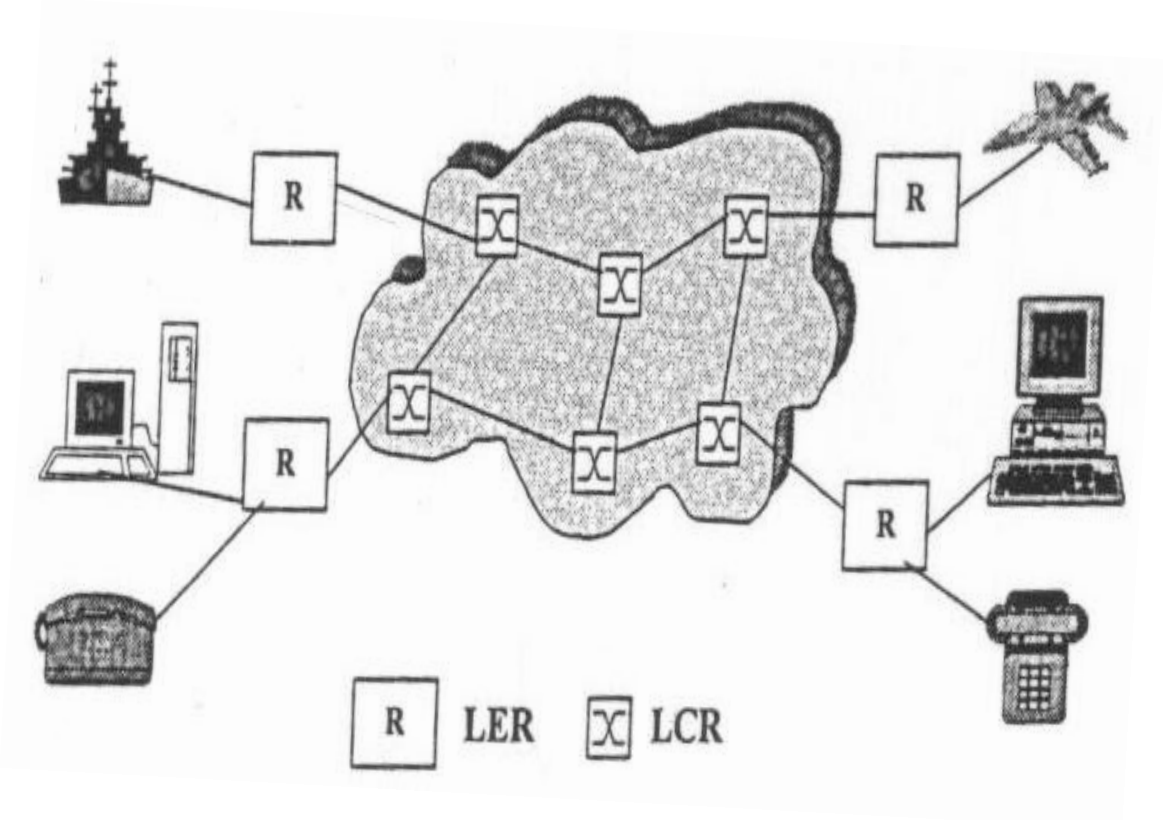
دانشگاه علم و صنعت ایران

شبکه های کامپیوتری پیشرفته



استاد : دکتر محمود فتحی

فهرست مطالب:

عنوان	صفحه
بخش ۱: مفاهیم پایه	۲
فصل ۱: مروری بر شبکه های کامپیوتری	۳
بخش ۲: آدرس دهی	۲۴
فصل ۲: آدرس دهی در شبکه های کامپیوتری	۲۵
فصل ۳: مسیریابی در مسیریابها	۳۸
فصل ۴: پروتکل های مسیریابی در شبکه	۴۵
فصل ۵: MultiCasting و پروتکلهای مسیریابی Multicast	۶۹
بخش ۳: سوئیچ داده	۸۰
فصل ۶: روشهای سوئیچ داده	۸۱
فصل ۷: شبکه های ATM و FrameRelay	۱۰۲
فصل ۸: ISA ،DiffServ و MPLS	۱۳۴
بخش ۴: پروتکلهای شبکه	۱۵۷
فصل ۹: پروتکل IP	۱۵۸
فصل ۱۰: پروتکل های IGMP و ICMP	۱۷۱
فصل ۱۱: کنترل اتصالات در شبکه	۱۷۹
فصل ۱۲: پروتکل های UDP و TCP	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 ۱:
مفاهیم پایه شبکه

فصل ۱: مروری بر شبکه های کامپیوتری

فصل ۱:

مروری بر شبکه های کامپیوتری

استفاده از شبکه های کامپیوتری در چندین سال اخیر رشد فراوانی کرده وسازمانها وموسسات 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 وتطبیق 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 ارتقاء می باید ویا یک شبکه از ابتدا طراحی می شود؟
- چه سرویس ها و خدماتی برروی شبکه ارائه خواهد شد؟

بطور کلی قبل از طراحی فیزیکی یک شبکه کامپیوتری ، ابتدا باید خواسته ها شناسایی وتحلیل شوند، مثلاً در یک کتابخانه چرا قصد ایجاد یک شبکه را داریم و این شبکه باید چه سرویس ها وخدماتی را ارائه نماید؛ برای تامین سرویس ها وخدمات مورد نظر اکثریت کاربران ، چه اقداماتی باید انجام داد ؛ مسائلی چون پروتکل مورد نظر برای استفاده از شبکه ، سرعت شبکه واز 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 وابزارهای جانبی مثل چاپگرها، اسکنرها ومانند اینها هستند که بطور مستقیم بمنظور استفاده مشترک از سخت افزار ونرم افزار، منابع اطلاعاتی ابزارهای متصل ایجاده شده است توجه داشته باشید که به تمامی تجهیزات سخت افزاری ونرم 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 وداده 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 وپرهیز 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 وسیستم ها در شبکه نسخه های دوم وپشتیبان تهیه کرد ودر 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 وآمادگی دایمی 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 وتبدیل به یک شبکه بزرگتر شود. در اینجا هزینه توسعه سیستم هزینه امکانات وتجهیزات مورد نیاز برای گسترش شبکه مد نظر است.
۶ - ارتباطات:کاربران می توانند از طریق نوآوریهای موجود مانند پست الکترونیکی ویا 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[1] یا گره[2] 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 ویا 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 وآدرس 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 وهمچنین 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[3]
۲ - شبکه مبتنی بر سرویس دهنده[4]
۳ - شبکه سرویس دهنده / سرویس گیرنده[5]

مدل شبکه نظیر به نظیر:

در این شبکه ایستگاه ویژه ای جهت نگهداری فایل های اشتراکی وسیستم عامل شبکه وجود ندارد. هر ایستگاه می تواند به منابع سایر ایستگاه ها در شبکه دسترسی پیدا کند. هر ایستگاه خاص می تواند هم بعنوان سرویس دهنده و هم بعنوان 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 بعهده 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 وفایل 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 وسرویس دهنده پس از اجرای وظیفه محوله ، نتایج حاصل را به ایستگاه در خواست کننده عودت می دهد. در این مدل حجم اطلاعات مبادله شده شبکه ، در مقایسه با مدل مبتنی بر سرویس دهنده کمتر است واین 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 تواند 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 ، چاپگرها، هاب ها، سیم ها ، کابل ها وسایر رسانه هایی که برای اتصال ابزارهای شبکه استفاده می شوند. سازگار کننده ها[1]،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 سازگارکننده در این است که به دریافت وترجمه سیگنال ها ی درون داد از شبکه از جانب یک ایستگاه کاری وترجمه وارسال برون داد به کل شبکه می پردازد.

اجزا ءشبکه :

اجزا اصلی یک شبکه کامپیوتری عبارتند از :

۱ - کارت شبکه(NIC[2]) : برای استفاده از شبکه وبرقراری 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 وگیرنده بصورت سخت افزاری وبرای کنترل ارسال ودریافت داده نصب می گردد.

۲ - رسانه انتقال[3] : رسانه انتقال کامپیوتر ها را به یکدیگر متصل کرده وموجب برقراری ارتباط بین کامپیوتر های یک شبکه می شود . برخی از متداولترین رسانه های انتقال عبارتند از : کابل زوج سیم بهم تابیده، کابل کواکسیال وکابل فیبر نوری .

---

[1] - Adaptors

[2] - Network Interface Card

[3] - Transmission Medium

۳ - سیستم عامل شبکه (NOS[1]):سیستم عامل شبکه برروی 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 وپروتکل بین رایانه ها وبا مدیریت نرم افزاری موسوم به سیستم عامل شبکه را شبکه محلی گویند. کامپیوتر سرویس گیرنده باید از طریق کامپیوتر سرویس دهنده به اطلاعات وامکانات به اشتراک گذاشته دسترسی یابند. همچنین ارسال ودریافت 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 وپیاده سازی می باشند.

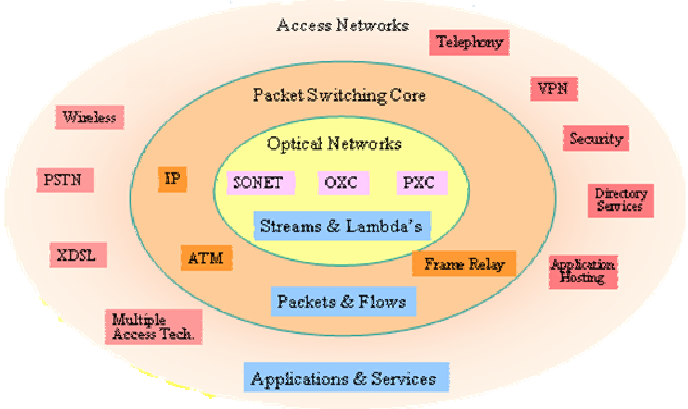
  ۲ - از سرعت نسبتا بالایی برخوردارند.

  ۳ - دارای یک ارتباط دایمی 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 واز طریق خطوط مخابراتی به یکدیگر متصل می شوند. کاربران هر یک از این شبکه ها می توانند به اطلاعات ومنابع به اشتراک گذاشته شده توسط شبکه های دیگر دسترسی یابند. از این فناوری با نام شبکه های راه دور[2] نیز نام برده می شود. در شبکه گسترده سرعت انتقال داده نسبت به شبکه های محلی خیلی کمتر است. بزرگترین ومهم ترین شبکه گسترده ، شبکه جهانی اینترنت می باشد.



تصویر ۱-۱: ساختار لایه ای اینترنت

[1] Network Operating System -
[2] Long Haul Network -

توپولوژی شبکه :

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

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

  نقاط ضعف این توپولوژی آن است که عملیات کل شبکه به هاب وابسته است. این بدان معناست که اگر هاب از کار بیفتد، کل شبکه از کار خواهد افتاد . نقاط قوت توپولوژی ستاره عبارتند از:
  - نصب شبکه با این توپولوژی ساده است.
  - توسعه شبکه با این توپولوژی به راحتی انجام می شود.
  - اگر یکی از خطوط متصل به هاب قطع شود ، فقط یک کامپیوتر از شبکه خارج می شود.

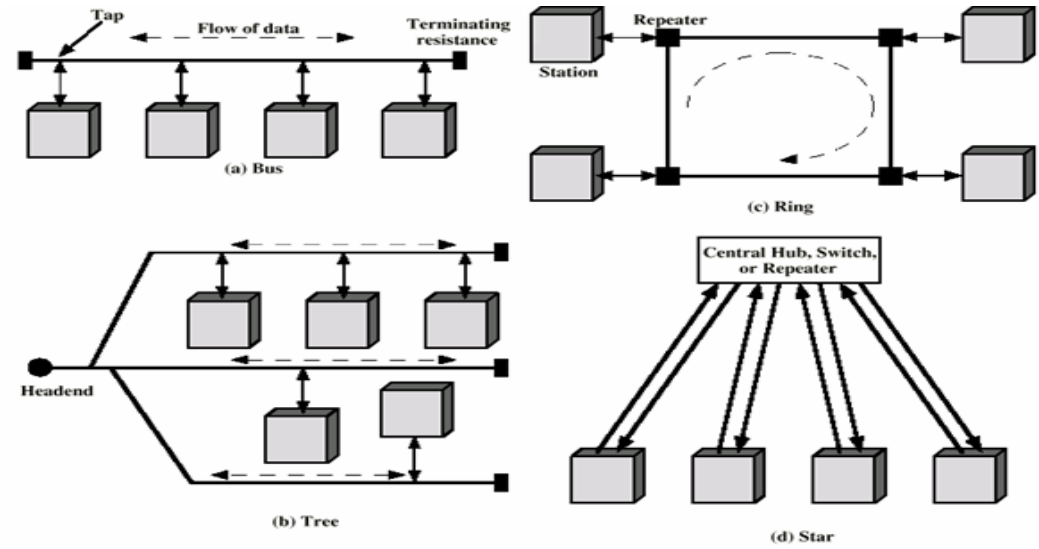
- توپولوژی حلقوی(Ring): این توپولوژی توسط شرکت IBM اختراع شد وبهمین دلیل است که این توپولوژی بنام IBM Tokenring مشهور است.در این توپولوژی کلیه کامپیوتر ها به گونه ای به یکدیگر متصل هستند که مجموعه آنها یک حلقه را می سازد. کامپیوتر مبدا اطلاعات را به کامپیوتری بعدی در حلقه ارسال نموده و آن کامپیوتر آدرس اطلاعات را برای خود کپی می کند، آنگاه اطلاعات را به کامپیوتر بعدی در حلقه منتقل خواهد کرد و به همین ترتیب این روند ادامه پیدا می کند تا اطلاعات به کامپیوتر مبدا برسد. سپس کامپیوتر مبدا این اطلاعات را از روی حلقه حذف می کند. نقاط ضعف توپولوژی فوق عبارتند از:
  - اگر یک کامپیوتر از کار بیفتد ، 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 توپولوژی فوق عبارتند از :
  - نصب شبکه با این توپولوژی ساده است.
  - توسعه شبکه با این توپولوژی به راحتی انجام می شود.
  - در این توپولوژی از کابل فیبر نوری میتوان استفاده کرد.

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

- توپولوژی توری(Mesh): در این توپولوژی هر کامپیوتری مستقیما به کلیه کامپیوترهای شبکه متصل می شود. مزیت این توپولوژی آن است که هر کامپیوتر با سایر کامپیوتر ها ارتباطی مجزا دارد. بنابراین ، این توپولوژی دارای بالاترین درجه امنیت واطمینان می باشد. اگر یک کابل ارتباطی در این توپولوژی قطع شود ، شبکه همچنان فعال باقی می ماند. از نقاط ضعف اساسی این توپولوژی آن است که از تعداد زیادی خطوط ارتباطی استفاده می کند، مخصوصا زمانیکه تعداد ایستگاه ها افزایش یابند. به همین جهت این توپولوژی از نظر اقتصادی مقرون به صرفه نیست. برای مثال ، در یک شبکه با صد ایستگاه کاری ، ایستگاه شماره یک نیازمند به نود ونه می باشد. تعداد کابل های مورد نیاز در این توپولوژی با رابطه N(N-1)/2 محاسبه می شود که در آن N تعداد ایستگاه های شبکه می باشد.
- توپولوژی درختی(Tree): این توپولوژی از یک یا چند هاب فعال یا تکرار کننده برای اتصال ایستگاه ها به یکدیگر استفاده می کند. هاب مهمترین عنصر شبکه مبتنی بر توپولوژی در ختی است؛ زیرا کلیه ایستگاه ها را به یکدیگر متصل می کند. وظیفه هاب دریافت اطلاعات از یک ایستگاه و تکرار وتقویت آن اطلاعات و سپس ارسال آنها به ایستگاه دیگر می باشد.
- توپولوژی ترکیبی (Hybrid): این توپولوژی ترکیبی است از چند شبکه با توپولوژی متفاوت که توسط یک کابل اصلی بنام Back bone به یکدیگر مرتبط شده اند . هر شبکه توسط یک Bridg به کابل Back bone متصل می شود.



تصویر۱-۲: برخی توپولوژی های رایج شبکه

مدل OSI[1]:

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.

[1] - Open System Interconnection

- 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 رابط ها انتخاب شوند.

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

۱ - لایه فیزیکی : به انتقال بیتهای خام برروی کانال ارتباطی مربوط می شود. در اینجا مدل طراحی با رابط های مکانیکی ، الکتریکی ، ورسانه انتقال فیزیکی که زیر لایه فیزیکی قراردارند سروکار دارد.

۲ - لایه پیوند داده : مبین نوع فرمت هاست مثلا شروع فریم ، پایان فریم، اندازه فریم وروش انتقال فریم . وظایف این لایه شامل موارد زیر است :مدیریت فریم ها ، خطایابی وارسال مجدد فریم ها، ایجاد تمایز بین فریم ها داده وکنترل وایجاد هماهنگی بین کامپیوتر ارسال کننده ودریافت کننده داده ها. پروتکل های معروف برای این لایه عبارتند از :

- پروتکل SDLC که برای مبادله اطلاعات بین کامپیوتر ها بکار می رود و اطلاعات را به شکل فریم سازماندهی می کند.
- پروتکل HDLC که کنترل ارتباط داده ای سطح بالا زیر نظر آن است وهدف از طراحی آن این است که با هر نو ع ایستگاهی کارکند از جمله ایستگاههای اولیه ، ثانویه وترکیبی.

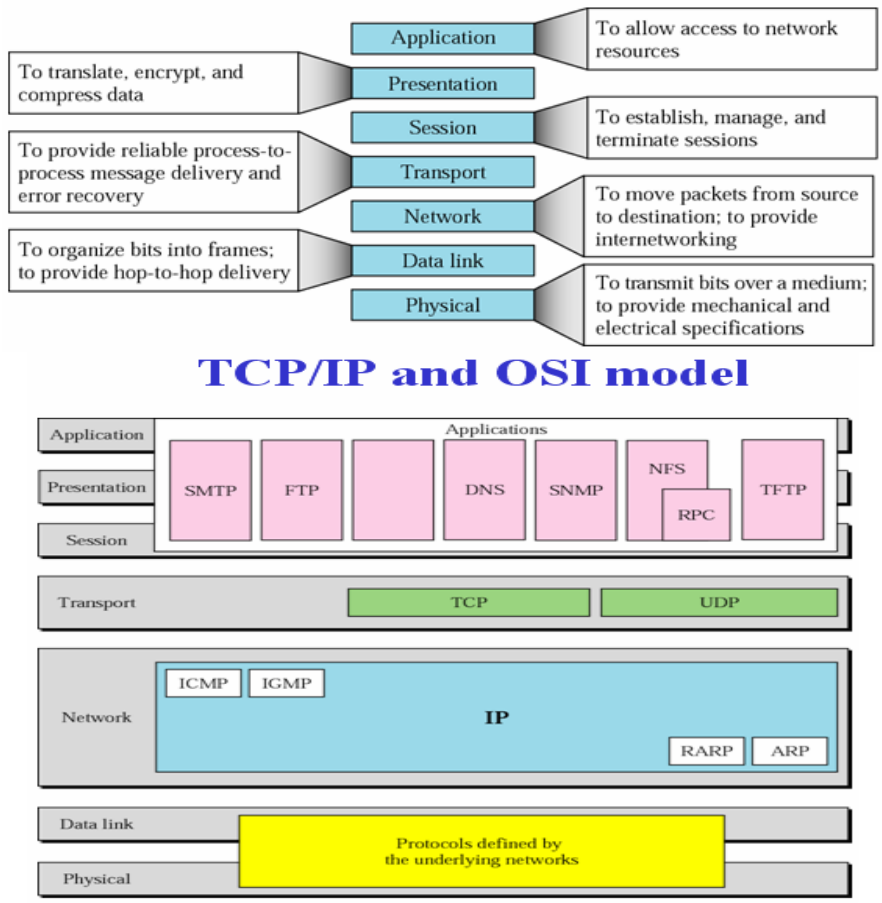
۳ - لایه شبکه : وظیفه این لایه ، مسیر یابی می باشد ، این مسیر یابی عبارتست از : تعیین مسیر متناسب برای انتقال اطلاعات . لایه شبکه آدرس منطقی هر فریم را بررسی می کند . و آن فریم را بر اساس جدول مسیر یابی به مسیر یاب بعدی می فرستد . لایه شبکه مسئولیت ترجمه هر آدرس منطقی به یک آدرس فیزیکی را بر عهده دارد. پس می توان 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 برعهده دارد. لایه انتقال پس از ارسال یک فریم به مقصد ، منتظر می ماند تا سیگنالی از مقصد مبنی بر دریافت آن فریم دریافت کند. در صورتیکه لایه محل در منبع سیگنال مذکور را از مقصد دریافت نکند. مجددا اقدام به ارسال همان فریم به مقصد خواهد کرد.

۵ - لایه اجلاس : وظیفه برقراری یک ارتباط منطقی بین نرم افزار های دو کامپیوتر ی 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 می کند، سپس از ایستگاه ، درخواست نام کاربر، ورمز عبور را خواهد کرد. این فرایند نمونه ای از یک اجلاس می باشد.

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

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



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[1]): از مهمترین ومشهورترین پروتکل های مورد استفاده در شبکه اینترنت است این بسته نرم افزاری به اشکال مختلف برای کامپیوتر ها وبرنامه ها ی 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 ابررایانه 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

[1] - Transmission Control Protocol I/nternet Protocol

از فاکتورهای مهم که این پروتکل بعنوان یک پروتکل ارتباطی جهانی مطرح می گردد، به موارد زیر می توان اشاره کرد:

- این پروتکل در چار چوب UNIX Operating System ساخته شده وتوسط اینترنت بکار گرفته می شود.
- برروی هر کامپیوتر قابل پیاده سازی می باشد.
- بصورت حرفه ای در شبکه های محلی وگسترده مورد استفاده قرار می گیرد.
- پشتیبانی از مجموعه برنامه ها وپروتکل های استاندارد دیگر چون پروتکل انتقال فایل، FTP ، وپروتکل دو سویه PPP .

بنیاد واساس پروتکل TCP/IP آن است که برای دریافت و ارسال داده ها یا پیام پروتکل مذکور ؛ پیام ها و داده ها را به بسته های کوچکتر وقابل حمل تر تبدیل می کند ، سپس این بسته ها به مقصد انتقال داده می شود ودر نهایت پیوند این بسته ها به یکدیگر که شکل اولیه پیام ها وداده ها را بخود می گیرد ، صورت می گیرد.

یکی دیگر از ویژگی های مهم این پروتکل قابلیت اطمینان آن در انتقال پیام هاست یعنی این قابلیت که به بررسی وبازبینی بسته ها ومحاسبه بسته های دریافت شده دارد. در ضمن این پروتکل فقط برای استفاده در شبکه اینترنت نمی باشد. بسیاری از سازمان وشرکت ها برای ساخت وزیر بنای شبکه خصوصی خود که از اینترنت جدا می باشد نیز در این پروتکل استفاده می کنند.

- پروتکل سیستم ورودی وخروجی پایه شبکهNet Bios، واسطه یا رابطی است که توسط IBM بعنوان استانداردی برای دسترسی به شبکه توسعه یافت . این پروتکل داده ها را از لایه بالاترین دریافت کرده وآنها را به شبکه منتقل می کند. سیستم عاملی که با این پروتکل ارتباط برقرار می کند سیستم عامل شبکه NOS، نامیده می شود کامپیوتر ها از طریق کارت شبکه خود به شبکه متصل می شوند. کارت شبکه به سیستم عامل ویژه ای برای ارسال اطلاعات نیاز دارد. این سیستم عامل ویژه را Net BIOS می نامند که در حافظه ROM کارت شبکه ذخیره شده است. BIOS Net همچنین روشی را برای دسترسی به شبکه ها با پروتکل های مختلف مهیا می کند . این پروتکل از سخت افزار شبکه مستقل است . این پروتکل مجموعه ای از فرامین لازم برای در خواست خدمات شبکه ای سطح پایین را برای برنامه های کاربردی فراهم می کند تا جلسات لازم برای انتقال اطلاعات در بین گره ها ی یک شبکه را هدایت کنند.

  در حال حاضر وجود Net BIOS Net BEUI امتیازی جدید می دهد که این امتیاز درواقع ایجاد گزینه انتقال استاندارد است و Net BEUI[1] در شبکه های محلی بسیار رایج است. همچنین قابلیت انتقال سریع داده ها را نیز دارد . اما چون یک پروتکل غیر قابل هدایت است به شبکه های محلی محدود شده است.

ابزارهای اتصال دهنده[2] :

ابزارهای اتصال به یک شبکه اضافه می گردند تا عملکرد وگستره شبکه وتوانایی های سخت افزاری شبکه را ارتقاء دهند . گستره وسیعی از ابزارهای اتصال در شبکه وجود دارند اما شما احتمالاً برای کار خود به ابزارهای ذیل نیازمند خواهید بود:

---

[1] - Net BIOS Enhansed User Interface

[2] - Connectivity Devices

۱. تکرار کننده: تکرار کننده وسیله ای است که برای اتصال چندین سگمنت یک شبکه محلی بمنظور افزایش وسعت مجاز آن شبکه مورد استفاده قرار می گیرد . هر تکرار کننده از درگاه ورودی[1] خود داده ها را پذیرفته وبا تقویت آنها ، داده ها را به درگاهی خروجی خود ارسال می کند. یک تکرار کننده در لایه فیزیکی مدل OSI عمل می کند. هر کابل یا سیم بکار رفته در شبکه که بعنوان محلی برای عبور و مرور سیگنال هاست آستانه ای دارد که در آن آستانه سرعت انتقال سیگنال کاهش می یابد و در اینجا تکرار کننده بعنوان ابزاری است که این سرعت عبور را در طول رسانه انتقال تقویت می کند.

۲. هاب: ابزاری هستند در شبکه که برای اتصال یک یا بیش از دو ایستگاه کاری به شبکه مورد استفاده قرار می گیرد ویک ابزار معمول برای اتصال ابزارهای شبکه است . هابها معمولاً برای اتصال سگمنت های شبکه محلی استفاده می شوند. یک هاب دارای در گاهی های چند گانه است. وقتی یک بسته در یک درگاهی وارد می شود به سایر در گاهی ها کپی می شود تا اینکه تمامی سگمنت های شبکه محلی بسته ها را ببینند. سه نوع هاب رایج وجود دارد:

- هاب فعال : که مانند آمپلی فایر عمل می کند و باعث تقویت مسیر عبور سینگال ها می شود واز تصادم وبرخورد سیگنال ها در مسیر جلوگیری بعمل می آورد . این هاب نسبتا قیمت بالایی دارد.
- غیر فعال : که بر خلاف نوع اول که در مورد تقویت انتقال سیگنال ها فعال است این هاب منفعل است.
- آمیخته :که قادر به ترکیب انواع رسانه ها کابل کواکسیال نازک ،ضخیم و... بوده و باعث تعامل درون خطی میان سایر هابها می شود.

۳. مسیریاب: در شبکه سازی فرایند انتقال بسته های اطلاعاتی از یک منبع به مقصد عمل مسیریابی است که تحت عنوان ابزاری تحت عنوان مسیریاب انجام می شود. مسیریابی یک شاخصه کلیدی در اینترنت است زیرا که باعث می شود پیام ها از یک کامپیوتر به کامپیوتر دیگر منتقل شوند. این عملکرد شامل تجزیه وتحلیل مسیر برای یافتن بهترین مسیر است. مسیریاب ابزاری است که شبکه های محلی را بهم متصل می کند یا به بیان بهتر بیش از دو شبکه را بهم متصل می کند. مسیریاب بر حسب عملکردش به دو نوع زیر تقسیم می شود:

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

۴. دروازه[2]: دروازه ها در لایه کاربرد مدل OSI عمل می کنند. کاربرد آن تبدیل یک پروتکل به پروتکل دیگر است. زمانیکه که در ساخت شبکه، هدف استفاده از خدمات اینترنت است، دروازه ها مقوله های مطرح در شبکه سازی خواهند بود.

۵. پل : یک پل برای اتصال سگمنت های یک شبکه " همگن " به یکدیگر مورد استفاده قرار می گیرد. یک پل در لایه پیوند داده ها، عمل می کند. پل ها فریم ها را بر اساس آدرس مقصدشان ارسال می کنند. آنها همچنین می توانند جریان داده ها را کنترل نموده وخطاهایی را که در حین

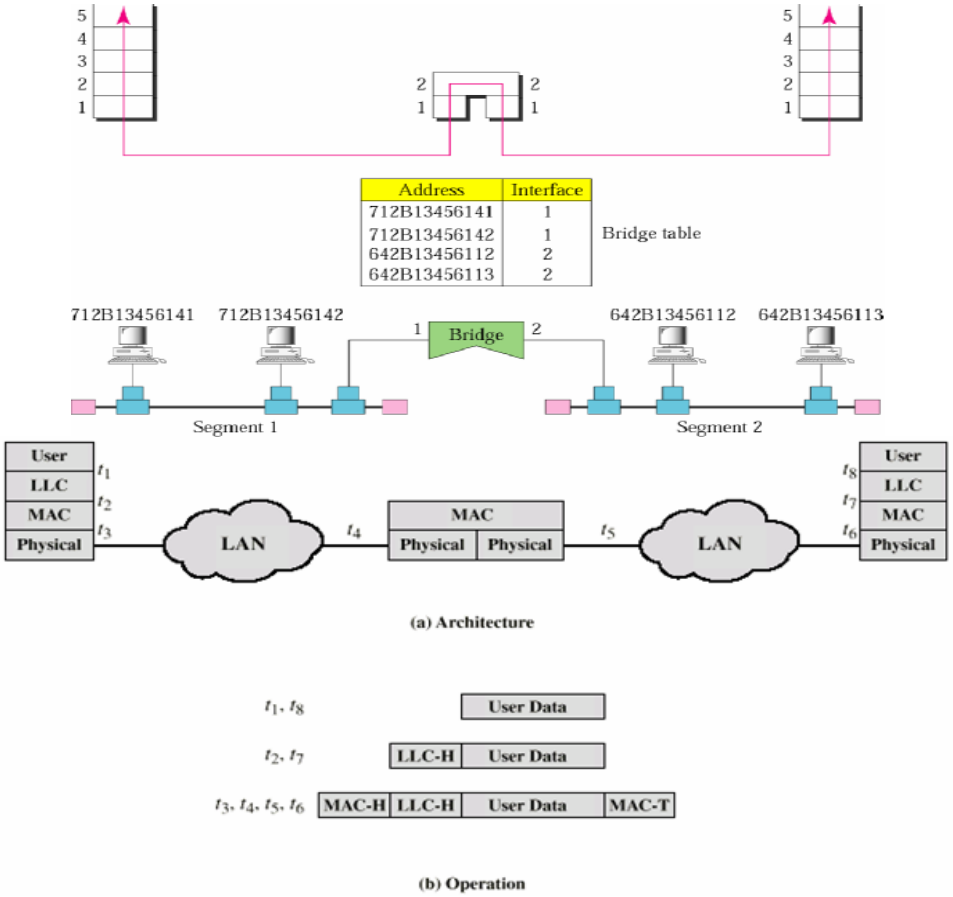
---

[1] Port -

[2] Gateway -

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

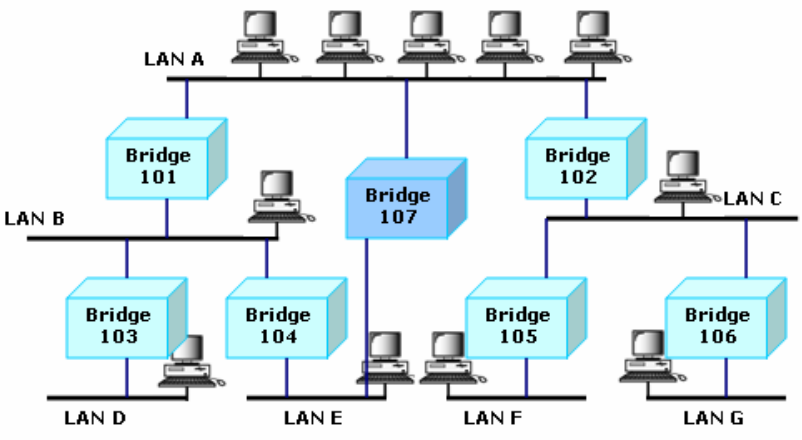
پل ها قادر به فیلتر کردن فریم ها می باشند. فیلتر کردن فریم برای حذف فریم هـای عمـومی یـا همگانی که غیر ضروری هستند مفید می باشد، پل ها قابل برنامه ریزی هستند ومی تـوان آنهـا را به گونه ای برنامه ریزی کرد که فریم های ارسال شده از طرف منـابع خاصـی را حـذف کننـد. بـا تقسیم یک شبکه بزرگ به چندین سگمنت و استفاده از یک پل برای اتصال آنها به یکدیگر ، توان عملیاتی شبکه افزایش خواهد یافت . اگر یک سگمنت شبکه از کار بیفتـد ، سـایر سـگمنت هـای متصل به پل می توانند شبکه را فعال نگه دارند ، پـل هـا موجـب افـزایش وسـعت شـبکه محلـی می شوند.



تصویر ۱-۴: ساختار تبادل داده بین سگمنتهای 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 بخشهای 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 :Source Routing یا Transparent .

در SourceRouting آدرس پل مورد نظر را در بسته قرار می گیرد.

در Transparent خود پل ها اطلاعات با هم رد و بدل می کنند.

BPDU(Bridge Protocol Data Unit)

در این روش از Spanning Tree استفاده می شود 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 Forwareding

پل ها بسته هایی را با هم رد و بدل می کنند و تاخیرخود را از پلهای دیگر و همچنین هزینه مسیر را اندازه گیری می کنند. بدین ترتیب درخت Spanning ساخته می شود .

۶. سوئیچ : سوئیچ نوع دیگری از ابزارهایی است که برای اتصال چند شبکه محلی به یکدیگر مورد استفاده قرار می گیرد که باعث افزایش توان عملیاتی شبکه می شود. سوئیچ وسیله ای است که دارای درگاه های متعدد است که بسته ها را از یک درگاه می پذیرد، آدرس مقصد را بررسی می کند و سپس بسته ها را به درگاه مورد نظر که متعلق به ایستگاه میزبان با همان آدرس مقصد می باشد، ارسال می کند. اغلب سوئیچ های شبکه محلی در لایه پیوند داده های مدل OSI عمل می کند.

سوئیچ ها بر اساس کاربردشان به متقارن[1] و نامتقارن[2] تقسیم می شوند. در نوع متقارن ، عمل سوئیچینگ بین سگمنت هایی که دارای پهنای باند یکسان هستند انجام می دهد یعنی 10 Mbps به 10 Mbps و... سوئیچ خواهد شد. اما در نوع نامتقارن این عملکرد بین سگمنت هایی با پهنای باند متفاوت انجام می شود.

دو نوع سوئیچ وجود دارد که عبارتند از :

[1] Symmetric -
[2] Asymmetric

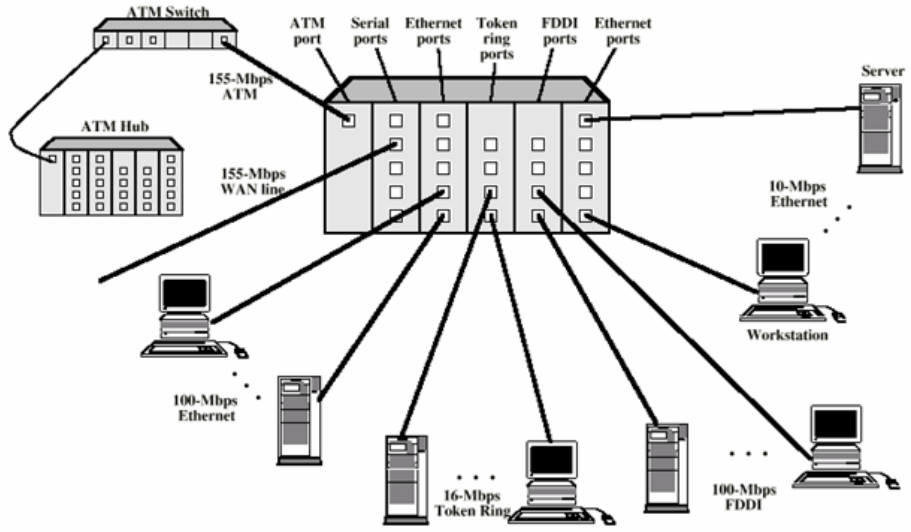
- سوئیچ Cut-through : این نوع سه یا چهار بایت اول یک بسته را می خواند تا آدرس مقصد آنرا بدست آورد ، آنگاه آن بسته را به سگمنت دارای آدرس مقصد مذکور ارسال می کند این در حالی است که قسمت باقی مانده بسته را از نظر خطایابی مورد بررسی قرار نمی دهد.
- سوئیچ Store-and-forward : این نوع ابتدا کل بسته را ذخیره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

HUB، 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/CDکه برای شبکه های اترنت و اترنت سریع می باشد .
- نسل دوم : شبکه های FDDI .
- نسل سوم : ATM LAN :

یک هاب به صورت چند پروتکلی می باشد؛ یعنی پورتهای برای اترنت 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 داه های مختلف داشته باشند . برای افزایش سرعت و کاهش پهنای باند از MLT استفاده می شود . یعنی تغییرات جزئی درنظر گرفته نمی شود و تغییر سیگنالهای بزرگ در نظر گرفته می شود.

