافر برای انجام بازسازی، احساس کند، این اطلاعات باید به یک لایه بالاتر، انتقال یابد. در حقیقت بسیاری از پروتکلهای لایه بالاتر جهت حداقل اندازه PDU، تنظیم شده یا می شوند. این اطلاعات می تواند برای دریافت کننده جهت تخصیص بافر، بکار رود. CPCS ۳۲ بیتی، تمام PDU CRC را حفاظت می کند که در مقایسه با آن، در نوع $\frac{3}{4}$ AAL ۳/۴ بکار رود. ۱۰ CRC بیتی برای هر PDU SAR، فراهم می گردد، نوع ۵ حمایت قویتری را در برابر خطاهای بیتی فراهم می آورد. بعلاوه ۳۲ CRC بیتی یک تشخیص قوی بهم ریختگی ترتیب سلول، شرایط خطایی که ممکن است تحت شرایط خرابی شبکه رخ دهد، را فراهم می آورد.

Payload لایه بالایی با بیتیایی بدون استفاده، پر می شود تا همه PDU های CPCS، مضری از ۴۸ بایت گردد. SAR PDU ۴۸ بایت Payload شامل است که بخشی از CPCS PDU را حمل می نماید. نبود سربارهای پروتکل، چند معنی دارد:

- بدليل عدم وجود شماره توالی، دریافت کننده باید فرض کند که تمام PDU های SAR با ترتیب درست جهت بازسازی، دریافت شده اند. فیلد CRC در PDU CPCS، نامزد است تا آن را تایید کند.

- نبود فیلد MID به معنی آنست که امکان تقسیم سلولهای PDU های مختلف وجود ندارد. بنابراین هر PDU پی در پی، بخشی از CPCS PDU جاری را و یا اولین دسته CPCS بعدی را حمل می نماید. جهت تشخیص بین این دو حالت، بین نوع ATM SDU در فیلد نوع Payload در سرآیند سلول ATM، مورد استفاده قرار می گیرد (تصویر ۷-۴). یک CPCS PDU شامل صفر یا بیشتر SAR متواالی با بیت نوع SDU تنظیم شده به صفر، است که بدنبال آن یک PDU SAR با بیت نوع SDU تنظیم شده به یک، می آید.
- نبود فیلد LI به معنی آنست که هیچ راهی برای موجودیت SAR برای تشخیص بین بیتهاي CPCS PDU و پرشده در آخرین SAR وجود ندارد. بنابراین هیچ راهی برای موجودیت SAR برای یافتن دنباله CPCS PDU در آخرین SAR وجود ندارد. برای اجتناب از این موقعیت، لازم است تا Payload CPCS PDU با بیتهاي غیر ضروری پر شود تا آخرین بیت دنباله CPCS در آخرین بیت SAR آخر ، قرار گیرد.



تصویر ۷-۶: نمونه ای از انتقال AAL5

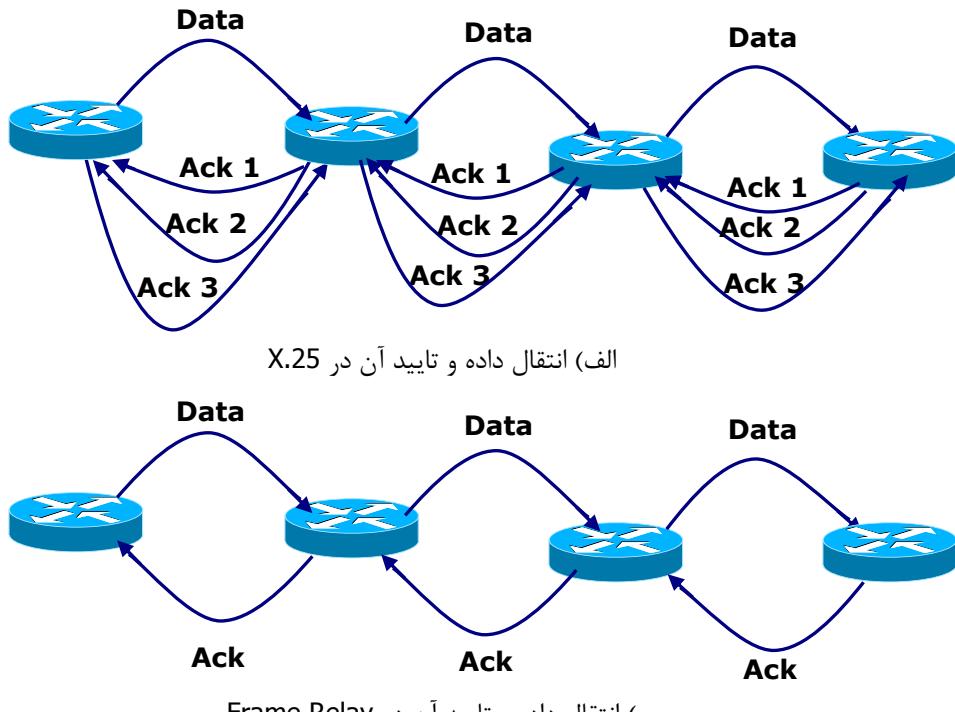
تصویر ۷-۷، نمونه ای از انتقال AAL ۵ را نشان می دهد. CPCS PDU شامل بخش پرشده با بیتهاي غیر ضروری و دنباله، به دسته های ۴۸ بایتی، تقسیم شده است. هر دسته در یک سلول ATM منفرد انتقال می یابد.

Frame Relay :۷-۷

همانند ATM Frame Relay جهت فراهم آوردن انتقال موثرter از طرح X.25. استانداردهای Frame Relay، قبل از ATM کامل شده است و تولیدات تجاری آن نیز زودتر وارد شده اند. بر این اساس، تعداد زیادی از محصولات مبتنی بر Frame Relay نصب شده اند. اکنون تمایلات به سمت ATM شبکه های با سرعت بالا، تغییر نموده است، اما بدلیل اینکه Frame Relay هنوز عمومیت دارد، در این قسمت به بررسی آن می پردازیم.

پس زمینه:

- دید سنتی به سوئیچ بسته ای، کاربرد X.25 را باعث شد که نه تنها رابط کاربر- شبکه را معرفی می نمود، بلکه طراحی داخلی شبکه را نیز تحت تاثیر قرار می داد. چند خاصیت کلیدی طرح X.25 بشرح زیر می باشد:
- بسته های کنترل تماس جهت برپاسازی و خاتمه مدارات مجازی، برروی کانال و مدار مجازی یکسان با بسته های داده، منتقل می شوند، در حقیقت سیگنال دهی در یک باند، مورد استفاده قرار گرفته است.
 - مالتی پلکس مدارات مجازی در لایه ۳ اتفاق می افتد.
 - هر دو لایه ۲ و ۳، مکانیزم های کنترل جریان و خط را شامل می شوند.



تصویر ۷-۱۷: مقایسه مکانیزم انتقال داده و تایید آن در X.25 و Frame Relay

این طرح سربار قابل توجهی را باعث می شد. در هر پرش در شبکه، پروتکل کنترل پیوند داده، تبادل یک فریم داده و یک فریم تایید را شامل می گردد. بعلاوه در هر گره میانی، جداول وضعیت باید برای هر مدار مجازی، حفظ گردد تا جنبه های مدیریت تماس و کنترل جریان و خط را پروتکل X.25 مورد بررسی قرار بگیرد. همه این سربارها ممکن است در زمان وجود یک احتمال خطأ در اتصالات شبکه، توجیه شوند. این طرح ممکن است چندان با امکانات تماس دیجیتال مدرن، مناسب نباشد. شبکه های امروزی از شیوه های انتقال دیجیتال قبل اعتماد بر روی اتصالات با کیفیت و قابلیت اعتماد بالا که اکثر آن فیبر نوری است، استفاده می کنند. بعلاوه با استفاده از فیبر نوری و انتقال دیجیتال، نرخهای داده بالا، قابل دسترس هستند. در چنین محیط هایی، سربار X.25 نه تنها مورد نیاز نیست، بلکه بهره وری موثر از نرخ داده های بالای موجود را نیز کاهش می دهد.

Frame Relay جهت حذف بخش عمده سربار تحويل X.25 بر سیستمهای کاربران نهایی و شبکه های سوئیچ بسته ای، طراحی شده است. تفاوت های عمده بین Frame Relay و سرویس سوئیچ بسته ای X.25 متداول، بشرح زیر است:

- سیگنال دهی کنترل تماس بر روی یک اتصال منطقی جدا از داده کاربر، منتقل می گردد. بنابراین گره های حیاتی نیازمند حفظ جداول وضعیت و یا پردازش پیامهای مرتبط با کنترل تماس بر روی یک اتصال واحد نیستند.

- مالتی پلکس و سوئیچ اتصالات منطقی در لایه ۲، بجای لایه ۳، اتفاق می‌افتد که نتیجه آن حذف پردازش یک لایه کامل است.
- کنترل جریان و کنترل خطاب پوش به پرش، وجود ندارد. کنترل جریان و خطاب انتها به انتهای، اگر مورد استفاده قرار بگیرد، مسئولیت لایه های بالاتر می‌باشد.

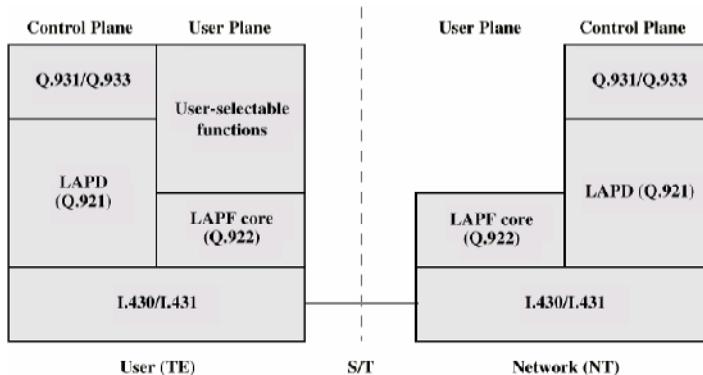
بنابراین با Frame Relay یک فریم داده تنها کاربر از مبدأ به مقصد ارسال می‌گردد و در مقصد، یک تایید در یک لایه بالاتر تولید شده و در یک فریم، بازگردانده می‌شود. تبادل پرش به پرش فریمهای داده و تایید وجود ندارد.

اجازه بدھید نگاهی به مزايا و معایب اين طرح بياندازيم. مهمترین عيب Frame Relay در مقاييسه با X.25 عدم وجود توانايي کنترل جريان و خطاب اتصال به اتصال می باشد(اگرچه Frame Relay کنترل جريان و خطاب انتها را فراهم نمی کند، بر احتی اين امر در يك لایه بالاتر، فراهم می آيد). در X.25 چند مدار مجازی بروی يك اتصال فيزيکي حمل می‌گردد و LAPB در سطح اتصال، برای ايجاد انتقال مطمئن از يك منبع به شبکه سوئیچ بسته ای و از شبکه سوئیچ بسته ای به مقصد، موجود است. بعلاوه، در هر پرش در شبکه، پروتکل کنترل انتقال می‌تواند جهت اطمینان، بکار رود. با استفاده از Frame Relay، کنترل اتصال پرش به پرش از دست می‌رود. اگرچه با افزایش اطمینان انتقال و امکانات سوئیچ، این يك عيب عمدی نیست.

مزیت Frame Relay آنست که ما پردازش اتصال ساده و موثر داریم. توابع مورد نیاز پروتکل در رابط کاربر-شبکه، بدليل پردازش درون شبکه ای، کاهش می‌یابد. بعنوان يك نتیجه، تاخیر کمتر و گذردهی بالاتر را می‌توان انتظار داشت. مطالعات نشانگر بهبود توان عملیاتی، با استفاده از Frame Relay، در مقاييسه با X.25، می‌باشد. توصیه نامه ITU-T I.233 می‌کند که Frame Relay می‌تواند جهت کسب سرعت 2 Mbps، بکار رود.

معماری پروتکل :Frame Relay

تصویر ۱۸-۷، معماری پروتکل Frame Relay را برای پشتیبانی از سرویس حامل حالت فریم را نشان می‌دهد. باید به ۲ طرح مجزا توجه شود. یک طرح کنترل(C) که در برپاسازی و خاتمه اتصالات منطقی، بکار می‌رود و طرح کاربر(U)، که مسئول انتقال داده کاربر بین مشترکین، می‌باشد. بنابراین پروتکلهای طرح C بین یک مشترک و یک شبکه، است و در حالیکه پروتکلهای طرح U، توابع انتها به انتهای را فراهم می‌آورد.



تصویر ۱۸-۷: معماری پروتکل رابط کاربر-شبکه

طرح کنترل:

طرح کنترل برای سرویس حامل حالت فریم همانند سیگنال دهنی کانال عمومی برای سرویسهای سوئیچ مداری، می‌باشد که در آن یک کانال منطقی مجزا برای کنترل اطلاعات کنترلی، بکار می‌رود. در لایه پیوند داده، LAPD (Q.921) جهت ایجاد سرویس کنترل پیوند داده مطمئن، با کنترل خطاب و جریان بین کاربر(TE) و

شبکه (NT) بروی کanal D، مورد استفاده قرار می گیرد. سرویس پیوند داده جهت تبادل پیامهای سیگنال دهی کنترل Q.933 بکار می رود.

طرح کاربر:

برای انتقال واقعی اطلاعات بین کاربران نهایی به پروتکل طرح کاربر، LAPF (روال دسترسی به اتصال برای سرویس‌های حامل حالت فریم) می باشد که در Q.922 تعریف شده است. Q.922 یک نسخه پیشرفته از Q.921 (LAPD) می باشد. تنها توابع مرکزی و هسته Frame Relay برای LAPF مورد استفاده قرار می گیرند.

- تعیین کردن حدود: تنظیم موقعیت و شفافیت فریم.
- مالتی پلکس و عکس مالتی پلکس فریم با استفاده از فیلد آدرس.
- بازرگانی فریم جهت اطمینان از اینکه شامل یک عدد صحیح از بایت‌های اولویت به صفر بیت افزودن و یا صفر بیت استخراج.
- بازرگانی فریم جهت اطمینان از نه خیلی طولانی و نه خیلی کوتاه بودن آن.
- تشخیص خطاهای انتقال.
- توابع کنترل تراکم.

توابع مورد آخر به تازگی به LAPF، افزوده شده اند و سایر توابع نیز توابع LAPD، می باشند.

توابع هسته LAPF، در طرح کاربر تشکیل یک زیرلایه از لایه پیوند داده را می دهد. این یک سرویس حامل انتقال فریم‌های پیوند داده از یک مشترک به دیگری را فراهم می آورد که هیچ کنترل جریان و خطابی را ندارد. در بالای آن، کاربر ممکن است توابع پیوند داده اضافی یا لایه شبکه انتها به انتها را نیز انتخاب نماید. اینها بخشی از سرویس Frame Relay، نیستند. برایه توابع هسته، شبکه Frame Relay، به عنوان سرویس لایه پیوند اتصال گرا، خواص زیر پیشنهاد می دهد:

- پیش رزرو ترتیب انتقال فریم از لبه شبکه به لبه دیگر آن
- احتمال پایین فقدان بسته

Flag	Address	Information	FCS	Flag
<---1--->	<----2-4---->	<-----Variable----->	<----2---->	<---1--->

(a) Frame format

Upper DLCI	C/R	EA 0
Lower DLCI	FECN BECN	DE EA 1

(b) Address field - 2 octets (default)

Upper DLCI	C/R	EA 0
DLCI	FECN BECN	DE EA 0
Lower DLCI or DL-CORE control	D/C	EA 1

(d) Address field - 4 octets

Upper DLCI	C/R	EA 0
DLCI	FECN BECN	DE EA 0
Lower DLCI or DL-CORE control	D/C	EA 1

(c) Address field - 3 octets

EA	Address field extension bit
C/R	Command/response bit
FECN	Forward explicit congestion notification
BECN	Backward explicit congestion notification
DLCI	Data link connection identifier
D/C	DLCI or DL-CORE control indicator
DE	Discard eligibility

LAPF هسته فرمت ۱۹-۷ تصویر

انتقال داده کاربر:

عملکرد Frame Relay برای انتقال داده کاربر، با نگاهی به فرمت فریم آن که در تصویر ۷a-۱۹، تشریح شده است، بهتر شرح داده می‌شود. این فرمتی است که برای حداقل توابع پروتکل LAPF (پروتکل هسته LAPF)، تعريف شده است. فرمت با یک حذف آشکار، شبیه به LAPD و LAPB می‌باشد: فیلد کنترل وجود ندارد. این فرمت مفاهیم زیر را در بر دارد:

- تنها یک نوع فریم، جهت انتقال داده کاربر، وجود دارد و هیچ فریم کنترلی وجود ندارد.
- امکان استفاده از سیگنال دهی در یک مسیر، وجود ندارد و یک اتصال منطقی، تنها داده کاربر را حمل می‌نماید.

توابع فیلدهای بررسی توالی پرچم و فریم، همانند نمونه‌های LAPD و LAPB هستند. فیلد اطلاعات، داده لایه بالاتر را حمل می‌کند. در صورتیکه کاربر قصد پیاده سازی توابع کنترل داده اضافی انتها به انتها را داشته باشد، یک فریم پیوند داده می‌تواند در این فیلد، حمل گردد. بویژه، یک انتخاب عمومی، استفاده از پروتکل کامل LAPF (پروتکل کنترل LAPF)، جهت انجام توابع بالای هسته LAPF، می‌باشد. توجه کنید که پروتکلهای پیاده شده به این شیوه بین مشترکین نهایی، سخت است و برای شبکه‌های Frame Relay نیز شفاف است.

فیلد آدرس، طول ۲ بایتی پیش فرض را دارد، ولی ممکن است به ۳ یا ۴ بایت نیز گسترش یابد. این فیلد، شناسه اتصال پیوند داده (DCLI)، ۱۰ یا ۱۷ یا ۲۴ بیتی را حمل می‌کند. DCLI همان توابع شماره مدار مجازی در X.25 را سرویس می‌دهد و به اتصالات منطقی Frame Relay، امکان مالتی پلکس برروی یک کانال تنها را می‌دهد. همانند X.25، شناسه اتصال تنها ارزش محلی دارد: هر انتهای اتصال منطقی، DCLI خودش را از شماره‌های تخصیص نیافرته محلی منبع، تخصیص می‌دهد و شبکه باید یکی را به دیگری نگاشت کند. راه دیگر، استفاده از DCLI یکسان در هر دو انتهای می‌باشد که نیازمند برخی انواع مدیریت سراسری مقادیر DCLI می‌باشد.

فیلد آدرس و این رو DLCI، بوسیله بیتها امتداد فیلد آدرس مشخص می‌شود. بیت CIR، خاص کاربرد است و بوسیله پروتکل Frame Relay استاندارد، بکار نمی‌رود. بیتها باقیمانده در فیلد آدرس با کنترل تراکم بکار می‌روند.

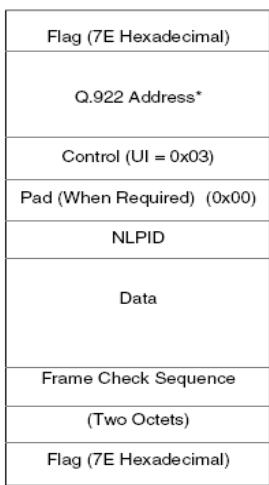
:Frame Relay برروی IP

همه پروتکلهای باید بسته هایشان را در یک فریم ضمیمه Q.922 A، قرار دهند. بعلاوه فریمها شامل اطلاعات کافی جهت تعیین پروتکل حمل شده در PDU می‌باشند، تا دریافت کننده را قادر به انجام پردازش صحیح برروی بسته ورودی نماید. فرمت این امر بصورت زیر خواهد بود:

- فیلد کنترل، فیلد کنترل Q.922 می‌باشد. عمدتاً مقدار UI(0X03) بکار برده می‌شود، مگر آنکه برای مقدار دیگری توافق گردد. استفاده از XID (0XAF یا 0XBF)، مجاز می‌باشد.
- فیلد PAD برای تنظیم بخش داده (فراتر از سرآیند محصورسازی) فریم برای قرار دادن اندازه آن در مضری از ۳۲ بیت، بکار می‌رود. در صورت امکان، PAD یک بایتی با مقدار صفر، خواهد بود.
- فیلد NLPID بوسیله ISO و ITU-T FRAHAM شده است. این فیلد حاوی مقادیری برای پروتکلهای متفاوت بسیاری، شامل CLNP، IP، و پروتکل دستیابی به زیر شبکه (SNAP^۱) IEEE، می‌باشد. این فیلد به دریافت کننده می‌گوید که چه پروتکلی در بسته ها محصور شده است. مقادیر این فیلد در ISO/IEC TR 9577، تعريف شده اند. مقدار 0X00 برای NLPID در ISO/IEC TR 9577، به عنوان یک لایه شبکه تهی یا مجموعه غیرفعال، تعريف شده است. بدلیل عدم تشخیص آن از یک

فیلد PAD و بی معنی بودن آن در زمینه طرح محصورسازی، مقدار 0X00 برای NLPID در محصورسازی Frame Relay نامعتبر می باشد.

بطور عمومی یک اندازه فریم حداقل و یک اندازه فریم حداکثر برای Frame Relay، پیاده سازی شده است. یک شبکه باید حداقل طول ۲۶۲ بایت و حداکثر ۱۶۰۰ بایتی یا بیشتر (متنااسب با تصمیمات تهیه کننده Frame Relay) را پشتیبانی کند. یک DTE باید مجاز به تنظیم اندازه حداکثر طول فریم، باشد.



تصویر ۷-۲۰: فرمت بسته Frame Relay براساس Q.922

دو نوع پایه از بسته های داده منتقل شده در شبکه Frame Relay وجود دارند: بسته های مسیردهی شده^۱ و بسته های پل شده^۲. این بسته ها فرمتهای مجزایی داشته و باید شامل یک شاخص که جهت تفسیر صحیح محتويات فریم در مقصد، مورد استفاده قرار می گیرد، باشد. این شاخص در اطلاعات سرآیند SNAP و NLPID قرار می گیرد.

ایستگاه های Frame Relay ممکن است جهت پشتیبانی از تبادل تعیین هویت (XID^۳) تعریف شده در ضمیمه ۳ Q.922، انتخاب گردند. این تبادل XID، اجازه می دهد تا پارامترهای زیر در ابتدای مقداردهی اولیه مدار Frame Relay، محاوره گردد: اندازه حداکثر طول فریم، زمان سنج انتقال مجدد و حداکثر تعداد فریم های اطلاعات ارائه نشده. اگر این تبادل مورد استفاده قرار نگیرد، این مقادیر باید بصورت ثابت، بوسیله توافق دوجانبه نقاط انتهایی اتصالات پیوند داده (DLC)، پیکربندی گردد و یا باید از مقادیر پیش فرض مشخص شده در بخش ۹-۷ Q.922، استفاده شود.

ایستگاه هایی نیز هستند که می خواهند در مورد یک پروتکل آدرس دهی بروی کانالهای مجازی ثابت(VPC)، بصورت پویا تصمیم گیری کنند. این امر ممکن است بوسیله ARP محصور شده در یک بسته Relay کد شده SNAP، انجام گیرد.

بدلیل ناتوانی شبیه سازی Broadcast در یک محیط Frame Relay، یک نمونه تعیین آدرس تغییر یافته، توسعه یافته است که به آن ARP معکوس می گویند و شیوه ای را برای تصمیم گیری در مورد یک آدرس پروتکل در زمان وجود آدرس فیزیکی، توصیف می نماید. در یک شبکه Frame Relay، آدرس سخت افزار هویدا، DLCI

¹ Routed Packet

² Bridged Packet

³ Exchange Identification

می باشد. پشتیبانی از ARP معکوس نیازمند پیاده سازی این خصوصیت نیست، اما این خصوصیت جهت پیکربندی رابط Frame Relay، مفید است.

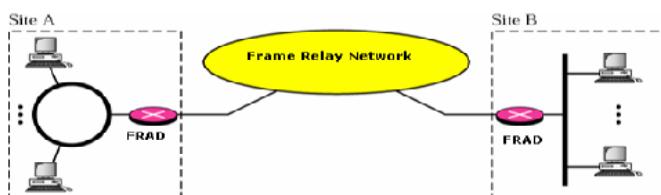
ایستگاه ها باید قادر باشند تا بیش از یک آدرس IP در یک subnet IP یکسان، برای یک DLCI خاص، بروی یک رابط Frame Relay، نگاشت کنند. این نیاز از کاربردهایی همانند یک دستیابی راه دور، ناشی می گردد که سرورها باید همانند پراکسی های ARP برای تعداد زیادی مشتری که به هر کدام از آنها یک آدرس IP یکتا تخصیص یافته است که پنهانی باند را بروی DLC یکسان به اشتراک گذاشته شده است، عمل کنند. طبیعت پویای چنین کاربردهایی نتیجه اش انتساب آدرس تکرارپذیر، بدون تاثیر بر وضعیت DLC، می باشد. داده گرامهای IP جهت انتقال بر روی یک شبکه Frame Relay باید درون فریمهای آن قرار بگیرد. برای این منظور، IP می تواند به دو صورت درون این فریمهها قرار گیرد: مقدار NLPID^۱، نشان دهنده IP و یا مقدار SNAP، نشان دهنده NLPID.

اگرچه هر دوی این محصورسازیها با تعاریف ارائه شده حمایت می شوند، استفاده از هر کدام از این مکانیزمها برای محصورسازی داده های IP، مفید خواهد بود. بنابراین داده IP می تواند با استفاده از مقدار OxCC برای NLPID که نشانگر یک بسته IP می باشد، محصور گردد. این گزینه موثرتر است؛ زیرا این روش بدون سرآیند ۴۸ SNAP بیت کمتر ارسال می کند و با محصورسازی IP در یک شبکه X.25 نیز سازگار می باشد.

ایجاد VPN با Frame Relay

یک شبکه خصوصی مجازی را می تواند ایجاد کند. اگر یک سازمان چند LAN داشته باشد و این شبکه با فواصل زیادی از هم قرار داشته باشد و برای اینکه ظاهرآ یک شبکه به نظر برسد دو راه وجود دارد:

- ۱- از خطوط Leased استفاده کنیم که چندان مفید نیست زیرا همیشه خط را مشغول می کند.
- ۲- راه دوم استفاده از سوئیچینگ بسته ای است. اگر X.25 استفاده کنیم، سریار زیادی ایجاد می شود همچنین سرعت پایین دارد. به همین دلیل از شبکه های Frame Relay برای این منظور استفاده می شود (نرخ انتقال بالایی دارد). این شبکه ها به شدت برای انتقال صوت مفید است زیرا هزینه را پایین می آورد.



تصویر ۷-۲۱: ایجاد VPN به کمک FRAD

^۲: یک نوع مسیریاب است با این تفاوت که مسیریابی انجام نمی شود و بلکه فقط بسته ها را انتقال می دهد.

خلاصه فصل:

یک رابط انتقال بسته ساده و موثر، می باشد. ATM از بسته های با طول ثابت ، به نام سلول، استفاده می نماید. استفاده از طول ثابت و فرمت ثابت ، یک شیوه موثر برای انتقال با سرعت بالا بروی شبکه های می باشد. برخی از ساختارهای انتقال ممکن است برای انتقال سلولهای ATM بکار برود. یک گزینه ، استفاده از جریان پیوسته سلولها، بدون ساختار مالتی پلکس تحمیل شده در رابط، می باشد. همزمانی در یک طرح سلول به سلول،

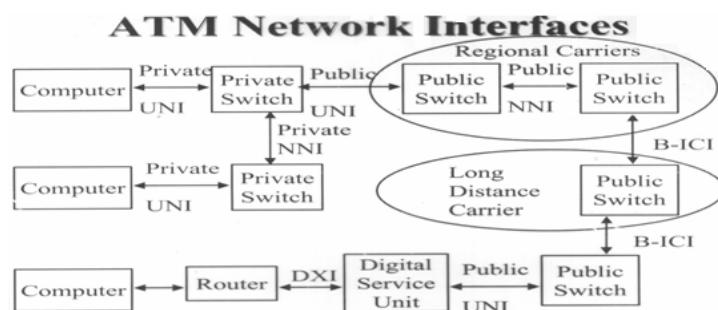
^۱ Network Level Protocol ID -

^۲ Frame Relay Access Device -

اساس کار می باشد. گزینه دوم، قرار دادن سلولها در یک پوشش مالتی پلکس تقسیم زمان همزمان ، می باشد. در این حالت، جریان بیتی در رابط، یک ساختار چهار چوب خارجی بروی طبقات دیجیتال همزمان(SDH)، دارد. ATM هر دو سرویس زمان واقعی و غیر زمان واقعی را فراهم می آورد. یک شبکه مبتنی بر ATM، می تواند دامنه گسترده ای از دامنه ترافیک ، شامل جریانات TDM همزمان همانند T1، با استفاده از سرویسهای با نرخ بیت ثابت(CBR)، صوت و تصویر فشرده شده با استفاده از سرویس نرخ بیت متغیر زمان واقعی(rt-VBR)، ترافیک با نیازمندیهای کیفیت سرویس مشخص، با استفاده از سرویس VBR غیر زمان واقعی(nrt-VBR) و ترافیک مبتنی بر IP، با استفاده از سرویسهای نرخ بیت موجود(ABR) و نرخ بیت نامعین (UBR)، را پشتیبانی نمایند.

استفاده از ATM نیاز به یک لایه تطبیق برای پشتیبانی از پروتکلهای انتقال اطلاعات غیر مبتنی بر ATM را بوجود می آورد. لایه تطبیق AAL(ATM) اطلاعات کاربر را در بسته های ۴۸ بایتی برای قرار دادن در سلولهای ATM بسته بندی می کند. این ممکن است شامل جمع نمودن بیتها از یک جریان بیتی و یا تقسیم یک فریم به قطعات کوچکتر، باشد.

ساختار کلی یک رابط شبکه ATM در تصویر زیر ارائه شده است. در این طرح، اتصالات به دو دسته خصوصی و عمومی تقسیم شده اند. تبادل اطلاعات در دورن شبکه های ATM از نوع خصوصی می باشد ؛ ولی تبادل داده آنها با شبکه های بیرونی، از نوع عمومی می باشد. همچنین در این تصویر رابطهای کاربر-شبکه و شبکه-شبکه، مشخص شده اند.



تصویر ۷-۲۲: طرح رابط شبکه ATM

فصل ۸

MPLS و DiffServ، ISA

اجزا شبکه اینترنت به دو سرویس ^1ISA و ^2DSA (Diffservice) مجهز شده است. اکنون از DSA بیش از ISA استفاده می شود . مشکلی که اینترنت کنونی دارد این است که QoS ندارد . یعنی نمی تواند بر اساس یک کیفیت خاص سرویس دهی کند . کیفیت به پنج عامل تقسیم می شود : تغییرات تاخیر^۳ ، میزان خطا ، گم شدن بسته ، تاخیر ، بازده.

اینکه اینترنت QoS ندارد یعنی نمی توان به پارامترهای فوق اعتماد کرد . مثلاً نمی توان گفت یک سرویس برای ارسال بسته ها با حداقل تأخیر ۱ میلی ثانیه نیاز داریم . ISA ، DSA به منظور ایجاد QoS در اینترنت وجود آمده اند . (DSA جدیدتر است و در حال رشد). البته MPLS را هم می توان برای ایجاد QoS و رزرو کردن منابع (با قابلیت اعتماد) دانست .

:ISA

هدف این است که منابع شبکه را بتوان برای یک ارتباط رزرو کرد . به همین دلیل ISA از یک پروتکل بنام RSV^۴ استفاده می کند. این پروتکل قبل از ارتباط منابع (بافرها ، ظرفیت ها ، ...) را رزرو می کند و به مسیریابها خبر می دهد و این ارتباط را تضمین می کند .

Routing ها هم باید تغییر کنند چون قبل مسیریابی توسط (براساس) مینیمم تأخیر بوده است ولی باید تلاش کرد که Routing هم براساس QoS باشد . مثلاً در یک ارتباط ماهواره ای با اینکه تأخیر زیاد است ولی گذردهی بسیار بالا است ، بر ارتباط زمینی ترجیح داده می شود . یکی از مسائل مورد بحث امروزی Routing است یعنی مسیریابی براساس QoS (حمایت IP بر روی QoS توسط ISA) .

انواع ترافیک :

• انعطاف پذیر^۵ : این نوع ترافیک به گونه ای است که می توانیم پارامترهای QoS را در دامنه وسیعی داشته باشیم . یعنی در محدوده زیادی پارامترهای مختلفی داشته باشیم (delay و گذردهی در جاهای مختلف ، متفاوت باشد) . مثلاً برای Email ، تأخیر یا گذردهی مهم نیست . بطور خلاصه ترافیک انعطاف پذیر حساسیت زیادی نسبت به پارامترهای QoS ندارد یعنی در محدوده وسیعی می توانند تغییر کند (ولی بالاخره یک محدوده دارند) .

• غیر قابل انعطاف^۶ : در این نوع ترافیک ، مجبوریم که پارامترهای QoS را در حد خوبی انتظار داشته باشیم؛ یعنی حداقلها برای تاخیر ، بازده ، تغییرات تاخیر و فقدان بسته وجود داشته باشد . نمونه این ترافیک ، ترافیکهای کاربردهای زمان واقعی می باشد . دستیابی به این نیازمندیها در یک محیط با تغییرات متفاوت تاخیر و فقدان های در اثر تراکم ، مشکل است .

با توجه به ترافیک غیر قابل انعطاف ، دو نیازمندی جدید برای معماری اینترنت ، تعریف گردید . اول آنکه برخی رسانه های انتقال نیازمند رفتارهای امتیازی برای کاربردهای با درخواست نیازمندی بالا ، می باشند . کاربردها باید قادر باشند تا نیازمندیهای خود را بازگو کنند؛ چه نیازمندیهای قبل از زمان وقوع برای برخی توابع درخواست سرویس و چه برای نیازمندیهای زمان اجرا ، بوسیله فیلدهای سرآیند بسته IP .

نیازمندی دوم در پشتیبانی ترافیک غیر قابل انعطاف در یک معماری اینترنت آنست که ترافیک قابل انعطاف باید هنوز پشتیبانی گردد . کاربردهای غیر قابل انعطاف نیازمندیهایشان در اثر تراکم کم نمی شود . بنابراین در زمان تراکم ، ترافیک غیر قابل انعطاف همچنان عملکرد بارگذاری بالای خود را خواهد داشت و ترافیک قابل انعطاف از

Integrated Service Architecture - ^۱
Differentiated Service Architecture - ^۲

Jitter - ^۳

Resource ReSerVation setup Protocol - ^۴

Elastic - ^۵

Inelastic - ^۶

شلوغی خارج می شود. یک پروتکل رزرو می تواند این موقعیت را با رد کردن درخواست سرویس ها کنترل کند. در این حالت برخی منابع جهت مدیریت ترافیک های قابل انعطاف آزاد می گردد.

مسیریابها قبل از اینکه بتوانند ISA را بطور کامل پیاده سازی کنند از دو مکانیزم باید استفاده کنند :

- الگوریتم مسیریابی : اغلب پروتکلهای مسیریابی در حال استفاده در اینترنت به مسیریابهای اجازه

می دهند تا حداقل تاخیر را انتخاب کنند. مسیریابها برای بدست آوردن وضعیت تاخیر در سراسر

اینترنت، اقدام به معاوضه اطلاعات می کنند. مسیریابی حداقل تاخیر به توازن بارگذاری کمک

می کند، بنابراین از تراکم می کاهد و به کاهش تاخیر بین اتصالات مجزای TCP کمک می کند.

- دور ریختن بسته: زمانیکه بافر یک مسیریاب سرریز گردد، مسیریاب بسته ها را دور می ریزد. بسته

های دور ریخته شده از بسته های جدید هستند. تاثیر فقدان بسته در یک اتصال TCP آنست که

فرستنده باید بارگذاری خود را کاهش دهد که این خود به سبک شدن تراکم اینترنت کمک

می کند.

این ابزارها بخوبی جواب می دهند، اما همانطور که قبلًا هم گفته شد این تکنیکها برای انتقالهای متغیر کنونی اینترنت ناکافی هستند. ISA یک معماری سراسری است که در آن مکانیزمهای بهترین تلاش، بهبود یافته اند. در RFC 1633، یک جریان قابل تشخیص از بسته های IP تعریف شده است که بوسیله یک فعالیت یک کاربر ایجاد شده اند و نیازمندیهای QoS یکسان دارند. یک Flow با یک اتصال TCP، در دو مورد متفاوت است: یک طرفه است و می تواند Multicast شود. بعلاوه یک بسته IP، به عنوان عضوی از یک Flow در پایه آدرسهای IP مبدأ و مقصد و شماره پورتها و نوع پروتکل، شناخته می شود. شناسه Flow در IPV6 معادل Flow در ISA نیست اما می تواند در آینده در ISA بکار رود.

توابع عملیاتی در ISA که برای مدیریت تراکم و ایجاد QoS در انتقال مورد استفاده قرار می گیرند عبارتند از:

• کنترل پذیرش^۱ : برای انتقال ISA، QoS نیازمند آنست که عملیات رزرو برای یک Flow جدید، صورت گیرد. اگر مسیریابها مجموعاً به این نتیجه رسیدند که منابع کافی برای تضمین QoS درخواستی وجود ندارد، Flow پذیرش نمی شود. پروتکل RSVP مسئول انجام این رزرو می باشد.

• الگوریتم مسیریابی: تصمیم مسیریابی ممکن است برپایه پارامترهای یک QoS متغیر باشد و تنها بر پایه تاخیر. برای مثال، پروتکل مسیریابی OSPF می تواند مسیرها را برپایه QoS انتخاب کند.

• سیاست صفتگاری^۲ : یک عنصر حیاتی ISA، رویه صفتگاری موثری است تا بتواند نیازمندیهای متفاوت Flow های متفاوت را در نظر بگیرد.

• رویه دور ریختن^۳ : یک رویه صفتگاری مشخص می کند که اگر چند بسته در صفحه خروج از یک پورت هستند، کدام بسته باید منتقل گردد. مطلب مهم دیگر انتخاب و زمان حذف یک بسته است. یک سیاست دور ریختن می تواند عنصر مهمی در مدیریت تراکم و رسیدن به QoS تضمین شده، باشد.

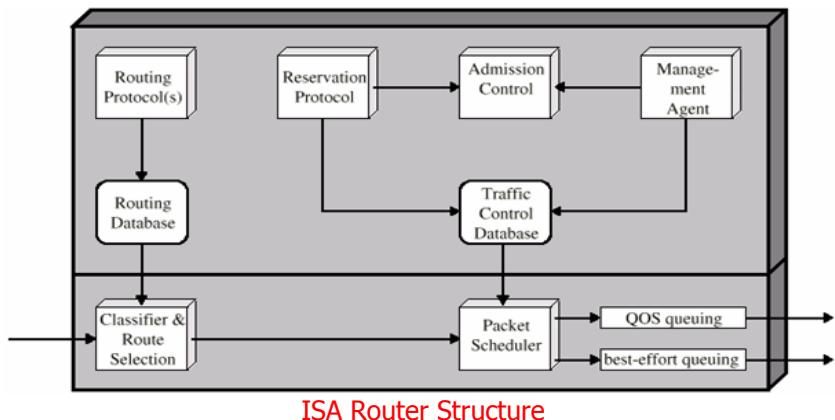
اجزاء ISA

مسیریابی که می خواهد ISA را پیاده سازی کند باید بخش‌های زیر را داشته باشد :

Admission Control - ^۱

Queuing Discipline - ^۲

Discard Policy - ^۳



ISA هسته اصلی پروتکل RSVP می باشد .

همانطور که قبلاً گفته شد ISA اولین تلاش برای دادن QoS به شبکه های کامپیوتری بر اساس اینترنت می باشد . انگیزه این سرویس با استفاده از شبکه Mbone پیدا شد . Multicast یک شبکه Mbone بوده است که ویژه انتقال صوت و ویدئو طراحی شده بود و باعث پیدایش ISA گردید .

شبکه اینترنت به صورت Datagram بوده است و سوئیچ مرکز به ISA یک پیشرفت قابل ملاحظه محسوب می شود .

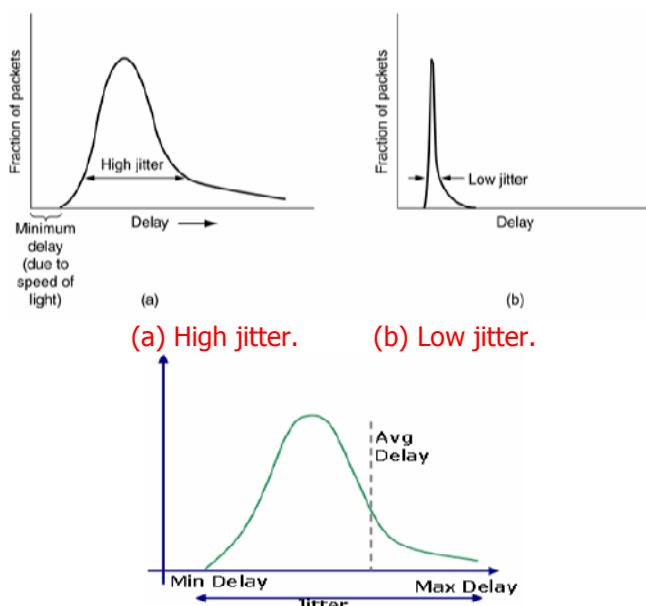
گروههای کاری :

(Integrated Service Over Specific Link Layer) INTSERV -۱

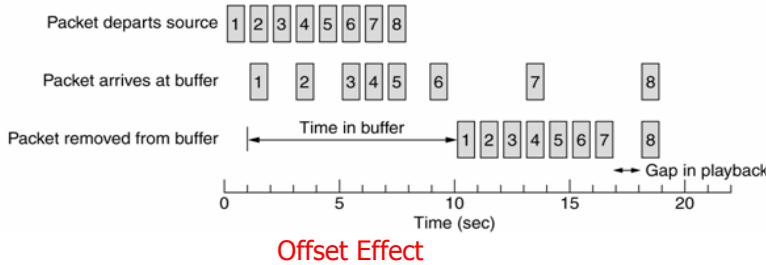
ISSLL -۲

RSVP -۳

یکی از پارامترهای QoS ، تأخیر (Delay) است . کاربردهایی که بصورت زمان واقعی هستند محدودیتی در زمینه تأخیر دارند .

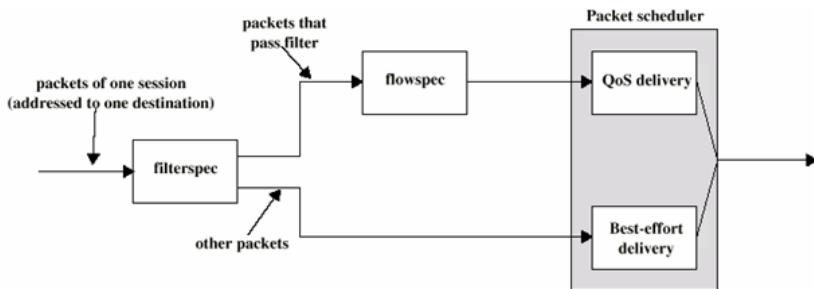


وقتی بسته ها ارسال می شوند (بسته از مبدأ بصورت منظم و با فواصل یکسان ارسال می شوند) ممکن است با همان فاصله بین بسته ها در گیرنده دریافت نشود (به دلیل تأخیر) . برای کارهای Real time می توان یک offset در نظر گرفت و بعد از این offset بسته ها به صورت منظم و پشت سرهم دریافت می شوند . با افزودن بافر هر چند مقداری تأخیر اضافه کرده ایم ولی باعث می شود که کارهای Real time بصورت بهتری انجام شوند . افزودن offset و پشت سرهم کردن بسته ها را می توان با استفاده از بافر پیاده سازی کرد (playout buffer)



Offset Effect

در ISA کاربرد باید مشخصات ترافیکی مورد نیاز خود را مشخص کند. سپس رزرواسیون منابع صورت می‌گیرد. اگر شبکه توانست منابع را برای رسیدن به کارآبی مطلوب رزرو کند انتقال اطلاعات صورت می‌گیرد. بیشترین معیار QoS، تأخیر بسته‌ها می‌باشد.



QoS ISA Router

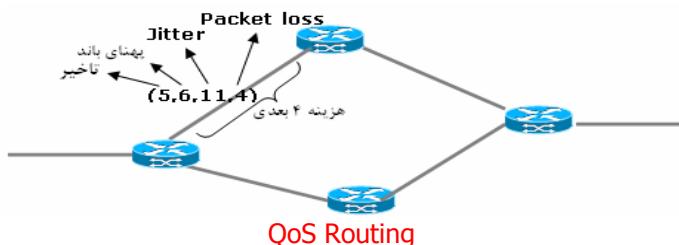
در ابتدا کاربر نیازهای خود را با Flow Identification مشخص می‌کند سپس بعد از بیان نیازها مسیریاب دو کار انجام می‌دهد:

(۱) QoS Routing: پیدا کردن hop بعدی که درخواست رزرواسیون باید ارسال شود.

(۲) کنترل پذیرش: آیا منابع کافی برای این کاربر وجود دارد یا خیر؟

بعد از آنکه عمل رزرواسیون موفق بود اطلاعات برای Flow رزرو شده در جدول رزرواسیون قرار می‌گیرد. زمانی که بسته‌ای می‌آید واحد شناسایی Flow، بسته‌ها را شناسایی می‌کند و نگاه می‌کند که آیا با های رزرو شده مطابقت دارد یا خیر. اگر مطابقت داشته باشد آن را در صف قرار می‌دهد سپس packet scheduler بسته را بعد از اختصاص منابع به Flow ارسال می‌کند.

• QoS Routing (انتخاب مسیر): مسیریابی‌های فعلی بر اساس مینیمم تأخیر در یک منطقه محلی کار می‌کنند و قادر نیستند که بر اساس سایر پارامترهای QoS مسیریابی کنند. مثلاً ممکن است ما مسیری را بخواهیم که پهنای باند آن 25 Mbps باشد. در این صورت مینیمم تأخیر مهم نیست. ممکن است یک مسیر با تأخیر زیاد (لینک ماهواره‌ای) بتواند پهنای 25Mbps را حمایت کند در حالیکه از نظر تأخیر بھی نیست. (یعنی پارامتر پهنای باند از پارامتر تأخیر در لینک ماهواره‌ای مهمتر است)



یعنی هزینه دیگر یک بعدی نیست (مثلاً ۴ بعدی است (5,6,11,4))

مسیریابی درنهایت باید node بعدی را که رزرواسیون در آن باید انجام بگیرد را بدهد.

روشهای ISA به دلیل پیچیدگی QoS Routing از سیستم مسیریابی موجود IP استفاده می‌کنند یا یک سرور مرکزی بدین منظور اختصاص می‌دهند (این کار فقط node بعدی را می‌دهد). این جملات به این معنی

است که پیاده سازی مسیریابی با چند پارامتر عملاً صورت نمی گیرد. بعد از پیدا کردن نود بعدی باید حالت های رزرواسیون در hop بعدی نصب شود . این کار در زیر توضیح داده شده است :

Reservation Setup : باید پروتکلی باشد که از hop به hop بتواند در امتداد یک مسیر حالت های

رزرواسیون را نصب کند . پروتکل همچنین اطلاعاتی درباره مشخصات ترافیک و نیازهای منابع در رابطه با خصوصیات ترافیک و نیازهای منابع باید حمل کند تا مشخص شود که رزرواسیون می تواند صورت گیرد یا خیر . این پروتکل در صورت خراب شدن یک لینک هم باید بتواند کار کند (تغییر توبولوژی) .

رزرو کردن منابع باید شامل مسائل مالی (مادی) هم باشد: Authentication , Authonization , billing . قبل از رزرو کردن منابع باید مشخص شود که چه کسی هزینه این کار را پرداخت خواهد کرد (شناسائی هم مهم است) برای این کار RSVP در نظر گرفته شده است .

به دلیل پیچیدگیهای بسیار زیاد ، ISA در پیاده سازی با شکست مواجه شده است و بیشتر جنبه تحقیقاتی به خود گرفته است (ISA Diffserv جای ISA را گرفته است) .

• کنترل پذیرش: این واحد بررسی می کند تا مشخص کند که آیا منابع کافی برای این فلوی جدید وجود دارد یا خیر . اگر منابع کافی نیستند جلوی ارتباط گرفته می شود . قبل از هر رزرواسیون باید از این تست عبور کرد (قبول یا رد) . بنابراین هم قبول شدن رزرواسیون و هم اندازه گیری منابع جزء این بخش هستند .

اندازه گیری منابع (آیا کافی است یا خیر) در کنترل پذیرش به دو صورت انجام می شود :

۱) براساس پارامتر

۲) براساس اندازه گیری واقعی

-اندازه گیری براساس پارامتر : بر اساس یک مسیری پارامترهایی مشخص می شود و البته پارامترهای واقعی مشکل است زیرا مثلاً در انتقال ویدئو نرخ انتقال براساس محتویات تصویر تغییر می کند . مثلاً اگر با دوربین بخواهیم تصویر یک نفر را ارسال کنیم حرکت کردن سر یا حرکت نکردن سر باعث تغییر محتویات ارسال می شود .

-براساس اندازه گیری واقعی : در این روش شبکه اندازه گیری واقعی انجام می دهد . چند روش برای این کار وجود دارد :

۱. Simplesum : اگر مجموعه پهنای باند برای node های جاری و جدید از ظرفیت لینک بیشتر شود ، منابع کافی نیست و آن را رد می کند .

۲. Measuredsum : بار واقعی (نه پهنای باند خواسته شده) که معمولاً کمتر از پهنای باند است .

۳. Acceptance region : با دادن مدل آماری منابع می توان ناحیه قبول برای یک نوع ترافیک را بدست آورد .

Newestimate = $(1-w) \text{oldestimate} + (w * \text{new measurement})$

w = $0.1+0.1$ (متوسط گیری نمائی)

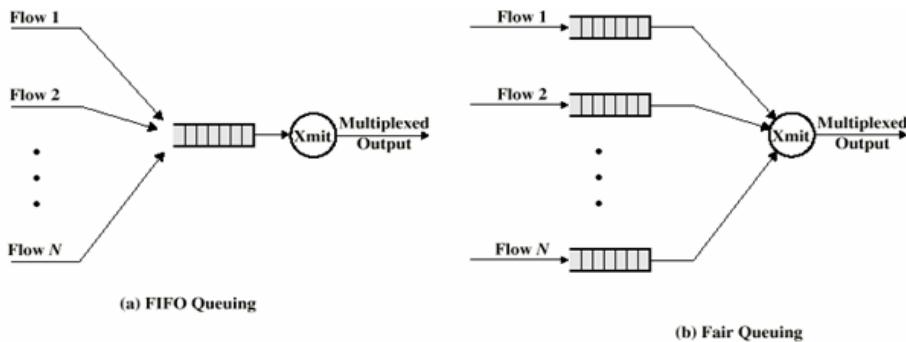
اگر w کم باشد یعنی به تغییرات لحظه ای بهای کمتری داده می شود و به تغییرات قدیمی (که قبلاً به دست آمده) ارزش بیشتری داده می شود (چون ضرب آن $1-w$ است) و اگر w زیاد باشد به تغییرات لحظه ای بهای بیشتری داده می شود .

Flow Identification : هر بسته که وارد مسیریاب می شود باید پردازش شود تا مشخص شود که مربوط به فلوی قدیمی است یا خیر . نوع flow با ۵ فیلد زیر مشخص می شود :

آدرس IP مبدأ ، آدرس IP مقصد ، پروتکل ID (TCP , UDP , ...) ، پورت مقصد ، پورت مبدأ . این فیلدها از بسته ها استخراج می شوند و بررسی می شود که آیا قبلاً هم FLOW هایی با این مشخصات وجود داشته است یا خیر . میلیونها FLOW می تواند در مسیریاب وجود داشته باشد .

باید در محدوده زمانی بسیار محدودی صورت گیرد . بعضی ها برای این کار روش‌های سخت افزاری را پیشنهاد کرده اند (مثل CAM) .

Packet Scheduling : ارسال یا دور ریختن بسته در این واحد انجام می گیرد . دور ریختن یعنی اینکه نتوان منابع را رزرو کرد . برای هر خروجی میتوان یک صف داشت یا کلاً برای خروجی می توان یک صف داشت . روش FCFS برای این کار چندان مناسب نیست زیرا ممکن است یک بسته بزرگ بخواهد رد شود و تا ارسال کامل آن ، جلوی بسته های دیگر گرفته می شود و کاربردهایی که با تأخیر برستند و یا اولویت بالاتری دارند سرویس سریعتر نمی گیرند . این دو اشکال، استفاده از این روش را کمتر کرده است (FIFO).(Queuing)



به همین دلیل به جای استفاده از یک صف برای تمام خروجیها می توان برای هر خروجی یک صف در نظر گرفت . این روش Fair Queuing نامیده می شود . البته در این روش هم ممکن است بسته بزرگ وجود داشته باشد و مشکلات روش اول به تعداد کمی وجود داشته باشد .

روش مناسبی که استفاده می شود Waiting Fair Queuing است (WFQ) در این روش خطی که شلوغتر است سرویس بیشتری می گیرد بدون آنکه برای دیگران مزاحمتی ایجاد کند (این بسته بین بسته های دیگر ارسال می شود) .

Packet scheduling یعنی اینکه بسته ها چگونه انتقال داده شود .

1-DiffServ

متدهای ISA و RSVP جهت حمایت از QoS در اینترنت و شبکه های خصوصی، مورد توجه هستند. اگرچه ISA بصورت عمومی و RSVP بصورت خاص، ابزارهای مفیدی در این زمینه هستند، اما دارای پیچیدگی زیادی برای پیاده سازی می باشند. بعلاوه آنها امکان مقایسه پذیری خوب جهت مدیریت حجم عظیم ترافیک ، بدليل وجود سیگنالهای کنترلی مورد نیاز زیاد جهت هماهنگ سازی QoS یکپارچه پیشنهادی را بدليل نیاز به حفظ اطلاعات وضعیت در مسیریابها، را ندارد.

همزمان با رشد اینترنت، کاربردهای مختلف نیز رشد کرده و این موضوع، یک نیاز فوری برای ایجاد لایه های متفاوت QoS برای Flow های ترافیکی مختلف، بوجود آورد. معماری DiffServ (RFC 2475) جهت ایجاد یک پیاده سازی راحت و آسان، با سریار ابزاری کم برای پشتیبانی از سرویس های شبکه با اجراهای پایه متفاوت، طراحی گردید.

ویژگیهای کلیدی DiffServ جهت کارایی و توسعه آسان، عبارتند از:

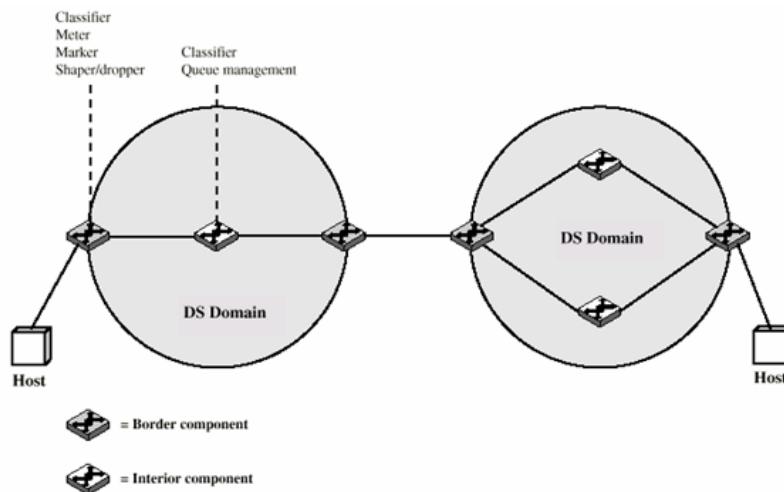
• بسته های IP جهت QoS مورد نیاز در انواع سرویس موجود در IPv4 و یا کلاس ترافیک IPv6، برچسب گذاری می شوند و نیازی به تغییر IP نیست.

¹ Differentiated Services –

- یک توافق سطح سرویس(SLA) بین تهیه کننده سرویس (دامنه اینترنت) و مشتری همانند قبل برای استفاده از DiffServ، ایجاد می گردد. به این ترتیب نیازی به یکی کردن مکانیزم DiffServ با کاربردها نیست. بنابراین کاربردهای موجود برای استفاده از DiffServ نیازی به تغییر ندارند.
 - DiffServ یک مکانیزم توافق درونی را تهیه می کند. سرویسهای شبکه با همه ترافیکها با مقدار DiffServ یکسان، رفتار مشابه دارند. برای مثال اتصالات چندگانه صوت نه بصورت جدا، بلکه بصورت تجمعی، مدیریت می گردند. این امر زمینه مقیاس پذیری خوبی جهت شبکه ها و بارگذاری ترافیکهای بزرگ ، وجود می آورد.
 - DiffServ در مسیریابهای متفاوت بوسیله صفت بندی و ارسال بسته ها بر اساس مقدار DiffServ پیاده سازی می گردد. مسیریابها با هر بسته بصورت جداگانه برخورد می کنند و مجبور نیستند اطلاعات وضعیت روی بسته های Flow را ذخیره کنند.
 - نوع سرویس DiffServ بوسیله دامنه DiffServ، مشخص می گردد که به عنوان بخش پیوسته ای از اینترنت مطرح می شود که در آن سیاستهای DiffServ ثابتی مدیریت می شود. یک دامنه DiffServ تحت کنترل یک موجودیت مدیر می باشد. سرویسهای ایجاد شده در دامنه DiffServ، در یک توافق سطح سرویس(SLA) که یک سرویس قراردادی بین یک مشتری و یک تهیه کننده سرویس می باشد که سرویسهای ارسال را که کاربر باید جهت بسته های کلاسهای متفاوت دریافت نماید را مشخص می نماید، معرفی شده اند.
 - یک مشتری ممکن است یک سازمان کاربر و یا یک دامنه DiffServ دیگر باشد. زمانیکه SLA ایجاد گردید، مشتری بسته ها را با علامت گذاری می کند تا کلاس بسته مشخص گردد. تهیه کننده سرویس باید اطمینان دهد که مشتری حداقل QoS موردن توافق برای بسته های هر کلاس را می گیرد. برای ایجاد آن QoS، تهیه کننده سرویس باید سیاستهای ارسال مقتضی را در هر مسیریاب، بر اساس مقدار DiffServ، پیاده سازی نماید و باید کارایی ایجاد شده برای هر کلاس را بطور مداوم، اندازه گیری نماید.
 - اگر یک مشتری بسته هایی را برای مقصودی در دامنه همان DiffServ، ارائه دهد، انتظار می رود سرویس موردن توافق را ارائه دهد. اگر مقصد در خارج از دامنه DiffServ مشتری باشد، دامنه DiffServ سعی در انتقال بسته ها از طریق سایر دامنه های DiffServ بی که می توانند سرویس های مقتضی و مناسب با سرویس درخواستی را ارائه دهند، می نماید.
- براساس RFC 1812، نیازمندیهای مسیریابهای IPv4، نیازمندیهای لازم برای ایجاد سیاست صفحه گذاری به دو دسته تقسیم می شوند:
- سرویس صفحه:
 - مسیریابها باید سرویسهای صفحه برپایه تقدم را ایجاد نمایند. سرویس صفحه برپایه تقدم به معنی این است که در زمانیکه یک بسته جهت انتقال به خروجی در یک پیوند (منطقی) انتخاب شد، بسته با تقدم بالاتر در صفحه تقدم، ارسال گردد.
 - هر مسیریابی ممکن است سایر روالهای مدیریت گذردگی برپایه سیاست را نیز پیاده سازی نماید تا سیاست تقدم سختگیرانه تری را بوجود آورند، اما باید قادر باشند تا این سیاستها را گاهی کنار بگذارند.
 - کنترل تراکم؛ زمانیکه یک مسیریاب بیش از اندازه ظرفیت خود بسته ورودی دریافت کند ، باید بخشی از بسته ها را دور ببریزد.
 - یک مسیریاب ممکن است بسته ای را که به تازگی دریافت کرده دور ببریزد؛ این آسان ترین و نه بهترین سیاست می باشد.

- بصورت ایده آل، مسیریاب بسته را باید از نشستی انتخاب کند که براساس اجازه های داده شده از سوی سیاست QoS بصورت شدیدی با پیوند بدرفتاری می کند. یکی از سیاستهای توصیه شده در محیطهای Datagram، استفاده از صف FIFO و دور ریختن بسته های انتخاب شده بصورت اتفاقی، از صف می باشد. یک الگوریتم معادل در مسیریابها، استفاده از صفحهای عدالت (Fair) است که در آن دور ریختن از صفحهای طولیتر انجام می شود. یک مسیریاب ممکن است از این سیاستها، برای تعیین بسته ای که باید دور ریخته شود، استفاده کند.
- اگر سرویس صف برپایه اولویت پیاده سازی و فعال گردید، مسیریاب باید بسته هایی را که اولویت بالاتری نسبت به سایر بسته ها دارد، دور بریزد.
- یک مسیریاب ممکن است بسته هایی را که سرآیند آنها نیازمندی به حداقل TOS را اعلام می کند، برخلاف قانون بالا حفظ نماید.
- یک مسیریاب ممکن است از بسته های تکه شده محافظت نماید، زیرا در تصوری، حذف یک قطعه می تواند بدلیل نیاز به ارسال مجدد همه قطعات توسط مبدأ، باعث ایجاد تراکم گردد.
- جهت کمک به جلوگیری از آشفتگی و یا قطع تابع مدیریت، یک مسیریاب ممکن است بسته های استفاده شده برای کنترل مسیریابی، کنترل پیوند و یا مدیریت شبکه، را دربرابر دور ریختن، محافظت نماید. مسیریابهای اختصاصی (همانند مسیریابهایی که میزبانهای همه منظوره نیستند، سرورهای پایانه و ...)، می توانند یک دستیابی نزدیک به این قانون را بوسیله حفاظت از بسته هایی که مبدأ و یا مقصدشان خود مسیریاب است، داشته باشند.

ساختار دامنه های DiffServ در تصویر زیر نمایش داده شده است:



یک DiffServ، مجموعه ای از مسیریابهای متوالی می باشد. به این ترتیب امکان اتصال هر مسیریاب داخل دامنه با سایر مسیریابهای دامنه بدون نیاز به مسیرهایی با مسیریابهای خارج از دامنه، فراهم می گردد. در یک دامنه، تفسیر کد DiffServ یکسان می باشد؛ بنابراین سرویس فراهم شده در تمام مسیریابهای یک دامنه، یکسان خواهد بود.

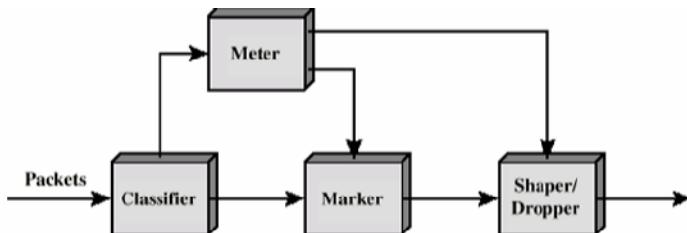
مسیریابها در یک دامنه DiffServ، یا گره های مرزی می باشند و یا گره های درونی. گره های داخلی مکانیزم ساده تری تنها برپایه مقدار DiffServ. جهت مدیریت بسته ها (سیاستهای صف گذاری و دور ریختن بسته

ها) دارند. خصوصیات DiffServ در برخورد با ارسال بسته در یک مسیریاب به عنوان رفتار در هر پرش (¹PHB) مطرح است. این PHB، باید در همه مسیریابها وجود داشته باشد و مخصوصاً PHB تنها بخشی از DiffServ است که در مسیریابهای درونی، پیاده سازی می‌گردد.

مسیریابهای مرزی نیز مکانیزم PHB را دارند، اما مکانیزم‌های شرایط پیچیده تر ترافیکی لازم است تا سرویس‌های مورد نیاز، فراهم گردد. بنابراین مسیریابهای درونی تابعیت و سربارکمتری برای فراهم آوردن سرویس‌های DiffServ، دارند و این در حالیست که اکثر پیچیدگی بر روی مسیریابهای مرزی می‌باشد. تابع یک گره مرزی نیز می‌تواند از طرف کاربردهای سیستم میزبان، بوسیله سیستم میزبان متصل به دامنه، فراهم گردد. تابع شرایط ترافیکی شامل ۵ عنصر می‌باشد:

- طبقه بندی کننده^۲: طبقه بندی کننده، جداکننده بسته‌ها به کلاس‌های مختلف. طبقه بندی کردن، پایه ایجاد سرویس‌های متفاوت می‌باشد. یک طبقه بندی کننده ممکن است تنها ترافیک‌های مختلف را برپایه مقدار DiffServ جدا کند (رفتار طبقه بندی کننده متراکم) و یا براساس چندین فیلد در سرآیند بسته و یا حتی قسمت داده بسته، عمل کند (طبقه بندی کننده چند فیلدی).
 - پیمانه^۳: پیمانه وظیفه اندازه گیری ترافیک برای پیروی از یک پروفایل را دارد. پیمانه تعیین می‌نماید که آیا یک کلاس جریان بسته رسیده در سطح تضمین شده برای سطح سرویس آن کلاس است و یا از آن تجاوز کرده است.
 - نشانه گذار^۴: نشانه گذار وظیفه نشانه گذاری مجدد بسته‌ها را با مقادیر DiffServ جدید بر حسب نیاز، به عهده دارد. این امر ممکن است برای بسته‌های اتفاق بیافتد که از پروفایل خود تجاوز نموده‌اند. برای مثال، برای یک گذردهی تضمین شده برای کلاس سرویس معین، هر بسته‌ای در آن کلاس که از گذردهی در بازه‌های زمانی مشخص، تجاوز کند، ممکن است جهت مدیریت بهترین تلاش، دوباره نشانه گذاری گردد.
 - همچنین نشانه گذاری مجدد در مرزهای بین دو دامنه DiffServ، مورد نیاز باشد. برای مثال، اگر یک کلاس ترافیکی با اولویت پشتیبانی بالا دریافت شود و مقدار آن در یکی ۳ و در دامنه بعدی ۷ باشد، بسته‌ها در دامنه اول با اولویت ۳ منتقل شده و در زمان ورود به دامنه بعدی، مجددًا با مقدار اولویت ۷ شماره گذاری می‌شوند.
 - هشیار^۵: سیاست ترافیکی که بوسیله به تاخیر انداختن بسته‌ها، در صورت لزوم، زمینه جلوگیری از تخطی جریان یک کلاس خاص از نرخ ترافیکی مشخص شده در پروفایل آن را فراهم می‌آورد.
 - دور انداز^۶: وظیفه دور انداختن بسته‌ها در زمانیکه نرخ ترافیک بسته‌های یک کلاس خاص از معین شده در پروفایلش، تجاوز کرد را دارد.
- تصویر زیر رابطه بین این ۵ عنصر را نشان می‌دهد.

Per-Hop Behavior - ^۱
Classifier - ^۲
Meter - ^۳
Marker - ^۴
Sharper - ^۵
Dropper - ^۶



پس از طبقه بندی یک جریان، حجم مصرف منابع آن باید محاسبه گردد.تابع سنجش حجم بسته را در بازه زمانی مشخص، جهت تعیین اجابت یک جریان با توقوفات ترافیکی، اندازه گیری می کند. در صورت پرترافیک بودن میزبان، یک نرخ داده و یا نرخ بسته ساده، ممکن نیست بتواند خصایص ترافیکی مورد نیاز را برآورده نماید. اگر یک جریان ترافیکی از پروفایل خودش تجاوز نمود، چندین حالت ممکن است اتفاق بیافتد. بسته های جداگانه در تخطی از پروفایلشان ممکن است جهت مدیریت کیفیت پایینتر و یافتن اجازه انتقال در دامنه DiffServ، مجدداً نشانه گذاری شود. یک مسیریاب هشیار ترافیکی ممکن است بسته های فراوان رسیده را در یک بافر ذخیره کند و بعداً به تدریج در بازه های زمانی طولانی تر آنها را ارسال می کند. یک دوراندار، اگر بافر انتقال تاخیری پر شود، ممکن است بسته ها را دور ببریزد.

:¹MPLS

استاندارد MPLS نشانگر تلاشهای جاری در زمینه تکامل سوئیچ لایه ای می باشد. هدف اولیه MPLS ترکیب کردن نمونه های تعویض برچسب² با مسیردهی های متداول لایه شبکه های می باشد. این ترکیب زمینه ساز کارایی بهتر در زمینه انتقال داده ها و قراردادن توابع پیشرفته QoS در شبکه می باشد. نمونه های اصلی MPLS برروی IPv4 تمرکز کرده اند، اما هسته این فناوری برای سایر پروتکلهای لایه شبکه نیز قابل توسعه می باشد. همچنین MPLS امروزه تنها محدود به فناوریهای خاص لایه پیوند نمی باشد و می تواند برروی هر محیطی که بسته های لایه شبکه می توانند برروی آن عبور نمایند، عمل نماید. خواص پایه MPLS در RFC 3031 قرار دارد.

:MPLS بر مرواری

در یک محیط MPLS، مسیردهی متداول لایه ۳ یا شبکه (مسیردهی IP)، مسیر در طول شبکه را مشخص می نماید. زمانیکه مسیر مشخص شد، بسته های داده از طریق گره های شبکه در طول شبکه منتقل می گردد. در یک شبکه بدون اتصال متداول، هر مسیریاب یک الگوریتم مسیریابی لایه ۳ را اجرا می کند. همزمان با عبور بسته در شبکه، هر مسیریاب تصمیم گیری مستقلی را برای ارسال بسته اعمال می نماید. با استفاده از اطلاعات موجود در سرآیند بسته و اطلاعات بدست آمده از الگوریتم مسیریابی، مسیریاب مقصد بعدی تحويل بسته را مشخص می نماید. در یک شبکه در یک شبکه IP، این فرایند شامل تطبیق آدرس مقصد ذخیره شده در سرآیند IP برای هر بسته با مسیرهای مشخص در جدول مسیریابی IP می باشد. این فرایند مقایسه، مقصد پرش بعدی بسته را مشخص می نماید. این تجزیه و تحلیل و دسته بندی، می تواند شدیداً نیازمند CPU باشد. در محیطهای متداول بدون اتصال، این فرایند در هر گره میانی در بین دو گره پایانی اتفاق می افتد.

:MPLS انتقال مدل

¹ Multiprotocol Label Switching -
² Label swapping -

در یک محیط MPLS، مسیر بهینه در طول شبکه بصورت پیشرفته مشخص می‌گردد. سپس با ورود بسته به شبکه MPLS، روتراهای مرز ورود با استفاده از اطلاعات سرآیند لایه ۳، جهت تخصیص یکی از مسیرهای مشخص به بسته‌ها استفاده می‌نماید. این تخصیص برای افزودن یک برجسب ارجاعی به مسیر انتها به بسته، بکار می‌رود. این برجسب به بسته داده در طول انتقال آن در شبکه پیوند می‌خورد. سایر مسیریابهای میانی مسیر از اطلاعات برجسب برای مشخص کردن مقصود پرش بعدی استفاده می‌نماید. بدلیل آنکه این مسیریابها تنها با اطلاعات برجسب کار می‌کنند، تجزیه و تحلیل‌ها و کلاس‌بندیهای پر CPU در سرآیند لایه ۳ تنها در نقاط ورودی اتفاق می‌افتد.

جدا از کاهش نیازمندی به پردازش در هسته شبکه، MPLS مزیتهای دیگری را نیز بر مسیردهی‌های متداول لایه ۳ دارد:

۱- مهندسی ترافیک^۱: مهندسی ترافیک فرایند انتخاب مسیرهای شبکه، بگونه‌ای که بهره برداری از تمام منابع شبکه با استفاده از الگوهای ترافیکی حاصل، به یک اندازه باشد.

مسیریابی بر پایه الگوریتمهای IGP متداول می‌تواند باعث انتخاب مسیری در شبکه گردد که بهره برداری نامتوازن از ابزارهای شبکه را باعث می‌گردد. در این محیط‌ها، برخی از ابزارهای شبکه بیش از حد بارگذاری دارند و در حالیکه برخی دیگر زیر حد بهره وری قرار دارند. یک حد پایین مهندسی می‌تواند با دستکاری معیارهای IGP مربوط با پیوندهای شبکه، فراهم آید. اگرچه این تلاش برای مدیریت در محیط‌های با تعداد بالای مسیرهای زائد، مشکل می‌باشد.

برای کسب مزایای مهندسی ترافیک، MPLS می‌تواند به همراه الگوریتمهای IGP مورد استفاده قرار بگیرد. استاندارد MPLS می‌تواند توانایی مسیرهای مشخص برای مسیردهی و عبور بسته‌های داده در شبکه را مشخص نماید. این مسیردهی صریح بسته‌های داده اطمینان می‌دهد که یک جریان مشخص از داده از مسیر مشخص شده استفاده می‌نماید. با نظرات و مدیریت این جریانات داده، بهره برداری موثر از منابع شبکه قابل حصول می‌باشد. مسیردهی صریح از طریق گزینه‌های مسیردهی مبداء در مسیریابی IP متداول، حاصل می‌گردد. با وجود این، به دلیل مصرف CPU بالا در این فرایند، استفاده از آن محدود است. با استفاده از MPLS استفاده موثر از مسیردهی صریح ممکن می‌گردد.

همچنین MPLS توانایی تجزیه و تحلیل فیلدهای خارج از سرآیند بسته IP را در زمان تعیین مسیر صریح برای بسته داده فراهم می‌آورد. برای مثال، مدیر شبکه می‌تواند سیاستهای جریان ترافیک را برپایه مکان و زمان ورود بسته به شبکه تعیین کند. در شبکه‌های مرسوم، این اطلاعات تیها در مبادی ورودی در دسترس می‌باشند. تجزیه و تحلیل اضافی زمینه ساز مدیریت با کنترل بالاتر و در نتیجه سطوح سرویس قابل پیش‌بینی بهتر می‌گردد.

۲- کیفیت سرویس مسیردهی: کیفیت سرویس مسیردهی، توانایی انتخاب یک مسیر برای یک جریان داده مشخص می‌باشد تا مسیر سطح سرویس مورد تقاضا را براورده نماید. این سطوح سرویس می‌توانند سطوح قابل قبول در پهنهای باند، تاخیر و یا فقدان بسته را در شبکه فراهم آورند. این امر زمینه ساز هوشمندی در ارائه سطوح متفاوت در سرویسها برپایه سیاستهای کلی شبکه، می‌باشد.

فراهم آوردن یک مسیر شبکه برای ارائه یک QoS مورد تقاضا، اغلب نیازمند استفاده از مسیردهی صریح می‌باشد. برای مثال، تخصیص یک مسیر برای یک جریان نیازمند تخصیص پهنهای باند خاص، سرراست می‌باشد. اگرچه، این احتمال وجود دارد که ترکیب پهنهای باند چند جریان از ظرفیت مسیر موجود بیشتر گردد. در این حالت، جریانات مستقل، حتی موارد با مبادی ورودی و خروجی یکسان، ممکن است نیازمند مسیردهی جداگانه گردد. این امر نیازمند سطح دانه بندی کوچکتر^۲ می‌باشد که توسط استاندارد مهندسی ترافیک، فراهم می‌گردد.

Traffic Engineering – ^۱
finer level of granularity – ^۲

- در زمینه فراهم آوردن کیفیت سرویس مسیردهی در یک محیط MPLS دو دیدگاه وجود دارد:
- برچسب MPLS شامل کلاس سرویس (CoS) اطلاعات باشد. با جریان یافتن ترافیک در شبکه، این اطلاعات می‌تواند برای اولویت بندی هوشمند ترافیک در هر گره شبکه بکار رود.
 - شبکه MPLS می‌تواند چندین مسیر بین نقاط ابتدایی و انتهایی پیش‌بینی کند. هر مسیر برای حصول سطوح مختلف سرویس مورد ارزیابی و مهندسی قرار می‌گیرد.

این دیدگاه بسادگی بسته‌ها را به یک کلاس از طبقه بندی سرویس دسته بندی می‌کند. سیاستهای مدیریت محلی شبکه تعیین کننده سرویسهای فراهم شده برای هر طبقه می‌باشد.

۳- پشتیبانی از چند پروتکلی: استاندارد MPLS پشتیبانی از پروتکلهای لایه شبکه موجود، همانند AppleTalk، IPX، IPV6، IPV4، Token-Ring، ATM، FDDI و پیوندهای Point to Point را فراهم می‌آورد. فعالیتها در جریان است تا این پشتیبانی، سایر انواع شبکه و پروتکل را نیز در برگیرد.

اجزای یک شبکه MPLS:

در این بخش مفاهیم کلیدی و لغت شناسی یک محیط MPLS ارائه می‌گردد.

لغت شناسی:

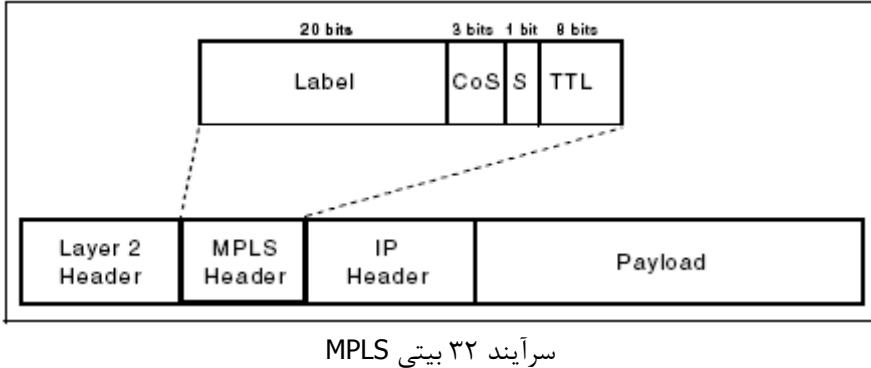
- کلاس هم ارزی ارسال (FEC^۱): یک FEC گروهیست از بسته‌های لایه ۳ که بصورت مشابه انتقال می‌یابند. همه بسته‌ها در این گروه از مسیر یکسانی در شبکه منتقل می‌شوند و اولویت یکسانی دارند. بسته‌های FEC ممکن است اطلاعات سرآیند لایه ۳ متفاوتی را داشته باشند. اگرچه، برای ساده سازی تصمیم در مورد انتقال، بن بسته‌ها از هم جدا نمی‌شوند. نمونه‌های رایج FEC عبارتند از:
 - مجموعه‌ای از بسته‌ها که مسیر مشخص یکسانی را در جدول مسیردهی IP دارند.
 - مجموعه‌ای از بسته‌ها که مسیر مشخص یکسانی را در جدول مسیردهی IP و تنظیمات نوع سرویس یکسانی در سرآیند IP دارند.

در شبکه MPLS، یک FEC توسط یک برچسب مشخص می‌گردد.

- برچسب و بسته‌های برچسب خورده: براساس آنچه در بالا ذکر گردید، یک برچسب، یک FEC واحد را مشخص می‌نماید. یک برچسب بصورت محلی بین ۲ ابزار MPLS ارزشمند می‌باشد. این برچسب می‌بین یک توافق بین ۲ ابزار می‌باشد که توصیف کننده نگاشت بین یک برچسب و یک FEC می‌باشد. این حقیقت که برچسبها بصورت محلی دارای ارزشند زمینه ساز گسترش مقیاس پذیری MPLS در محیط‌های بزرگ گردیده است؛ زیرا نیازی به استفاده از برچسب مشابه در پرش وجود ندارد. برچسب MPLS می‌تواند متناسب با فناوری لایه ۲ مورد استفاده، در موقعیتهای گوناگون فریم داده قرار گیرد. اگر فناوری لایه ۲ از فیلد برچسب پشتیبانی نماید، برچسب MPLS در این فیلد قرار می‌گیرد. در یک شبکه ATM، فیلدهای VPI/VCI می‌توانند جهت ذخیره برچسب MPLS ذخیره بکار روند. در شبکه‌های Frame Relay نیز فیلد DLCI می‌تواند به این منظور مورد استفاده قرار گیرد.

^۱ Forwarding equivalency class –

اگر فناوری لایه ۲ بصورت دورنی برچسب را مورد پشتیبانی قرار ندهد، برچسب MPLS در یک سرآیند گسترش یافته به این منظور قرار می‌گیرد. این سرآیند بین سرآیند لایه ۲ و سرآیند IP قرار می‌گیرد. به این ترتیب امکان استفاده از سرویس MPLS بر روی هر فناوری لایه ۲ ای فراهم می‌گردد.



محتويات سرآیند MPLS عبارتند از:

- یک فیلد برچسب شامل مقدار واقعی برچسب MPLS.
- یک فیلد CoS که می‌تواند برای تاثیر گذاری بر سیاستهای صفت‌گذاری و دور ریختن در شبکه ای که بسته در حال عبور از آن می‌باشد، بکار رود.
- یک فیلد S (پشته) که می‌تواند یک پشته برچسب سلسله مراتبی^۱ را حمایت کند.
- یک فیلد TTL^۲ که IP مرسوم را پشتیبانی می‌نماید.

یک بسته برچسب دار در بسته ای ذخیره می‌گردد که برچسب رمز شده دارد. برای پشتیبانی از توابع پیشرفتی MPLS، بسته ممکن است واقعاً بیش از یک برچسب داشت باشد. به این وضعیت پشته برچسب می‌گویند. پشته یک رابطه ترتیب یافته بین برچسب‌های مجرزا را ایجاد می‌نماید. پشته بصورت LIFO مدل شده است. این ویژگی بعداً در بخش "پشته برچسب و سلسه مراتب برچسب" مورد بحث قرار می‌گیرد.

مسیریاب پشته برچسب(LSR)^۳: یک مسیریاب برچسب پشته، یک گره MPLS است که علاوه بر آن قابلیت انتقال بسته‌های لایه ۳ خود را نیز دارد. ۲ نوع مهم LSR در یک شبکه MPLS وجود دارد:

- گره Ingress متصل کننده شبکه MPLS با گره فاقد توانایی اجرای توابع MPLS. این گره وظیفه مدیریت ترافیک ورودی به شبکه MPLS را دارد.
- گره Egress متصل کننده شبکه MPLS با گره فاقد توانایی اجرای توابع MPLS. این گره وظیفه مدیریت ترافیک خروجی از شبکه MPLS را دارد.

مدخل برچسب ارسال پرش بعدی(NHLFE)^۱: یک NHLFE بوسیله یک گره MPLS، جهت انتقال بسته‌ها بکار می‌رود. حداقل برای هر FEC منتقل شده توسط گره، یک NHLFE وجود دارد. هر گره وظیفه نکهدارنده اطلاعات یک NHLFE را برپایه اطلاعات زیر دارد:

hierarchical label stack – ^۱

time-to-live – ^۲

Label stack router – ^۳

- آدرس پرش بعدی بسته
- عملیات انجام شده برروی پسته
 - جانشین سازی برچسب بالای پسته با برچسب جدید
 - برداشتن برچسب قدیمی از بالای پسته
 - جانشین کرده برچسب بالای پسته با برچسب با مقدار جدید خاص و انتقال یک یا چند برچسب خاص به پسته برچسب. با خاتمه این فرایند، پسته حداقل شامل ۲ برچسب MPLS می باشد.

- محصورسازی پیوند داده^۲ مورد استفاده برای انتقال بسته(اختیاری)
- رمزگذاری پسته داده مورد استفاده جهت انتقال بسته (اختیاری)
- هر داده مورد لزوم دیگر جهت پردازش صحیح بسته.

نگاشت برچسب ورودی(IJM): ILM بوسیله یک گره MPLS جهت انتقال بسته های برچسب خورده، مورد استفاده قرار می گیرد. برچسب یک بسته ورودی به عنوان یک ارجاع به ILM بکار می رود. اطلاعات ILM به گره اجازه انتخاب مجموعه ای از NHLFE ها را می دهد که دربردارنده دستورات انتقال می باشد.

ممکن است ILM یک برچسب را به گروهی از NHLFE ها نگاشت کند این امر زمینه ساز توانایی ایجاد توازن بارگذاری برروی چندین مسیر با هزینه یکسان ، می باشد.

نگاشت به FEC(FTN NHLFE): FTN بوسیله یک گره MPLS جهت پردازش بسته های رسیده بدون برچسب، اما محتاج برچسب برای انتقال، بکار می رود. بسته داده فاقد برچسب در گره Ingress FEC خاص تخصیص داده می شود. این FEC به عنوان ارجاعی به FTN بکار می رود. نگاشت FTN اجازه می دهد تا گره مجموعه ای از NHLFE محتوى دستورات انتقال را انتخاب نماید. این فرایند توسط یک گره Ingress از شبکه MLPS انجام می شود.

ممکن است FTN یک برچسب را به گروهی از NHLFE ها نگاشت کند این امر زمینه ساز توانایی ایجاد توازن بارگذاری برروی چندین مسیر با هزینه یکسان ، می باشد.

تعویض برچسب:

تعویض برچسب فرایندی است که توسیط یک گره MPLS جهت انتقال یک بسته داده به ابزار مقصد پرش بعدی، بکار می رود. این فرایند فارغ از برچسب دار بودن یا نبودن بسته دریافتی انجام می گیرد و مشابه فرایند انتقال ترافیک در مدارات مجازی در ATM و Frame Relay می باشد.

انتقال یک بسته برچسب دار:

یک گره MPLS برچسب بالای پسته بسته دریافتی را ارزیابی می نماید و از ILM جهت نگاشت برچسب با یک NHLFE استفاده می کند. عمل NHLFE نشان دهنده مقصد انتقال بسته و عملیات بر روی پسته می باشد. با استفاده از این اطلاعات، گره برچسب جدید را رمز کرده و بسته حاصل را منتقل می نماید.

انتقال بسته بدون برچسب:

Next hop label forwarding entry - ^۱

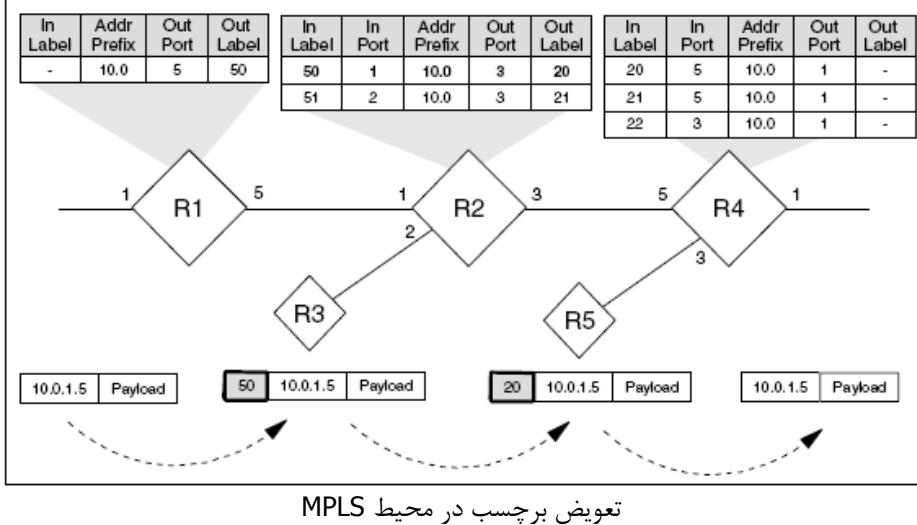
data link encapsulation - ^۲

Incoming label map - ^۳

FEC-to-NHLFE map - ^۴

یک گره MPLS سرآیند لایه شبکه و هر گونه اطلاعات درخور و مورد نیاز جهت تعیین یک FEC را ارزیابی می کند. گره از FTN جهت نگاشت FEC به NHLFE استفاده می نماید. در این حالت پردازش بسته همانند بسته های برچسب دار می باشد. مقصد انتقال بسته و عملیات واقع شده بر روی پشتہ توسط NHLFE مشخص می گردد. با استفاده از این اطلاعات، گره پشتہ برچسب جدید را رمز نموده و بسته حاصل را ارسال می نماید.

تصویر زیر نشاندهنده تعویض برچسب در یک محیط MPLS می باشد:



توجه نمایید که در محیط تعویض برچسب، مسیریاب پرش بعدی همیشه توسط اطلاعات MPLS معین می گردد. این امر می تواند سبب گردد تا بسته از مسیری متفاوت از مسیرهای مشخص شده توسط الگوریتمهای مسیریابی مرسوم، منتقل گردد.

برداشتن پرش یکی مانده به آخر:

یکی از توانایی های MPLS برداشتن یک برچسب در گره یکی مانده به آخر بجای گره Egress می باشد. از دید ساختاری، چنین پردازشی مجاز می باشد. هدف برچسب انتقال یک بسته در شبکه به یک گره Egress می باشد. زمانی که گره یکی مانده به آخر تصمیم گرفت تا بسته را به گره Egress منتقل کند، برچسب دیگر هیچ عملکردی را ندارد و دیگر در بسته مورد نیاز نیست.

گره ماقبل آخر برچسب را از پشته برداشت و بسته را براساس اطلاعات آدرس بعدی NHLFE منتقل می نماید. زمانیکه گره Egress بسته را دریافت نمود، یکی از دو فعالیت زیر اتفاق می افتد:

بسته محتوی برچسب است. این وضعیت زمانی اتفاق می افتد که گره ماقبل آخر بسته ای با

حداقل ۲ برچسب را پردازش کرده باشد. در این حالت، برچسب بالای پشته، برچسبی است که گرنه Egress برای تصمیم گیری در مورد انتقال بسته، باید آن را پردازش نماید.

بسته فاقد برچسب می باشد. در این حالت، Egress LSP یک بسته لایه شبکه استاندارد را

دریافت نموده است. گره از جدول مسیردهی محلی خود جهت تصمیم گیری در مورد انتقال بسته استفاده می نماید.

مسیر سوئیچ برچسب (LSP):

یک LSP مجموعه ای از گره های طی شده بوسیله بسته های متعلق به یک FEC خاص را ارائه می دهد. این مجموعه، یک لیست مرتب و یک طرفه می باشد. مسیر حرکت ترافیک از سمت گره ابتدایی لیست به سمت گره انتهایی لیست می باشد. در تصویر قبل، LSP برابر است با <R1, R2, R3>.

یک شبکه MPLS می تواند به یکی از دو صورت زیر برقرار گردد:

☒ **کنترل LSP مستقل**: هر LSR یک تصمیم مستقل برای تخصیص یک برچسب به یک FEC را

می گیرید. سپس برچسب را بین گره های هم درجه خود توزیع می نماید. این شیوه همانند

مسیردهی IP متداول است که هر گره مستقلاً برای نحوه ارسال بسته، تصمیم گیری می کند.

☒ **کنترل LSP مرتب شده**: یک LSR برچسب را تنها به FEC مشخصی تخصیص می دهد که

برای آن egress LSR برای آن FEC باشد و یا یک تخصیص برچسب از گره بعدی برای آن FEC دریافت

کند. در محیط سیاست گذاری مهندسی ترافیک، کنترل LSP مرتب شده، جت اطمینان از آنکه

FEC مشخصی در یک مسیر ویژه حرکت نماید، بکار برده می شود.

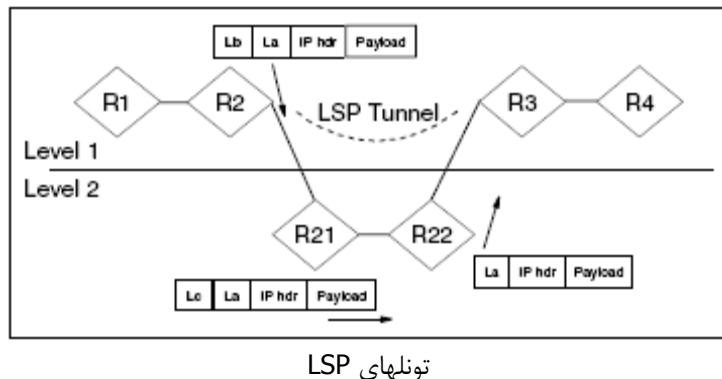
در قسمت "پروتکلهای توزیع برچسب"، روالهای مورد استفاده جهت تبادل اطلاعات برچسب در یک محیط MPLS ارائه می گردد.

پشته برچسب و طبقات برچسب:

یک بسته برچسب دار می تواند شامل بیش از یک برچسب باشد. این برچسب ها بصورت پشته آخرین ورود-اولین خروج نگه داری می شوند. پشتہ، یک سری طبقات مرتب را بین مجموعه برچسب ها پیاده سازی می کند. این طبقه بندی زمانی بکار می رود که یک گره MPLS یک بسته را به گره MPLS دیگری تحويل می دهد، اما این گرهها، مسیریابهای متوالی در یک مسیر Hop-by-Hop برای بسته نمی باشند. در این وضعیت، یک تونل بین دو گره MPLS ایجاد می گردد. تونل به عنوان یک LSP ایجاد می گردد و تعویض برچسب جهت انتقال ترافیک در امتداد تونل بکار می رود.

مجموعه ترافیک انتقالی از طریق تونل شامل یک FEC می گردد. هر LSR در تونل باید یک برچسب را به این FEC مناسب بنماید.

برای انتقال یک بسته از طریق تونل، گره Ingress تونل یک برچسب را به پشته می افزاید که توسط گره Egress تونل قابل درک و بازیابی می باشد. سپس گره Ingress تونل یک برچسب دیگر را به پشته می افزاید که جهت انتقال داده در طول تونل بکار می رود و قابل درک و بازیابی توسط گره پرش بعدی می باشد. برای مثال یک شبکه ممکن است شامل یک LSP بصورت $R1, R2, R3, R4$ باشد. در این مثال R2 و R3 بصورت مستقیم به همدیگر متصل نشده اند، اما هر دو نقطه انتهایی یک تونل LSP می باشند. توالي حقیقی LSR مورد عبور واقع شده در طول شبکه عبارت است از $R1, R2, R21, R22, R3, R4$. تصویر زیر این وضعیت را نمایش می دهد:



یک بسته عبوری در این شبکه در طول یک LSP سطح ۱ به صورت $R1, R2, R3, R4$ عبور می نماید و سپس در زمان عبور از $R2$ به $R3$ از یک LSP سطح ۲ به شکل $R2, R21, R22, R3$ عبور می نماید. از منظر دید LSP سطح ۱، ابزارهای هم مرتبه $R1, R2$ و $R3$ می باشند. از منظر دید سطح ۲، ابزار هم مرتبه $R21, R2, R3$ می باشد.

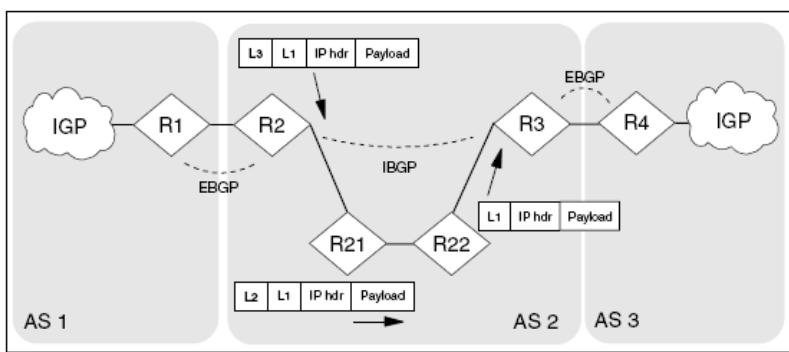
با استفاده از این دیاگرام، عملیات زیر در حین ارسال یک بسته از طریق تونل LSP رخ می دهد:

- $R2$ یک بسته برچسب دار را از $R1$ دریافت می کند. بسته شامل یک برچسب منفرد می باشد.
عمق پشته برچسب، یک است.
- $R2$ این برچسب را برمی دارد و یک برچسب قابل ادراک توسط $R3$ را جانشین آن می سازد. این برچسب L_a نامید می شود.
- همچنین $R2$ باید یک برچسب قابل ادراک توسط $R21$ را نیز اضافه نماید. $R2$ این برچسب را به بالای برچسب سطح ۱ موجود می افزاید. این برچسب L_b نامیده می شود. اکنون پشته برچسب شامل ۲ مدخل می باشد.
- $R2$ بسته را به $R21$ ارسال می کند.
- $R21$ برچسب سطح ۲ (L_b) افزوده شده توسط $R2$ را بر می دارد و یک برچسب لایه ۲ قابل درک توسط $R22$ را جانشین آن می سازد. این برچسب L_c نامیده می شود. $R21$ برچسب سطح ۱ را پردازش نمی کند. اکنون پشته برچسب شامل ۲ مدخل می باشد.
- $R21$ بسته را به $R22$ ارسال می سازد.
- $R22$ برچسب سطح ۲ افزوده شده بوسیله $R21$ را بررسی کرده و مشاهده می کند که پرش ماقبل آخر در تونل $R2-R3$ می باشد. $R22$ برچسب سطح ۲ (L_c) را برداشت و بسته را به سمت $R3$ می فرستد. پشته برچسب شامل یک مدخل می باشد.

پشته های MPLS در یک محیط BGP

شبکه تصویر زیر سه سیستم Autonomous را نشان می دهد. محیط شامل ۲ کلاس مسیردهی IP می باشد:

- هر سیستم Autonomous یک IGP را برای حفظ ارتباط در AS ها، اجرا می کند. برای مثال $R2$.
- $R2, R21$ و $R3$ ممکن است از OSPF برای حفظ مسیر در ۲ AS استفاده می شود.
- هر سیستم Autonomous BGP را برای حفظ ارتباط بین AS ها اجرا می کند. برای مثال، مسیریابی لبه $R1, R2, R3$ و $R4$ برای تبادل اطلاعات مسیردهی بین AS می استفاده می کند.



اتصال سیستم های Autonomous در یک محیط MPLS

در این شبکه ساده، خوشایند است تا از توزیع مسیرهای آموخته شده BGP برای ابزارهایی که مسیریابهای BGP نیستند (برای مثال R21 و R22)، اجتناب گردد. این امر سبب کاهش پردازش های CPU مورد نیاز جهت نگهداری جدول مسیردهی IP در ابزارها می گردد. همچنین این امر زمینه ساز حذف اجرای الگوریتم مسیریابی BGP در این ابزارها می باشد.

یک پشته MPLS LSP می تواند به این منظور مورد استفاده قرار گیرد. در این پیکربندی، مسیرهای BGP تنها به BGP های همسان توزیع شده است و نه به مسیریابهای درونی که در مسیر Hop-by-Hop بین همسان ها وجود دارد. تونلهای LSP بگونه ای پیکربندی می شود تا:

هر زوج یک برجسب را برای هر آدرس Prefix توزیع می نماید که از طریق BGP توزیع می گردد.

این برجسب ها برای زوجها موجود در یک AS توزیع می شود.

IGP یک مسیر میزبان برای هر مسیریاب مرزی BGP را نگهداری می نماید. هر مسیریاب درونی، یک برجسب برای مسیر میزبان به هر IGP همسایه توزیع می نماید.

وضعیتی را در نظر بگیرید که R2 یک بسته فاقد برجسب برای یک شبکه متصل شده از طریق 3 AS را دریافت می نماید. بسته ممکن است در ابتدا از یک LAN محلی متصل به R2 و یا R2 دیگری در 2 AS آمده باشد. بسته در صورتیکه از 1 AS آمده باشد، قبلًا برجسب خورده است.

R2 جدول ارسال IP محلی را جستجو می نماید تا بهترین مسیر برای آدرس مقصد مورد درخواست را مشخص نماید. این مسیر از طریق BGP مشخص می گردد. پرش بعدی R3، BGP خواهد بود.

R3 قبلًا یک برجسب برای طولانی ترین تطبیق ممکن ارائه داده و آن را به R2 توزیع می نماید. این برجسب L1 نامیده می شود.

بنابراین همه ابزارهای 2 در IGP شرکت می کنند، یک مسیر به R3 در جدول مسیریابی برای تمام ابزارهای موجود در 2 AS مشاهده می گردد:

▪ R22 قبلًا یک برجسب را برای R3 ایجاد نموده و این برجسب را به R21 توزیع می نماید. این برجسب L2 نامیده می شود.

▪ R21 قبلًا یک برجسب را برای R3 ایجاد نموده و این برجسب را به R2 توزیع می نماید. این برجسب L3 نامیده می شود.

R2 یک بسته داده با مقصد 3 AS را با ایجاد یک پشته برجسب، فراهم می آورد. مدخل اولیه بر روی پشته با ورود L1 به آن ایجاد می گردد. مدخل بالایی پشته برروی پشته با ورود L3 به آن ایجاد می گردد. سپس بسته برجسب خورده به پرش بعدی R21، ارسال می گردد.

R21 بسته برجسب دار را دریافت نموده و برجسب بالایی پشته را بررسی می نماید. با استفاده از اطلاعات NHLEF، R21 برجسب L3 را با برجسب L2 جانشین می نماید. سپس بسته برجسب خورده به پرش بعدی R22، ارسال می گردد.

R22 بسته برجسب دار را دریافت نموده و مدخل بالایی را بررسی می نماید. بدلیل آنکه R22 پرش ماقبل آخر در تونل R2-R3 می باشد، R22 برجسب L2 را از بالای پشته برداشته و بسته داده را به R3 می فرستد. اکنون پشته برجسب در حیث انتقال به R3 تنها دارای یک برجسب می باشد.

R3 یک بسته داده برچسب دار را دریافت نموده و برچسب L1 در بالای پشته را بررسی می نماید.
با استفاده از اطلاعات NHLFE، R3 برچسب قدیمی را با برچسب ارائه شده از سوی R4 جانشین کرده و بسته را ارسال می نماید.

هر زمان که یک گره MPLS یک برچسب را به یک بسته برچسب دار موجود می افزاید، برچسب جدید باید مطابق یک FEC باشد که برچسب جدید را تخصیص می دهد.

پروتکلهای توزیع برچسب

پروتکل توزیع برچسب، مجموعه ایست از روالهایی که به یک گره MPLS اجازه می دهند تا برچسبها را به سایر گره های همسان توزیع نماید. این امر بوسیله یک LSR جهت آگاه سازی درگیری درمورد یک تخصیص برچسب و مفهوم آن می باشد. این تبادل، یک توافق عمومی را بین گره های همسان ایجاد می نماید.

هر گره MPLS در یک IGP محلی شرکت می کند تا ساختر شبکه را مشخص نماید و جداول مسیردهی را پر نماید. پروتکلهای توزیع برچسب این اطلاعات را جهت ایجاد برچسب ها بکار می برد. پس از اجرای یک پروتکل توزیع در هر گره، کل شبکه MPLS باید دارای یک مجموعه کامل از مسیرها و برچسبهای متناظر باشد. همچنین، پروتکلهای توزیع برچسب ارتباطات بین گره هی همسان را تحت نظارت قرار می دهند تا توانایی های MPLS هر زوج را بدانند.

انواع پروتکل های توزیع برچسب

معماری MPLS، یک معماری توزیع مورد لزوم مشخص ندارد و همچنین تنها یک پروتکل تنها نیز وجود ندارد. به این دلیل، استانداردهای متفاوتی از آن تحت توسعه قرار دارند. این استانداردها را می توان در ۲ گروه طبقه بندی نمود:

۱. توسعه پروتکلهای موجود:
برچسب در جریانات داده موجود، در پروتکلهای جاری، ارائه شده است. ۲ نمونه آن عبارتست از:
 - توسعه BGP : در بسیاری از حالات، FECها جهت مشخص کردن آدرسهای پیشرت توزیع شده توسط زوجهای BGP بکار می رود. می توان از این مزیت جهت توزیع برچسبهای MPLS در ابزارهای مشابه استفاده نمود. بعلاوه، استفاده از بازتابنده های مسیر BGP جهت توزیع برچسبها می تواند سبب پیشرفت عمده در مقیاس پذیری گردد.
 - توسعه RSVP : این پیشنهادات در برگیرنده گسترش استاندارد RAVP جهت پشتیبانی برای ایجاد و توزیع اطلاعات LSP می باشد. این امر زمینه ساز تخصیص منابع در طول مسیر انتهای می گردد.

۲. توسعه پروتکلهای جدید:
انواع جدید پروتکل نیز جهت توزیع برچسب با اهداف خاص، در حال توسعه می باشد. این پروتکلهای منفرد نمی توانند بر روی پروتکلهای مسیردهی موجود در هر پرش در طول مسیر، عمل نمایند. این امر در موقعي که یک LSP باید از گره هایی عبور نماید که یکی از انواع خاص پروتکلهای موجود را پشتیبانی نمی نمایند، جهت توابع توزیع برچسب، توسعه داده شده است.

^۱ BGP route reflectors -

متدهای توزیع برچسب

دو متد جهت مقداردهی اولیه ارتباط بین گره های MPLS برای تبادل اطلاعات برچسب وجود دارد:
Downstream برحسب تقاضا: یک LSR می تواند یک تخصیص برچسب را برای یک FEC خاص
بنماید.

Downstream بدون درخواست¹: یک LSR می تواند تخصیص برای LSRها را بدون هیچگونه
درخواست اطلاعات صریح، توزیع نماید.

هر دو این تکنیکهای توزیع می تواند برای توزیع در شبکه یکسان در زمان یکسان، بکار رود. برای یک
مجموعه ای از زوجها، Upstream LSR و Downstream LSR باید با تکنیک مورد استفاده، مطابقت داشته باشد.

ادغام جریان²

ادغام جریان، گردهم آوری تعداد زیادی از جریانات داده در یک جریان Downstream یکه می باشد. ابزار
انجام دهنده ادغام، بگونه ای جریانات منفرد را یکی می سازد تا گره های MPLS متوالی با آنها همانند یک جریان
منفرد عمل نمایند. جریان ادغام شده بوسیله یک برچسب منفرد، ارائه می شود. با ارسال بسته های ادغام شده،
اطلاعات ورود بسته ها با برچسبهای ورودی متفاوت، از بین می رود.
ادغام جریان، یک جزء اصلی از توسعه پذیری MPLS می باشد.

ادغام در یک محیط مبتنی بر فریم

ادغام جریان در یک محیط مبتنی بر فریم، سرراست می باشد. ابزار انجام دهنده ادغام، چندین برچسب
Upstream و Downstream را به یک برچسب نگاشت می نماید. هیچ تغییری در روالهای تعویض برچسب
رایج صورت نمی گیرد.

ادغام در یک محیط ATM

ادغام جریان در یک محیط ATM پیچیده می باشد. در ATM، بسته های داده در یک AAL5 PDU قرار
گرفته اند و به عنوان سلول های ATM ارسال می گردند. این سلولها دارای مقدار VPI/VCI خاص می باشند. همه
سلولهای VPI/VCI بصورت پشت سرهم ارسال می گردند. الزاماً است تا تمام سوئیچهای ATM موجود در مسیر
داده، ترتیب سلولها را رعایت نمایند. ابزار انتهایی، PDU های دریافتی متوالی و با توالی صحیح را بازیابی و یکپارچه
می کند.

درصورت وقوع ادغام جریان مستقیم MPLS در یک محیط ATM، با مشکل موجه می شویم. در این حالت،
سلول های ورودی از چند VC، در یک VC خروجی یکه، جداده می شوند. مشکل در زمان بازسازی PDU های اصلی
رخ می دهد، زیرا سرآیند سلولهای ATM شامل اطلاعات ترتیب اصلی نمی باشد.

۲ متد برای جلوگیری از درهم چینی سلولها در طی ادغام جریان در یک محیط ATM وجود دارد:
ادغام VC اجازه می دهد چندین VC ورودی در یک VC خروجی یکه ادغام گردد. گره MPLS انجام
دهنده ادغام سلولهای یک فریم AAL5 را از سلولهای یک فریم AAL5 دیگر جدا نگاه می دارد.
برای این منظور، سوئیچ ATM ارسال سلولهای یک فریم را تا زمان ارسال سلولهای فریم در حال

Unsolicited Downstream - ¹
Stream merge - ²

ارسال، به تعویق می‌اندازد. با دریافت نشانگر خاتمه ارسال، فریم بعدی می‌تواند بصورت کامل ارسال گردد. این نوع بافر کردن و توانایی ذخیره و ارسال، بطور مشخص در سوئیچهای ATM موجود، وجود ندارد.

ادغام VP اجازه می‌دهد تا چندین VP در یک VP خروجی یکه، ادغام گردد. VCI متفاوت در VP

ادغامی برای تشخیص فریمهای مبادی مختلف بکار می‌رود.

ادغام VP دارای این مزیت می‌باشد که با درصد بالایی از تجهیزات ATM موجود در شبکه های جاری، سازگار می‌باشد. همچنین تاخیر روش قبلی در نقاط ادغام را ندارد و همچنین نیازمندیهای بافر کردن جدید را نیز ندارد.

اصلی‌ترین ضعف این روش آنست که نیازمند تخصیص مختصات VCI در هر VP می‌باشد.

ویژگیهای معماری MPLS، هر دو روش ادغام VP و ادغام VC را پشتیبانی می‌نماید. سوئیچهای ATM شرکت کننده در MPLS باید توانایی آن را داشته باشند تا تشخیص دهنده سوئیچهای همسایه از ادغام VP و یا ادغام VC استفاده کرده اند و یا ادغامی انجام نداده اند.

سوئیچ Lambda چندپروتکلی

راه حل‌های بهبود هزینه و مقیاس پذیری برای معماری، پیچیدگیهای داده ای شبکه را افزایش می‌دهد. همچنین این راه حلها باید ویژگیهای بهبود کارایی را نیز فراهم آورند. برخی از این نیازمندیها توسط استاندارد MPLS عنوان گردید. این نیازمندیهای تجاری، قابل اعمال بر شبکه های انتقالی نوری (OTN)¹ می‌باشد. در نتیجه، تلاشها در جهت توسعه ویژگیهایی برای یکسان سازی توابع MPLS در ابزارهای OXC² در حال انجام است. نام این فعالیت MPλS می‌باشد.

توسعه توابع MPLS به شبکه های نوری مزیتهایی را به همراه دارد:

این روند می‌تواند به عنوان اهرمی در جهت توسعه تکنیکهای MPLS برای فراهم آوردن

متدولوژی برای فراهم آوردن کانالهای نوری بلادرنگ، بکار رود. این زمینه ساز توسعه و ترقی سریعتر این فن آوریها می‌گردد.

این روند می‌تواند دید واحدی را برای مدیریت شبکه برای هر دو محیط داده ای و نوری فراهم آورد. این امر سبب ساده سازی تلاشها کلی می‌گردد.

این تلاش می‌تواند معماری واحدی را فراهم آورد که اجاز می‌دهد تا یک LSP از ترکیبی از مسیریابها و ابزار OXC عبور نماید. این امر زمینه ساز آنست تا شبکه در وضعیتی قرار بگیرد تا پهنهای باند بر حسب درخواست واقعی را فراهم آورد.

این تلاشها مسیریابهای IP را در موقعیتی قرار می‌دهد تا توانایی یکسان سازی احتمالی مالتی پلکس تقسیم چگالی موج (DWDM)³ با ظرفیت بالا را کسب نمایند.

توسعه توابع MPLS به شبکه های نوری برپایه برخی مشابهت های بین دو نوع شبکه می‌باشد:

در MPLS، یک مسیر Point to Point را ارائه می‌دهد که توسط مجموعه ای از بسته های برچسب دار مورد عبور واقع می‌شود. در MPλS، یک کانال نوری دنباله دار برای توصیف اتصال نوری Point to Point بین دو نقطه دسترسی، مورد استفاده قرار می‌گیرد.

¹ Optical Transport Network

² optical cross-connect

³ Dense Wave Division Multiplexing

در یک شبکه MPLS، یک رابطه بین یک زوج <پورت ورودی، برچسب ورودی> و زوج <پورت خروجی، برچسب خروجی> ایجاد می نماید. بطور مشابه، در شبکه نوری، یک OXC یک رابطه را بین یک زوج <پورت ورودی، کانال نوری ورودی> و زوج <پورت خروجی، کانال نوری خروجی> ایجاد می نماید. پس از برپاسازی، این روابط قابل تغییر بوسیله بسته های داده نمی باشند.

در یک شبکه MPLS، یک LSR وظیفه کسب، توزیع و نگهداری اطلاعات وضعیت شبکه را دارد. یک OXC نیز وظیفه ای مشابه در یک OTN بر عهده دارد.

در یک شبکه MPLS، یک LSR مسئول ایجاد و نگهداری LSP‌ها، متناسب با سیاستهای مهندسی ترافیک موجود می باشد. یک OXC نیز وظیفه ای مشابه در یک OTN بر عهده دارد.

در یک شبکه MPLS، یک LSP فاقد جهت می باشد. در یک OTN، یک کانال نوری دنباله دار نیز فاقد جهت می باشد.