شبکه های محلی ATM سه نوع دارند:

۱. شبکه های ATM محلی خالص : هر نود مستقیماً به سوئیچ ATM متصل است.
۲. شبکه های مرسوم ATM : شبکه های غیر ATM از طریق مبدلهایی 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 پهنای باند:

پهنای باند[1] ، به تفاوت بین بالاترین و پایین‌ترین فرکانسهایی که یک سیستم ارتباطی می‌تواند ارسال کند گفته می‌شود. به عبارت دیگر منظور از پهنای باند مقدار اطلاعاتی است که می‌تواند در یک مدت زمان معین ارسال شود. برای وسایل دیجیتال، پهنای باند برحسب بیت در ثانیه و یا بایت در ثانیه بیان می‌شود. برای وسایل آنالوگ، پهنای باند، برحسب سیکل در ثانیه بیان می‌شود. دو روش برای ارسال اطلاعات از طریق رسانه‌های انتقالی وجود دارد که عبارتند از: روش ارسال مبتنی بر باند[2] و روش ارسال باند پهن[3].

در یک شبکه LAN، کابلی که کامپیوترها را به هم وصل می‌کند، فقط می‌تواند در یک زمان یک سیگنال را از خود عبور دهد، به این شبکه یک شبکه مبتنی بر باند می‌گوئیم. به منظور عملی ساختن این روش و امکان استفاده از آن برای همه کامپیوترها، داده‌ای که توسط هر سیستم انتقال می‌یابد، به واحدهای جداگانه‌ای به نام بسته[4]، شکسته می‌شود. در واقع در کابل یک شبکه LAN، توالی بسته های تولید شده توسط سیستم‌های مختلف را شاهد هستیم که به سوی مقاصد گوناگونی در حرکت‌اند.

برای مثال وقتی کامپیوتر شما یک پیام پست الکترونیکی را انتقال می‌دهد، این پیام به بسته های متعددی شکسته می‌شود و کامپیوتر هر بسته را جداگانه انتقال می‌دهد. کامپیوتر دیگری در شبکه که بخواهد به انتقال داده بپردازد نیز در یک زمان یک بسته را ارسال می‌کند. وقتی تمام بسته هایی که بر روی هم یک انتقال خاص را تشکیل می‌دهند، به مقصد خود می‌رسند، کامپیوتر دریافت کننده آنها را به شکل پیام الکترونیکی اولیه بر روی هم می‌چیند. این روش پایه و اساس شبکه‌های سوئیچ بسته ای می‌باشد 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 می‌شوند. از مثالهای شبکه ارسال باند پهن که ما هر روز از آن استفاده می‌کنیم، شبکه تلویزیون است. در این حالت فقط یک کابل به منزل کاربران کشیده می‌شود، اما همان یک کابل، سیگنالهای مربوط به کانالهای متعدد تلویزیون را بطور همزمان حمل می‌نماید. از روش ارسال باند پهن به طور روز افزونی در شبکه‌های WAN استفاده می‌شود.

از آنجائیکه در شبکه‌های LAN در یک زمان از یک سیگنال پشتیبانی می‌شود، در یک لحظه داده‌ها تنها در یک جهت حرکت می‌کنند. به این ارتباط Half-Duplex گفته می‌شود. در مقابل به سیستم‌هایی که می‌توانند بطور همزمان در دو جهت با هم ارتباط برقرار کننده Full-Duplex گفته می‌شود. مثالی از این نوع ارتباط شبکه تلفن می‌باشد. شبکه‌های LAN با داشتن تجهیزاتی خاص بصورت Full-Duplex عمل کنند.

کابل شبکه:

پیش از اینکه در مورد انواع کابل‌ها و پهنای باند مربوط به آنها، به بحث بپردازیم، ذکر این نکته ضروری است که نوع کابل انتخابی شما بطور مستقیم به توپولوژی شبکه تان وابسته است. در این قسمت سعی گردیده توپولوژی 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

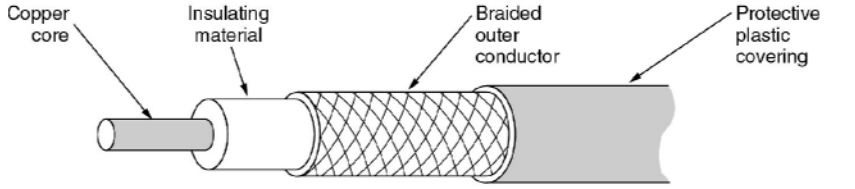
---

[1] - BandWitdh
[2] - Baseband
[3] - Broadband
[4] - Packet

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



تصویر ۱-۷: کابل کواکسیال

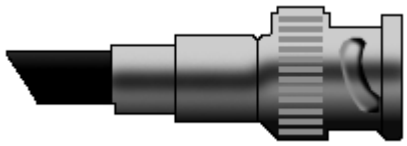
اجزای کابل کواکسیال بشرح زیر می باشد:

- 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.

رایج‌ترین نوع اتصال دهنده مورد استفاده در کابل کواکسیال ، BNC[1] می‌باشد. انواع مختلفی از سازگار کننده‌ها برایBNCها وجود دارند شامل:Barrel connector , Tconnector وTerminator.



تصویر ۱-۸: اتصال دهنده BNC

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

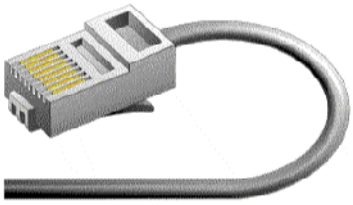
[1] - Bayonet-Neill-Concelman

باید دانست که از عبارتهایی مانند 10 Base 5 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 10 Base 2 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[1]، 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:

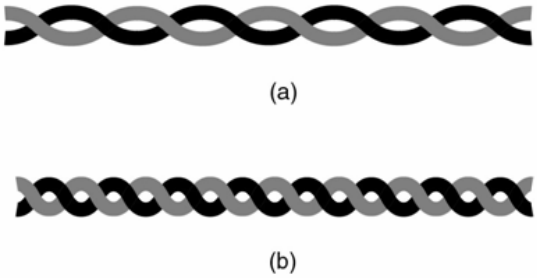
- UTP[2]: کابل ارزان قیمتی است که نصب آسانی دارد و برای شبکه‌های LAN سیم بسیار مناسبی است، همچنین نسبت به نوع دوم کم‌وزن‌تر و انعطاف‌پذیرتر است. مقدار سرعت دیتای عبوری از آن ۴ مگابیت در ثانیه تا ۱۰۰ مگابیت در ثانیه می‌باشد. این کابل می‌تواند تا مسافت حدوداً ۱۰۰ متر یا ۳۲۸ فوت را بدون افت سیگنال انتقال 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 ۱-۹: 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، ۱۰مگابیت در ثانیه، ۱۶مگابیت در ثانیه و ۱۰۰مگابیت در ثانیه.برای شبکه‌های کوچک و خانگی استفاده از کابل CAT3 توصیه می‌شود.



(a)

(b)

تصویر ۱-۱۰: کابل UTP نوع ۳(a) و نوع ۵(b)

- STP[3] : 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 اثرگذاری 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

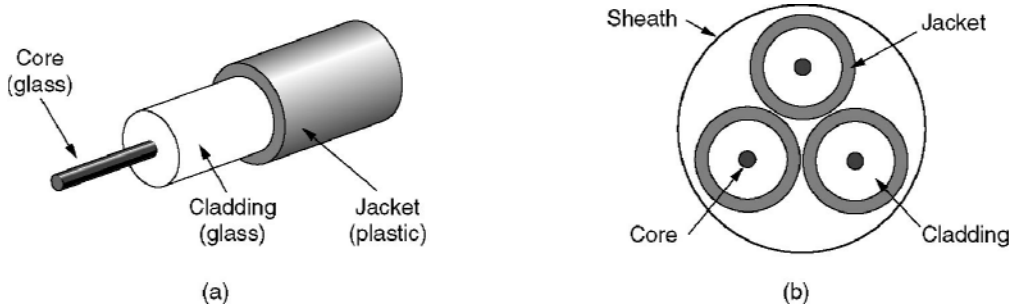
مـــذکور بـــدون افـــت ســـیگنال طـــی مـــی کنـــد برابـــر بـــا ۵۰۰ متـــر معـــادل ۱۶۴۰ فـــوت اســـت. در شبکه‌هایی با توپولوژی اتوبوسی و حلقه‌ای از دو نوع اخیر استفاده می‌شود. گفته شد که در این نوع کابـل، ۴ جفت سیم بهم تابیده بکار می‌رود که از دو جفت آن یکـی بـرای فرسـتادن اطلاعـات و دیگـری بـرای دریافـت اطلاعات عمل می‌کنند.

در شبکه‌هایی با نام اترنت سریع دو نوع کابل به چشم می‌خورد:

- 100 Base TX: یعنی شبکه‌ای که در آن از کابل UTP نوع CAT5 استفاده شده و عملاً دو زوج سـیم در انتقال دیتا دخالت دارند (دو زوج دیگر بیکار مـی‌ماننـد)، سـرعت در آن ۱۰۰ مگابیـت در ثانیـه و روش انتقال مبتنی بر باند است.
- 100 Base T4: تنها تفاوت آن با نوع بالا این است که هر چهار جفت سیم در آن بکار گرفته می‌شوند.

کابل فیبر نوری کاملاً متفاوت از نوع کواکسیال و زوج سیم بهم تابیده شده، عمل مـی‌کنـد. بـه جـای اینکـه سیگنال الکتریکی در داخل سیم انتقال یابد، پالسهایی از نور در میان پلاستیک یا شیشه انتقال می‌یابد. این کابل در برابر امواج الکترومغناطیس کاملاً مقاومت می‌کند و نیز تأثیر افت سیگنال بر اثر انتقال در مسافت زیاد را بـسیار کـم در آن می‌توان دید. برخی از انواع کابل فیبر نوری می‌توانند تا ۱۲۰ کیلومتر انتقال داده انجام دهند. همچنین امکـان به تله انداختن اطلاعات در کابل فیبر نوری بسیار کم است. کابل مذکور دو نوع را در بر می‌گیرد:

- حالت تنها[1]: که در این کابل دیتا با کمک لیزر انتقال می‌یابد و بصورت ۱۲۵/۸،۳ نشان داده می‌شـود کـه در آن ۸،۳ میکرون قطر فیبر نوری و ۱۲۵ میکرون مجموع قطر فیبر نوری و محافظ آن می‌باشد. این نوع که خاصـیت انعطاف‌پذیری کم و قیمت بالایی دارد برای شبکه‌های تلویزیونی و تلفنی استفاده می‌گردد.
- حالت چندگانه[2]: که در آن دیتا بصورت پالس نوری انتقال می‌یابد و بصورت ۱۲۵/۶۲،۵ نشان داده می‌شود کـه در آن ۶۲،۵ میکرون قطر فیبر نوری و ۱۲۵ میکرون مجموع قطر فیبر نوری و محـافظ آن مـی‌باشـد. ایـن نـوع مسافت کوتاهتری را نسبت به حالت تنها طی می‌کند و قابلیـت انعطـاف‌پـذیری بیـشتری دارد. قیمـت آن نیـز ارزان‌تر است و در شبکه‌های کامپیوتری استفاده می‌شود. بطورکلی کابل فیبر نوری نسبت به دو نوع کواکـسیال و زوج سیم بهم تابیده قیمت بالایی دارد و نیز نصب آن نیاز به افراد مـاهری دارد. شـبکه‌هـای 100 Base FX، شبکه‌هایی هستند که در آنها از فیبر نوری استفاده می‌شود، سرعت انتقال در آنها ۱۰۰ مگابیت در ثانیه بـوده و روش انتقال مبتنی بر باند می‌باشد. امروز، با پیشرفت تکنولوژی در شبکه‌های فیبر نـوری مـی‌تـوان بـه سـرعت ۱۰۰۰ مگابیت در ثانیه دست یافت. در شکل صفحه بعد یک کابل فیبر نوری مشاهده می‌شود.



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

بطور کلی توصیه‌هایی در مورد نصب کابل شبکه وجود دارد:

---

[1] - Single Mode

[2] - Multi Mode

- 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 کابل‌کشی نمایید، کابلها را بوسیله حفاظت‌کننده‌هایی بپوشانید.
- دو سر کابل را نشانه‌گذاری کنید.

کارت شبکه[1]:

کارت شبکه یا NIC ، که عموماً در شیارهای گسترش[2] کامپیوتر قرار می‌گیرد، وسیله‌ای است که بین کامپیوتر و شبکه‌ای که کامپیوتر جزئی از آن است، اتصال برقرار می‌نماید. هر کامپیوتر در شبکه می‌بایست یک کارت شبکه داشته باشد که به باس گسترش سیستم[3] اتصال می‌یابد و برای کابل شبکه به عنوان یک واسطه عمل می‌کند. در برخی کامپیوترها، کارت شبکه با مادربورد یکی شده است، اما در بیشتر مواقع شکل یک کارت گسترش را به خود می‌گیرد که یا به ISA[4] و یا به PCI[5] 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 لایهٔ 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 الکتریکی قابل انتقال بر روی کابل شبکه تبدیل می‌نماید. 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 متناسب 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.

---

[1] - Network Interface Adapter
[2] - Expansion Slot
[3] - Expansion Bus System's
[4] - Industry Standard Architecture
[5] - peripheral component interconnect

کارت شبکه قابل نقل و انتقال[1] :

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(VPN[2]):

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 می شود. منظور از یک شبکه خصوصی شبکه ای است که بطور آزاد در اختیار و دسترس عموم نیست. VPN به این دلیل مجازی نامیده می شود 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 می دهد. پیاده سازی VPN معمولا اتصال دو یا چند شبکه خصوصی از طریق یک تونل رمزشده انجام می شود. در واقع به این وسیله اطلاعات در حال تبادل بر روی شبکه عمومی از دید سایر کاربران محفوظ می ماند. VPN را می توان بسته به شیوه پیاده سازی و اهداف پیاده سازی آن به انواع مختلفی تقسیم کرد.

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

- VPN رمزشده : VPN های رمز شده از انواع مکانیزمهای رمزنگاری برای انتقال امن اطلاعات بر روی شبکه عمومی استفاده می کنند. یک نمونه خوب از این VPN ها ، شبکه های خصوصی مجازی اجرا شده به کمک IPSec هستند.
- VPN رمزنشده : این نوع از VPN برای اتصال دو یا چند شبکه خصوصی با هدف استفاده از منابع شبکه یکدیگر ایجاد می شود. اما امنیت اطلاعات در حال تبادل حائز اهمیت نیست یا این که این امنیت با روش دیگری غیر از رمزنگاری تامین می شود. 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 می شوند. (MPLS VPN) در این مواقع می توان در لایه های بالاتر از رمزنگاری مانند SSL استفاده کرد.

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

دسته بندی VPN 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 می شود در حجم ترافیک رمز شده تاثیر دارد. همچنین سطح شفافیت VPN برای کاربران آن نیز با توجه به لایه پیاده سازی مطرح می شود.

---

[1] - Portable Computer Network Adapters

[2] - Network Virtual Private

- VPN 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 پروتکلهایی مانند ATM یا Frame Relay به هم متصل کرد.با وجودی که این مکانیزم راه حل مناسبی به نظر می رسد اما معمولا روش ارزانی نیست چون نیاز به یک مسیر اختصاصی لایه ۲ دارد. پروتکلهای Frame Relay و ATM 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.
- VPN 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 مشروح خواهیم پرداخت.
- VPN 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 VPNها 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:

- VPN 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.
- VPN اکسترانتی : 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 معمولا برای سناریوهای B2B که در آن دو شرکت می خواهند به ارتباطات تجاری با یکدیگر بپردازند، استفاده می شود.

بخش ۲:
آدرس دهی

فصل ۲: آدرس دهی در شبکه های کامپیوتری
فصل ۳: مسیریابی در مسیریابها
فصل ۴: پروتکلهای مسیریابی در شبکه
فصل ۵: Multicasting و پروتکلهای مسیریابی Multicast

فصل ۲:

آدرس دهی در شبکه های کامپیوتری

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

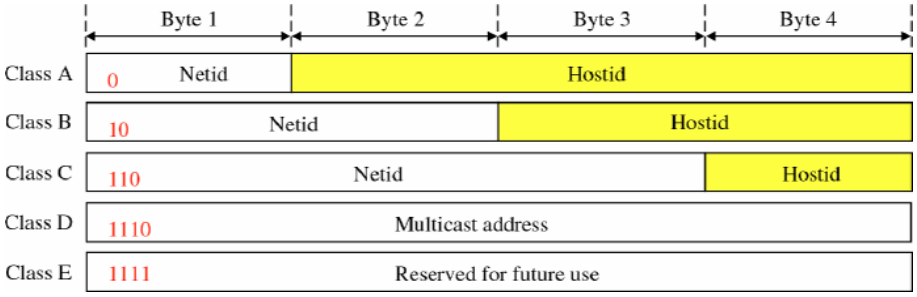
۱. آدرس فیزیکی (در لایه های فیزیکی و اتصال داده)

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 شبکه۲ 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 هستند . 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.
- HostIdتمام یک: آدرس Broadcast.
- 127.X.Y.Z : آدرس loop Back. 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.Nپیامی را ارسال بکند می تواند از آدرس 0.0.0.N جهت آدرس مقصد استفاده کند.

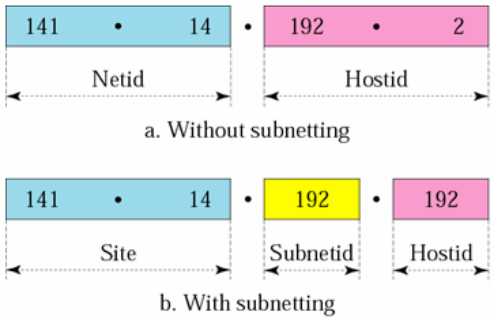
آدرس شبکه ،کلاس آدرس ، بلاک و دامنه آدرس در بلاک را مشخص می نماید. مثلاً 223.168.21.124 را در نظر بگیرید، بلاک آدرس شبکه آن 223.168.21.0 از کلاس C و دامنه آدرس آن 223.168.21.0 تا 223.168.21.225 می یابد.

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

Broadcast مستقیم آدرس: پیامی است که توسط یک مسیریاب برای تمام Hostهای عضو شبکه محلی ارسال می گردد.

Broadcast محدود آدرس: پیامی است که توسط یک Host داخل شبکه محلی برای سایر اعضای آن شبکه ارسال می گردد. این پیام فقط داخل همان شبکه است و مسیریابها در حین خروج از شبکه آن را بلاک می کنند.

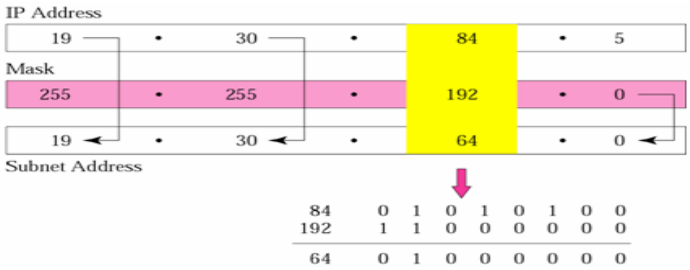
اگر بخواهیم از ساختار طبقاتی برای آدرس دهی در شبکه استفاده نمائیم باید از Subnet استفاده نمائیم:



روشهای پیدا کردن Subnet:

۱. صریح(Straight): آدرس IP را با آدرس Mask شبکه بیت به بیت AND می شود.

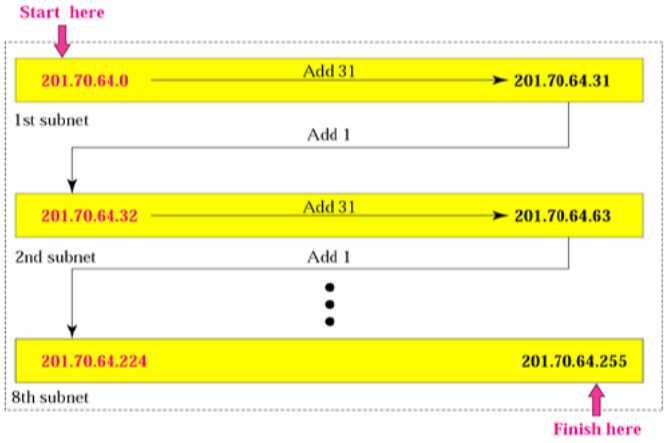
۲. میانبر(Shortcut): قسمتهایی از آدرس IP که مقدار معادل آن در Mask ۲۵۵ است را عیناً در Subnet کپی می کنیم. برای قسمتهایی از Mask که مقدار ۰ دارند، مقدار صفر را در Subnet را موقعیت معادل آن کپی می کنیم. برای سایر قسمتها، مقدار IP را با Mask ، بیت به بیت AND می کنیم. به مثال زیر توجه نمائید:



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 می باشد.

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 می گیریم. تعداد یکهای Mask پیش فرض ۲۴ می باشد. بنابراین تعداد یکهای Mask Subnet ۲۴+۳=۲۷ می باشد و تعداد صفرها ۳۲-۲۷=۵ می باشد.بنابراین ۸ Subnet هر کدام با $۲^{۵}$=۳۲ آدرس خواهیم داشت. Subnet Mask در این حالت برابر است با:

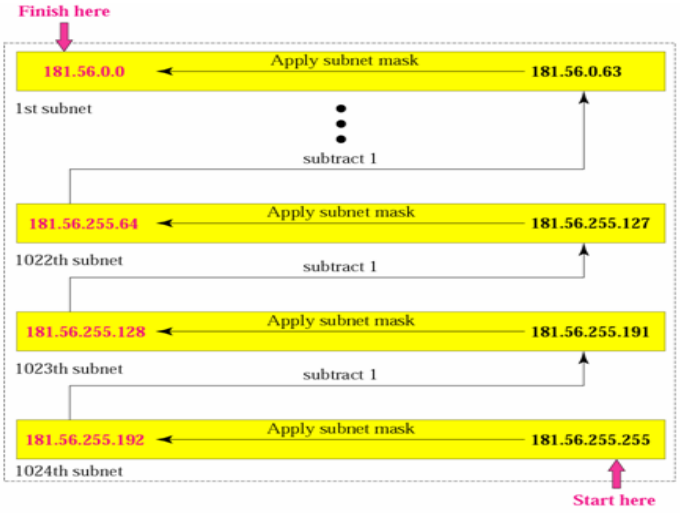
11111111 11111111 11111111 11100000 یا 255.255.255.224



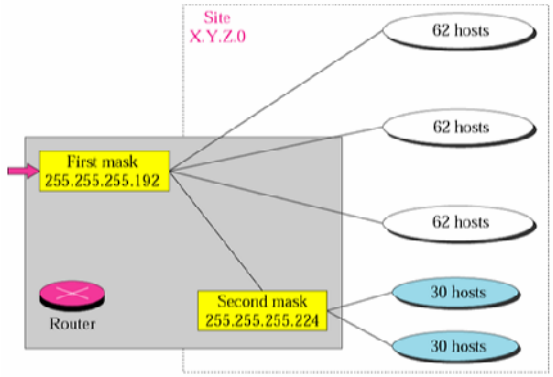
مثـال: یـک شـرکت فـضای آدرس 181.56.0.0(کـلاس B) را دارد. ایـن شـرکت نیازمنـد ۱۰۰۰ Subnet می باشد. این Subnet را طراحی کنید.

تعداد یکهای Mask پیش فرض ۱۶ می باشد. ۱۰۰۰ توانی از ۲ نیـست. اولـین عـدد تـوان ۲، ۱۰۲۴ اسـت. بنابراین نیازمند ۱۰ یک دیگر در Subnet Mask هستیم(۲۶=۱۰+۱۶). تعداد صفرها نیـز ۶=۲۶-۳۲ اسـت. بنـابراین Subnet Mask عبارتست از:11000000 11111111 11111111 11111111 یا 255.255.255.192.

تعداد Subnetها ۱۰۲۴ ، هر Subnet ۶۴=2^6 آدرس.



می توان Subnet هایی در Subnet های 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.قوانین حاکم بر Supernet عبارتند از:

- تعداد بلاکها باید توانی از ۲ باشد.
- فضای آدرس بلاکها باید پیوسته باشد.
- بایت سوم آدرس اول باید بر تعداد بلاکها، قابل تقسیم باشد.

مثال: یک شرکت نیازمنـد Supernet از ۱۶ آدرس کـلاس C مـی باشـد.Supernet Mask آن را مـشخص نمائید.

برای ۱۶ کلاس نیازمند ۴ بیت می باشیم.بنابراین Supernet Mask این فضا عبارتست از:

11111111 11111111 1111**0000** 00000000 یا 255.255.240

مثال: یک شـرکت نیازمنـد ۶۰۰ آدرس مـی باشـد. کـدامیک از فـضاهای بلاکهـای کـلاس C زیـر بـرای 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

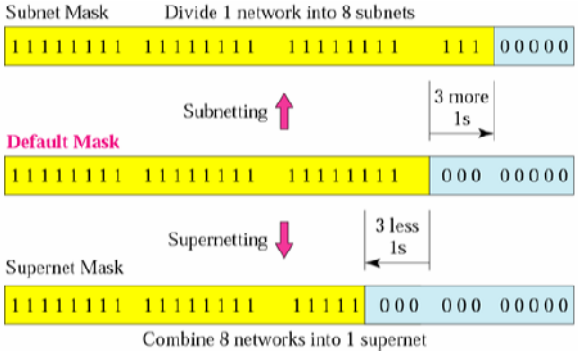
۱- نه. تنها سه بلاک وجود دارد.

۲- نه.فضای بلاکها پیوسته نیست.

۳- نه.۳۱ در بلاک اول قابل تقسیم نیست.

۴-بله. هر سه شرط قابل برآورد است.

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



مثال: آدرس ابتـدایی یـک Supernet ، 205.16.32.0 مـی باشـد و Supernet Mask ، 255.255.248.0 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

تنها آدرس اول به این Supernet مربوط می شود.

مثال: یک Supernet دارای یک آدرس شروع 205.16.32.0 و یـک 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 توجـه بـه اخـتلاف سه بیتـی ایـن دو مـی تـوان نتیجـه گرفـت کـه ۸ بـلاک در ایـن Supernet وجـود دارد. ایـن بلاکهـا عبارتنـد از 205.16.32.0 تـا 205.16.39.0 . آدرس ابتـدایی عبارتـست از 205.16.32.0 و آخـرین آدرس عبارتـست از 205.16.39.255 .

آدرس دهی بدون کلاس[1] :

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؛ یـک شـرکت کوچـک بـه ۱۶ آدرس و یـک شرکت بزرگ به ۱۰۲۴ آدرس. در هر صورت تعداد آدرسهای بـلاک بایـد تـوانی از ۲ باشـد(۸،۴،۲،...). آدرس شـروع بلاک باید بر تعداد آدرسها قابل تقسیم باشد.مثلاً اگر بلاک ۴ آدرسه داشته باشـیم، آدرس ابتـدایی بایـد بـر ۴ قابـل تقسیم باشد. برای بلاک با کمتر از ۲۵۶ آدرس، تنها باید سمت راست ترین بایت آدرس چک شود و برای بلاکـی بـا کمتر از ۶۵۵۳۶ آدرس ۲ بایت سمت راست چک می شود.

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

[1] - ClassLess

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 17.17.32.0 این شرایط را دارد.

نماد /[1]:

A.B.C.D/n یک نماد برای نشان دادن تعداد یکهای Mask یک آدرس می باشد. نماد / را نماد CIDR[2] نیز می نامند.

مثال: یک سازمان کوچک یک بلاک با آدرس شروع و طول پیشوندی 205.16.37.24/29(در نماد /) را دارد . دامنه بلاک را تعیین کنید.

آدرس ابتدایی 205.16.37.24است. 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 00011**000
Ending : **11001111 00010000 00100101 00011**111

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 --> 205.16.37.31

کلاسهای A،B وC 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 درصورتیکه یکی از آدرسهای شبکه بصورت 167.199.170.82/27 باشد، را تعیین نمائید.

طول پیشوند ۲۷ است که به معنی آنست که باید ۲۷ بیت 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 01010010 است که با صفر کردن ۵ بیت آخر آن 01000000 و یا 64 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. subnet ها و دامنه آدرس آنها را مشخص کنید.

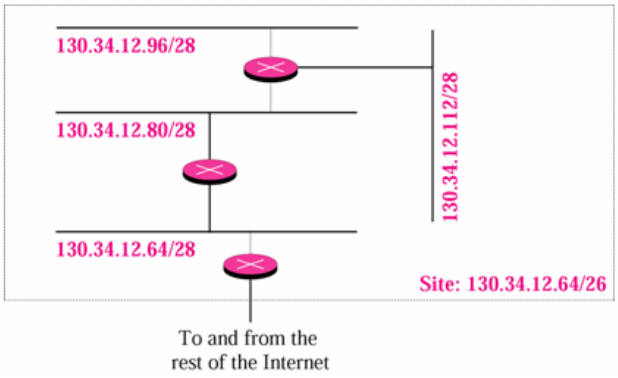
طول پسوند ۶ است. به عبارت دیگر هر بلاک ۶۴ آدرس ($۲^۶$) دارد.بنابراین اگر ۴ subnet بخواهیم هر کدام ۱۶ آدرس خواهند داشت. بنابراین طول پیشوند در این حالت 28=2+26 می باشد.

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.

---

[1] - Slash notation
[2] - Classless Inter Domain Routing

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 فـضای آدرس را بین سه گروه زیر توزیع کند:

گروه اول ۶۴ مشتری هرکدام 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 چنـد آدرس بـدون استفاده باقیمانده است.

گروه ۱: در این گروه هر مشتری نیازمند ۲۵۶ آدرس است. ایـن بـه معنـی طـول ۸ ($۲^۸$=۲۵۶)بـرای پـسوند اسـت. بنابراین طول پیشوند برابر است با ۳۲-۸=۲۴

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 × 256 = 16,384

گروه دوم: در این گروه هر مشتری نیازمند ۱۲۸ آدرس است. این به معنـی طـول ۷ ($۲^۷$=۱۲۸)بـرای پـسوند اسـت. بنابراین طول پیشوند برابر است با ۳۲-۷=۲۵.

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 × 256 = 16,384

گروه سوم: در این گروه هر مشتری نیازمند ۶۴ آدرس است. این به معنی طول ۶ ($۲^۶$=۶۴)برای پسوند است. بنابراین طول پیشوند برابر است با ۳۲-۶=۲۶.

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 × 64 = 8,192

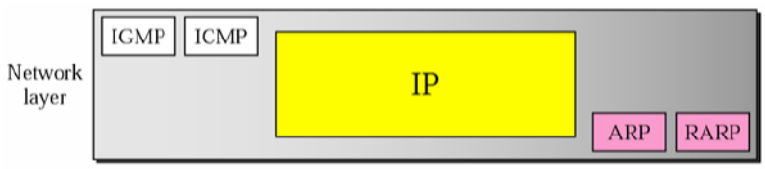
بنابراین مجموع آدرسهای موجود: ۶۵۵۳۵

مجموع آدرسهای تخصیصی: ۴۰۹۶۰

مجموع آدرسهای بدون استفاده:۲۴۵۷۶

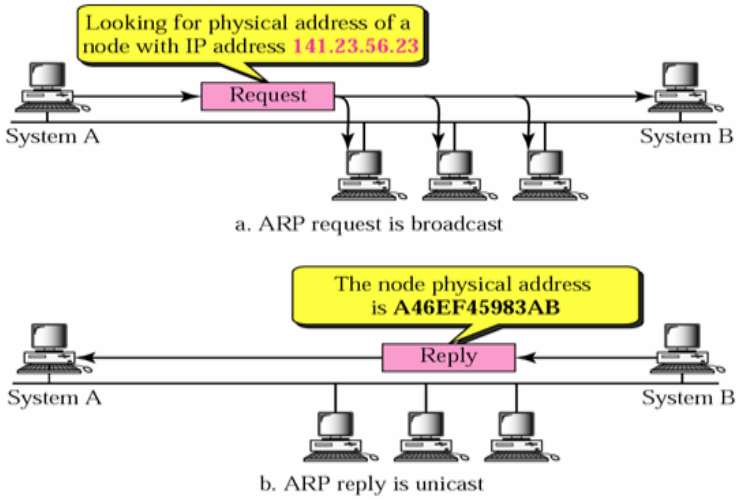
یافتن آدرس در شبکه:

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

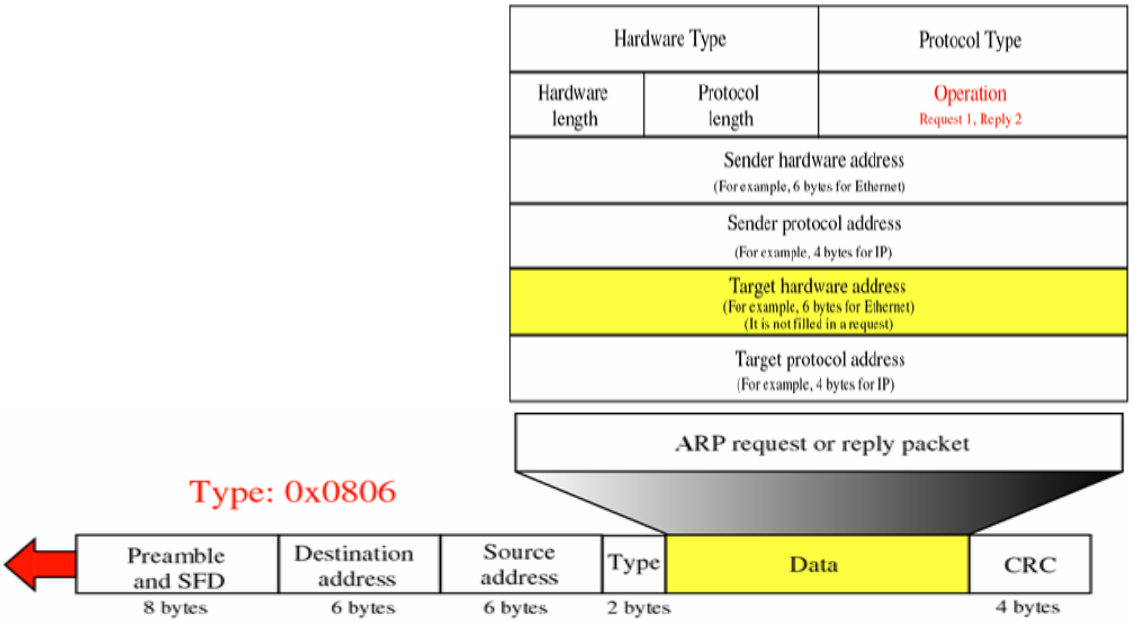


ARP[1] :

پروتکلی است که آدرس فیزیکی (آدرس کارت شبکه) را بر می گرداند . وقتی بستـــه به مـسیریابی رسـید که بـــاید این مسیریاب بسته را بر روی LAN بگذارد (برای یک کـــــامپیوتر مشخص) ، این مسیریاب بایـد آدرس فیزیکی (۴۸ بیتی) را داشته باشد . (زیرا در شبکه LAN آدرس IP معنی ندارد و باید آدرس بسته MAC اسـتفاده شود) در غیر این صورت بسته نمـــــی تواند در LAN حرکت کند . پروتکلی که آدرس فیزیکـی را بدست می آورد ARP است .



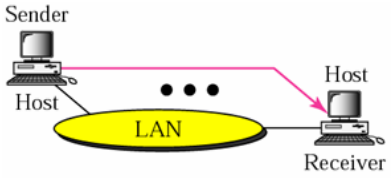
ARP فرمت خاص خود را دارد و با یکی از بسته های خود آدرس IP مقصد را قرار داده و بـسته را بـه LAN می فرستد . اندازه بسته ARP و RARP، ۲۸ بایت می باشد.



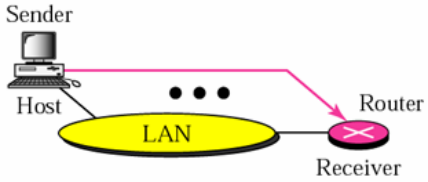
ARP به چهار شکل مورد استفاده قرار می گیرد:

[1] - Address resolution protocol

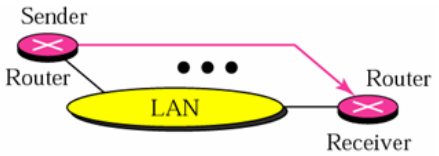
۱. تبادل بسته بین دو میزبان در یک شبکه. آدرس IP مقصد همان آدرس مقصد در بسته داده می باشد.



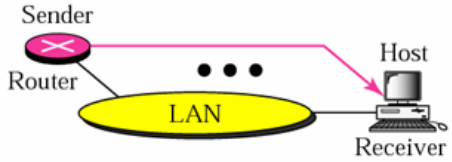
۲. یک میزبان می خواهد بسته ای را به میزبانی در شبکه دیگر بفرستد. بنابراین باید ابتدا بسته به مسیریاب شبکه تحویل داده شود. آدرس IP مقصد آدرس مسیریاب می باشد.



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

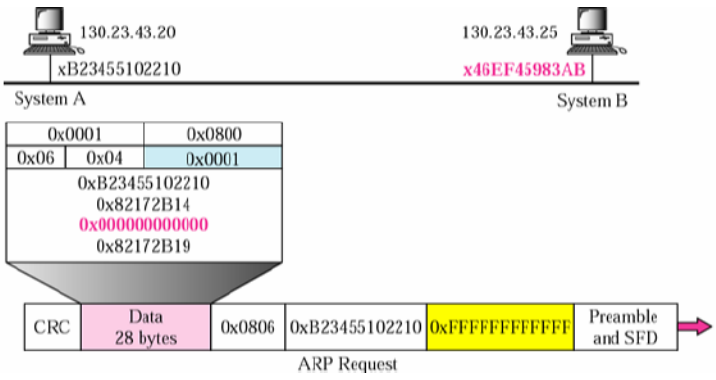


۴. مسیریاب بسته ای را دریافت کرده که باید به میزبانی در شبکه خودش تحویل داده شود. آدرس IP مقصد همان آدرس مقصد در بسته داده می باشد.