در محیط MP\LS، این امکان وجود خواهد داشت تا فیبر در OTN به عنوان مجموعه ای از پیوندها بکار رود که هر پیوند در بردارنده مجموعه ای از کانالهای IP است. یک پروتکل مسیردهی IP (با توسعه ها) اطلاعات ساختار شبکه فیبر نوری، پهنای باند موجود و سایر اطلاعات وضعیتی مناسب را توزیع خواهد کرد. اطلاعات جهت محاسبه مسیرهای صریح برای کانالهای نوری دنباله دار بکار خواهد رفت. سپس پروتکلهای توزیع MPLS این کانالهای دنباله دار را می سازند.

با توسعه این فن آوری، تفاوت های مهمی بین یک شبکه MPLS و یک OTN قابل بیان است:

در یک شبکه MPLS، اطلاعات ارسال شده به عنوان بخشی از برچسب موجود در هر بسته داده ارسال می شود. در یک OTN، اطلاعات سوئیچ از روی طول موج یا کانال نوری بدست می آید.

در یک OTN، مفهوم ادغام برچسب وجود ندارد. یک OXC نمی تواند چند طول موج را در یک طول موج ادغام کند.

یک OXC نمی تواند عملیات گذاشتن و برداشتن برچسب در پشته را انجام دهد. در یک دامنه نوری، طول موج قابل مقایسه با برچسب می باشد. مفاهیم گذاشتن و برداشتن از پشته در فن آوریهای نوری موجود، وجود ندارد.

بخش ۴:

پروتکل های شبکه

فصل ۹: پروتکل IP

فصل ۱۰: پروتکل های ICMP و IGMP

فصل ۱۱: کنترل اتصالات در شبکه

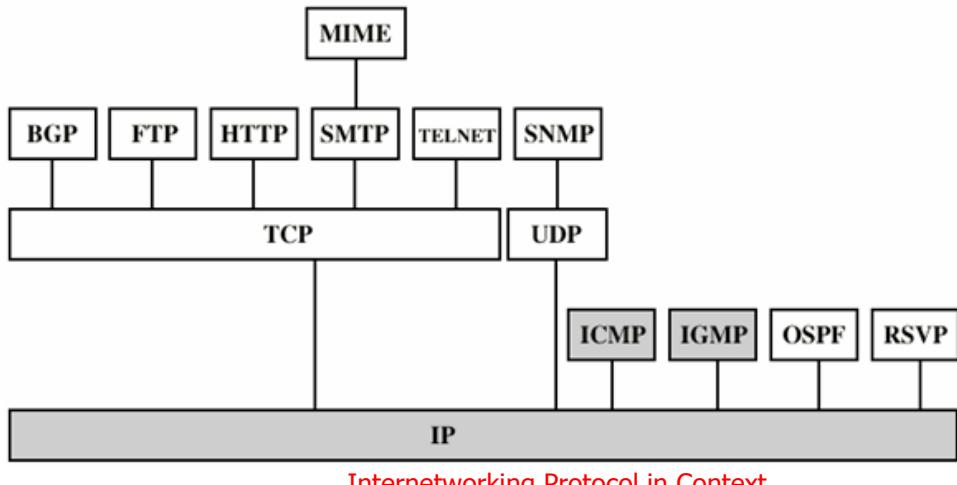
فصل ۱۲: پروتکله های UDP و TCP

www.samavi.info

فصل ۹:

پروتکل IP

پروتکل IP بستر مناسبی برای تبادلات بین شبکه‌ای است ولی IP به صورت بدون اتصال است و TCP می‌تواند اتصال گرا است.



Internetworking Protocol in Context

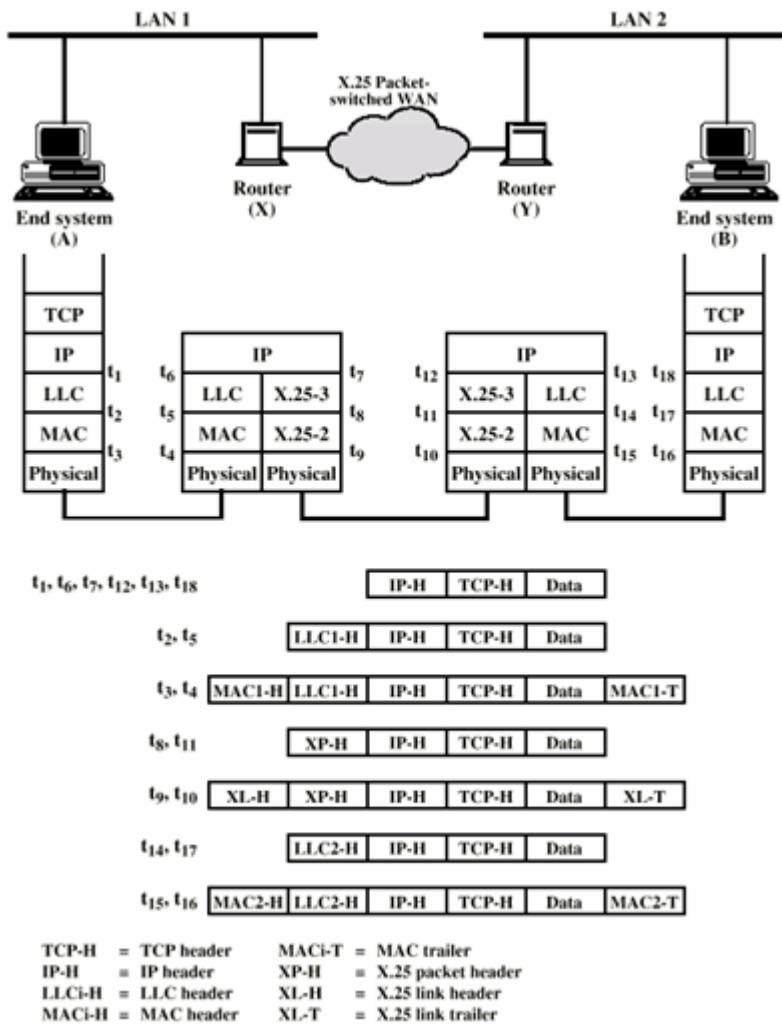
UDP: برای موقعی که رسیدن Data به مقصد چندان مهم نیست.

OSPF: مسیریابی

RSVP : رزرو منابع برای تخصیص یک پهنه‌ای باند به شبکه. چون در نسل آینده اینترنت باید QoS را SUPPORT کند . این موضوع (RSVP) اهمیت زیادی پیدا کرده است .

IP یک پروتکل انتقال بین شبکه هاست یعنی برای INTERNETWORKING مناسب است. باید بتواند موانع زیر را بر طرف کند . (موانعی که باعث مشکل شدن اتصال دو شبکه می شوند .)

- روش‌های مختلف آدرس دهی در شبکه‌های مختلف
- تفاوت در اندازه بسته‌ها در شبکه‌های مختلف
- اختلاف در نحوه دسترسی به شبکه‌ها
- اختلاف در TIMEOUT‌ها .
- تفاوت در روش‌های مختلف کنترل خطا .
- روش‌های مسیریابی .
- روش‌های مختلف کنترل دسترسی کاربران .
- اتصال گرا بدون اتصال بودن شبکه‌های فرعی .
- گزارش وضعیت ، (شامل اطلاعات آماری [مثلاً تعداد پرینت در یک زمان مشخص و... [و...)



IP Data Transfer over Internet

نکاتی که در طراحی IP باید در نظر گرفت عبارتند از :

Routing, DataGRAM, FRAGMENTATION& ASSEMBLY, ERROR CONTROL, FLOW CONTROL

(سؤال) شبکه اینترنت با توجه به گستردگی قابل توجهی که دارد و INTERNETWORKING کامل است .

آیا می توان گفت که اینترنت یک WAN است؟ اینترنت هم یک WAN نیست . زیرا WAN باید تعریف بسته هایی در لایه ۲،۳ داشته باشد ولی اینترنت با اینکه Data را منتقل می کند WAN نیست؛ یعنی WAN یک بستر برای انتقال Data می باشد ولی اینترنت بستر نیست ولی از این بستر هم استفاده می کند. اینترنت می تواند هم روی WAN پیاده سازی شود و هم روی LAN .

سرویسهای IP

دو سرویس فراهم می کند (برای لایه بالای خود)

SEND (ارسال بسته به لایه پایین)

برای لایه بالا یا خود DELIVER (دریافت بسته ها از لایه پایین هنگام دریافت).

پارامترهای SEND

آدرس اینترنت مبدأ و مقصد ، پروتکل ، نوع سرویس ، شناسنامه ، قطعه بندی کردن ، طول عمر ، طول داده و OPTION و داده.

(پارامتر های DELIVER هم به همین صورت است)

عملیات در مبدأ برای ارسال بسته های IP :

1. ساخت دیتاگرام IP با توجه به پارامترهای SEND

۲. انجام عملیات CHECK SUM (فقط برروی HEADER)

۳. مسیریابی (اگر مقصد در همین LAN است تحویل داده شده و اگر نباشد به ROUTER داده شود).

۴. انتقال دیتاگرام به پروتکل زیرین

عملیات ROUTER:

• انجام عملیات Checksum (اگر Checksum موجود در بسته یکسان نباشد

بسته دور ریخته می شود)

• کاهش طول عمر (یک واحد)

• انجام مسیریابی برای یافتن مسیریاب بعدی

• اگر طول بسته بسیار بزرگ باشد قطعه بندی کردن بسته ها

• قطعه بندی کردن بسته ها در صورت نیاز (با توجه به طول بسته) اگر طول بسته زیاد باشد قطعه بندی می شود و اگر طول بسته کم باشد از PADING استفاده میکند یعنی بیتهاي اضافي به آن می چسباند.

• ساخت HEADER جدید

• انتقال دیتاگرام به شبکه

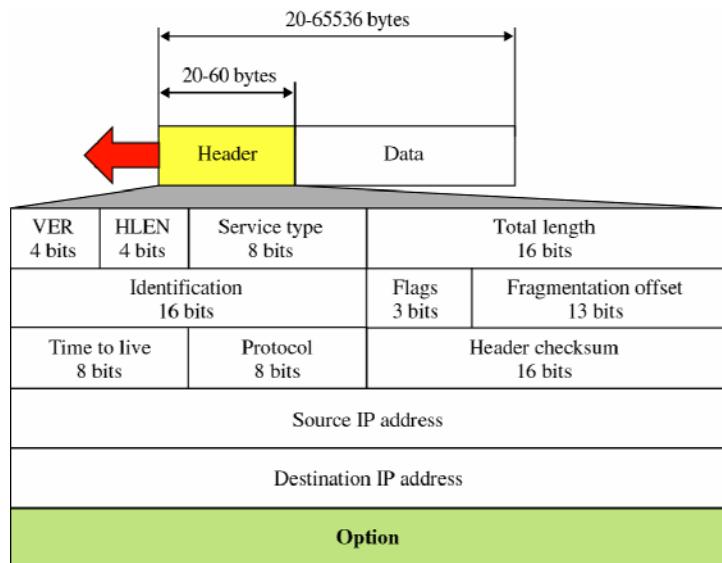
عملیات در گیرنده :

• انجام عملیات Checksum (اگر یک نباشد دور ریخته شود)

• اگر بسته دریافتی یک قطعه از بسته بزرگ است نگهداری شده تا قطعه های بعدی آن هم دریافت شوند.

• عبور داده با استفاده از پارامتر DELIVER

فرمت بسته های IP:



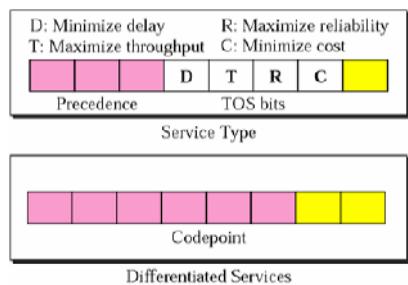
مربوط به IP مورد استفاده را مشخص می کند. (مثلاً بسته توسط IP6 یا IP4 فرستاده شده)

IP version (VER): طول Header را مشخص می کند (براساس ۳۲ بیتی). از آنجا که عدد مشخص شده در این قسمت عددتاً در مبنای ۱۶ ذکر می شود، باید در 4^4 ضرب شود تا طول سرآیند بسته مشخص شود.

- Service type: یعنی چه سرویسی باید به این بسته داده شود تا به مقصد برسد. شامل بیتهاي زير است - قابلیت اطمینان (کم یا زیاد) (۱ بیت).

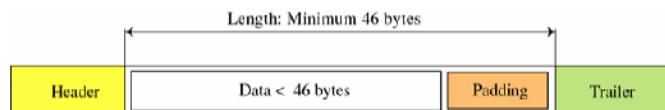
- اولویت (سه بیت): اگر دو بسته با هم برستند با توجه به این سه بیت تصمیم گرفته می شود.

- گذردهی (۱ بیت) (کم یا زیاد) .
 - تأ خیر (کم یا زیاد) .



ممکن است بجای نوع سرویس از Differentiated Services استفاده شود. زیرفیلدهای گفته شده در این قسمت در IP نسخه ۴ استفاده نمی شود.

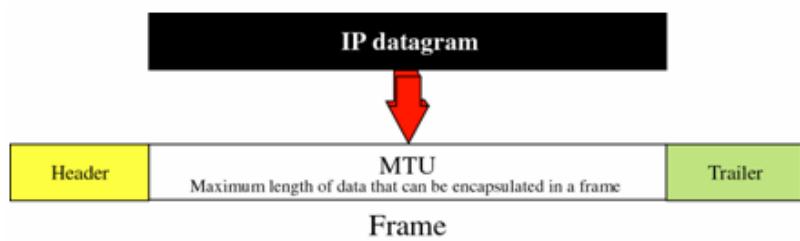
Total length : طول کل بسته را مشخص می کند. در شکل فوق $64\text{kbyte} \leq 2\text{Bytes}$ حداکثر طول بسته است (زیرا این فیلد ۱۶ بیتی است). طول کلی شامل طول بخش داده بعلاوه طول سرآیند می باشد. اگر طول قسمت داده از ۴۶ بایت کمتر باشد، با استفاده از Padding این کمبود جبران می شود.



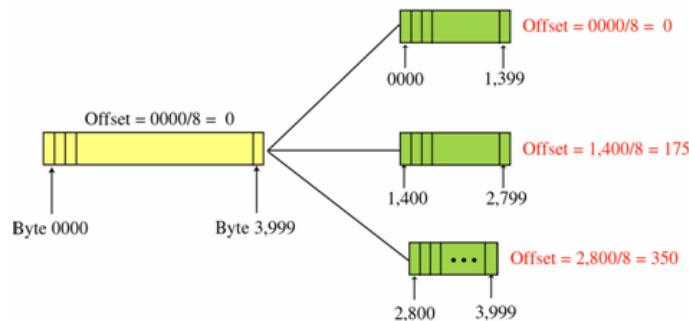
Identification : برای شناسائی بسته بکار می رود . باعث می شود که بسته بصورت یکتا باشد .
((id + آدرس مبدأ + آدرس مقصد) یک بسته یکتا می سازد)

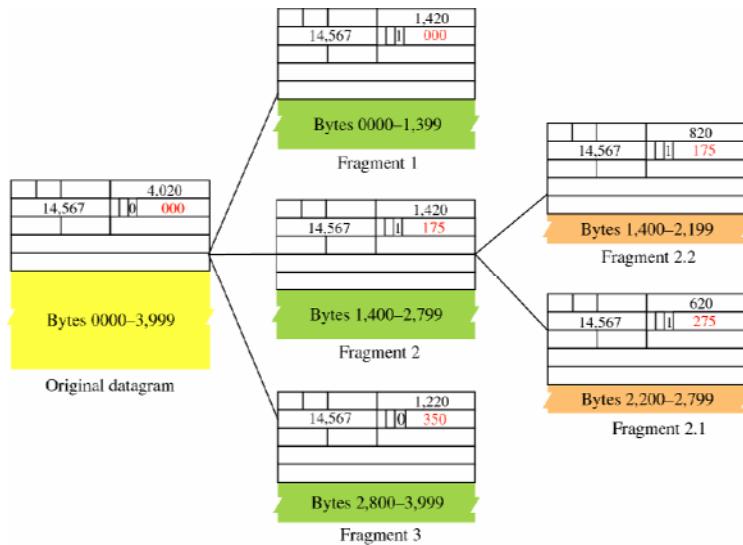
Flags : سه بیت است که از دو بیت آن استفاده می شود (یک بیت don 't fragment است و بیت دیگر (more

اگر بیت Fragment صفر باشد، آفست آن در فیلد بعدی (fragment offset) قرار داده می شود و اگر بیت more یک باشد یعنی بیش از یک fragment دارد. غیر از این fragment های دیگری هم هست). علت قطعه قطعه کردن بسته های IP بزرگتر بودن آنها از اندازه MTU در فریم می باشد.



مثال:





وقتی $more = 0$ است یعنی این قطعه اخرين قطعه است .

offset - نشان دهنده اين است که اين قطعه در کجاي بسته اصلی قرار داشته است .

TTL : وقتی بسته از هر مسیریاب که عبور می کند یکی از این فیلد کم می کند .

Protocol : پروتکل لایه بالایی را مشخص می کند . (Icmp, Tcp, Udp)

Header checksum : برای کنترل خطای برای خود header استفاده می شود .

برای کل بسته ، کنترل خطای وجود ندارد (درون بسته) .

source add & dest add : آدرسهای مبدأ و مقصد را مشخص می کنند .

option padding : در این قسمت option های زیر می توانند قرار داده شوند :

time stamping : هر زمان که در یک مسیریاب می گذرد ، زمان را یادداشت می کند .

Router recording : بسته IP از هر جا که رد می شود شماره مسیریاب را در بسته ذخیره می کند .

source routing : آیا از source routing استفاده شده است ؟

security : مثلاً چه نوع رمز گذاری استفاده شده است .

مثال: بسته IP با طرح ۸ بیت اول بصورت 01000010 ، دریافت می شود. چرا این بسته توسط گیرنده دور

ریخته می شود؟

۴ بیت سمت چپ(0100) نشان دهنده نسخه IP می باشد و درست است. ۴ بیت بعد (0010) طول سرآیند را مشخص می کند که برابر با $2^4 = 16$ می باشد و این مقدار اشتباه است؛ زیرا حداقل طول سرآیند بسته IP ۲۰ است. پس بسته در طول مسیر انتقال خراب شده است.

مثال: یک بسته IP با مقدار HLEN برابر 1000 دریافت می شود. تعداد بایت‌های Option در این بسته چقدر است؟

مقدار HLEN، ۸ است. بنابراین طول کل سرآیند برابر با $8 \times 4 = 32$ است. سرآیند اصلی ۲۰ بایت اول را تشکیل می دهد و ۱۲ بایت بعدی Option هستند.

مثال: یک بسته IP با HLEN ۵ و مقدار طول کلی فیلد ۰۰۲۸ دریافت شده است. چند بایت داده در این بسته حمل می شود؟

مقدار HLEN ۵ است. بنابراین طول سرآیند $5 \times 4 = 20$ بایت است و Option وجود ندارد. طول کلی ۴۰ بایت است که نشانگر آنست که ۲۰ بایت داده در این بسته حمل می شود ($40 - 20 = 20$).

مثال: بسته IP با مقادیر مبنای ۱۶ زیر برای ابتدای بسته، دریافت می گردد. تعداد پرشهای بسته قبل از دور ریخته شدن آن چند است؟ این بسته مربوط به کدام پروتکل لایه بالاتر می باشد؟
45000028000100000102.....

برای یافتن فیلد TTL، باید از ۸ بایت اول (۱۶ عدد مبنای ۱۶) پرش کنیم. فیلد TTL در بایت نهم قرار دارد که مقدار ۰۱ را دارد. این به این معناست که بسته قبل از دور ریخته شدن تنها می‌تواند یک پرش داشته باشد. فیلد پروتکل، بایت بعدی است (۰۲) که مشخص می‌کند این بسته به پروتکل IGMP مربوط می‌شود.

مثال: یک بسته با بیت M با مقدار صفر دریافت می‌شود. این بسته اولین قطعه، قطعه میانی و یا قطعه آخری می‌باشد؟ آیا می‌توانید بگوئید بسته تکه تکه شده است یا نه؟

مقدار صفر برای بیت M به معنی آنست که قطعه دیگری وجود ندارد و قطعه دریافتی، آخرین قطعه می‌باشد. اگرچه نمی‌توانیم بگوئیم که بسته اصلی تکه تکه شده است یا نه. یک بسته بدون تکه تکه شدن به عنوان آخرین قطعه درنظر گرفته می‌شود.

مثال: یک بسته با بیت M با مقدار یک دریافت می‌شود. این بسته اولین قطعه، قطعه میانی و یا قطعه آخری می‌باشد؟ آیا می‌توانید بگوئید بسته تکه تکه شده است یا نه؟

بیت M با مقدار یک نشانگر آنست که حداقل یک قطعه دیگر، وجود دارد. قطعه دریافتی می‌تواند قطعه اول و یا یک قطعه میانی باشد؛ اما قطعه آخر نخواهد بود. اما نمی‌توانیم بگوئیم که این قطعه اولی است یا جزء قطعات وسطی است. برای این منظور نیازمند اطلاعات بیشتر (مقدار آفست قطعه) هستیم. ولی با این وجود بدلیل یک بودن M با قاطعیت می‌توانیم بگوئیم که بسته تکه تکه شده است.

مثال: یک بسته با مقدار یک برای M و یک آفست قطعه صفر دریافت می‌شود. آیا این قطعه، اولین قطعه، قطعه میانی و یا قطعه آخری می‌باشد؟

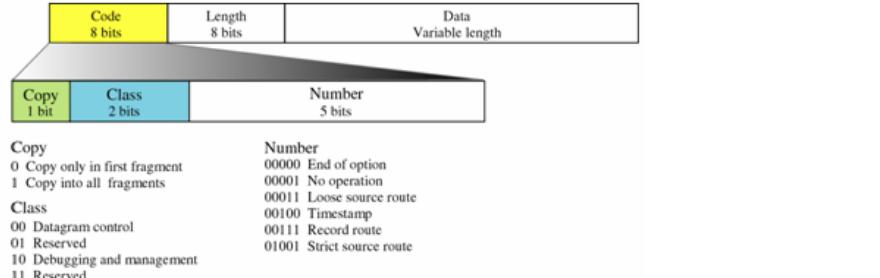
بدلیل یک بودن بیت M، ممکن است بسته قطعه اول باشد و یا یکی از قطعات میانی باشد. بدلیل صفر بودن آفست قطعه، این قطعه، اولین قطعه می‌باشد.

مثال: یک بسته با آفست ۱۰۰ دریافت می‌شود. شماره اولین و آخرین بایت آن چیست؟
برای یافتن شماره بایت اول قطعه، کافی است تا مقدار آفست را در ۸ ضرب کنیم. بنابراین شماره بایت اول برابر ۸۰۰ می‌باشد. بدلیل عدم اطلاع از طول داده‌ها، نمی‌توانیم شماره آخرین بایت قطعه را مشخص کنیم.

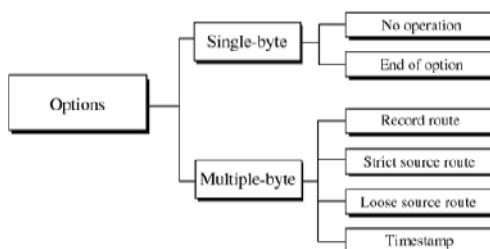
مثال: یک بسته با آفست ۱۰۰، HLEN ۵ و با مقدار ۱۰۰ بایت کل طول، دریافت شده است. شماره اولین و آخرین بایت آن چیست؟

شماره اولین بایت $100 \times 8 = 800$ است. طول کل بسته ۱۰۰ بایت و طول سرآیند ۲۰ بایت ($5 \times 4 = 20$) می‌باشد؛ بنابراین طول بخش داده ۸۰ بایت است. اگر شماره بایت اول ۸۰۰ باشد، شماره بایت آخر ۸۷۹ می‌باشد.

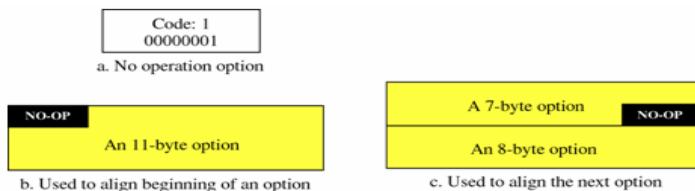
فرمت Option های بسته IP



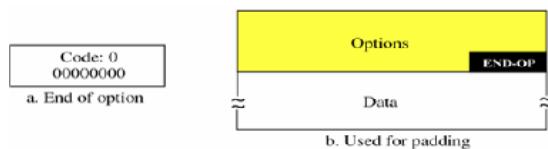
طبقه بندی IP Option های



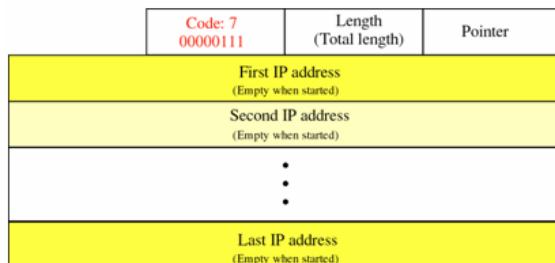
موارد استفاده از :No Operation Option



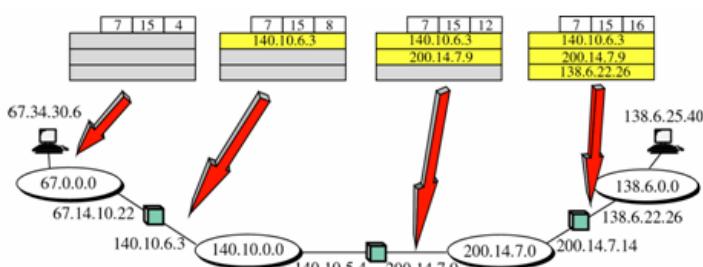
موارد استفاده از :End of Option



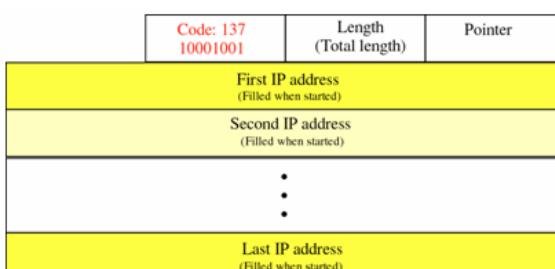
فرمت بسته Record Route Option



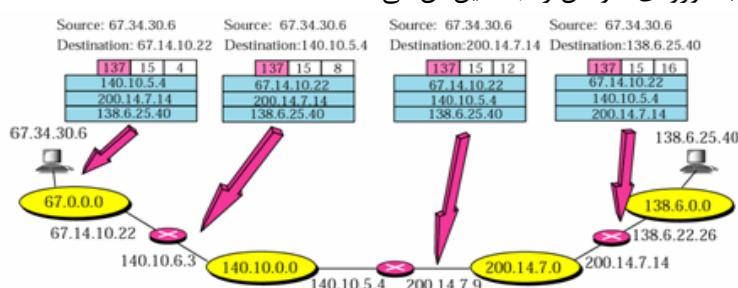
پس از عبور از هر مسیریاب، IP رابط خروجی آن مسیریاب در بسته نوشته می شود. قسمت آدرسها از ابتدای خالی است.



فرمت بسته Strict Source Route



ابتدا IP رابط ورودی از مسیریاب دوم تا مقصد، در بسته ثبت شده است. هر مسیریاب ، IP رابط مسیریاب بعدی را برداشته و IP رابط ورودی خودش را جانشین آن می کند.



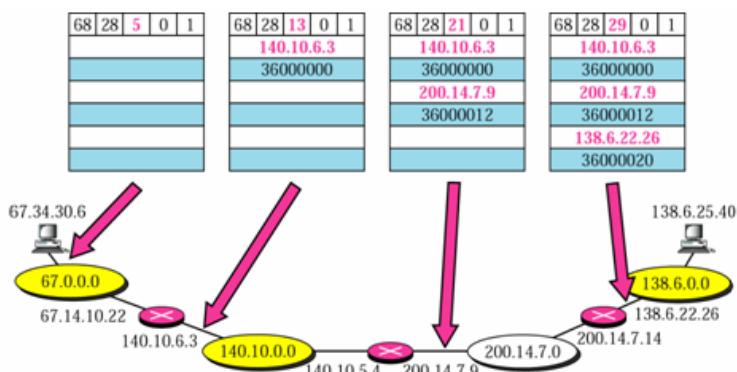
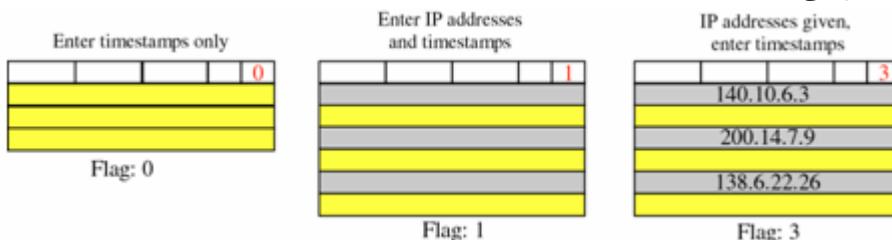
فرمت بسته loose Source Route

Code: 131 1000011	Length (Total length)	Pointer
First IP address (Filled when started)		
Second IP address (Filled when started)		
⋮		
Last IP address (Filled when started)		

فرمت بسته Timestamp

Code: 68 01000100	Length (Total length)	Pointer	O-Flow 4 bits	Flags 4 bits
First IP address				
Second IP address				
⋮				
Last IP address				

در Timesatmp، هر مسیریاب زمان خود را در بسته می نویسد. اطلاعات ثبت شده در هر مسیریاب بوسیله Flag مشخص می گردد.



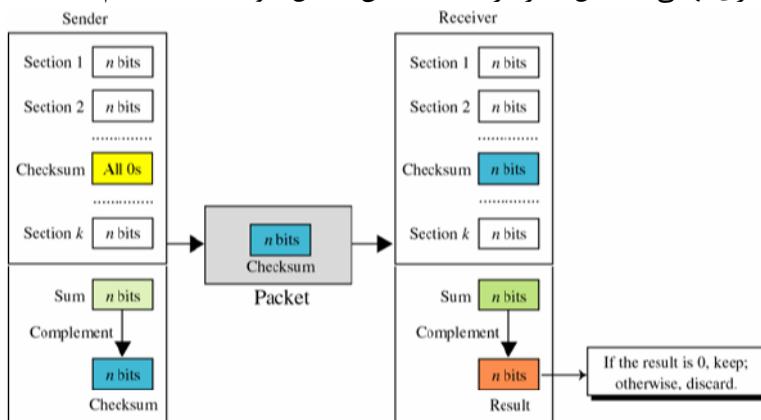
با توجه به فرمت loose source route و Strict source route های Option، تنها Option های Loose source route باشد در همه قطعات کپی شوند و نیازی به کپی کردن سایر Option ها در قطعات، بجز قطعه اول، نمی باشد. همچنین تنها جهت دیباگ و اشکالزدایی مورد استفاده قرار می گیرد و سایرین جهت مقاصد کنترلی مورد استفاده قرار می گیرند.

Checksum

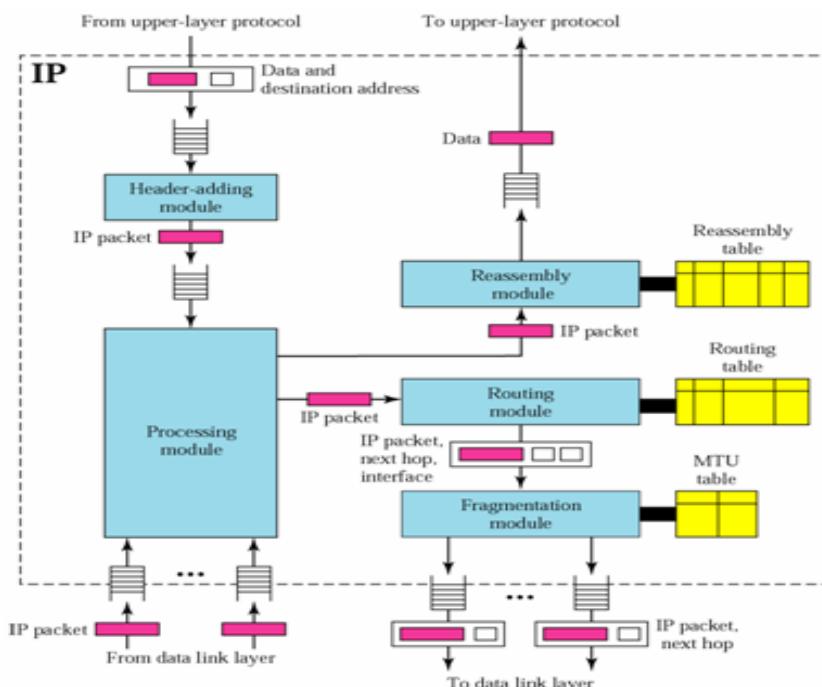
1. تقسیم بسته به k قسمت n بیتی
2. جمع تمام قسمتها با یکدیگر بصورت مکمل یک

۳. مکمل کردن جواب

در ابتدا در سمت فرستنده، مقدار صفر بهChecksum تخصیص داده شده و مقدارChecksum براساس این مقدار بدست می آید و در فیلدChecksum قرار می گیرد. در گیرنده، دوبارهChecksum محاسبه شده و این بار باید پس از مکمل گیری نهایی، حاصل صفر گردد تا اطمینان حاصل شود که بسته سالم است.



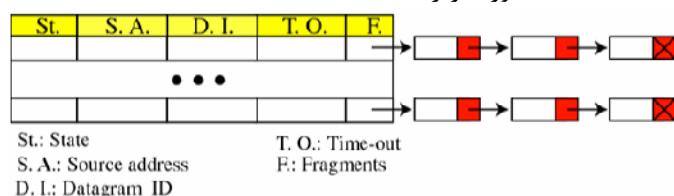
ساختار IP بصورت زیر می باشد:



جدول MTU، حداقل اندازه قسمت داده برای هر رابط را مشخص می کند. طرح جدول MTU بصورت زیر می باشد:

Interface Number	MTU
.....
.....
.....
.....

جدول Reassembly، جهت سرهم کردن قطعات بسته های تکه تکه شده قبل از تحویل به لایه های بالاتر بکار می رود. طرح جدول Reassembly بصورت زیر است:



IPV6

چرا IPV6 مورد لزوم است ؟ آدرس‌های ۳۲ بیتی موجود در IPV4 ، نیازهای کنونی و آینده را برآورده نمی‌کند . (چند بیت از این ۳۲ بیت هم برای HEADER و ... استفاده می‌شود) مثلاً در زمینه موبایلها هم که می‌خواهند از اینترنت استفاده کنند، تخصیص آدرس IP به این گوشیها فعلًا برآورده نمی‌شود .

مزایای IPV6 :

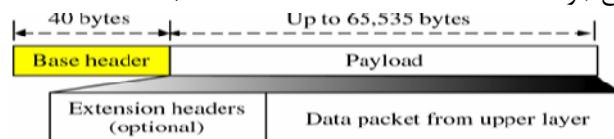
- آدرس ۱۲۸ بیتی است . ۱۰ به توان ۲۳ ضرب در ۶ آدرس برای هر متر مربع از کره زمین یعنی برای هر مولکول یک آدرس می‌تواند اختصاص یابد !!!

- OPTION های زیاد و امکان سریعتر پردازش شدن بسته های IPV6

- امکان آدرس‌های Multi cast

- دادن آدرس‌های IPV6 به صورت Automatic

- پشتیبانی اختصاصی منبع (ICMP V6 = ICMP V4 + IGMP V6)

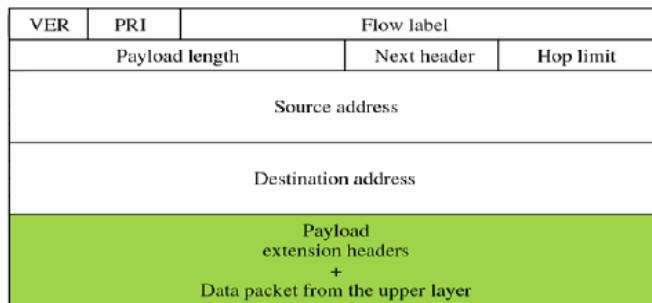


IPV6 Format

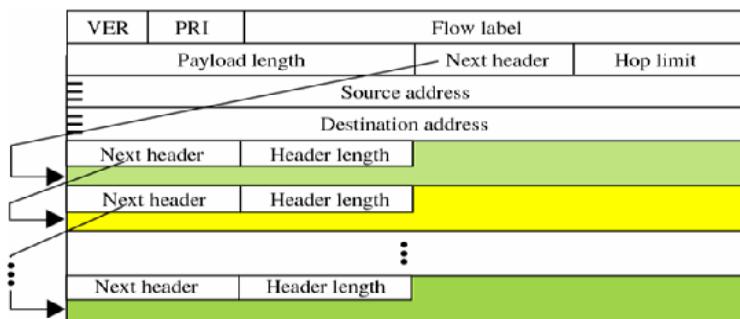
های زیادی در IPV6 می‌تواند وجود داشته باشد :

Autentication H. ,Fragment H. , Routing H . , Hop-to-Hop optional header , Destination option H , Security payload H .

یک دلیل برای اینکه بسته های IPV6 سریعتر پردازش می‌شوند این است که سرآیندهای مختلفی در این بسته ها قرار دارد و با توجه به اطلاعات درون سرآیندها می‌توان پردازش بهتری انجام داد.



Next Header	Code
Hop-by-hop option	0
ICMP	2
TCP	6
UDP	17
Source routing	43
Fragmentation	44
Encrypted security payload	50
Authentication	51
Null (No next header)	59
Destination option	60



• 4 بیت است (برای نمایش عدد 6 و ...).

• کلاس بسته را مشخص می کند (به خاطر اولویت) (8 بیت است).

• مشخص می کند که مسیریاب باید چه سرویسی به این بسته بدهد (20 بیت است).

• Flow label : مشخص می کند که مسیریاب باید چه سرویسی به این بسته بدهد (20 بیت است).

• Payload length : طول کل بسته را مشخص می کند (ماکزیمم طول بسته همان k 64 است . یعنی طول بسته نسبت به Ipv4 تغییری نکرده است) .

• Next header : سرآیند بعدی را مشخص می کند که می تواند سرآیندهای optional (گفته شده در بالا باشد یا سرآیند Tcp باشد . (8 بیت است)

• Hop limit : طول عمر بسته . یعنی بسته چه تعداد hop را می تواند رد کند و از بین نرود (8 بیت است).

• Source add : آدرس مبدأ را مشخص می کند (128 بیت) .

• Dest add : آدرس مقصد را مشخص می کند (128 بیت).

چون به سمت محیط های با کیفیت بالای انتقال می رویم ، احتمالاً سرآیندهای IPV6 دارای CHECKSUM نیستند (کنترل خطای End-toEnd وجود دارد زیرا این کنترل خطای Tcp انجام می شود نه در مسیریابها) .

- امروزه مجموعه ای از بسته ها که خصوصیات مشترکی دارند (مثلاً آدرس مشابه به هم دارند) flow می نامند . اکنون flow مهمنتر از packet processing است .

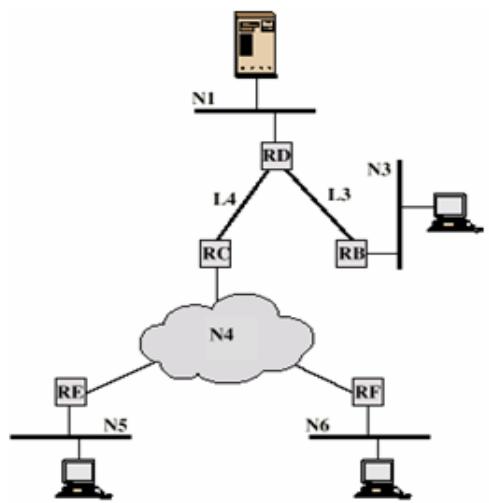
- مثلاً برای انجام یک chat تصویری online ممکن است سه flow وجود داشته باشد flow تصویری : که تصویر را ارسال می کند . صوتی : که صوت را ارسال می کند . text (flow) : عبارات type شده . هرچند که هر سه دارای آدرس های مشابه هستند .

مهمترین مسأله در این مورد شناسائی نوع flow است . مسأله packet classification در باره این موضوع است . در IPV6 یک فیلد برای flow وجود دارد (flow label) . مسیریاب با نگاه کردن به این فیلد ، سرویس مورد نظر را به آن می دهد .

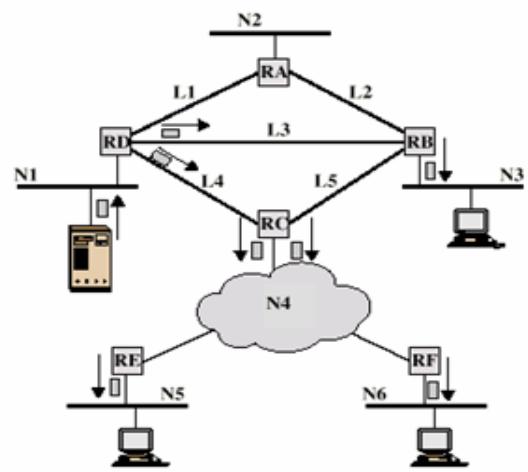
- کمی با موضوع Traffic class : کمی با موضوع flow label تفاوت دارد . مثلاً مشخص می کند که چه مقدار delay یا throughput یا ... مورد نیاز است .

- بدون اینکه بسته copy شود ، چگونه می توان بسته را به مقصد های مختلفی تحویل داد ؟

این موضوع در LAN کاملاً جا افتاده است و ساده است ولی در WAN چون مسیرهای ارتباطی زیادی بین مسیریابها وجود دارد ، کمی مشکل به نظر می رسد (مثلاً در video conference Data base ها یا ... استفاده می شود) برای اینکار باید شبکه را بعنوان یک Spanning Tree بینیم . node ریشه ، ارسال کننده بسته است و نودهای دیگر بعنوان برگها دریافت کننده Multicast هستند .



(a) Spanning tree from source to multicast group



(b) Packets generated for multicast transmission

فصل دا:

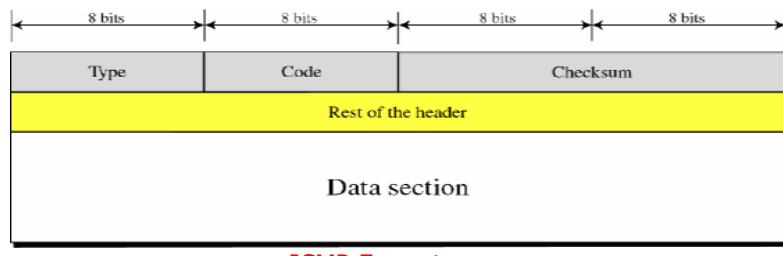
پروتکل های ICMP و IGMP

پروتکلهای ICMP و IGMP در لایه شبکه قرار دارند:



:¹ICMP

این پروتکل وظیفه دارد که چنانچه اتفاقی غیرمنتظره در شبکه اینترنت رخ دهد، آن را گزارش دهد. این پروتکل مستقیماً با IP کار می کند و آن بصورت زیر است :



ICMP Format

TYPE : ۸ بیت است و نوع پیغام را مشخص میکند .

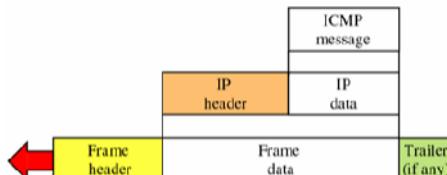
CODE : هشت بیت است و در برخی از پیغام ها پیغام را مشخص تر میکند .

Checksum : ۱۶ بیت است که برای کنترل خطای در بسته ICMP استفاده میشود .

Rest of the header : ۳۲ بیت است و پارامترهای پیغام را مشخص می کند .

بخش اطلاعات : داده ها (که بستگی به نوع پیغام ، مفهوم خاص خود را دارد) (مثلاً ممکن است Address mask باشد)

نحوه قرار گرفتن پیام ICMP در تصویر زیر نمایش داده شده است:



پیامهای ICMP به دو دسته کلی تقسیم می شوند:

- ۷ - گزارش خطای

(Query) - ۸ - پرسوچو

مواردی که پیام های خطای ICMP ارسال نمی گردد:

۱ - پیام های خطای ICMP برای بسته های حاوی پیام خطای ICMP ارسال نمی گردد.

۲ - برای بسته های تقسیم شده، فقط برای قسمت اول پیام خطای ارسال می گردد و برای سایر قسمتها پیامی ارسال نمی گردد.

۳ - پیام خطای برای بسته های با آدرس Multicast ارسال نمی گردد.

۴ - پیام خطای برای آدرس های خاص همانند 127.0.0.0 و ۰.۰.۰.۰ ارسال نمی گردد.

همیشه پیامهای خطای ICMP را به مبدأ گزارش می نماید. انواع این پیام ها عبارتند از:

۱ - مقصد در دسترس نیست(Destination Unreachable)

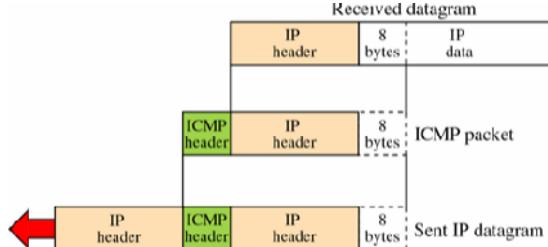
۲ - خاموش شدن منبع(Source Quench)

۳ - تخطی زمانی(Time Exceeded)

۴ - مشکلات پارامتر(Parameter Problems)

۵- تعیین مسیر دوباره (Redirection)

پیامهای خطا علاوه بر نوع و کد موجود در سرآیندشان که نوع پیام را مشخص می نماید، سرآیند IP بسته معیوب و ۸ بایت اول آن را نیز به فرستنده باز می گرداند.



فرمت بسته های مختلف ICMP در ادامه ارائه شده است:

۱- مقصد در دسترس نیست:

Type: 3	Code: 0 to 15	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

این پیام با کد ۲ و ۳ فقط بوسیله میزبان و با سایر کدها فقط بوسیله مسیریاب ایجاد می شود.

مسیریابها توانایی تشخیص تمام مشکلاتی که مانع از تحویل بسته می شود را ندارد و از سوی دیگر مکانیزم کنترل جریان در پروتکل IP وجود ندارد.

۲- خاموش شدن منبع:

Type: 4	Code: 0	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

این پیام می تواند جهت هر Datagram ی که در اثر تراکم، چه در مسیریاب و چه در میزبان، دور ریخته می شود، تولید گردد. منبع به این ترتیب در جریان دور ریخته شدن بسته ها بدلیل تراکم شده و باید سرعت ارسال Datagram ها را تا برطرف شدن تراکم، کاهش دهد.

۳- تخطی زمانی:

Type: 11	Code: 0 or 1	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

این پیام در مسیریاب برای بسته هایی ارسال می گردد که فیلد TTL آنها صفر شده است(کد صفر) و باید دور ریخته شوند. همچنین اگر مقصد در بازه زمانی مشخص، همه قسمتهای یک داده تقسیم شده را دریافت نکند، داده های دریافتی را دور ریخته و یک پیام تخطی زمانی به مبدأ ارسال می کند(کد یک).

۴- مشکلات پارامتر:

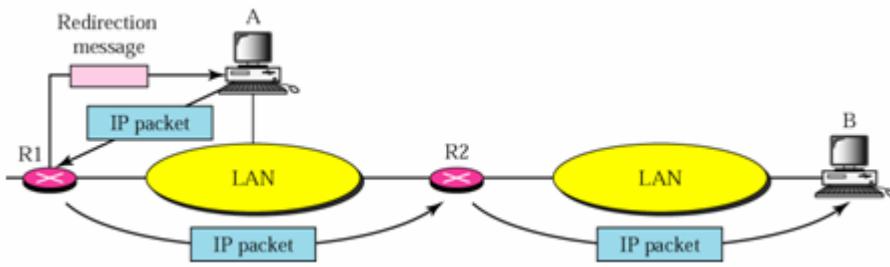
Type: 12	Code: 0 or 1	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

این پیام می تواند توسط یک مسیریاب یا مقصد تولید گردد. کد صفر نشانگر مشکل در سرآیند و کد یک نشانگر مشکل در فیلد Option می باشد. در این پیام یک اشاره گر در فیلد بدون استفاده پیام قرار می گیرد.

-۵- تعیین مسیر دوباره:

Type: 5	Code: 0 to 3	Checksum
IP address of the target router		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

یک میزبان در ابتدا کارش را با یک جدول مسیریابی کوچک شروع می کند و در ادامه این جدول کامل تر شده و بروز می گردد. یکی از ابزارهای کمک به این مهم، پیام تعیین مسیر دوباره می باشد. در حالتیکه میزبان مسیر انتخابی را برای ارسال بسته ها انتخاب کند، مسیریاب محلی دریافت کننده پیام، با یک پیام تعیین مسیر دوباره، ضمن اعلام IP مسیریاب صحیح، به فرستنده اشتباہ بودن مسیر انتخابی را متذکر می شود.



کد ۱

کد ۲

Network Specific(Specified Service):۳

کد ۴

مسیریاب این پیام را فقط برای میزبانهای شبکه محلی خودش می فرستد.

پیامهای پرسوچوی ICMP شامل موارد زیر می باشد:

۱- درخواست و پاسخ Echo

۲- درخواست و پاسخ Time Stamp

۳- درخواست و پاسخ Mask آدرس

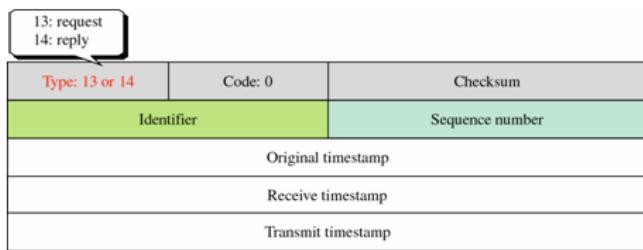
۴- تقاضای مسیریاب و اعلان (Solicitation & Advertisement)

این پیامها جهت بررسی وضعیت شبکه مورد استفاده قرار می گیرند.

۱- پیام درخواست Echo می تواند توسط یک میزبان و یا مسیریاب در شبکه ارسال گردد و مسیریاب یا میزبان دریافت کننده پیام، آن را بوسیله یک پیام پاسخ Echo جواب می دهد. این پیامها می توانند توسط مدیر شبکه جهت بررسی عملکرد پروتکل IP مورد استفاده قرار گیرند. اکثر اوقات دستور Ping به این منظور مورد استفاده قرار می گیرد.

8: Echo request 0: Echo reply		
Type: 8 or 0	Code: 0	Checksum
Identifier		Sequence number
Optional data Sent by the request message; repeated by the reply message		

-۲- پیام درخواست و پاسخ Time Stamp می تواند جهت محاسبه RTT بین یک مبدأ و یک مقصد حتی در حالت عدم همزمانی بین آنها بکار رود.



جهت محاسبه RTT بشكل زیر عمل می شود:

Sending time = value of receive timestamp - value of original timestamp

Receiving time = time the packet returned - value of transmit timestamp

Round-trip time = sending time + receiving time

Time difference = receive timestamp - (original timestamp field + one-way time duration)

برای نمونه مقادیر زیر را در نظر بگیرید:

Value of original timestamp: 46

Value of receive timestamp: 59

Value of transmit timestamp: 60

Time the packet arrived: 67

Sending time = $59 - 46 = 13$ milliseconds

Receiving time = $67 - 60 = 7$ milliseconds

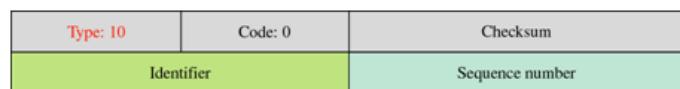
Round-trip time = $13 + 7 = 20$ milliseconds

Time difference = $59 - (46 + 10) = 3$

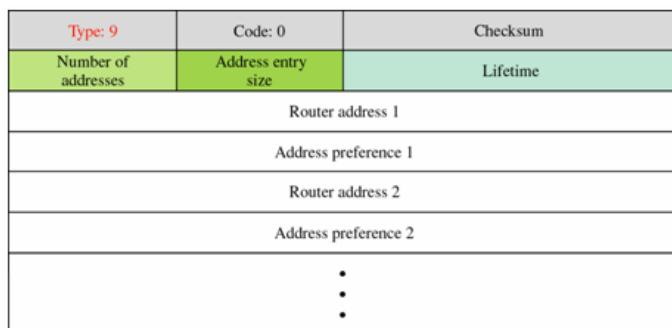
-۳- درخواست و پاسخ Mask آدرس:



-۴- تقاضای مسیریاب:

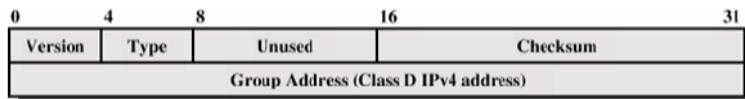


-۵- اعلان :



: IGMP

- پروتکل IGMP، یک پروتکل مدیریت گروه است که به مسیریابهای Multicast می‌کند تا لیستی از اعضای ثابت مرتبط با هر رابط مسیریاب را ایجاد و بروز رسانی نماید. فرمت کلی پیام‌های این پروتکل بشکل زیر می‌باشد:



IGMP Format

Version=1 -

Type - مقدار صفر دارد اگر Host گزارش بدهد و یک است اگر مسیریاب یک درخواست ارائه نماید.

Group Address - برای پیام‌های درخواست صفر و در غیر این صورت آدرس یک گروه معتبر است.

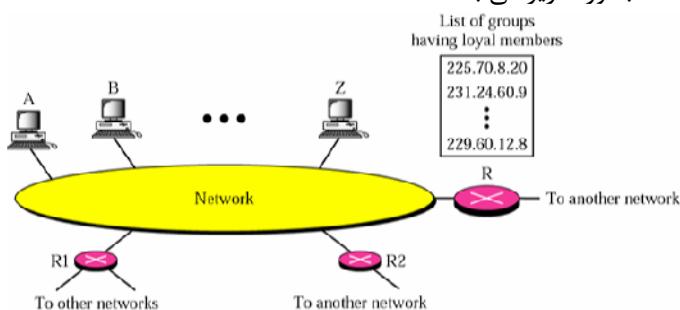
انواع پیامهای IGMP

۱. گزارش عضویت(Membership Report)

۲. گزارش ترک(Leave Report)

۳. برسوچو: شامل دو نوع عام(General) و خاص(Special). وجه تمایز این دو پیام در آن است که در نوع عام مقدار فیلد آدرس گروه صفر است.

عملکرد کلی IGMP بصورت زیر می‌باشد:



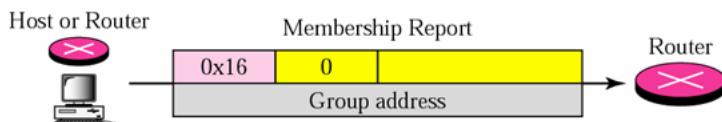
- میزبان برای افزوده شدن به یک گروه، پیام‌های گزارش عضویت را ارسال می‌نمایند. این پیام دو بار و پشت سرهم ارسال می‌گردد.

• آدرس گروه مورد درخواست جهت افزوده شدن.

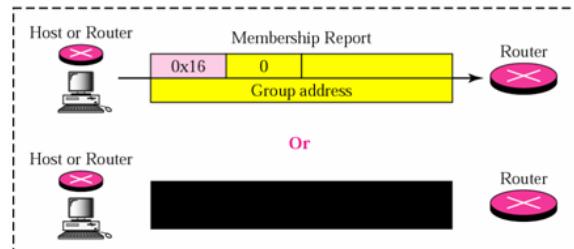
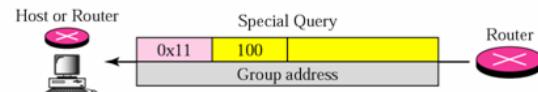
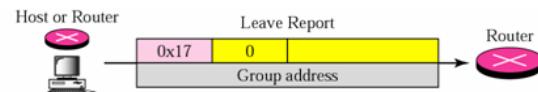
• در IP Datagram این آدرس همانند آدرس مقصد multicast است.

• همه host‌های در یک گروه پیام را دریافت می‌کنند.

• مسیریابها برای دریافت تمام گزارش‌ها، به همه آدرس‌های multicast گوش می‌کنند.



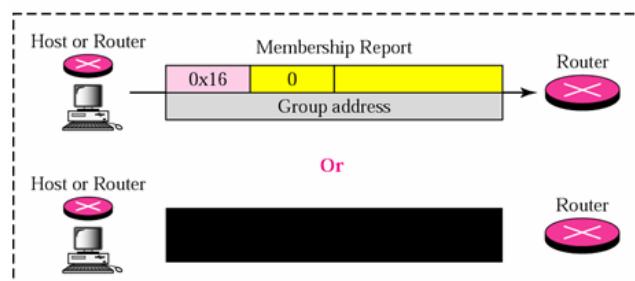
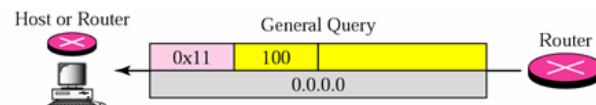
- میزبان برای حذف شدن از گروه از پیام ترک گروه استفاده می‌کند. سرور جهت اطمینان از صحت پیام ترک دریافته، یک پیام پرسوچوی خصوصی به میزبان می‌فرستد و میزبان در صورت نیاز به ماندن در گروه یک پیام عضویت را ارسال خواهد کرد؛ و گرنه از گروه حذف خواهد شد.



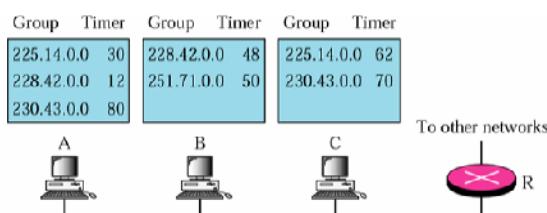
- مسیریابها بصورت دوره ای پیام های پرسجودی عام را منتشر می کنند.

- درخواست برای تمام میزبان ها بصورت Multicast ارسال می شود.

- میزبان های متقاضی باقیماندن در گروه باید همه پیام های ارسالی به همه میزبان ها را خوانده و با ذکر گروه هایی که عضو آنست به آنها پاسخ دهد.



مثال: شبکه ای با سه میزبان و یک مسیریاب در نظر بگیرید. در زمان صفر یک پیام پرسجود به میزبانها می رسد. هر میزبان یک مقدار تصادفی به تایمر هر مدخل جدول عضویتش می دهد. توالی پاسخ های ایستگاه ها را مشخص نمائید.



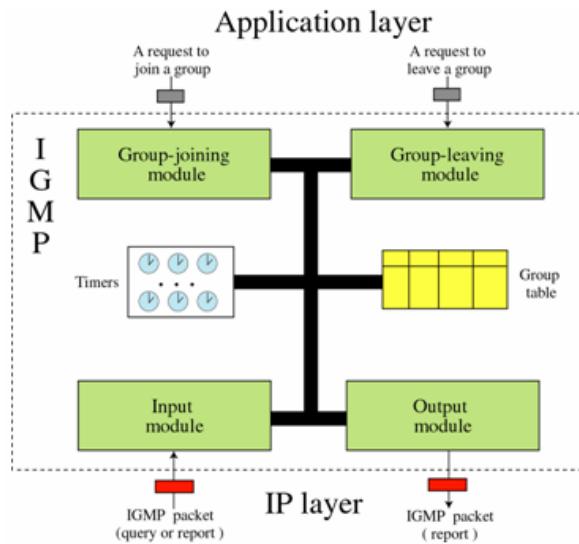
زمان ۱۲: تایمر آدرس 228.42.0.0 در میزبان A به پایان رسیده است و این میزبان یک پیام عضویت را ارسال می کند که بواسیله مسیریاب و همه میزبانها دریافت می گردد. میزبان B تایم خود برای این آدرس را لغو می نماید.

زمان ۳۰: تایمر آدرس 225.14.0.0 در میزبان A به پایان رسیده است و این میزبان یک پیام عضویت را ارسال می کند که بواسیله مسیریاب و همه میزبانها دریافت می گردد. میزبان C تایم خود برای این آدرس را لغو می نماید.

زمان ۵۰: تایمر آدرس 251.70.0.0 در میزبان B به پایان رسیده است و این میزبان یک پیام عضویت را ارسال می کند که بوسیله مسیریاب و همه میزبانها دریافت می گردد.

زمان ۷۰: تایمر آدرس 230.43.0.0 در میزبان C به پایان رسیده است و این میزبان یک پیام عضویت را ارسال می کند که بوسیله مسیریاب و همه میزبانها دریافت می گردد. میزبان A تایم خود برای این آدرس را لغو نماید.

بسته IP حامل پیام IGMP دارای مقدار ۲ در فیلد پروتکل و مقدار ۱ در فیلد TTL خود می باشد. ساختار IGMP بشكل زیر می باشد:



ساختار جدول گروه نیز بشكلي زير می باشد:

State	Interface No.	Group Address	Reference Count
.....
.....
.....

State: Free, Delaying, Idle

Reference Count: Number of processes interested

يعنى در IPV6 دیگر IGMP وجود ندارد و ICMP V6 = ICMP V4 + ICMP V6 کار هر دو را انجام می دهد .

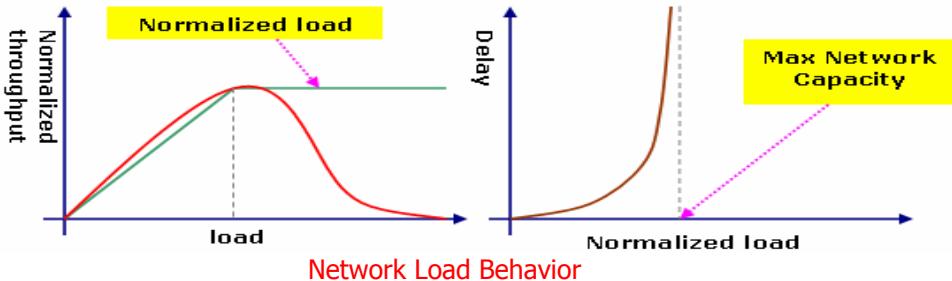
فصل ۱۱:

کنترل اتصالات در شبکه

استفاده بهینه از شبکه ها :

الگوریتم مسیریابی نقش مهمی در استفاده در از شبکه ها دارد ولی کنترل ترافیک هم از موارد مورد توجه است. باید مواطبه باشیم که تراکم پیش نباید و اگر اتفاق افتاد روش حل آن چیست.

اگر بسته ارسالی در یک شبکه زیاد شود از یک حد، بسته های دریافتی هم از یک حد فراتری رود ولی این بسته به صورت ایده آن است در عمل وقتی بسته های ارسالی بسیار زیاد شود. بسته های دریافتی هم می توانند کم شود.



يعنى اگر بسته های ارسالی زیاد شود، تاخیر بی نهایت می شود پس به طور کلی تراکم باعث افزایش تاخیر و کم شدن بسته های دریافتی می شود.

سیاستهای ترافیک :

۱- اگر نتوان بسته را ارسال کرد باید بافر شود. باید دو نوع بافر داشته باشیم: بافر ارسال و بافر دریافت هنگام اتفاق افتادن تراکم، بالاخره بسته هایی باید دور ریخته شوند و باید باز باید فرستاد شود. پس ممکن است باز هم باعث ایجاد تراکم شود پس راه حل خوبی نیست.

۲- اگر تراکم ایجاد شود. باید کنترل تراکم باعث بالا رفتن ترافیک شبکه می شود. کنترل تراکم به سه روش انجام می شود

(الف) آگاه کردن مبدأ تا بسته های کمتری بفرستد.

(ب) تغییر مسیر به وسیله الگوریتمهای مسیریابی

(ج) از بسته های اندازه گیری END-TO-END استفاده شود.

• برای اندازه گیری تاخیر می توان یک بسته به مقصد ارسال کرد و Delay رفت و برگشت را اندازه گرفت. اگر این Delay از یک حدی بیشتر شد، می فهمیم که تراکم پیش آمده است. ولی چون بسته های کنترلی فرستاده می شود، خودش باعث تراکم می شود.

• روش دیگر این است که اطلاعات کنترلی در خود داده قرار می گیرد که این روش سربار کمتر دارد (مانند بیتهاي BECN/FECN در شبکه Frame RELAY).

در هر لایه تصمیمات می تواند باعث کنترل تراکم شود و می توان کنترل ترافیک انجام داد (يعنى فقط در لایه شبکه کنترل ترافیک انجام نمی شود).

مثلا در لایه پیوند داده ها سیاست های زیر می تواند در تراکم نقش داشته باشد:

۱. سیاست انتقال مجدد

۲. سیاست CACHE

۳. سیاست ACK

۴. سیاست کنترل FLOW

در سیاست انتقال مجدد اگر TIMEOUT کوچک باشد می تواند باعث تراکم شود.

سیاست CACHE : بسته هایی که اخیراً رسیده اند را نباید فوری از داخل CACHE پاک کرد بلکه ممکن است دوباره مورد نیاز باشند .

سیاست ACK: اگر هر بسته را زود ACK کند ، باعث تراکم می شود . به جای این کار می توان ۱۰ بسته را گرفت و بعد یک ACK فرستاد . پس سایز پنجره می تواند در کنترل مهم باشد .

سیاست کنترل FLOW: اینکه از کدام روش استفاده می شود عامل مهمی است .

عوامل دیگر :

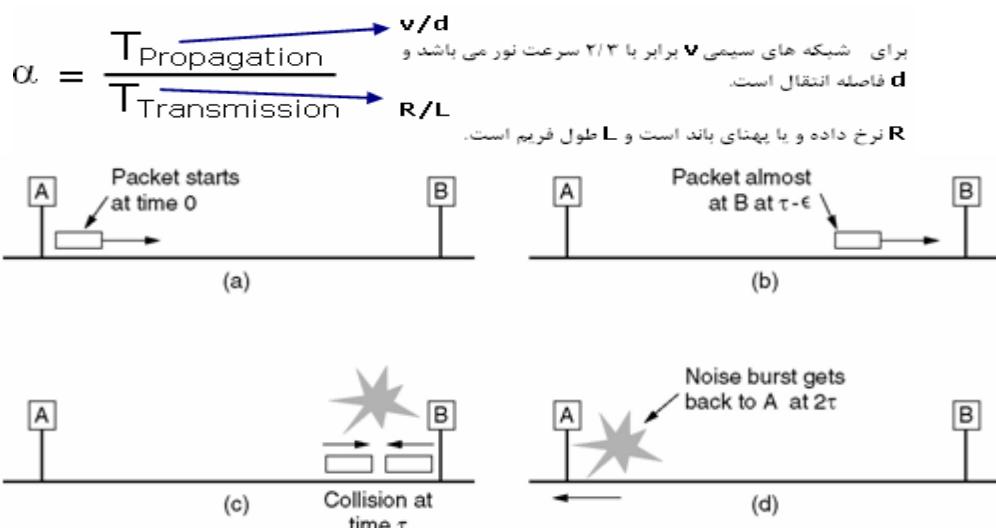
اگر الگوریتم مسیریابی هوشمند نباشد تراکم بالا می رود .

طول عمر بسته مهم است زیرا با سپری کردن طول عمر بسته ، بسته از بین می رود پس طول عمر نباید زیاد کوچک باشد . روش ارسال بسته ها ROUND ROBIN و روشن DISCARD کردن بسته ها مهم است .

پروتکل های دسترسی به محیط انتقال مشترک:

در شبکه های 100BASE T4 از ۴ سیم به جای یک سیم استفاده می شود (در T4) . این کار به خاطر افزایش سرعت انجام می شود . یک روش برای افزایش سرعت این است که در یک سیگنال تعداد بیت های بیشتری ارسال شود تا از پنهانی باند موجود بیتها بیشتری ارسال شود . روش دیگر استفاده از چند سیم به جای یک سیم است . در T4 یک سیم مخصوص رفت است و یک سیم مخصوص برگشت و دو سیم دیگر به صورت رفت و برگشت است یعنی سرعت را ۳ برابر می کند .

نکته مورد توجه این است که با افزایش سرعت باید فاصله را کاهش دهیم . در شبکه های LAN عددی وجود دارد (D) که باید در محدوده قابل قبولی باشد .

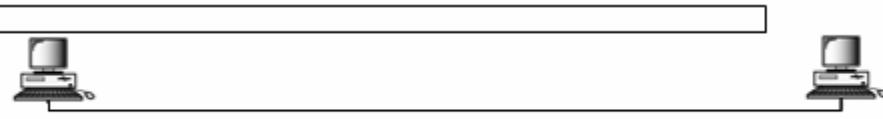


Collision detection can take as long as 2τ .

اگر D بسیار بزرگ باشد به خاطر مسئله حداقل طول فریم ، ممکن است در شبکه اشکال رخ دهد .



در شکل فوق ممکن است اشکال رخ دهد زیرا اگر B به کanal گوش کند می بیند که خط اشغال نیست (در B) بنابراین می تواند بسته بفرستد و در صورت ارسال بسته ممکن است با بسته ارسالی از طرف A برخورد کند . ولی در شکل زیر مشکلی به وجود نمی آید .

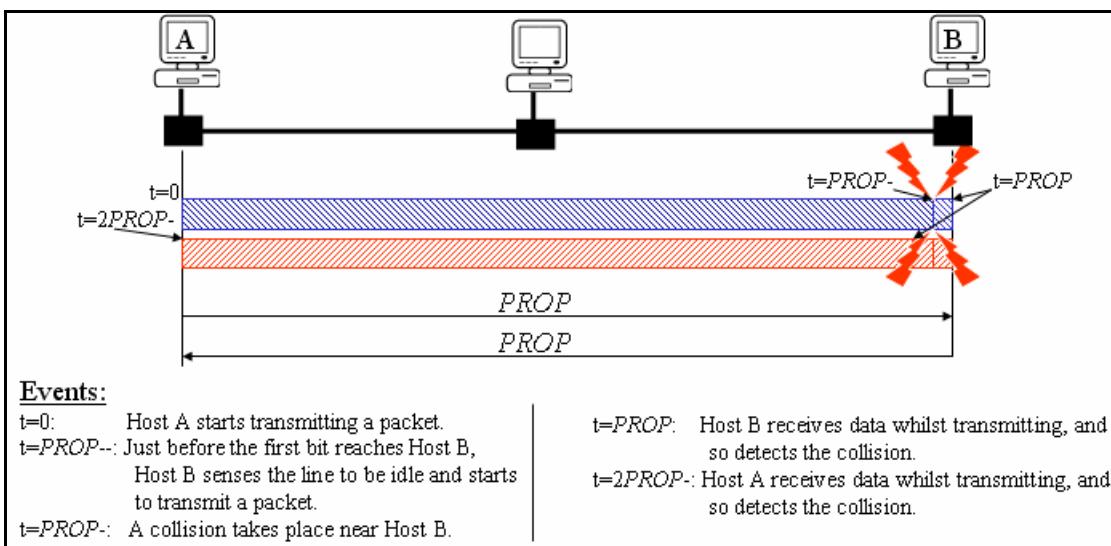


Terminator

پس در شبکه ۱ با اینکه بسته تمام شده است اگر تصادف رخ دهد کشف نمی شود ولی در ۲ می توان کشف کرد. در شبکه های RING یک TOKEN RING وجود دارد که همه Station به این RING وصل می شوند. همچنین یک Token وجود دارد که هر کامپیوتری که این TOKEN را در اختیار داشته باشد، می تواند بسته هایش را ارسال کند. یکی از Station ها هم به صورت ناظر عمل می کند.

در شبکه های LAN UTILIZATION در شبکه های LAN بستگی به $U = 1/(a+1)$ دارد. هر چه a کمتر باشد لبیستر است، و یا a برای توان زیر کوچک در نظر گرفت.

در شبکه های LAN همواره می توان انتظار برخورد بسته های داده ارسالی توسط نودهای شبکه با یکدیگر را داشت.(Collision).



برای اینکه مطمئن شویم که یک بسته بدون هیچگونه تصادمی ارسال می شود، سیستم های میزبان باید قبل از اتمام ارسال بسته قادر به تشخیص تصادم باشند. برای اینکه سیستم میزبان بتواند قبل از اتمام ارسال بسته، تصادم را تشخیص بدهد نیازمند آییم که حداقل طول بسته مشخص باشد:

$$TRANSP > 2 * PROP$$

از سوی دیگر داریم:

$$PROP_{max} = d/c$$

که در آن d طول مسیر انتقال بسته در شبکه و c سرعت انتقال در محیط فیزیکی شبکه است. برای شبکه های سیمی مقدار c بین 2×10^8 تا 2.5×10^8 متر بر ثانیه درنظر گرفته می شود. به عنوان نمونه برای یک فاصله ۱۵۰۰ متری و سرعت شبکه ۱۰ مگابیت بر ثانیه ای، حداقل طول بسته بصورت زیر محاسبه می شود:

$$PROP_{max} = d/c = 1500/2.5 \times 10^8 = 6\mu s$$

$$TRANSP > 2PROP = 12\mu s$$

$$\text{Packet Size} \geq (12\mu s) * 10Mb/s = 120 \text{ bits}$$

زمان ارسال داده ها نیز بصورت زیر محاسبه می شود:

$$\text{Transmission Time} = TRANSP + \text{wasted time between packets}$$

اگر P را احتمال تصمیم گیری یک نod برای انتقال بسته یا عدم ارسال بسته در یک بازه زمانی فرض

کنیم، بهترین توان کاری (p) برای شبکه بصورت زیر محاسبه می گردد:

$$\alpha(p) = \binom{N}{1} p(1-p)^{N-1}$$

$$\frac{d\alpha}{dp} = N(1-p)^{N-1} - pN(N-1)(1-p)^{N-2}$$

$$a_{max} \approx 36\% \approx 40\% \quad \text{When} \quad p=1/N$$

در این حالت تعداد واحد زمانی زمان تلف شده قبل از ارسال موفقیت آمیز یک بسته برابر است با:

$$A = (a * 0) + (1-a)(1+A)$$

$$a = a_{max} ==> A = 1.5$$

$$\text{Transmission Time} = \text{TRANSP} + 1.5 (2 * \text{PROP})$$

$$\text{Transmission Time} \approx \text{PROP} = d/c \quad (1)$$

از سوی دیگر زمان انتقال را می توان بصورت نسبت پهنهای باند شبکه به طول بسته های ارسالی نیز

تعریف نمود:

$$\text{Transmission Time} = \text{Network Bandwidth} / \text{Frame Length} \quad (2)$$

بنابراین با توجه به (۱) و (۲) می توان گفت زمان صرف شده برای انتقال داده ها در شبکه ای با فاصله d ، برابر است با نسبت پهنهای باند شبکه به طول فریم های ارسالی در شبکه.

پارامترهای محاسبه شده در این قسمت در تکنیک CSMA/CD در LAN کاربرد دارند.

لایه حمل و نقل :

- قابل اطمینان (مانند X.25 , Framerelay lan) : لایه حمل و نقل نسبتاً ساده است.
- غیر قابل اطمینان (اینترنت و پروتکل IP) : لایه حمل و نقل پیچیده است زیرا تغییرات زیادی در اثر این لایه بوجود می آید .

برای توصیف سرویس های مختلف مسائل زیر وجود دارند :

۱- نوع سرویس :

- Datagram : Connection-Less
 - استفاده دارد . مانند UDP و چند رسانه ای .
 - Connection -Oriented
 - ۱. ایجاد اتصال
 - ۲. انتقال داده ها
 - ۳. اتمام اتصال

که در انتقال Reliable داده مورد نیاز است . مانند TCP و E-mail .

۲- کیفیت سرویس (QoS) هم در Connection-Less و هم در Connection -Oriented است و هم در

(Connection -Less) در دست دادن آن (

- خطأ و میزان از دست دادن آن (در Connection -Less)
 - تأخیر ماکزیمم و متوسط مطلوب
 - گذردگی متوسط و مینیمم
 - سطوح اولویت

- تأخیر ایجاد اتصال (در Connection -Oriented)

- احتمال باز نشدن اتصال (بعد از گذشت ماکزیمم زمان تأخیر هنوز اتصال برقرار نشود)

- زمان متوسط انتقال بسته از مبدأ به مقصد

- نسبت بسته های خراب شده به کل بسته ها (Residual error rate)

- احتمال قطع شدن اتصال بدون درخواست کاربران (Resilience)

برخی از سرویسها نیاز به گذردهی بالا دارند و قابل اطمینان زیاد مانند E-mail, FTP نیاز به سطوح مختلف اولویت دارد. یک کاربرد ممکن است تاخیر کم بخواهد.

۳- انتقال داده ها : نحوه انتقال داده بین دو کاربر به سه صورت است :

- (SX) Simplex •
- (HDX) Halfduplex •
- (FDX) Fullduplex •

با کاربر : Interface-۴

- از طریق صدا زدن Procedure

- از طریق Interrupt

DMA-

۵- مدیریت (ارتباط) : ایجاد اتصال به دو صورت است :

- متقارن : در هر دو طرف فرستنده و گیرنده ، هر دو با امتیاز یکسان تقاضای ایجاد اتصال می کنند.
- نامتقارن : یکی شروع کننده ایجاد اتصال است (Active Open) و دیگری در حالت listen و آماده برقراری ارتباط است (Passive Open).

قطع ارتباط (مربوط به مدیریت ارتباط است) :

- Graceful (ملایم) : زمانی که ارتباط قطع شده است ، هنوز هم گیرنده می تواند داده ها را تا انتهای تحویل بگیرد .

این داده ها پس از قطع ارتباط رسیده است ولی پذیرفته می شود .

- Abrupt- (تند) : زمانی که ارتباط قطع شده است هیچ داده ای را نمی پذیرد .

۶- تحویل فوری :

باید لایه حمل و نقل امکاناتی را فراهم کند که داده هایی را که اهمیت زیادی دارند بتوانند سریعتر ارسال و دریافت شوند .

۷- گزارش وضعیت : امکان دادن گزارش فراهم باشد :

- مشخصات کارایی یک انتقال (گذردهی ، متوسط تأخیر و ...)

- آدرسها (شبکه و حمل و نقل)

- نوع پروتکل در حال استفاده

- مقدار جاری تایمراهی مختلف لایه حمل و نقل

- حالات مختلف پروتکل

۸- ایمنی :

امکان رمز گذاری و کنترل دسترسی و مسیریابی از طریق مسیرهای امن برقرار باشد .

یکی از موضوعات مهم SSL است (Secure Socket Layer) . که ایمنی یک سایت را باعث می شود (سایتها تجارتی بیشتر به این موضوع نیاز دارند).

مکانیزمهای پروتکل در مورد شبکه های مطمئن (Ian 802.3 , Famerelay , x.25) :

به هر حال به دلیل مرتب رسیدن و سالم رسیدن ، کار لایه حمل و نقل بسیار ساده تر از حالتی است که شبکه زیرین Connection-Less باشد .

- آدرس دهی (وقتی که لایه زیرین C-oriented باشد) :

(Transport Service Accses Point) TSAP یا کاربر : پورت ID

حمل و نقل (..., TCP, UDP) ID

آدرس ایستگاه (آدرس Host)

شماره شبکه (آدرس شبکه)

چگونه لایه حمل و نقل مبدأ آدرس لایه حمل و نقل مقصد را پیدا می کند؟

۱- لایه حمل و نقل قبل از ارسال آدرس مقصد را کاملاً داشته باشد.

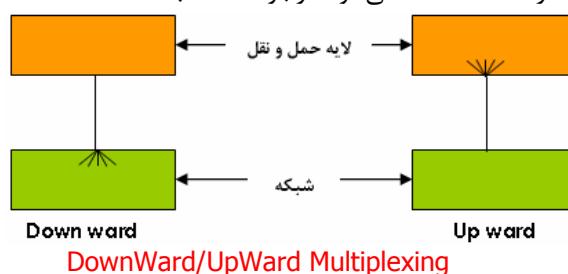
۲- سرویس هایی که دائماً استفاده می شوند، مشهور هستند (با شماره پورت خاص صدا زده می شوند).

۳- ایجاد نام های سرور: سرویس ها با نام Generic صدا زده می شوند و سرور وظیفه پیدا کردن

سرویسها از طریق نام سرور را داشته باشد.

مالتی پلکس:

به دو صورت upward و downward می تواند وجود داشته باشد.

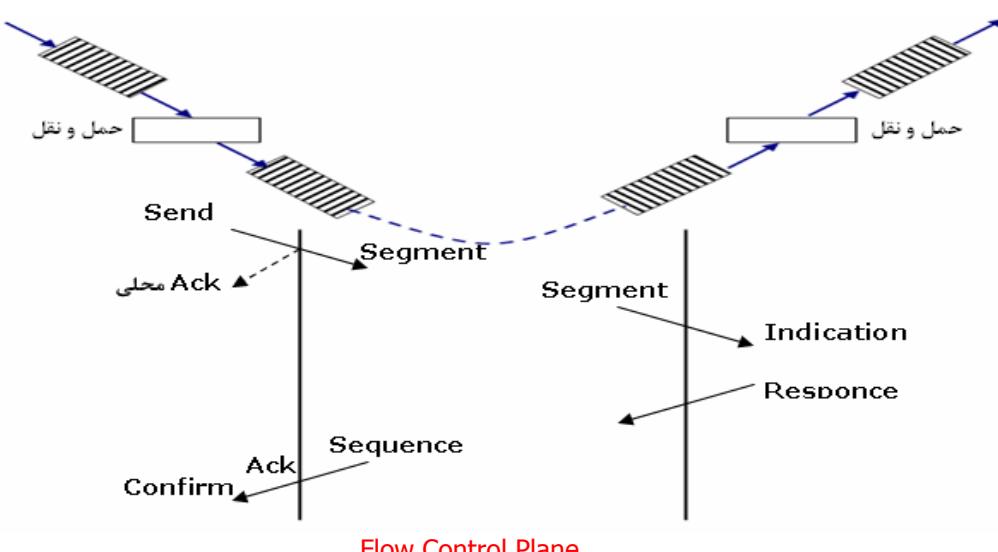


Downward/Upward Multiplexing

در Upward، چندین سرویس لایه حمل و نقل که گذردهی پائین دارند از طریق یک کانال مجازی $x.25$ ارسال می شوند. در Downward، یک کاربرد لایه حمل و نقل به دلیل زیاد بودن گذردهی (Throughput) از چند کانال مجازی انتقال صورت می گیرد. هر یک، یک کانال مجازی $x.25$ باشد.

کنترل FLOW:

به هر حال صفاتی زیادی در لایه حمل و نقل وجود دارد که در صورت تراکم باید با آنها برخورد مناسب صورت بگیرد.



Flow Control Plane

حداقل ۴ صفت وجود دارد.

چهار روش برای رفع نیاز کنترل Flow در لایه حمل و نقل می تواند وجود داشته باشد:

- ۱- کاری انجام نگیرد (قطعه های زیادی از بافرها دور ریخته می شوند و ارسال کننده چون ACK دریافت نمی کند دوباره بسته را می فرستد (به جای قطعه های جدید ، قطعه های قدیمی ارسال می شوند) .
- ۲- جلوی دریافت قطعه های بعدی را بگیرد (وقتی بافر پر است دریافت قطعه های جدید صورت نمی گیرد).

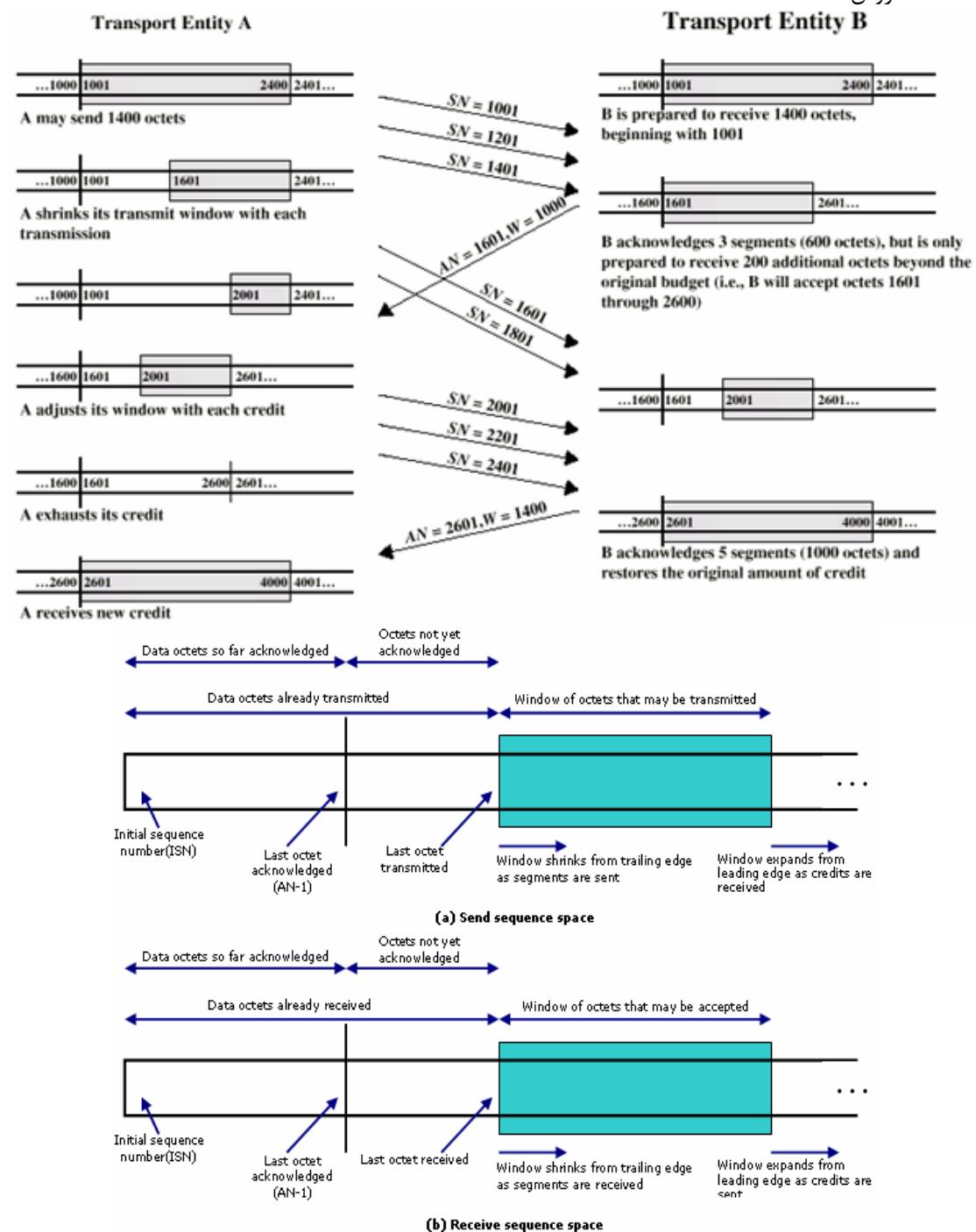
۳- پروتکل ثابت پنجره های افزان (Sliding Window):

- استفاده از seqno

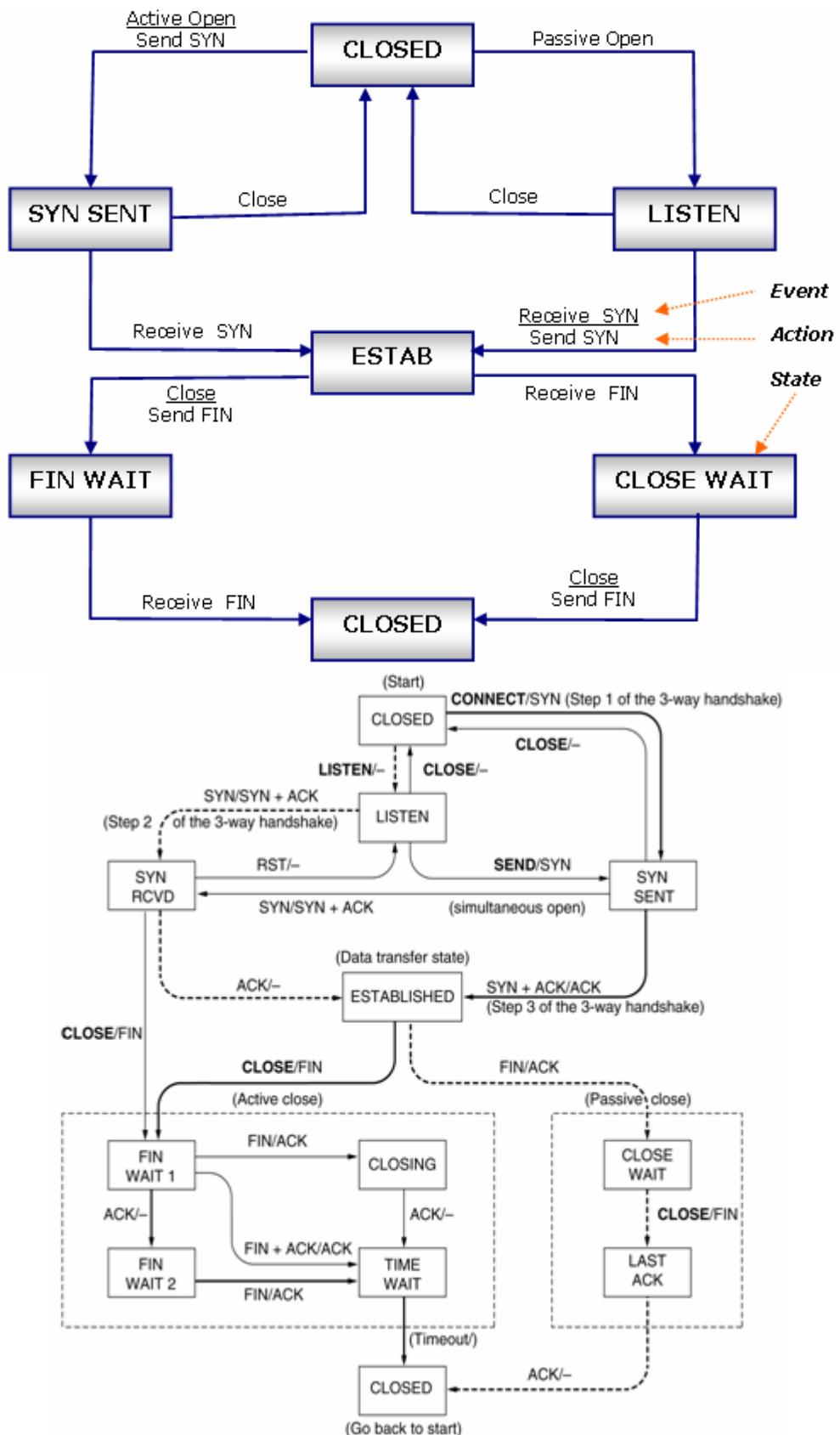
- استفاده از ACK برای جلو بردن پنجره

- استفاده از پنجره

۴- روش Credit:



ایجاد و اتمام اتصال (در مورد شبکه های reliable و لایه حمل و نقل)



اهداف اصلی :

- امکان فراهم آوردن پارامترهایی از قبیل طول قطعه ، طول پنجره و QoS و ...
- تیریگر کردن منابع حمل و نقل (بافرها ورودی به جداول اتصال و ...)

ایجاد اتصال :

در ابتدا کاربر لایه حمل و نقل در وضعیت CLOSE است (اتصال بازی وجود ندارد) . با استفاده از یک فرمان Passive open مشخص میکند که به صورت Passive آماده باز کردن یک اتصال است (از طرف سرور) . کاربر ممکن است با یک فرمان close عقیده اش عوض شده و به وضعیت close برود .

بعد از ارسال فرمان کاربر به حالت Listen می رود یعنی آماده است که به فرمان اتصال از طرف دیگر گوش داده و اتصال باز ایجاد نماید . از طرف Client کاربر می تواند با ارسال فرمان Active Open به وضعیت Syncsent برود (و در این وضعیت اگر عقیده اش عوض شود به حالت close برگردد) و قطعه SYNC را بفرستد که این قطعه به موجودیت طرف مقابل (سرور) رسیده و به معنی یک Req برای ایجاد اتصال می باشد . اگر مقصد در حالت listen بود این SYNC را دریافت کرده و به وضعیت ایجاد اتصال رفته و یک فرمان SYNC نیز ارسال می نماید . بعد از دریافت SYNC ، سرور ۳ کار نجام می دهد :

۱-سیگنال دادن به کاربر که یک اتصال باز آماده است .

۲-ارسال SYNC به لایه حمل و نقل طرف دیگر (Client) جهت تأیید اتصال .

۳-قرار دادن اتصال در وضعیت Established .

زمانی که SYNC به طرف دیگر (Client) رسید او نیز به حالت ایجاد اتصال می رود . زمانی که یک فرمان Close از هر طرف دریافت شد به وضعیت Close برمی گردد .

قطع اتصال :

به دو صورت است : Abrupt , graceful

در شبکه Reliable به صورت graceful است :

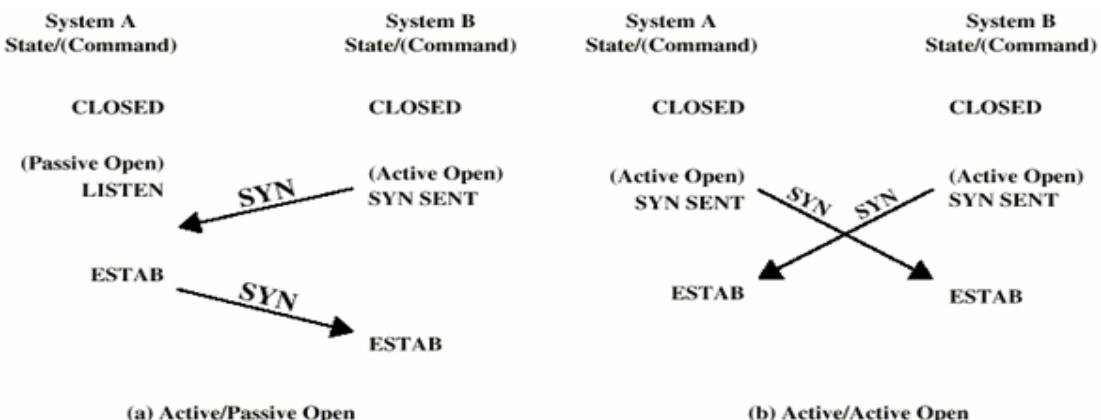
• طرف Client : در پاسخ به فرمان close کاربر یک قطعه بنام Fin به طرف دیگر ارسال می کند . بعد از ارسال Fin وضعیت به Finwait تغییر می کند (در این حالت لایه حمل و نقل کماکان دریافت داده ها را قبول می کند (graceful) .

زمانی که Fin از طرف دیگر آمد قطع ارتباط انجام گرفته و به کاربر اطلاع داده می شود .

• طرف Server : وقتی که Fin دریافت شد اتصال به وضعیت close wait می رود در این حالت داده از کاربر قبول می شود و به سمت دیگر ارسال می شود (graceful)

وقتی که کاربر فرمان close را صادر کرد لایه حمل و نقل در پاسخ یک Fin می فرستد و اتصال قطع می شود . در شکل زیر ، ایجاد اتصال بین سرور و client را نشان می دهد :

الف - در ابتدا A,B در وضعیت CLOSE هستند .



ب - در ابتدا A,B در وضعیت Active باشند (هر دو به صورت همزمان می خواهند در ایجاد اتصال به صورت فعال شرکت کنند)

یعنی در این حالت هر دو به حالت syncsent می‌روند و حالت Listen وجود ندارد. یه حمل و نقل برای لایه شبکه Unreliable, Connection-Less : (مثلاً لایه شبکه IP باشد) در این حالت بسته‌ها به صورت نامرتب می‌رسند.

مسائل مورد بررسی :

مرتب دریافت شدن ، نحوه ارسال مجدد ، تشخیص دوبله رسیدن ، کنترل Flow ، ایجاد اتصال ، قطع اتصال ، رفع خرابی

مرتب دریافت شدن : برای هر بسته باید Sequence number در نظر گرفته شود (TCP ، شماره قطعه ، تا کجا ارسال شده ، تا کجا آماده دریافت)

نحوه ارسال مجدد : ACK دادن Frame ها (گروهی) .

تایمراهای مختلف (مدیریت تایمراهی مختلف بسیار پیچیده است) :

تايمر انتقال مجدد

تايمر اتصال مجدد

تايمر پنجره

تايمر انتقال مجدد Sync

تایمر غیر فعال کننده

تایمِر حضور

زمان تایمراه یا به صورت ثابت است و یا به صورت پویا. در تایم پویا، تغییرات شبکه (مانند ترافیک و عوامل دیگر) باعث می‌شود که تنظیم آن صورت گیرد. تنظیم تایم در لایه حمل و نقل یکی از موضوعات بسیار مهم است.

تشخیص دوبله رسیدن: اگر ACK گم شود، کپی ها باید مجدداً ارسال شود. ممکن است کپی ها زمانی دریافت شوند که هنوز اتصال قطع نشده است یا ممکن است که کپی بعد از بستن اتصال دریافت شده باشد:

۱) گیرنده فرض می کند که ACK گم شده و کپی را بدهد (اگر مشخص نباشد که گم شدن در اثر گم شدن ACK است یا گم شدن واقعی اطلاعات).

۲) طراحی فضای Seq no مهم است (آنقدر بزرگ باشد که احتمال کمی مجدد وجود نداشته باشد).

کنترل Flow : تقریباً مثل روش Connection-Oriented است (روش Credit)

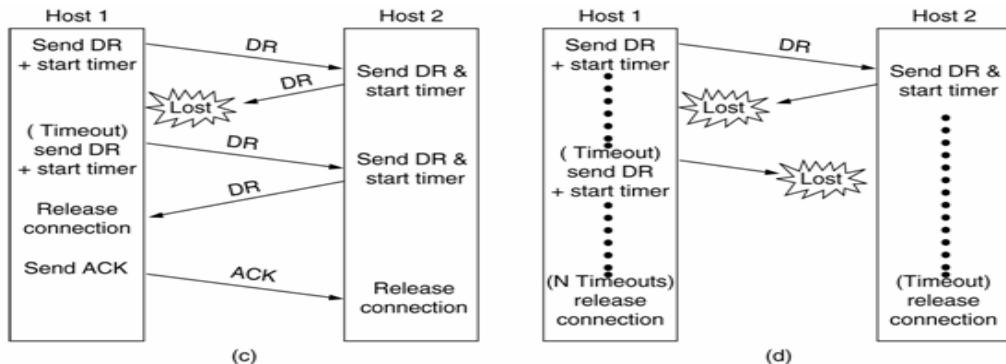
: CreditAckn نامه ارسال شود : $N+M$ تا $N+1$ های قطعه های رسیده فریم ری یعنی :

ایجاد اتصال

قطع اتصال رفع خرابی

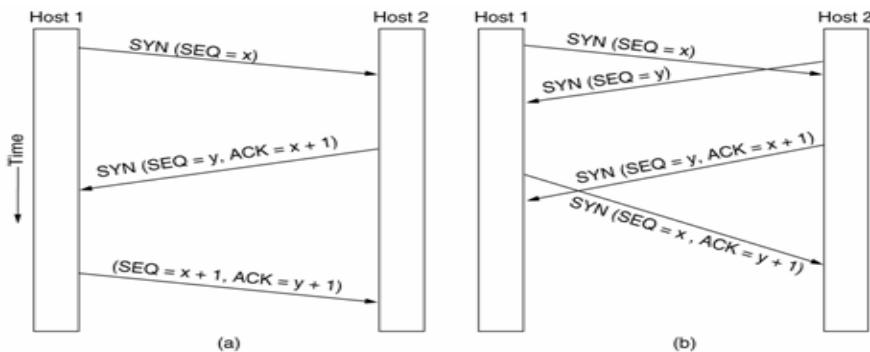
ایجاد اتصال در شبکه های نامطمئن :

با رد و بدل کردن فریمهای Syn اتصال برقرار می شود . یک Syn به B می فرستد و B جواب را با یک Syn می دهد و اتصال برقرار می شود . به هر حال در این روش Syn دو طرفه ممکن است اشکالاتی بوجود آید . ممکن است Syn گم شود . یا از یک اتصال قدیمی وارد سیستم شود و اتصال مخدوش شود .

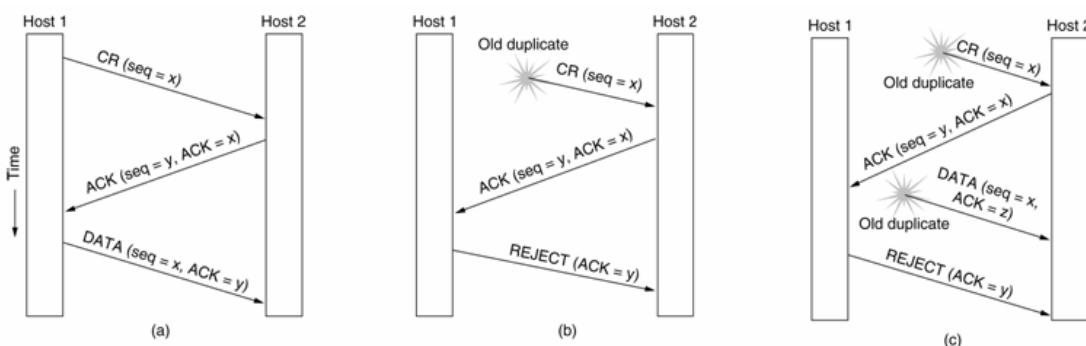


یک راه حل این است که درخواستها شماره گذاری شوند . این هم اشکالاتی دارد که ممکن است Synk بررس و اتصال مخدوش شود .

قطع اتصال : همزمان درخواست اتصال می کنند) و سپس A با فرض اینکه اتصال برقرار است شروع به ارسال اطلاعات می کند 1 Snr+1 که B آن را نمی پذیرد زیرا برای Syni B اتصال است و داده باید 1 باشد



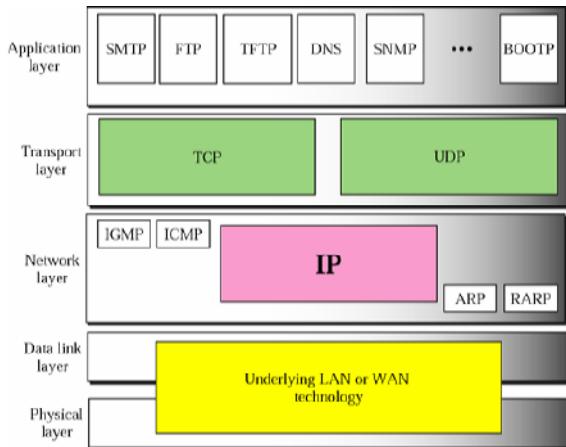
راه حل این است که هر طرف شماره Syn و ترتیب داده ها (SN) از طرف قبل را مجزا جواب دهنده که این روش بنام 3-Way hand shake می باشد حالتی جدید در دیاگرام حالت پروتکل حمل و نقل ایجاد می شود و قطعه های کنترلی جدید مانند RST (Reset) افزوده می شود .



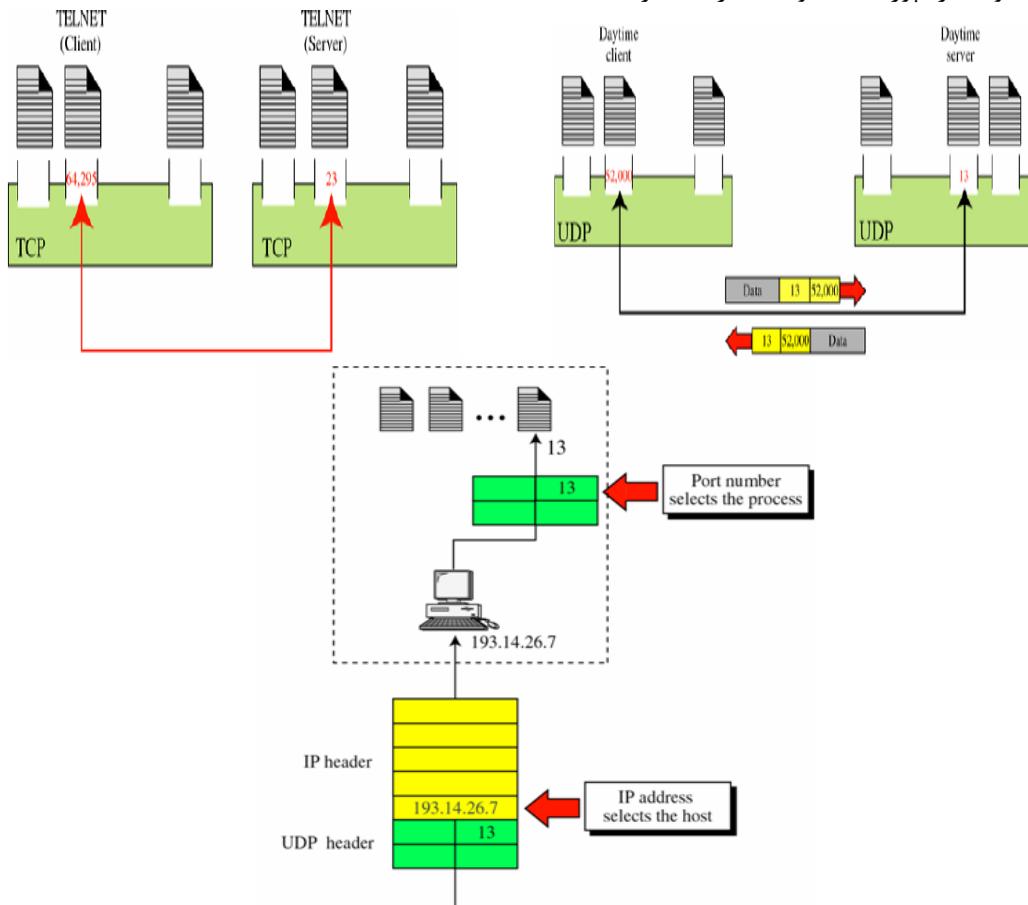
فصل ۱۲:

پروتکل های TCP و UDP

TCP و UDP در لایه حمل و نقل قرار دارد:



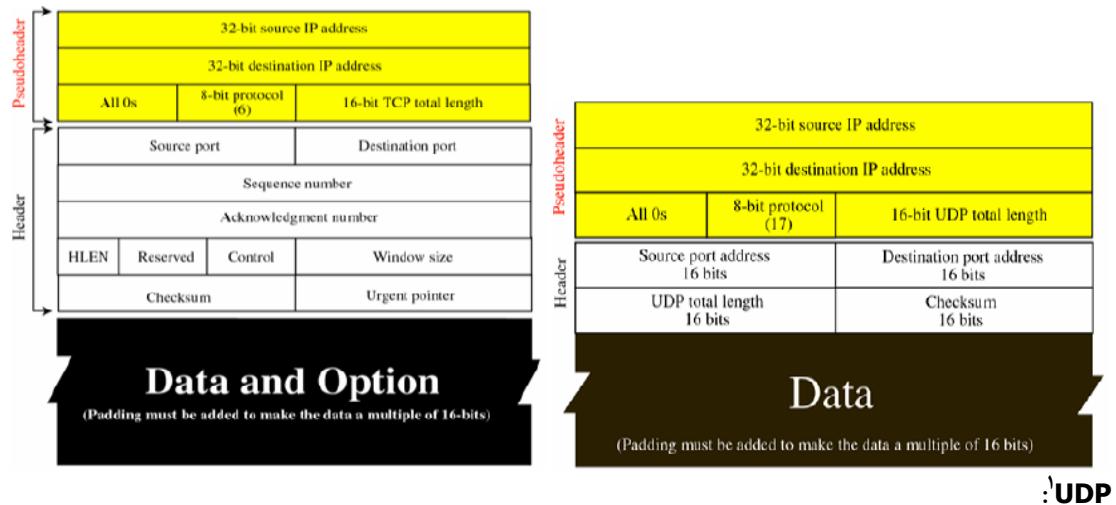
برخلاف IP که بصورت میزبان به میزبان می باشد، TCP و UDP بصورت پردازش به پردازش می باشد. در TCP و UDP از شماره پورت جهت مشخص کردن پردازش استفاده می کنند. شماره پورت یک مقدار ۱۶ بیتی می باشد و شماره پورت TCP و UDP از یکدیگر جدا هستند.



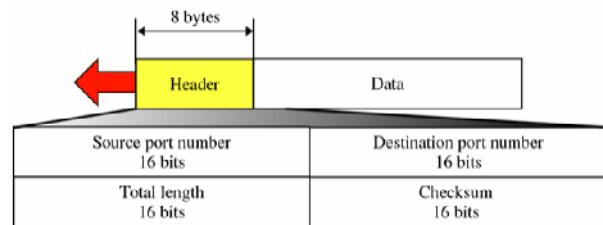
شماره پورتها در دامنه IANA بصورت زیر می باشد:

۱. شماره پورتهای مشهور (۰۰-۲۳)
 ۲. شماره پورتهای ثبت شده (۰۰-۱۵۱۴۹)
 ۳. شماره پورتهای پویا (۰۰-۱۵۲۴۹-۳۵۵۸)
- آدرس سوکت عبارت است از آدرس IP و آدرس پورت.

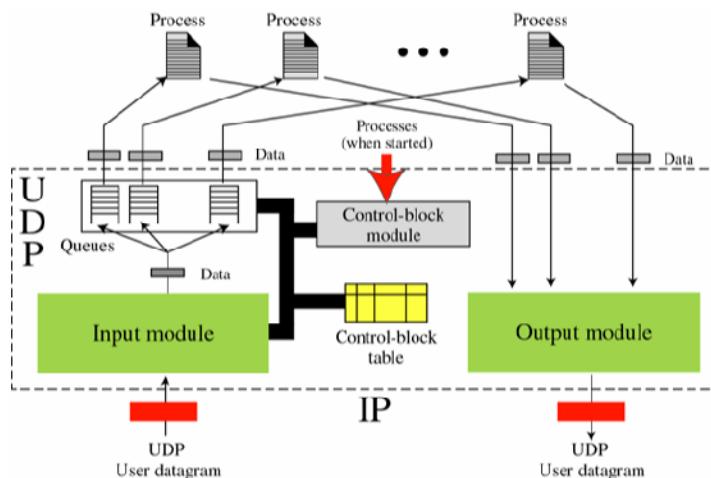
در بسته های TCP و UDP از شبیه سرآیند(Pseudoheader) جهت کمک به استفاده می شود. این شبیه سرآیندها اطلاعاتی همچون آدرس IP مبدأ و مقصد، شماره پروتکل و طول بسته UDP و یا TCP قرار گرفته است. همچنین اگر طول قسمت داده این بسته ها کمتر از حد مجاز باشد(مضبوی از ۱۶ نباشد)، با استفاده از Padding طول آن تا حد مجاز افزایش می یابد.



سرآیند بسته های UDP بشکل زیر می باشد:



طول بسته های UDP برابر است با طول بسته های IP منهای طول سرآیند بسته های IP. طرح داخلی UDP بشکل زیر می باشد:



جهت تشریح این ساختار جدول کنترل بلاک زیر را در نظر بگیرید:

State	Process ID	Port Number	Queue Number
IN-USE	2,345	52,010	34
IN-USE	3,422	52,011	
FREE			
IN-USE	4,652	52,012	38
FREE			

فرض کنید یک بسته Datagram برای شماره پورت مقصد 52,012 دریافت می شود. مازول ورودی جدول کنترل بلاک را برای این شماره پورت جستجو کرده و آن را پیدا می کند. صفحه شماره ۳۸ به این پورت اختصاص یافته است که این به معنی آن است که این پورت قبلًا مورد استفاده قرار گرفته است. مازول ورودی داده را به صفحه ۳۸ می فرستد و جدول کنترل بلاک تغییر نمی یابد.

چند ثانیه بعد یک پردازش شروع می گردد و از سیستم عامل یک شماره پورت را درخواست می نماید. سیستم عامل پورت شماره 52,014 را تخصیص می دهد. اکنون پردازش شماره شناسایی خود (4,978) و شماره پورت تخصیصی را به مازول کنترل بلاک ارسال می کند و این مازول نیز یک مدخل را در جدول ایجاد می نماید. مازول صفحی را در این لحظه به مدخل تخصیص نمی دهد، زیرا هیچ Datagram بی از کاربر برای این مقصد دریافت نشده است.

State	Process ID	Port Number	Queue Number
IN-USE	2,345	52,010	34
IN-USE	3,422	52,011	
IN-USE	4,978	52,014	
IN-USE	4,652	52,012	38
FREE			

اکنون یک بسته Datagram کاربر برای پورت 52,011 می رسد. مازول ورودی جدول را چک کرده متوجه می شود که هیچ صفحی برای این مقصد تخصیص داده نشده است، زیرا این اولین بسته Datagram کاربر می باشد که برای این مقصد دریافت می گردد. مازول یک صفحه را ایجاد کرده و به آن یک شماره (۴۳) تخصیص می دهد.