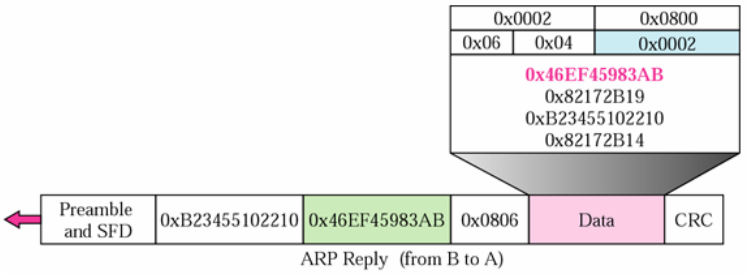


پیام ARP بصورت Broadcast ارسال می گردد، درحالیکه پاسخ آن بصورت Unicast می باشد.میزبانهای مقصد به آدرس IP بسته ARP نگاه می کنند . اگر آدرس موجود در بسته با آدرس IP خود یکی باشد ، به بسته جواب می دهند یعنی آدرس فیزیکی خود را در بسته ARP قرار می دهند و ارسال می کنند . حال مسیریاب مقصد با دانستن آدرس فیزیکی 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) .

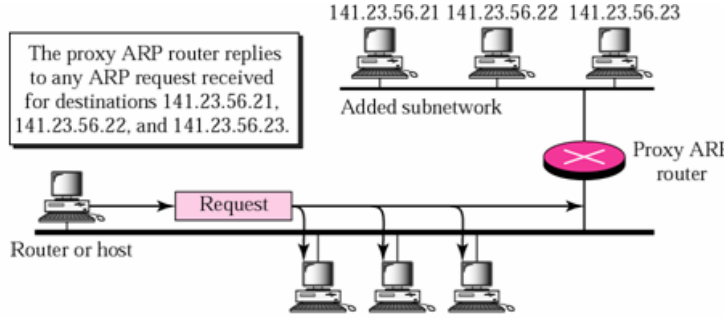
مثال: سیستم A از طریق یک پیام ARP درخواست خود را برای کسب آدرس فیزیکی سیستم B درشبکه منتشر می کند. فیلد Operation یک است (درخواست) و آدرس فیزیکی ماشین مقصد تمام یک است(آدرس Broadcast).



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.

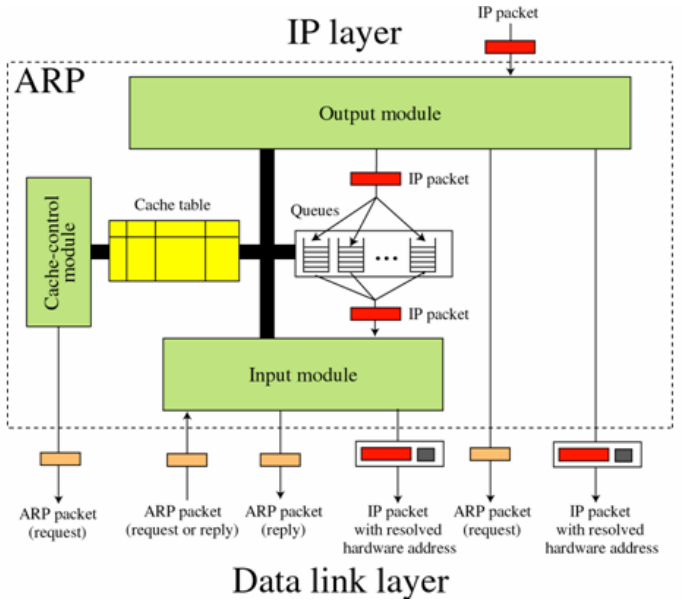


مسیریاب Proxy ARP مسیریابی در شبکه است که به پیامهای ARP بخشهای مختلف شبکه در خصوص آدرسهای فیزیکی میزبانهای واقع در سایر بخشهای شبکه پاسخ می دهد. حسن این روش جلوگیری از انتشار بیهوده پیام ARP در کل شبکه و درنتیجه کاهش بار ترافیکی شبکه و همچنین افزایش سرعت پاسخ گویی به درخواستها می باشد. دلیل افزایش سرعت 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 طولانیی 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 بشکل زیر می باشد:



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

State	Queue	Attempt	Time-out	Protocol Addr.	Hardware Addr.
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 می ماند.

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.

State	Queue	Attempt	Time-out	Protocol Addr.	Hardware Addr.
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 R(Resolved) تغییر داده و مقدار ۹۰۰ را به فیلد Time-out تخصیص می دهد و آدرس فیزیکی هدف (E34573242ACA) را نیز به مدخل می افزاید. در ادامه ماژول به صف ۱۸ رفته و بسته هایی موجود در آن را یکی یکی به لایه پیوند داده ارسال می کند.

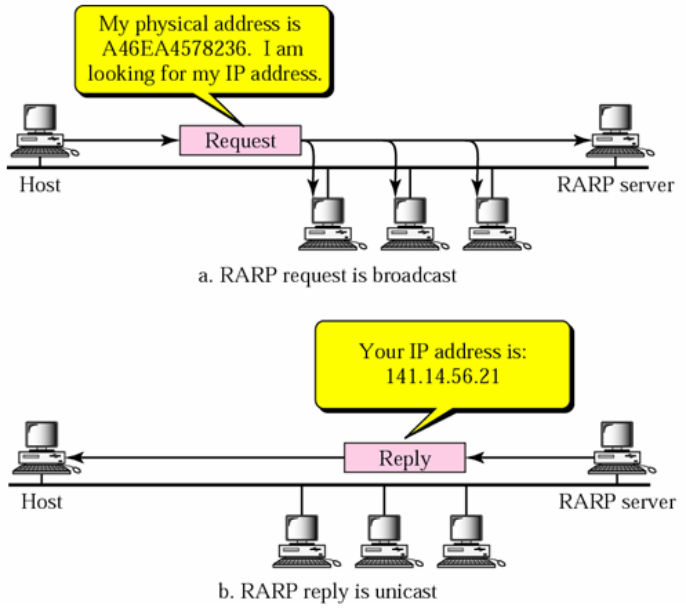
State	Queue	Attempt	Time-out	Protocol Addr.	Hardware Addr.
R	5		900	180.3.6.1	ACAE32457342
P	2	2		129.34.4.8	
P	14	5		201.11.56.7	
R	8		450	114.5.7.89	457342ACAE32
P	12	1		220.55.5.7	
P	23	1		116.1.7.22	
R	9		60	19.1.7.82	4573E3242ACA
R	18		900	188.11.8.71	E34573242ACA

۲۵ ثانیه بعد، ماژول کنترل کش(Cache)، مدخلهای جدول را بروز مـی کنـد. مقـدار Time-out بـرای سـه مدخل Resolved شده ابتدایی به اندازه ۶۰ کاهش می یابد و برای مدخل انتهایی Resolved به انـدازه ۲۵ کـاهش می یابد. حالت مدخل ماقبل آخر بدلیل صفر شدن Time-out آن ، به F(Free) تغییر می کند. برای سه مـدخل بـا حالت P، مقدار فیلد Attempt یکی افزایش می یابد. پس از این افزایش یک واحدی، انـدازه فیلـد Attempt بـرای پروتکل آدرس IP 201.11.56.7 از حد مجاز بیشتر شده و بنابراین حالت مدخل این آدرس نیز به F تغییر می یابـد و صف آن حذف می گردد.

State	Queue	Attempt	Time-out	Protocol Addr.	Hardware Addr.
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

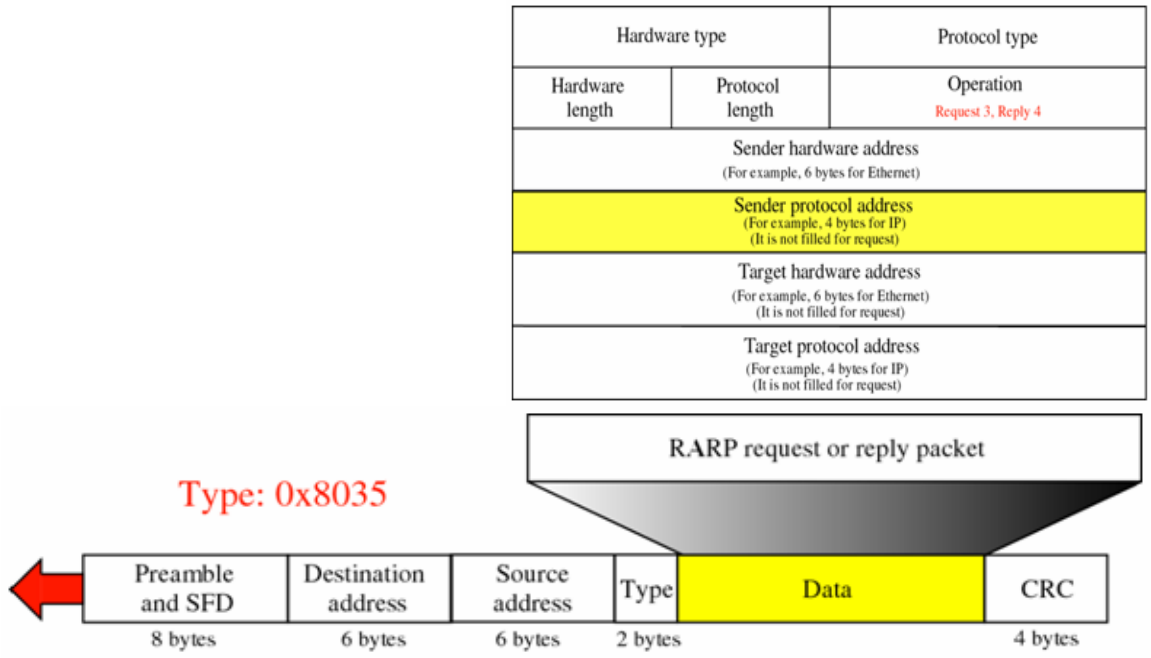
RARP[1] :

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



فرمت بسته های PARP بصورت زیر است:

[1] - Reverse address resolution protcol



مقدار فیلد operation برای این بسته ها ۳ برای درخواست و ۴ برای پاسخ است. همانند ARP، بسته های درخواست RARP،Broadcast شده و پاسخ آن Unicast می گردد.

در کامپیوترهای بدون دیسک متصل به شبکه، PARP نمی تواند اطلاعاتی همچون اطلاعاتی همچون Subnet Mask، آدرس IP مسیریاب و آدرس IP سرور را فراهم کند. برای همین از پروتکل های BootP و DHCL استفاده می شود.

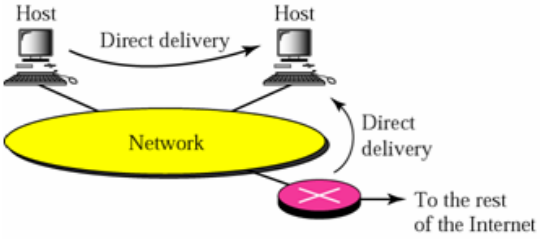
فصل ۳:

مسیریابی در مسیریابها

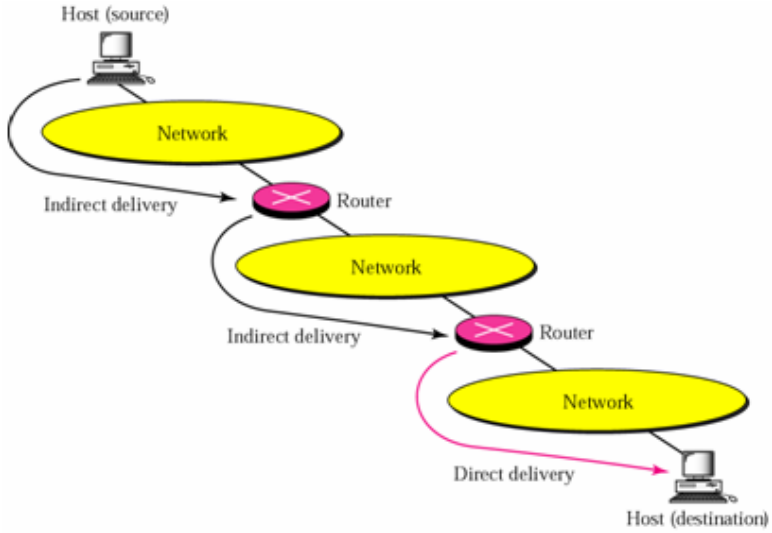
در ارتباطات مبتنی بر اتصال[1]، پروتکل لایه شبکه ابتدا یک اتصال را برقرار مـی کنـد در حالیکـه در ارتبـاط بدون اتصال[2] ، پروتکل لایه شبکه برای هر بسته بصورت جداگانه عمل کرده و عملیات انجام گرفته بـرای هـر بـسته ارتباطی با سایر بسته ندارد.

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:

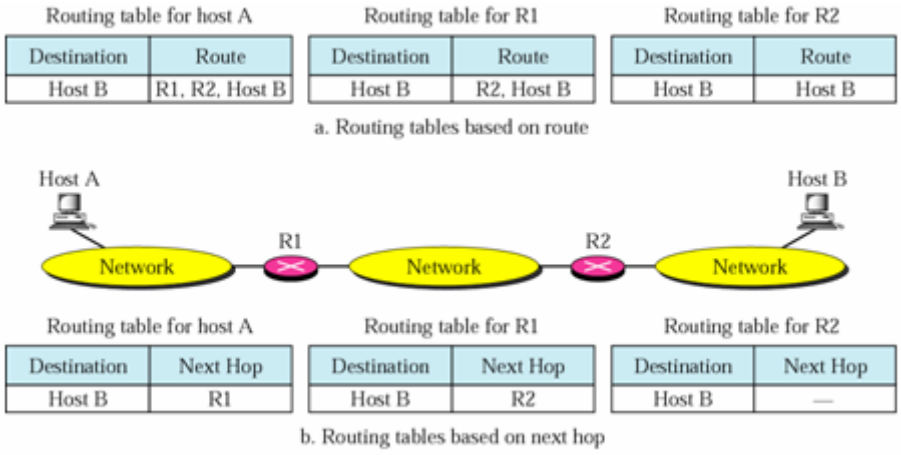
۱- مسیریابی پرش بعدی(Next-hop Routing)

- 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.

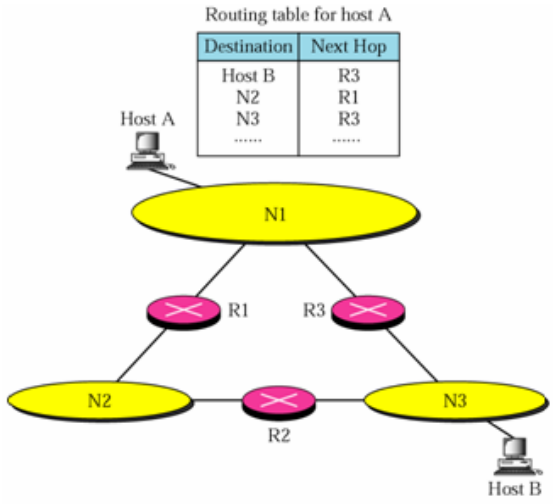
---

[1] - Connection Oriented

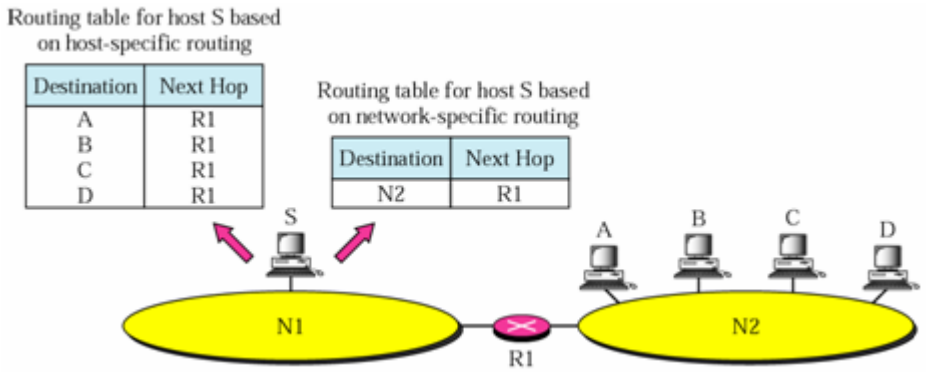
[2] - Connectionless



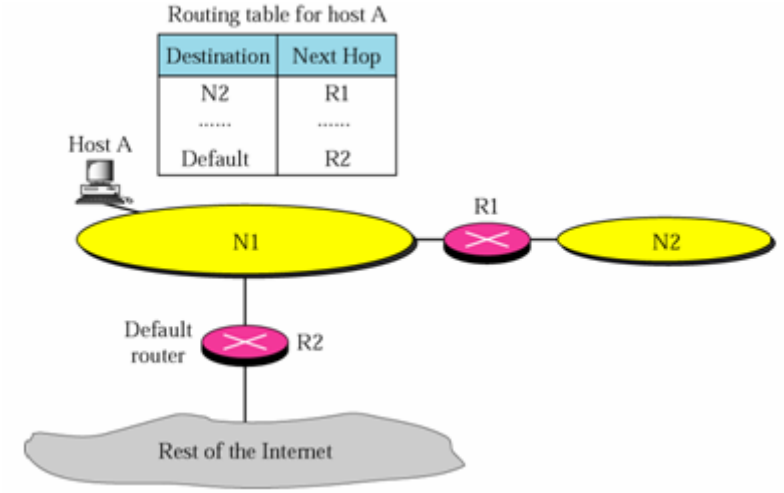
۲- مسیریابی شبکه مشخص(Network-specific Routing) : تعیین آدرس پرش بعدی براساس شبکه های مقصد.



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



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

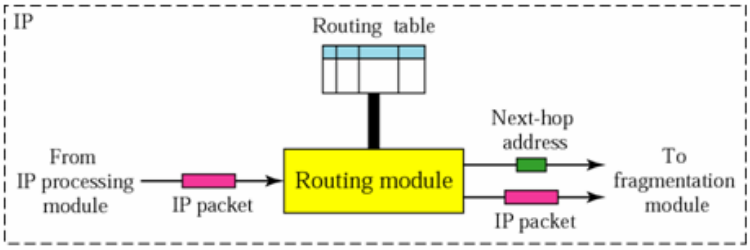


جداول مسیریابی به دو صورت هستند:

۱- جداول ایستا: اطلاعات این جداول بصورت دستی وارد می شود.

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

اطلاعات جدول مسیریابی از طریق ماژول 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: افزوده شده بوسیله تعیین مسیر مجدد.
- M: تصحیح شده بوسیله تعیین مسیر مجدد.

ترتیب قرارگرفتن سطرهای جدول مسیریابی بصورت زیر است:

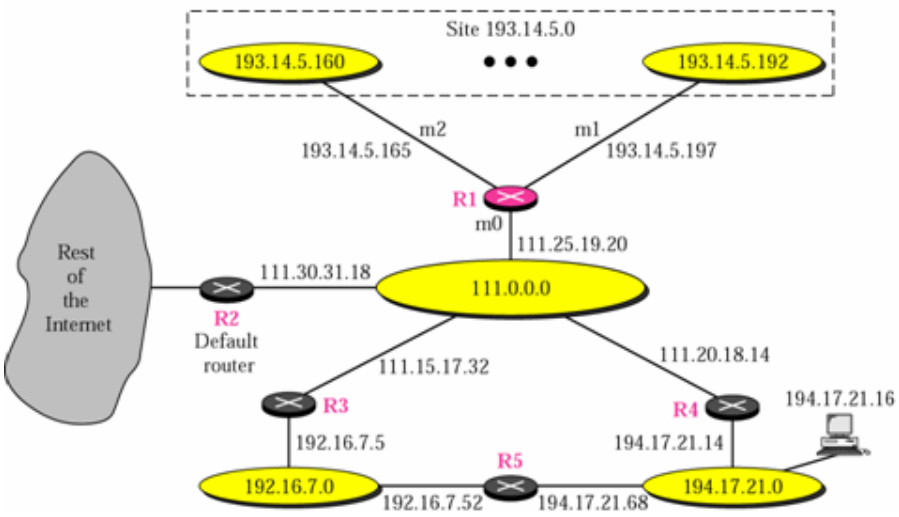
۱- آدرس تحویل مستقیم

۲- 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 قبلی 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

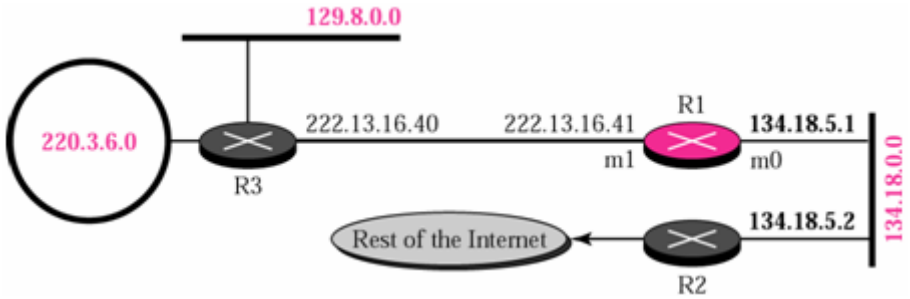
200.34.12.34 & 255.255.255.0 ➔ 200.34.12.0 no match

200.34.12.34 & 255.255.255.0 ➔ 200.34.12.0 no match

Default

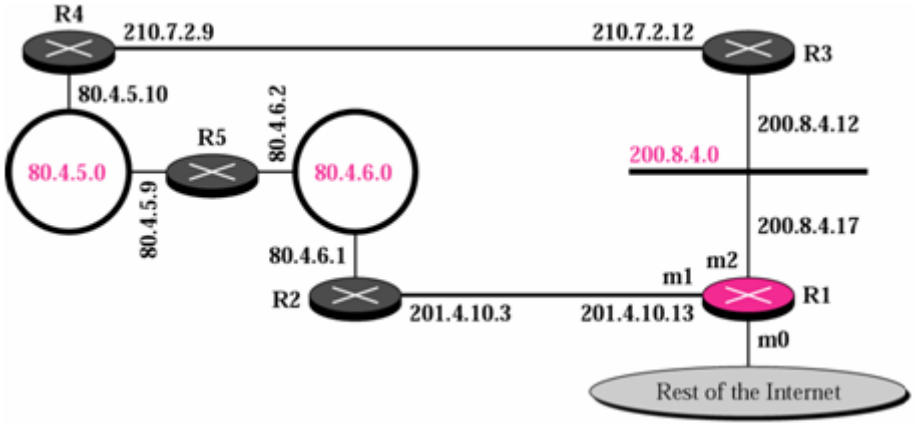
200.34.12.34 & 0.0.0.0 ➔ 0.0.0.0. **match**

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

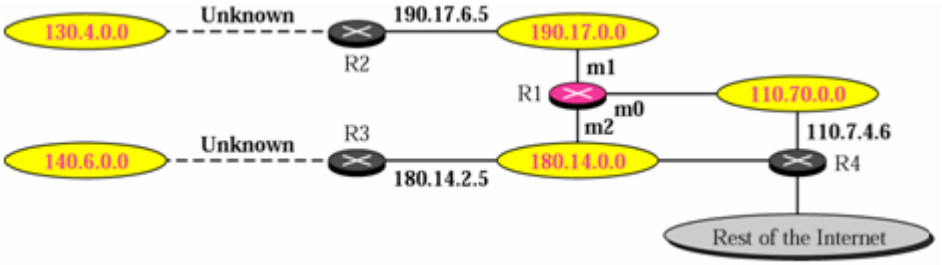
مثال: جدول مسیریابی مسیریاب R1 را رسم کنید.



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. توپولوژی شبکه آن را رسم نمائید.

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 تامل می باشند:

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

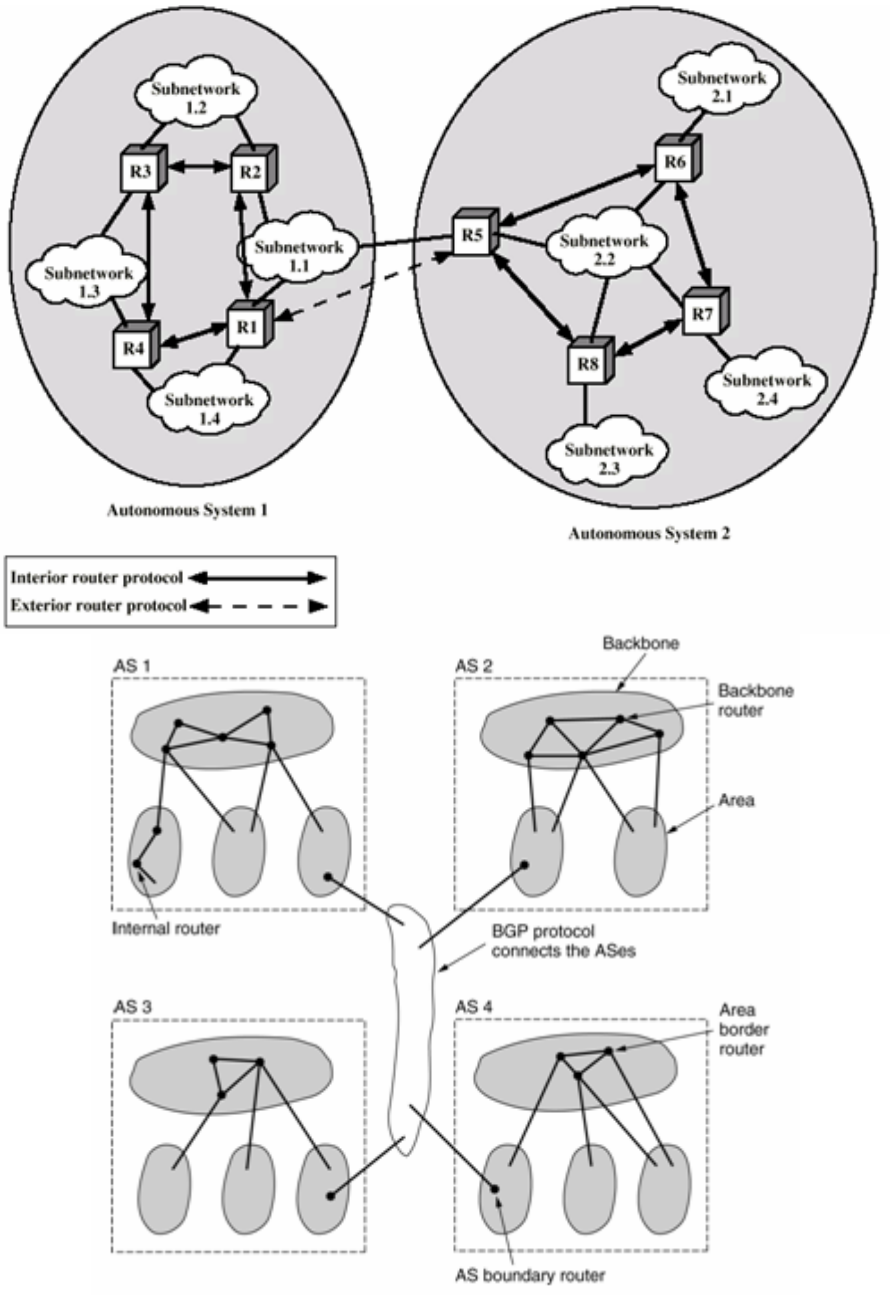
در آدرس دهی کلاسی، هر آدرس خودش حاوی اطلاعاتی است که جستجو در جدول مسیریابی را آسان می کند؛ اما در مورد آدرس دهی بدون کلاس اینگونه نیست.

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 (as) (سیستم) می گویند (Autonomous system) .سپس این AS ها به هم وصل می شوند و شبکه اینترنت را بوجود می آورند .بنابراین دو نوع مسیریابی داریم : مسیریابی داخلی AS و مسیریابی بین AS .

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



The relation between ASes, backbones, and areas in OSPF

در واقع شبکه های WAN به صورت Store & Forward کار می کنند. یعنی بسته از مدا به سوئیچ منتقل می شود . بسته در Switch ذخیره می شود،Switch آدرس ها را استخراج می کندو سپس اگر خط خروجی اشغال نباشد (آزاد باشد) ، بسته را Forward می کند.

Next Hop Forwareding: هر سوئیچ فقط موظف است سوئیچ بعدی که بسته را می تواند دریافت کند، مشخص کند؛ یعنی مهم نیست که بسته چه زمانی به مقصد می رسد.

استقلال از مبدأ : در تصمیم گیریRouting 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 :
  تعدادNode های میانی(بایدMIN باشد)، هزینه ، تأخیر ، گذردهی.
- زمان تصمیم گیری:
  ۱.هر بسته (درDataGRAM)
  ۲.هر ارتباط(در Virtual Circuit)
- محل تصمیم گیری (مسئول پیدا کردن مسیر) :
  ۱.هرNode
  ۲.Node مرکزی
  ۳.Node آغاز کننده(Source Routing)
- منبع جمع آوری اطلاعات :
  ۱.هیچ(استاتیک)
  ۲.در مسیریابی DYNAMIC باید برای یافتن مسیر اطلاعاتی جمع آوری شود.
  ۳.محلی (مسیریابی LOCAL است نه GLOBAL)
  ۴. Node های مسیر
  ۵.کل Node ها
  ۶.Node های همسایه
- زمان بهنگام سازی(زمان چک کردن هزینه تعویض مسیر)
  ۱.پیوسته
  ۲.پریودیک
  ۳.تغییربار زیاد
  ۴.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 مبداء و مقصد در شبکه، پیکربندی می شود. مسیرها ثابت هستند و یا حداکثر تنها با تغییر ساختار شبکه، تغییر می یابند. بنابراین هزینه اتصال مورد استفاده در مسیریابهای هوشمند[1]، 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

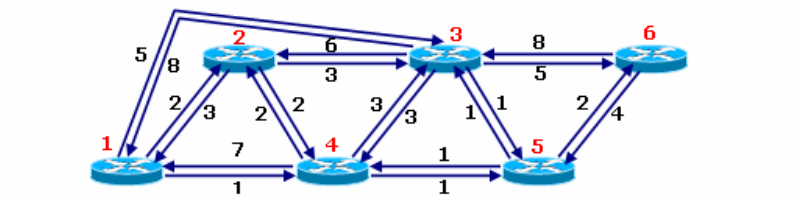
ممکن است در یک مرکز کنترل شبکه قرار گرفته باشد. ماتریس برای هر زوج مبداء و مقصد، گره بعدی را مشخص می نماید.

توجه داشته باشید که لازم نیست که مسیر کامل برای هر زوج از گره های ممکن، ذخیره گردد. بعلاوه اینکه، 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 آغاز می شود. تنها برقراری تماس با باقیمانده مسیر R_1 که بخشی از مسیر A به Y است، لازم است. R_2 به عنوان کم هزینه ترین مسیر از A به Y تعریف می گردد. اکنون اگر هزینه R_1 بیشتر از هزینه R_2 بود، مسیر X-Y می تواند با استفاده از مسیر R_2 بهبود یابد. اگر هزینه R_1 از R_2 کمتر بود، R_2، کم هزینه ترین 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 ۱ به گره ۶ با استفاده از گره ۴، آغاز می گردد. دوباره با محاسبه در ماتریس، مسیر گره ۴ به گره ۶ از گره ۵ می گذرد. سرانجام، مسیر از گره ۵ به گره ۶، یک اتصال مستقیم به گره ۶ است. بنابراین مسیر کامل از گره ۱ به گره ۶، ۶-۵-۴-۱ می باشد.

با این ماتریس سراسری، جداول مسیریابی می توانند در هر گره توسعه داده شده و در هر گره ذخیره گردند. با توجه به استدلال پاراگرف 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 می کند.

با مسیریابی ثابت، تفاوتی بین مسیریابی برای داده گرام و مدارات مجازی وجود ندارد. همه بسته ها از یک مبداء داده شده به یک مقصد داده شده، از یک مسیر یکسان جریان می یابند. مزیت مسیریابی ثابت، سادگی و کارکرد خوب آن در شبکه های مطمئن با بارگذاری پایدار، می باشد. ضعف این روش فقدان انعطاف پذیری می باشد. 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 گره های خارج از دسترس، یک گره بعدی ثانویه برای هر مقصد را فراهم می نماید. برای مثال گره های بعدی ثانویه در دایرکتوری گره ۱ ممکن است ۳،۳،۲،۳،۴ باشد.



از نود

به نود	1	2	3	4	5	6
1	-	1	5	2	4	5
2	2	-	5	2	4	5
3	4	3	-	5	3	5
4	4	4	5	-	4	5
5	4	4	5	5	-	5
6	4	4	5	5	6	-

جدول نود ۱

مقصد	نود بعدی
2	2
3	4
4	4
5	4
6	4

جدول نود ۲

مقصد	نود بعدی
1	1
3	3
4	4
5	4
6	4

جدول نود ۳

مقصد	نود بعدی
1	5
2	5
4	5
5	5
6	5

جدول نود ۴

مقصد	نود بعدی
1	2
2	2
3	5
5	5
6	5

جدول نود ۵

مقصد	نود بعدی
1	4
2	4
3	3
4	4
6	6

جدول نود ۶

مقصد	نود بعدی
1	5
2	5
3	5
4	5
5	5

مسیریابی ثابت

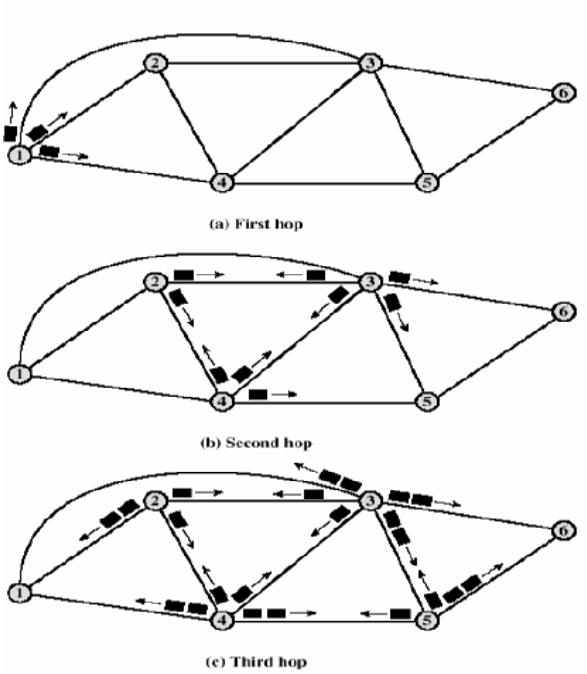
مسیریابی سیل آسا:

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 ۳و ۴ ارسال می کند. گره ۴ نیز کپی هایی 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 رسند. این بسته ها باید شناسه یکتایی 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 مقدارحداکثرممکن 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. دراولین 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 رسند، بدلیل رسیدن به مقصد، دوباره ارسال نخواهند شد.اگرچه ۲۲ کپی جدیداً ایجادشده، 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.
- بدلیل آزمایش تمام مسیریابها، حداقل یک کپی از بسته به مقصد می رسد که می تواند بعنوان 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 می تواند جهت ارسال پیام های اضطراری مورد استفاده قرار بگیرد. یک مثال از این قبیل کاربردها در یک شبکه نظامی می باشد که هدف مهمی برای تخریب گسترده، می باشد. بدلیل خاصیت دوم، روش سیل آسا ممکن است جهت برپاسازی اولیه یک مدار مجازی، بکار رود. خاصیت سوم بیان می کند که روش سیل آسا می تواند برای انتشار داده های مهم به همه گره ها، مفید باشد. همچنین چنین طرح هایی جهت انتشار اطلاعات مسیریابی نیز بکار می رود. ضعف این روش، بار ترافیکی بالایست که تولید می شود 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 می گیرد.

مسیریابی اتفاقی:

مسیریاب اتفاقی یک روش سیل آسای ساده و قوی، با دوری جستن تا حد ممکن از بار ترافیکی، می باشد. با مسیریابی اتفاقی، یک گره تنها یکی از مسیرهای خروجی خود را برای ارسال دوباره یک بسته دریافتی، انتخاب می کند. اتصال خروجی بصورت اتفاقی انتخاب می شود ، به استثنای اتصالی که بسته از آن رسیده است. اگر همه اتصالات بصورت یکسان و مشابه انتخاب شوند، یک گره می تواند اتصالات خروجی را به شیوه Round Robin ، مورد بهره برداری قرار می دهد.

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

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

P_i: احتمال انتخاب اتصال i

R_i: نرخ انتقال داده در اتصال i

جمع بر روی همه اتصالات خروجی نامزد، انجام می گیرد. این طرح باید توزیع ترافیکی خوبی را فراهم آورد. توجه کنید که احتمال می تواند برپایه هزینه های 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 بیشترکه مبادله می شود و فرکانسهای 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 برروی 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 بکندی این کار انجام بدهد.

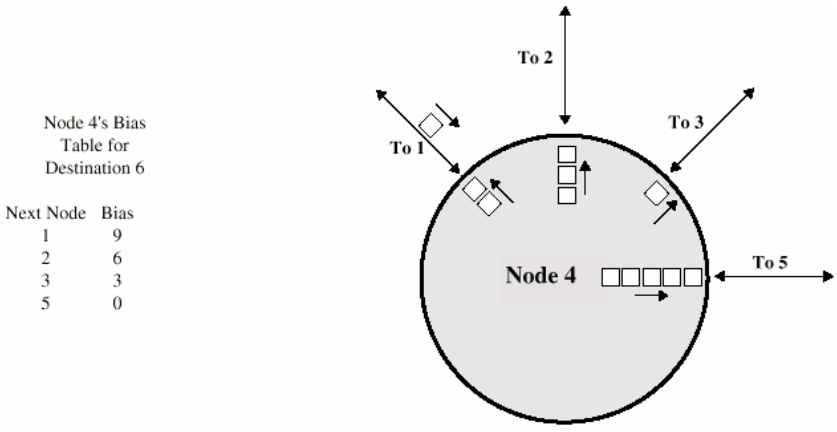
با وجود این مخاطرات جدی، مسیریابیهای تطبیقی به دو دلیل بسیار شایع می باشند:

- 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 بیاندازد.