State	Process ID	Port Number	Queue Number
IN-USE	2,345	52,010	34
IN-USE	3,422	52,011	43
IN-USE	4,978	52,014	
IN-USE	4,652	52,012	38
FREE			

پس از چند ثانیه یک Datagram برای پورت 52,222 می رسد. مازول ورودی جدول را چک کرده و مدخلی را برای این مقصد پیدا نمی کند. دور ریخته می شود و یک درخواست به ICMP برای ارسال یک پیام "در دسترس نبودن پورت" به مبدأ، ایجاد می شود.

پس از چند ثانیه یک پردازش می خواهد یک Datagram ارسال نماید. پردازش داده ها را به مازول خروجی تحويل داده و این مازول پس از افزودن سرآیند UDP، آن را ارسال می کند.

TCP

در TCP جریانی از بایتها بین فرستنده و گیرنده منتقل می شود. فرستنده و گیرنده جهت ارسال و دریافت بایتها از بافرهای ارسال و دریافت استفاده می کنند. جهت بهبود ارسال بایتها در سگمنتهايی قرار گرفته و سپس ارسال می گردد. بایتهاي داده ارسالی در هر اتصال بوسیله TCP شمرده می شود. شمارش با یک عدد تصادفی آغاز می شود.

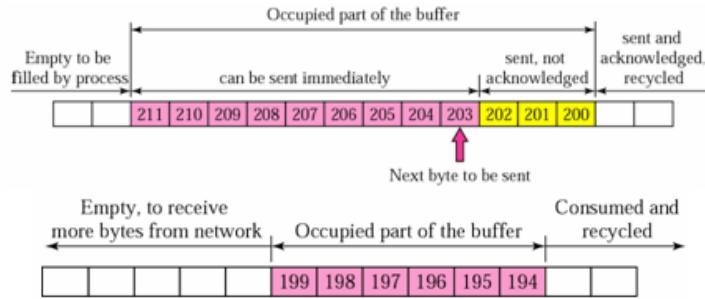
مثال: یک اتصال TCP قصد ارسال یک فایل ۶۰۰۰ بایتی را دارد. اولین بایت با شماره ۱۰۰۱۰ گذاری شده است. شماره توالی هر سگمنت با فرض ارسال ۴ سگمنت ۱۰۰۰ بایتی و یک سگمنت ۲۰۰۰ بایتی در پایان، را مشخص کنید.

Segment 1	-->	10,010	(10,010 to 11,009)
Segment 2	-->	11,010	(11,010 to 12,009)
Segment 3	-->	12,010	(12,010 to 13,009)
Segment 4	-->	13,010	(13,010 to 14,009)
Segment 5	-->	14,010	(14,010 to 16,009)

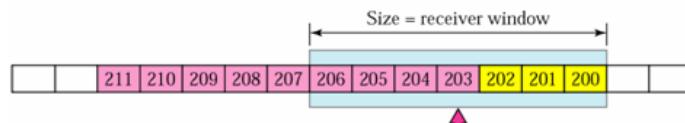
مقدار شماره توالی در هر سگمنت، شماره بایت اول داده موجود در هر سگمنت را مشخص می‌کند. مقدار فیلد Acknowledgment در یک سگمنت، شماره بایت بعدی یک دسته را که انتظار دریافت آن می‌رود را مشخص می‌نماید. شماره Acknowledgment بصورت تجمعی می‌باشد.

پنجره لغزان:

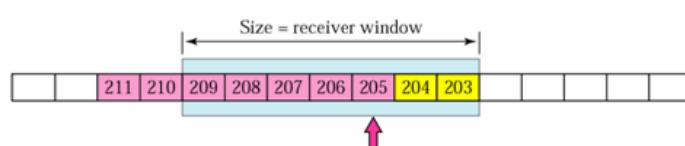
پنجره لغزان (Sliding Window) برای کارایی بیشتر ارسال و کنترل جریان داده بکار می‌رود تا مقصد در داده‌ها غوطه ور نمی‌شود. پنجره لغزان TCP بایت گرا است. طرح بافر فرستنده و پنجره دریافت کننده در تصاویر زیر آمده است:



اندازه پنجره لغزان بوسیله پنجره دریافت کننده معین می‌گردد. اگرچه اندازه واقعی پنجره می‌تواند بدليل تراکم در شبکه کوچکتر شود.

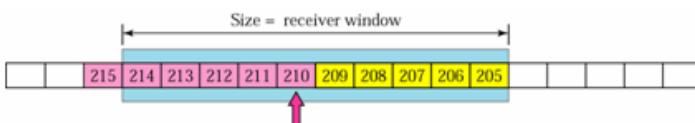


a. Before

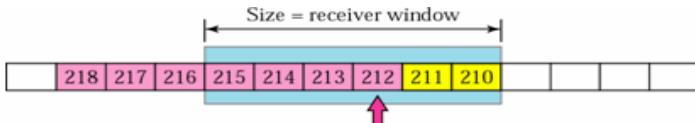


b. After

اندازه پنجره لغزان ممکن است افزایش یابد.



و یا ممکن است اندازه آن کاهش یابد.



نکاتی در مورد پنجره لغزان TCP:

۱. مبداء مجبور نیست تا تمام داده‌های ممکن در اندازه کامل پنجره را ارسال کند.

۲. اندازه پنجه می تواند بوسیله مقصد افزایش و یا کاهش یابد.

۳. مقصد می تواند یک Acknowledgment را در هر زمانی ارسال کند.

اگر به هر دلیلی همچون معیوب بودن و یا گم شدن سگمنت ارسالی، برای آن و یا سگمنت‌های بعد از آن در فاصله زمانی مشخص (به اندازه out Ack) یعنی دریافت ننمایید، فرستنده مجدداً داده‌های ارسالی پس از آخرین Ack دریافتی را ارسال می نماید. همچنین از آنجاییکه گیرنده در ارسال ACK محدودیتی ندارد، اگر یک هم گم شود و فرستنده ACK بعدی را دریافت کند، فرستنده با فرض عدم ارسال ACK توسط گیرنده، بر اساس ACK جدید اقدام به ارسال داده می کند.

تایمراهی TCP عبارتند از:

۱. Retransmission: پس از برقراری یک ارتباط، وقتی فرستنده بسته‌ای برای پردازش به مقصد

ارسال می‌کند، ضمن نگهداری موقت آن در یک بافر، برای آن یک زمان سنج را تنظیم و فعال می نماید و اگر در مهلت مقرر، پیام تایید آن دریافت نشد، آن بسته دوباره ارسال می گردد. این زمان سنج در ابتدا به یک مقدار پیش فرض تنظیم می گردد و سپس شروع به شمارش معکوس می نماید. هرگاه مقدار آن به صفر رسید و پیام تاییدی دریافت نشد، رویداد انقضای زمان سنج ارسال مجدد بوقوع می پیوندد و پردازش TCP فرستنده را وادار به ارسال مجدد آن بسته می شود و مراحل قبلی مجدداً تکرار می گردد.

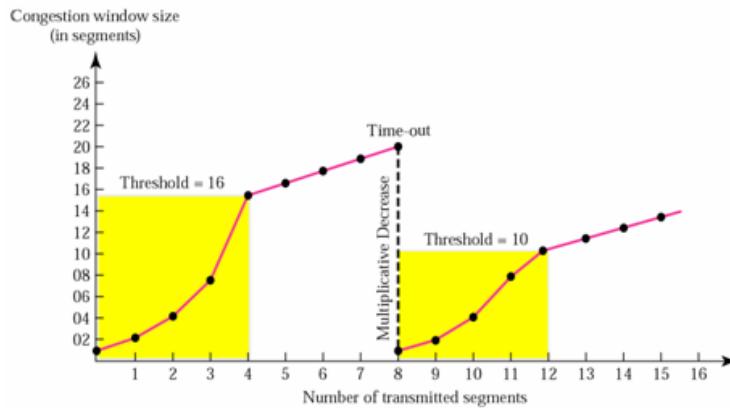
عملکرد این زمان سنج بسیار ساده است. اما نکته مهم در مورد آن مقدار پیش فرض زمان سنج می باشد. این زمان برای شبکه‌های محلی سریع، بسیار کوتاه و در حد هزارم ثانیه می باشد و برای شبکه‌های WAN طولانی و در حد چند ثانیه می باشد. بنابراین اگر زمان سنج فرض مقدار پیش فرض کوتاهی داشته باشد، برای انتقالات فواصل دور، قبل از آنکه بسته به مقصد برسد و تایید ارسال شده آن به مبدأ برسد، بدلیل انقضای زمان زمان سنج، بسته دوباره ارسال می گردد که این موضوع باعث ایجاد سربار ترافیکی بیهوده در شبکه می گردد. از سوی دیگر، مقدار طولانی برای این زمان سنج، باعث می گردد تا در شبکه‌های محلی و سریع، هنگام بروز یک خطأ، تاخیر زیادی بوجود آید. بهترین راه حل، تنظیم زمان سنج بصورت پویا، با استفاده از روش‌های طبیقی و پویا، می باشد؛ چرا که بازده TCP بشدت به آن وابسته است.

۲. Persistence: در پروتکل TCP وقتیکه یکی از طرفین ارتباط، مقدار بافر آزاد خود را در فیلد اندازه پنجه صفر اعلام کند، ناگزیر است تا پردازش طرف مقابل را مسدود نماید. در چنین حالتی پس از آنکه مقداری از فضای بافر پرشده، تخلیه گردید، این موضوع به طرف مقابل اعلام می گردد تا سیستم عامل، پردازش مسدود شده را احیا نماید و ادامه ارسال از طرف مقابل، ممکن گردد، در غیر این صورت، بن بست و یا تاخیر بینهایت برای پردازش، بوجود می آید. با استفاده از این زمان سنج، پس از آزاد شدن فضای بافر، در فواصل زمانی منظم یک بسته TCP برای پرسوه مسدود شده، ارسال می گردد تا ضمن آگاهی از آخرین وضعیت فضای بافر، پردازش بتواند احیا گردد.

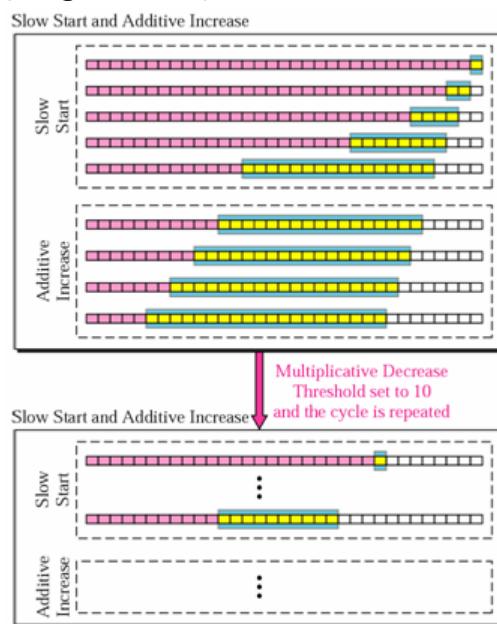
۳. Keep alive: ممکن است طرفین یک ارتباط به هر دلیلی ارسال اطلاعات را موقتاً متوقف نمایند و هیچ داده‌ای مبادله نگردد، هرچند ارتباط TCP فعال و باز باشد. از سوی دیگر ممکن است یکی از طرفین به دلیلی همچون خرابی سخت افزار یا نرم افزار، بدون اطلاع، ارتباط را قطع نماید. برای تمایز بین این دو حالت، فرستنده اطلاعات با استفاده از این زمان سنج در بازه‌های زمانی منظم، یک بسته TCP فاقد داده را برای مقصد ارسال می کند و درصورتیکه پیام تایید آن، دریافت گردد، فرستنده درمی یابد که ارتباط TCP باز و فعال می باشد. در غیر این صورت ارتباط TCP به صورت یک طرفه قطع می گردد و تمام بافرها و فضای ایجاد شده، آزاد می گردد. زمان پیش فرض این زمان سنج بین ۵ تا ۴۵ ثانیه می باشد.

ممکن است یک ارتباط TCP، بسته شود، ولی هنوز بسته های سرگردان برروی شبکه وجود داشته باشند که پس از بسته شدن ارتباط TCP به مقصد برسند. لذا در این پروتکل، پس از بسته شدن یک ارتباط با شماره پورت خاص، بقیه پردازش ها تا مدتی حق استفاده از شماره پورت این تماس را ندارند. مقدار پیش فرض این زمان سنج دقیقاً دو برابر مقدار پیش فرض زمان حیات بسته IP، بحسب ثانیه، بین ۳۰ تا ۱۲۰ ثانیه، می باشد. به این زمان سنج، زمان سنج Quiet نیز گفته می شود.

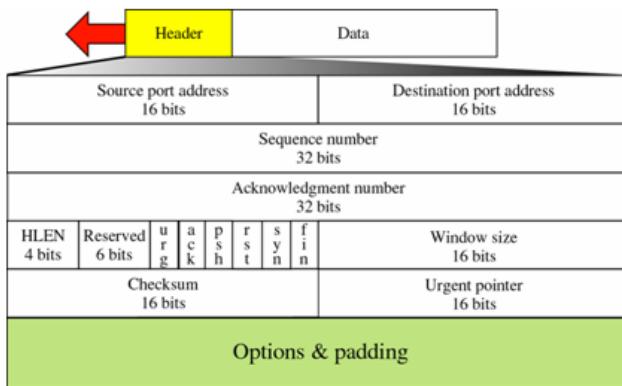
Dilil گم شدن بسته ها را تراکم در شبکه می دارد و حال آنکه در صورت صحیح بودن این فرض ارسال دوباره سگمنت گم شده، نه تنها عامل تراکم را حذف نمی کند، بلکه آن را تشیدید می نماید. در تصویر زیر مکانیزم تعیین اندازه پنجره تراکم در TCP امده است. این مکانیزم جهت کنترل تراکم در TCP بکار می رود.



ابتدا TCP اقدام به ارسال بسته می نماید تا آنجا که بر اثر تراکم Ack بی دریافت ننماید. در این حالت مقدار آستانه به اندازه نصف اندازه پنجره تراکم زمان Time out تعیین می شود و اندازه پنجره تا کمترین سطح ممکن کاهش می یابد. تا سطح آستانه، اندازه پنجره بصورت نمایی رشد کرده و از آن به بعد تا زمان Time out جدید، اندازه آن بصورت خطی رشد می کند. با وقوع Time out جدید، دوباره حد آستانه تعیین شده و عملیات تغییر اندازه پنجره تراکم تکرار می گردد. تصویر زیر نحوه تغییر اندازه پنجره را بوضوح نشان می دهد.



طرح ساختار سگمنت TCP در ادامه آمده است.



فیلدهای کنترلی در سگمنت TCP عبارتند از:

- URG: اشاره گر فوری معتبر است. در صورتیکه این بیت مقدار 1 داشته باشد معین می کند که در فیلد اشاره گر فوری مقداری قابل استناد و معتبر قرار دارد و بایستی مورد پردازش قرار گیرد. در صورتیکه مقدار این بیت صفر باشد، فیلد اشاره گر فوری، شامل مقدار نامعتبر و قابل استنادی نیست و از آن چشم پوشی می شود.
- Ack: تایید معتبر است. اگر در این بیت مقدار یک قرار داشته باشد، عددی که در فیلد تایید قرار دارد، دارای مقدار معتبری است.
- PSH: درخواست برای Push. اگر در این بیت مقدار یک قرار گرفته باشد، فرستنده اطلاعات از گیرنده تقاضا می کند که داده های موجود در این بسته را بافر نکند و در اسرع وقت آن را جهت پردازش های بعدی تحويل برنامه کاربردی مالک آن بدهد. این عمل گاهی برای برنامه هایی مشابه TelNet، ضروری است.
- RST: راه اندازی مجدد اتصال. اگر در این بیت مقدار یک قرار گیرد، ارتباط بصورت یک طرفه و ناتمام قطع می گردد. یک Abnormaly Ended به معنی است که یکی از طرفین ارتباط، به دلایلی همچون نقص سخت افزاری یا نرم افزاری، مجبور به خاتمه ارتباط فعلی می شود. همچنین بیت RST می تواند به عنوان علامت عدم پذیرش برقراری ارتباط، بکار رود. اگر یکی از طرفین ارتباط، یک بسته دریافت نماید که در آن بسته RST مقدار یک داشته باشد، ارتباط بصورت نامتعادل قطع می گردد.
- SYN: شماره توالی همزمانی. این بیت نقش اساسی در برقراری یک ارتباط بازی می کند. نحوه برقراری یک ارتباط TCP در ادامه بررسی می گردد.
- FIN: خاتمه دادن اتصال. اگر یکی از طرفین ارتباط، داده دیگری برای ارسال نداشته باشد، در هنگام ارسال آخرین بسته خود، این بیت را یک می کند و در حقیقت ارسال اطلاعات را بصورت یکجانبه قطع می نماید. اگرچه در این حالت ارسال اطلاعات خاتمه یافته است، اما طرف مقابل هنوز ممکن است درحال ارسال اطلاعات باشد. زمانی ارتباط کاملاً خاتمه می یابد که طرف مقابل نیز با ارسال یک بسته با مقدار یک برای بیت FIN، خاتمه ارسال اطلاعات را نشان دهد.

:TCP ها در Option

• تک بیتی

۱. No Operation

No Operation

Option ابتدای یک

Option بعدي

۲. End of Option

پایان option ها

○ استفاده در Padding

• چند بیتی

۱. ماکزیمم اندازه سگمنت

۲. ضریب مقیاس پنجره

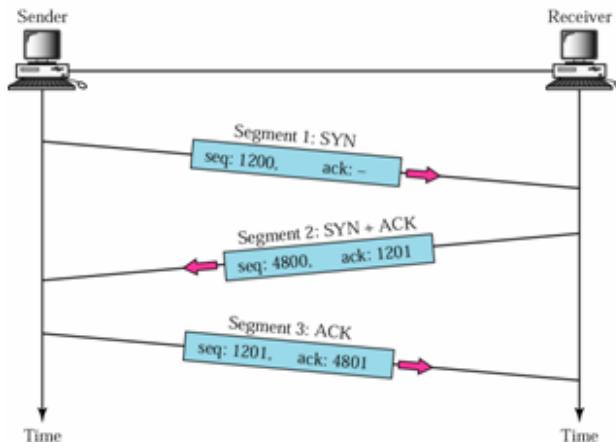
۳. Time Stamp

برای آغاز یک اتصال از "دست دهی" سه طرفه استفاده می کند. روند این عمل بصورت زیر می باشد:

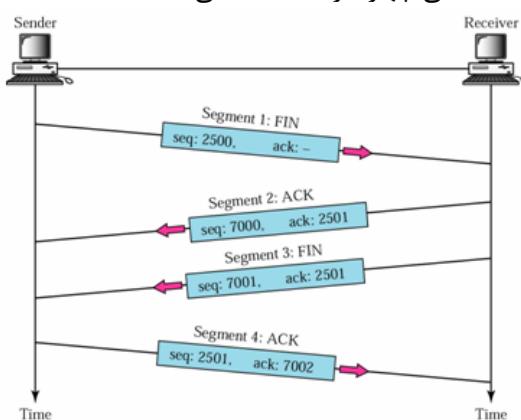
۱. شروع کننده ارتباط، یک بسته TCP بدون داده و با تنظیمات بیتهاي $ACK=0$, $SYN=1$ برای طرف مقابل ارسال می کند. در حقیقت ارسال چنین بسته ای به معنی تقاضا برای برقراری ارتباط می باشد.

۲. در پاسخ به درخواست ارتباط دریافتی، درصورتیکه طرف مقابل ارتباط تمایلی به برقراری ارتباط داشته باشد، بسته ای را برمی گرداند که بیت $SYN=1$ و بیت $ACK=1$ می باشد. این بسته نقش پذیرش یک ارتباط را دارد. درصورت عدم تمایل، فرستنده با یک بسته با مقدار $FIN=1$ خاتمه ارتباط را متنزکر می شود.

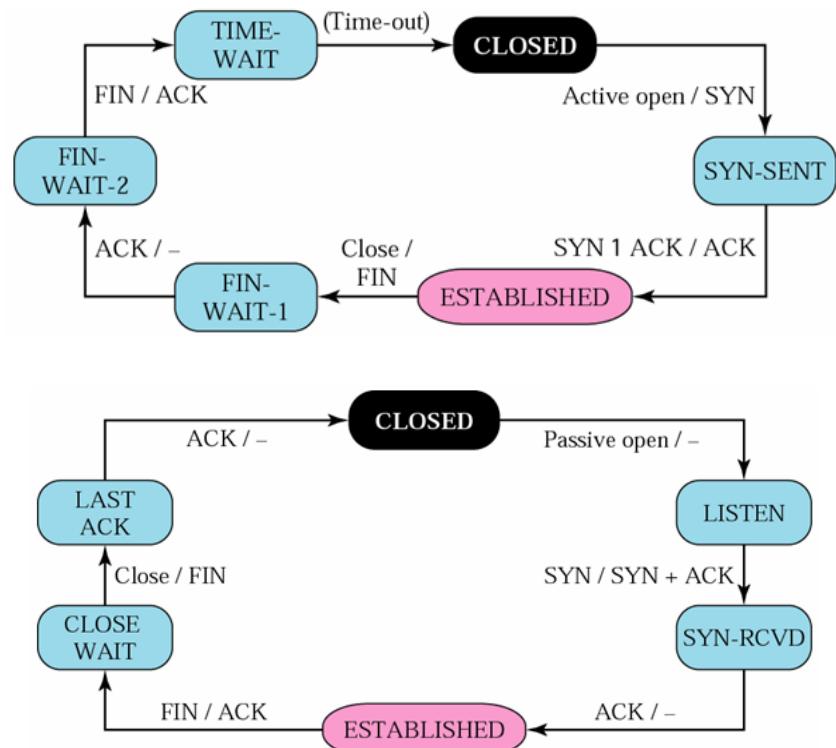
۳. فرستنده اقدام به ارسال اطلاعات می نماید(بیت $SYN=1$ و بیت $ACK=1$).



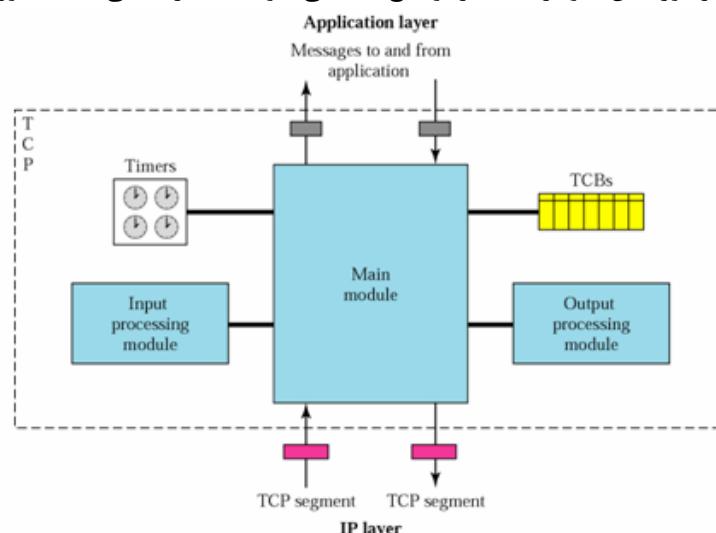
و برای خاتمه اتصال از دست دهی چهار طرفه استفاده می کند.



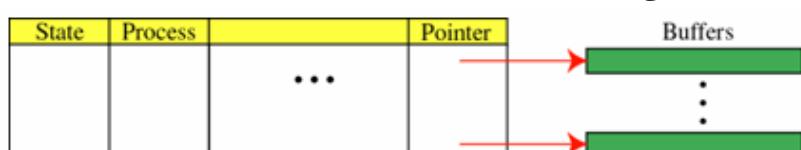
براین اساس نمودارهای گذر حالت زیر را می توان برای فرستنده و گیرنده ارائه داد:



در فصل بعد در مورد این نمودارها بیشتر توضیح داده می شود. ساختار داخلی TCP بصورت زیر می باشد:



ساختار ¹TCB بصورت زیر می باشد:



Transmission Control Block - ¹

فصل ۱۳:

پروتکلهای مدیریت شبکه

با رشد اندازه و پیچیدگی شبکه ها و فعالیتهای بین شبکه ای مبتنی بر TCP/IP، لزوم مدیریت شبکه اهمیت فراوان می یابد.

RFC 1052 را ارائه داد که در بردارنده ۲ شیوه می باشد:

پروتکل ساده مدیریت شبکه (SNMP^۱)

ISO CMIS/CMIP^۲ پروتکل سرویس اطلاعات متعارف / اطلاعات مدیریت متعارف

بطور خلاصه، IAB عنوان می دارد که باید از SNMP استفاده کرد. SNMP آنقدر متداول گشته است که به استاندارد رایج صنعتی جهت گزارش اطلاعات مدیریتی برای یک شبکه مبتنی بر IP بدل شده است.

۱-۱۳: پروتکل ساده مدیریت شبکه و مروری بر MIB^۳

چهارچوب مدیریت شبکه SNMP عبارتست از:

تعداد زیادی گره های مدیریت شده، که هر کدام یک موجودیت (یا Agent) SNMP دارند. یک SNMP Agent سرویست در میزبان مدیریت شده که پاسخگوی درخواستهای SNMP برای مدیران می باشد. یک Agent باید در هر میزبان IP قرار داشته باشد تا امکان مدیریت میزبان بوسیله یک مدیر SNMP را فراهم آورد. وظیفه مدیریت/پشتیبانی از پایه اطلاعات مدیریتی (MIB) را بر روی میزبان IP مقیم در آن برعهده دارد.

حداقل یک موجودیت SNMP با کاربردهای مدیریتی (مدیر). یک مدیر SNMP، کاربردی است که بروی یک ایستگاه مدیریتی اجرا شده و درخواست اطلاعات مدیریتی را از یک Agent SNMP، با استفاده از پروتکل SNMP دارد.

MIB برای هر موجودیت. پروتکل مورد استفاده بین یک Agent و مدیر SNMP می باشد. پروتکل مورد استفاده بین یک Agent و یک sub-Agent می تواند DPI/SMUX/AgentX و یا هر پروتکل اختصاصی دیگر باشد.

IAB توصیه می کند کخ تمام ساختارهای IP و TCP در شبکه، شامل تمام میزبانها، دروازه ها و سایر ابزارهای IP دار، قابل مدیریت بوسیله SNMP باشند و باید حداقل MIB-II را بکار ببرند. توجه کنید که پروتکل قدیمی SGMP^۴ (RFC 1156) و MIB-I (RFC 1028)، جهت استفاده توصیه نشده اند. یک پروتکل استاندارد اینترنت می باشد. وضعیت آن مورد توصیه است و خصوصیات جاری آن را می توان در RFC 1157، پروتکل ساده مدیریت شبکه (SNMP) پیدا نمود. MIB-II نیز وضعیتی مشابه SNMP اطلاعات آن را می توان در RFC 1213 مورد توصیه است. برایه مدیریت اطلاعات پایه: MIB-II: پیدا نمود. اطلاعات بیشتر را می توان در RFC 1155 (MIB-II) RFC 1213 (SMI) RFC 1157 و RFC 1157 (SNMP) یافت.

۲-۱۳: ساختار و هویت اطلاعات مدیریت(SMI^۵)

Simple Network Management Protocol – ^۱

Common Management Information Services/Common Management Information Protocol – ^۲

Management Information Base – ^۳

Simple Gateway Monitoring Protocol – ^۴

Structure and identification of management information – ^۵

قوانين نحوه توصیف اشیاء مدیریتی و نحوه دستیابی پروتکلهای مدیریتی به این اشیاء را ارائه می‌دهد. مفهوم اشیاء مدیریت شده در یک زیر مجموعه از ASN.1¹ ارائه شده است نوع شئی تعریفی از ۵ فیلد تشکیل شده است:

شئی: یک نام متنی که توصیفگر شئی نامیده می‌شود، به همراه یک نوع شئی همراه با شناسه شئی.

Syntax: دستورالعمل خلاصه برای نوع شئی. می‌تواند از نوع SimpleSyntax انتخاب شود Network ApplicationSyntax (Integer, Octet String, Object Identifier, Null) یا (Address, Counter, Gauge, Timeticks, Opaque) و یا انواع گسترده‌تر دیگر کاربرد باشد (به .(RFC 1155

تعریف: توصیف متنی از معنی شناسی نوع شئی.

دسترسی: یکی از Not-Accessible, Read-only, Read-write و یا

وضعیت: یکی از Optional, Mandatory و یا

به عنوان یک نمونه وضعیت زیر را ببینید:

```
OBJECT
sysDescr { system 1 }
Syntax OCTET STRING
Definition This value should include the full name and version
identification of the system's hardware type, software
operating system, and networking software. It is
mandatory that this contain only printable ASCII
characters.
Access read-only.
Status mandatory.
```

این مثال تعریف یک شئی در MIB را نشان می‌دهد. نام آن sysDescr است و به گروه system تعلق دارد (۱۳-۳ را ببینید).

یک شئی مدیریت شده علاوه بر توصیف شامل شناسه نیز می‌باشد. این امر با کمک شناسه شئی ASN.1، همانند یک شماره تلفن، انجام می‌گیرد و شماره گروه‌ها برای مناطق مختلف رزرو می‌گردد. در مدیریت شبکه‌های مبتنی بر TCP/IP شماره‌های تخصیصی 1.3.6.1.2 بوده و SMI از این به عنوان پایه‌ای برای تعریف اشیاء جدید استفاده می‌نماید.

شماره 1.3.6.1.2 بوسیله ادغام گروه‌های با شماره‌های با معنای زیر بکار می‌رود:

اولین گروه، معرف گره Administartor می‌باشد:

○ (۱) برای ISO

○ (۲) برای CCITT

○ (۳) برای ISO-CCITT

گروه دوم برای گره Administartor ISO (۳) تعریف شده است تا توسط سایر سازمانها بکار رود.

گروه سوم جهت استفاده در وزارت دفاع آمریکا (DoD)، (۶) تعریف شده است.

در گروه چهارم، DoD مشخص ننموده است که چگونه گروهش را مدیریت می‌نماید، بنابراین انجمن اینترنت مقدار (۱) را برای آن فرض نموده است.

- گروه پنجم توسط IAB بصورت زیر مقداردهی شده است:
- (۱) برای استفاده از فهرست OSI در اینترنت
 - (۲) برای شناساندن شئی برای اهداف مدیریتی
 - (۳) برای شناساندن شئی برای اهداف آزمایشی
 - (۴) برای شناساندن شئی برای استفاده اختصاصی

در مثال قبل، "system" در کنار نام شئی، به مفهوم آنست که شناسه شئی 1.3.6.1.2.1.1.1 می باشد. این اولین شئی در اولین گروه (سیستم) در MIB می باشد.

MIB : ۳-۱۳

MIB اشیائی را معرفی می کند که ممکن است برای مدیریت هر لایه در پروتکل TCP/IP بکار رود. ۲ نسخه وجود دارد: MIB-I و MIB-II. MIB-I در RFC 1156 معرفی شده و اکنون به عنوان یک پروتکل قدیمی با وضعیت بدون توصیه، دسته بندی می شود.

MIB-II در RFC 1213 تشریح شده است. گروه های تعریف شده عبارتند از:

#	اشیاء برای	گروه
۷	اطلاعات پایه سیستم	System
۲۳	الحالات شبکه	Interfaces
۳	ترجمه آدرس	AT
۴۲	پروتکل اینترنت	IP
۲۶	پروتکل پیام کنترل اینترنت	ICMP
۱۹	پروتکل کنترل انتقال	TCP
۷	پروتکل داده گرام کاربر	UDP
۱۸	پروتکل دروازه خروجی	EGP
۳۹	موجودیتهای کاربردهای SNMP	SNMP
# = تعداد اشیاء در گروه		

جدول ۱-۱۳: تعاریف گروه های MIB-II

همچنین در تعریف، فضایی برای یک گروه انتقال وجود دارد تا رسانه انتقالی زیرین را توصیف نماید. هر گره مدیریت شده تنها گروه های مقتضی را پشتیبانی می نماید. برای مثال، در صورت عدم وجود دروازه، نیازی به پشتیبانی گروه EGP نیست. در صورت نیاز به گروهی، همه اشیاء واقع در گروه باید مورد پشتیبانی قرار بگیرند. لیست اشیاء مدیریت شده تعریف شده از میان آن عناصر مورد نیاز ضروری مشتق شده است. این شیوه گرفتن تنها اشیاء مورد نیاز، محدود سازنده نیست، از این رو SMI مکانیزم های توسعه پذیری را همانند تعریف یک نسخه جدید از MIB و تعریف اشیاء خصوصی و یا غیر استاندارد را فراهم می آورد. در زیر مثالهایی از اشیاء در هر گروه ارائه شده است. لیست کامل در RFC 1213 آمده است. در RFC 2011 و 2012 RFC 2013 اطلاعات بروز شده IP، TCP و UDP ارائه شده است.

گروه سیستم

- sysDescr : توصیف کامل سیستم (نسخه، HW و OS)
- sysObjectID : شناسه شئی فروشنده

sysUpTime : بازه زمانی از آخرین مقدار دهی اولیه مجدد	○
sysContact : نام شخص تماس گیرنده	○
sysServices : سرویس ارائه شده توسط سیستم	○
	گروه واسط <input checked="" type="checkbox"/>
ifIndex : شماره واسط	○
ifDescr : توصیف واسط	○
ifType : نوع واسط	○
ifMtu : اندازه بزرگترین داده گرام IP	○
ifAdminStatus : وضعیت واسط	○
ifLastChange : بازه زمانی ورود واسط به وضعیت جاری	○
ifINErrors : تعداد بسته های ورودی حاوی خطا	○
ifOutDiscards : تعداد بسته های خروجی دور ریخته شده	○
	گروه ترجمه آدرس <input checked="" type="checkbox"/>
(MIB-I) deprecated : atTable	○
(MIB-I) deprecated : atEntry	○
atIfIndex : شماره واسط	○
atPhysAddress : آدرس فیزیکی وابسته به محیط انتقال	○
atNetAddress : آدرس شبکه منطبق با آدرس فیزیکی وابسته به محیط انتقال	○
media	○
	IP گروه <input checked="" type="checkbox"/>
ipForwarding : نشانه اینکه آیا این موجودیت یک دروازه IP است	○
ipInHdrErrors : تعداد داده گرام ورودی دور ریخته شده بدلیل خطا در سرآیند IP	○
شان	
ipInAddrErrors : تعداد داده گرام ورودی دور ریخته شده بدلیل خطا در آدرس IP	○
شان	
ipInUnknownProtos : تعداد داده گرام ورودی دور ریخته شده بدلیل پروتکل	○
ناشناخته یا مورد حمایت واقع نشده	
ipReasmOKs : تعداد داده گرام IP که با موفقیت دوباره سازی شده اند	○
ipRouteDest : آدرس IP مقصد	○
	ICMP گروه <input checked="" type="checkbox"/>
icmpInMsgs : تعداد پیام ICMP دریافتی	○
icmpInDestUnreachs : تعداد پیام ICMP عدم در دسترس بودن مقصد دریافتی	○
icmpInTimeExcds : تعداد پیام ICMP تخطی از بازه زمانی دریافتی	○
icmpInSrcQuenches : تعداد پیام ICMP خاموش بودن منبع دریافتی	○
icmpOutErrors : تعداد پیام ICMP ارسال نشده بدلیل مشکلات در ICMP	○
	TCP گروه <input checked="" type="checkbox"/>
tcpRtoAlgorithm : الگوریتم تعیین انقضای بازه زمانی برای ارسال دوباره هشت تاییهای بدون تایید	○
tcpMaxConn : محدودیت تعداد اتصالات TCP مورد حمایت موجودیت	○

tcpActiveOpens	◦
SYN-SENT	
tcpInSegs	◦
: تعداد سگمنت دریافتی، شامل آنهایی که حامی خطا بوده اند	
tcpConnRemAddress	◦
: آدرس IP راه دور برای این اتصال TCP	
tcpInErrs	◦
: تعداد سگمنت دور ریخته شده بدلیل فرمت خراب	
tcpOutRsts	◦
: تعداد reset تولید شده	
UDP گروه	<input checked="" type="checkbox"/>
udpInDatagrams	◦
: تعداد داده گرام UDP تحويل داده شده به کاربران UDP	
udpNoPorts	◦
: تعداد داده گرام UDP دریافتی بدلیل عدم وجود کاربرد در پورت مقصد	
udpIn Errors	◦
: تعداد داده گرام UDP دریافتی بدلیل عدم تحويل به دلایلی بجز عدم وجود کاربرد در پورت مقصد	
udpOutDatagrams	◦
: تعداد داده گرام UDP ارسالی برای این موجودیت	
EGP گروه	<input checked="" type="checkbox"/>
egpInMsgs	◦
: تعداد پیام EGP دریافتی فاقد خطا	
egpInErrors	◦
: تعداد پیام EGP دارای خطا	
egpOutMsgs	◦
: تعداد پیام EGP تولید شده محلی	
egpNeighAddr	◦
: آدرس IP همسایه این موجودیت	
egpNeighState	◦
: وضعیت EGP سیستم محلی با توجه به همسایه این موجودیت	
EGP	

این لیست محتوی تعریف کامل MIB نیست؛ اما یک نمونه از اشیاء تعریف شده در هر گروه را ارائه می دهد.
 این مازولها در حال حاضر IPv4 را حمایت می نمایند.
 برای تشریح این، گروه واسط شامل ۲ شئی با سطح بالا می باشد: تعداد واسط متصل به گره (ifNumber) و جدول محتوی اطلاعات آن واسط (ifTable). هر مدخل (ifEntry) در آن جدول شامل اشیائی برای یک واسط خاص می باشد. در میان آنها، نوع واسط (ifType) در درخت MIB با استفاده از نماد ASN.1 بوسیله ۱.3.6.1.2.1.2.2.1.3 تعريف شده است و برای یک وفق دهنده token-ring مقدار متغیر منطبق با آن ۹ است که به معنی iso88025-tokenRing می باشد (تصویر زیر را ببینید).

بخش IMB در IMB-specific

اشیاء زیر را به پایگاه داده MIB-II افزوده است:

```
* IBM SNMP agent DPI port
DPI_port 1.3.6.1.4.1.2.2.1.1. number 2

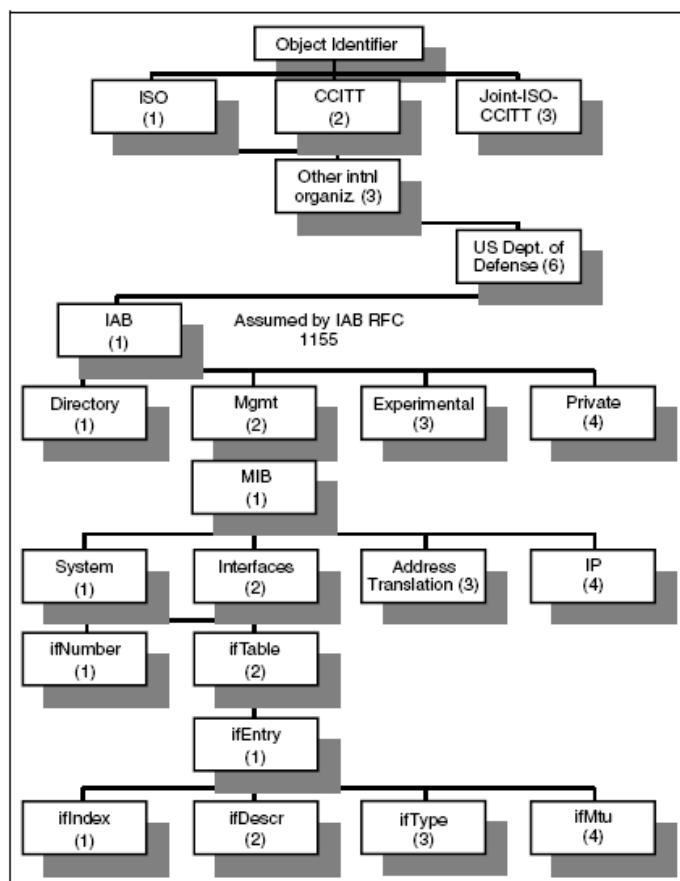
* IBM "ping" round-trip-time table
RTTaddr 1.3.6.1.4.1.2.2.1.3.1. internet 60
minRTT 1.3.6.1.4.1.2.2.1.3.2. number 60
maxRTT 1.3.6.1.4.1.2.2.1.3.3. number 60
aveRTT 1.3.6.1.4.1.2.2.1.3.4. number 60
RTTtries 1.3.6.1.4.1.2.2.1.3.5. number 60
RTTResponses 1.3.6.1.4.1.2.2.1.3.6. number 60
```

:که

DPI_port شماره پورت بین subAgent و Agent را بر می گرداند.

*Ping به میزبان راه دور را به یک مدیر SNMP می دهد. RTT نمادی برای جدول Round Trip Time می باشد.

- RTTaddr : آدرس میزبان
- MinRTT : حداقل Round Trip Time
- MaxRTT : حداکثر Round Trip Time
- AveRTT : میانگین Round Trip Time
- RTTtries : تعداد Ping های انجام شده تا کنون
- RTTresponses : تعداد پاسخ های رسیده



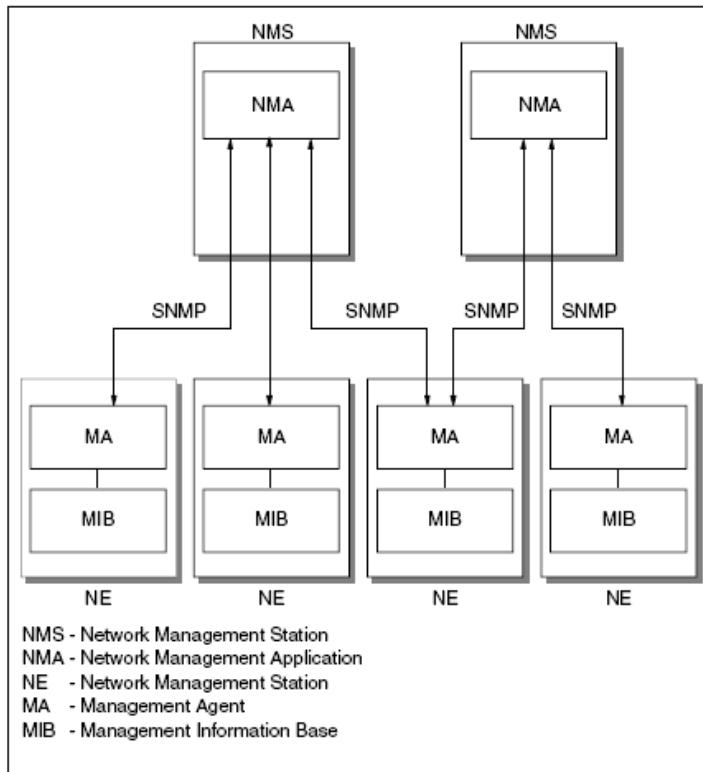
شکل ۱-۱۳: MIB-II- شناسه شئی تخصیصی برای شبکه مبتنی بر TCP/IP

SNMP : ۴-۱۳

Snmp حاصل بهبودهای سالها تجربه SGMP را در بردارد و مجاز است تا با اشیاء تعريف شده در MIB با توصیفات ارائه شده در SIM کار کند. RFC 1157 ایستگاه مدیریت شبکه (NMS^۱) را به عنوان یک مجری کاربردهای مدیریت شبکه(NMA^۲) که عناصر شبکه (NE^۳) همانند میزبانها، دروازه ها و پایانه های سرور را تحت نظارت و کنترل دارد. این عناصر شبکه از یک Agent مدیریتی(MA^۴) جهت اجرای توابع مدیریت شبکه مورد درخواست بوسیله ایستگاه های مدیریت شبکه،

Network Management Station -	¹
Network Management Applications -	²
Network Elements -	³
Management Agent -	⁴

استفاده می نمایند. SNMP جهت تبادل اطلاعات مدیریت شبکه بین ایستگاه های مدیریت شبکه و Agent ها در عناصر شبکه بکار می رود.



شکل ۲-۱۳: اجزاء SNMP

توابع مدیریت Agent شامل دو دسته متغیرهای تغییر دهنده (set) و یا بررسی کننده (get) می باشند که توابع اصلی مدیریت را ب دو دسته محدود می سازند و از پروتکلهای پیچیده بیشتر جلوگیری می کنند. از سوی دیگر، از NE به NMS، از تعداد محدودی پیام های ناخواسته (Trap)، جهت تعیین رویدادهای ناهمزمان استفاده می شود. به همین شکل در جهت حفظ سادگی، تبادل اطلاعات تنها نیازمند یک سرویس داده گرام نامطمئن می باشد و هر پیام بصورت کاملاً مجزا توسط یک داده گرام انتقالی، ارائه می گردد. همچنین این شیوه به معنی مناسب بودن SNMP برای استفاده با دامنه وسیعی از پروتکلهای انتقالی می باشد. RFC 1157، تبادل اطلاعات از طریق پروتکل UDP را مورد بحث قرار داده است؛ اما می توان از دامنه وسیعی از پروتکلهای انتقالی استفاده نمود. موجودیتهای مقیم در ایستگاه های مدیریتی و عناصر شبکه با یکدیگر، با استفاده از SNMP ارتباط دارند را موجودیتهای کاربرد SNMP^۱ می نامند. زوج پردازشی ایجاد کننده آن، موجودیتهای پروتکل^۲ می باشند. یک SNMP Agent با مجموعه دلخواهی از موجودیتهای کاربرد SNMP یک انجمن SNMP^۳ نامیده می شود که هر کدامشان برای مشخص بودن در زمان حضور در انجمن، بوسیله یک رشته ۸ تایی مشخص می گردند. یک پیام در پروتکل SNMP شامل شناسه نسخه، نام انجمن SNMP و یک PDU می باشد. لازم است تا تمام پیاده سازیهای SNMP از ۵ نوع PDU حمایت نمایند:

GetRequest : بازگردنده مقادیر یک شئی مشخص از MIB

GetNextRequest : حرکت در میان بخشی از MIB

SetRequest : تغییر مقادیر یک شئی خاص از MIB

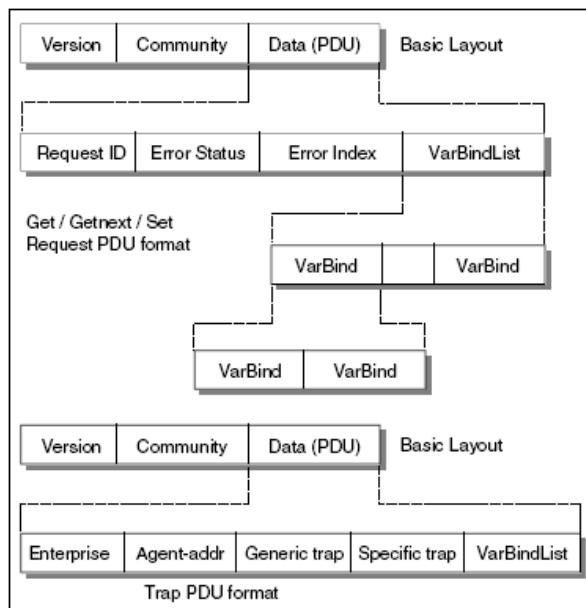
^۱ SNMP application entities

^۲ protocol entities

^۳ SNMP community

SetRequest و GetNextRequest، یک GetRequest و یک GetResponse : پاسخ یک GetResponse : توانایی اجزاء شبکه برای ایجاد رویدادهایی برای ایستگاه های مدیریت شبکه، همانند Trap : مقداردهی اولیه Agent restart و خطای پیوند. ۷ نوع Trap در RFC 1157 معرفی گردیده است: authenticationFailure، linkUp، linkDown، warmStart، coldStart، enterpriseSpecific و egpNeighborLoss

فرمت این پیامها به شکل زیر می باشد:



شکل ۳-۱۳: فرمت پیام -SNMP Request و set

در حال حاضر سه نسخه از SNMP موجود می باشد که به ترتیب SNMPv1، SNMPv2 و SNMPv3 نامیده می شود. توابع امنیتی موجود در SNMP به دو شکل زیر می باشد:

- مدل امنیتی مبتنی بر انجمن^۱، که در آن داده ها فقط توسط یک کلمه عبور که نام انجمن است حفاظت می شوند. این سطح امنیتی توسط مدل امنیتی مبتنی بر انجمن SNMPv1 و SNMPv2c فراهم می گردد.
- مدل امنیتی سطح کاربر(USM)، که سطوح امنیتی مختلف برپایه اطلاعات مدیریتی سطح دسترسی کاربر را فراهم می آورد. برای پشتیبانی از این سطح امنیتی، ساختار SNMPv3 توابع امنیتی متفاوتی را تعریف نموده است؛ همانند USM برای تایید اعتبار و پوشیدگی و مدل کنترل دسترسی مبتنی بر View(VACM)^۲) که توانایی کم کردن دسترسی به اشیاء MIB مختلف بر پایه یک per-user را فراهم می آورد و استفاده از تایید اعتبار و رمزگذاری داده برای پوشیدگی.

SNMPv2 : ۵-۱۳

community-based security model - ^۱
user-based security model - ^۲
view-based access control model - ^۳

ساختار SNMPv2 در آوریل ۱۹۹۳ ارائه گردید و مشتمل بر RFC12 می باشد که اولین آنها RFC 1441 می باشد که یک مقدمه است. در آگوست ۱۹۹۳، همه RFC ۱۲ در قالب یک استاندارد با وضعیت‌های انتخابی، ارائه گردید.

این ساختار دارای سیاستهای زیر می باشد:

- ساختار اطلاعات مدیریتی (SMI)**: تعاریف زیر مجموعه ASN.1 برای ایجاد مازولهای MIB (به RFC 2578 مراجعه شود).
- قردادهای متنی^۳**: تعاریف مجموعه اولیه قراردادهای متنی موجود در همه مازولهای MIB (به RFC 2579 مراجعه شود).
- اعمال پروتکل**: تعاریف عملکرد پروتکل با توجه به ارسال و دریافت PDU‌ها (به RFC 1905 مراجعه شود).
- نگاشت انتقال**: تعاریف نگاشت SNMPv2 به یک مجموعه اولیه از دامنه‌های انتقال، بدليل استفاده از آن در شرایط مختلف. نگاشت به UDP ارجح ترین نگاشت می باشد. همچنین RFC، IPX، DDP، OSI و ... را نیز تعریف نموده است (به RFC 1906 مراجعه گردد).
- تجهیزات پروتکل**: تعاریف MIB برای SNMPv2 (به RFC 1907 مراجعه شود).
- ساختار مدیریتی**: تعاریف ساختار مدیریتی SNMPv2، مدل مبتنی بر کاربر برای SNMPv2 و مدل مبتنی بر انجمان SNMPv2 (به RFC های ۱۹۰۹، ۱۹۱۰ و ۱۹۱۱ مراجعه شود).
- توضیحات تطبیق**: تعاریف توانایی‌های Agent (به RFC 2578 مراجعه شود).

SNMPv2 موجودیت

یک موجودیت SNMPv2 یک پردازش واقعیست که اعمال مدیریت شبکه را تولید / یا پاسخ به پیام‌های پروتکل SNMPv2 با استفاده از عملیاتهای پروتکل SNMPv2 انجام می دهد. همه اعمال ممکن یک موجودیت می تواند توسط یک زیر مجموعه از اعمال ممکن متعلق به دسته تعریف شده مدیریتی خاص، محدود گردد (بخش "دسته SNMPv2"^۱ را ببیند). یک موجودیت SNMPv2 می تواند عضو چند دسته SNMPv2 باشد. پایگاه داده‌های محلی زیر توسط یک موجودیت SNMPv2 نگهداری می شود:

- یک پایگاه داده برای تمام دسته‌های شناخته شده توسط موجودیت SNMPv2 که می تواند:
 - اعمال محلی
 - اعمال حاصل از تعاملات پروکسی با بخشها و یا ابزار راه دور
 - اعمال حاصل از سایر موجودیتهای SNMPv2

پایگاه داده دیگری که تمام منابع اشیاء مدیریت شده آشنا برای آن موجودیت SNMPv2 را در بردارد.

و حداقل یک پایگاه داده دیگر که ارائه دهنده یک سیاست کنترل دسترسیست که حقوق دسترسی مناسب با دسته‌های SNMPv2 را تعریف می نماید.

یک موجودیت SNMPv2 می تواند به عنوان یک Agent یا مدیر SNMPv2 عمل نماید.

1 Structure of Management Information -

2 Textual conventions -

3 SNMPv2 party -

دسته SNMPv2

یک دسته SNMPv2 یک محیط مفهومی با اجرای مجازی می باشد که عملکرد محدودی به جهت امنیت یا سایر اهداف، برای یک زیرمجموعه تعریف شده اجرایی برای همه اعمال ممکن یک موجودیت SNMPv2 مشخص را دارد (به بخش "موجودیت SNMPv2" مراجعه نمایید). به لحاظ معماری، هر دسته SNMPv2 شامل موارد زیر می باشد:

- یک شناسه یکه و واحد دسته.
- یک موقعیت منطقی شبکه که در آن دسته اجرا می گردد؛ و بوسیله اطلاعات دامنه پروتکل انتقال و آدرس انتقال مشخص می گردد.
- یک پروتکل تایید اعتبار و پارامترهای مرتبط بگونه ای که همه پیام های ناشی از پروتکل دسته، به عنوان اصلی و بدون عیب تایید اعتبار گردد.
- یک پروتکل محترمانگی و پارامترهای مرتبط، بگونه ای که تمام پیامهای پروتکل دریافتی دسته را در برابر افشا شدن، محافظت نماید.

GetBulkRequest

در RFC 1905 GetBulkRequest تعریف شده است و بنابراین بخشی از اعمال پروتکل می باشد. یک GetBulkRequest به عنوان یک درخواست یک کاربرد SNMPv2 تولید و منتقل می گردد. اهداف GetBulkRequest، جهت درخواست انتقال یک حجم بالقوه زیاد از اطلاعات، شامل ، اما نه محدود به ، بازیابی کارامد و سریع جداول بزرگ، می باشد. GetNextRequest از GetBulkRequest در بازیابی جداول بزرگ اشیاء MIB، کارامد تر می باشد. نحوه نگارش GetBulkRequest بصورت زیر می باشد:

```
GetBulkRequest [ non-repeaters = N, max-repetitions = M ]  
  ( RequestedObjectName1,  
    RequestedObjectName2,  
    RequestedObjectName3 )
```

که:

شناسه شئی MIB همانند sysUpTime و اشیاء به ترتیب فرهنگ لغت مرتب شده اند. هر شناسه شئی دارای ساختاری با حداقل یک متغیر می باشد. برای مثال، یک شناسه شئی ipNetToMediaPhysAddress دارای یک ساختار متغیر برای هر آدرس IP در جدول ARP و محتویت مرتبط با آدرس MAC ، می باشد. مقادیر غیر تکراری را مشخص می نماید که به معنی آنست که شما تنها محتویات متغیر بعدی به شئی مشخصی را در درخواست خود از N شئی اول نام بده شده در بین پرانتزها، می خواهید. این همانند عملکرد GetNextRequest می باشد.

M: مقدار حداکثر بازتکرارها^۱ را که به معنی درخواست شما از باقیمانده (تعداد درخواست شده اشیاء N) اشیاء محتوى متغیرهای M بعدی به اشیاء مشخص شده توسط شما در درخواست می باشد را مشخص می نماید. همانند یک GetNextRequest تکرار شده است اما تنها یک درخواست را منتقل می گردد.

با GetBulkRequest شما می توانید بطور موثر محتویات متغیر بعدی یا M متغیر بعدی را با تنها یک درخواست بدست آورید.

¹ max-repetitions –

جدول ARP زیر را برای یک میزبان مجری SNMPv2 agent در نظر بگیرید:

Interface-Number	Network-Address	Physical-Address	Type
1	10.0.0.51	00:00:10:01:23:45	static
1	9.2.3.4	00:00:10:54:32:10	dynamic
2	10.0.0.15	00:00:10:98:76:54	dynamic

تصویر ۱۳-۴: جدول ARP یک میزبان مجری SNMPv2 agent

یک مدیر SNMPv2 درخواست زیر را برای کسب sysUpTime تکمیل جدول ARP می فرستد:

```
GetBulkRequest [ non-repeaters = 1, max-repetitions = 2 ]
  ( sysUpTime,
    ipNetToMediaPhysAddress,
    ipNetToMediaType )
```

موجودیت SNMPv2 نقش یک Agent را بازی کرده و اطلاعات زیر را در قالب یک PDU ارسال می کند:

```
Response (( sysUpTime.0 = "123456" ),
  ( ipNetToMediaPhysAddress.1.9.2.3.4 = "000010543210" ),
  ( ipNetToMediaType.1.9.2.3.4 = "dynamic" ),
  ( ipNetToMediaPhysAddress.1.10.0.0.51 = "000010012345" ),
  ( ipNetToMediaType.1.10.0.0.51 = "static" ))
```

موجودیت SNMPv2 در نقش یک مدیر پاسخ را چنین ادامه می دهد:

```
GetBulkRequest [ non-repeaters = 1, max-repetitions = 2 ]
  ( sysUpTime,
    ipNetToMediaPhysAddress.1.10.0.0.51,
    ipNetToMediaType.1.10.0.0.51 )
```

موجودیت SNMPv2 در نقش یک Agent پاسخ را چنین ادامه می دهد:

```
Response (( sysUpTime.0 = "123466" ),
  ( ipNetToMediaPhysAddress.2.10.0.0.15 = "000010987654" ),
  ( ipNetToMediaType.2.10.0.0.15 = "dynamic" ),
  ( ipNetToMediaNetAddress.1.9.2.3.4 = "9.2.3.4" ),
  ( ipRoutingDiscards.0 = "2" ))
```

این پاسخ نشانگر پایان جدول برای موجودیت SNMPv2 در نقش یک مدیر می باشد. با کمک GetNextRequest شما نیازمند ۴ درخواست برای بازگرداندن همین اطلاعات می باشید. اگر در این مثال، مقدار حداکثر بازتکرار برای GetBulkRequest را ۳ تعیین می گردید، تنها نیازمند یک درخواست بودیم.

InformRequest

یک InformRequest به عنوان یک درخواست از یک کاربرد در یک موجودیت مدیر SNMPv2 به جهت آگاه سازی کاربرد دیگری که به عنوان یک موجودیت مدیر SNMPv2 نیز عمل می نماید، از اطلاعات MIB View یک دسته محلی برای کاربرد ارسال، تولید و ارسال می گردد. بسته به عنوان یک خبر برای مدیر دسته ای دیگر در مورد اطلاعات قابل دسترسی از دسته مبداء (ارتباط مدیر با مدیر از طریق مزهای دسته ها) بکار می رود. دو متغیر اول در لیست متغیرهای یک InformRequest از نوع sysUpTime.0 و sysUpTime.i snmpEventID می باشند.

SNMPv2 برای MIB ۶-۱۳

این MIB اشیاء مدیریت شده توصیف کننده رفتار موجودیت SNMPv2 را تعریف می کند. اما یک جایگزین MIB-II نیست. در زیر جهت درک بهتر موضوع نمونه ای آورده شده است:

```
sysName OBJECT-TYPE
  SYNTAX          DisplayString (SIZE (0..255))
  MAX-ACCESS      read-write
  STATUS          current
```

```

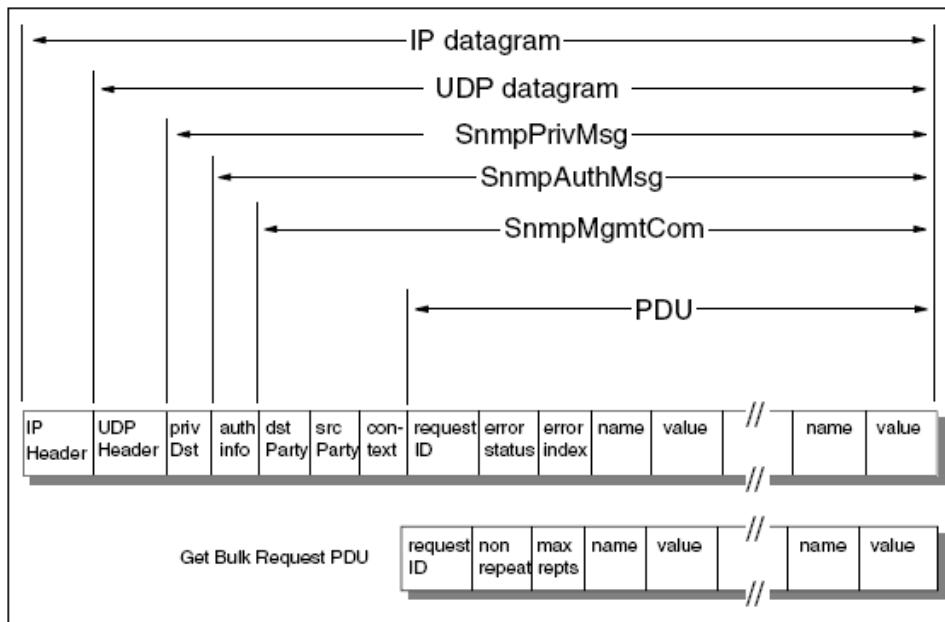
DESCRIPTION
    "An administratively-assigned name for this managed node.
     By convention, this is the node's fully-qualified domain
     name. If the name is unknown, the value is the zero-length
     string."
::= { system 5 }
warmStart NOTIFICATION-TYPE
STATUS current
DESCRIPTION
    "A warmStart trap signifies that the SNMPv2
     entity, acting in an agent role, is reinitializing
     itself such that its configuration is unaltered."
::= { snmpTraps 2 }

```

۷-۱۳: مدل جدید مدیریت

هدف مدل مدیریتی برای SNMPv2 تعریف نحوه اعمال ساختار مدیریتی جهت کسب مدیریت شبکه موثر در پیکربندی ها و محیط های مختلف می باشد.

مدل مستلزم استفاده از شناسه هایی برای زوج هایی است که پیام های SNMPv2 را مدیریت می نمایند. بنابراین، از مدل مدیریتی مبتنی بر انجمان در SNMPv1 صرفه نظر شده است. با تعریف بدون ابهام مبداء و نامزد دریافت کننده هر پیام SNMPv2، این استراتژی جدید برپایه طرح انجمانی قدیمی برای هر دو با حمایت از یک مدل کنترل دسترسی مناسب تر به همراه اجازه استفاده موثر از پروتکلهای امنیتی نامتفقان (کلید عمومی) در آینده، بھبود می یابد. تصویر زیر فرمت پیام جدید را نشان می دهد.



SNMPv2: فرمت پیام ۵-۱۳

: شامل یکی از PDU هی زیر می باشد:

- GetNextRequest ○
- GetRequest ○
- Inform ○
- Report ○
- Response ○
- SNMPv2-Trap ○
- SetRequest ○

SNMP Trap دارای فرمت PDU متفاوتی است که قبلاً تشریح گردید. GetBulkRequest حال حاضر فرمتی مشابه با سایر درخواستها دارد.

snmpMgmtCom : ID دسته مبدأ (srcParty)، ID دسته مقصد (dstParty) و محتويات

PDU را اضافه می کند. محتويات شامل اطلاعات مدیریتی مورد ارجاع در ارتباط می باشد.

snmpAuthMsg : اين فيلد به عنوان اطلاعات تایید اعتبار از پروتکل تایید اعتبار مورد استفاده

بوسيله آن دسته، يکار می رود. snmpAuthMsg براساس ASN.1 BER¹ سريال گذاري شده و قابلیت رمز نگاری دارد.

snmpPrivMsg : پیام خصوصی SNMPv2 یک ارتباط مدیریت شده حاوی تایید اعتبار

SNMPv2 می باشد که (احتمالاً) از افشاء شدن محفوظ است. یک مقصد خصوصی (privDst) به

آدرس دسته مقصد افزوده شده است.

سپس اين پیام در داده گرام متداول UDP/IP محصور شده و از طریق شبکه برای مقصد ارسال می گردد.

SNMPv3

SNMPv3 گستره دیگری از معماری SNMP می باشد و در RFC های ۲۵۷۰ تا ۲۵۷۳ تشریح شده است.

SNMPv3 موارد زیر را پشتیبانی می نماید:

فرمت جدید پیام

تایید اعتبار برای پیام ها

امنیت برای پیام ها

کنترل دسترسی

حمایت از SNMPv2

مدل امنیتی مبتنی بر کاربر تشریح شده در RFC 2574 از MD5 و الگوریتمهای Hash استفاده می نماید. این امر زمینه ساز جامعیت، امنیت و پوشیدگی داده می باشد. همچنین از پروتکلهای تایید اعتبار- HMAC-MD5-96، HMAC-SHA-96 و بوصورت اختیاری، پروتکل رمزگذاری CBC-DES حمایت می نماید.

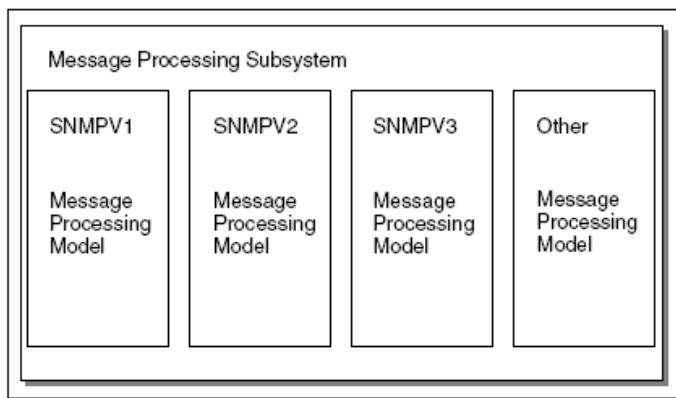
مدل کنترل دسترسی مبتنی بر View در RFC 2575، نحوه تعریف View ها به عنوان زیر مجموعه هایی از درخت کامل MIB را نشان می دهد. سپس کنترل دسترسی برای این View ها در دسترس می باشد.

به دلیل ساختار مازولهار SNMP، تغییر مازولهای مجزا، تغییر مستقیمی بر سایر مازولهای ندارد. این امر امکان تعريف SNMPv3 را بر روی مدل موجود فراهم می سازد. برای مثال، برای افزودن فرمت جدید پیام SNMPv2 و SNMPv3 را به زیر سیستم پردازش پیام، افزود. تصویر زیر ساختار طرح را نمایش می دهد.

پروتکل تایید اعتبار و پوشیدگی

پروتکل تایید اعتبار مکانیزمی را فراهم می سازد که به وسیله آن ارتباطات مدیریتی SNMPv3 منتقل شده از یک دسته، می تواند قابلیت اعتماد شروع از آن دسته را فراهم آورند. پروتکل پوشیدگی مکانیزمی را فراهم می آورد که به وسیله آن ارتباطات مدیریتی SNMPv3 منتقل شده به یک دسته، در برابر افشاء شدن حفاظت گردد. رفتارهای عده ای که پروتکل امنیتی SNMPv3 در برابر آنها مصونیت ایجاد می نماید عبارتند از:

¹ - ASN.1 BER specifies the Basic Encoding Rules for OSI Abstract Syntax Notation One, according to ISO 8825.



شکل ۱۳-۶: زیر سیستم پردازش پیام SNMP

- تغییر اطلاعات
- تغییر ظاهر^۱
- تغییر جریان پیام
- افشاء شدن

سرویسهای امنیتی زیر حفاظت لازم در برابر رفتارهای بالا فراهم می‌آورند:

- جامعیت داده:** بوسیله الگوریتم digest پیام DM5 فراهم می‌گردد. یک ۱۲۸ digest بیتی بر روی بخش طرح شده یک پیام SNMPV3 محاسبه شده و به عنوان بخشی از پیام، به گیرنده ارسال می‌گردد.
- تایید اعتبار داده در مبداء:** به بوسیله یک پیشوند برای هر پیام با یک مقدار سرّی مشترک شده بین مبداء پیام و گیرنده آن قبل از digest.
- تاخیر یا بازپس فرستادن پیام:** فراهم شده بوسیله یک مقدار timestamp در هر پیام.
- محرمانگی داده:** فراهم شده بوسیله پروتکل پوشیدگی متقارن که بخش مقتضی از پیام را براساس یک کلید سرّی که تنها برای فرستنده و گیرنده پیام آشناست، رمز می‌گردد. این پروتکل با الگوریتم رمز نگاری متقارن، در مد بلاک سرّی زنجیره‌ای، که بخشی از DES است، بکار می‌رود. بخش مشخص شده یک پیام SNMPV3 رمز نگاری شده و به عنوان بخشی از پیام ارسالی به مقصد، به آن افزوده می‌گردد.

^۱ Masquerade –

بخش ۵:

شبکه های بی سیم

فصل ۱۴: شبکه های محلی بی سیم

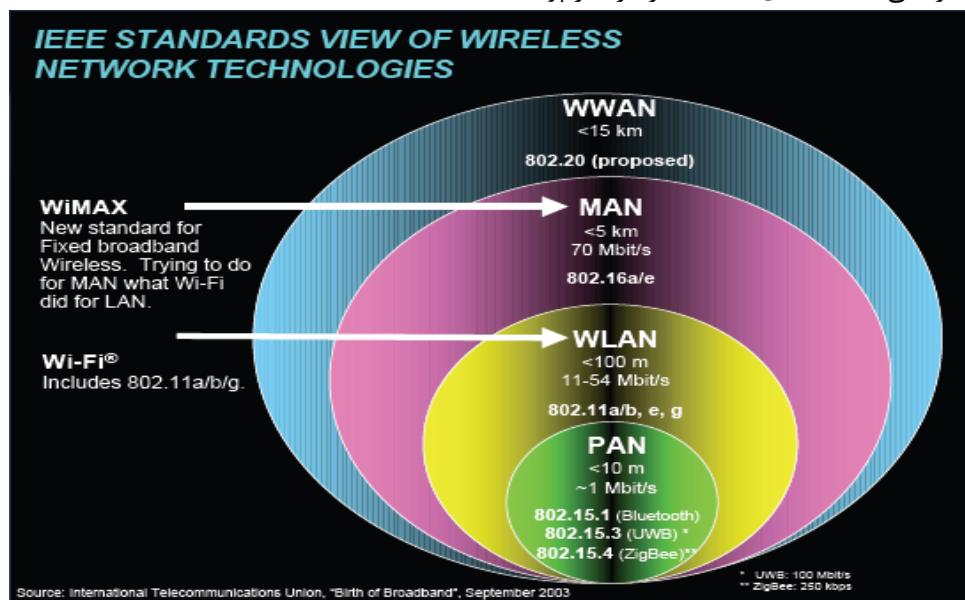
فصل ۱۴:

شبکه های محلی بی سیم

وقتی از شبکه سخن به میان می‌آید، اغلب کابل شبکه به عنوان وسیله انتقال داده در نظر گرفته می‌شود. در حالیکه چندین سال است که استفاده از شبکه سازی بی‌سیم در دنیا آغاز گردیده است. تا همین اواخر یک LAN بی‌سیم با سرعت انتقال پایین و خدمات غیرقابل اعتماد و مترادف بود، اما هم اکنون فناوریهای LAN بی‌سیم خدمات قابل قبولی را با سرعتی که حداقل برای کاربران معمولی شبکه کابلی پذیرفته شده می‌باشد، فراهم می‌کنند. تکنولوژی شبکه‌های بی‌سیم، با استفاده از انتقال داده‌ها توسط امواج رادیویی، در ساده‌ترین صورت، به تجهیزات سخت‌افزاری امکان می‌دهد تا بدون استفاده از بسترهای فیزیکی همچون سیم و کابل، با یکدیگر ارتباط برقرار کنند. شبکه‌های بی‌سیم بازه‌ی وسیعی از کاربردها، از ساختارهای پیچیده‌ی چون شبکه‌های بی‌سیم سلولی - که اغلب برای تلفن‌های همراه استفاده می‌شود - و شبکه‌های محلی بی‌سیم (WLAN) گرفته تا انواع ساده‌بی‌چون هدفون‌های بی‌سیم، را شامل می‌شوند. از سوی دیگر با احتساب امواجی همچون مادون قرمز، تمامی تجهیزاتی که از امواج مادون قرمز نیز استفاده می‌کنند، مانند صفحه کلیدها، ماوس‌ها و برخی از گوشی‌های همراه، در این دسته‌بندی جای می‌گیرند. طبیعی‌ترین مزیت استفاده از این شبکه‌ها عدم نیاز به ساختار فیزیکی و امکان نقل و انتقال تجهیزات متصل به این گونه شبکه‌ها و همچنین امکان ایجاد تغییر در ساختار مجازی آن‌هاست. از نظر ابعاد ساختاری، شبکه‌های بی‌سیم به سه دسته تقسیم می‌گردند: WPAN، WLAN و WWAN.

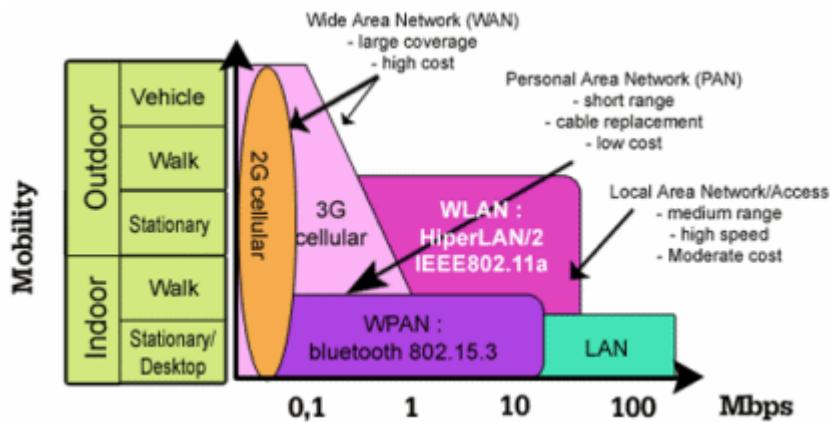
مفهوم از WWAN، که مخفف Wireless WAN است، شبکه‌ایی با پوشش بی‌سیم بالاست. نمونه‌یی از این شبکه‌ها، ساختار بی‌سیم سلولی مورد استفاده در شبکه‌های تلفن همراه است. WLAN پوششی محدود‌تر، در حد یک ساختمان یا سازمان، و در ابعاد کوچک یک سالن یا تعدادی اتاق، را فراهم می‌کند. کاربرد شبکه‌های WPAN^۱ یا برای موارد خانه‌گی است. ارتباطاتی چون Bluetooth و مادون قرمز در این دسته قرار می‌گیرند.

شبکه‌های WPAN از سوی دیگر در دسته‌ی شبکه‌های Ad Hoc نیز قرار می‌گیرند. در شبکه‌های Ad hoc یک سخت‌افزار، به‌محض ورود به فضای تحت پوشش آن، به‌صورت پویا به شبکه اضافه می‌شود. مثالی از این نوع شبکه‌ها، Bluetooth است. در این نوع، تجهیزات مختلفی از جمله صفحه کلید، ماوس، چاپگر، کامپیوتر کیفی یا جیبی و حتی گوشی تلفن همراه، در صورت قرار گرفتن در محیط تحت پوشش، وارد شبکه شده و امکان رد و بدل داده‌ها با دیگر تجهیزات متصل به شبکه را می‌یابند. تفاوت میان شبکه‌های Ad hoc با شبکه‌های محلی بی‌سیم در ساختار مجازی آن‌هاست. به عبارت دیگر، ساختار مجازی شبکه‌های محلی بی‌سیم بر پایه‌ی طرحی ایستاست درحالی‌که شبکه‌های Ad hoc از هر نظر پویا هستند.



تصویر ۱-۱۴: انواع متفاوت شبکه‌های بی‌سیم

۱- Wireless Personal Area Network



تصویر ۲-۱۴: نمودار سرعت انواع مختلف شبکه های بی سیم

۱-۱۴: شبکه های محلی بی سیم

اولین شبکه محلی بی سیم تجاری توسط Motorola پیاده‌سازی شد. این شبکه، به عنوان یک نمونه از این شبکه‌ها، هزینه بالا و پهنای باندی پایین را تحمیل می‌کرد که ابداً مقرنون به صرفه نبود. از همان زمان به بعد، در اوایل دهه ۹۰ میلادی، پروژه‌ی استاندارد ۸۰۲.۱۱ در IEEE شروع شد. پس از نزدیک به ۹ سال کار، در سال ۱۹۹۹ استانداردهای ۸۰۲.۱۱a و ۸۰۲.۱۱b توسط IEEE نهایی شده و تولید محصولات بسیاری بر پایه یعنی استانداردها آغاز شد. نوع a، با استفاده از فرکانس حامل 5GHz، پهنای باندی تا 54Mbps را فراهم می‌کند. در حالی که نوع b با استفاده از فرکانس حامل 2.4GHz، تا 11Mbps پهنای باند را پشتیبانی می‌کند. با این وجود تعداد کانال‌های قابل استفاده در نوع b در مقایسه با نوع a، بیشتر است. تعداد این کانال‌ها، با توجه به کشور مورد نظر، تفاوت می‌کند. در حالت معمول، مقصود از WLAN استاندارد ۸۰۲.۱۱b است.

WLAN (بی سیم) از امواج الکترومغناطیسی (رادیویی یا مادون قرمز) برای انتقال اطلاعات از یک نقطه به نقطه دیگر استفاده می‌کنند. امواج رادیویی اغلب به عنوان یک حامل رادیویی تلقی می‌گردند، چرا که این امواج وظیفه انتقال انرژی الکترومغناطیسی از فرستنده را به گیرنده دورتر از خود بعده دارند. داده هنگام ارسال برروی موج حامل رادیویی سوار می‌شود و در گیرنده نیز به راحتی از موج حامل تفکیک می‌گردد. به این عمل مدولاسیون اطلاعات به موج حامل گفته می‌شود. هنگامیکه داده با موج رادیویی حامل مدوله می‌شود، سیگنال رادیویی دارای فرکانس‌های مختلفی علاوه بر فرکانس اصلی موج حامل می‌گردد. به عبارت دیگر فرکانس اطلاعات داده به فرکانس موج حامل اضافه می‌شود. در گیرنده رادیویی برای استخراج اطلاعات، گیرنده روی فرکانس خاصی تنظیم می‌گردد و سایر فرکانس‌های اضافی فیلتر می‌شوند.

توپولوژی این شبکه‌ها بصورت پویا می‌باشد و به دلایلی همچون نیاز به مصرف توان پایین، این شبکه‌ها عمدهاً بصورت اتصال کامل تمام گره‌ها به آن قرار ندارد. انتشار امواج در این شبکه‌ها، متقاضان نیست و بدليل کار برخی از اینها در فرکانس 2.4 GHz امواج رادیویی، امکان تداخل امواج این شبکه‌ها با شبکه‌های بی سیم دیگر، تلفن‌های بی سیم، و امواج مایکروویو، وجود دارد.

ساختار و اجزای شبکه محلی بی سیم:

در یک WLAN، عمدهاً، یک دستگاه فرستنده و گیرنده مرکزی به نام نقطه دسترسی(AP^۱) وجود دارد. AP با استفاده از کابل شبکه استاندارد، به شبکه محلی سیمی متصل می‌گردد. در حالت ساده، گیرنده AP وظیفه دریافت، ذخیره و ارسال داده را بین شبکه محلی سیمی و WLAN بعده دارد. AP با آنتنی که به آن متصل است، می‌تواند در

^۱ Access Point –

محل مرتفع و یا هر مکانی که امکان ارتباط بهتر را فراهم می‌کند، نصب شود. هر کاربر می‌تواند از طریق یک کارت شبکه بی‌سیم^۱، به WLAN متصل شود. این کارت‌ها به صورت استاندارد برای رایانه‌های شخصی و کیفی ساخته می‌شوند. کارت WLAN به عنوان واسطه بین سیستم عامل شبکه کاربر و امواج دریافتی از آتن عمل می‌کند. سیستم عامل شبکه عملاً درگیر چگونگی ارتباط ایجاد شده نخواهد بود.

WLAN‌ها از دو توپولوژی حمایت می‌کنند:

- توپولوژی Ad hoc^۲
- توپولوژی ساختاردار^۳

در توپولوژی Ad hoc کامپیوترها به شبکه بی‌سیم مجهز هستند و مستقیماً با یکدیگر به شکل نظیر به نظیر^۴، ارتباط برقرار می‌نمایند. کامپیوترها برای ارتباط باید در محدوده یکدیگر قرار داشته باشند. این نوع شبکه برای پشتیبانی از تعداد محدودی از کامپیوترها، مثلاً در محیط خانه یا دفاتر کوچک طراحی می‌شود.

این نوع شبکه که به شبکه Mesh نیز معروف است، شبکه‌ای پویا از دستگاه‌های بی‌سیم است که به هیچ نوع زیرساخت موجود یا کنترل مرکزی وابسته نیست. در این شرایط، دستگاه‌های شبکه همچنین به مانند گره‌هایی عمل می‌کنند که کاربران از طریق آنها می‌توانند داده‌ها را انتقال دهند، به این معنی که دستگاه هر کاربر بعنوان مسیریاب و تکرارکننده، عمل می‌کند. این شبکه نوع تکامل‌یافته شبکه Point-to-Multipoint است که در آن همه کاربران می‌باشد برای استفاده از شبکه دسترسی مستقیم به نقطه دستیابی مرکزی داشته باشند. در معماری Mesh کاربران می‌توانند بوسیله چند پرش^۵، از طریق گره‌های دیگر به نقطه مرکزی وصل شوند، بدون اینکه به ایجاد هیچگونه پیوند مستقیم RF نیاز باشد. بعلاوه در شبکه Mesh در صورتیکه کاربران بتوانند یک پیوند فرکانس رادیویی برقرار کنند، نیازی به AP نیست و کاربران می‌توانند بدون وجود یک نقطه کنترل مرکزی با یکدیگر، فایلها، نامه‌های الکترونیکی و صوت و تصویر را به اشتراک بگذارند. این ارتباط دو نفره، به آسانی برای دربرگرفتن کاربران بیشتر قابل گسترش است.

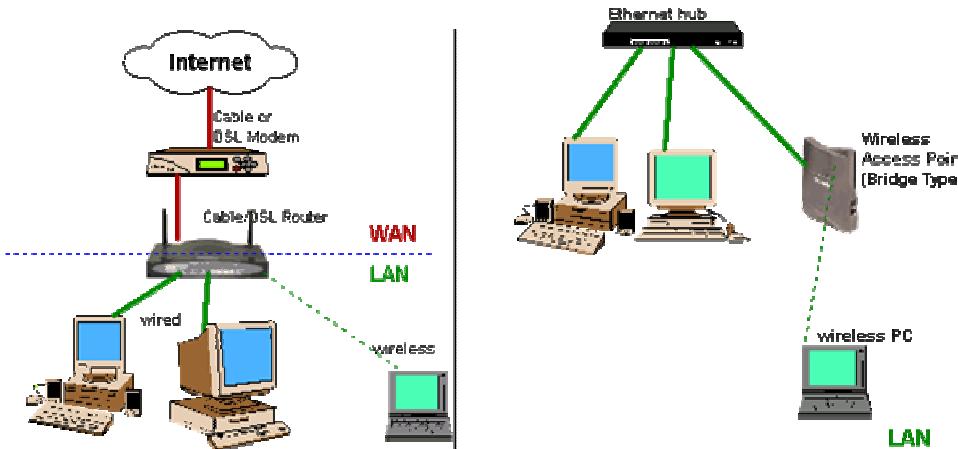
توپولوژی ساختاردار اصولاً برای گسترش و افزایش انعطاف‌پذیری شبکه‌های کابلی معمولی بکار می‌رود. بدین شکل که اتصال کامپیوترهای مجهز به تکنولوژی بی‌سیم را با استفاده از AP به آن ممکن می‌سازد. در برخی موارد، یک AP کامپیوتری است که کارت شبکه بی‌سیم را کنار کارت شبکه معمولی، که AP را به یک LAN کابلی متصل می‌کند، دارا می‌باشد. کامپیوترهای بی‌سیم با استفاده از AP به عنوان واسطه با شبکه کابلی ارتباط برقرار می‌کنند. اساساً عنوان یک پل عمل می‌کند، زیرا سیگنال‌های شبکه بی‌سیم را به سیگنال‌های شبکه کابلی تبدیل می‌کند. مانند تمام تکنولوژی‌های ارتباطی بی‌سیم، شرایط مسافتی و محیطی می‌توانند بر روی عملکرد ایستگاه‌های سیار بسیار تأثیر گذار باشند. یک AP می‌تواند ۱۰ تا ۲۰ کامپیوتر را پشتیبانی کند، بسته به اینکه میزان استفاده آنها از LAN چقدر است. این پشتیبانی تا زمانی ادامه دارد که آن کامپیوترها در شعاع تقریبی ۱۰۰ تا ۲۰۰ فوت نسبت به AP قرار داشته باشند. موانع فیزیکی مداخله کننده این عملکرد را به طرز چشمگیری کاهش می‌دهند.

۱ Wireless Adapter -

۲ Infrastructure -

۳ Peer to Peer -

۴ Multi-Hop -

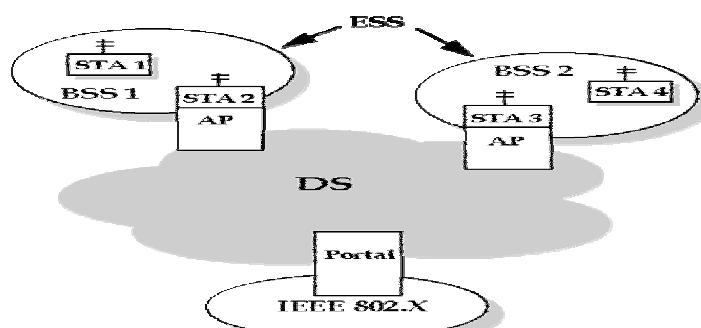


تصویر ۱۴-۳: شیوه های اتصال شبکه بی سیم به شبکه سیمی و اینترنت

در شکل فوق یک AP از طریق یک کابل به شبکه LAN متصل شده است. در اینجا وظیفه یک AP دریافت اطلاعات از سرویس گیرندها از طریق هوا و ارسال آن اطلاعات از طریق یک پورت به Hub می باشد. AP به عنوان یک پل ارتباطی بین شبکه WLAN و شبکه LAN عمل می کند.

ناحیه ای که توسط یک AP تحت پوشش قرار می گیرد^۱ (و در برخی موارد سلول) نامیده می شود. هر ایستگاه در داخل BSS می تواند به AP دسترسی پیدا کند. وظیفه یک AP ایجاد هماهنگی بین سرویس گیرندها شبکه WLAN و یک شبکه LAN می باشد.

به منظور گسترش بخش بی سیم و تحت پوشش قرار دادن سرویس گیرندها بیشتر، می توان از AP های متعدد در مناطق مختلف استفاده کرد، و یا اینکه یک نقطه توسعه (EP)^۲ را بکار گرفت. EP، یک تقویت کننده سیگنال های بی سیم است که به عنوان ایستگاهی بین سرویس گیرندها بی سیم و AP عمل می کند. اگر شبکه از چند BSS استفاده کند، BSS ها بوسیله یک ستون فقرات بنام سیستم توزیع (DS)^۳ به هم اتصال می یابند. DS عموماً یک شبکه کابلی است، اما می توان آن را بی سیم هم در نظر گرفت. همچنین به چنین طرحی که شامل چند BSS می باشد، ESS^۴، می گویند.



تصویر ۱۴-۴: یک شبکه محلی بی سیم چند بخشی

شعاع پوشش شبکه بی سیم بر اساس استاندارد ۸۰۲.۱۱ به فاکتورهای بسیاری بستگی دارد که برخی از آنها به شرح زیر هستند :

- پهنهای باند مورد استفاده

Basic Service Set - ^۱

Extension point - ^۲

Distribution System - ^۳

Extended Service Set - ^۴

- منابع امواج ارسالی و محل قرارگیری فرستندهها و گیرندهها
- مشخصات فضایی قرارگیری و نصب تجهیزات شبکه‌ی بی‌سیم
- قدرت امواج
- نوع و مدل آتن

شعاع پوشش از نظر تنوری بین ۲۹ متر (برای فضاهای بسته‌ی داخلی) و ۴۸۵ متر (برای فضاهای باز) در استاندارد 802.11b متغیر است. با این وجود این مقادیر، مقادیری متوسط هستند و در حال حاضر با توجه به گیرنده‌ها و فرستنده‌های نسبتاً قدرتمندی که مورد استفاده قرار می‌گیرند، امکان استفاده از این پروتکل و گیرنده‌ها و فرستنده‌های آن، تا چند کیلومتر هم وجود دارد که نمونه‌های عملی آن فراوان‌اند.

با این وجود شعاع کلی که برای استفاده از این پروتکل (802.11b) ذکر می‌شود چیزی میان ۵۰ تا ۱۰۰ متر است. این شعاع عملکرد مقداریست که برای محل‌های بسته و ساختمان‌های چند طبقه نیز معتبر بوده و می‌تواند مورد استناد قرار گیرد.

Countries	Frequency range	Maximum RF power level	Rules for DSSS and FHSS
U.S. ¹ , Canada, and Latin America (FCC Part 15,247)	902-928 MHz 2,400-2,483.5 MHz 5,750-5,850 MHz	1W (at ERP, ² and maximum 6 dBi antenna gain)	DSSS: Receiver processing gain >10 dB FHSS: 75 hops or more
Europe, ³ (ETSI ⁴ 300 328)	2,400-2,483.5 MHz	100 mW (at EIRP, ⁵)	DSSS: Power spectrum density maximum 10 mW/MHz FHSS: 20 hops or more
Japan (MPT, ⁶ Ordinances 78 and 79)	2,471-2,497 MHz	Not specified	DSSS/FHSS: Power spectrum density maximum 10 mW/MHz
Australia	2,400-2,450 MHz	500 mW	

1. In Canada, not the 5,750-5,850-MHz band
2. ERP-Effectively radiated power
3. In France/Spain, only the 2,445-2,483.5/2,475-MHz band
4. ETS-European Telecommunication Standard
5. EIRP-Equivalent isotropically radiated power

MPT-Ministry of Posts and Telecommunications (in Japan)

جدول ۱-۱۴: سطوح پهنه‌ای باند و توان مصرفی در شبکه‌های محلی بی‌سیم

۲-۱۴: شبکه‌های بی‌سیم، مزایا و معایب

در این قسمت به برخی مزایای یک WLAN نسبت به یک شبکه کابلی می‌پردازیم. از WLAN‌ها می‌توان در مکانهایی که امکان کابل‌کشی وجود ندارد استفاده کرد و بدون نیاز به کابل‌کشی آنها را گسترش داد. استفاده کننده WLAN می‌تواند کامپیوتر خود را بدون قطع کابل، به هر نقطه از سازمان منتقل کند. با وجود اینکه سخت‌افزار مورد نیاز برای WLAN گرانتر از تجهیزات شبکه سیمی است، ولی بهره‌وری و انعطاف‌پذیری آن باعث می‌شود که در طول زمان قیمت تمام شده کمتر شود، بخصوص در محیطهایی که شبکه مورد نظر پیوسته در حال انتقال و تغییر مدام است.

سیستمهای WLAN می‌توانند با فناوریهای مختلف شبکه ترکیب شوند و شبکه‌هایی با کاربردها و امکانات خاص را به نحو مطلوبی ایجاد کنند. پیکربندی این شبکه‌ها براحتی قابل تغییر است و این شبکه‌ها می‌توانند از حالت نقطه به نقطه تا شبکه‌هایی با زیرساختار پیچیده با صدها کاربر متحرک گسترش یابند. در شبکه‌های بی‌سیم مدیران شبکه می‌توانند جابجایی، گسترش و اصلاح شبکه را آسانتر انجام دهند و با استفاده از این سیستم به نصب کامپیوترهای شبکه در ساختمانهای قدیمی و یا مکانهایی که امکان کابل‌کشی در آنها وجود ندارد و نیز مکانهایی که فاصله آنها از یکدیگر زیاد است بپردازنند و بدین شکل امکان دسترسی سریع به اطلاعات را فراهم کنند.

- با وجود تمام این مزایا، می‌توان موارد زیر را جزو معایب شبکه‌های بی‌سیم نامید:
- محدودیت پهنه‌ای باند: علاوه بر محدودیتهای پهنه‌ای باند **ISM** در نقاط مختلف دنیا، محدودیتهای دیگر پهنه‌ای باند نیز وضع می‌گردد که خود عاملی جهت کاهش پهنه‌ای باند می‌باشد.
 - محدودیت توان مصرفی: بدلیل سیار بودن ایستگاه‌ها در این شبکه، آنها باید از انرژی ذخیره شده در باتریهای خود استفاده نمایند. این موضوع نیازمندی به شیوه‌های کاهش توان مصرفی در ابزارهای متحرک را شدیداً تحت تأثیر قرار می‌دهد.
 - توان خروجی محدود: توان خروجی محدود **IEEE 802.11** زمینه کاهش برد امواج را فراهم می‌آورد. به همین دلیل، جهت افزایش برد شبکه، نیازمند استفاده از سخت افزار اضافی هستیم که این خود باعث افزایش هزینه‌های ایجاد و نگهداری شبکه می‌گردد.
 - امنیت فیزیکی محدود: نویز پذیری این شبکه‌ها بالا می‌باشد و همچنین بدلیل عدم وجود رسانه سخت افزاری انتقال داده (رسانه انتقال داده هوا است)، هیچ کنترل و محدودیتی در جلوگیری از شنود غیر مجاز داده‌های ارسالی در شبکه، وجود ندارد.
 - تپولوزی پویا: وجود ساختارهای پویا، زمینه ساز ایجاد شیوه‌های مدیریتی پیچیده گره‌های شبکه، می‌باشد.
 - انتقال چند مسیره یک ارسال: بدلیل انتشار امواج در هوا، امکان انتقال اطلاعات ارسالی یکسان در شبکه، توسط چند گره مختلف وجود دارد.
 - کیفیت پایین کانالهای رادیویی: امواج رادیویی در برابر نویزها بسیار حساس و آسیب پذیر می‌باشد.

پارامترهای مؤثر در انتخاب و پیاده‌سازی یک سیستم WLAN:

۱. برد محدوده پوشش: اثر متقابل اشیاء موجود در ساختمان (نظیر دیوارها، فلزات و افراد) می‌تواند بر روی انرژی انتشار اثر بگذارد و در نتیجه برد و محدوده پوشش سیستم را تحت تأثیر قرار دهد. برای سیگنالهای مادون قرمز، اشیاء موجود در ساختمان مانع دیگر بشمار می‌رود و در نتیجه محدودیتهای خاصی را در شبکه بوجود می‌آورد. بیشتر سیستمهای WLAN از امواج رادیویی RF استفاده می‌کنند، زیرا می‌تواند از دیوارها و موانع عبور کند. برد (شعاع پوشش) برای سیستمهای WLAN بین ۱۰ تا ۳۰ متر متغیر است.
۲. سرعت انتقال داده: همانند شبکه‌های کابلی، سرعت انتقال داده واقعی در شبکه‌های بی‌سیم، به نوع محصولات و تپولوزی شبکه بستگی دارد. تعداد کاربران، فاکتورهای انتشار مانند برد، مسیرهای ارتباطی، نوع سیستم WLAN استفاده شده، نقاط کور و گلوگاههای شبکه، از پارامترهای مهم و تأثیرگذار در سرعت انتقال داده بحسب می‌آیند. عنوان یک مقایسه با مودمهای امروزی (با سرعت ۵۶ کیلو بیت در ثانیه) سرعت عملکرد WLAN ها در حدود ۳۰ برابر سریعتر از این مودمهاست.
۳. سازگاری با شبکه‌های موجود: بیشتر سیستمهای WLAN با استانداردهای صنعتی متداول شبکه‌های کابلی نظیر Ethernet و Token Ring سازگار است. با نصب درایورهای مناسب در ایستگاههای WLAN، سیستمهای عامل آن ایستگاهها دقیقاً مانند سایر ایستگاههای موجود در شبکه LAN کابلی بکار گرفته می‌شود. سازگاری با دیگر محصولات WLAN: به سه دلیل مشتریان هنگام خرید محصولات WLAN باید مراقب باشند که سیستم موردنظر بتواند با سایر محصولات WLAN تولیدکنندگان دیگر سازگاری داشته باشد:

- ممکن است هر محصول از تکنولوژی خاصی استفاده کرده باشد، برای مثال سیستمی که از فناوری FHSS استفاده کند نمی‌تواند با سیستمی با فناوری DSSS کار کند.
 - اگر فرکانس کار دو سیستم با یکدیگر یکسان نباشد، حتی در صورت استفاده از فناوری مشابه، امکان کارکردن با یکدیگر فراهم نخواهد شد.
 - حتی تولیدکنندگان مختلف اگر از یک فناوری و یک فرکانس استفاده کنند، بدلیل روش‌های مختلف طراحی ممکن است با سایر محصولات دیگر سازگاری نداشته باشد.
۴. تداخل و اثرات متقابل: طبیعت امواج رادیویی در سیستمهای WLAN ایجاد می‌کند تا سیستمهای مختلف که دارای طیفهای فرکانسی یکسانی هستند، بر روی یکدیگر اثر تداخل داشته باشند. با این وجود اغلب تولیدکنندگان در تولید محصولات خود تمهدیاتی را برای مقابله با آن بکار می‌گیرند، به نحوی که وجود چند سیستم WLAN نزدیک به یکدیگر، تداخلی در دیگر سیستمهای موجود نمی‌آورد.
۵. ملاحظات مجوز فرکانسی: در اغلب کشورها ارگانهای ناظر بر تخصیص فرکانس رادیویی، محدوده فرکانس شبکه‌های WLAN را مشخص کرده‌اند. این محدوده ممکن است در همه کشورها یکسان نباشد. معمولاً سازندگان تجهیزات WLAN فرکانس سیستم را در محدوده مجاز قرار می‌دهند. در نتیجه کاربر نیاز به اخذ مجوز فرکانسی ندارد. این محدوده فرکانس به ISM معروف است. محدوده بین‌المللی این فرکانسها ۹۰۲-۹۲۸ مگاهرتز، ۲/۴-۲/۴۸۳، ۵/۱۵-۵۳۵ گیگاهرتز و ۵/۷۲۵-۵/۸۷۵ گیگاهرتز است. بنابراین تولیدکنندگان تجهیزات WLAN باید این محدوده مجوز فرکانسی را در سیستمهای خود رعایت کنند.
۶. سادگی و سهولت استفاده: اغلب کاربران در مورد مزیتهای WLAN ها اطلاعات کمی دارند. می‌دانیم که سیستم عامل اصولاً به نحوه اتصال سیمی و یا بی‌سیم شبکه وابستگی ندارند. بنابراین برنامه‌های کاربردی بر روی شبکه بطور یکسان عمل می‌نمایند. تولیدکنندگان WLAN ابزار مفیدی را برای سنجش وضعیت سیستم و تنظیمات مورد در اختیار کاربران قرار می‌دهند. مدیران شبکه به سادگی می‌توانند نصب و راهاندازی سیستم را با توجه به تپولوژی شبکه موردنظر انجام دهند. در WLAN کلیه کاربران بدون نیاز به کابل کشی می‌توانند با یکدیگر ارتباط برقرار کنند. عدم نیاز به کابل کشی موجب می‌شود که تغییرات، جابجایی و اضافه کردن در شبکه به آسانی انجام شود. در نهایت به موجب قابلیت جابجایی آسان تجهیزات WLAN مدیر شبکه می‌تواند قبل از اینکه تجهیزات شبکه را در مکان اصلی خود نصب کند، ابتدا آنها را راهاندازی کند و تمامی مشکلات احتمالی شبکه را برطرف سازد و پس از تایید نهایی در محل اصلی جایگذاری نماید و پس از پیکربندی، هرگونه جابجایی از یک نقطه به نقطه دیگر را بدون کمترین تغییرات اصلاح نماید.
۷. امنیت: از آنجایی که سرمنشأ فناوری بی‌سیم در کاربردهای نظامی بوده است، امنیت از جمله مقولات مهم در طراحی سیستمهای بی‌سیم بشمار می‌رود. بحث امنیت هم در ساختار تجهیزات WLAN به نحو مطلوبی پیش‌بینی شده است و این امر شبکه‌های بی‌سیم را بسیار امن‌تر از شبکه‌های سیمی کرده است. برای گیرنده‌هایی که دستیابی مجاز به سیگنالهای دریافتی ندارند، دسترسی به اطلاعات موجود در WLAN بسیار مشکل است. به دلیل تکنیکهای پیشرفته رمزگاری برای اغلب گیرنده‌های غیرمجاز دسترسی به ترافیک شبکه غیرممکن است. عموماً گیرنده‌های مجاز باید قبل از ورود به شبکه و دسترسی به اطلاعات آن، از نظر امنیتی مجوز لازم را دارا باشند.
۸. هزینه: برای پیاده‌سازی یک WLAN هزینه اصلی شامل دو بخش است: هزینه‌های زیرساختار شبکه مانند AP‌های شبکه و نیز هزینه کارتهای شبکه جهت دسترسی کاربران به WLAN.

هزینه‌های زیرساختار شبکه به تعداد AP‌های موردنیاز شبکه بستگی دارد. قیمت یک AP بین ۱۰۰۰ تا ۲۰۰۰ دلار می‌باشد. تعداد AP‌های شبکه به شاعع عملکرد شبکه، تعداد کاربران و نوع سرویسهای موجود در شبکه بستگی دارد و هزینه کارتهای شبکه با توجه به یک شبکه رایانه‌ای استاندارد حدود ۳۰۰ تا ۵۰۰ دلار برای هر کاربر می‌باشد. هزینه نصب و راهاندازی یک شبکه بی‌سیم به دو دلیل کمتر از نصب و راهاندازی یک شبکه سیمی می‌باشد:

- هزینه کابل‌کشی و پیدا کردن مسیر مناسب بین کاربران و سایر هزینه‌های مربوط به نصب تجهیزات در ساختمان، بخصوص در فواصل طولانی که استفاده از فیبر نوری یا سایر خطوط گرانقیمت ضروری است، بسیار زیاد است.
- به دلیل قابلیت جابجایی، اضافه کردن و تغییرات ساده در WLAN، هزینه‌های سربار، برای این تغییرات و تعمیر و نگهداری آن بسیار کمتر از شبکه سیمی است.

۹. قابلیت گسترش سیستم: با یک شبکه بی‌سیم می‌توان شبکه‌ای با تپولوژی بسیار ساده تا بسیار پیچیده را طراحی کرد. در شبکه‌های بی‌سیم با افزایش تعداد AP‌ها، می‌توان محدوده فیزیکی تحت پوشش و تعداد کاربران موجود در شبکه را تا حد بسیار زیادی گسترش داد. شاعع عملکرد این شبکه تا حدود ۲۰ کیلومتر می‌باشد.

۱۰. اثرات جانبی: توان خروجی یک سیستم بی‌سیم بسیار پایین است. از آنجایی که امواج رادیویی با افزایش فاصله به سرعت مستهلك می‌گردند و در عین حال، افرادی را که در محدوده تشبع RF هستند، تحت تاثیر قرار می‌دهند، باید ملاحظات حفظ سلامت با توجه به مقررات دولتی رعایت گردد. با این وجود اثرات مخرب این سیستمها زیاد نمی‌باشد.

امنیت در شبکه‌های بی‌سیم:

در حال حاضر عملاً تنها پروتکلی که امنیت اطلاعات و ارتباطات را در شبکه‌های بی‌سیم بر اساس استاندارد ۸۰۲.۱۱ WEP^۱ فراهم می‌کند. این پروتکل با وجود قابلیت‌هایی که دارد، نوع استفاده از آن همواره امکان نفوذ به شبکه‌های بی‌سیم را به نحوی، ولو سخت و پیچیده، فراهم می‌کند. نکته ای که باید به خاطر داشت اینست که اغلب حملات موفق صورت گرفته در مورد شبکه‌های محلی بی‌سیم، ریشه در پیکربندی ناصحیح WEP در شبکه دارد. به عبارت دیگر این پروتکل در صورت پیکربندی صحیح درصد بالایی از حملات را ناکام می‌گذارد، هرچند که فی‌نفسه دچار نواقص و ایرادهایی نیز هست.

بسیاری از حملاتی که بر روی شبکه‌های بی‌سیم انجام می‌گیرد از سویی است که نقاط دسترسی با شبکه‌ی سیمی دارای اشتراک هستند. به عبارت دیگر نفوذگران بعضاً با استفاده از راههای ارتباطی دیگری که بر روی مخدوم‌ها و سخت‌افزارهای بی‌سیم، خصوصاً مخدوم‌های بی‌سیم، وجود دارد، به شبکه‌ی بی‌سیم نفوذ می‌کنند که این مقوله نشان دهنده اشتراکی هرچند جزءی میان امنیت در شبکه‌های سیمی و بی‌سیمیست که از نظر ساختاری و فیزیکی با یکدیگر اشتراک دارند.

سه قابلیت و سرویس پایه توسط IEEE برای شبکه‌های محلی بی‌سیم تعریف می‌گردد:

- Authentication: هدف اصلی WEP ایجاد امکانی برای احراز هویت مخدوم بی‌سیم است. این عمل که در واقع کنترل دسترسی به شبکه‌ی بی‌سیم است. این مکانیزم سعی دارد که امکان اتصال مخدوم‌هایی را که مجاز نیستند به شبکه متصل شوند از بین ببرد.

^۱ Wired Equivalent Privacy

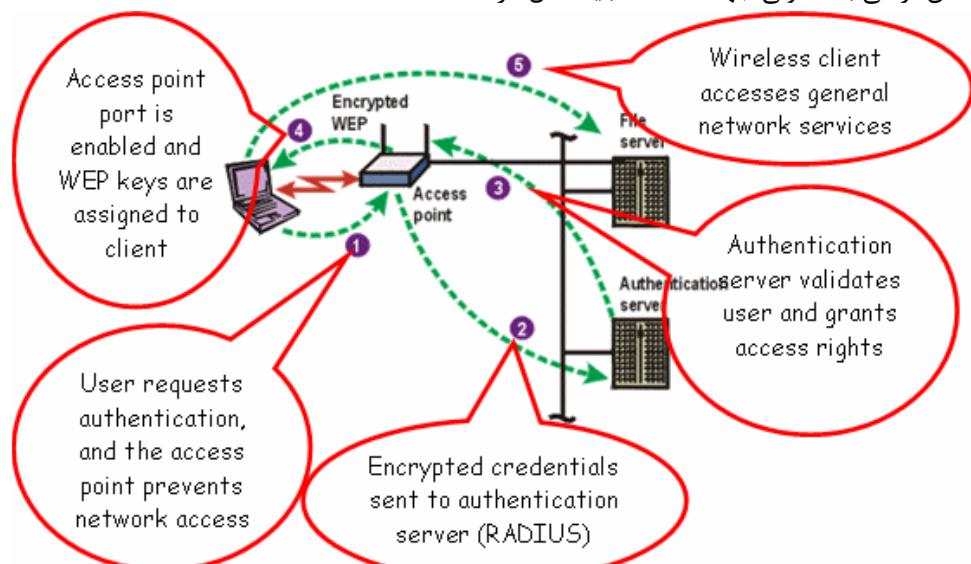
- محرومانه‌گی^۱: محرومانه‌گی هدف دیگر WEP است. این بُعد از سرویس‌ها و خدمات WEP با هدف ایجاد امنیتی در حدود سطوح شبکه‌های سیمی طراحی شده است. سیاست این بخش از WEP جلوگیری از سرقت اطلاعات در حال انتقال بر روی شبکه‌ی محلی بی‌سیم است.
- جامعیت: هدف سوم از سرویس‌ها و قابلیت‌های WEP طراحی سیاستی است که تضمین کند پیام‌ها و اطلاعات در حال تبادل در شبکه، خصوصاً میان مخدوم‌های بی‌سیم و نقاط دسترسی، در حین انتقال دچار تغییر نمی‌گردند. این قابلیت در تمامی استانداردها، بسترها و شبکه‌های ارتباطاتی دیگر نیز کم‌وپیش وجود دارد.

نکته‌ی مهمی که در مورد سه سرویس WEP وجود دارد نبود سرویس‌های معمول Auditing و Authorization در میان سرویس‌های ارایه شده توسط این پروتکل است. تمام گره‌های استفاده کننده از WEP فقط با وجود کلید WEP قابل دسترس می‌باشد.

دارای ۲ نمونه می‌باشد:

- رمزگذاری ۶۴ بیتی که تنها ۴۰ بیت آن واقعاً استفاده می‌شود.
- رمزگذاری ۱۲۸ بیتی که ۱۰۴ بیت آن مورد استفاده قرار می‌گیرد.

نمونه ۶۴ بیتی، طرح استاندارد و پیش فرض رمز گذاری می‌شود، وای برای شکسته می‌شود. طرح ۱۲۸ بیتی مطمئن‌تر می‌باشد، ولی جهت استفاده باید فعال گردد.



تصویر ۱۴-۵: نحوه تایید اعتبار یک گره با رمز گذاری WEP

در شبکه IEEE 802.11i، جهت بهبود امنیت، مکانیزم‌های زیر مورد استفاده قرار گرفته است:

• TKIP

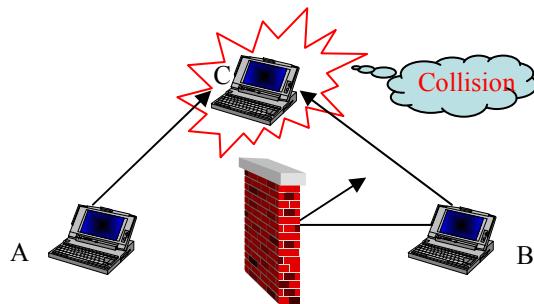
- عنوان WEP2 شناخته می‌شود.
- ایجاد جریان رمز RC4 بوسیله امنیت RSA

¹ Confidentiality -
² Temporal Key Integrity Protocol -

- کلید ۱۲۸ بیتی موقت ترکیب شده با آدرس MAC کامپیوتر مشتری
- تغییر کلید در هر ۱۰,۰۰۰ بسته^۱
- AES •
- ترکیب استاندارد 802.11i با AES
- نیازمندی به یک پردازنده جهت اعمال ، باعث نیازمندی به تغییر AP های موجود شده است.
- 802.1x •
- استفاده از طرح های سایر اعضای 802.1x
- چهارچوب برای تبادلات امن اتصالات

گره های پنهان:

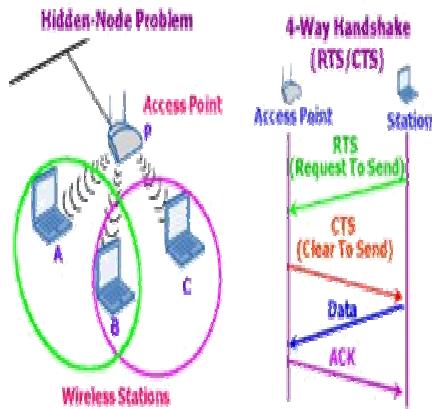
یکی از مشکلات شبکه های بی سیم ۸۰۲.۱۱، گره های پنهان می باشد. در تصویر زیر ، گره C گره های A و B را می بیند. گره های A و B در دید یکدیگر نیستند. بنابراین این امکان وجود دارد که A و B بخواهند در یک زمان با C تماس داشته باشند، سیگنالهای ارسالی آنها دچار تصادم می شود.



تصویر ۱۴-۶: مشکل گره های پنهان

بعنوان نمونه مثال ، تصویر زیر را درنظر بگیرید. ایستگاه های A و B می توانند با AP تماس مستقیم داشته باشند. A و B می توانند همدیگر را ببینند. تنها راه تماس A و C با یکدیگر، از طریق AP می باشد. این دو گره از یکدیگر پنهان می باشند. جهت رفع مشکل گره های پنهان، از دست دهی ۴ طرفه استفاده می شود. در این حالت پس از تست خالی بودن رسانه انتقال(ها) از هرگونه ترافیک، گره مبداء یک درخواست ارسال بسته های داده(RTS) را منتشر می کند. گیرنده ، در صورت عدم وجود مشکل، درجواب بسته دریافتی یک پیام CTS ارسال می کند. تمام گره های شبکه که این دو بسته را دریافت کرده اند، باید به اندازه زمان مشخص شده در دو بسته ، از ارسال داده خودداری نمایند. مبداء داده های خود را ارسال می کند و مقصد پس از دریافت همه داده، یک پیام تایید، می فرستد.