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 متداول جهت طبقه بندی استراتژیهای مسیریابی تطبیقی، مبتنی بر اطلاعات مبداء 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 باشند. 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] (B_i) برای هر مقصد I داشته باشد. برای هر بسته ورودی رسیده برای گره i، 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.



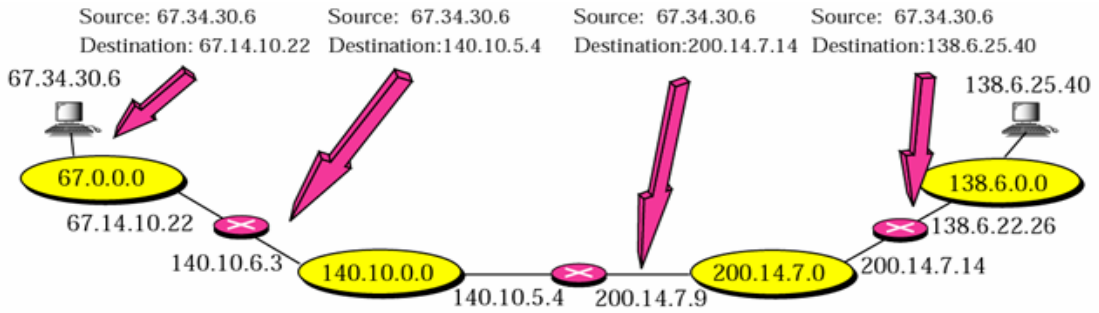
نمونه ای از مسیردهی تطبیقی مجزا

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 انباشت 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. برپایه طول کنونی صفها و مقادیر تمایل B_6 برای اتصالات خروجی، حداقل مقدار $Q+B_6$، ۴ 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 برپایه اطلاعات محلی هستند، به ندرت مورد استفاده قرار می گیرند؛ زیرا آنها اطلاعات موجود را بخوبی بکار نمی برند. 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 برند. اینچنین استراتژیهای تطبیقیی می تواند بصورت توزیع شده و یا متمرکز باشد. در حالت توزیع شده، هر گره اطلاعات تاخیر را با سایر گره ها معاوضه می نماید. برپایه اطلاعات ورودی، یک گره سعی در برآورد بازده شبکه کرده و الگوریتم مسیریابی کمترین هزینه را اعمال می نماید. در حالت متمرکز، هر گره وضعیت تاخیر انتشارش را به یک گره مرکزی ، گزارش می دهد. این گره مسیرها را برپایه این اطلاعات ورودی، طراحی نموده و اطلاعات مسیریابی را به گره ها، باز می گرداند.

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

[1] Bias -

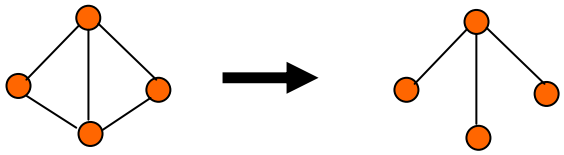


Source Routing

Bridge در لایه ۲ استفاده می شود. برای هنگامی مفید است که بخواهیم دو یاچند LAN را بـه هـم متـصل کنیم ولی برای WAN مناسب نیست در صورتی که مسیریاب در لایه ۳ است. مـسیریابی در پلهـا بـه شـکلهای زیـر می باشد:

- Source Routing
- Transparent Bridge

در transparent Bridge از پروتکل BPDU استفاده مـی شـود. در ایـن روش از spanning tree اسـتفاده می شود. در این روش بین مقصد و مبدأ یک مسیر وجود دارد بنابراین یـک بـسته از مقـصد بـه مبـدأ مـی رسـد . پروتکلBPDU (رد و بدل اطلاعات) در پلها، ریشه و سـایر گـره هـا وجـود دارد، پـس از رد و بـدل شـدن اطلاعـات، مسیریابی مربوط مشخص می شود، یعنی مسیرهای را که جز درخت نیست، پیدا می کند،


Spanning Tree

FLOW BASED Routing :

یک سری ROUTERو Node به هم متصل شده اند و یک توپولوژی را ایجاد کرده اند . به هر مسیر یـک هزینه افزوده می شود که معمولا طول صف یا تاخیر است سپس یک الگوریتم کوتـاهترین مـسیر اعمـال مـی شـود (مانند دیکسترا) و مسیر مینیم هزینه را بین مبدا و مقصد پیدا می کند،

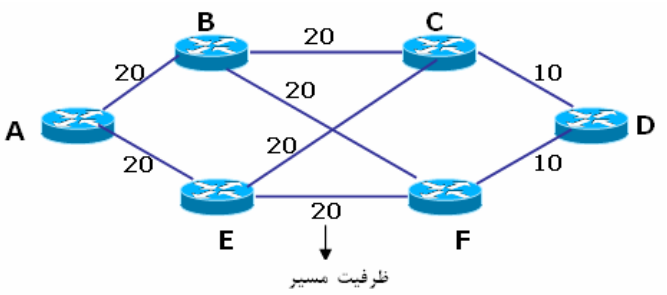
برای هزینه علاوه بر تاخیر، بار(Load) را هم باید در نظر گرفت. روش flow based routing، روشـی اسـت که علاوه بر تاخیر، بار را هم در نظر می گیرد.

FLOWدر شبکه کامپیوتری دومعنی دارد .یکی بار، یعنی میزان انتقال اطلاعات است (که هـدف مـا همـین 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 بـرای FLOW (دسته مشترک) مسیریابی انجام می شود . (برای اینکار از TCAM در مسیریاب ها استفاده می شود)

۱.توپولوژی شبکه (مسیریاب ها چگونه به هم متصل شده اند)

۲.ماتریس ترافیک

۳.ماترس ظرفیت که ظرفیت هر مسیر را بر حسب Xbps مشخص می کند .



ماتریس ترافیک (ترافیک برحسب بسته بـر ثانیـه). یعنی در یک مقطع زمانی وضعیت مـسیرها اینگونـه بوده است.

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 ظرفیت

i	خط	λ_i	C_i(kbps)	μC(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 بـسته وجـود دارد (9+4+1) که λ_i را در جدول فوق نشان مـی دهـد . در مـدل سـازی شـبکه از مـدل توزیـع پواسـن استفاده می شود .

T : زمان سرویس + زمان انتظار(زمان ورود بسته به خروج). $T = 1/(\mu * C - \lambda)$

μ : نرخ سرویس(نرخ خروج)

۱/μ =۸۰۰: 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)

بـرای محاسـبه وزن هـر مـسیر T آن را بـر مجمـوع T_i تقـسیم مـی کنـیم.مـثلاً بـرای AB داریم $W_{AB} = T_1/(T_1 + T_2 + ...) = 0.171$.

نکته ای که باید در نظر گرفت آنست که در محل فوق فرض کردیم که تاخیر بسیار ناچیز اسـت و بـسته هـا (بیت ها) پشت سر هم می آیند که توانستیم بگوییم 1/bps=اندازه.

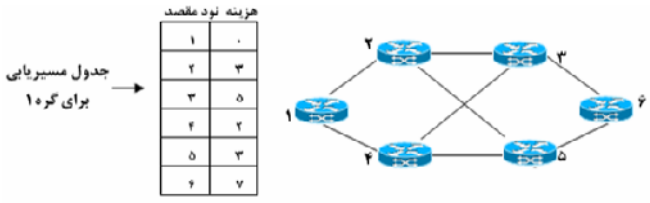
الگوریتم های مسیریابی در اینترنت :

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

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

در روش Distance Vector هر یک ازROUTER ها یک بردار تاخیر دارند که تاخیر MIN به هر Node را دارد البته Node بعدی را هم به نحوی مشخص می کند . هر مسیریاب در یک پریود زمانی بردار تاخیر خود را به همسایه های خود می فرستد .

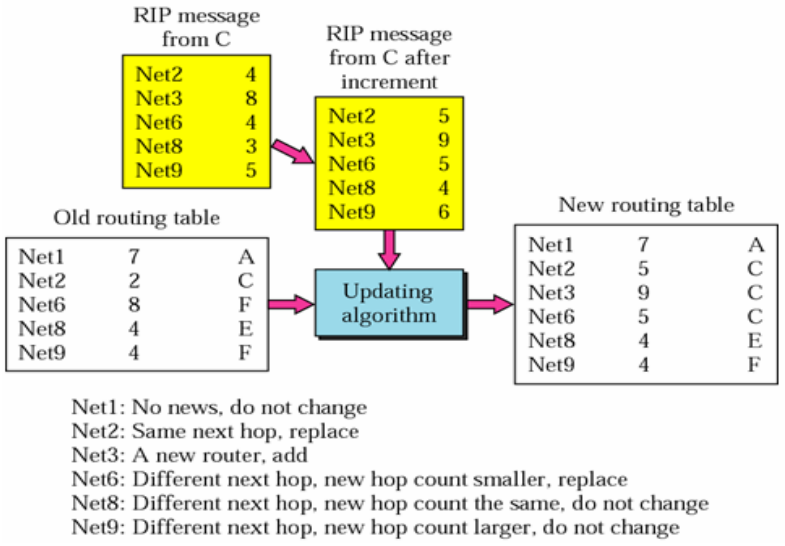
هر Node با توجه به بردارهای دریافتی، بردار جدیدی ایجاد می کند وMin تأخیر را برای هر مسیر پیدا می کند.



Distance Vector

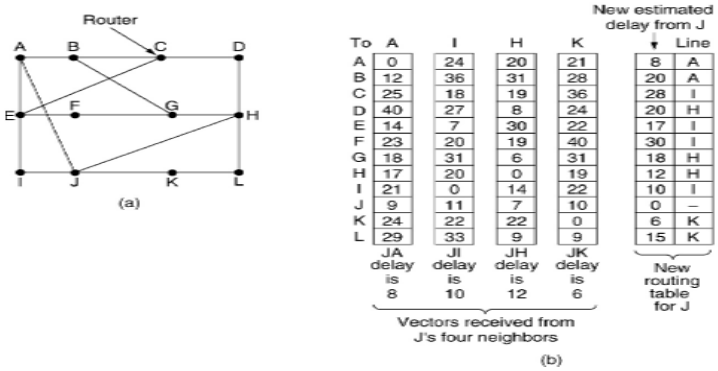
محاسبه تأخیر چگونه انجام می شود ؟

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



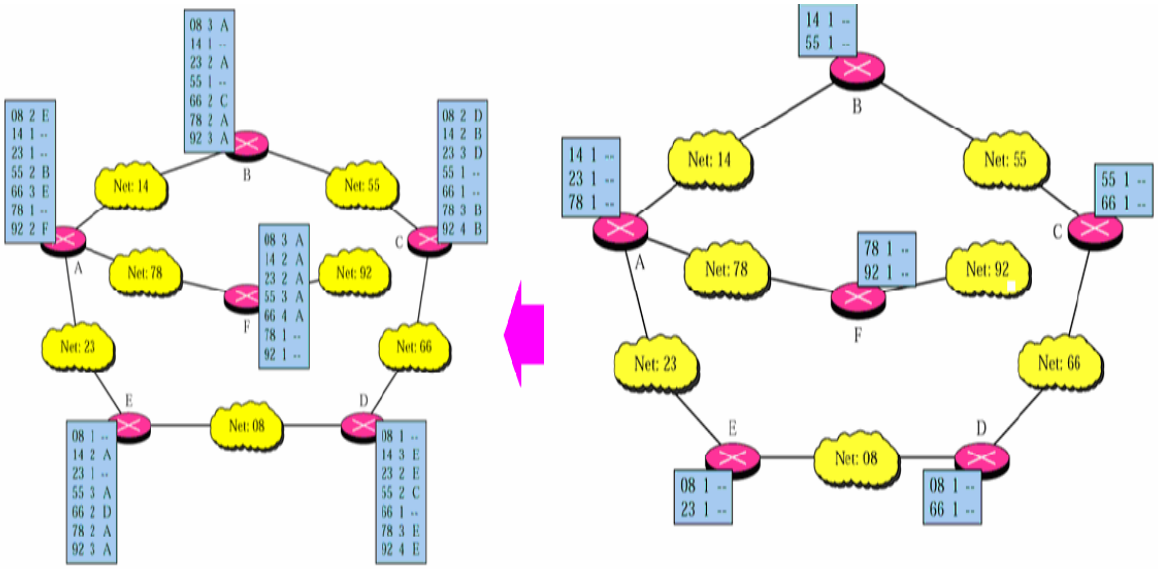
Updating Vector Table

مثال: در زیر ابتدا مسیریاب C جدول مسیریابی خود را بروز نموده است ودر 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:

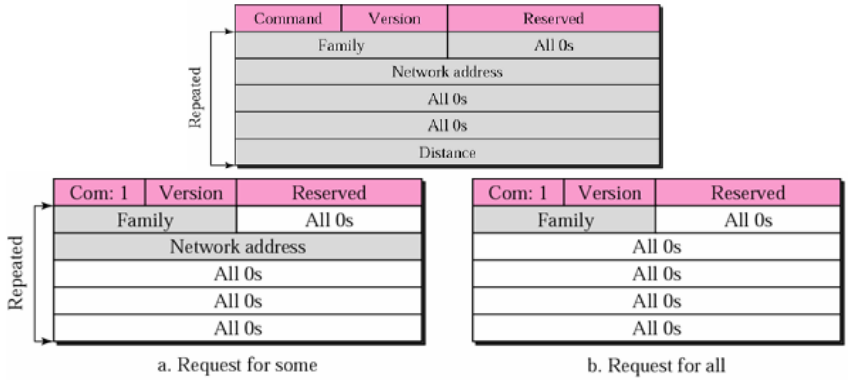


Updating Vector Table Example

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



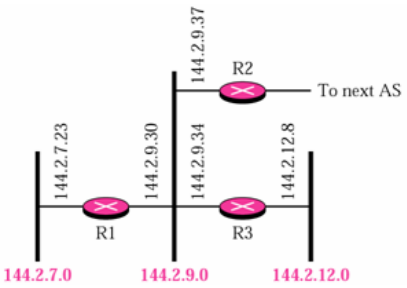
فرمت بسته های RIP و پاسخ آنها بصورت زیر می باشد:



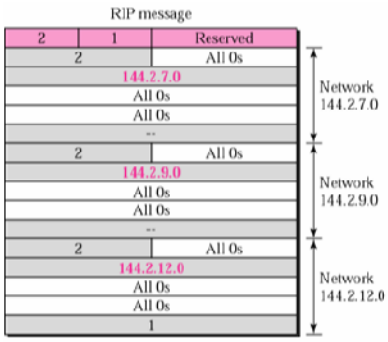
a. Request for some

b. Request for all

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،144.2.9.0 و 144.2.12.0 را اعلان کند. پاسخ دوره ای (بسته بروز رسانی) بصورت زیر است:



تایمرهای RIP شامل موارد زیر می باشد:

۱. دوره ای(Periodic):۲۵-۳۵ ثانیه

۲. انقضاء(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 تایمرها در این زمان درحال اجرا می باشد.

تایمر دوره ای:۱

تایمر انقضاء: ۱۵=۵-۲۰

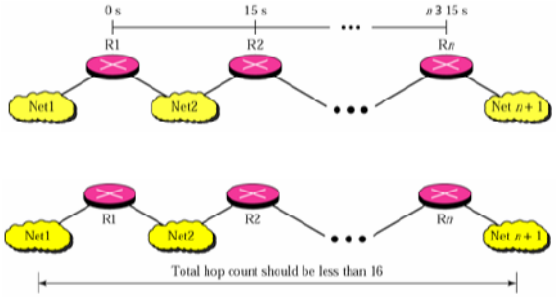
تایمر مجموعه زباله: ۵

مشکلات RIP:

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 .

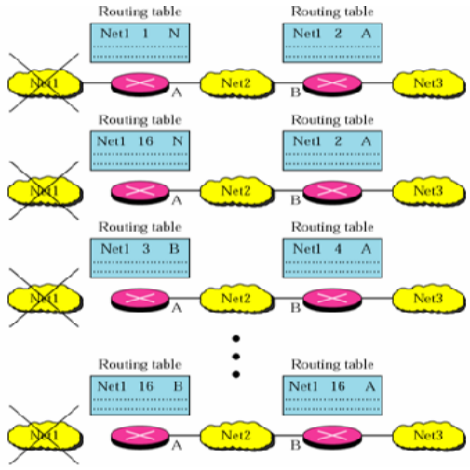
۳- یکی دیگر از عیوب این روش کند بودن است (Slow convergence) .چون باید هر نود و تأخیرش را با کلیه نودهای دیگر به دست آورد. بنابراین باید تعداد پرشها موجود کمتر از ۱۶ باشد.



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 روشDistance Vector هم این مشکل وجود دارد و باعث می شود که تأخیر کاملاً بهینه نباشد ولی در روش State Link چون از TIME استفاده می شود به نوعی (تا حدودی) مشکل را حل کرده است .

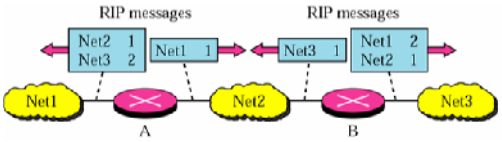
۶- بی ثباتی(Instability) از دیگر مشکلات RIP می باشد. برای درک این مفهوم تصویر زیر را در نظر بگیرید.



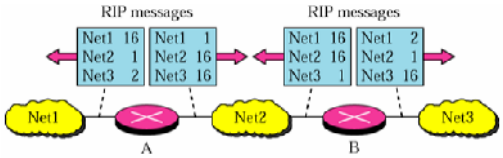
مسیریاب A به شبکه Net1 متصل است و مسیریاب B از طریق مسیریاب A به این شبکه متصل است. با قطع اتصال مسیریاب A با شبکه Net1، مقدار هزینه تا این شبکه را به حداکثر (۱۶) می رساند تا عدم اتصال با آن را نشان می دهد. اما این قطع اتصال هنوز به مسیریاب B گزارش نشده است. قبل از اعلام این وضعیت به مسیریاب B، مسیریاب B جدول بروز شده جدید خود را برای مسیریاب A می فرستد. مسیریاب A، به تصور اینکه مسیریاب B با این شبکه ارتباط دارد، جدول خود را با اطلاعات جدید، بروز می کند. جدول مسیریاب B نیز با اطلاعات اشتباه مسیریاب A، بروز می شود. این چرخه تا آنجا ادامه می یابد تا هزینه هر دو جدول برای این شبکه به ۱۶ برسد.

برای رفع این مشکلات ۲ راه پیش بینی شده است:

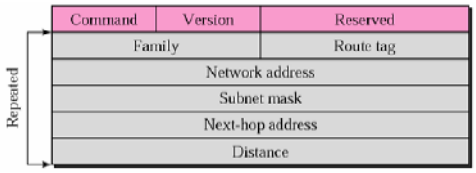
۱. Split Horizon: در این روش اطلاعات مسیرهایی از یک رابط مسیریاب ارسال می گردد که از آن رابط دریافت نشده است.



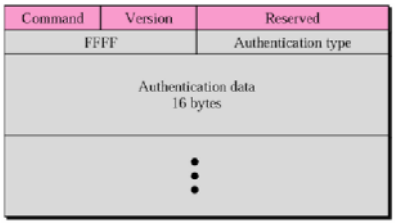
۲. Poison Reverse: در این حالت اطلاعات کامل جدول مسیریابی بر روی تمام رابط ها پخش می شود. اما اگر اطلاعات شبکه ای از یک رابط بدست آید، اطلاعات ارسالی آن شبکه از همان رابط ، مقدار ۱۶ خواهد داشت.



نسخه دوم RIP از CIDR پشتیبانی می کند. فرمت این RIP بصورت زیر می باشد:



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



RIP از پورت ۵۲۰ UDP استفاده می کند.

Link State:

در این روش چند مرحله وجود دارد :

۱) یادگیری همسایه ها

۲) اندازه گیری هزینه هرخط

۳) ساخت بسته های Link State

۴) توزیع بسته هایLink 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 ازLink State استفاده می کند .

یادگیری همسایه ها:

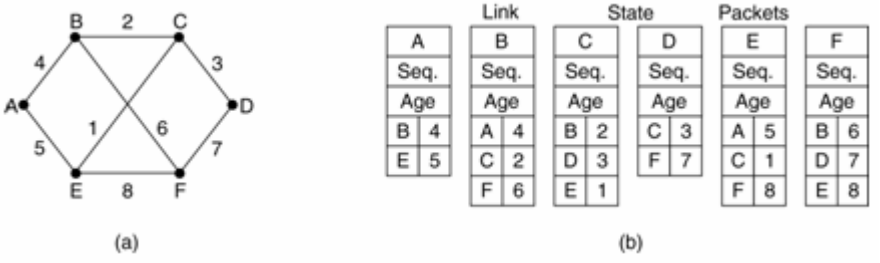
هر مسیریاب وقتی وارد شبکه می شود باید همسایه هایش را بشناسد و این کار باید به صورت خودکار صورت گیرد . هر مسیریاب آدرس خودش را می فرستد و خودش را معرفی می کند(آدرس هر مسیریاب یکتا است).

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 گرد)

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 ز مانی 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 SEQ NO آن نگاه می کند اگر شماره بیشتری نسبت به قبل داشته باشد آن را منتشر می کند و بسته قبلی را دور می ریزد و اگر بسته جدید دارای SEQ NO کمتری نسبت به قبلی باشد دور ریخته می شود و از انتشار روبه جلوی آن خودداری می کند ، پسNumber SEQUENCE به همراه فیلدAGE به این دلیل اضافه شده اند که از ترافیک بیهوده جلوگیری شود.

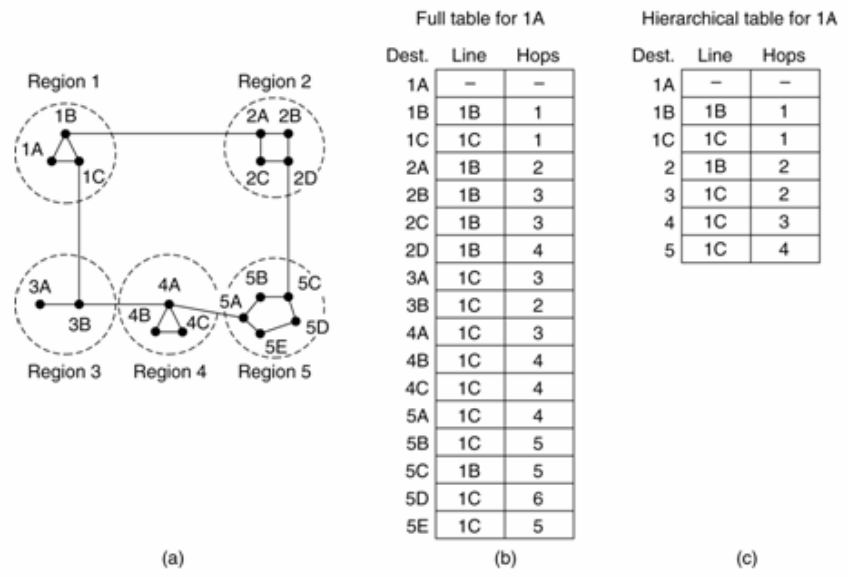
بسته های Link State هم ACK می شوند.

Source	Seq.	Age	Send flags A	Send flags C	Send flags F	ACK flags A	ACK flags C	ACK flags F	Data
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 کهB بسته هایی را از A , C , F دریافت می کند . چگونه ACK ها منتشر می شوند؟بسته ارسالی از E از طریقA,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.

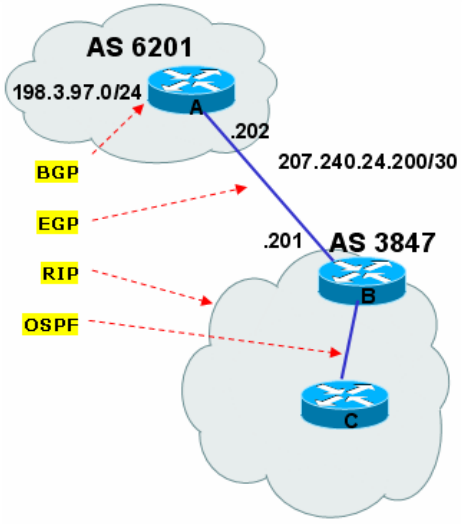


Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4



Multilevel Link State

OSPF, RIP به صورت INTERIOR ROUTER هستند یعنی فقط با ناحیه داخلی خود ارتباط دارند ولی BGPوEGP به صورت EXTERIOR است.

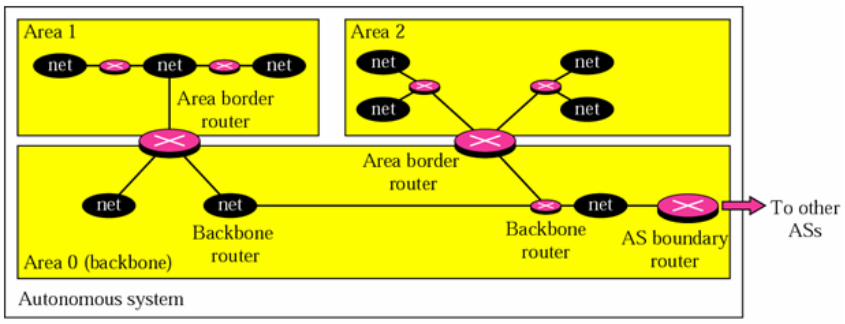
محاسبه تأخیر :

وقتی بسته ها رسید هر مسیریاب با توجه به زمـان رفـت و برگـشت و بـا اسـتفاده از الگـوریتم هـایی ماننـد دیکسترا ، کوتاهترین مسیر و تأخیر را محاسبه می کند یعنی تأخیر هم با استفاده از بسته هـای Link State و بـه دست آوردن گراف شبکه محاسبه می شود .(مانند Link State)

OSPF[1]:

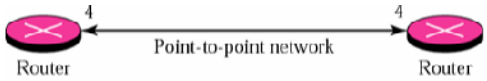
مسیریابهای AS به چهار دسته تقسیم می شود:

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

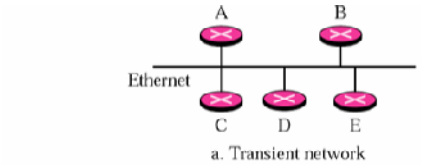


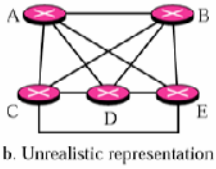
انواع اتصالات در AS:

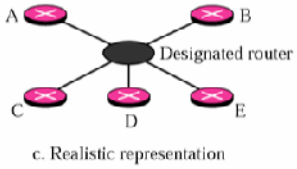
- Point to Point: در این ورش دو مسیریاب مستقیماً با شماره پورت یکـسان بـه همـدیگر متـصل هستند.



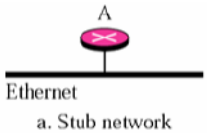
- Transiant: در این روش یک مسیریاب به نام Designated Router وظیفه ارائه اطلاعات شـبکه را برعهده دارد. در شبکه چند مسیریاب وجود دارد.

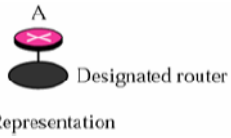






- Stub: فقط یک مسیریاب به شبکه متصل است.

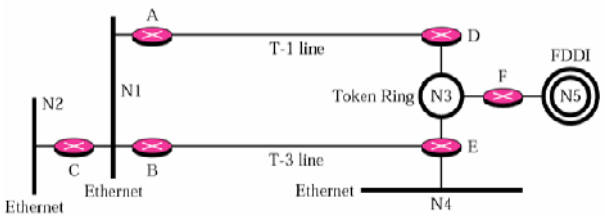




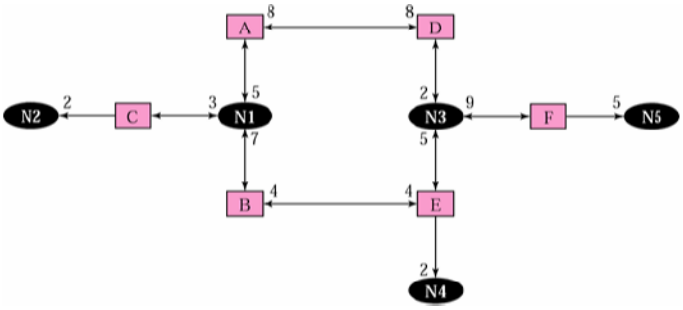
- Virtual

[1] - Open Shortest Path First

مثال: طرح شبکه زیر را با انواع اتصلات بازسازی نمائید.

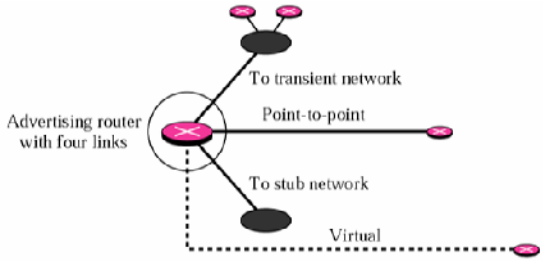


دقت کنید که مسیریابهای با اتصال نقطه به نقطه فقط نیازمند شماره پورت برای ارتباط با هم هستند.



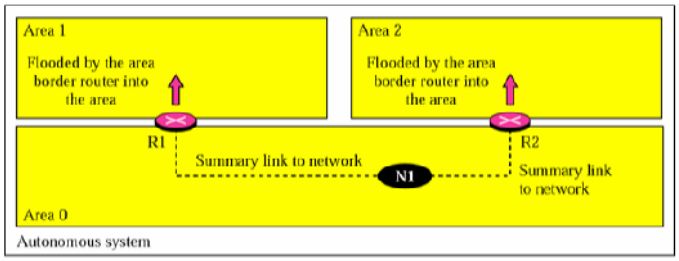
انواع اعلان وضعیت اتصال[1]:

- Router Link: مسیریاب اعلان کننده لینکهای مختلف را می پذیرد.



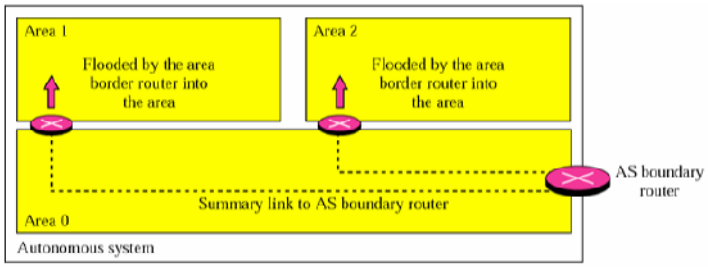
- Network Link: یک شبکه و مجموعه مسیریابهای متصل به آن را شامل می شود.

- Summery Link to Network: اطلاعات شبکه های داخل نواحی توسط مسیریابهای لبه نـواحی به سایر نواحی منتقل می شود.

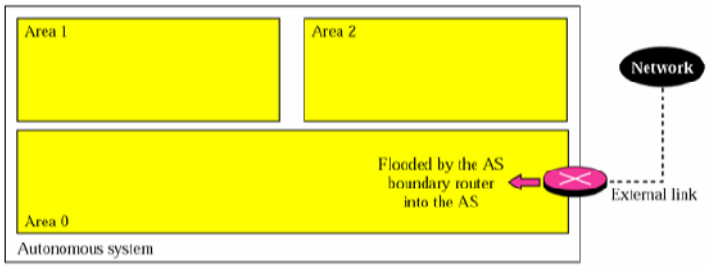


- Summery Link to AS Boundary Router: انتقال اطلاعات داخل AS از مـسیریاب مـرزی AS به سایر نواحی AS.

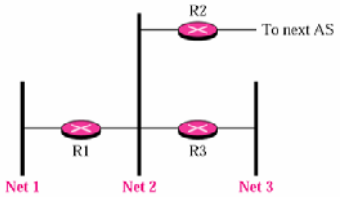
[1] - Link State Advertisment



- External Link: انتقال داده های خارج از AS به داخل AS از طریق مسیریاب مرزی AS.



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.

R1 دو اتصال دارد:Net1 و Net2.

R2 یک اتصال دارد:Net2.

R3 دو اتصال دارد:Net2 و Net3.

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

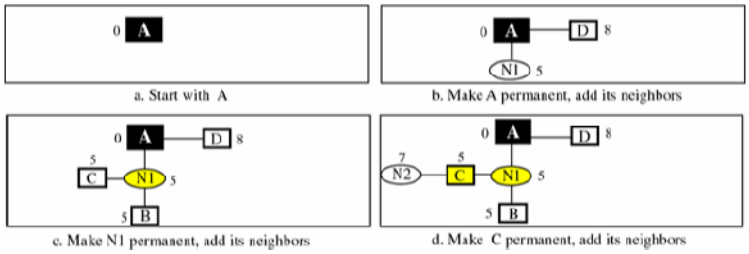
همه سه شبکه باید Network Link ها را اعلان نمایند.

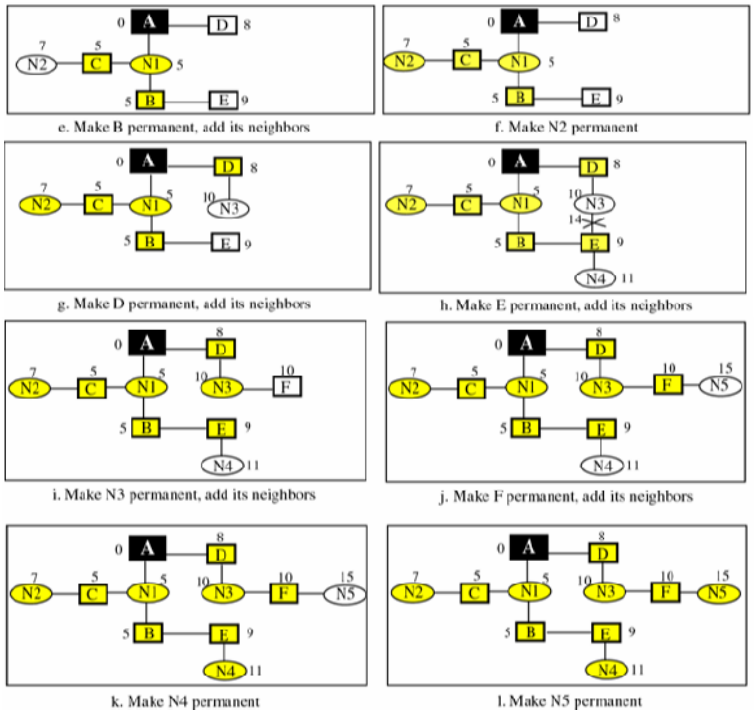
اعلان Net1 بوسیله R1 انجام می گیرد، زیرا تنها مسیریاب متصل به آن است و بنابراین Designated Router می باشد.

اعلان Net2 بوسیله R1 یا R2 و یا R3 ، براساس اینکه کدامیک از آنها به عنوان Designated Router انتخاب 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.

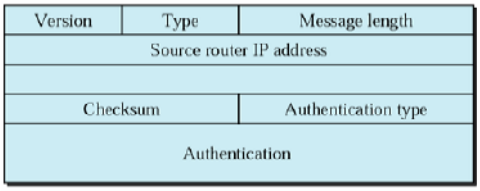
در OSPF، همه مسیریابها پایگاه Link State یکسان دارند. نحوه محاسبه کوتاهترین مسیر در تصاویر زیر نمایش داده شده است:



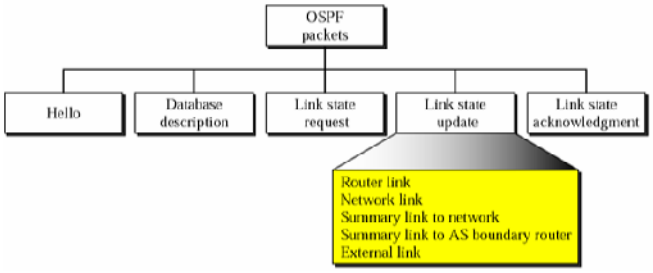


هزینه هر گره از گره قبلی در کنار آن درج شده است. در هر بار اجرای الگوریتم کوتاهترین مسیر، مسیر با کمترین هزینه انتخاب می شود و توسعه داده می شود. چنانچه با توسعه یک مسیر یک حلقه بوجود آید باید با انتخاب کوتاهترین مسیر تا گره جدید، حلقه بوجود آمده را حذف کرد.