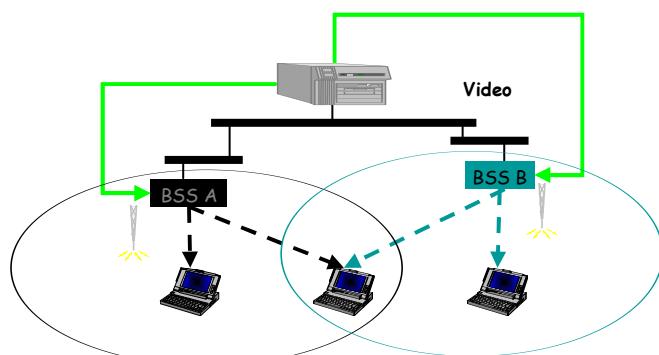
در مقابل این روش، روش دست دهی ۲ طرفه ، جهت انتقال داده با حجم محدود نیز وجود دارد که در آن فرستنده پس از خالی دیدن رسانه انتقال ، اقدام به ارسال داده می کند. اگر جواب تایید داده دریافت گردید، داده ها سالم به مقصد رسیده است، و گرنه فرستنده باید دوباره سعی در ارسال داده ها بنماید.



تصویر ۷-۱۴: گره های پنهان و دست دهی ۴ طرفه

سرگردانی^۱:

یکی از مشکلات شبکه ای بی سیم حالتی است که در آن یک گره در شبکه در موقعیتی قرار بگیرد که همزمان تحت پوشش بیش از یک BSS قرار بگیرد. در این حالت دسترسی به این گره از مسیرهای متفاوت ممکن می باشد. تصویر زیر این موضوع را به نمایش می گذارد. گره میانی در این تصویر در وضعیت سرگردانی قرار دارد. در این تصویر سرور ویدئو، از طریق BSS A و BSS B می تواند با این ارتباط برقرار کند. اگر این گره به AP در BSS A نزدیکتر باشد، انتقال از طریق BSS A انجام می شود. همین حالت در مورد BSS B عیناً تکرار می گردد. این مشکل بدلیل متحرک بودن ایستگاه های ۱۱، ۰۲، ۰۸ رخ می دهد.



تصویر ۸-۱۴: سرگردانی گره در شبکه بی سیم

۳-۱۴: مدیریت مصرف توان

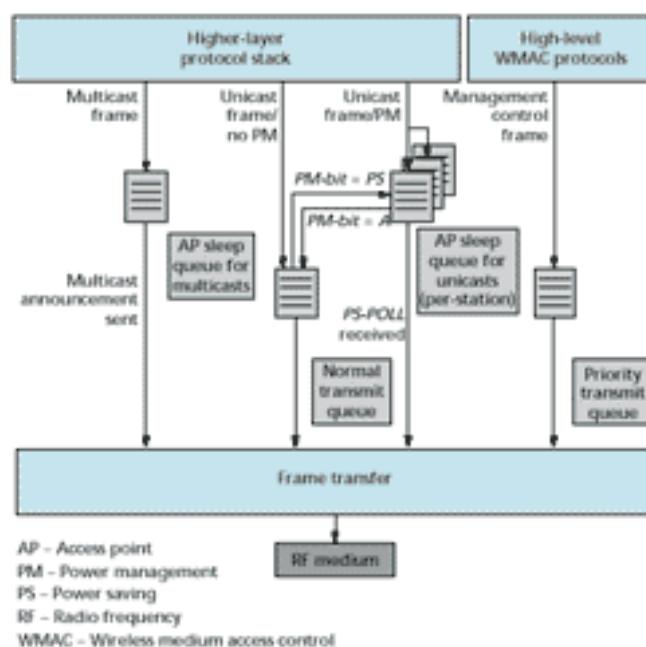
از آنجا که بخش عمده کاربران شبکه های بی سیم را کاربران ابزارهای موبایل تشکیل می دهند، ۱۱، ۰۲، ۰۸ دارای خصایص جهت پشتیبانی از مدیریت مصرف توان، می باشد. زمانیکه یک ایستگاه یک فریم را ارسال می کند، فریم حاوی یک بیت مدیریت توان (PM)، می باشد. این بیت نشانگر وضعیت کنونی مدیریت توان، ایستگاه می باشد. اگر PS=MP، ایستگاه در وضعیت ذخیره توان(PS^۳) است و اگر PM=1، ایستگاه در وضعیت فعال می باشد. در یک شبکه با AP همانند شبکه یک فرودگاه، AP ها وضعیت ایستگاه ها را جهت مدیریت ترافیک ایستگاه ها، بکار می برند.

¹ Roaming

² Power Saving

اگر یک ایستگاه در وضعیت PS باشد، AP تمام پیامهای آن را بافر می کند. برای مثال با یک طرح منظم، در هر ۱۰۰ میلی ثانیه، AP یک فریم Beacon را ارسال می کند. این فریم حاوی آدرس ایستگاه هاییست که AP پیامهای بافر شده برای آنها را نگه داشته است. ایستگاه های در وضعیت خواب^۱، خود را با زمانبندی ارسال فریمهای Beacon هماهنگ می کنند. هر ایستگاه این فریم را می خواند تا از وضعیت پیامهای بافر شده خود آگاهی یابد. اگر فریم مشخص کند که پیامهای بافر شده ای برای ایستگاه وجود دارد، ایستگاه به وضعیت بیدار^۲ می رود و به AP اجازه ارسال پیامهای بافر شده را می دهد. این شیوه مدیریت توان بصورت Unicast یا پیامهای ایستگاه خاص عمل می کند.

در وضعیت پیامهای Multicast، رویه متفاوتی اجرا می شود. برای پیامهای Multicast، در فریم Beacon تغییراتی اعمال می شود. در یک زمان ارسال چندتایی Unicast Beacon از پیش تعیین شده، فیلد دیگری در فریم Multicast جهت نمایش بافرشدن پیامهای Multicast، بکار می رود. بکار می رود. زمانیکه یک پیام Beacon دریافت گردد، پیامهای Multicast بلافاصله ارسال می گردد. زمانیکه یک ایستگاه یک فریم Beacon را دریافت می کند، دروضعیت بیدار باقی می ماند تا پیام Multicast را دریافت نماید. تصویر زیر نمودار یک ساختار صف بندی AP را نشان می دهد. اگر ایستگاهی فریم Beacon را دریافت نکند، همه ارسالهایش متوقف می گردد.



The 802.11 power management scheme for an access point.

تصویر ۹-۱۴: طرح مدیریت توان یک AP

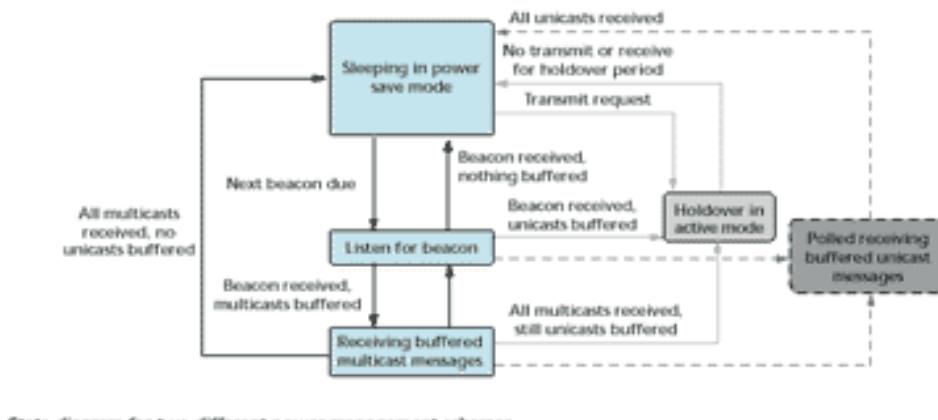
بلک ارسال فریم تنها بخشی می باشد که مستقیماً با بخش RF کار می کند. انتقال فریم دو صف ورودی دارد، فریمهای انتقال نرمال و فریمهای انتقال اولیت دار. صف اولویت جهت زمانبندی مدیریت دورنی و پروتکل کنترل فریم، بکار می رود و صف نرمال جهت فریم های دریافتی از لایه های بالاتر، در پشته شبکه، همانند داده های کاربر، استفاده می گردد. یک صف Multicast منفرد برای همه ایستگاه های متصل به AP وجود دارد و صفحهای Unicast مجزا برای هر ایستگاه نیز وجود دارد.

¹ Doze

² Awake

هر زمان که یک ایستگاه اجازه ارسال فریم را بدهد، پیام جلوی صفت Unicast ایستگاه، به انتقال فریم با انتقال با اولویت بالا، تحويل می‌گردد. زمانیکه یک ایستگاه در وضعیت PS (PS=PM) باشد، پیامی را به AP می‌فرستد، که نشان می‌دهد که در حالت A قرار دارد (A=PM) (دیگر اجازه دادن مطرح نیست)، همه پیامهای Unicast بافر شده به صفت انتقال نرمال، انتقال می‌یابد. زمانیکه یک ایستگاه در وضعیت فعال، پیامی را به AP می‌فرستد که بوضعیت خواب (PS=PM) رفته است، همه پیامهای آن از صفت انتقال نرمال به صفت خواب Unicast ایستگاه ها، انتقال می‌یابد.

نمودار زیر یک بلاک دیاگرام از دو طرح مدیریت توان را نشان می‌دهد: طرح استاندارد ۱۱a و ۱۱b و یک طرح پیشرفته توسعه داده شده برای The Wave LAN.



تصویر ۱۴-۱۰: نمودار دو طرح متفاوت مدیریت توان مصرفی

گره های ایستگاه پایانی، زمانیکه انتقالی وجود ندارد، بین یک حالت خواب و حالت گوش دادن برای یک Beacon، سوئیچ می‌کنند. زمان سنج ایستگاه، ایستگاه را برای یک فریم Beacon بیدار می‌کند. اگر پیامی بافر نشده باشد، ایستگاه بلافاصله به وضعیت خواب بر می‌گردد. این چرخه در هر دو طرح استاندارد ۱۱a و ۱۱b (با رنگ آبی و خاکستری روشن) و طرح پیشرفته The Wave LAN (با رنگ آبی و خاکستری تیره)، وجود دارد و اجازه می‌دهد تا ایستگاه در ۹٪ زمانش در وضعیت خواب، قرار داشته باشد.

در طرح استاندارد، زمانیکه پیام بافر شده تشخیص داده شد، ایستگاه در وضعیت بیدار باش قرار می‌گیرد و منتظر دریافت پیامهای Multicast و یا سرکشی فعال AP جهت پیامهایش می‌ماند. طرح پیشرفته یک وضعیت HoldOver را اضافه کرده است که در موقعیت‌های تشخیص انتقال و یا وجود پیامهای بافر شده، استفاده می‌شود. این وضعیت HoldOver بصورت موقت ایستگاه را از وضعیت خواب به وضعیت فعال در می‌آورد و PM را به A تنظیم می‌کند. سپس AP اقدام به ارسال همه پیامهای بافر شده می‌کند و صفت Unicast ایستگاه را متوقف می‌کند. این ایستگاه تا پایان دوره HoldOver فعال می‌ماند (معمولًاً بین ۳ تا ۵ ثانیه) و در این مدت ایستگاه بدون هرگونه فعالیت ارسال و یا دریافت می‌باشد.

مزیت این وضعیت HoldOver در آنست که اکثر فعالیتهای LAN بصورت انفجاری می‌باشد. انفجاری دوره هایست که در آن در دوره های زمانی، هیچ ترافیکی بوسیله دوره های ترافیک سنجین، جریان نمی‌یابد. با فعال نگه داشتن ایستگاه در دوره HoldOver، نیازی به تشکیل صفت نمی‌باشد. همچنین، سیستم نمونه برداری پیام، مورد استفاده برای دریافت پیامهای بافر شده، نسبتاً ناکارا می‌گردد. سرانجام، اگر ایستگاه برای مدتی در وضعیت خواب قرار داشته باشد، می‌توان بصورت دستی ایستگاه را برای هر کاربردی جهت حفظ ارتباطاتش با شبکه، و دریافت ترافیکهای مرتبط، برای مدت کافی در وضعیت بیدار قرار داد. بعنوان یک نمونه از تفاوت توان مصرفی،

برای The Wave LAN، حالت انتقال ۳۰۰ میلی آمپر، حالت دریافت ۲۵۰ میلی آمپر و حالت خواب ۹ میلی آمپر، صرف می نماید؛ بنابراین ذخیره توان ، قابل توجه خواهد بود.

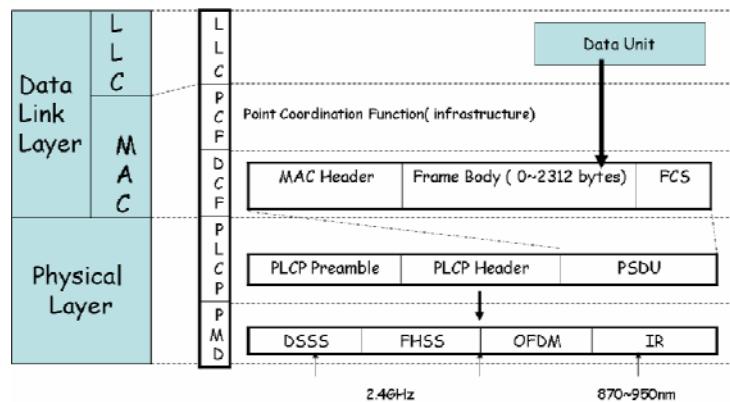
۱۴-۴: خانواده ۸۰۲،۱۱

- ۸۰۲.۱۱a: با وجود آنکه ۸۰۲.۱۱b بیشتر به عنوان پایه استانداردهای اصلی ۸۰۲،۱۱ تعریفی IEEE، مطرح می گردد، ۸۰۲.۱۱a یک جابجایی فناوری مهیج سریعتر به قلمرو جدید را را به می دهد. این پروتکل از OFDM در لایه فیزیکی خود، بعنوان مکانیزم انتقال داده خود استفاده می نماید. مهمترین پیشرفت در ۸۰۲.۱۱a را می تواند نرخ انتقال داده بغایت سریع آن دانست. با سرعت تئوری ۵۴Mbps، اگر کاربران در یک محیط بدون مانع با فاصله ۲۰ متری AP باشند، می توانند سرعت بالاتری را بدست آورند. در عمل کاربران در یک اداره سنتی با تعیین موقعیت صحیح AP می توانند سرعت ۳۶ Mbps - ۲۰ را بدست آورند. بدلیل استفاده از دامنه فرکانس ۵GHz در لایه فیزیکی، می توان از تداخل امواج با سایر ابزارها، صرفه نظر کرد. این بزرگترین مزیت ۸۰۲.۱۱a در برابر ۸۰۲.۱۱b می باشد که بصورت بسیار گسترده مسعد انواع تداخلات می باشد.
- ۸۰۲.۱۱b: با در نظر گرفتن اسلاف استاندارد شبکه های بی سیم ۸۰۲.۱۱ ۸۰۲.۱۱b هنوز هم در باند فرکانس رادیویی ۲.۴GHz و فروسرخ، عمل می نماید. پیشرفت‌های این پروتکل در رشد نرخ انتقال آن از ۵.۵-۱۱Mbps و بهبود دامنه آن، می باشد. دقت کنید که این تنها یک نرخ نظری سرعت انتقال ، تحت شرایط بینه شبکه و محیط می باشد. نرخ گذرهای واقع بینانه ۸۰۲.۱۱b ، در حدود ۴-۵Mbps می باشد.
- ۸۰۲.۱۱c: این استاندارد مسئول کمک به اطمینان یافتن از موثر بودن اتصالات پلهای بین AP ها می باشد. شرکتها و مراکز علمی و تحقیقاتی، در زمان نیاز به توسعه شبکه خود به محیط‌های مختلف همانند یک ساختمان و سایر گسترش‌های شبکه، از این پروتکل جهت ارتباطات پلی^۱، بهره می برند.
- ۸۰۲.۱۱d: بعد از شروع کار، ۸۰۲.۱۱ مقداری درمورد توجه جهت رفتن به سمت سایر طرحهای مشهور، نگران بود. مقدمه گروه کاری استاندارد ۱۱، نظراتی را درمورد ازدیاد گسترده و تطبیق ۸۰۲.۱۱، یک تجربه مورد پسند سراسری، ارائه داده است. ۸۰۲.۱۱ یک گروه استاندارد نوظهور است که بدبان افزودن و تعریف نیازمندیهای فیزیکی PHY جدیدیست که با استانداردهای تنظیم شده و موجود در سایر کشورها، همگون باشد. این استاندارد یک اعتبار خاص را برای گروه دارد و در آن از باند ۵GHz بعنوان فرکانس متفاوت مهیج از یک کشور تا کشور دیگر، استفاده شده است.
- ۸۰۲.۱۱e: استانداردی است که جهت افزایش بهره وری انتقال بی سیم صوت و تصویر پیوسته برپایه یک تأخیر، بکار گرفته شده است. استاندارد ۸۰۲.۱۱ در آغاز پذیرش ، فاقد هرگونه مکانیزم اولویت دهی سازمان دهی ترافیک شبکه بی سیم، می باشد. توجه گروه کاری استاندارد ۸۰۲.۱۱، بروی ترقی و بهبود کیفیت سرویس برای صوت و تصویر در تمام استاندارد ۸۰۲.۱۱ می باشد. پیاده سازی این استاندارد باعث می گردد تا با LAN های بی سیم کنونی عقب افتاده سازگار باشد و بهبود شدید انتقال و ارائه داده، کمک می کند.

- ۸۰۲.۱۱f: هدف اصلی گروه کاری استاندارد ۸۰۲.۱۱f، کمک به هدف همسازی درونی بین AP های فروشنده های مختلف، می باشد. پروتکل ۱۱۰۲،۱۱ بدون محدودیتهای خاصی، جهت انعطاف پذیری حداکثر، در زمان کار با سیستم های متفاوت، طراحی شده است. اگرچه، تکثیر سریع تکنیک های شبکه های بی سیم از سوی تعدادی از فروشندها، زمینه نیاز به ایجاد یک استاندارد جهت مجاز نمودن کاربران به حداکثر کردن قدرت جابجاییشان را فراهم آورد. توجه گروه کاری ۸۰۲.۱۱f، کمک به ترقی ۱۱۰۲،۱۱ و مجاز ساختن آن به سازگاری بیشتر بین تولیدکنندگان بی سیم مختلف و تولیداتشان، می باشد.
- ۸۰۲.۱۱g: این پروتکل از یک فرکانس کاری مشابه ۸۰۲.۱۱b در دامنه ۲.۴GHz استفاده نموده و از کلید کد تعریفی(CCK) ۸۰۲.۱۱b، جهت اطمینان از انطباق و سازگاری با شبکه های عقب مانده کار کننده با نرخ انتقال ۵.۵-۱۱Mbps، بهره می برد. این استاندارد با ۸۰۲.۱۱a در زمینه های حداکثر سرعت نظری ۵۴Mbps و متوسط گذردهی مشابه با آن، رقابت می نماید. این عقل سلیم ۸۰۲.۱۱g را می رساند که فناوری OFDM از ۸۰۲.۱۱a را مورد استفاده قرار داده تا سرعت آن را بدست آورد و هنوز هم در دامنه فرکانس ۲.۴GHz، عمل می کند. ۸۰۲.۱۱g امروزه در زمینه های مختلف، در سطح ثابتی قرار دارد
- ۸۰۲.۱۱h: این پروتکل جهت انطباق با قوانین عملکرد ۵GHz در اروپا(۸۰۲.۱۱a)، ارائه شده است. مزیت این پروتکل در کنترل انتقال و انتخاب پویای فرکانس می باشد. به این ترتیب کاربران ۸۰۲.۱۱a توانایی پرش به کانالهای دیگر، در زمان وقوع تداخل را دارند. از دیگر تواناییهای این استاندارد می توان به تکنیکهای مدیریت توان و کنترل توان انتقال به کاربران، جهت کاهش تداخل کاربران و ورود آنها به محیط های تحت پوشش مجاور، می باشد.
- ۸۰۲.۱۱i: پس از موفقیت رمزگذاری WEP در آگوست ۲۰۰۱، گروه کاری ۸۰۲.۱۱i، بیشتر مورد توجه قرار گرفت؛ بویژه آنکه هدف اصلی آن بهبود امنیت بی سیم بود. ۸۰۲.۱۱i یک گروه استاندارد ۲ سطحیست که هردو به اهداف مرتبط با ۸۰۲.۱۱x (بخشی از استاندارد ۱۱۰۲،۱۱ نیست) و امنیت شبکه و همچنین نگاهی عمیق تر به امنیت ثابت WEP بنام جامعیت کلید موقت(TKI)، توجه نموده است.
- ۸۰۲.۱۱n: این استاندارد به عنوان پاسخ سریع به کمبود سرعتهای شبکه های بی سیم موجود، مطرح شده است. با سرعت عملکرد ۱۰۰ Mbps، این پروتکل براحتی سرعتی ۲ برابر سرعت انتقال شبکه های بی سیم کنونی دارد و در عین حال قابلیت انطباق با مدلهاي عقب مانده b و g را نیز دارد. اگرچه در حال حاضر این نوع کامل نشده است، اما چندین فروشنده اقدام به ارائه محصولات Per-n بربایه پیش نویسهای اولیه آن نموده اند.
- ۸۰۲.۱۱ng: این استاندارد را می توان نسل بعدی استاندارد ۱۱۰۲،۱۱ نامید. از ویژگیهای آن می توان به سرعت انتقال بالاتر و مدولاسیون Ultra-Wideband، اشاره نمود.

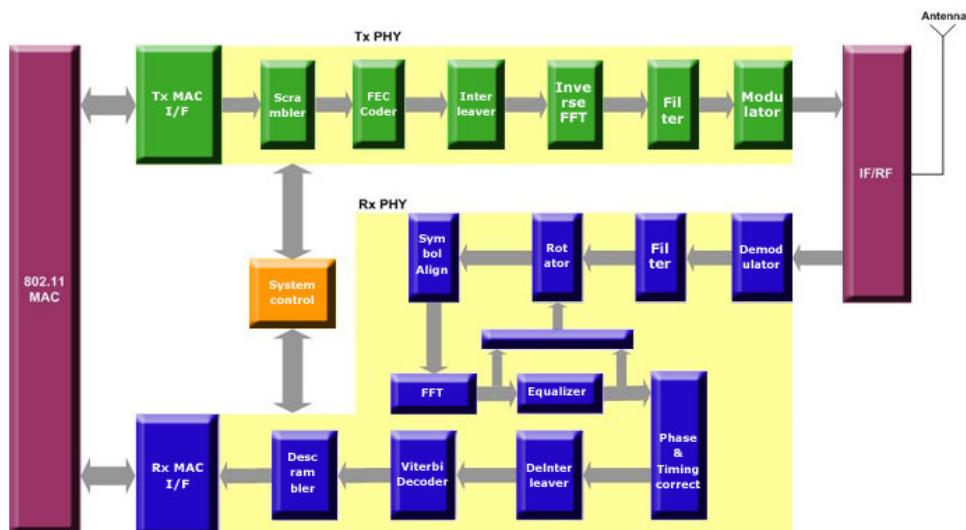
۵-۵: لایه فیزیکی

همانطور که دیدیم، باند ۲.۴GHz تنها باند مورد استفاده در دنیا نیست. استاندارد ۱۱۰۲،۱۱ تنها به لایه های MAC و فیزیکی شبکه های بی سیم می پردازد.



تصویر ۱۴-۱۰: لایه MAC و فیزیکی در ۸۰۲،۱۱

لایه فیزیکی ۸۰۲،۱۱ با بیتها سروکار دارد. این لایه به مباحث نحوه انتقال و دریافت داده و تبدیل داده به سیگنالهای RF در فرستنده و بازیابی آنها در گیرنده، می پردازد.^۴ پیاده سازی برای لایه فیزیکی ۸۰۲،۱۱ وجود دارد: فروسرخ یا مادن قرمز (IR)، OFDM، FHSS و DSSS.^۳ طرح IR از اشعه فروسرخ جهت انتقال داده استفاده می کند، همانند کنترل تلویزیون، و سایر طرح ها از فرکانس های رادیویی (FR)، استفاده می کنند. طرح های DSSS و FHSS بر مبنای طیف گسترده^۴ عمل می کنند که در سال ۱۹۴۰ توسط Hedy Lamarr، هنرپیشه زن هالیوود (استرالیایی الاصل)، در سن ۲۶ سالگی، در خلال جنگ جهانی دوم ابداع گردیده است.



تصویر ۱۴-۱۱: بلاک دیاگرام لایه فیزیکی ۸۰۲.۱۱a

FHSS

سیستم FHSS تمام پهنهای باند را به تعدادی زیر باند با پهنهای کم، کanal، تقسیم می کند و در طول دوره انتقال، بصورت پیوسته اقدام به پرش بین کانالها، می نماید. در این شیوه، فرستنده یک بسته را در یک فرکانس ارسال می کند و سپس به کanal بعدی، می رود و بسته بعدی را می فرستد و این عمل تکرار می گردد. سیگنال FHSS برای مدت زمان معینی در هر باند باقی می ماند. در ۸۰۲،۱۱، این زمان معادل ۳۰۰ msec می باشد.

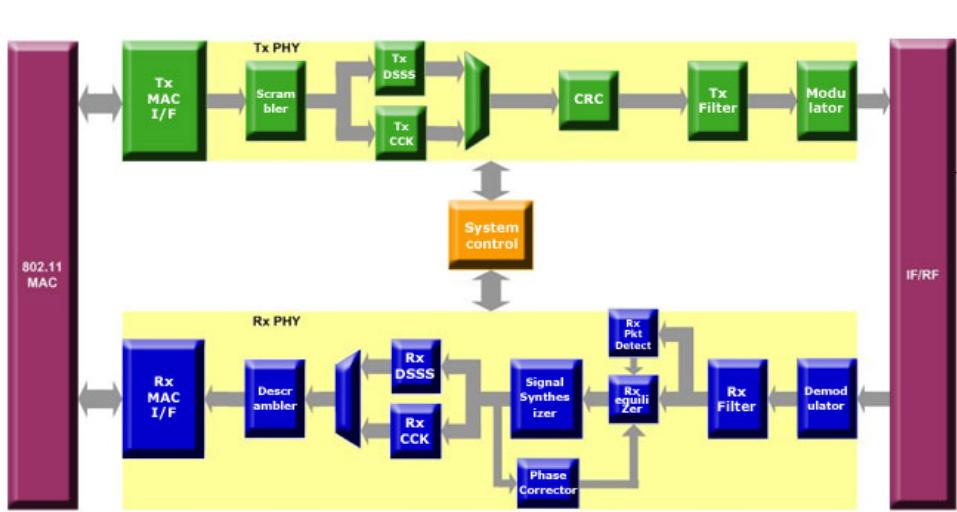
Infrared -¹

Frequency Hopping Spread Spectrum -²

Direct-Sequence Spread Spectrum -³

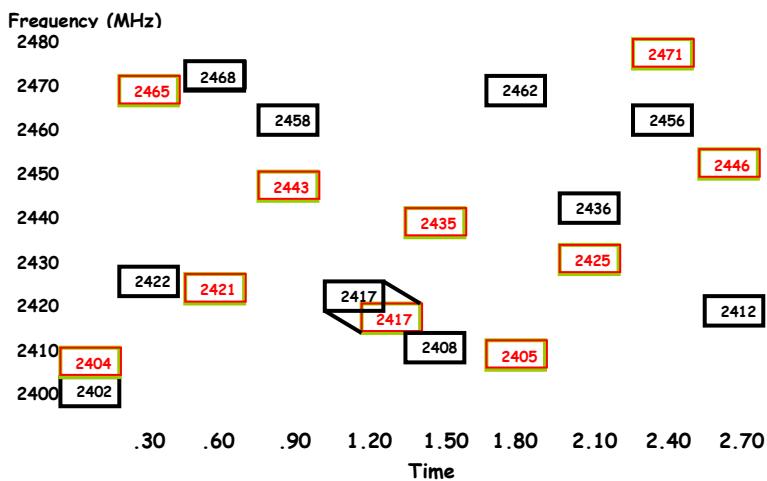
Spread Spectrum -⁴

ترتیب پرش، بصورت شبه تصادفی می باشد (کامپیوتر نمی تواند مقادیر تصادفی واقعی ایجاد نماید، اما می تواند این عمل را با دقت خوبی انجام دهد، به همین دلیل از عبارت شبه تصادفی استفاده می شود). توالی و الگوی پرش فرکانس بوسیله موقعیت جغرافیایی شبکه، تعیین می گردد. برای نمونه ژاپن سه توالی و ۴ الگو را فراهم می آورد، اسپانیا سه توالی و ۹ الگو، فرانسه ۳ توالی و ۱۱ الگو و آمریکا و بقیه اروپا، ۳ توالی و ۲۶ الگو را فراهم می آورند.



تصویر ۱۲-۱۴: بلاک دیاگرام لایه فیزیکی 802.11b

از مزایای پرش فرکانس می توان به تاثیر جانبی آن در کمک به اجتناب از تصادم، اشاره نمود. بدليل ارسال سیگнал، تنها در بازه کوتاه در هر کanal، تصادم بسیار کمتر رخ می دهد. با نرخ ۱ MHz برای پهنای هر کanal، تعداد آنها باز هم به موقعیت شبکه بستگی دارد. در ژاپن، ۲۳ کanal بین 2.495 GHz تا 2.473 GHz تعریف شده است و در آمریکا ۷۹ کanal بین 2.402 GHz تا 2.48 GHz، تعریف شده است.



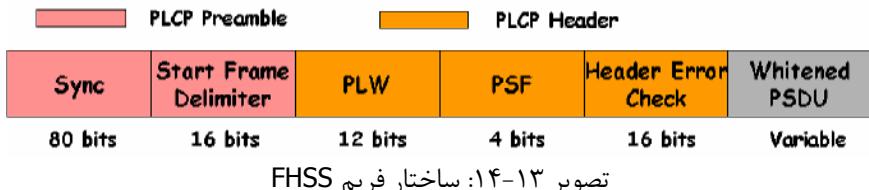
تصویر ۱۳-۱۴: کاهش امکان تصادم با استفاده از طرح پرش فرکانس

مسئله مهم دیگر در الگوریتم FHSS، استفاده از تمام کانال های موجود، قبل از استفاده مجدد از یک کاتال می باشد. انتقال دهنده FHSS جریان بیتی را قلی از ارسال از خود، به جریانی از نمادها، تبدیل می کند، که هر نماد دربرگیرنده یک یا چند بیت می باشد. سیگنال از طریق روش قطع متناوب شیفت فرکانسی(FSK)، انطباق را

^۱ Frequency Shift Keying -

انجام می دهد. نوع FSK به تعداد فرکانس‌های تلفیق مورد نیاز، بستگی دارد. اگر دو فرکانس تلفیق مورد استفاده قرار گیرد، از FSK دودویی (BFSK) استفاده می شود و اگر ۴ فرکانس استفاده شود، از FSK چهارگانه، استفاده می شود.

سیگنال انطباق داده شده FSK، همان چیزی است که در طول انتقال داده و دریافت، متناوباً پرش فرکانس دارد. ۸۰۲،۱۱ مبتنی بر FHSS از نوع سومی از انطباق FSK، بنام Gaussian FSK، نیز استفاده می نماید. با وجود استفاده Gaussian FSK در ۸۰۲،۱۱ مبتنی بر FHSS و کسب نرخ بیت بالاتر در کانالها، این طرح نسبت به نویز و سایر عوامل تضعیف کننده، حساسیت بیشتری دارد.



تصویر ۱۴-۱۳: ساختار فریم FHSS

- Sync: ترکیبی از صفر و یک متناوب جهت آگاه سازی دریافت کننده.
- حائل شروع فریم: تعیین کننده آغاز یک فریم: ۰۰۰۰۱۱۰۰۱۰۱۱۱۱۰۱.
- PLW: طول PSDU را مشخص می کند.
- PSF: نرخ داده Whitend PSDU را مشخص می کند.
- کنترل خطای سرآیند: CRC ۱۶ بیتی کنترل خطای سرآیند.
- Whitend PSDU: انتقال دهنده، نمادهای خاصی را در هر ۴ بایت، جهت حداقل کردن ولتاژ DC، قرار می دهد.

:DSSS

آخرین پیاده سازی لایه فیزیکی ۸۰۲،۱۱ DSSS می باشد. این طرح توسط Apple, Lucent, Farallon و سایر تولیدکنندگان شبکه های بی سیم ۸۰۲،۱۱، پیاده سازی می گردد. DSSS با FHSS متفاوت است. بجای تقسیم پهنهای باند به کانالهایی و سپس سوئیچ کردن بین آنها، DSSS سیگنال را در تمام پهنهای باند می گستراند و به این ترتیب بهره وری پهنهای باند را افزایش می دهد. همانند FHSS، جریان بیتها، به جریان نمادهای تبدیل می گردد، که هر نماد، یک یا چند بیت را دربردارد.

تعداد بیتها بوسیله تکنیک تلفیق^۳ مورد استفاده، مشخص می گردد. البته برخلاف FHSS، DSSS تلفیق خودش را برمنای قطع متناوب شیفت مرحله ای (PSK)^۴، بنیان نهاده است. جریان نمادهای تلفیق PSK به یک سیگنال مقادیر مختلط، تبدیل می گردد که پس از آن به یک تراشه منتشر کننده، داده می شود. تراشه منتشر کننده، یک سیگنال شبه نویز^۵، سیگنال PN، را به این سیگنال می افزاید تا یک توالی تراشه، ایجاد نماید. ۸۰۲،۱۱ مبتنی بر DSSS، توالی تراشه را برروی ۱۱ تراشه توالی Barker^۶، قرار می دهد. توالی Barker تنها یک سری مقادیر مثبت و منفی است که جهت انتقال در سیگنال، بکار می رود. برای مثال شما یک پالس همانند تصویر زیر دارید:



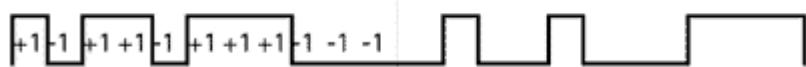
تصویر ۱۵-۱۴: یک پالس نمونه

PSDU Length Word - ^۱
PLCP Signaling Field - ^۲
Modulation - ^۳
Phase Shift Keying - ^۴
Pseudo-Noise - ^۵
Eleven-Chip Barker Sequence - ^۶

اگر این پالس را با توالی زیر تلفیق دهیم:

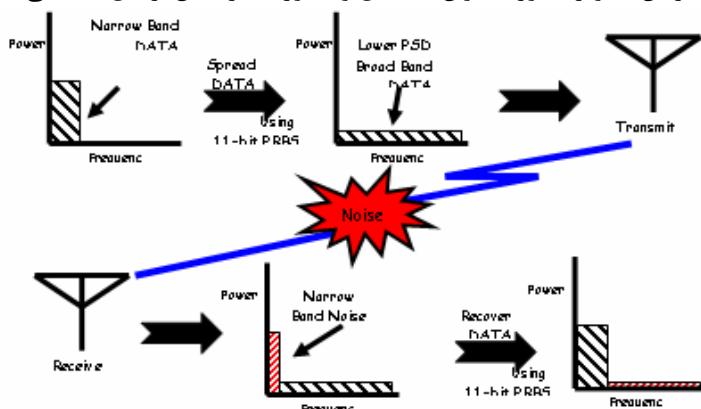
$$+1-1+1+1-1+1+1+1-1-1-1$$

و سپس پالس را در هر انتقال تغییر دهیم(بالا اگر پایین بود و پایین اگر بالا بود)، و یا موقعیت آن را در حالات بدون درخواست ارسال حفظ نمایید، پالس تلفیق یافته ای همانند تصویر زیر، خواهد داشت:

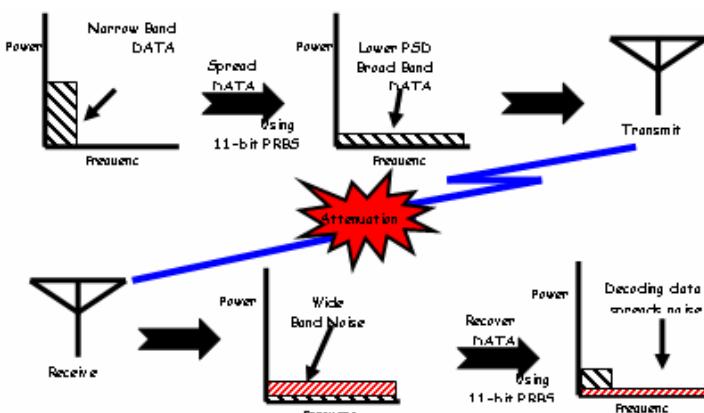


تصویر ۱۶-۱۴: پالس تلفیق یافته نمونه

اگرچه پالسها ، برای نیمه دوم پالس، خارج از توالی هستند، توالی پس ۱۱امین قطع مورد استفاده ، تکرار می گردد. بنابراین با اینکه آخرین قطع a-1 است و اولین قطع a+1 است، این حالت مانند یک بازنشانی و نه یک گذار ، عمل می کند. مرحله ای در قطع دوم، a-1، صورت می پذیرد، که یک گذار می باشد. گستراندن سیگنال بر مبنای این توالی، پهنای باند مورد استفاده را گسترش می دهد و پنهانی باند موثر را از ۱ MHz به ۱۱ MHz افزایش می دهد و این در حالیست که هنوز می توان، در صورت نیاز، آن را به ۵/۵ و یا ۱ Mbps کاهش داد. گسترش سیگنال همچنین زمینه کاهش تاثیر پذیری آن در برابر تداخل را فراهم می آورد؛ بطوریکه برای تحت تاثیر قرار دادن تمام یک بلاک داده ، تداخل باید در تمام طول باند، رخ دهد. همچنین گسترش، توان سیگنال منتقل شده را ، بدلیل اعمال توان خروجی به تمام پهنای باند، کاهش می دهد(میرایی). هر دو تاثیر در تصاویر زیر نشان داده شده است. درین تصویر محور α ، توان سیگنال و محور β فرکانس ارسال داده می باشد.



تصویر ۱۷-۱۴: تاثیر نویز بر داده های ارسال شده



تصویر ۱۸-۱۴: تاثیر میرایی بر داده های ارسال شده

سپس خروجی گسترش دهنده به یک تلفیق دهنده تربیع^۱ منتقل می شود . سپس تحویل انتقال دهنده نهایی می گردد. ۱۱، ۲۰، ۸۰ مبتنی بر DSSS، ۲ نرخ بیت دارد: ۱ Mbps با استفاده از PSK و BPSK و ۲ با استفاده از تربیع PSK (QPSK).



- Sync: ترکیب یکی در میان صفر و یک است و برای آگاه کردن گیرنده ، بکار می رود.
- حائل شروع فریم: ابتدای فریم را مشخص می نماید: 1111001110100000.
- سیگنال: تعیین نرخ داده سیگنال.
- سرویس: برای استفاده های آتی، رزرو شده است(تمام صفر).
- طول: نشان دهنده تعداد میکروثانینه های مورد نیاز جهت انتقال فریم، است.
- تست توالی فریم: ۱۶ بیتی جهت تست خطا.
- PSDU: MSDU می ارسالی

مادون قرمز:

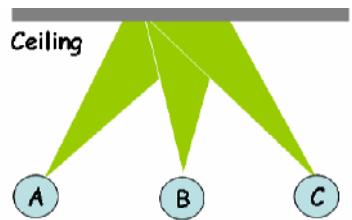
۱۱ از امواج منتشر شونده IR استفاده می نماید. برخلاف فرستنده و دریافت کننده های متداول خطی فروسرخ ، همانند تلویزیون و کنترل از راه دور، ابزار ۱۱، ۲۰، ۸۰ های مبتنی بر IR، از طریق انتشار سیگنال به یک سقف، که وظیفه بازتاباندن داده بر محیط تا زمان رسیدن به مقصد را برعهده دارد، عمل انتقال را انجام می دهد. این عمل در مورد داده های دریافتی نیز صورت می گیرد. در ارتباطات مادون قرمز از فرکانس های بالا - دقیقاً زیر طیف نور مرئی - استفاده می شود. در این روش سیگنالها نمی توانند از اشیاء و دیوارها عبور کنند. این امر بکارگیری تکنولوژی مادون قرمز را محدود می سازد. بطور کلی در ارتباطات داخل ساختمان که فاصله ایستگاهها کم باشد از این روش استفاده می شود. بعلاوه در داخل ساختمان نیازمند سقفی جهت بازتاباندن طول موجهای دامنه ۸۵۰ نانومتری فرو سرخ، لازم است. بعلاوه بر نیازمندی به سقف، وجود برد تقریباً ۱۰ متری، آن را مناسب اتفاقهای کوچک، همانند یک اطاق کاری دارای یک چاپگر فروسرخ، نموده است.

۱۱ فروسرخ از دون نرخ داده پشتیبانی می کند: 1Mbps و 2Mbps . در سرعت 1Mbps، هر جریان داده به ۴ بخش^۲ تقسیم می شود. امواج رادیویی بخارتر برد، پهناهی باند و پوشش مکانی بیشتر، از نور مادون قرمز کاربرد بیشتری دارند. سپس هر بخش به یکی از ۱۶ پالس ممکن ، در طول تلفیق و انتقال، تبدیل می شود. این تکنیک تلفیق، تلفیق موقعیت ۱۶ پالسی^۳ نامیده می شود. در نرخ 2Mbps ، تلفیق تاحدی متفاوت می باشد. جریان داده به زوج بیتها تقسیم می گردد و زوج به یکی از ۴ پالس ممکن تلفیق می یابد.

¹ Quadrature Modulator -

² Quartet -

³ 16 Pulse Position Modulation -



**Passive Ceiling Reflection
(Diffused Infrared)**

تصویر ۱۴: استفاده از IR در ۱۱-۲۰

OFDM

استاندارد IEEE 802.11a از طرح لایه فیزیکی OFDM استفاده می نماید که در آن سیگنالهای داده به ۵۲ زیرحمل کننده^۱ مجزا، جهت تهیه نرخ انتقال داده ۶، ۹، ۱۲، ۳۶، ۲۴، ۱۸ و یا ۵۴ Mbps، استفاده می کند. نرخ داده های ۶، ۹، ۱۲ و ۲۴ Mbps اجباری هستند.^۴ نقش زیرحمل کننده های رهبر را برعهده دارند که سیستم می تواند از آنها بعنوان مرجعی برای ندیده گرفتن فرکانس و یا شیفت مرحله ای سیگنال در طی انتقال، استفاده نماید. یک شبکه توالي دودویی از طریق زیرکانالهای رهبر، جهت جلوگیری از تولید خطوط طیفی، ارسال می گردد.^{۴۸} زیرحمل کننده باقیمانده، مسیرای مجزای بی سیم را جهت انتقال اطلاعات به شیوه موازی، فراهم می آورند. فضای فرکانس زیرحمل کننده های حاصل، ۰.۳۱۲۵ MHz (برای 20 بازه FSK) بازه ۶۴ FSK کانس زیرحمل کننده، می باشد.

هدف اولیه لایه فیزیکی OFDM، هدایت انتقال واحدهای داده پروتکل MAC(MPDUها)، توسط لایه MAC ۱۱-۲۰ می باشد. لایه فیزیکی OFDM به بخش تقسیم می شود: پروتکل همگرایی لایه فیزیکی (PLCP)^۲ و زیر لایه های وابسته فیزیکی (PMD)^۳.

لایه MAC با PLCP از طریق ویژگیهای اصلی از طریق سرویس فیزیکی AP ارتباط برقرار می کند. با اشاره لایه MAC، PLCP، MAC ها رابرای انتقال، مهیا می سازد. همچنین PLCP فریمها را وارد شده از طریق رسانه بی سیم، به لایه MAC تحويل می دهد. زیر لایه MAC به زیر لایه PMD را بوسیله نگاشت MPDU ها بدورن یک ساختار فریم مناسب برای انتقال بوسیله PMD، را کاهش می دهد. با توجه به جهت PLCP انتقال و دریافت موجودیتهای فیزیکی بین دو ایستگاه را از طریق رسانه بی سیم، فراهم می آورد. جهت فراهم آوردن این سرویس، PMD مستقیماً با محیط هوا، ارتباط برقرار کرده و عمل انطباق و بازیابی فریم های انتقالی را انجام می دهد. PLCP و PMD، جهت انجام توابع انتقال و دریافت، از سرویس های ابتدایی استفاده می نمایند.

تصویر زیر فرمت فریم یک فریم IEEE 802.11a را نمایش می دهد. فیلد مقدمه^۴، به دریافت کننده، رسیدن یک سیگنال OFDM ورودی و همگام سازی بازیاب فریم را اطلاع می دهد. مقدمه، حاوی ۱۲ نماد می باشد. نماد کوتاه بود و جهت برپاسازی کنترل بهره خودکار (AGC)^۵ و احتمال دریافت فرکانس های بزرگ برای حامل سیگنال، بکار می رود. دریافت کننده از نمادهای طولانی، جهت میزان سازی دقیق خود استفاده می نماید. به کمک مقدمه، دریافت کننده تا دریافت اولین فریم داده ورودی، ۱۶ میلی ثانیه زمان دارد.

Subcarrier -	۱
Physical Layer Convergence Protocol -	۲
Physical Medium Dependent -	۳
Preamble -	۴
Automatic Gain Control -	۵



فیلد سیگنال، حاوی ۲۴ بیت می باشد که نرخ داده و طول فریم را دربردارد. نسخه ۸۰۲.۱۱a از ترکیب قطع متناوب شیفت مرحله ای دودویی (BPSK)، PSK جهار بخشی (QPSK) و تلفیق دامنه ۴ بخشی (QAM)، براساس نرخ داده مورد نیاز، نشان داده شده در جدول ۲-۱۴، استفاده می نماید. فیلد طول، طول فریم برحسب بایت را نشان می دهد. مقدمه PLCP و فیلد سیگنال، با BPSK تبدیل و با سرعت ۶ Mbps، بدون توجه به نرخ داده مشخص شده در فیلد سیگنال، ارسال می گردد. نرخ بازیابی، براساس نرخ داده انتخابی، می باشد.

Data Rate (Mbps)	Modulation	Coding Rate	Coded bits per subcarrier	Coded bits per OFDM symbol	Data bits per OFDM symbol
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	16-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

جدول ۲-۱۴: تکنیک های تلفیق

فیلد سرویس، ۱۶ بیتی است که اول آن، جهت همزنمانی بازیاب بسته، صفر می باشد و سایر ۹ بیت باقیمانده، جهت استفاده های آتی، رزرو شده می باشند (تنظیم شده به صفر). احمد داده سرویس PLCP، Payload ارسال شده از لایه MAC می باشد. فیلد Pad، حداقل حاوی ۶ بیت است، اما در واقع تعداد بیتها آن به اندازه ایست که فیلد داده، بصورت مضربی از تعداد بیتها کد در یک نماد OFDM (۴۸، ۹۶، ۱۹۲ و یا ۲۸۸)، گردد. Scrambler داده، با استفاده از یک مولد توالی ۱۲۷ بیتی، همه بیتها فیلد داده را با الگوهای بیتی تصادفی، جهت جلوگیری از جریانهای طولانی صفر یا یک، تغییر می دهد.

با شیوه انطباق ۸۰۲.۱۱a در OSDM، مجموعه سیگنالهای دودویی به گروه ها (نمادها) یک، دو، چهار . یا شش بیتی، برحسب نرخ داده انتخابی، تقسیم می شوند و بوصرت ترکیبی از مقادیر مختلف، در می آیند. برای مثال، اگر نرخ داده ۲۴ Mbps انتخاب گردد، PLCP بیتها داده را به ۱۶ QAM نگاشت می نماید.

پس از نگاشت، PLCP مقادیر مختلف را نرمافزاری می کند تا میانگین توان مصرفی یکسانی برای تمام نگاشتها حاصل گردد. PLCP، هر نماد، با دوره تنابو ۴ میکروثانیه ای، را به زیرحمل کننده خاصی، انتساب می دهد. یک تغییر شکل عکس فوریه سریع (IFFT)، قبل از انتقال، با زیرحمل کننده ها ترکیب می گردد.

همانند سایر طرحهای لایه فیزیکی ۱۱، ۱۰۲، ۸۰۲، ۱۱ PLCP یک پروتکل تخمین آزاد بودن کانال را بوسیله گزارش مشغول بودن و یا آزاد بودن لایه MAC، از طریق سرویس AP، پیاده سازی می کند. لایه MAC، از این اطلاعات جهت تعیین پی آمد دستورات انتقال یک MDSU، استفاده می نماید.

فرکانسی کاری برای لایه OFDM در ۱۱، ۱۰۲، ۸۰۲ MHz، به سه باند بدون مجوز ۱۰۰ MHz تقسیم می گردد: ۵.15-۵.25 MHz، ۵.25-۵.35 MHz و ۵.725-۵.825 MHz کانال ۲۰ وجود دارد و هر باند محدودیت توان خروجی خود را دارد. در آمریکا، کد آئین نامه فدرال، عنوان ۴۷، بخش ۱۵/۴۰۷، این فرکانسها را، تنظیم می نماید.

Quadrature Amplitude Modulation - ^۱
Inverse Fast Fourier Transform - ^۲

استاندارد 802.11a نیازمند آنست که دریافت کنندگان، یک دامنه محدود dBm 82-65 را بر اساس نرخ داده انتخابی، داشته باشند.

IEEE شبکه های بی سیم 802.11a و 802.11b را در سال ۱۹۹۹ استاندارد نمود تا فناوری استانداردی را بوجود آورد تا بین شیوه های رمزگذاری فیزیکی مختلف، فرکانسها و کاربردهایی همانند استاندارد اترنت ۸۰۲.۳ عمل کننده با سرعتهای ۱۰۰ و ۱۰۰۰ Mbps، بروی فیر نوری و کابلهای مختلف، ارتباط برقرار کند. استاندارد 802.11b برای کار در باند 2.4 GHz با استفاده از تکنیک DSSS، طراحی شده است. از سوی دیگر، استاندارد 802.11a، برای کار در باند 5 GHz، طراحی شده است. استاندارد 802.11a از طرح OFDM استفاده می کند.

استاندارد 802.11a، که نرخ سرعتهایی تا 54 Mbps را پشتیبانی می کند، شبکه های سریعتری نسبت به 802.11b، که از سرعتهای حداقل 11 Mbps پشتیبانی می کند، می باشد. همانند اترنت و اترنت سریع، 802.11a و 802.11b از یک MAC یکسان، استفاده می نمایند. اگرچه اترنت سریع از طرح لایه فیزیکی یکسانی با اترنت استفاده می کند(فقط سریعتر است)، 802.11a از یک طرح کاملاً متفاوت استفاده می نماید، بنام OFDM، استفاده می نماید.

۱FCC، طیف موج 300 MHz را برای کاربردهای بدون مجوز در بلاک 200 MHz در دامنه 5.15 GHz تا 5.35 GHz و 100 MHz در 5.725 GHz تا 5.825 MHz، تخصیص داده است. این طیف به سه ناحیه کاری تقسیم شده است. اولین MHz 100، در پایین ترین بخش، با توان خروجی حداقل 50 MW، محدود شده است. دوم، توان خروجی 250 mW را دارد و بالاترین MHz 100، جهت کاربردهای بیرون ساختمان، نامزد می باشد و حداقل توان خروجی آن 1 W است. در مقام مقایسه، کارتهای 802.11b می توانند با توان خروجی 1 W در آمریکا، عمل کنند. اگرچه بسیاری از کارتاهای مدرن امروزی، به دلایلی همچون حفظ باتری و گرما، تنها بخشی از حداقل توان خروجی موجود (30 mW) را استفاده می نمایند.

استاندارد 802.11a، برخی از معیارهای کاراییش را بواسطه فرکانس کاری بالاتر، بدست می آورد. افزایش طیف از 2.4 GHz به 5 GHz، باعث کم شدن برد می گردد. 802.11a برای غلبه بر این کاهش برد مقدار^۲ EIRP خود را تا حداقل 50 MW افزایش می دهد.

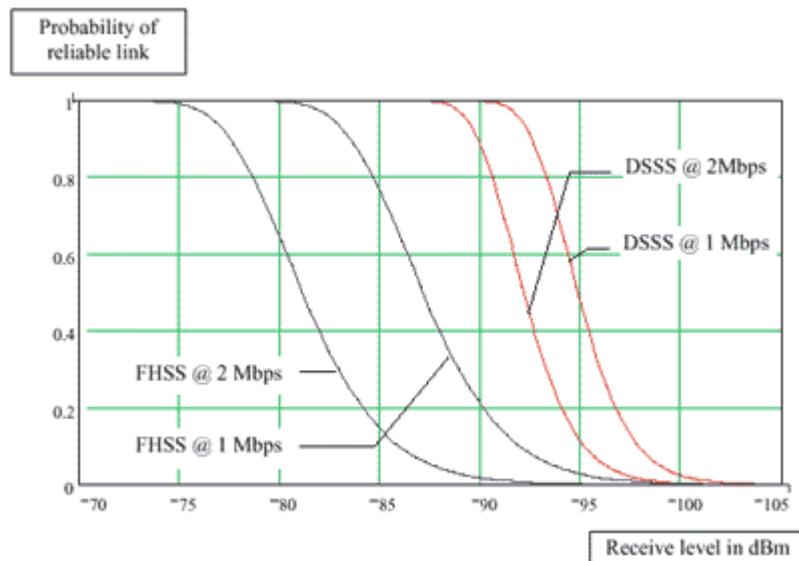
OFDM در اصل جهت اهداف درون ساختمانی بی سیم، توسعه یافته است و کارایی بالاتری را نسبت به راه حل های طیف گسترده، ارائه می دهد. OFDM با تقسیم یک حامل داده با سرعت بالا به چندین زیرحمل کننده با سرعت پایین تر، که آنها به شیوه DMT انتقال موازی، همانند روش مورد استفاده در مودم های ADSL را انجام می دهند، کار می کند. هر حامل سرعت بالا، پهنای MHz 20 داشته و به ۵۲ زیرکانال، هر کدام تقریباً 300 KHz تقسیم می گردد. OFDM از ۴۸ زیرکانال، جهت انتقال داده استفاده می نماید.

هر زیر کانال پیاده شده در OFDM، تقریباً 300 KHz پهنا دارد. با کمترین حد سرعت، BPSK جهت رمزگذاری 125 Kbps برای هر کانال مورد استفاده قرار می گیرد و در نتیجه، سرعت به 6 Kbps یا 6,000 Kbps می رسد. با استفاده از قطع متناوب شیفت فاز ۴ گانه(QPSK)، می توان به سرعت ۲ برابر برای هر کانال (250 Kbps) و سرعت کل 12 Mbps دست یافت. با استفاده از ۱۶ سطح تلفیق دامنه ای ۴ بخشی (4QAM)، ۴ بیت در هر تر رمز گذاری می شود و می توان نرخ 24 Mbps را بدست آورد. استاندارد 802.11a تمام محصولات این پروتکل را مجبور به حمایت از این نرخ داده های پایه می کند.

مقایسه با DSSS و FHSS

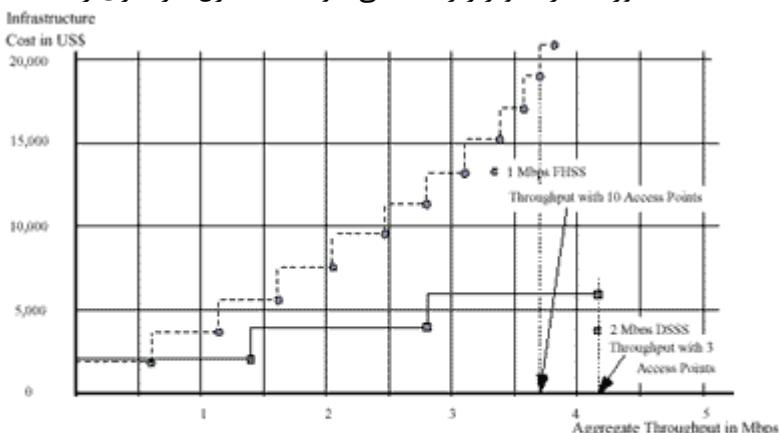
Federal Communications Commission - ^۱
Equivalent Isotropic Radiated Power - ^۲

در مقایسه DSSS با FHSS، باید توجه داشت که DSSS برخی مزایا آنی را بر FHSS دارد. اولین آنها تلفیق نیرومند تر می باشد و همچنین دامنه بزرگتر، حتی زمانیکه با توان سیگنال در مقایسه با سیستم FHSS عمل می کند، را داراست. حال آنکه رفتار پرش کانال FHSS، فرکانس‌های سراسری بیشتری را در اختیار آن قرار می دهد و درنتیجه تداخل بین کانالهای همسایه، تعداد کل سیستم های FHSS تخصیصی را محدود می سازد. با این وجود، FHSS یک برتری بر DSSS دارد و آن کاهش موقرانه آن به نسبت DSSS می باشد، که باعث عملکرد بهتر آن، تحت شرایط کاری بد می باشد. بخش عمده این برتری، بدلیل عدم طیف گسترده FHSS برروی تمام پهنای باند، همانند DSSS، می باشد. بدلیل اعمال سیگنال FHSS برروی باندهای کم عرض، نوسان آن بیشتر بوده و بنابراین FHSS می تواند بهتر در برایر تداخل عمل کند. همچنین جنبه پرش FHSS به اجتناب از تصادم فریم ها نیز کمک می کند. این مزایا بوسیله این حقیقت که DSSS در فواصل بزرگتر، نسبت به FHSS مطمئن تر عمل می کند، محدود شده است. این موضوع در نمودار زیر به نمایش درآمده است.



تصویر ۱۴-۲: مقایسه DSSS با FHSS

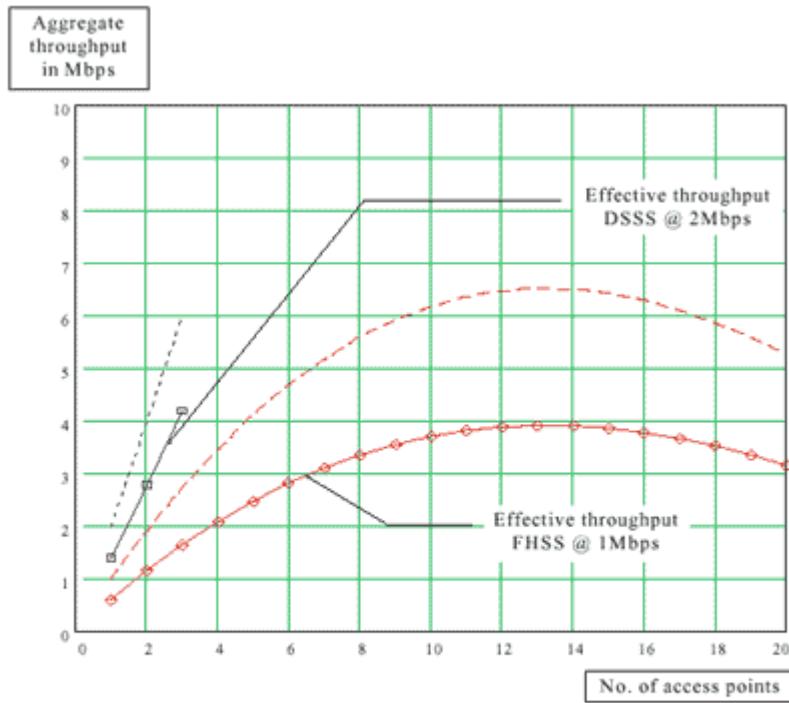
مزیت دیگر DSSS، بازده آن می باشد. DSSS قادر به ارائه کارایی بهتر با تعداد AP کمتر نسبت به FHSS می باشد. بعلاوه، همانطور که در تصویر زیر دیده می شود، نقاط تنزل سریعتری را نسبت به DSSS دارد.



تصویر ۱۴-۳: مقایسه هزینه AP بعنوان تابعی از گذردگی مورد نیاز در DSSS و FHSS

Based on data with access points deployed within the same cell to boost aggregate throughput.
Note that FHSS can never go beyond 4 Mbps (adding access points would just decrease throughput and add to the cost) while DSSS can get up to 4.2 Mbps (additional access points would give the same throughput and add to the cost) with 3 access points.

بعلاوه، DSSS از تعداد بیشتری AP استفاده می نماید که یک پهنهای باند متراک بالاتر سراسری را نسبت به FHSS، فراهم می آورد.



تصویر ۲۴-۱۴: مقایسه نسبت گذردگی با تعداد AP در DSSS و FHSS

بعلاوه در کنار هم گذاشتن شبکه ها، DSSS سرعت بالاتری را با AP کمتر نسبت به FHSS، ارائه می دهد.

۶-۱۴ MAC لایه

پس از بررسی لایه فیزیکی، اجازه بدھید به لایه بالاتر این استاندارد، لایه MAC، نگاهی بیاندازیم. به عنوان یک استاندارد شبکه بی سیم، MAC استاندارد ۸۰۲.۱۱، با شبکه های سیمی، همانند اترنت، فرق دارد. نمونه ای از این تفاوت آنست که AP در ۸۰۲.۱۱ بعنوان یک پل بین شبکه سیمی و شبکه بی سیم، عمل می کند، که در شبکه های سیمی فرض نشده است. بعلاوه فریمهای ۸۰۲.۱۱، دارای ویژگیهای یکتاوی می باشد که به ارسال و دریافت داده در شبکه بی سیم، کمک می کند.

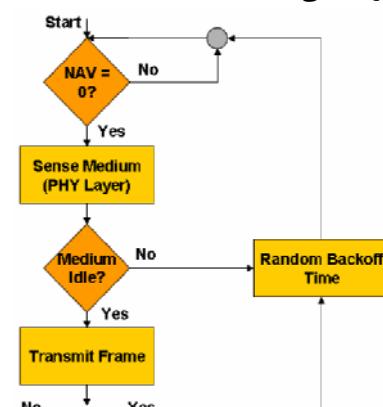
هر فریم دارای کنترل توالی و فیلرهای سعی مجدد است که برای به حداقل رساندن تداخل بین فریمهای مورد استفاده قرار می گیرد. از آنجاکه RF همه جهته می باشد، صرفه نظر از AP یی که ایستگاه نهایی با آن در ارتباط است، فریم های ایستگاه توسط هر AP قرار گرفته در دامنه برد ایستگاه، دریافت می گردد. در این موارد فیلد توالی می تواند در مورد تضمیم گیری در مورد این موضوع بکار رود. عطف به فیلد کنترل توالی، می توانید فیلدهای نوع/زیر نوع و دوره نیز به منظور کمک به ارتباطات مطمئن با وجود گره های پنهان، داشته باشید. همچنین فیلدهای کنترل توالی با فیلدهای قطعه قطعه کردن نیز کار می کند، که اجازه می دهد هر فریم، در صورت بد بودن شرایط، بعداً به قطعات کوچکتری تقسیم بشود. همچنین فیلدهای به DS و از DS نیز هستند که به برپاسازی و استفاده از کانال تنهای بی سیم Backbone، بکار می رود.

CSMA/CA

از یک طرح MAC مشابه طرح CSMA/CD اترنت، بنام CSMA/CA تفاوت بین این دو در آنست که ۸۰۲،۱۱ بدنیال اجتناب از تصادم می باشد (CA) و درحالیکه در اترنت تشخیص خط وجود دارد(CD). دلیل این امر آنست که شبکه بی سیم بصورت توزیع شده می باشد، و تلاش جهت تشخیص تصادم، غیر ممکن است، زیرا یک سیگنال ضعیف شده ورودی می تواند یک فریم و یا یک نویز باشد. CA در ۸۰۲،۱۱، جهت جلوگیری سراسری از تصادم، طراحی شده است. این طرح باعث کاهش شанс تصادم در طی دوره زمانی که احتمال بالای برای تصادم وجود دارد، که زمان پس از پایان ارسال یک ایستگاه می باشد، می گردد. در این زمان، چندین ایستگاه منتظر دستیابی به رسانه انتقال می باشند و سعی در ارسال داده های خود می کنند. برای اجتناب از این تصادم، ۸۰۲،۱۱ از یک ترتیب بازیابی معکوس^۲ اتفاقی، استفاده می نماید.

- باشهای زمانی مورد استفاده در این تکنیک، بترتیب اندازه شان از کوچک به بزرگ، به شرح زیر می باشند:
- **SIFS**: جهت یک CTS ACK MPDU بجز قطعه اول و در پاسخ به نمونه برداری PCF مورد استفاده قرار می گیرد.
 - **PIFS**: در زمان کار با PCF^۵، جهت کسب اولویت دسترسی به رسانه انتقال بکار می رود.
 - **DIFS**: در زمان کار با DCF^۷، جهت انتقال فریم های داده و مدیریت فریم ها، بکار می رود. در دست دهی دو و چهار طرفه، ایستگاه ها ابتدا باید به اندازه DIFS صبر کنند و سپس اقدام به چک کردن رسانه انتقال، جهت تعیین آزاد بودن یا نبودن آن بنمایند.

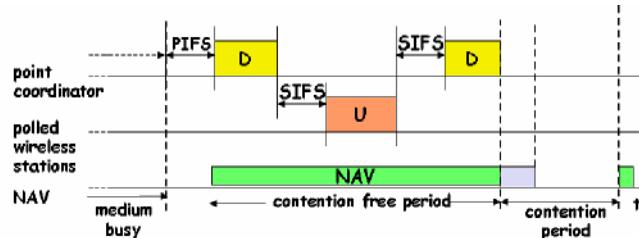
جهت جلوگیری از تصادم بروی رسانه انتقال، ازتابع هماهنگی توزیع شده (DCF) و الگوریتم بازیابی معکوس اتفاقی، استفاده می نماید. DCF یک پروتکل مبتنی بر مجادله می باشد. NAV^۸ یک شمارنده است که با مقدار رزرو در فیلد دوره آخرین فریم دریافتی، مقداردهی می گردد. این زمان بیانگر مدت زمانیست که یک ایستگاه جهت انتقال داده های خود، نیازمند می باشد.



تصویر ۲۵-۱۴: فلوچارت عملکرد CA

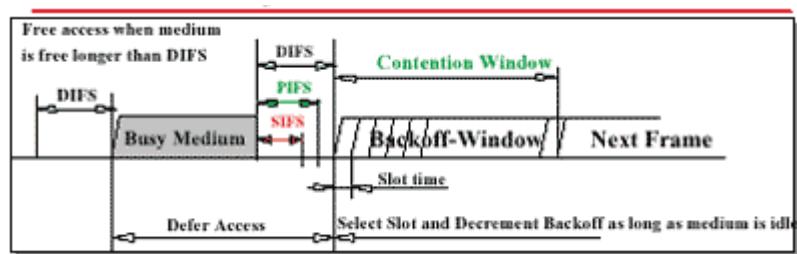
Carrier Sense Multiple Access/ Collision Avoidance - ^۱
BacK-off - ^۲
Short Interframe space - ^۳
PCF Interframe space - ^۴
Point Coordination Function - ^۵
DCF Interframe space - ^۶
Distributed Coordination Function - ^۷
Network Allocation Vector - ^۸

CSMA/CA همچنین دارای یک تابع هماهنگ نقطه (PCF) اختیاری می باشد که جهت برپاسازی یک AP به عنوان یک نقطه هماهنگ ساز، بکار می رود. در این تابع، نقطه هماهنگ کننده، اولویتهایی را به هر متقاضی، در یک فریم ارسالی، می دهد. گزینه PCF بسیار قدرتمند است؛ زیرا می تواند جهت سرویس‌های دارای محدودیت زمانی همچون صوت، صوت ببروی (VoIP) و ترافیک‌های چند رسانه‌ای، بکار رود.



D: downstream poll, or data from point coordinator
U: data from polled wireless station

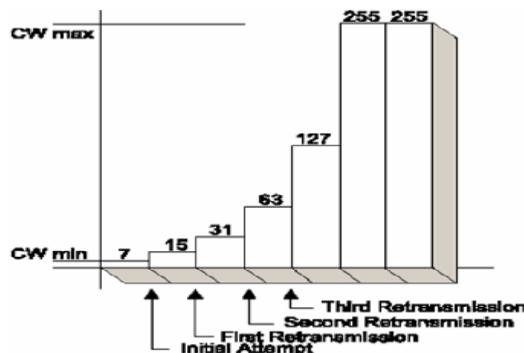
تصویر ۲۶-۱۴: عملکرد PCF



تصویر ۲۷-۱۴: نمودار زمانی عملکرد CA

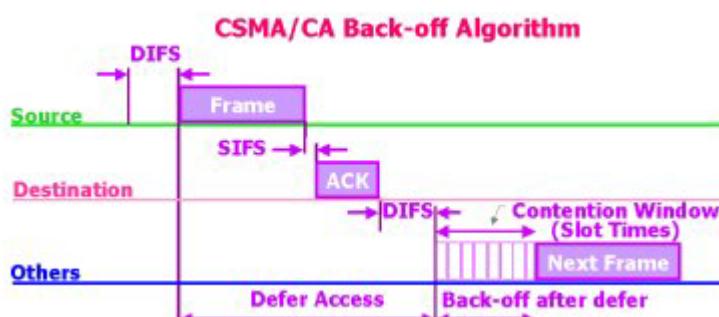
همانطور که در تصویر بالا مشاهده می شود، پس از دوره اشغال بودن رسانه انتقال، یک دوره فضای بین فریم (^{1}IFS)، که برای $80.2.11\text{ }\mu\text{sec}$ است، قرار دارد. همه ابزارهای باید به اندازه دوره IFS ، صبر نمایند. پس از IFS ، ابزارها یک زمان اتفاقی اضافی از بازه های μsec 20، که بوسیله یک الگوریتم بازیابی معکوس نمایی دودویی تعیین می گردد، نیز باید منتظر بمانند. این زمان بین دو مقدار حداقل زمان برای پنجره مجادله (CW_{min}) و حداکثر مقدار زمان پنجره مجادله (CW_{max}) می باشد. این دو مقدار، مقادیر از پیش تعیین شده ای هستند که تعیین صحیح آنها، تاثیر زیادی در ارسال موقع بسته های داده، دارد. در $802.11e$ ، جهت بهبود کیفیت سرویس برای کاربردهای زمان واقعی و صوتی و تصویری، از مقادیر کوچکتر CW_{min} ، برای این قبیل کاربردها، در برابر داده ها کاربردهای معمولی استفاده می شود. به این ترتیب شанс ارسال داده های با اولویت بالاتر و محدودیتهای زمانی سخت تر، بیشتر می گردد. پس از گذشته این زمان، رسانه انتقال آزاد بوده (هنوز هیچ ایستگاهی انتقال داده ندارد)، و ایستگاه می تواند سعی در انتقال داده بنماید. هر ایستگاه از مقادیر تصادفی (در واقع شبه تصادفی) خودش، به عنوان زمان انتظار استفاده می کند. این طرح شанс تصادم را کاهش می دهد. اگر یک تصادم مشخص شود، ابزارها به وضعیت بازه های زمانی انتظار، بر می گردند تا زمانیکه رسانه انتقال دوباره آزاد گردد.

¹ Interframe spacing period -



تصویر ۲۸-۱۴: مقادیر اتفاقی زمان انتظار اضافی

تفاوت دیگر در فریمهای تایید می باشد. با اینکه بسیاری از سیستمهای LAN، نیازمند برخی انواع فریمهای دریافتی تایید می باشند، طبیعت بی سیم ۱۱، ۲۰۲۱، برخی نیازمندیهای یکتا را در این زمینه، تحمیل می دارد. همانند سایر LANها، تمام تایید فریمهای خود را در پایان دریافت، انجام می دهد. اگرچه برخلاف اکثر LANها، ۲۰۲۱ این کار را در لایه MAC خود مدیریت می کند و این در حالیست که سایر LANها این کار را در لایه های بالاتر انجام می دهد. دلیل این امر نیازمندیهای زمانی تحمیل شده در ۲۰۲۱ می باشد. با زمان انتظار IFS به اندازه $50 \mu\text{sec}$ ، دریافت کننده باید یک تایید را در $10 \mu\text{sec}$ از تایید CRC برای فریم، ارسال کند. با انجام تمام این توابع در $10 \mu\text{sec}$ از دریافت فریم، دریافت کننده می تواند بلافصله تایید را ارسال نماید؛ زیرا سایر ایستگاه ها هنوز در دوره IFS خود می باشند و رسانه انتقال خالی می باشد. هرچند، این زمانهای پاسخ، مانع از مدیریت تایید در یک لایه بالاتر می گردد؛ بنابراین لایه MAC تایید را انجام می دهد. این سرعت عمل در توپولوژی معین یک مسئله بحرانی است، که بعداً بیشتر در مورد آن بحث می گردد. در یک نمودار عمومی از تایید، رفتار تایید بصورت زیر می باشد:



تصویر ۲۹-۱۴: نمودار کلی عملکرد تایید در ۲۰۲۱

در بتایی بخش MAC، به تفاوت‌های موجود در فیلدهای فریم ۲۰۲۱، اشاره شد و اینکه چگونه از آنها در مسئله گره های پنهان استفاده می شود. همانطور که قبلاً در بخش گره های پنهان نیز دیدیم، راسال داده همزمان گره های A و C می تواند باعث ایجاد تصادم گردد. راه حل، ترکیب فیلدهای به آز DS و استفاده از فریمهای ارسال/آماده جهت ارسال در ۲۰۲۱ می باشد. فیلدهای به آز DS، مسیر فریم ارسال شده را مشخص می کند، برخلاف اترنت که تنها آدرسهای MAC مبدأ و مقصد بکار می رود. در سیستم RTS/CTS، CTS/CTS، یک فریم RTS را به AP می فرستد، که به AP نشان می دهد که C آماده ارسال یک فریم می باشد. درین فریم یک مقدار زمانی وجود دارد که نشانگر زمانی است که C جهت ارسال فریم داده خود، به آن نیاز دارد. فیلدهایی که این داده را نگهداری می کند، فیلد طول می باشد.

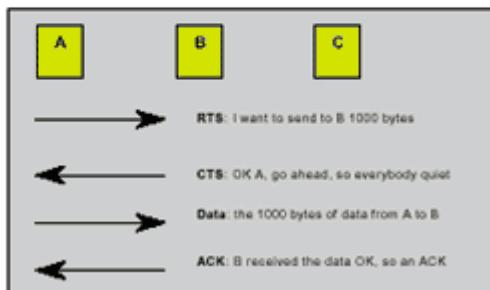
گره C می‌تواند پس از این به حالت انتظار برود. بلافتاله پس از خاتمه IFS و دوره بازیابی معکوس، یک فریم CTS برای C Broadcast می‌کند که توسط همه ایستگاه‌های تحت پوشش AP دریافت می‌گردد. این فریم CTS همان مقدار زمانی موجود در فریم RTS را دارد. سایر ایستگاه‌های دریافت کننده این فریم، به اندازه مقدار زمان مشخص شده در فریم CTS، انتقالشان را متوقف می‌کند. زمانیکه C فریم CTS را دریافت می‌کند، شروع به انتقال داده می‌کند. اولین نمودار زیر این فرایند را به شیوه پایه، تشریح می‌کند و نمودار بعدی برخی جنبه‌های ساختار RTS/CTS، ترکیب شده با رفتار بازیابی معکوس CSMA/CA را نشان می‌دهد.

A says to B: 'I'm going to send you data, and it will take 5 minutes'

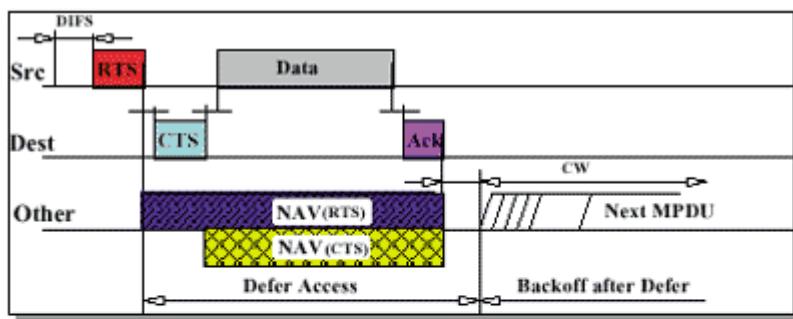
B says 'everybody quiet for 5 minutes!'

C hears this also, so he will not transmit while A is transmitting. When A stops transmitting, C knows that the air is free.

The benefit for the wireless LAN user is that the RTS/CTS will make the system more robust (against lost messages) and increases the performance of the system



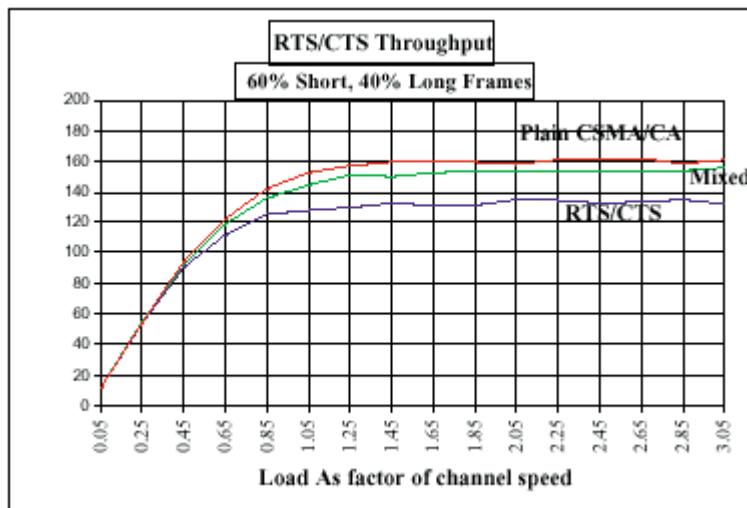
تصویر ۱۴-۳۰: انتقال داده CSMA/CA



- Duration field in RTS and CTS frames distribute Medium Reservation information which is stored in a **Net Allocation Vector (NAV)**.
- Defer on either NAV or "CCA" indicating **Medium Busy**.
- Use of RTS / CTS is optional but must be implemented.
- Use is controlled by a **RTS_Threshold** parameter per station.
 - To limit overhead for short frames.

تصویر ۱۴-۳۱: جزئیات اریال داده با CSMA/CA و بازیابی معکوس

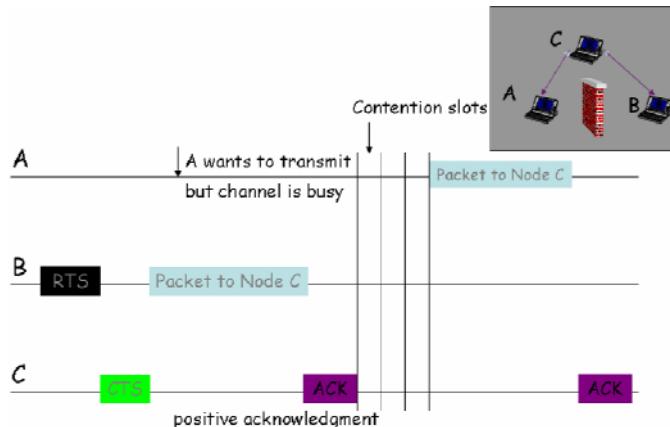
یکی دیگر از مزایای RTS/CTS، جلوگیری از تراکم می‌باشد که این موضوع باعث تحمیل سربار کمی به ۸۰۲.۱۱ می‌گردد. در مثال زیر، حتی در یک محیط خالص RTS/CTS، گذردگی در مقایسه با محیط‌های بدون RST/CTS، تقریباً ۱۳٪ کاهش یافته است.



تصویر ۱۴-۳۲: مقایسه گذرهای RTS/CTS با بدون

تأثیر محدود RTS/CTS بر گذرهای، دربرابر توانایی کاهش تصادم آن، آن را به خصیصه ای بسیار جذاب برای محصولات ۸۰۲،۱۱ تبدیل نموده است. باوجود آنکه خصیصه RTS/CTS یک گزینه اختیاری در ۸۰۲،۱۱ می باشد، جهت کاهش هزینه می توان از آن صرفه نظر نمود.

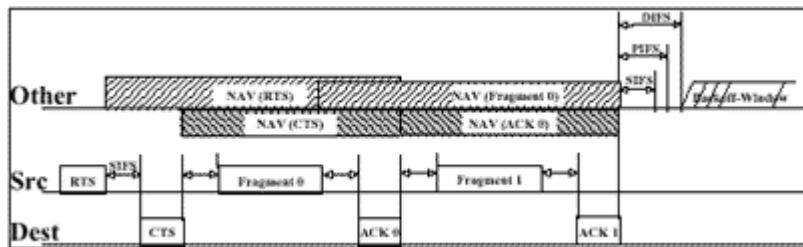
مثال: تصویر زیر نمونه یک محیط عملیاتی شبکه ۸۰۲،۱۱ است. در این تصویر A بدلیل مشغول بودن رسانه انتقال و کنترل آن توسط B، اجازه ارسال داده را ندارد. پس از پایان اتصال B به C، A می تواند جهت ارسال داده خود به C اقدام نماید.



تصویر ۱۴-۳۳: نمونه ای از محیط عملیاتی ۸۰۲،۱۱ و عملکرد RTS/CTS

سایر خواص MAC: ۸۰۲،۱۱

ویژگی دیگر MAC ۸۰۲،۱۱، قطعه قطعه کردن می باشد، که یک تکنیک برای شرایط ارسال ضعیف می باشد. برخلاف شبکه های بی سیم، شبکه های بی سیم، ۸۰۲،۱۱، باید با مواردی همچون تداخلات اطراف آنتن و یا منابع مایکروویو همانند واحدهای انتقال تلویزیون موبایل، مورد بحث قرار گیرد. برای غلبه بر تداخل، ۸۰۲،۱۱ اجازه می دهد تا یک فریم قطعه قطعه گردد.



تصویر ۱۴-۳۴: قطعه قطعه کردن فریم ۸۰۲،۱۱

بدلیل کوچک بودن قطعات، گره های پایانی و AP ها، می توانند بسیار سریعتر انتقال و دریافت را انجام دهند.علاوه، اندازه کوچتر قطعات به معنی تاثیر کمتر خطاها جهت تغییر در قطعات و تاثیر کلی آن در گذردهی می باشد. همچنین باید توجه داشت که تا زمان ارسال همه قطعات و دریافت تایید، فریم ارسال نشده تلقی می گردد. بنابراین ارسال کننده قطعات بر رسانه انتقال برای آن بازه زمانی، کنترل خواهد داشت.

سرانجام در مواردی از تداخل همانند مایکروویوها، تداخل بصورت انفجاری می باشد، بنابراین طول کوتاه تر قطعات به معنی مدیریت بهتر این قبیل تداخلات می باشد. ۸۰۲،۱۱ نیازمند پشتیبانی قطعه قطعه کردن در مقصد می باشد، اما این موضوع در فرستنده اختیاری است. همچنین ۸۰۲،۱۱ اجازه قطعه قطعه کردن پویا را، متناسب با طبیعت تداخل رخ داده، می دهد. با اجازه دادن جهت امکان قطعه قطعه کردن تمام وقت، فروشنده می تواند دریافت کننده خود را، با حذف هزینه افزوده شده پشتیبانی قطعه قطعه کردن پیشرفته، ارزانتر بسازد. با وجود این قطعه قطعه کردن به معنی انتقال بیشتر، سربار بالاتر و کاهش گذردهی می باشد.

در یک شبکه ۸۰۲،۱۱ هر AP تعداد منظمی از Beacon ها را در هر ۱۰۰ msec در میگردد. در هر AP موجود در دامنه خود، ارسال می نماید. در Beacon، داده هایی همچون TimeStamp کنونی، برای اهداف همزمان سازی، طرحی از ترافیک کنونی و نرخ داده پشتیبانی شده، قرار دارد. با دریافت این Beacon، هر گره انتهایی می توانند بصورت جداگانه تصمیم گیری کند و مشخص کند که آیا تلاشی برای اتصال به AP و یا AP های دیگر (در صورت وجود چند AP) انجام دهد یا خیر. یک گره انتهایی می تواند خود یک Beacon و یا درخواست پیام جستجو را به هر AP را در دامنه خود، ارسال کند که بوسیله یک پاسخ پیام جستجو و یا تقاضای Beacon، پاسخ داده می شود.

در حالت بالا و همچنین حالت سرگردانی، گره انتهایی، نه AP، کیفیت ارتباط (QC) سیگنال AP را تعیین می نماید و از سطح QC جهت تعیین AP مناسب اتصال، استفاده می نماید. اگر CQ سیگنال یک AP متصل شده، به زیر حد معینی نزول نمود، که بوسیله تعدادی از فاکتورها همانند طراحی، کاربرد، سرعت و غیره، تعیین می گردد، به دلایلی همچون تداخل، قطع برق و یا سرگردانی گره، گره فعل، به دنبال یک AP جدید می گردد. زمانیکه AP جدید یافت شد، گره نهایی به وضعیت جدید، منتقل می شود و با AP جدید متحده می گردد. AP جدید با هر دو گره انتهایی و گره انتهایی AP قبلی، جهت برقراری مجدد محل گره پایانی در شبکه، ارتباط برقرار می کند. AP ها از یک پروتکل دورن AP، جهت اطلاع دادن به یکدیگر در مورد تحويل و تحولات و سرگردانی گره های نهایی، استفاده می نمایند.

این موضوع به ۸۰۲،۱۱ اجاز می دهد تا از آدرس MAC، برای تحويل و تحول اطلاعات از AP قدیمی به AP جدید، استفاده شود و بنابراین به شبکه اجازه می دهد تا جلوی سرگردانی های بدون مجوز، از طریق استفاده از جداول آدرس/کلمه عبور MAC و غیره، گرفته شود.

فریمهای MAC

فریمهای MAC در ۸۰۲،۱۱ را می توان به سه دسته تقسیم نمود:

- فریمهای داده: بوسیله مسیر سرویس داده MAC، مدیریت می گردند و حاوی داده های کاربر می باشد.

Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	Frame Check Sequence
2	2	6	6	6	2	6	0 - 2312	4

MAC Header

تصویر ۱۴-۳۵: ساختار فریم داده ۸۰۲.۱۱

- فیلد کنترل فریم: حاوی اطلاعات کنترلی ارسال شده بین ایستگاه ها می باشد. این فیلد، خود دارای ساختار زیر می باشد:

Bit 0	Bit 15													
Protocol Version	Type	Subtype	To DS	From DS	More Frag.	Retry	Pwr. Mgmt	More Data	WEP	Order				
2	2	4	1	1	1	1	1	1	1	1				

تصویر ۱۴-۳۶: ساختار فیلد کنترل فریم

نسخه پروتکل: در حال حاضر صفر است.

نوع: نوع فریم مدیریتی، کنترلی و یا داده را مشخص می کند.

زیر نوع: تابع فریم را نشان می دهد.

به DS: اگر یک باشد، ارسال به سیستم توزیع شده را نشان می دهد.

از DS: اگر یک باشد، برگشت به سیستم توزیع شده را نشان می دهد.

قطعه بیشتر: اگر یک باشد، نشان دهنده وجود تعدادی قطعه MSDU در ادامه فریم جاری، می باشد.

تلاش مجدد: اگر یک باشد، نشانگر فریم دوباره ارسال شده می باشد.

مدیریت توان: یک بودن آن نشانگر وضعیت خواب برای ایستگاه می باشد.

WEP: اگر یک باشد، نشان می دهد که بدنه فریم، کد شده است.

ترتیب: اگر یک باشد، نشان می دهد اجباری بودن دریافت مرتب فریمهای می باشد.

- دوره ID: حاوی اطلاعات زمانی مورد نیاز جهت ارسال فریمهای بعدی است.
- آدرس های ۱ تا ۴: آدرس های خاص که متناسب با نوع فریم ارسالی از آنها استفاده می گردد.
- کنترل توالی: حاوی ۴ بیت شماره قطعه و ۱۲ بیت، شماره توالی می باشد.
- کنترل توالی فریم: حاوی نتیجه CRC جهت تشخیص خطأ، می باشد.

▪ فریم های مدیریتی: بوسیله مسیر داده سرویس مدیریت MAC، مدیریت می شود. در مواردی همچون تایید اعتبار، درخواست و ... بکار می رود. این فریمهای جهت برپاسازی و حفظ ارتباط بین ایستگاه ها و AP ها، بکار می روند.

 MAC Header

Frame Control	Duration/ ID	DA	SA	BSSID	Sequence Control	Not Used	Frame Body	Frame Check Sequence
2	2	6	6	6	2	6	0 - 2312	4

تصویر ۱۴-۳۷: ساختار فریم مدیریتی

انواع زیر نوع در این فریم ، بشرح زیر می باشد:

- وابستگی درخواست و پاسخ
- وابستگی مجدد درخواست و پاسخ
- بررسی درخواست و پاسخ
- Beacon
- ^۱ ATIM
- فسخ همکاری
- تایید و عدم تایید

▪ فریمهای کنترلی: ACK، CTS، RTS، سرکشی در وضعیت ذخیره توان. این فریمهها، جهت کمک به تحويل فریمهای بکار می رود.

 MAC Header

Frame Control	Duration/ ID	DA	SA	BSSID	Sequence Control	Not Used	Frame Body	Frame Check Sequence
2	2	6	6	6	2	6	0 - 2312	4

تصویر ۱۴-۳۸: ساختار فریم کنترلی

انواع زیر نوع در این فریم ، بشرح زیر می باشد:

- TRS
- CTS
- ACK
- ² PS Poll
- ^۳ CF End
- CF End + CF-ACK

^۱ Announcement Traffic Indication Message –

^۲ Power-Save Poll -

^۳ Contention-Free End -

بخش ۶:

امنیت در شبکه

فصل ۱۵: امنیت در شبکه

فصل ۱۰:

امنیت در شبکه

یک شبکه در معرض چهار نوع حمله قرار می‌گیرد:

۱-وقفه : باعث توقف کار شبکه می‌شود.

۲-استراق سمع

۳-دستکاری داده

۴-حمله از نوع افزودن اطلاعات

دونوع حمله داریم :

فعال : حمله‌ای که اختلال در کار شبکه ایجاد کند.

غیرفعال : حمله‌ای که اختلالی در کار شبکه ایجاد نمی‌کند و به تدریج داده‌ها را نابود می‌کند.

دیوار آتش^۱ :

دیواری است که برای امنیت در شبکه بکار می‌رود . که در سر راه ارتباط شبکه با دنیای خارج قرار دارد . مثلاً بسته‌ها را پردازش کرده و اجازه عبور یا عدم عبور را به بسته می‌دهد . می‌تواند ردیابی کند . یکسری قوانین یا *pol* دارد که به دیوار آتش اعمال می‌شود . دیوار آتش هم می‌تواند به صورت لایه لایه طراحی شود (مثل شبکه) .

اگر در لایه شبکه باشد ، بسته‌های IP را پردازش می‌کند (سرآیند IP)

اگر در لایه انتقال و حمل و نقل باشد سرآیندهای بسته را سرویس می‌دهد (امکان دادن Ftp و ... را می‌توان کنترل کرد)

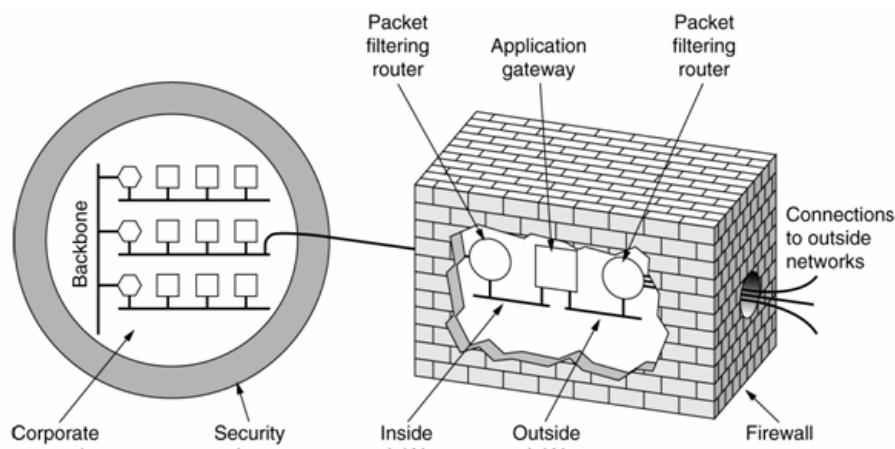
اگر در لایه کاربرد باشد باید به داده‌های داخل آن حساس باشد .

با استفاده از دیوار آتش می‌توانیم سرویسها را کنترل کنیم . اگر بخواهیم اجازه دسترسی به آدرس‌های مختلف را ندهیم از دیوار آتش در لایه IP استفاده می‌کنیم . آدرس مبدأ و مقصد و ... را در IP بررسی می‌کند .

در لایه حمل و نقل جلوی بعضی از سرویسها را می‌گیریم مانند : Telnet, FTP و ...

در لایه کاربرد ، داده‌ها و محتوای آنها توسط دیوار آتش انجام می‌شود .

اعضای جانبی دیوار آتش :



A firewall consisting of two packet filters and an application gateway

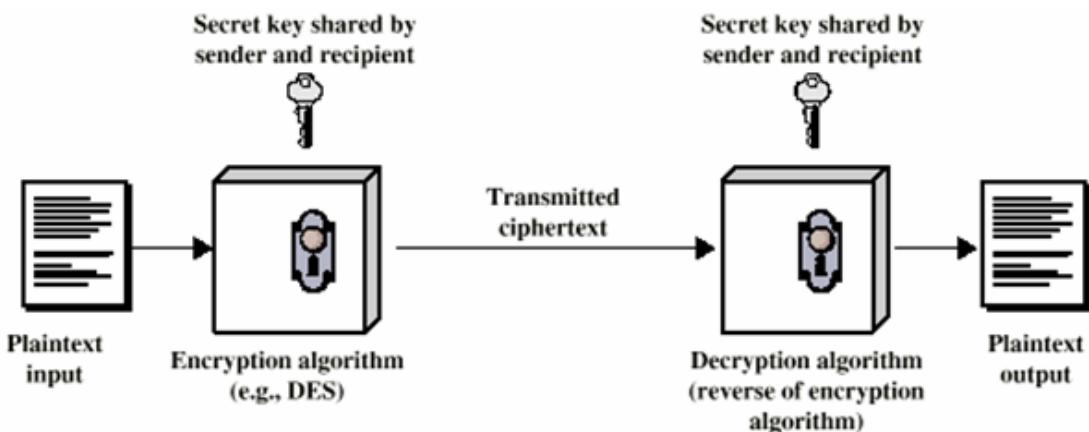
۱- سیستم رابط با کاربر : مدیر شبکه از طریق FireWall Interface رولهای خاص را به شبکه اعمال می کند .

۲- سیستم ثبت : در موقعی که یک حمله ای انجام می گیرد ردیابی می کند و آدرس حمله کننده را پیدا می کند .

۳- سیستم هشدار دهنده داشته باشد : مسئول شبکه را از ارتباطات ، بسته ها و آدرسهای مشکوک حذر کند .

با تمام این مسائل باز هم دیوار آتش نمی تواند به صورت صد در صد جلوی خرابکاری را بگیرد .

روشهای رمز نگاری :



۱) جانشینی : هر حرفی با حرفی دیگر جایگزین می شود . این روش می تواند یک جابجایی ساده باشد . اما امروزه هر جدولی برای رمزگذاری در نظر گرفته شود به راحتی با برنامه های کامپیوتری آشکار می شود . روش این کار چنین است که از آنتروپی حروف لاتین استفاده می شود . مثلاً میدانیم که حرف a درصد بیشتری در کلمات را به خود اختصاص می دهد ، آنتروپی دو حرفی هم داریم و ...

۲) جایگشتی^۱ : ترتیب قرار گرفتن حروف تغییر می کند مانند this که شود shit .

مثال : کلمه رمز مقابل که شماره ها ترتیب حروف در الفبا هستند .

M	E	G	A	B	U	C	K							
7	4	5	1	2	8	3	6							
p	l	e	a	s	e	t	r	Plaintext						
a	n	s	f	e	r	o	n	pleasetransferonemilliondollarsto						
e	m	i	l	l	i	o	n	myswissbankaccountsixtwotwo						
d	o	l	l	a	r	s	t	Ciphertext						
o	m	y	s	w	i	s	s	AFLLSKSOSELAWAIATOOSCTCLNMOMANT						
b	a	n	k	a	c	c	o	ESILYNTWRNNTSOWDPAEDOBUERIRICXB						
u	n	t	s	i	x	t	w							
o	t	w	o	a	b	c	d							

A transposition cipher

چون اصل حروف و کلمات در متن کد شده وجود دارند ، بالاخره امکان شکستن رمز وجود دارد و این نقطه ضعف این روش است و بعد پیغام به صورت زیر فرستاده می شود :

af mdtse , oot – llm

: Data Encryption Standard-۳

^۱ permutation –

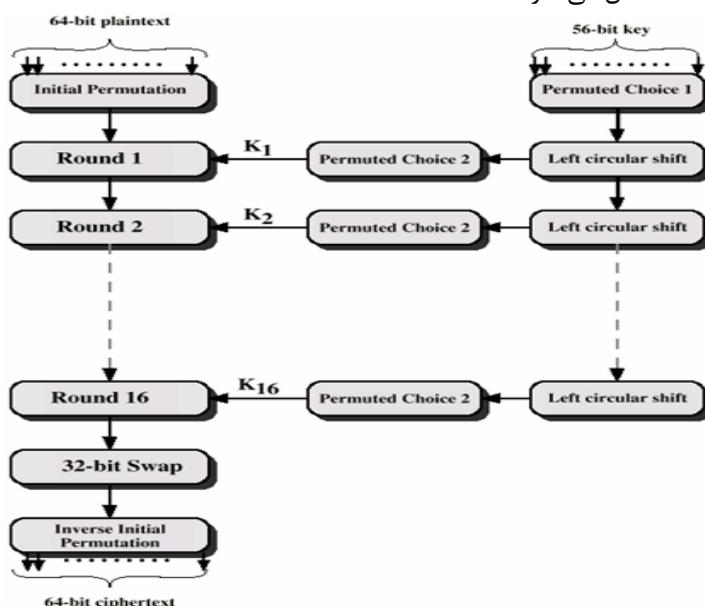
در ۱۶ مرحله عمل رمز نگاری انجام می شود یک کلید دارد که روی متن در هر مرحله اجرا می شود و در هر مرحله توابع خاصی روی آن انجام می شود . توسط IBM در اوایل دهه ۷۰ ایجاد شد . این رمز نگاری در دو حالت استفاده می شود :

۱- سیستمهای End – to –End (در لایه application)

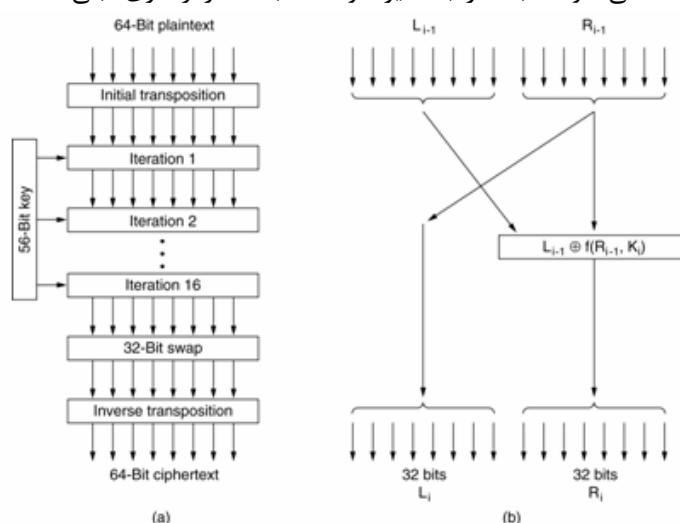
۲- روش پیوندی در نودها و مسیریابها عمل رمز نگاری و کشف آن انجام می شود .

الگوریتم DES^۱

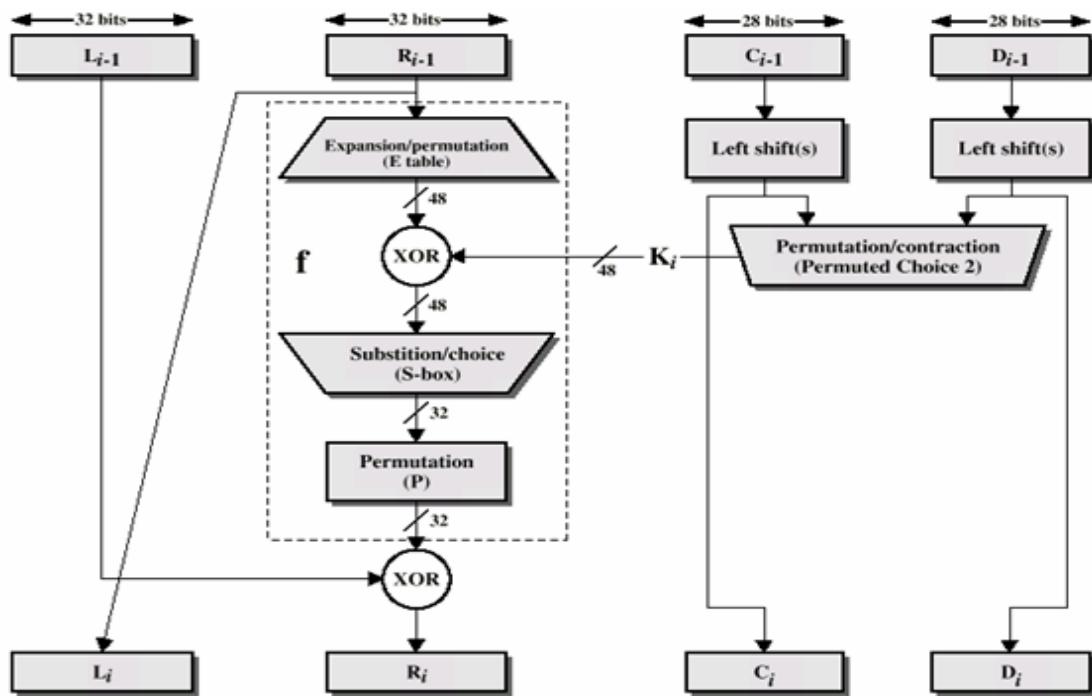
در اوایل دهه هفتاد توسط IBM توسعه یافت . اطلاعات بصورت بسته های ۶۴ بیتی در می آید و در ابتدای جایگشت روی داده ها اعمال می شود .



جزئیات تابع F : ابتدا رشته ۳۲ بیتی به یک دیتای ۴۸ بیتی تبدیل می شود . سپس عمل XOR با کلید ۴۸ بیتی انجام می شود و نتیجه باید به ۳۲ بیت تبدیل شود . یک کلید ۵۶ بیتی داریم که در تمام مراحل ۱۶ کلید ۴۸ بیتی از روی آن ساخته می شود . البته در ابتدای نیز خود داده با داده رمزنگاری قبلی XOR می شود .



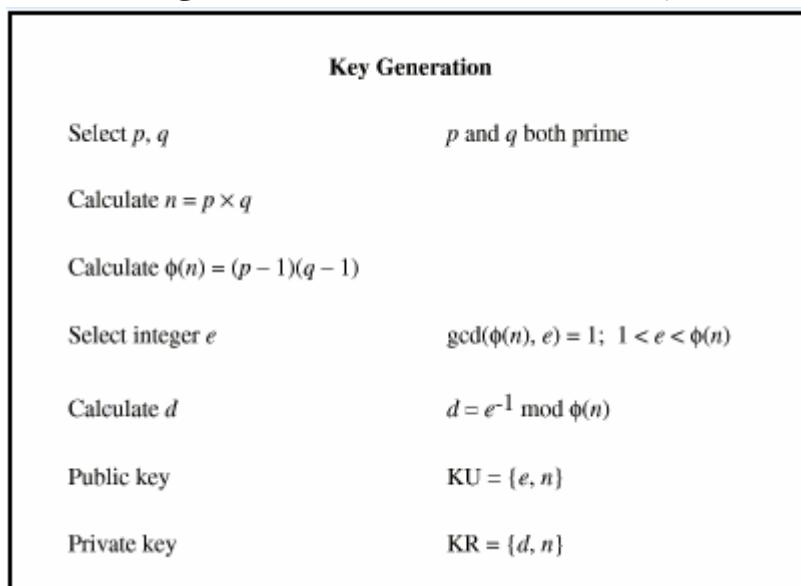
The Data encryption standard. (a) General outline.
(b) Detail of one iteration. The circled + means exclusive OR.

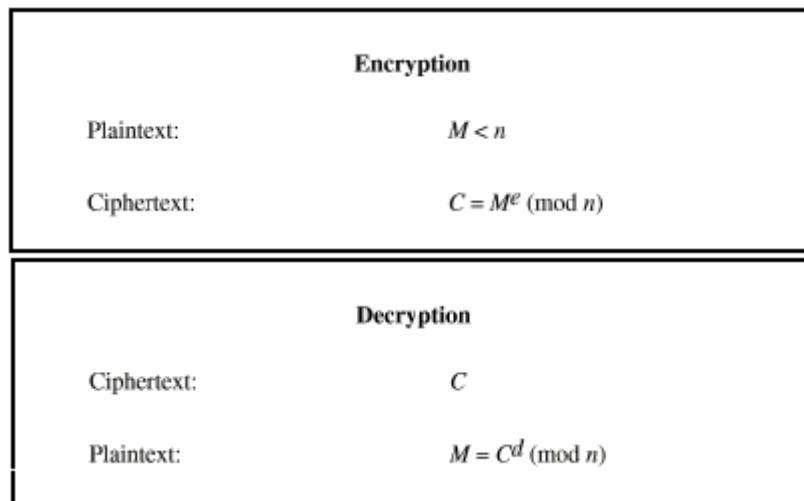


در رمز گشائی از همان کلید استفاده می شود ولی کلیدها بصورت روبرو هستند. با یک کلید ۵۶ بیتی تمام کلیدهای ۴۸ بیتی ساخته می شود. برای رمز گشائی همان مراحل تکرار می شود و کلیدهای بالا مشخص می شود. اشکال این روش این است که کلید بین رمزنگاری و رمز گشائی مشترک است.

رمزنگاری کلید عمومی (RSA) :

یک کلید برای رمزنگاری (عمومی) و یک کلید برای رمز گشائی (خصوصی). یعنی همه کلید رمزنگاری دارند ولی کلید رمز گشائی ندارند. البته کلید رمز گشائی از روی کلید رمزنگاری ساخته می شود و کار هر کسی نیست. در سال ۱۹۷۸ الگوریتم RSA بوجود آمد در ابتدا داده ها به عدد تبدیل می شوند.





ID ES OF
MA RC HX
0803 0418
0779 1983

یک داده به صورت مقابله داریم

ابتدا داده ها را به قسمت های دو کاراکتری تقسیم می کنیم
0 طبق قرارداد هر کاراکتر را به عدد تبدیل می کنیم مثلاً:

A:01
B:01
C:02

در مرحله بعد یک هفت عدد انتخاب می شود : کلید عمومی
(e, n) کلید خصوصی (d, n)

رمزگاری $c_i = p_i \pmod{n}$

رمز گشائی $p_i = c_i \pmod{n}$

باید عددی مثل d پیدا کرد تا بتوان رمز گشائی را با آن انجام داد . در روش RSA انتخاب کلید عمومی و خصوصی به صورت زیر است :

الف : دو عدد اول q, p انتخاب می شوند (تا جایی که می توانند باید بزرگ باشند (دویست رقمی))
ب : عدد n, Z به صورت زیر محاسبه می شوند :

$$n = p * q$$

$$z = (p-1)(q-1)$$

ج: عدد d را به گونه ای انتخاب کنید که نسبت به Z اول باشد .

د : بر اساس d عدد e به گونه ای انتخاب می شود که رابطه زیر برقرار باشد :

$$e * d \pmod{Z} = 1$$

مثال : فرض کنید که suzanne را بخواهیم رمز کنیم :

$$q = 11, p = 3$$

$$d = 7 : \text{یک عدد اول که نسبت به } Z = 20, n = 33 \text{ است انتخاب می شود:}$$

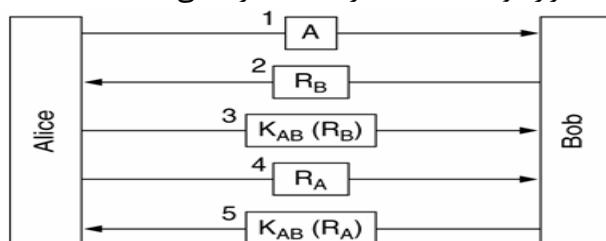
$$e = 23, e = 3 : 7 * e \pmod{20} = 1 \text{ یا } e \text{ را بدست می آوریم به گونه ای که}$$

Plaintext (P)		Ciphertext (C)		After decryption	
Symbolic	Numeric	P^3	$P^3 \pmod{33}$	C^7	$C^7 \pmod{33}$
S	19	6859	28	13492928512	19
U	21	9261	21	1801088541	21
Z	26	17576	20	1280000000	26
A	01	1	1	1	01
N	14	2744	5	78125	14
N	14	2744	5	78125	14
E	05	125	26	8031810176	05

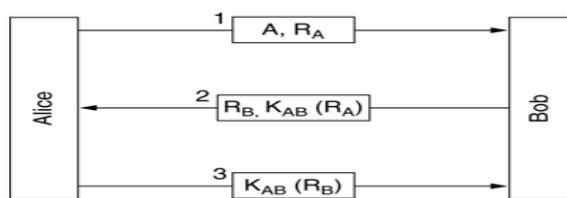
Sender's computation Receiver's computation

احراز هویت :

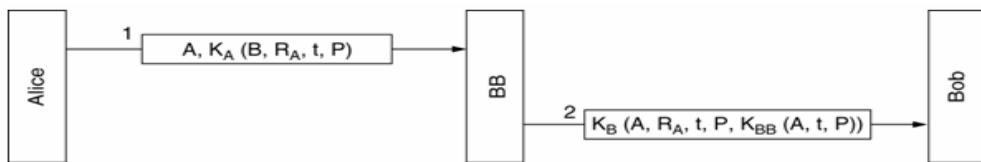
شکل رو برو مربوط به احراز هویت با استفاده از کلید مشترک می باشد .



عیب روش فوق این است که افشاری کلید می تواند باعث بوجود آمدن مشکلات شود به همین دلیل از روش احراز هویت با کلید عمومی و روش RSA استفاده می شود (در این روش کلید عمومی و کلید خصوصی وجود دارد .)



امضا های دیجیتالی :



اگر زمانی A منکر شود که پیام P را فرستاده است (و امضاء کرده است) ، B می تواند متن رمز شده K_BB(A,T,P) را به همراه متن اصلی پیام (متن P) و R_A به دادگاه ارائه کند . کلید K_BB در اختیار مرکز گواهی امضاء است که مورد اعتماد دادگاه می باشد . مرکز گواهی امضاء متن K_BB(A,T,P) را رمز گشائی کرده و با اصل پیام مورد دعوا مطابقت می دهد و اگر تطابق داشته باشد مسأله حل می شود .

گواهی دیجیتال :

یک فایل الکترونیکی است که بصورت یکتا هر مرور بر وب سرور را مشخص می کند . این گواهی امکان ارتباط امن را فراهم می کند . دارای کلید عمومی که برای امضاء استفاده شده است می باشد . (امضاء کننده گواهی دیجیتال نفر سومی است CA¹) که تمام شرکت کنندگان برای نگهداری و مدیریت کلیدها با CA توافق کرده اند . عهده دار انتشار ، ایجاد و امضاء گواهی ها و توزیع آنها می باشد . فیلد های گواهی دیجیتال به صورت زیر است :

Version

Serial number

Signtation algorithm IP

Issue name

Vadidity period

Public key information

Signature for the above field .

ابتدا فرستنده پیغام را بوسیله الگوریتم Hash تبدیل به یک Message digest می کند و از این پیغام ، پیغام ED را تولید می کند و برای گیرنده می فرستد . (گیرنده گواهی پیغام امضاء شده را چک می کند) . فرستنده : فرستنده = الگوریتم Hash + پیغام

¹ Certificate Authority -

Message digest + senderprira tekey = Encrypted digest (ED)

گیرنده گواهی پیغام امضا شده را چک می کند .

گیرنده: ED + Senderpmbdiekey = Recorer of message digest (I)

الگوریتم = Hash + Message digest (II)

گیرنده Message Digest را از دو راه (I) و (II) بدست می آورد که این دو باید باهم برابر باشند .

منابع:

- 1)William Stalling, 'Data and Computer Communication',2002
- 2)Tanenbaum,'Computer Network',2000
- 3)'Multimedia Communication and Data Communication'
- 4)Foruzan,'TCP/IP-FORUZAN',2003
- 5)Adolfo Rodriguez, John Gatrell, John Karas, Roland Peschke, 'TCP/IP Tutorial and Technical Overview', 2001,IBM Red Book



www.samavi.info