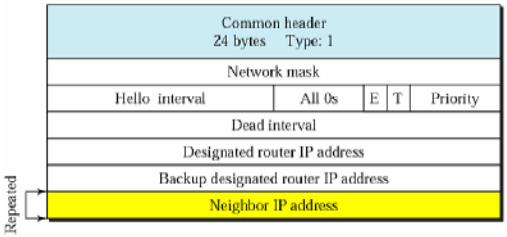
سرآیند بسته های OSPF شامل دو قسمت می شود. فرمت قسمت عمومی این سرآیند به شکل زیر می باشد:



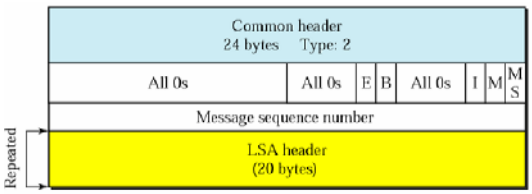
انواع بسته های OSPF:



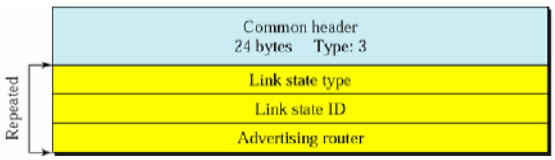
فرمت بسته Hello بصورت زیر می باشد:



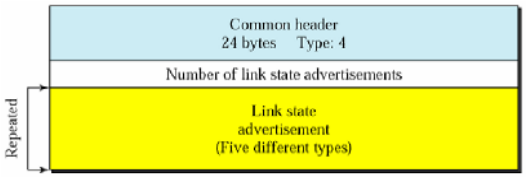
فرمت بسته Databas Description:



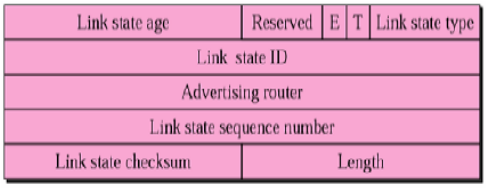
فرمت بسته درخواست Link State:



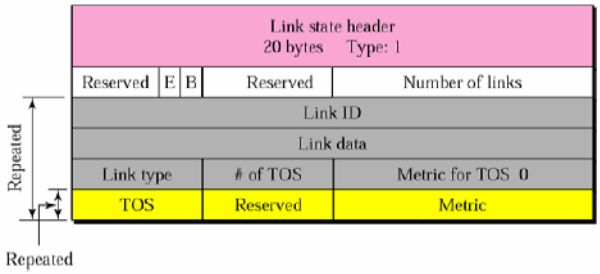
فرمت بسته بروز رسانی Link State:



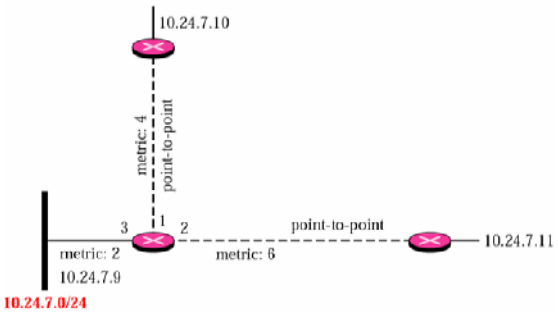
فرمت سرآیند بسته LSA:



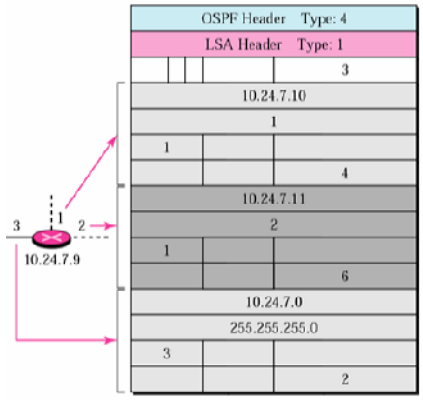
فرمت بسته Router Link LSA:



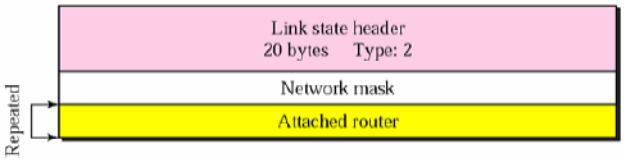
مثال: Router Link LSA ارائه شده توسط مسیریاب 10.24.7.9 چیست؟



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:

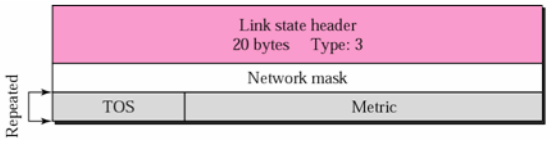


مثال: Network Link LSA طرح روبرو چیست؟

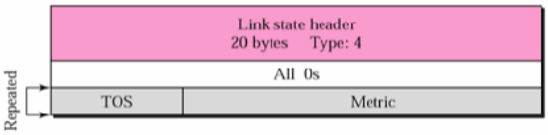
این شبکه دارای سه مسیریاب اتصالی می باشد.LSA آدرس Mask و آدرس مسیریابها را ارائه می دهد. دقت کنید تنها یک مسیریاب به عنوان Designated Router ، Network Link را اعلان می کند.

OSPF Header Type: 4
LSA Header Type: 2
255.255.255.0
10.24.7.14
10.24.7.15
10.24.7.16

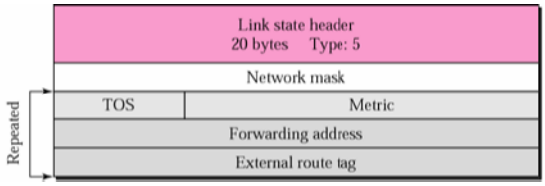
فرمت بسته Summary Link to Network LSA:



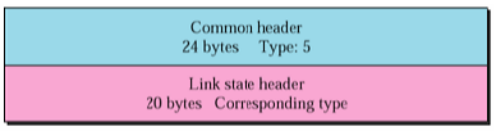
فرمت بسته Summary Link to AS boundary LSA:



فرمت بسته External Link:



فرمت بسته Link State Acknowledgment:



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

BGP[1]:

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 مسیریابهایی که BGP را اجرا می کنند یکدیگر را شناخته و ردوبدل اطلاعات می کنند .

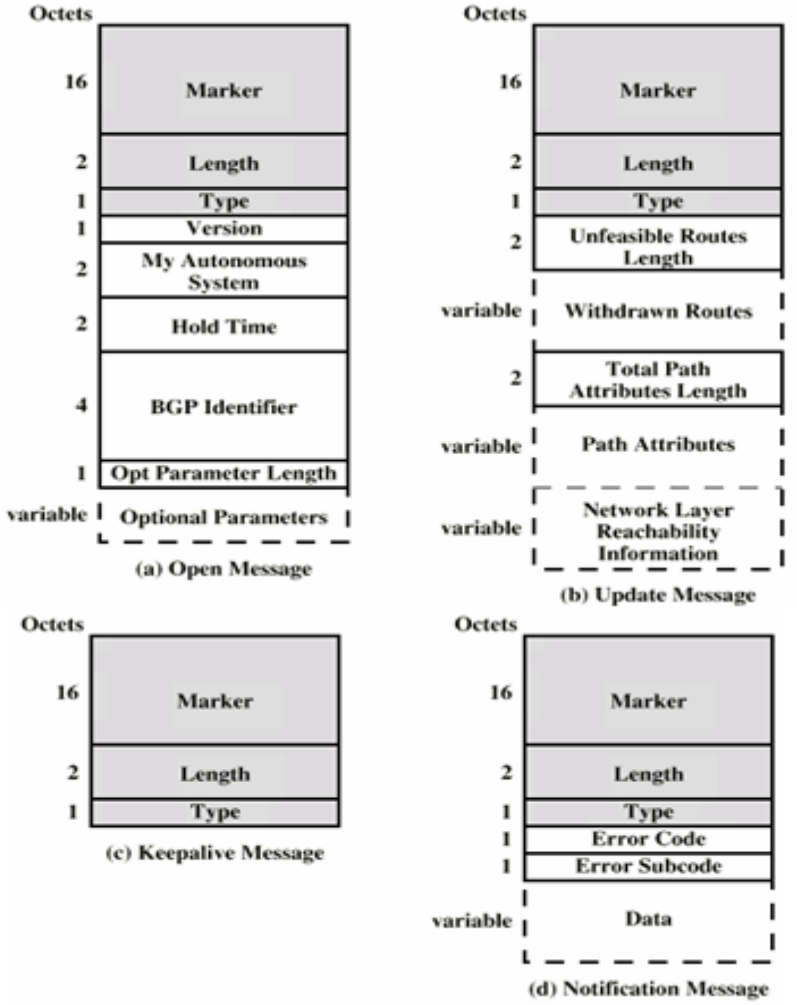
پیغامهای BGP :

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 خطا و بروز اشکال کاربرد دارد .



AS Messages

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

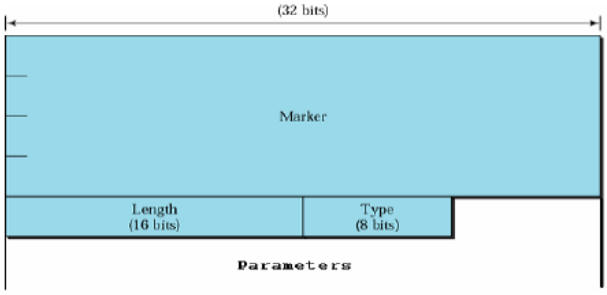
۱. Neighbour acquisition : وقتی دو مسیریاب که در همسایگی هم هستند بخواهند رابطه همسایگی برقرار کنند از این procedure استفاده می کنند . ممکن است این درخواست از طرف مسیریاب همسایه قبول نشود (فعلاً) . زمانی که دو مسیریاب آماده بودند با پیغامهای open , Keepalive این رابطه برقرار می شود .

[1] - Border Gateway Protocol

۲.Neighbour Reachability :بعد از برقراری ارتباط ، این procedure توسط ردو بدل کردن اطلاعات بـه صورت پیغامهای Keepalive رابطه همسایگی را بصورت دائم برقرار می کند .

۳.Network reachability : توسط رد وبدل کردن پیغامهای update صورت می گیرد یعنی هر مـسیریاب اطلاعات زیر شبکه خود را به مسیریاب دیگر ارسال می کند (یعنی به چند شبکه فرعی و چگونه متصل شـده اسـت).

وقتی که تغییراتی در زیر شبکه به وجود آید ، این تغییرها توسـط پیغامهـا بـه مـسیریابهای دیگـر مـنعکس می شود . پیغامهای 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

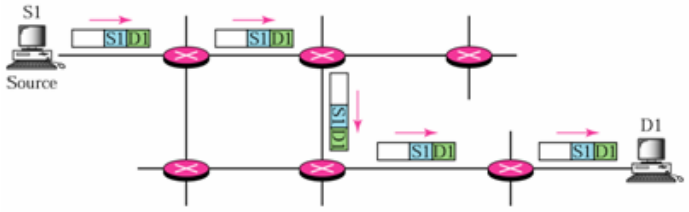
Keepalive فقط سه بخش بالائی را دارد و پارامتر ندارد .

فصل ۵:

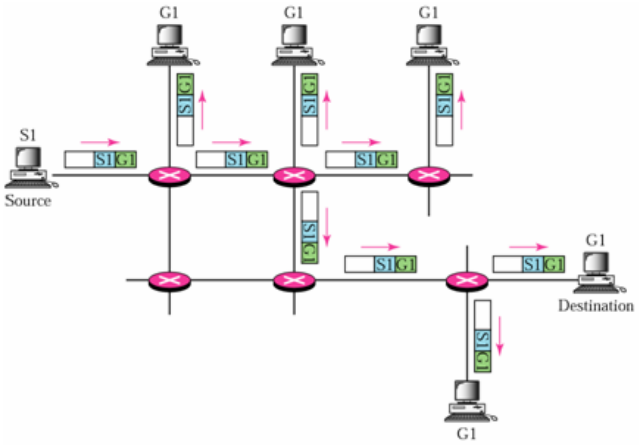
MultiCasting و پروتکل های مسیریابی Multicast

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

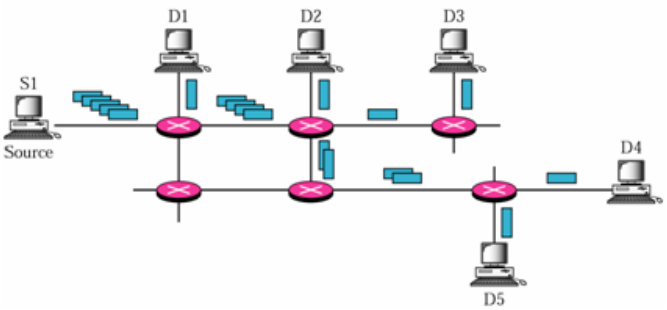
۱. Unicast : مسیریاب بسته دریافتی را تنها از یک رابط خود ارسال می کند. در این حالت گروهی از دریافت کننده ها وجود ندارد.



۲. Multicast : مسیریاب بسته دریافتی را ممکن است از چند رابط خود ارسال کند. بسته های با آدرس Multicast جهت اعضای 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. بعبارت دیگر، کاربرد ارسال Multicast ، جهت ایجاد تبادل موثرتر بین گرو ه 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 224.0.0.0 تا 239.255.255.255 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

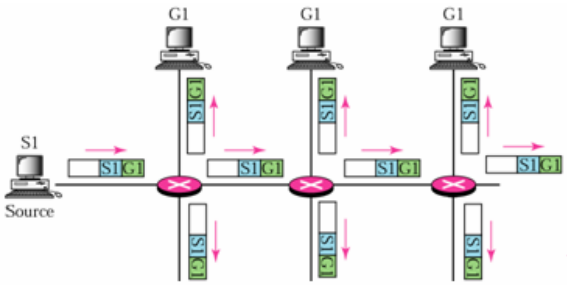
گروه مشخص، بسته هایی را ارسال می نماید، لازم نیست تا عـضو آن گـروه باشـد. میزبـان حتـی ممکن است اعضای گروه را نداند. دو نوع گروه میزبان وجود دارد.

- ثابت: 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 میزبـان، برحـسب نیاز، می تواند به یک گروه بـه پیونـدد و یـا از آن جـدا گـردد. یـک گـروه ثابـت، حتـی درصورت عدم وجـود عـضو بـرای آن، همچنـان بـاقی مـی مانـد. لیـست آدرسـهای IP تخصیصی به گروه های میزبان ثابت، در RFC 1700 ، آمده اسـت. ایـن آدرسـهای رزرو شده بشرح زیر می باشند:
  i. 224.0.0.0: آدرس رزرو شده پایه.
  ii. 224.0.0.1: همه سیستم ها در این زیر شبکه .
  iii. 224.0.0.2: همه مسیریابهای این زیر شبکه.
  iv. 224.0.0.9: همه مسیریابهای RIP2.
  v. 224.0.0.5: همه مسیریابهای OSPF.
  vi. 224.0.0.6: مسیریابهای OSPF Designated.

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

- موقت: هر گروهی که ثابت نباشد، موقت خواهد بود. گروه جهت تخصیص پویا در صورت نیاز، موجود می باشـد. گـروه هـای موقـت در زمـان صـفر شـدن تعـداد اعـضا، متوقـف می گردند.

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



Multicast در یک شبکه فیزیکی:

این پردازش، آسان می باشد. پردازش ارسال کننده، یک آدرس Multicast IP مقصد را مشخص مـی نمایـد. درایور دستگاه این آدرس را به آدرس فیزیکی منبطق با آن تبدیل می نماید و بسته ها را به مقصد ارسال می نمایـد. پردازشهای مقصد نیز با چک کردن درایورهای خود ، از دریافت بسته هـای داده گـرام بـا آدرس Multicast، مطلـع می گردند.

همانطور که قبلاً نیز گفته شد، جهت نگاشت آدرس IP کلاس D به آدرس فیزیکی مرتبط، تنهـا از ۲۳ بیـت سمت راست آدرس IP، استفاده می گردد. بدلیل چشم پوشی از ۵ بیت از آدرس IP در این حالت ، بیتهای ۵ تا ۹ از سمت چپ، این وضوع می تواند باعث نگاشت ۳۲ آدرس غیر-یکتا، در یک آدرس فیزیکی گردد. این موضوع نیـاز بـه

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

- برخی از آداپتورهای 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 آداپتورهای LAN، از مقادیر جدول درهم ساز[1]، 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.

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

Multicast در بین چند شبکه:

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 تحویل بسته ها، در زمان اجتناب از مسیردهی های حلقه و انتقالات ناقض، توسعه داده شده اند.

دو نیازمندی برای Multicast داده برروی 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 بوسیله RFC 2236 برای IGMP، تعریف 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.
  - TTL=0: داده گرام Multicast، با این مقدار، محدود به خود میزبان منبع می گردد.
  - TTL=1: چنین داده گرام هایی، به تمام میزبانهای دورن یک شبکه، که عضو گروه هستند، می رسد.
  - TTL=2 و یا مقدار بیشتر: یک داده گرام Multicast اینچنینی، بوسیله تمام میزبانهای 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 مقصد در این محدوده را ارسال نمی نمایند. از این آدرسها می توان جهت ارسال پیام عضویت در یک گروه، توسط یک میزبان ، استفاده نمود.

---

[1] Hash -

- 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 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 گردند، تا زمانیکه نزدیکترین سرویس دهنده پیدا شود.

جهت ارسال بسته های Multicast ، به کمک الگوریتمهای ارسال Multicast[1] و IGMP، مسیر ارسال بصورت یک درخت تشکیل می گردد. این درختها دارای انواع زیر می باشد:

۱- درخت مبتنی بر مبداء[2]: ترکیب مبداء و گروه ، درخت را مشخص می نماید.

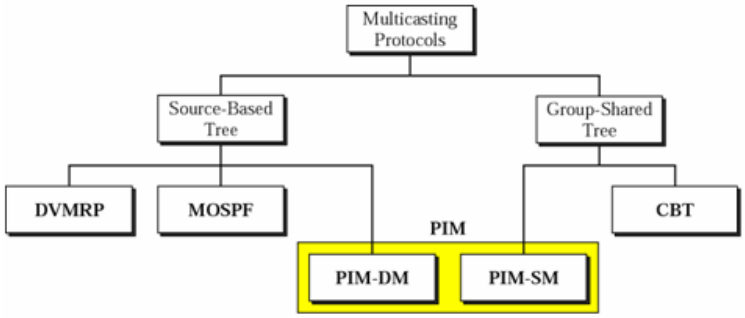
۲- درخت مشترک در گروه[3]: گروه طرح درخت را مشخص می کند.

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 مبداء 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 آوردند. ترکیب پروتکل های مسیریابی Multicast بصورت زیر می باشد:



انواع DVMRP[4]:

---

[1] - Multicast Forwarding Algorithms

[2] - Source based

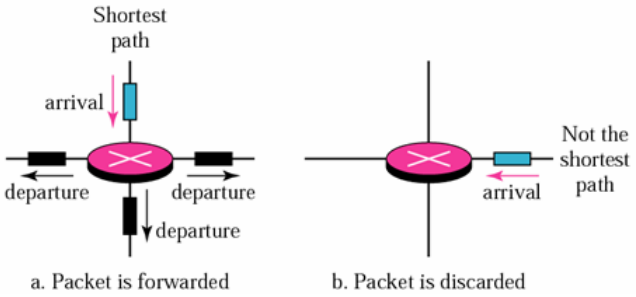
[3] - Group Shared

[4] - Distance Vector Multicast Routing Protocol

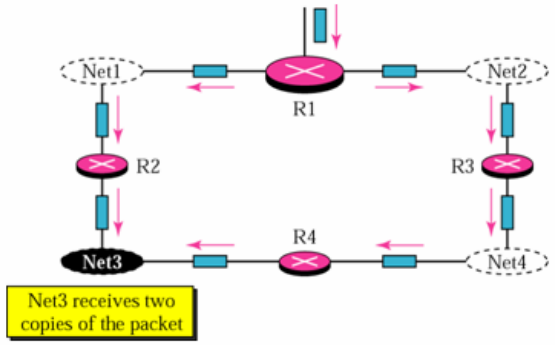
DVMRP یک پروتکل مسیردهی Multicast برپا شده، می باشد(RFC 1075). این استاندارد در ابتدا برای پردازش mrouted در برخی از سیستمهای یونیکس، ایجاد گردید. DVMRP یک پروتکل درونی می باشد و جهت ایجاد درختهای برای هر منبع، برای هر گروه[1] در درختهای تحویل Multicast در AS، بکار می رود.

DVMRP داده گرامهای Unicast راپشتیبانی نمی کند و مسیریابهای پشتیبانی کننده از Unicast توام با Multicast، باید با دو الگوریتم مسیردهی متفاوت، پیکربندی شوند. بدلیل وجود این پردازشهای جداگانه، ترافیکهای Unicast و Multicast، الزاماً مسیر یکسانی را در شکبه طی نخواهند کرد.

- ارسال مسیر معکوس(RPF[2]): مسیریاب بسته های رسیده با کوتاهترین از مبداء 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 تحویل سریع بسته ، بدلیل استفاده از کوتاه ترین مسیر ممکن بین مبداء و مقصد، اشاره نمود. همچنین با این روش بدلیل ایجاد درختهای جداگانه در گره، استفاده کاراتر از منابع شبکه را باعث می گردد، هر بسته تحویلی 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.

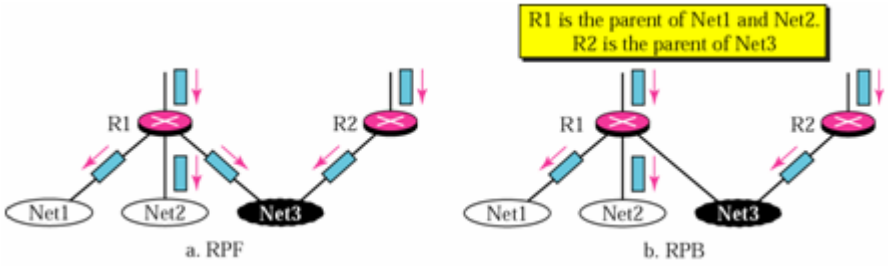


- مسیر معکوس Broadcast (RPB): در این روش جهت حل مشکل روش قبلی، از درخت کوتاهترین مسیر Broadcast از مبداء به هر مقصد استفاده می شود. به این ترتیب تضمین می گردد که هر مقصد تنها یک بسته را دریافت نماید. در درخت فوق هر شبکه به یک مسیریاب منتسب می شود و مسیریاب نقش والد آن شبکه را بازی می کند.

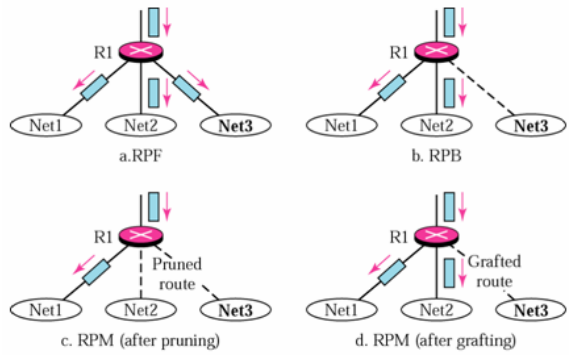
---

[1] - Per-Source Per-Group

[2] - Reverse Path Forwarding



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



ایجاد درخت تحویل Multicast:

یک مسیریاب Multicast بسته ها را به دو دسته از ابزارها، منتقل می کند: مسیریابها و میزبانهای پایین رو که اعضای یک گروه Multicast معین، می باشند. اگر یک مسیریاب Multicast وابستگی به همسایه های پایین رو خود، از طریق یک رابط خاص، ندارد، شبکه یک **شبکه برگ** می باشد. درخت تحویل ، با اطلاعات مسیریابی تشریح کننده این انواع مختلف مقصد، ساخته می شود.

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

در آغاز، همه شبکه های غیر برگ، در درخت تحویل Multicast، گنجانده شده اند. این به هر مسیریاب پایین رو ، امکان سهیم شدن در ترافیکهای ارسالی برای هر گروه را می دهد.

مسیریابهای متصل به یک شبکه برگ، یک رابط را درصورتیکه اعضای مرتبط با یک رابط ، دیگر در فعالیتهای گروه Multicast خاص، فعال نباشند، حذف می نماید. با انجام این کار، بسته های Multicast ، دیگر از طریق آن رابط ارسال نمی شوند. اگر یک مسیریاب قادر به حذف تمام رابطهای جریان پایین رو خود، برای گروه خاصی باشد، همسایه بالاتر خود را آگاه می سازد که نیازی به ترافیک برای زوج منبع و گروه خاص ، ندارد. این اطلاع دهی بوسیله ارسال یک پیام هرس شدن[1] به همسایه بالاتر، صورت می پذیرد. اگر یک همسایه بالاتر، چنین پیامی را از هریک از مسیریاب های پایین رو در یک رابط، دریافت نمود، این مسیریاب می تواند براحتی رابطش را از درخت تحویل Multicast، حذف نماید. این رویه در مورد مسیریابهای سطوح بالاتر نیز عیناً اتفاق می افتد و به این وسیله شاخه های اضافی درخت تحویل، حذف می گردد.

[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 تحویل 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.

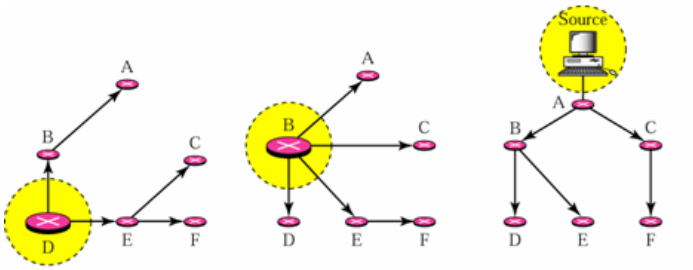
از آنجا که IP Multicast از عضویت پویا در گروه ، حمایت می کند، میزبانها ممکن است در هر زمانی به عضویت یک گروه Multicast درآیند. زمانی که این امر اتفاق افتاد، مسیریابهای DVMRP، از پیام های پیوند[1]، جهت اتصال مجدد شبکه به درخت تحویل Multicast، استفاده می نماید. یک پیام پیوند، به عنوان نتیجه دریافت یک گزارش 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 مجدداً 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 نگردند، تایید می گردند.

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

MOSPF[2]:

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



CBT[3]:

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 میعادگاه[4] استفاده می شود. مبداء، بدلیل آنکه

---

[1] - Graft Message

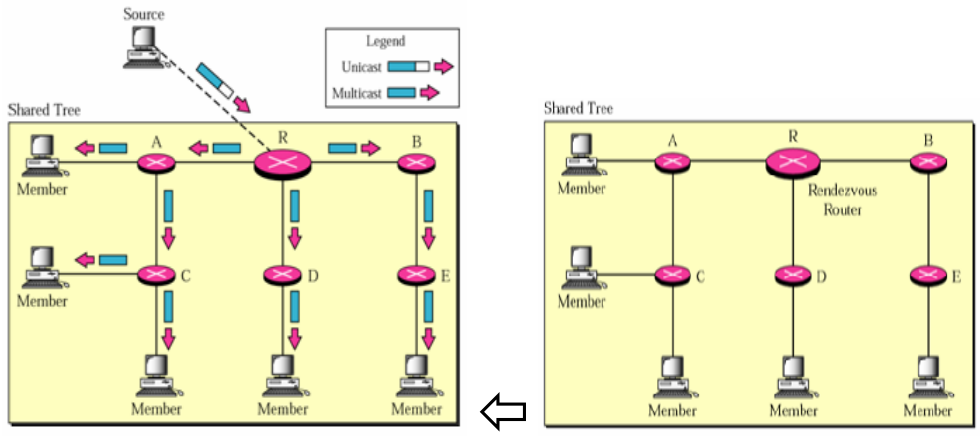
[2] - Multicast OSPF

[3] - Center Based Tree

[4] - Rendezvous

می تواند جزء گروه نباشد، بسته های Multicast را در بسته های Unicast محصور کرده و این بسته هـای Unicast را به مسیریاب میعادگاه می فرستد. این مسیریاب جزئی از درخت گروه می باشد. مسیریاب میعادگاه این بسته هـای 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 روشهای مشابه می باشد. در RPF، هـر ارسـال کننـده در یـک گـروه Multicast، درخت خودش را دارد. مشکل این روش، ایجاد مسیرهای احتمالی کمتر بهینه برای برخی منابع و دریافت کنندگان، می باشد.



PIM[1]:

پیچیـدگی MOSPF باعـث جلـب توجـه بـه PIM گردیـد. PIM یـک پروتکـل مـسیردهی Multicast دیگـر می باشد. برخلاف MOSPF، PIM از هرگونه پروتکل مسیردهی Unicast ، جـدا مـی باشـد. بـا ایـن وجـود بـا همـه پروتکلهای مسیردهی Unicast، کار می کند. PIM دو شیوه و یا عمل کرد را معرفی می کند:

- شیوه متراکم (PIM-DM[2])
- شیوه پراکنده (PIM-SM[3])، RFC 2362

شیوه متراکم و شیوه پراکنده، به تراکم اعضای گروه در یک ناحیه، ارجـاع مـی دهـد. یـک گـروه بـه عنـوان متراکم شناخته می شود، اگر احتمال یافتن حداقل یک عضو گروه، بالا باشد. این موضوع حتی در مورد انـدازه هـای 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 هـر دو شـیوه در یک گروه یکسان را می دهد.

PIM-DM:

ابزار PIM-DM، یک بسته را دریافت مـی کنـد، ایـن ابـزار، تاییـد اعتبـار ورودیهـا را بـا اسـتفاده از جـدول مسیردهی Unicast موجود ، انجام می دهند. اگر ورودیها، بهتـرین مـسیر بـه منبـع را مـنعکس نماینـد، مـسیریاب بسته های Multicast را منتشر می کند. بسته به همه رابطهایی که از درخت تحویـل Multicast حـذف نـشده انـد، ارسال می گردد.

---

[1] - Protocol Independent Multicast
[2] - Protocol Independent Multicast-Dense Multicast
[3] - Protocol Independent Multicast-Sparse Multicast

برخلاف DVMRP، PIM-DM تلاشی جهت محاسبه مسیریابهای مشخص Multicast، انجام نمی دهد. بلکه فرض می کند که مسیریابهای جدول مسیردهی Unicast، متقارن هستند.

همانند عملیات در یک محیط DVMRP، یک ابزار PIM-DM، بطور پیش فرض فرض می کند که همه رابطهای خروجی به سمت پایین نیازمند دریافت ترافیک Multicast دریافتی می باشند. مسیریابها دیتاگرامها را به همه نواحی شبکه، ارسال می کند. اگر برخی از نواحی، دریافت کننده هایی برای گروه Multicast خاصی را نداشته باشند، PIM-DM ، این شاخه ها را از درخت تحویل، حذف می نماید. فرایند حذف بدلیل آنکه PIM-DM اطلاعات دریافت کننده های پایین را از جدول مسیردهی Unicast بدست نمی آورد، فعال می شود. PIM-DM پیاده سازی راحتی دارد. تنها فرض لازم آنست که یک مسیریاب قادر باشد تا لیستی از درخواستهای هرس را حفظ نماید.

با شیوه های جریان دهی و هرس بکار رفته در PIM-DM، این پروتکل باید در محیطهای که اکثر میزبانهای یک دامنه نیازمند دریافت داده های Multicast باشند، بکار می رود. در چنین محیطهایی، اکثریت شبکه ها از درخت تحویل حذف نخواهند شد. سربار جریان دهی نیز کم می باشد. این پیکربندی در موارد زیر نیز مناسب می باشد:

- فرستنده ها و گیرنده ها در فاصله کمی از یکدیگر قرار دارند.
- تعداد فرستنده ها کم و تعداد دریافت کننده ها زیاد باشد.
- حجم ترافیک Multicast زیاد است.
- جریان ترافیک Multicast، ثابت است.

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

PIM-SM:

از این روش در محیط های پراکنده همانند WAN، استفاده می شود. این روش همانند CBT است اما از رویه های ساده تری استفاده می کند.

MBONE[1]:

MBONE در مارس ۱۹۹۲ پیاده سازی گردید. این شبکه اساساً جهت پروتکلهای Multicast، توسعه یافته است. اولین کاربرد این شبکه در نشست صوتی Muticast IETF، 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 درحال استفاده است.

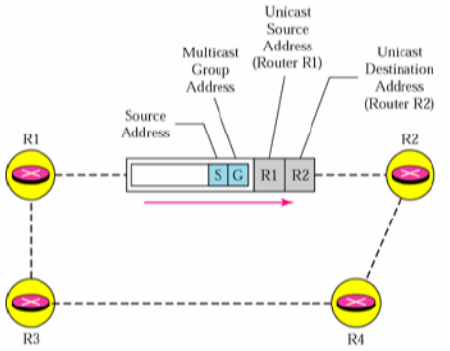
Multicast Backbone به عنوان یک شبکه پوشش مجازی، با استفاده از ساختار فیزیکی اینترنت، شروع شد. در آن زمان، مسیردهی Multicast ، در ابزارهای مسیردهی استاندارد، پشتیبانی نمی شد. اولین نقاط MBONE ، در سیستمهای یونیکس مجهز به پردازش مسیردهی mrouted، شکل گرفت. امروزه MBONE هنوز هم عملیاتی است، اما دیگر اتصالات Multicast بصورت محلی در بسیاری از مسیریابهای اینترنت، انجام می گیرد. تلاشهایی جهت یکپارچه کردن مستقیم MBONE با ساختار اینترنت، درحال انجام می باشد.

[1] - internet Multicast backBONE

ترافیکهای Multicast برروی همه قسمتهای اینترنت، جریان نمی یابند. بدلیل این محدودیت، MBONE بصورت مجموعه ای از نواحی شبکه های Multicast می باشد. این نواحی از طریق تونلهای مجازی به یکدیگر متصل شده اند. تونل ها نقش پل را بر روی برای نواحیی که از ترافیک Multicast حمایت نمی کنند، بازی می کنند.

یک مسیریاب که نیازمند ارسال بسته های Multicast به نواحی Multicast دیگر است، این بسته ها را در بسته های Unicast قرار می دهد. این بسته های محصور شده، از طریق مسیریابهای استاندارد اینترنت، منتقل می گردند. آدرس مقصد در بسته Unicast، نقطه انتهایی تونل می باشد. مسیریاب انتهای دیگر تونل، سرآیند را برداشته و بسته های Multicast را به گیرنده ها، ارسال می دارد.

تونلهای MBONE دارای پارمترهای اندازه ای و سطح اندازه می باشد. پارامترهای اندازه ای ، به عنوان یک هزینه در الگوریتمهای مسیردهی Multicast ، بکار می رود. الگوریتمهای مسیردهی، این مقادیر را برای انتخاب بهترین مسیر در شبکه، بکار می برند. تونلها از مقادیر اندازه ای متفاوت، جهت انتقال ترافیک نامتوازن در شبکه، استفاده می کند.



بخش ۳:
سوئیچ داده

فصل ۶: روشهای سوئیچ داده
فصل ۷: شبکه های ATM و FrameRelay
فصل ۸: ISA، DiffServ و MPLS

فصل ۶:

روش های سوئیچ داده

در سال ۱۹۷۰، سوئیچ بسته ای به عنوان معماریی 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.

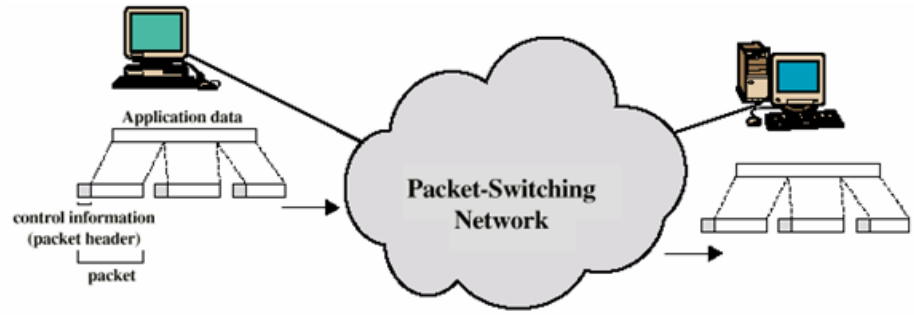
این فصل مروری دارد بر فناوری سوئیچ بسته ای و بسیاری از مزایای سوئیچ بسته ای (انعطاف پذیری، اشتراک منابع، قوی بودن،حساسیت) را به همراه هزینه خواهیم دید. یک شبکه سوئیچ بسته ای، مجموعه توزیع شده ای از گره های سوئیچ بسته ای است. بصورت ایده آل، تمام گره های سوئیچ بسته ای همیشه از وضعیت کل شبکه آگاهند. متاسفانه، بدلیل توزیع شده بودن گره ها، یک تاخیر زمانی بین تعویض وضعیت در بخشهایی از شبکه وجود دارد و دانش آن تغییرات در جای دیگری هستند. بعلاوه تبادل اطلاعات، خود شامل سربارهایی می باشد. بعنوان 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 درشبکه 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 هرکدام 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 متغییری 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 بدهید 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 تحویل 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 سریعترین 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[1]، تخصیص می یابد. در بسیاری از زمانها، اتصال ممکن است بدلیل 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 بپردازند؛ 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 درخواستهای 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 تحویل 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 حداکثر 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. سئوالی که می تواند مطرح شود آنست که شبکه چگونه این جریان بسته ها را جهت مسیریابی در شبکه و تحویل 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 درحالیست 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 گسترده 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 خطا، را فراهم کند. توالی به این حقیقت اشاره می کند که بدلیل جریان یافتن همه بسته ها از یک مسیر، آنها با همان ترتیب اولیه دریافت می گردند.کنترل خطا سرویسی است که اطمینان می دهد که نه تنها همه

[1] - 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، به گره B نرسد و یا با خطا 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، اجتناب از فاز برپاسازی اتصال می باشد. اگر یک ایستگاه بخواهد تنها یک یا تعداد کمی بسته را ارسال کند، تحویل داده گرامی سریعتر خواهد بود. مزیت دیگر داده گرام آنست که بدلیل 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 گردند. با استفاده از کانال 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، تحویل 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 تحویل داده گرامی، اگر یکی از گره ها از دست برود، بسته های بعدی ممکن است بتوانند مسیر جایگزین را بیابند و از آن گره بگذرند.

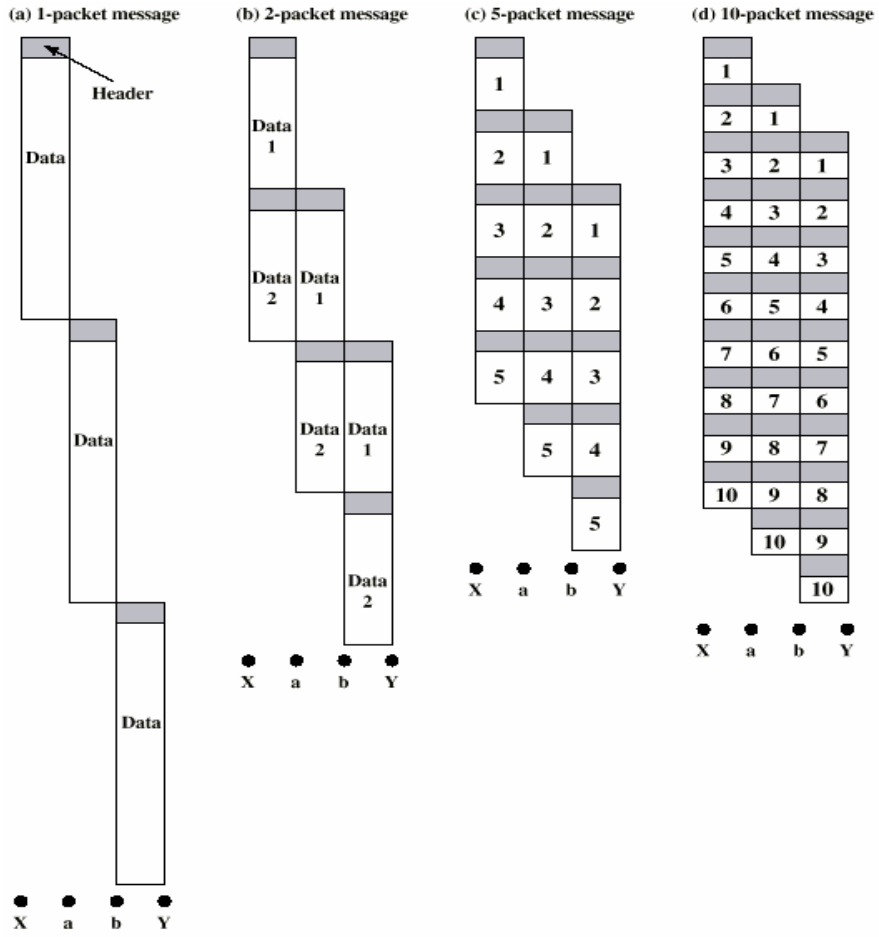
اکثر شبکه های سوئیچ بسته ای موجود، از مدارات مجازی برای اعمال داخلیشان استفاده می کنند. این موضوع جهت گیری تاریخی برای ایجاد شبکه ای که بتواند در توالی، سرویسهای مطمئن همانند یک شبکه سوئیچ مداری، ارائه دهد را نمایان می سازد. با این وجود، برخی از تهیه کنندگان شبکه های سوئیچ بسته ای خصوصی از عملکرد داده 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 Y، وجود دارد. پیام ارسالی ۴۰ بایت است و هر بسته ۳ بایت اطلاعات کنترلی دارد که در ابتدای بسته قرار گرفته و بعنوان سرآیند عمل می کند. اگر کل پیام بصورت یک بسته ۴۳ بایتی (۳بایت 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 Y 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 ، هرکدام ۲۰ بایت، تقسیم نموده ایم و البته هر کدام ۳ بایت سرآیند یا اطلاعات کنترلی دارند. در این حالت گره a، بلافاصله پس از دریافت اولین بسته از X ، بدون آنکه بخواهد منتظر دریافت بسته دوم شود، می تواند آن را ارسال نماید. بدلیل 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، بجای کاهش آن، می باشد. این بدلیل 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 تواند 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 ۶-۲: تاثیر اندازه بسته بر فریم انتقال

کارایی[1]:

یک مقایسه ساده از سوئیچ مداری و ۲ طرح سوئیچ بسته ای در تصویر ۶-۳ 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 $2*10^8$ 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 10 kbps، این زمان یک ثانیه می باشد.
- **تاخیر گره:** فاصله زمانیکه یک گره جهت انجام پردازش لازم، جهت سوئیچ داده لازم دارد.

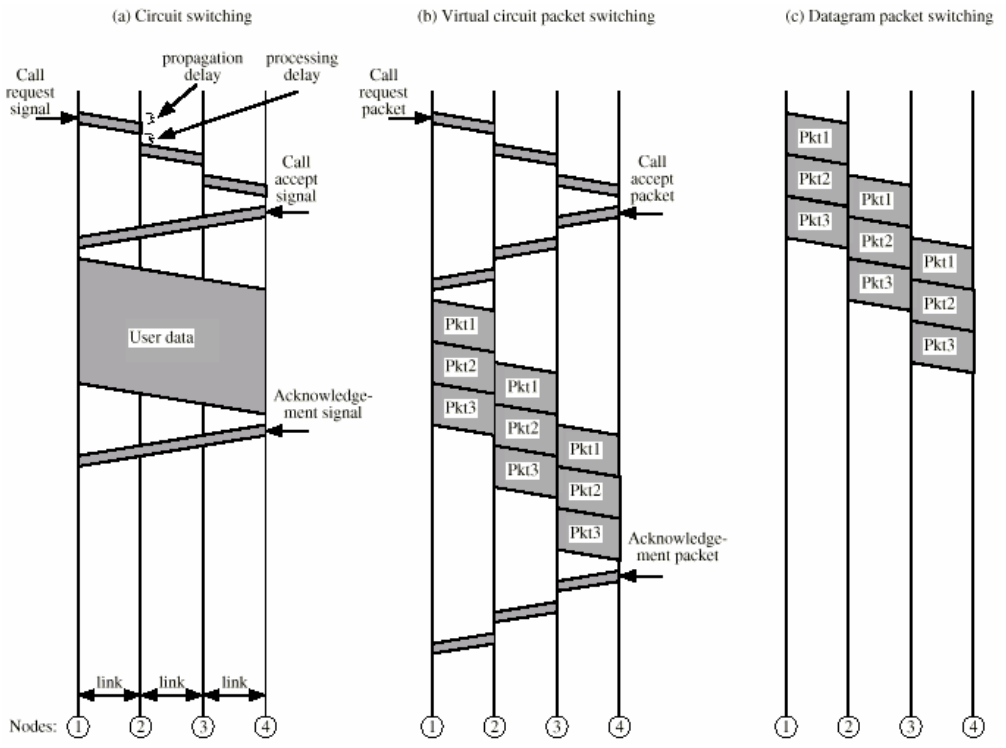
برای سوئیچ مداری، حجم تاخیر مشخصی قبل از ارسال پیام وجود دارد. ابتدا یک سیگنال درخواست تماس از طریق شبکه ارسال می گردد تا اتصال تا مقصد برپا گردد. اگر ایستگاه مقصد شلوغ نباشد، یک سیگنال پذیرش تماس، باز می گرداند. توجه کنید که یک تاخیر پردازش در هر گره، در طی درخواست تماس، تحمیل می گردد که این زمان در 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 متغییر 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، بدلیل 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 میزبان همانند اندازه شبکه، ساختار شبکه، الگوی بارگذاری و خصوصیات تبادلات خاص آن، بستگی دارد.



تصویر۶-۳: 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 تاخیر متغیر تعریف شده تا داده ها بصورت متغییر دریافت گردند. بعلاوه در سوئیچ بسته ای داده گرام، داده ها با ترتیبی متفاوت از ترتیب انتقال آنها ممکن است دریافت گردند.

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 مبداء به مقصد منتقل می شوند. برای سوئیچ بسته ای، داده آنالوگ باید قبل از انتقال به دیجیتال تبدیل گردد و بعلاوه هر بسته نیازمند بیتهای سربار همانند آدرس مقصد نیز می باشد.

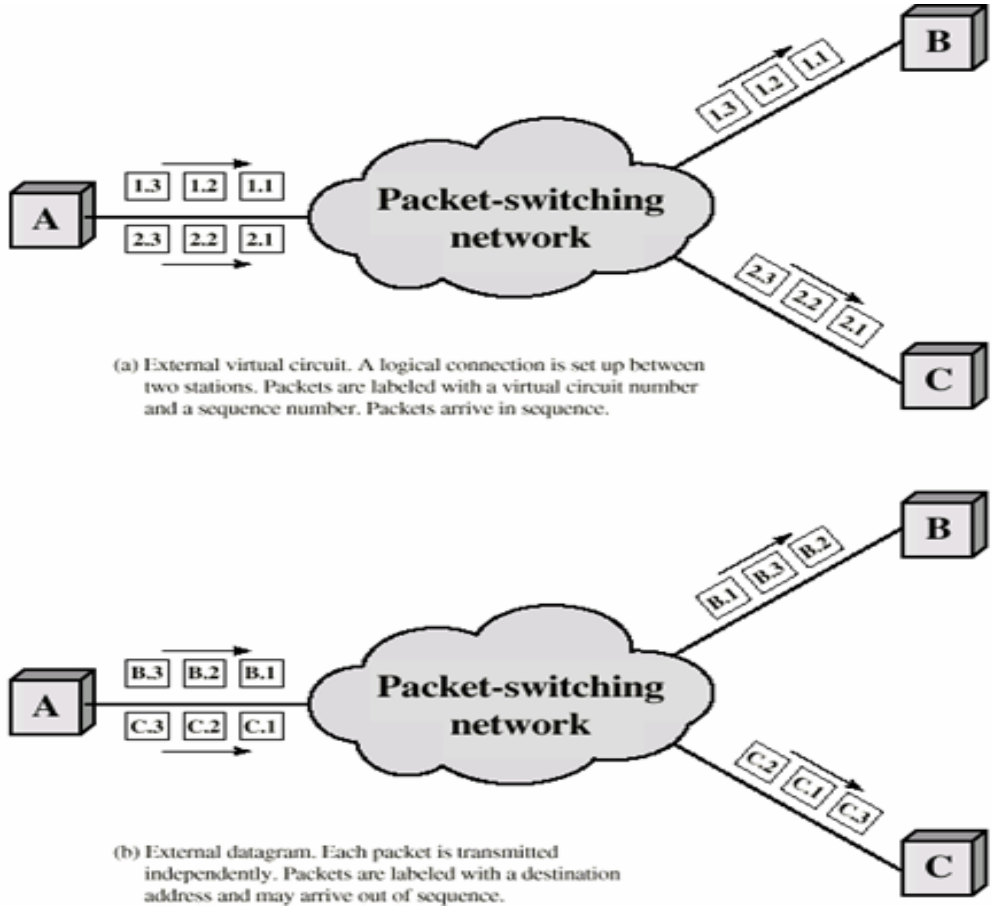
سوئیچ مداری	سوئیچ بسته ای داده گرام	سوئیچ بسته مدار مجازی
اختصاص مسیر انتقال	عدم اختصاص مسیر انتقال	عدم اختصاص مسیر انتقال
انتقال پیوسته داده	انتقال بسته ها	انتقال بسته ها
سرعت کافی جهت تعامل	سرعت کافی جهت تعامل	سرعت کافی جهت تعامل
پیامها ذخیره نمی شوند	بسته ها ممکن است تا زمان تحویل ذخیره شوند	بسته ها تا زمان تحویل ذخیره می 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 ناچیز	تاخیر انتقال بسته	تاخیر برپاسازی تماس ، تاخیر انتقال بسته
در صورت مشغول بودن تماس گرفته شده سیگنال اشغال	فرستنده ممکن است از عدم تحویل بسته آگاه شود	فرستنده متوجه می شود که اتصال رد شده است
بارگذاری اضافه ممکن است برپاسازی را مسدود کند، تاخیری برای تماسهای برپاسازی وجود ندارد	بارگذاری اضافی تاخیر تحویل بسته را افزایش می دهد	بارگذاری اضافه ممکن است برپاسازی را مسدود کند، تاخیری بسته ها افزایش می یابد
سوئیچ الکترومکانیکی یا کامپیوتری	گره های سوئیچ کوچک	گره های سوئیچ کوچک
کاربر مسئول حفظت در برابر فقدان بسته است	شبکه ممکن است مسئول بسته های جداگانه باشد	شبکه ممکن است مسئول بسته های متوالی باشد
معمولاً تبدیل سرعت یا کد ندارد	تبدیل سرعت و کد	تبدیل سرعت و کد
پهنای باند ثابت	استفاده پویا از پهنای باند	استفاده پویا از پهنای باند
بیت سربار پس از برپاسازی تماس وجود ندارد	بیتهای سربار در هر بسته	بیتهای سربار در هر بسته

جدول۶-۱: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 تصاویر۶-۴ و ۶-۵ 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 تحویل 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 می گیرد. این سرویس خارجی با مفهوم عملکرد مدار مجازی داخلی متفاوت است. یک نمونه مهم از سرویس مجازی خارجی، X.25 می باشد که در ادامه مورد بررسی قرار می گیرد.



(a) External virtual circuit. A logical connection is set up between two stations. Packets are labeled with a virtual circuit number and a sequence number. Packets arrive in sequence.

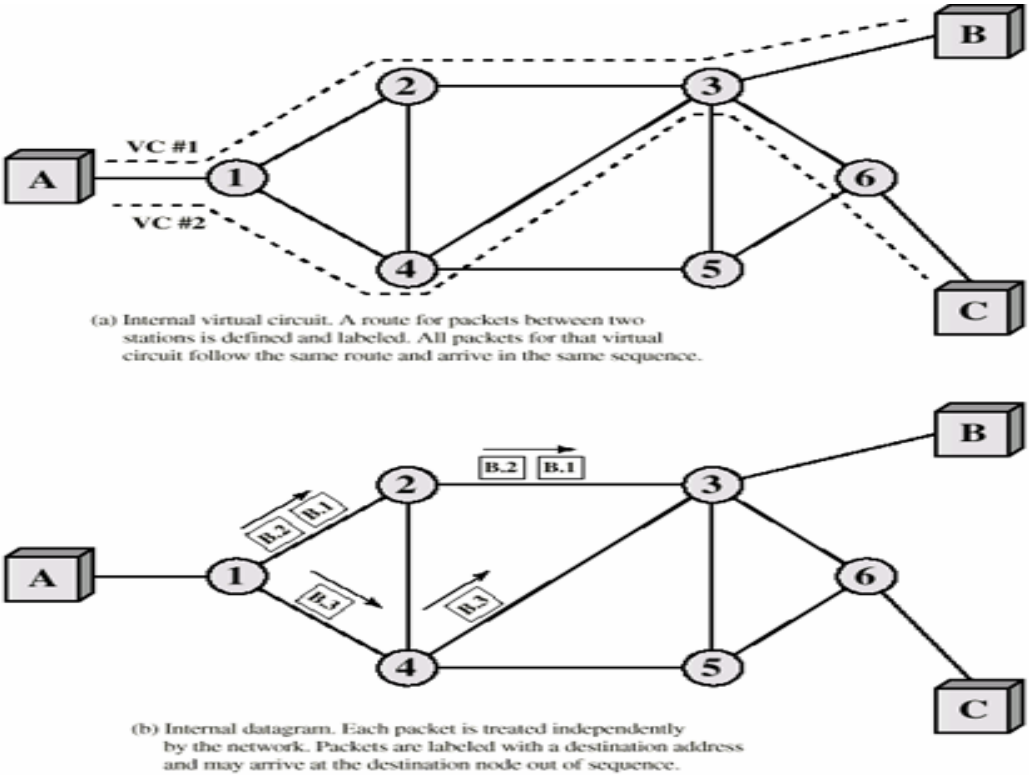
(b) External datagram. Each packet is transmitted independently. Packets are labeled with a destination address and may arrive out of sequence.

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

با سرویس بدون اتصال، شبکه بسته ها را جداگانه مدیریت می کند و ممکن است آنها را به ترتیب یا مطمئن تحویل نگیرد. این نوع سرویس، گاهی اوقات بنام سرویس داده گرام خارجی شناخته می شود 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 می کند. بنابراین بسته های متفاوت برای مدار مجازی خارجی یکسان، ممکن است مسیرهای متفاوتی داشته باشند. اگرچه، در صورت نیاز ، شبکه داده ها را در مقصد بافر می کند 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 می کند.
- داده گرام خارجی، مدار مجازی داخلی: هرچند شبکه یک اتصال منطقی را بین ایستگاه ها برای تحویل بسته برپا می کند، کاربر خارجی هیچ اتصالی را نمی بیند و بسادگی، بسته ها را یکی یکی دریافت می نماید. شبکه ممکن است اینچنین اتصالاتی را برای دوره های 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 گـرام هـردو داخلـی و یـا خـارجی، چگونه است. این موضوع به اهداف خاص طراحی برای تماسهای شبکه و ضرایب هزینه بستگی دارد. در ادامه، اقـدام به ارائه توضیحاتی در مورد معیارهای نسبی عملکرد داده گرام داخلی با مدار مجازی، می نمائیم.



(a) Internal virtual circuit. A route for packets between two stations is defined and labeled. All packets for that virtual circuit follow the same route and arrive in the same sequence.

(b) Internal datagram. Each packet is treated independently by the network. Packets are labeled with a destination address and may arrive at the destination node out of sequence.

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 بوسیله داده گرام داخلی، اجازه استفاده کارا از شبکه را می دهد. این روش نیازمند برقـراری تمـاس و نگـه داری بـسته هـا جهت ارسال مجدد آنها در زمان خطا نمی باشد. ویژگی آخر، در برخی از کاربردهای زمان واقعی مطـرح مـی گـردد. سرویس مدار مجازی می تواند توالی انتها به انتها و کنترل خطـا را فـراهم آورد. ایـن سـرویس جهـت پـشتیبانی از کاربردهای اتصال گرا همانند انتقال فایل و دسترسی از راه دور به پایانه، جذاب می باشـد. در عمـل، سـرویس مـدار مجازی متداولتر از سرویس داده گرام می باشد. اطمینـان و سـهولت یـک سـرویس اتـصال گـرا، جـذابتر از مزایـای داده گرام می باشد.

مسیریابی:

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

خصوصیات:

وظیفه مندی اولیه یک شبکه سوئیچ بسته ای، پذیرش بسته از ایستگاه مبداء و تحویل آن بـه یـک ایـستگاه مقصد می باشد. برای انجام این کار، یک مسیر در طول شبکه باید مشخص باشد. در حالت کلی، ممکن اسـت بـیش از یک مسیر وجود داشته باشد. بنابراین یک تابع مسیریابی باید اجرا شود. نیازمندیهای اولیه این تابع عبارتند از:

- صحیح بودن
- سادگی
- قوی بودن
- پایداری
- انصاف
- بهینه بودن
- موثر بودن

دو گزینه اول، خودشان خود توصیف هستند. قوی بودن به معنی آنست که شبکه توانایی تحویل 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 بدنبال قوی بودن هستند، باید از عهده نیازمندیهایی 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 دارند.

برای مثال، یک شبکه ممکن است بدلیل 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 بدهند. 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.

معیارهای کارایی	**منبع اطلاعات شبکه**
تعداد پرش	هیچ
هزینه	محلی
تاخیر	گره همسایه
بازده	گره های موجود در طول مسیر
	همه گره ها
زمان تصمیم گیری	
بسته(داده گرام)	**زمان بروزرسانی اطلاعات شبکه**
نشست(مدار مجازی)	پیوسته
	دوره ای
محل تصمیم	تغییرات عمده بارگذاری
در هر گره(توزیع شده)	تغییرات ساختار شبکه
گره مرکزی(متمرکز)	
گره آغاز کننده(منبع)	

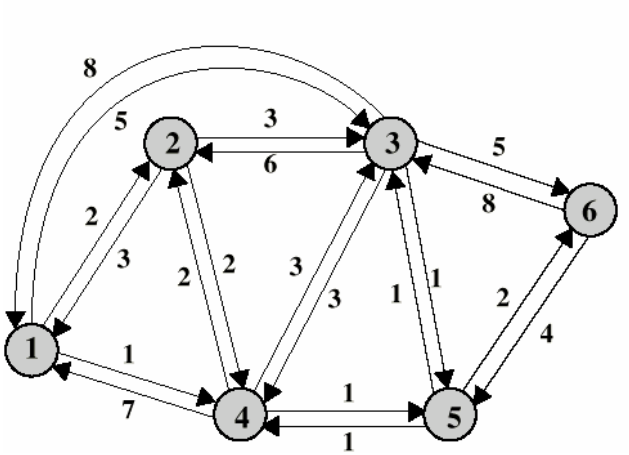
جدول ۶-۲: عناصر روشهای مسیردهی برای شبکه های سوئیچ بسته ای

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 این وجود بررسی این لیست باعث توضیح و دسته بندی مفاهیم مسیریابی می گردد.

معیارهای کارایی:

بطور کلی انتخاب یک مسیر برپایه برخی جنبه های معیارهای کارایی می باشد. یکی از ساده ترین ملاکها، انتخاب مسیر با کمترین پرش(پرش از روی کمترین تعداد گره) در طول شبکه، می باشد. این یک معیار ساده است و در آن باید مصرف منابع شبکه به حداقل برسد. هدف کلی ملاک کمترین تعداد پرش، کمترین هزینه مسیریابی می باشد. در این حالت، به هر پیوند یک هزینه تخصیص داده می شود و از این طریق برای هر زوج از ایستگاه های متصل، مسیر دورن شبکه با کمترین هزینه، براحتی محاسبه می گردد. برای مثال تصویر زیر یک شبکه را با دو خط ارتباطی بین گره های شبکه به معنی اتصال آنها و مقادیر متناسب که هزینه پیوند جاری را نشان می دهد، را توصیف می کند.

کوتاهترین مسیر از گره ۱ به ۶ ، ۶-۳-۱ با هزینه ۱۰=۵+۵ می باشد؛ اما مسیر با حداقل هزینه ۶-۵-۴-۱ با هزینه ۴=۲+۱+۱ می باشد. هزینه تخصیصی به هر پیوند جهت پشتیبانی یک یا چند هدف، طراحی می باشد. برای مثال، هزینه می تواندبصورت عکس نرخ انتقال داده باشد (نرخ داده بالاتر در یک پیوند = هزینه تخصیص پایینتر در پیوند) و یا نمایانگر تاخیر صف گذاری 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 ایستگاه ها، نسبتاً سر راست بوده و زمان پردازش باید در حد محاسبات باشد. بدلیل انعطاف پذیری بیشتر معیار حداقل هزینه، این روش متداولتر از ملاک حداقل پرش می باشد. در حال حاضر، الگوریتمهای مسیریابی کمترین هزینه متفاوتی، استفاده می شوند.

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 می گردد. زمانیکه عملکرد داخلی یک شبکه داده گرام است، تصمیم مسیریابی جداگانه برای هر بسته اتخاذ می شود. در ساده ترین حالت، همه بسته های

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 برحسب 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. عمده 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 متمرکز، 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، متغییرهای 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، تحویل داده شود، ممکن است از مسیر ۶-۵-۴-۱ 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 ۶-۵-۴-۱ ، 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[1] 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[2]، جهت وفق تصمیم مسیریابی با شرایط تغییر یافته، اطلاعات بصورت لحظه به لحظه، بروز می شوند.

---

[1] - Flooding

[2] - Adaptive

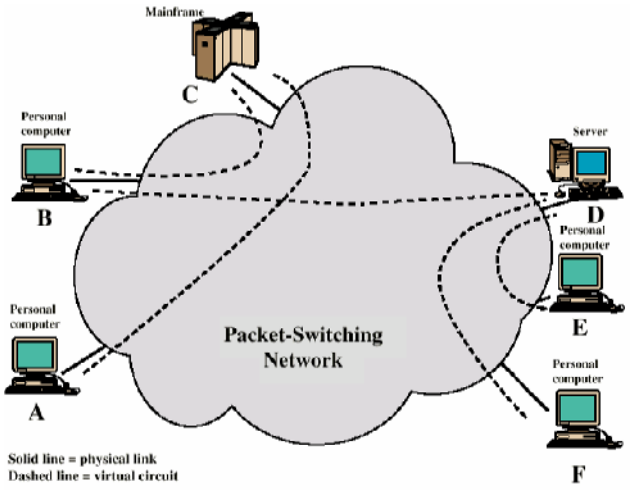
همانطور که ممکن است انتظار داشته باشید، زمانیکه اطلاعات زیادی وجود دارنـد و فرکانـسهای بروزرسـانی نیز بالا می باشد، شبکه می تواند تصمیمات مسیریابی خوبی بگیرد. از سوی دیگر، انتقال اطلاعـات، منـابع شـبکه را مصرف می کنند.

تعداد زیادی از استراتژیهای مسیریابی وجود دارند که بر روی نیازمنـدیهای مـسیریابی شـبکه هـای سـوئیچ بسته ای، بحث می کنند. بسیاری از این استراتژی ها برروی مسیریابی های بین شبکه ای نیز اعمـال شـده انـد. ۴ استراتژی کلیدی مطرح در این شبکه ها عبارتند از: ثابت، سیل آسا، اتفاقی و تطبیقی. این استراتژیها قـبلاً در فـصل ۴ مورد بررسی قرار گرفته اند.

X.25:

یکی از پروتکلهای پر استفاده X.25 می باشد که در سـال ۱۹۷۶، ارائـه شـده اسـت و از آن زمـان تـا کنـون 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 سـوئیچ بـسته ای بکـار رفتـه و در سـوئیچ 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، یـک رابـط فیزیکـی بـین یـک ایستگاه الحاقی (کامپیوتر، پایانه) و یک اتصال که ایستگاه را به گره سوئیچ بسته ای، متـصل مـی سـازد ، را معرفـی می نماید. در این استاندارد به ماشین های کاربران به عنوان ابزار پایانه[1] (DTE) و به گره های سـوئیچ بـسته ای کـه DTE به آنها متصل است را ابزار مدار پایان دار داده[2] (DCE) می گوینـد. X.25 از لایـه فیزیکـی بـا اسـتاندارد X.21 استفاده می نماید، اما استانداردهای دیگری همانند EIA-232 به عنوان جانشین نیز وجود دارند. سطح پیوند، جهـت انتقال مطمئن داده در طول اتصال فیزیکی، بوسیله ارسال داده بـصورت یـک تـوالی از فریمهـا، ایجـاد شـده اسـت.

[1] - Data Terminal Equipment
[2] - Data Circuit-terminating Equipment

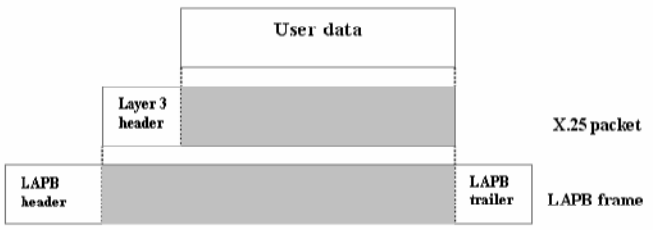
استاندارد سطح پیوند با عنوان LAPB[1](پروتکل دسترسی به پیوند متوازن)، شناخته می شود. LAPB زیر مجموعه ای از HDLC[2] می باشد.

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 ۶-۷ 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 هرکدام یک اتصال مدار مجازی به D، دارند.

تصویر ۶-۸، 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 درارتباط هستند.
- ایجاد شماره توالی[3] که می تواند جهت کنترل جریان[4] و خطا در پایه مدار مجازی، بکار می رود.

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



تصویر ۶-۸: داده های کاربر و اطلاعات کنترلی پروتکل X.25

سرویس مدار مجازی:

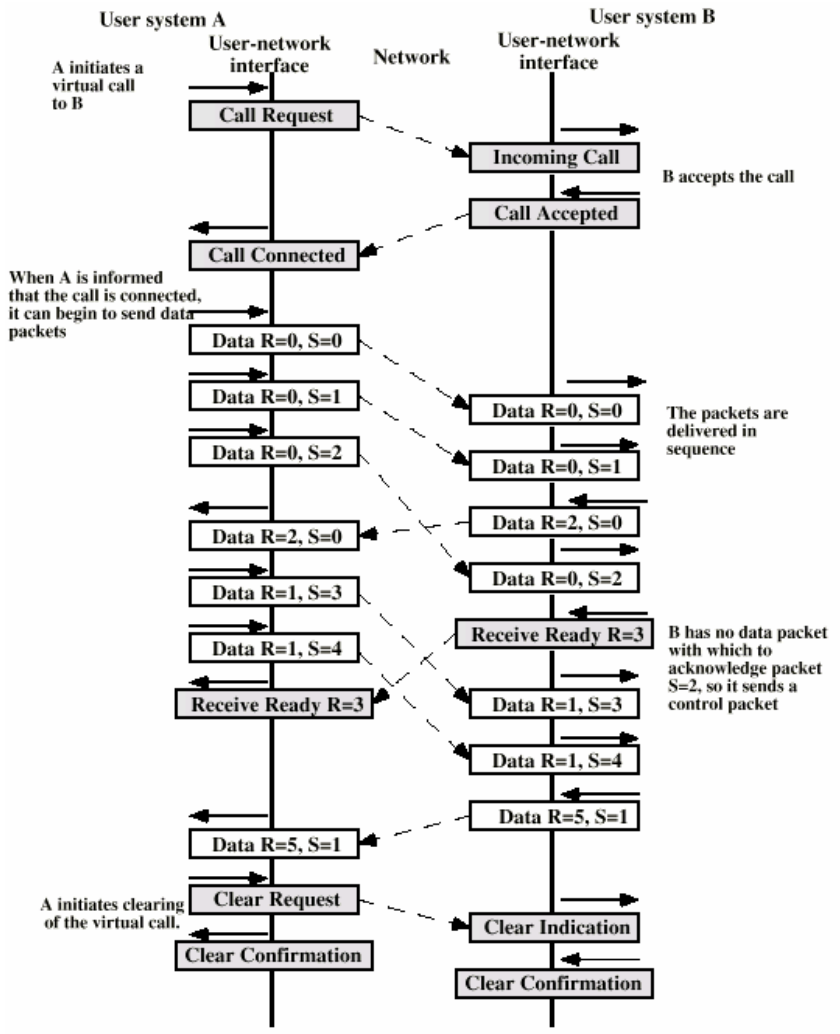
سرویس مدار مجازی X.25 برای دو نوع مدار مجازی، تهیه شده است. تماس مجازی[5] و مدار مجازی ثابت[6]. یک تماس مجازی، یک مدار مجازی برپا شده با استفاده از یک برپاسازی تماس و روال تماس خاتمه[7]، می باشد. یک مدار مجازی ثابت، یک مدار مجازی ثابت و تخصیص یافته توسط شبکه، می باشد. انتقال داده ها با تماسهای مجازی می باشد، اما نیازی به تماس برپاسازی و تماس خاتمه ، وجود ندارد.

تصویر ۶-۹، یک توالی رویداد خاص در یک تماس مجازی را نمایش می دهد. بخش سمت چپ تصویر، مبادله بسته ها بین ماشین کاربرA 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:

---

[1] - Link Access Protocol Balanced
[2] - High Level Data Link Control
[3] - Sequence Number
[4] - Flow
[5] - Virtual Call
[6] - Permanent Virtual Circuit
[7] - Call Clearing Procedure



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

۱- A درخواست یک مدار مجازی را از B، با ارسال یک بسته درخواست تماس به DCE A، اعلام می نماید. بسته شامل آدرسهای مبداء 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 B، هدایت می کند.

۳- DCE B، 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 DCE 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 A، 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.

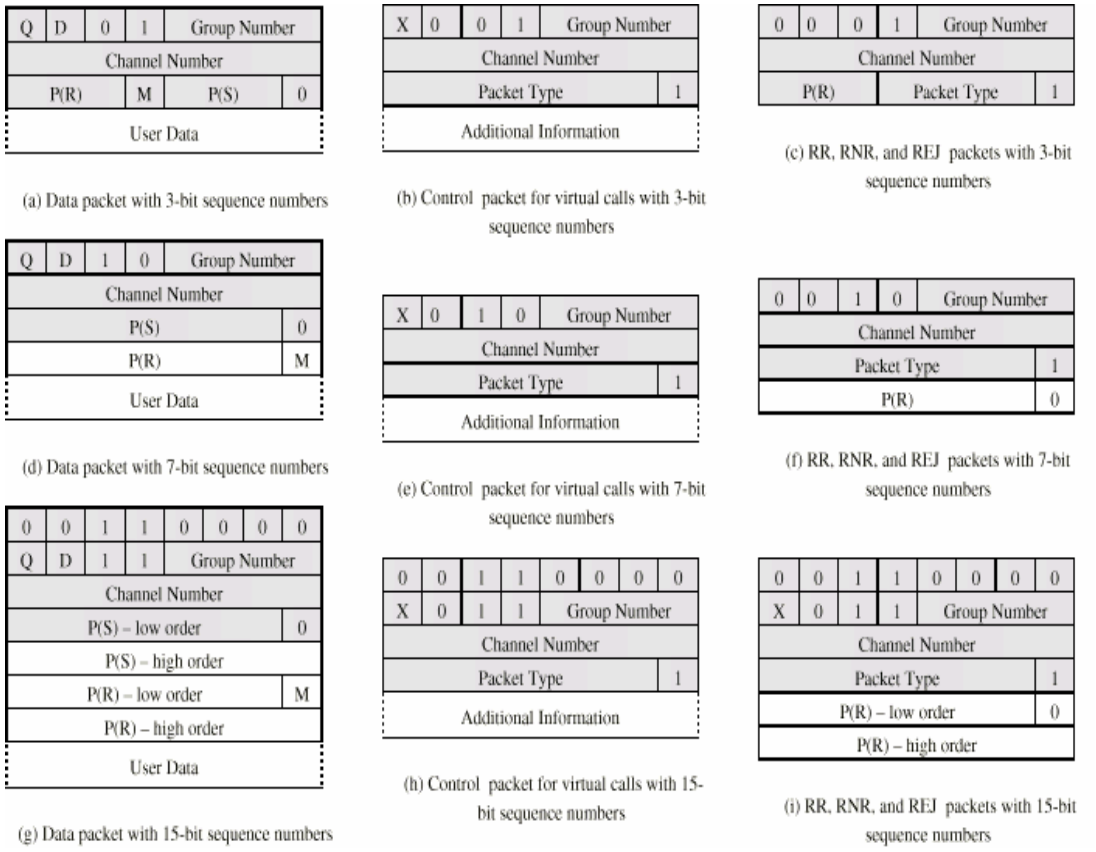
۷- A (یا B)، یک بسته درخواست خاتمه را برای خاتمه مدار مجازی، ارسال می کند و یک بسته تایید خاتمه را دریافت می نماید.

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 حداکثر، تقسیم شده و یک سرآیند ۲۴، ۳۲ 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 0011000، 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 خطا را در پایه های مدار مجازی، پشتیبانی می کنند. بیت Q، در استاندارد تعریف نشده است، اما به کاربر توانایی تشخیص دو نوع داده را می دهد.

بعلاوه جهت انتقال داده کاربر، X.25 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:



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 DTE تماس گیرنده و تماس گرفته شده.

- امکانات: یک توالی از مشخصات امکانات. هر مشخصه یک از یک کد امکانات ۸ بیتی و یا بیـشتر و صفر یا بیشتر کدهای پارمتر، تشکیل شده است. یک مثـال از امکانـات، مطالبـه هزینـه معکـوس[1] می باشد.

جدول ۶-۳ بسته های X.25 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 بـرای بـسته هـای داده را از مسیر فرعی عبور دهد. بسته وقفه ، بوسیله شبکه، با اولویت بالاتر نسبت به بسته های داده، به DTE مقـصد تحویـل 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 نمـی کنـد، بکار می رود. بسته های ثبت برای درخواست و تایید امکانات X.25، بکار می روند.

پارامترها	سرویس		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،کدخطا،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 خطا	X	X	اعلام بازنشانی	درخواست بازنشانی
-	X	X	تایید بازنشانی	تایید بازنشانی
آغاز دوباره				
دلیل آغاز مجدد، کد خطا	X	X	اعلام شروع مجدد	درخواست شروع مجدد
-	X	X	تایید شروع مجدد	تایید شروع مجدد
خطایاب				
کد خطا، توصیف خطا	X	X	خطایاب	

جدول۶-۳: انواع بسته ها و پارامترهای آنها

مالتی پلکس کردن[2]:

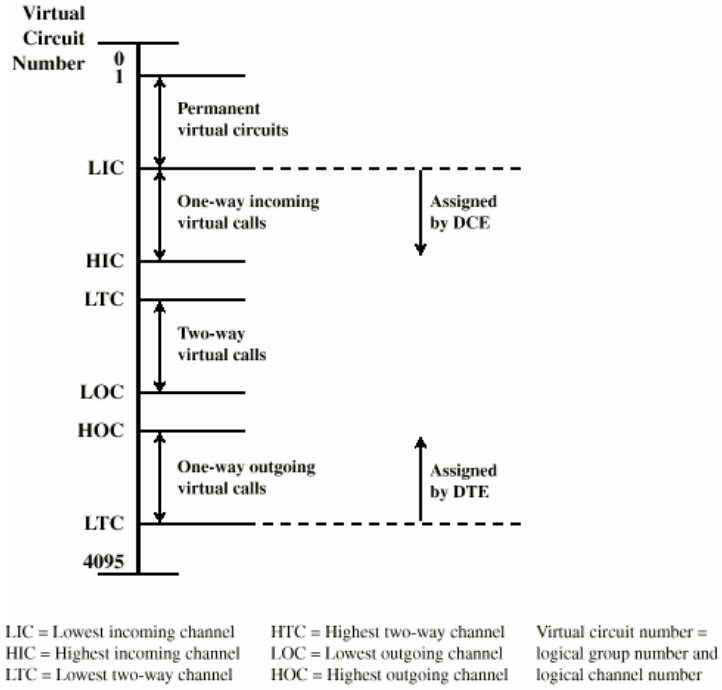
[1] Reverse Charging -

[2] Multiplexing -

شاید مهمترین سرویس ارائه شده در X.25، مالتی پلکس باشد. DTE A، اجازه برپاسازی ۴۰۹۶ مدار مجازی همانند با سایر DTE ها را برروی 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[1] را 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 ۶-۱۱ تبعیت می کند. شماره صفر اغلب رزرو شده و جهت تشخیص بسته های عمومی برای همه مدارات مجازی ، بکار می رود. شماره دامنه های متوالی 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 ها 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 DTE،یک 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 DTE و DCE 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.



تصویر ۶-۱۱: تخصیص شماره مدار مجازی

کنترل جریان و خطا:

کنترل جریان و خطا 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.

P(S) بوسیله DTE 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 برروی یک مدار مجازی، یکی بیشتر از مقدار بسته قبلی روی آن مدار می باشد(ماژول ۸، ۱۲۸ و یا ۳۲۷۶۸). P(R)، شامل شماره بسته بعدیی است که از طرف دیگر یک مدار مجازی، انتظار دریافت آن وجود دارد. این روش جهت تایید سوار بر پشت[1]، 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 پنجره 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 P(R) در بسته داده RR و یا RNR است و بنابراین کنترل جریان، ممکن است معنای محلی و یا انتها به انتها، برپایه تنظیمات بیت D، را باشد. زمانیکه D=0(حالت عمده)، تایید بین DTE و شبکه، بکار می رود. وقتی D=1 است، تایید از DTE راه دور می رسد.

طرح کنترل خطا برگشت -N ARQ می باشد. تایید منفی به معنی یک ردکردن[2](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**[3] 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 بسته با تایید E-E میانی				نمونه توالی های بسته						
				توالی ترکیبی			توالی اصلی			
	D	M	نوع بسته	D	M	نوع بسته	D	M	نوع بسته	
*	0	1	A	0	1	A	0	1	A	
	0	1	A				0	1	A	
	0	1	A	0	1	A	0	1	A	
	1	0	B				0	1	A	
*	0	1	A	1	0	B	0	1	A	
	0	1	A				1	0	B	
	1	0	B	توالی قطعات						
*	0	1	A							
	0	1	A	0	1	A	0	0	0	B
	1	0	B	0	0	B				
پایان توالی				*: گروهی از قطعات که می تواند ترکیب گردند.						

جدول ۶-۴: توالی بسته X.25

[1] - Piggyback Acknowledgment

[2] - Reject

[3] - Complete Packet Sequence

برای مشخص کردن این مکانیزم، X.25 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 بیتهای M و D، بستگی دارد. اگر D=1، یک تایید انتها به انتها بوسیله DTE دریافت کننده به DTE 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 انتها، قبل از خاتمه توالی بزرگتر، استفاده نماید.

جدول ۶-۴، 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[1] و آغاز دوباره[2]:

X.25 ، دو امکان را جهت بازیابی از خطا، 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 خطا 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 X.25 DTE-DCE، پشتیبانی نماید. DTE و یا DCE 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 مقابل می 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 DTE و یا DCE 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 داه 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 کانال مجازی. با کانالهای مجازی داخلی، یک مسیر بین دو نقطه انتهایی تشکیل می گردد و همه بسته ها برای آن کانال

---

[1] Reset-

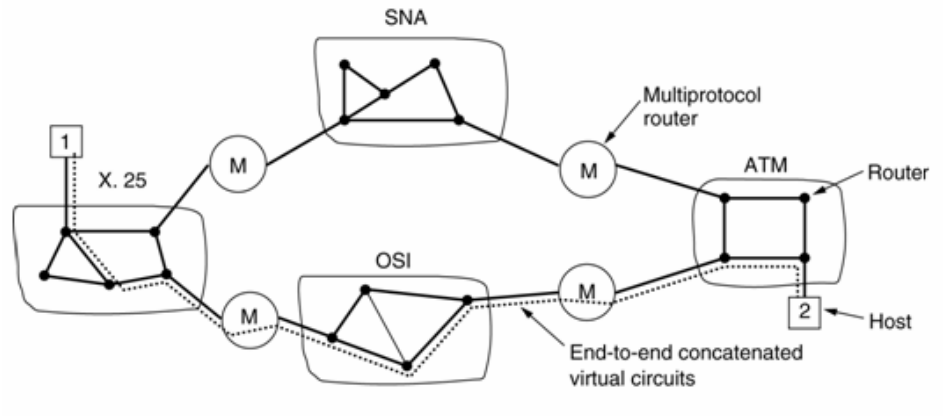
[2] Restart -

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.

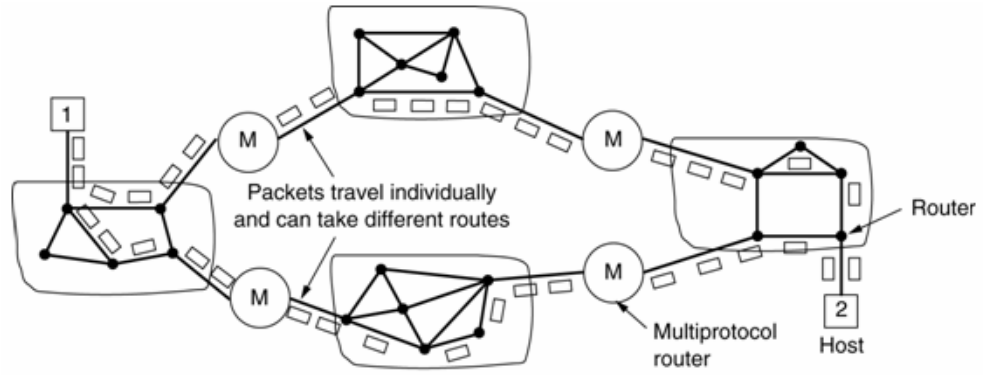
یک تابع مسیریابی در یک شبکه سوئیچ بسته ای، سعی در یافتن کم هزینه ترین مسیر در شبکه می کند که هزینه های آن شامل تعداد پرش، تاخیر مورد انتظار و سایر پارامترها می باشد. الگوریتمهای مسیریابی قابل تطبیق، براساس تبادل اطلاعات شرایط ترافیکی بین گره های شبکه عمل می کنند.

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 مجازی با سوئیچ بسته ای داده گرام کمک می کند. در تصویر ۶-۱۲ 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 ۶-۱۳، انتقال داده ها بین میزبانهای ۱ و۲، این بار با استفاده از شبکه های سوئیچ بسته ای داده گرام، انجام می گیرد. در این حالت بدلیل 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 ۶-۱۲: انتقال داده ها با روش سوئیچ داده مدار مجازی



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

فصل ۱۱:

شبکه های ATM و FrameRelay

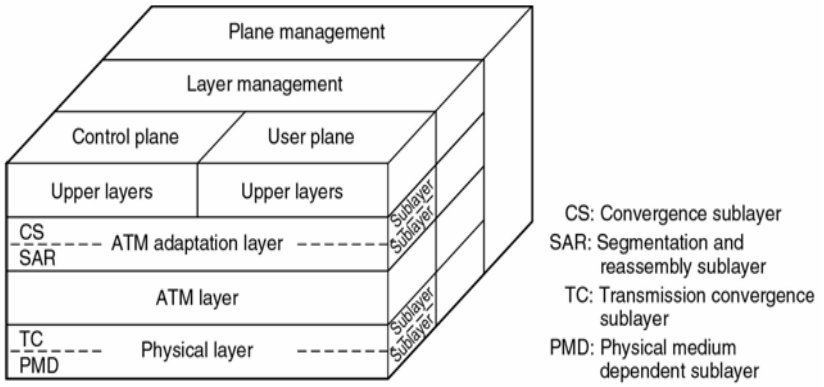
ATM[1]که با نام بازپخش سلول[2] نیز شناخته می شود، از مزایای قابلیت اعتماد و وفاداری امکانات دیجیتال مدرن برای تهیه سوئیچ بسته ای سریعتر از X.25، استفاده نموده است. ATM در ابتدا به عنوان بخشی از کار برروی شبکه های باند گسترده ISDN، توسعه داده شد؛ اما پس از آن کاربردهایی را در محیطهای غیر ISDN که نیازمند ارسال داده با نرخ بسیار بالا بودند، یافت.

ما با بحث در مورد جزئیات طرح ATM شروع کرده و سپس مفاهیم مهم لایه های تطبیق ATM(ALL[3]) را بررسی کرده و سرانجام مروری داریم بر یک طرح قدیمی تر، اما هنوز پر استفاده بنام FR، داریم.

۷-۱:معماری پروتکل:

ATM به شیوه ای مشابه با سوئیچ بسته ای X.25 و FR، عمل می کند. همانند سوئیچ بسته ای و FR، ATM داده ها را با قطعات بزرگ مجزا، منتقل می نماید. همچنین همانند سوئیچ بسته ای و FR، ATM نیز اجازه ایجاد چندین اتصال منطقی را جهت مالتی پلکس داده ها برروی یک واسط فیزیکی را مجاز می شمارد. در ATM، جریان اطلاعات در هر اتصال منطقی در بسته های با طول ثابت بنام سلول، سازماندهی می گردد.

ATM یک پروتکل ساده و موثر با حداقل قابلیتهای کنترل خطا و جریان، می باشد. این امر باعث کاهش سربار پردازش سلولهای ATM شده و سربار تعداد بیتهای مورد نیاز در هر سلول را نیز کاهش می دهد و بنابراین ATM با نرخهای داده بالا عمل می نماید. بعلاوه استفاده از سلول های با طول ثابت، پردازش مورد نیاز در هر گره ATM را ساده تر نموده است، که این خود جهت پشتیبانی از نرخ داده بالا در ATM، بکار می رود.



تصویر ۷-۱: معماری پروتکل ATM

استاندارد ATM که بوسیله ITU-T ارائه شده است، برپایه ساختار معماری نشان داده شده در تصویر ۷-۱ ، می باشد که یک معماری پایه را برای یک رابط بین کاربر و شبکه تشریح می نماید. لایه فیزیکی شامل مشخصاتی از یک محیط انتقال و یک طرح رمزنگاری سیگنال، می باشد. دامنه نرخ داده در لایه فیزیکی بین 25.6 Mbps تا 622.08 Mbps می باشد.نرخ های داده دیگر، بالاتر یا پایین تر، نیز ممکن می باشند.

دو لایه از معماری پروتکل، به توابع ATM مربوط می گردند. یک لایه عمومی ATM جهت تمام سرویسها وجود دارد که تواناییهای انتقال بسته را فراهم می آورد و یک لایه تطبیق ATM که وابسته به سرویس می باشد. لایه ATM، انتقال داده در سلولهای با طول ثابت و استفاده از اتصالات منطقی را توصیف می نماید. استفاده از ATM، نیاز به یک لایه تطبیق برای پشتیبانی از پروتکلهای انتقال داده ای که برپایه ATM نیستند را بوجود می آورد. AAL،

---

[1] - Asynchronous Transfer Mode

[2] - Cell Relay

[3] - ATM Adapation Layer

اطلاعات لایه های بالاتر را جهت انتقال بر روی یک شبکه ATM را به سلولهای ATM، نگاشت مـی کنـد و در پایـان 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 کنتـرل خطـا و جریـان، فـراهم 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 سیـستم بطـور کامـل اعمـال 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 پروتکلهایش می شود.

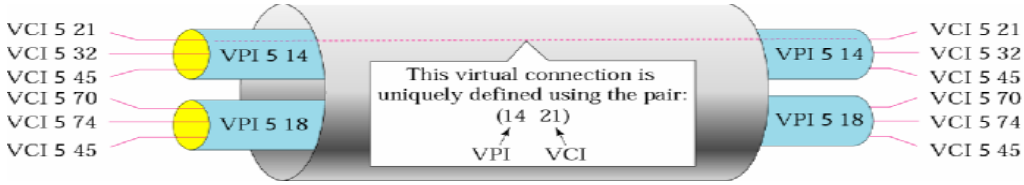
OSI layer	ATM layer	ATM sublayer	Functionality
3/4	AAL	CS	Providing the standard interface (convergence)
		SAR	Segmentation and reassembly
2/3	ATM		Flow control Cell header generation/extraction Virtual circuit/path management Cell multiplexing/demultiplexing
2	Physical	TC	Cell rate decoupling Header 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

۷-۲: اتصالات منطقی ATM:

اتصالات منطقی ATMبه عنوان اتصالات کانال مجازی(VCC[1]) نیز شناخته می شـود. یـک VCC، یـک طـرح قابل مقایسه با مدار مجازی در X.25 می باشد و واحد پایه سوئیچ در یک شبکه ATM می باشد. یـک VCC، بـین دو کاربر نهایی از طریق شبکه و یک نرخ متغییر جریان دو طرفه از سلولهای با طول ثابـت کـه در طـول شـبکه مبادلـه می شوند، برپا می شود. VCC همچنین برای تبادلات کاربر-شبکه (سـیگنالهای کنترلـی) و تبـادلات شـبکه-شـبکه (مدیریت و مسیردهی شبکه) نیز بکار می رود.

برای ATM، یک زیر لایه دوم پردازشی نیز تعریف شده است که مفاهیم مسیر مجـازی را مطـرح مـی نمایـد (تصویر ۷-۲). یک اتصال مسیر مجازی(VPC[2])، یک مجموعه از VCCهـا مـی باشـدکه نقـاط انتهـایی مـشابه دارنـد. بنابراین همه جریانهای سلولها برروی همه VCCها در یک VPC تنها، با یکدیگر سوئیچ می شوند.



تصویر ۷-۲: روابط اتصال ATM

مفهوم مسیر مجازی جهت پاسخ به روند شبکه با سرعت بـالا، توسـعه داده شـده کـه در آن، هزینـه کنتـرل شبکه، رشد کمتری را در برابر رشد هزینه سراسری شبکه، فراهم مـی آورد. تکنیـک مـسیر مجـازی بـا گـره بنـدی 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 برروی تعداد کمی از گروه های اتصالات، بجای تعداد زیادی از اتصلات منفـرد، اعمـال شوند.

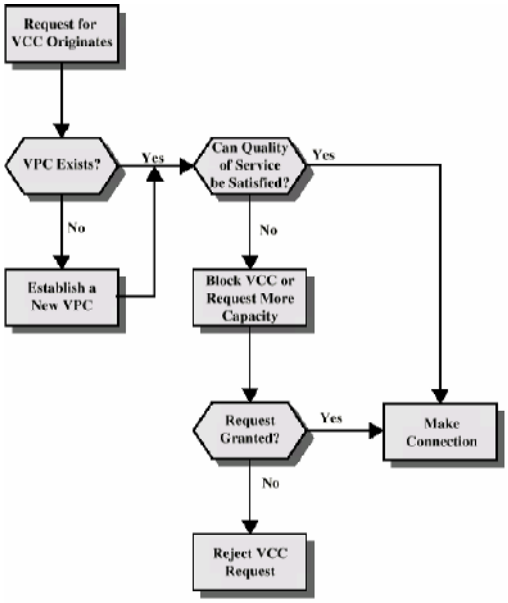
چند مزیت استفاده از مسیرهای مجازی در زیر لیست شده اند:

- توسعه کارایی و قابلیت اطمینان شبکه: شبکه با تعداد کمتری موجودیت سروکار دارد.
- کاهش پردازش و زمان برپاسازی اتصال کوتاه: بیشتر کار زمانی انجام می شود کـه مـسیر مجـازی برپا می گردد. با معکوس کردن ظرفیت یک اتصال مجازی در پیش بینی سـایر تماسـهای بعـدی، اتصالات کانال مجازی جدید می توانند با اجرای توابع کنترلی ساده در نقاط انتهایی اتـصال مـسیر مجازی، برپا شوند و پردازش تماس در عبور از گره ها، مورد نیاز نیست. بنابراین افـزودن کانالهـای مجازی جدید شامل حداقل پردازش می گردد.
- توسعه سرویسهای شبکه: مسیرمجازی در درون شبکه بکار می رود، اما برای کاربر نهایی نیز قابـل مشاهده است. بنابراین کـاربر ممکـن اسـت گـروه هـای کـاربری بـسته یـا شـبکه هـای بـسته از مجموعه ای از کانالهای مجازی را تعریف نماید.

تصویر ۷-۳ یک مسیر کلی پردازش برپاسـازی تمـاس، بـا اسـتفاده از کانالهـا و مـسیرهای مجـازی را نـشان می دهد. پردازش برپاسازی یک اتصال مسیر مجازی از طرف پردازش برپاسازی یک اتصال کانال مجازی منحصربفرد ، مجزا شده است:

- مکانیزمهای کنترل مسیر مجازی شامل محاسبه مـسیرها، تخـصیص ظرفیـت و ذخیـره اطلاعـات وضعیت اتصال می باشد.
- جهت برپاسازی یک کانال مجازی، ابتدا باید یک اتصال مسیرمجازی به گره مقـصد مـورد نظـر بـا ظرفیت موجود به حد کافی، جهت پشتیبانی از کانال مجازی، با کیفیت سـرویس مقتـضی، وجـود داشته باشـد. یـک کانـال مجـازی بوسـیله ذخیـره اطلاعـات وضـعیت مـورد نیـاز(نگاشـت کانـال مجازی/سرویس مجازی)، برپا می شود.

واژه شناسی مسیرمجازی و کانالهای مجازی در جـدول ۷-۲، بطـور خلاصـه آمـده اسـت. از آنجائیکـه اکثـر پروتکلهای لایه شبکه مورد بحث، تنها به رابط کاربر-شبکه مرتبط می باشد، مفاهیم مسیر مجـازی و کانـال مجـازی معرفی شده در توصیه نامه ITU-T، به هر دو رابط کاربر-شبکه و اعمال دورن شبکه ای، اشاره دارد.



تصویر ۷-۳: 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، سلول ها با همان ترتیبی تحویل داده می شوند که ارسال شده اند. اجازه بدهید سه کاربرد 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 سلول های 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، گسترده شده است. VCC ها 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 منحصربفرد
اتصال مسیر مجازی(VPC)	یک اتصال از پیوندهای VP گسترده 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 ITU-T I.150، خصوصیات زیر را برای اتصلات کانال مجازی ذکر می کند:

- کیفیت سرویس: یک کاربر یک VCC، بوسیله کیفیت سرویس تعیین شده بوسیله پارامترهایی همانند نرخ گم شدن سلول ها منتقل شده و بازه تغییرات تاخیر سلول، فراهم شده است.

- اتصالات کانال مجازی سوئیچ شده و دارای مدت محدود[1]: 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[2]: پارامترهای ترافیکی می توانند بین یک کاربر و شبکه برای هر VCC،مورد بحث قرار گیرند. سلولهای ورودی به VCC بوسیله شبکه مورد 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 VCCهای جدید، گفتگو کنند. خصوصیات VPC، یک سیاست برمبنای 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 VCCهای مورد استفاده در مدیریت شبکه ، مشاهده نمود.

سیگنال دهی کنترل[3]:

در ATM، مکانیزمی جهت برپاسازی و انتشار VPCها و VCCها 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 VCCها، I.150 ۴ 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- VCCهای 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 بدلیل نیاز ما به یک کانال ثابت، شاید با نرخ پایین، می توان از آن جهت برپاسازی VCCهای که می تواند جهت کنترل تماس بکار رود، استفاده کرد. چنین کانالهایی یک کانال Metasignaling نامیده می شود ، که جهت برپاسازی کانالهای سیگنال دهی مورد استفاده قرار می گیرد.

۳- کانال Metasignaling، می تواند جهت برپاسازی VCCها بین کاربر و شبکه ، برای سیگنال دهی کنترلی، بکار می رود. این کانال مجازی سیگنال دهی کاربر به شبکه، می تواند جهت برپاسازی VCCها، جهت حمل داده های کاربر بکار رود.

۴- همچنین کانال Metasignaling، می تواند جهت برپاسازی کانال سیگنال دهی کاربر به کاربر نیز ، بکار رود. اینچنین کانالی باید در یک VPC پیش برپاشده، برپا گردد. این موضوع می تواند جهت مجاز ساختن کاربران نهایی، بدون دخالت شبکه، جهت برپاسازی و انتشار VCCهای کاربر به کاربر جهت حمل داده های کاربر، بکار رود.

برای VPCها، سه روش[1] در I.150، تعریف شده است:

۱- یک VPC می تواند برمبنای یک مدت محدود، بوسیله توافق قبلی، برقرار گردد. در این حالت سیگنال دهی کنترلی وجود ندارد.

۲- برپاسازی/انتشار VPC، می تواند بصورت کنترل شده توسط مشتری باشد. در این حالت مشتری از یک سیگنال دهی VCC، برای درخواست VPC، استفاده می نماید.

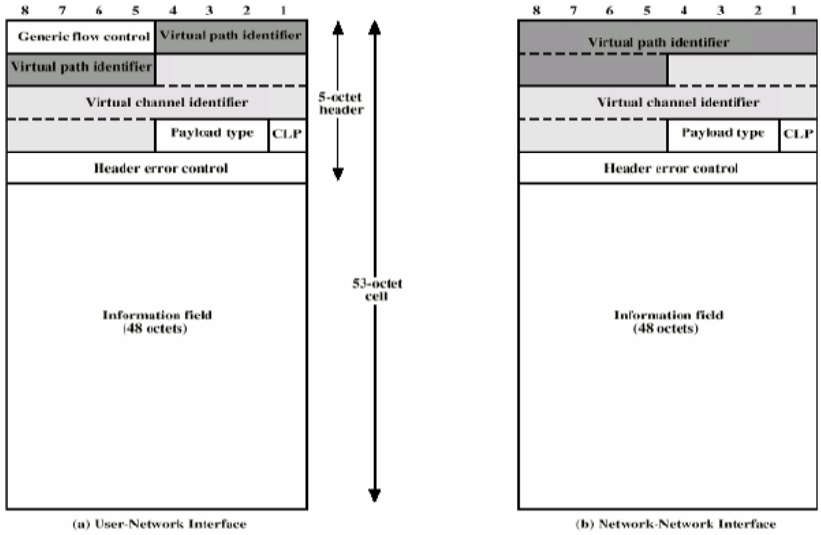
۳- برپاسازی/انتشار VPC، ممکن است بصورت کنترل شده توسط شبکه باشد. در این حالت، یک VPC را برای راحتی خودش برپا می کند. مسیر ممکن است شبکه به شبکه، کاربر به شبکه و یا کاربر به کاربر، باشد.

۷-۳: سلولهای ATM

ATM از سلولهایی با طول ثابت استفاده می کند که ۵ بایت آن سرآیند و ۴۸ بایت بخش داده آن می باشد. چندین مزیت در استفاده از سلولهای کوچک و با طول ثابت، وجود دارد. اول آنکه استفاده از سلول های کوچک می تواند تاخیر صف گذاری را برای سلول های با اولویت بالا، کاهش دهد؛ زیرا چنین سلولی اگر با فاصله زمانی کوتاهی پس از یک سلول با اولویت پایین تر ، از راه برشد، می تواند دستیابی به یک منبع، همانند انتقال دهنده را بدست آورد. دوم آنکه واضح است سلولهای با طول ثابت، با کارایی بالاتری می توانند سوئیچ شوند، که این برای نرخ داده بالای ATM ، بسیار مهم است. با سلولهای با طول ثابت، پیاده سازی مکانیزم سوئیچ در سخت افزارها، ساده تر می گردد.

---

[1] - 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[1])، 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[2]) و پایانه های نرخ بیتی متغییر(VBR[3])، می گردد که یک عنصر ظرفیت تظمین شده، دارند(CBR و VBR در بخش ۷-۵، توضیح داده شده اند). مکانیزم کنونی GFC در ادامه توضیح داده شده است.

کد PT	تفسیر		
000	سلول داده کاربر	بدون تراکم	نوع SDU=0
001	سلول داده کاربر	بدون تراکم	نوع SDU=1
010	سلول داده کاربر	با تراکم	نوع SDU=0
011	سلول داده کاربر	با تراکم	نوع SDU=1
100	سلول OAM دار سگمنت		
101	سلول OAM دار انتها به انتها		
110	سلول مدیریت منابع		
111	رزرو شده جهت توابعی آتی		

OAM:Operation,Administration,Maintenance SDU:Service Data Unit

جدول۷-۳: تفسیرکدهای فیلد نوع Payload

[1] Generic Flow Control -
[2] Constant Bit Rate -
[3] Variable Bit Rate -

شناسه مسیر مجازی(VPI[1])، 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 کانال مجازی(VCI[2])، برای مسیردهی از/به 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[3])، 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 ۴۸ 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 VCCهای کاربر را بدون تاثیر بر داده های کاربر، فراهم می آورد. بنابراین فیلد PT می تواند اطلاعات کنترلی درونی را فراهم آورد.

بیت اولویت فقدان سلول(CLP[4])، می تواند به عنوان راهنمایی برای شبکه در حین تراکم، مورد استفاده قرار بگیرد. مقدار صفر نشانگر آنست که سلول اولیت 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 نرخ توافق شده) را به شبکه وارد کند، با CLP یک، تا درصورت عدم وجود تراکم در شبکه، به مقصد تحویل 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 سوئیچی 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 بدهد، 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 خطا و 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[5])، 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[6])، در یک ATM WAN می باشد. مخصوصاً، CCT نامزد تهیه سرویس خوب برای ترافیک های انفجاری با حجم بالا با طول پیام متغیر، می باشد.

---

[1] - Virtual Path Identifier
[2] - Virtual Channel Identifier
[3] - Service Data Unit
[4] - Cell Loss Priority
[5] - User-Network Interface
[6] - Controlled Cell Transfer

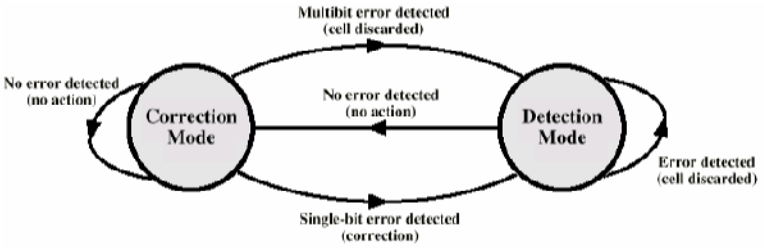
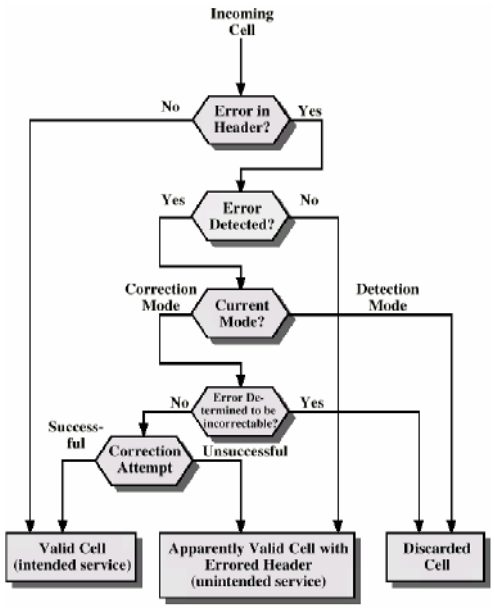


Figure 11.5 HEC Operation at Receiver

تصویر ۷-۵: عملکرد HEC در دریافت کننده

کنترل خطای سرآیند:

هر سلول ATM، شامل ۸ بیت کنترل خطای سرآیند(HEC[1]) می باشد که برپایه 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 موجودکه شامل فیلد کنترل خطا هستند، همانند HDCL، داده هایی که بعنوان ورودی محاسبه در خطا بکار می روند ، بسیار بزرگتر از اندازه کد خطای نتیجه می باشد. این امر تشخیص خطای کد را 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 بدلیل وجود افزونگی کافی در کد، جهت بازیابی الگوهای خطای خاص، می باشد.



تصویر ۷-۶: تاثیر خطا بر سرآیند سلول

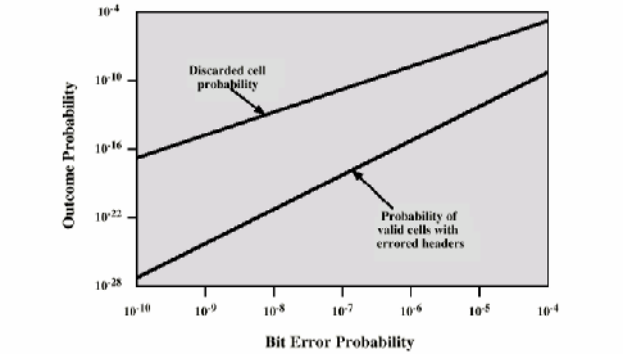
تصویر ۷-۵، عملکرد الگوریتم HEC را در دریافت کننده، نشان می دهد. در ابتدا، الگوریتم تصحیح خطای دریافت کننده در حالت پیش فرض برای تصحیح یک بیت خطا، می باشد. با ورود هر سلول، محاسبه مقدار HEC، انجام می گیرد. مادامیکه خطایی تشخیص داده نشود، دریافت کننده، در حالت تصحیح خطا باقی می ماند. زمانیکه یک خطا تشخیص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

[1] - Header Error Control

بیت خطا وجود داشته باشد، آن را تشخیص می دهد. در این حالت دریافت کننده به حالت تشخیص می رود . در این حالت تلاشی در جهت تصحیح خطا انجام می گیرد. دلیل این تغییر آنست که یک اختلال انفجاری و یا رویداد دیگر، ممکن است باعث مجموعه متوالی از خطاها می باشد، حالتی که HEC، جهت تصحیح کد ناکافی می باشد. دریافت کننده مادامیکه سلولهای خطادار دریافت می گردد، در حالت تشخیص باقی می ماند. زمانیکه یک سرآیند، آزموده شده و خطایی در آن یافت نشد، دریافت کننده، دوباره به حالت تصحیح برمی گردد. فلوچارت تصویر ۷-۶، پی آمد خطاها را در سرآیند سلول، نمایش می دهد.

تابع حمایت در برابر خطا، بازیابی از خطاهای تک بیتی سرآیند و احتمال پایین تحویل بسته های با سرآیند معیوب، تحت شرایط خطاهای انفجاری را فراهم می آورد. خصوصیت خطا سیستم های انتقال فیبری، ترکیبی از خطاهای تک بیتی و انفجاری بزرگ، می باشد و برای برخی سیستم های انتقال، توانایی تصحیح خطا، بدلیل وقتگیر بودن آن، ممکن است حذف شود.

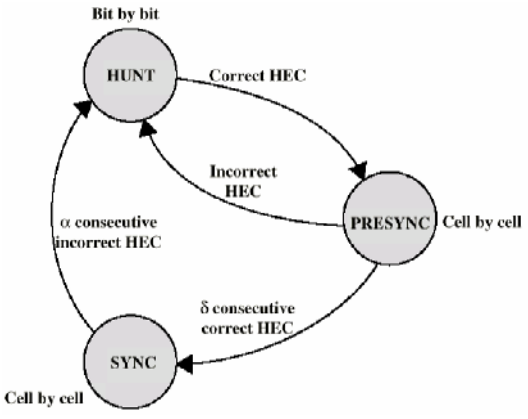
تصویر ۷-۷، برپایه I.432 ITU-T، می باشد و نشان می دهد که چگونه خطاهایی بیتی اتفاقی بر احتمال وقوع سلولهای دور ریخته شده و سلولهای معتبر با سرآیند معیوب، در زمان استفاده از HEC، تاثیر می گذارد.



تصویر ۷-۷: احتمال خطای بیتی

۷-۴: انتقال سلولهای ATM

I.432، بیان می کند که سلولهای ATM و یکی از چند نرخ داده 622.08 Mbps، 155.52 Mbps، 51.84 Mbps و یا 25.6 Mbps ، ممکن است منتقل شوند. ما نیازمند تعیین ساختار انتقال مورد استفاده جهت حمل Payloadها، می باشیم. 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:

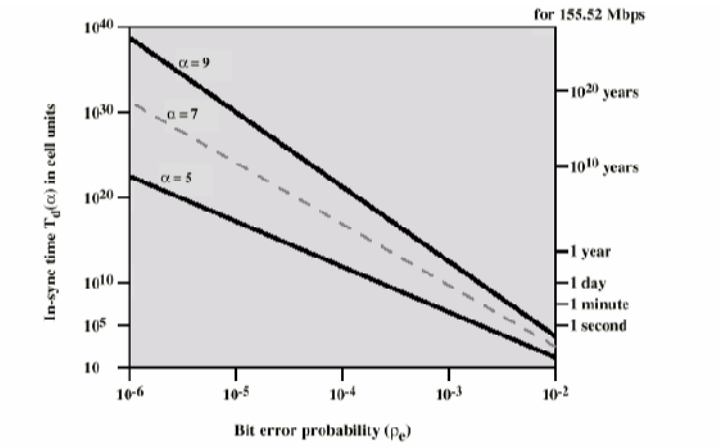
برای لایه فیزیکی برپایه سلول هیچ چهارچوب گذاریی، تحمیل نمی شود. ساختار رابط شامل جریان سلولهای ۵۳ بایتی است. بدلیل عدم وجود چهارچوب خارجی تحمیلی در روش مبتنی بر سلول، برخی از فرمهای همزمانی لازم می باشد. همزمانی بر مبنای فیلد کنترل خطای سرآیند(HEC)، در سرآیند سلول، بدست می آید. روال این جریان به شکل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

۱- در موقعیت HUNT، یک الگوریتم توصیف[1]، 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 متوالی قانون رمزگذاری را تایید می نماید.

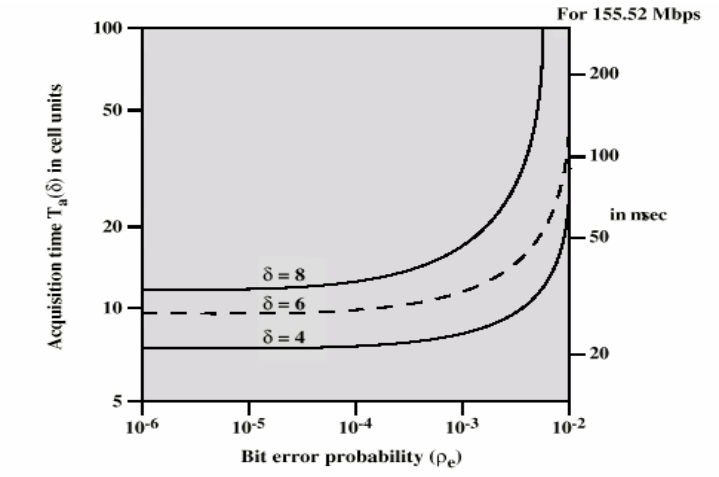
۳- در حالت SYNC، HEC جهت تشخیص و تصحیح خطا بکار می رود و سلول توصیف شده در صورت تشخیص α مرتبط خطای متوالی توسط HEC، از دست رفته تلقی می شود.

مقادیر δ و α ، پارمترهای 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 ۷-۹ و ۷-۱۰ برپایه I.432، تاثیر 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 خطا، حفظ می نماید(با α ، بعنوان یک پارامتر). تصویر دوم نشاندهنده میانگین زمانی، برای بدست آوردن همزمانی، بعنوان تابعی از نرخ خطا، می باشد(با δ ، بعنوان یک پارامتر).



تصویر۷-۹: تاثیر خطاهای بیتی اتفاقی برروی توصیف کارایی سلول

[1] Delineation -



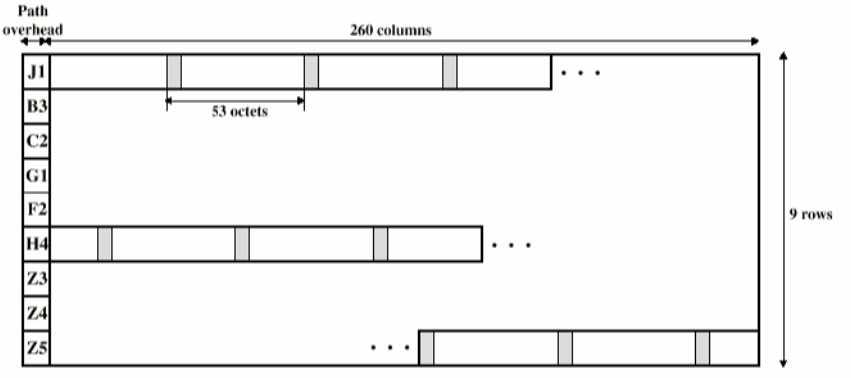
تصویر۷-۱۰: زمان استفاده در برابر احتمال خطای بیتی

مزیت استفاده از طرح انتقال مبتنی بر سلول، سادگی رابطی می باشد که بواسطه آن هر دو تابع حالت ارسال[1] و انتقال[2]، 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 STM1(STS-3) را تحمیل می 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 (۲۳۴۰ بایت)، که یک مضرب صحیح از طول سلول(۵۳ بایت) نیست، یک سلول ممکن است از مرزهای یک Payload ، گذر کند.

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



تصویر ۷-۱۱: STM1 Payload برای انتقال سلول ATM مبتنی بر SDH

[1] Transmission -
[2] Transfer -

مزایای روش مبتنی بر SDH، بشرح زیر می باشد:

- می تواند جهت Payload های مبتنی بر ATM و یا (STM[1])، بکار می رود و این امکان را فراهم می آورد تا ظرفیت بالای انتقال مبتنی بر فیبر ساختاردار، برای یک سوئیچ مداری متغییر را گسترش داده و کاربردها را تخصیص داده و سپس به سهولت به سمت پشتیبانی از ATM برورد.
- 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 گردند. برای مثال، ۴ جریان ATM مجزا ، هرکدام با یک نرخ بیت 155 Mbps(STM1)، می توانند با هم ترکیب شوند تا یک واسط 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 ترافیکیی، بصورت جریان سلولهای ۵۳ بایتی از طریق یک کانال مجازی ارسال و مدیریت می گردند. 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، تحویل 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 واقعی[2]
  - نرخ بیت متغیر غیر زمان واقعی(nrt-VBR)
  - نرخ بیت موجود(ABR[3])
  - نرخ بیت نامعین(UBR[4])

سرویسهای زمان واقعی:

مهمترین تفاوت بین کاربردها، اندازه تاخیر و تغییرات تاخیری[5] 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

---

[1] - Synchronous Transfer Module

[2] - Non Real Time

[3] - Available Bit Rate

[4] - Unspecified Bit Rate

[5] - Jitter

جریان 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 تحویل داده های زمان واقعی در شبکه ATM، بالا می باشد.

نرخ 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 تلوزیون، آموزش از راه دور)
- بازیابی صوت/تصویر(مثل تصویر مورد درخواست، کتابخانه صوتی)

نرخ 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 ترافیکیی داشته و می تواند استفاده بیشتری از مالتی پلکس ثابت، برای افزایش کارایی شبکه را فراهم آورد.

نرخ 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.

نرخ 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) 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[1]، با استفاده از ظرفیت بدون استفاده سایر سرویسها، ارسال می گردند 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[2]" گفته می شود. مثالهایی از کاربردهای VBR در زیر آمده است:

- انتقال متن/داده/تصویر، پیغام دهی، توزیع، بازیابی
- پایانه راه دور (مثل ارتباط برقرار کردن راه دور[3])

نرخ داده موجود:

کاربردهای انفجاری که از یک پروتکل انتها 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 دهند. 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، تعریف گشته است. کاربردهایی که از ABR استفاده می نمایند، یک نرخ سلول حداکثر(PCR[4]) را مشخص می کنند که از آن استفاده خواهند کرد و یک نرخ سلول حداقل(MCR[5]) 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 مبداء، استفاده می نماید تا اطمینان یابد که ظرفیت، منصفانه تخصیص یافته است. هیچ ظرفیت بدون استفاده ای توسط مبداء های ABR، بای 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 ۷-۱۲، 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

---

[1] - FIFO

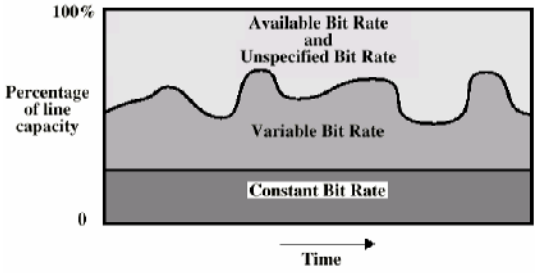
[2] - Best Effort

[3] - Telecommuting

[4] - Peak Cell Rate

[5] - Minimum Cell Rate

استفاده از ATM نیاز به یک لایه تطبیق جهت پشتیبانی از پروتکلهای انتقال اطلاعات که برپایه ATM نیستند، را ایجاد می نماید. دو نمونه از این پروتکلها PCM[1] صوت و پروتکل اینترنت(IP)، می باشد. PCM صوت، یک کاربرد است که جریانی از بیتها را از یک سیگنال صوت، تولید می کند. 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 شبکه های مبتنی بر IP به شبکه های ATM متصل هستند، یک راه ساده که یک جریان نرم و ثابت از بیتها به دریافت کننده، فراهم گردد ، نگاشت بسته های 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 ازسلولها، در گیرنده می باشد. با مجاز شدن IP برروی ATM، هر ساختار موجود IP می تواند برروی شبکه ATM بکار رود.



تصویر ۷-۱۲: 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 بسته های بزرگ داده در فیلد اطلاعات سلولهای 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 می دهد، تعریف نموده است. کلاس بندی برپایه آن بوده است که یک ارتباط زمانی باید بین مبداء و مقصد حفظ گردد، چه اینکه کاربر نیازمند یک نرخ بیت ثابت باشد و چه اینکه انتقال ، اتصال گرا باشد یابدون اتصال باشد. طبقه بندی سیستم، اکنون دیگر در اسناد ITU-T دیده نمی شود، اما مفهوم آن جهت توسعه پروتکل های AAL، مفید می باشد. 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.

[1] - Pulse Code Modulation

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

جدول ۷-۴: مقایسه سرویسهای ATM با اینترنت

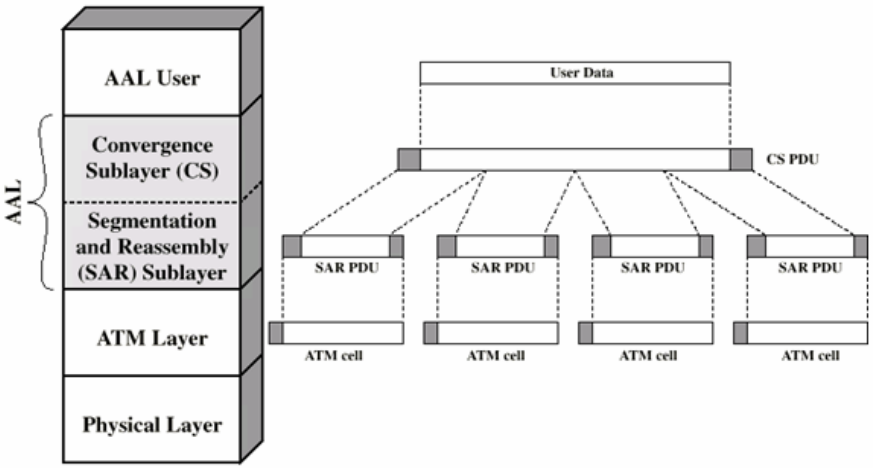
	CBR	rt-VBR	nrt-VBR	ABR	UBR
AAL 1	تقلید مدار، ISDN، صوت برروی ATM				
AAL 2		صوت و تصویر VBR			
AAL 3/4			سرویس داده عمومی		
AAL 5	تقلید LAN	صوت براساس نیاز، تقلید LAN	Frame Relay,ATM، تقلید LAN	تقلید LAN	IP برروی ATM

جدول ۷-۵: پروتکلها و سرویسهای AAL

جدول ۷-۵، ۴ پروتکل AAL را با طبقات سرویس معرفی شده توسط انجمن ATM، نمایش می دهد. موجودیتهای جدول، نشانگر انواع کاربردهایی است که AAL و ATM می توانند با یکدیگر، آنها را پشتیبانی نمایند. آنها به شرح زیر می باشند:

- تقلید مدار: به پشتیبانی از ساختارهای انتقال TDM همزمان، همانند T1، بر روی یک شبکه ATM، اشاره می کند.
- صوت و تصویر VBR: اینها کاربردهای زمان واقعی هستند که بصورت فشرده منتقل می شوند. یکی از تاثیرات فشرده سازی، آنست که یک نرخ بیت متغیر می تواند کاربرد را حمایت نماید که نیازمند یک تحویل جریان بیتی پیوسته به مقصد می باشد.
- سرویسهای داده عمومی: این شامل سرویسهای پیام دهی و تراکنش می باشد که نیازمند پشتیبانی زمان واقعی نیستند.
- IP بر روی ATM: انتقال بسته ها IP توسط سلولهای ATM.
- محصورسازی چند پروتکل بر روی ATM(MPOA[1]): پشتیبانی گستره متغیری از پروتکلهای جدا از IP(همانند IPX، Apple Talk، DECNET) ، برروی ATM.
- تقلید LAN (LANE): پشتیبانی از ترافیک LAN به LAN از طریق شبکه های ATM، با شبیه سازی توانایی LAN Broadcast (انتقال از یک ایستگاه به تعداد زیادی ایستگاه). LANE جهت مجاز ساختن یک انتقال ساده از محیط یک LAN به محیط یک ATM، می باشد.

[1] - Multi Protocol Over ATM



تصویر۷-۱۳: پروتکلهای AAL و PDUها

پروتکلهای AAL:

لایه AAL به دو زیر لایه تقسیم می گردد: زیرلایه همگرایی(CS[1]) و زیر لایه قطعه قطعه کردن و بازسازی(SAR[2]). 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[3]) به AAL منتقل می گردد که به سادگی آدرس کاربرد می باشد. بنابراین این زیر لایه وابسته به کاربرد می باشد.

زیر لایه قطعه قطعه کردن و بازسازی ، مسئول بسته بندی اطلاعات دریافتی از DS به درون سلولها 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.

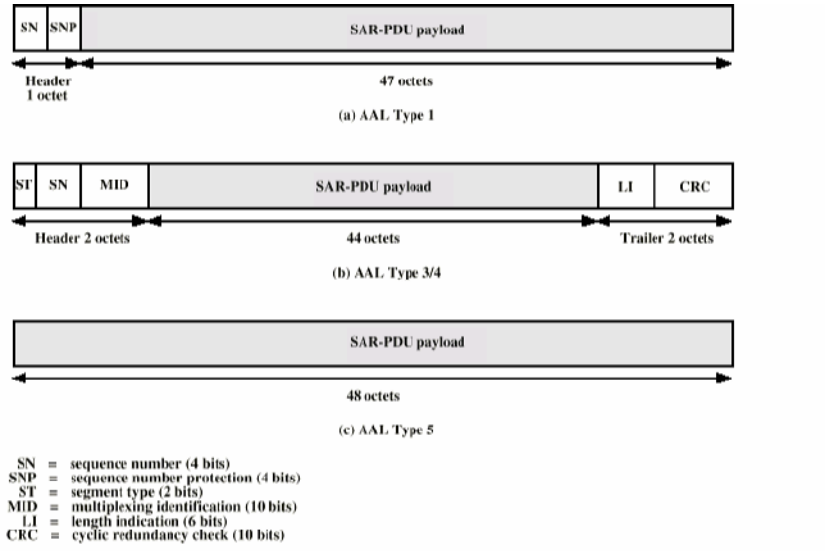
تصویر ۷-۱۳ معماری پروتکل عمومی برای ATM و AAL را نشان می دهد. یک بلاک داده لایه بالاتر در یک واحد داده پروتکل (PDU[4]) یکتا، محصور شده است که شامل داده لایه های بالاتر و احتمالاً یک سرآیند و دنباله حاوی اطلاعات پروتکل در سطح CS، می باشد. سپس این PDU ی CS به لایه پایین SAR منتقل می گردد و به تعدادی بلاک تقسیم می شود. هر کدام از این بلاکها در یک PDUی 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 PDUی 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 زیرلایه 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 زیرلایه CS، محصور شده است. در حقیقت این زیر لایه که به عنوان بخش عمومی زیر لایه همگرایی (CPCS[5])، مورد ارجاع قرار می گیرد، احتمال اینکه توبع اضافی یا خاص بر روی سطح CS، اعمال گردند، را باز گذاشته است. سپس PDUی CPCS منتقل می شود که در آنجا به اندازه بلاکهای Payload، شکسته می شود. هر بلاک Payload، می تواند در یک PDUی SAR قرار گیرد که طول کلی ۴۸ بایتی دارد. هر PDUی SAR ۴۸ بایتی، می تواند در یک سلول ATM منفرد، قرار بگیرد.

---

[1] - Convergence Sublayer
[2] - Segmentation And Reassembly
[3] - Service Access Point
[4] - Protocol Data Unit
[5] - Common Part Convergence Sublayer

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



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

نوع ۱ AAL:

برای بررسی عملکرد نوع ۱، یک منبع نرخ ثابت را مورد بررسی قرار می دهیم. در این حالت، تنها وظیفه پروتکل SAR، قرار دادن بیتها به درون سلولها ، جهت انتقال و استخراج آنها در مقصد، می باشد. هر بلاک ، بوسیله یک شماره توالی(SN[1])، همراهی می گردد تا PDUهای معیوب ، قابل ردیابی باشند. فیلد SN ۴ بیتی شامل یک بیت شناسه زیر لایه همگرایی (CSI[2]) و سه بیت شمارش توالی (SC[3])، می باشد. در انتقال، زیر لایه CS، جهت زیر لایه SAR، یک مقدار CSI، جهت قرار گرفتن در فیلد SN را فراهم می آورد. در گیرنده، زیر لایه SAR، این مقدار را به سمت بالا، جهت زیر لایه CS، ارسال می نماید. بیت CSI در مبادله اطلاعات به شیوه زیر مورد استفاده قرار می گیرد: سه بیت شمارش توالی یک ساختار چهارچوب، شامل ۸ سلول متوالی را شامل می گردد، شماره های صفر تا هفت. مقدار سلولهای ۱، ۳، ۵ و ۷، بعنوان یک مقدار زمانی ۴ بیتی، تعبیه می گردد. این مقدار جهت اندازه گیری تفاوت اندازه فرکانس بین ساعت مرجع شبکه و ساعت انتقال دهنده، بکار می رود. در هر سلول با شماره زوج، CSI می تواند جهت پشتیبانی دسته بندی اطلاعات، از یک لایه بالاتر، بکار می رود. اگر بیت CSI در یک سلول با شماره زوج (۲، ۴، ۶)، به یک تنظیم گردد. اولین بیت PDU Paylaodی SAR، اشاره گری است که شروع دسته ساخت یافته بعدی در Payload این سلول و سلول بعدی را نشان می دهد. در این حالت، زوج سلولها (۱-۰، ۳-۲، ۵-۴، ۷-۶)، 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 می دهد. مقدار آفست ۹۳، جهت مشخص کردن پایان Payload ۹۳ بایتی، همزمان با خاتمه یک دسته ساخت یافته، مورد استفاده قرار می گیرد. مقدار آفست مجازی ۱۲۷، زمانیکه هیچ مرز ساختاری مشخص نشده باشد، بکار می رود.

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

---

[1] - Sequence Number
[2] - Convergence Sublayer Indication
[3] - Sequence Count

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 افزونگی دوره ای (CRC[1]) ۳ بیتی محاسبه شده بر مبنای فیلد ۴ بیتی SN و یک بیت توازن می باشد. بیت توازن بگونه ای تنظیم می گردد تا توازن سرآیند ۸ بیتی SAR، زوج باشد.

هیچ PDUی CSیی برای نوع ۱ تعریف نشده است. تابع زیر لایه CS برای نوع ۱، بوسیله ساعت و همزمانی ابتدایی ، عمل کرده و یک سرآیند CS جداگانه مورد نیاز نمی باشد.

نوع ۲ AAL:

سایر انواع پروتکل، ۲، ۳/۴ و ۵، با اطلاعات نرخ بیت متغیر ، سروکار دارند. نوع ۲ جهت کاربردهای آنالوگ همانند تصویر و صوت که نیازمند اطلاعات زمانی، بدون نیاز به نرخ بیت ثابت هستند، نامزد می باشد. خصوصیات اولیه پروتکل ۲ (SAR و CS)، حذف شده اند و نسخه جاری I.363، سرویسها و توابع فراهم شده را لیست کرده است.

نوع ۳/۴ AAL:

خصوصیات پایه نوع ۳ و ۴ AAL، در فرمت PDU و عملکرد، بسیار شبیه به هم بودند. براین اساس، ITU-T تصمیم گرفت که این دو را در یک پروتکل منفرد، در زیر لایه های SAR و CS، ترکیب نماید، که به عنوان نوع ۳/۴ شناخته می شود.

انواع سرویس فراهم شده توسط نوع ۳/۴ AAL، می تواند در ۲ بعد توصیف گردد:

۱- سرویس ممکن است اتصال گرا یا بدون اتصال باشد. در فرم اول، هر دسته داده ارائه شده به لایه SAR (واحد داده سرویس SAR و یا SDU[2] ی SAR)، بطور مستقل عمل می کند. در حالت بعدی، امکان تعریف اتصالات منطقی SAR چندگانه بر روی یک اتصال ATM منفرد، وجود دارد.

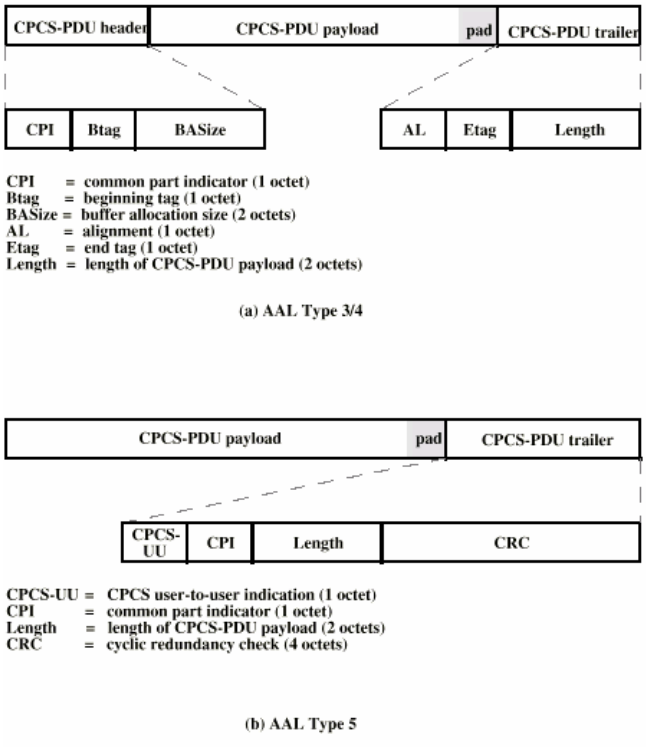
۲- سرویس ممکن است حالت پیام[3] یا جریان[4] داشته باشد. سرویس حالت پیام، داده دسته بندی شده را منتقل می نماید. بنابراین هر پروتکل OSI مرتبط و کاربردی، می خواهد در این طبقه جا بگیرد. مخصوصاً LAPD یا Frame Relay تمایل به قرار گرفتن در حالت پیام دارند. یک بلاک دسته منفرد از لایه بالای AAL، در یک یا چند سلول، منتقل می گدد. سرویس حالت جریان، از انتقال داده پیوسته با سرعت پایین با نیازمندیهای تاخیر کم، پشتیبانی می کند. ممکن است در کمترین حالت، تنها یک بیت در یک دسته با طول ثابت AAL، قرار گیرد. هر دسته در یک سلول منتقل می شود.

نوع ۳/۴ AAL، سرویس انتقال داده خود را با پذیرش دستهای داده از لایه بالایی بعدی و ارسال هر کدام به یک کاربر AAL مقصد، فراهم می آورد. از آنجائیکه لایه ATM، انتقال داده را به Payload های ۴۸ بایتی یک سلول، محدود می سازد، لایه AAL، حداقل یک تابع قطعه کردن و بازسازی را باید فراهم آورد.

عملکرد نوع ۳/۴ AAL، بشرح زیر می باشد. یک دسته داده از زیر لایه بالاتر، همانند یک PDU، در درون یک PDU در زیر لایه CPCS، محصور می گردد. سپس PDUی CPCS به زیر لایه SAR منتقل می گردد که به دسته های Payload ۴۴بایتی، تقسیم می گردد. هر دسته Payload می تواند در یک PDUی SAR قرار بگیرد که شامل یک سرآیند و یک دنباله برای طول کلی ۴۸ بایت می باشد. هر PDUی SAR ۴۸ بایتی در یک سلول ATM منفرد، قرار می گیرد.

---

[1] - Cyclic Redundancy Check
[2] - Service Data Unit
[3] - Message Mode
[4] - Streaming Mode



تصویر۷-۱۵: PDUی CPCS

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

- نشان دهنده بخش عمومی(۱ بایت): تغییر فیلدهای باقیمانده در سرآیند PDUی CPCS 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 PDU Payloadی CPCS را بر حسب بایت، مشخص می نماید.
- برچسب شروع[1](۱ بایت): عددیست که مرتبط با یک PDUی CPCS 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 PDUی CPCS پیاپی تغییر می دهد که براساس آن گیرنده قادر به تشخیص سرآیند و دنباله هر PDUی CPCS مرتبط با هم ، گردد.
- اندازه تخصیص بافر(۲ بایت): نشاندهنده حداکثر اندازه بافر مورد نیاز برای بازسازی SDUی CPCS، در موجودیت همتای دریافت کننده می باشد. برای حالت پیام، این مقدار برابر با طول PDU Payloadی CPCS ، می باشد. برای حالت جریان، این مقدار، بزرگتر یا مساوی طول PDUی CPCS، می باشد.

Payload لایه بالایی بعدی با بیتهای غیر لازم کشیده می شود[2] تا در یک حد ۳۲ بیتی قرار گیرد. دنباله PDUی CPCS، شامل سه فیلد می گردد:

- تنظیم(۱ بایت): یک بایت پرکننده که تنها به منظور اینکه طول PDUی CPCS، ۳۲ بیتی شود، مورد استفاده قرار می گیرد.

---

[1] Beginning Tag -

[2] Pad out -

- برچسب انتها(۱ بایت): با فیلد Btag در سرآیند بکار می رود.
- طول(۲ بایت): طول فیلد Payload PDU ی CPCS.

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 PDUی CPCS، توانا می سازد.

تصویر b ۷-۱۵ ، فرمت PDUی 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 PDUی SAR، منتقل می گردد. هر PDUی SAR در یک سلول ATM منفرد منتقل می شود. فیلدهای سرآیند PDUی SAR ، جهت اهداف پردازش قطعات SDU در انتقال و بازسازی آنها در زمان پذیرش در مقصد، بکار می رود:

- نوع سگمنت: ۴ نوع PDU ی SARوجود دارد. یک پیام متوالی منفرد (SSM)، یک SDUی SAR کامل را شامل می گردد. اگر SDUی SAR به دو یا چند PDUی SAR تقسیم شود، اولین PDUی SAR، آغاز پیام(BOM) و آخرین PDUی SAR، پایان پیام(EOM) می باشد. و هر PDUی SAR میانی، ادامه پیام(COM[1]) می باشد.
- شماره توالی: در بازسازی یک PDUی SAR، جهت اطمینان از دریافت تمام PDUهای SAR و الحاق صحیح آنها، بکار می رود. یک مقدار شماره توالی ، برای یک SDUی 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 PDUهای SAR می باشد که یک PDU یSAR 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 PDUی SAR، شامل فیلدهای زیر می باشد:

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

یک خصیصه مشخص از ۳/۴ AAL آنست که می تواند جریانهای متفاوت داده را برروی یک اتصال ATM مجازی یکسان (VPI/VCI)، مالتی پلکس کند. برای سرویسهای اتصال گرا، هر اتصال منطقی بین کاربران AAL متفاوت می تواند برروی 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.

[1] - Continuation of Message

نوع ۵ AAL:

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 گرا، 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 نوع۳/۴ SAR و PDUی CPCS، مورد نیاز نمی باشد. برای مثال، با سرویسهای اتصال گرا، به فیلد MID، نیازی نیست، VPI/VCI 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 ۷-۱۴ و b ۷-۱۵ ، فرمتهای PDUی SAR و PDUی CPCS برای نوع ۵ را نشان می دهند. در مقایسه با نوع ۳/۴، حجم سربار زیر وجود دارد:

نوع ۵	نوع ۳/۴
۸ بایت برای SDUی AAL	۸ بایت برای SDUی AAL
صفر بایت برای سلول ATM	چهار بایت برای سلول ATM

جهت درک عملکرد نوع ۵، اجازه بدهید با سطح CPCS، شروع نمائیم. PDUی CPCS (تصویر b۱۱-۱۵) دنباله ای با فیلدهای زیر دارد:

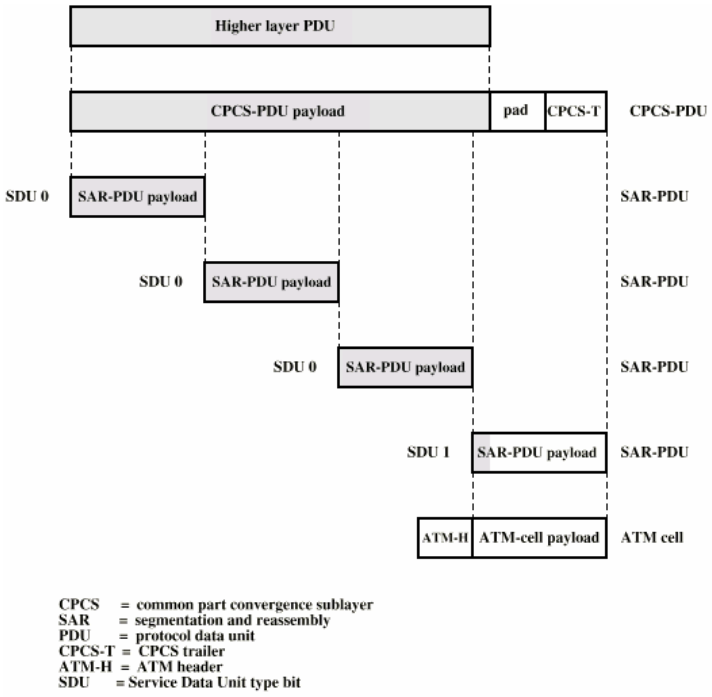
- نشانه کاربر به کاربر CPCS(۱ بایت): جهت انتقال اطلاعات شفاف کاربر به کاربر بکار می رود.
- نشانه بخش عمومی(۱ بایت): جهت تفسیر فیلدهای باقیمانده در دنباله PDUی CPCS، بکار می رود. در حال حاضر، تنها یک تفسیر وجود دارد.
- طول(۲ بایت): طول فیلد Payload PDUی CPCS.
- CRC(۴ بایت): جهت تشخیص خطاهای بیتی در PDUی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

توجه کنید که امکانABSize 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 حداکثر اندازه PDU، تنظیم شده یا می شوند. این اطلاعات می تواند برای دریافت کننده جهت تخصیص بافر، بکار رود. CRC ۳۲ بیتی، تمام PDUی CPCS را حفاظت می کند که در مقایسه با آن، در نوع ۳/۴ AAL، که یک CRC ۱۰ بیتی برای هر PDUی SAR، فراهم می گردد، CRC نوع ۵ حمایت قویتری را در برابر خطاهای بیتی فراهم می آورد. بعلاوه CRC ۳۲ 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 بیتهایی بدون استفاده ، پر می شود تا همه PDUهای CPCS، مضربی از ۴۸ بایت گردد. PDU ی SAR شامل ۴۸ بایت Payload است که بخشی از PDUی CPCS را حمل می نماید. نبود سربارهای پروتکل، چند معنی دارد:

- بدلیل 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 PDUی CPCS، نامزد است تا آن را تایید کند.

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



تصویر۷-۱۶: نمونه ای از انتقال AAL5

تصویر ۷-۱۶، نمونه ای از انتقال ۵ AAL را نشان می دهد. PDUی CPCS شامل بخش پرشده با بیتهای غیر ضروری و دنباله، به دسته های ۴۸ بایتی، تقسیم شده است. هر دسته در یک سلول ATM منفرد انتقال می یابد.

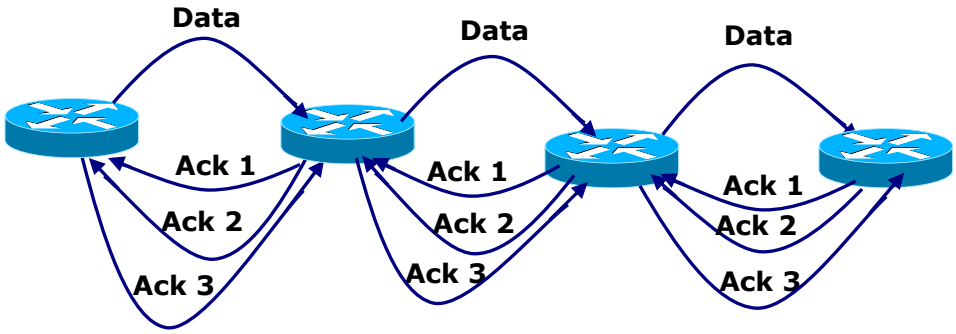
۷-۷: Frame Relay

Frame Relay همانند ATM، جهت فراهم آوردن انتقال موثرتر از طرح X.25، طراحی گردیده است. 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، جهت شبکه های با سرعت بالا، تغییر نموده است، اما بدلیل اینکه Frame Relay هنوز عمومیت دارد، در این قسمت به بررسی آن می پردازیم.

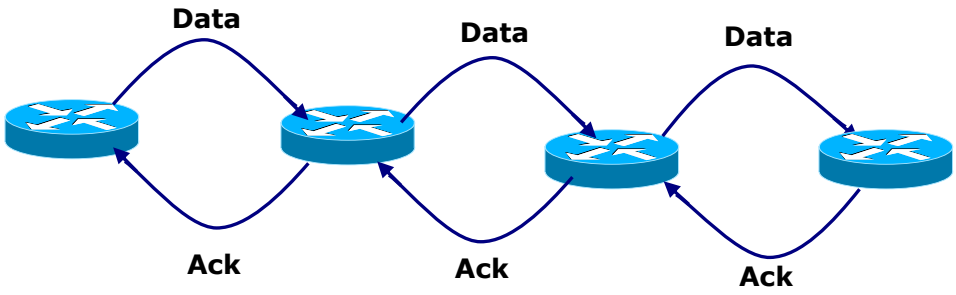
پس زمینه:

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، مکانیزمهای کنترل جریان و خطا را شامل می شوند.



الف) انتقال داده و تایید آن در X.25



ب) انتقال داده و تایید آن در Frame Relay

تصویر۷-۱۷: 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 خطای پروتکل X.25، مورد بررسی قرار بگیرد. همه این سربارها ممکن است در زمان وجود یک احتمال خطا 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 قابل اعتماد برروی 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 محیطهایی ، 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 تحویل X.25 بر سیستمهای کاربران نهایی و شبکه های سوئیچ بسته ای ، طراحی شده است. تفاوتهای عمده بین Frame Relay و سرویس سوئیچ بسته ای X.25 متداول، بشرح زیر است:

- سیگنال دهی کنترل تماس برروی 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 می افتد که نتیجه آن حذف پردازش یک لایه کامل است.
- کنترل جریان و کنترل خطا پرش به پرش، وجود ندارد. کنترل جریان و خطای انتها به انتها، اگر مورد استفاده قرار بگیرد، مسئولیت لایه های بالاتر می باشد.

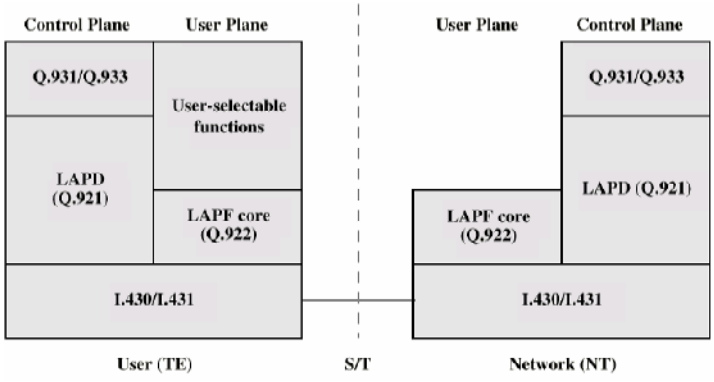
بنابراین با Frame Relay یک فریم داده تنهای کاربر از مبداء به مقصد ارسال می گردد و در مقصد، یک تایید در یک لایه بالاتر تولید شده و در یک فریم ، بازگردانده می شود. تبادل پرش به پرش فریمهای داده و تایید، وجود ندارد.

اجازه بدهید نگاهی به مزایا و معایب این طرح بیاندازیم. مهمترین عیب Frame Relay در مقایسه با X.25، عدم وجود توانایی کنترل جریان و خطای اتصال به اتصال می باشد(اگرچه Frame Relay کنترل جریان و خطای انتها به انتها را فراهم نمی کند، براحتی این امر در یک لایه بالاتر، فراهم می آید) . در X.25، چند مدار مجازی برروی یک اتصال فیزیکی حمل می گردد و LAPB در سطح اتصال، برای ایجاد انتقال مطمئن از یک منبع به شبکه سویئچ بسته ای و از شبکه سوئیچ بسته ای به مقصد، موجود است. بعلاوه، در هر پرش در شبکه، پروتکل کنترل انتقال می تواند جهت اطمینان ، بکار رود. با استفاده از Frame Relay ، کنترل اتصال پرش به پرش از دست می رود. اگرچه با افزایش اطمینان انتقال و امکانات سوئیچ، این یک عیب عمده نیست.

مزیت Frame Relay آنست که ما پردازش اتصال ساده و موثر داریم. توابع مورد نیاز پروتکل در رابط کاربر-شبکه، بدلیل پردازش درون شبکه ای، کاهش می یابد. بعنوان یک نتیجه، تاخیر کمتر و گذردهی بالاتر را می توان انتظار داشت. مطالعات نشانگر بهبود توان عملیاتی، با استفاده از Frame Relay، در مقایسه با X.25، می باشد. توصیه نامه ITU-T I.233، عنوان می کند که Frame Relay می تواند جهت کسب سرعت 2 Mbps ، بکار رود.

معماری پروتکل Frame Relay:

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



تصویر۷-۱۸: معماری پروتکل رابط کاربر-شبکه

طرح کنترل:

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

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

طرح کاربر:

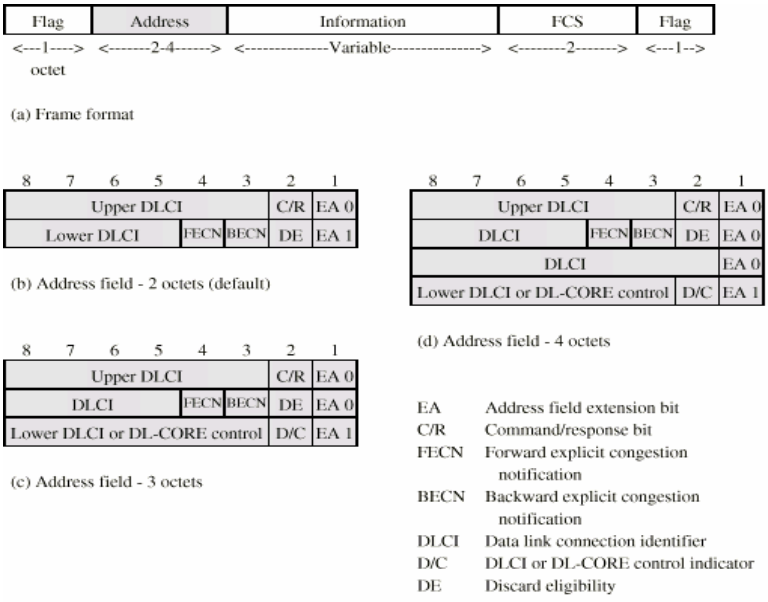
برای انتقال واقعی اطلاعات بین کاربران نهایی به پروتکل طرح کاربر، LAPF(روال دسترسی به اتصال برای سرویسهای حامل حالت فریم) می باشد که در Q.922 تعریف شده است. Q.922 یک نسخه پیشرفته از LAPD(Q.921) می باشد. تنها توابع مرکزی و هسته LAPF برای Frame Relay مورد استفاده قرار می گیرند.

- تعیین کردن حدود: تنظیم موقعیت و شفافیت فریم.
- مالتی پلکس و عکس مالتی پلکس فریم با استفاده از فیلد آدرس.
- بازرسی فریم جهت اطمینان از اینکه شامل یک عدد صحیح از بایتهای اولویت به صفر بیت افزودن و یا صفر بیت استخراج.
- بازرسی 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 خطایی 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. برپایه 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



تصویر ۷-۱۹:فرمت هسته LAPF

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 می شود. این فرمتی است که برای حداقل توابع پروتکل LAPF(پروتکل هسته LAPF)، تعریف شده است. فرمت با یک حذف آشکار، شبیه به LAPD و LAPB می باشد: 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 می نماید.

توابع فیلدهای بررسی توالی پرچم و فریم، همانند نمونه های LAPD و LAPB هستند. فیلد اطلاعات، داده لایه بالاتر را حمل می کند. در صورتیکه کاربر قصد پیاده سازی توابع کنترل داده اضافی انتها به انتها را داشته باشد، یک فریم پیوند داده می تواند در این فیلد، حمل گردد. بویژه، یک انتخاب عمومی، استفاده از پروتکل کامل LAPF (پروتکل کنترل LAPF)، جهت انجام توابع بالای هسته LAPF، می باشد. توجه کنید که پروتکلهای پیاده شده به این شیوه بین مشترکین نهایی، سخت است و برای شبکه های 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، ۱۷ و یا ۲۴ بیتی را حمل می کند. DCLI همان توابع شماره مدار مجازی در X.25 را سرویس می دهد و به اتصالات منطقی Frame Relay، امکان مالتی پلکس برروی یک کانال تنها را می دهد. همانند X.25، شناسه اتصال تنها ارزش محلی دارد: هر انتهای اتصال منطقی، DCLI خودش را از شماره های تخصیص نیافته محلی منبع، تخصیص می دهد و شبکه باید یکی را به دیگری نگاشت کند. راه دیگر، استفاده از DCLI یکسان در هر دو انتها می باشد که نیازمند برخی انواع مدیریت سراسری مقادیر DCLI می باشد.

فیلد آدرس و از این رو DLCI، بوسیله بیتهای امتداد فیلد آدرس مشخص می شود. بیت CIR، خاص کاربرد است و بوسیله پروتکل Frame Relay استاندارد، بکار نمی رود. بیتهای باقیمانده در فیلد آدرس با کنترل تراکم بکار می روند.

IP برروی Frame Relay:

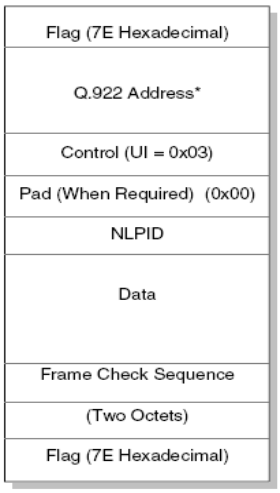
همه پروتکلها باید بسته هایشان را در یک فریم ضمیمهQ.922 A، قرار دهند. بعلاوه فریمها شامل اطلاعات کافی جهت تعیین پروتکل حمل شده در PDU می باشند، تا دریافت کننده را قادر به انجام پردازش صحیح برروی بسته ورودی نماید. فرمت این امر بصورت زیر خواهد بود:

- فیلد کنترل، فیلد کنترل Q.922 می باشد. عمدتاً مقدار UI(0X03) بکار برده می شود، مگر آنکه برای مقدار دیگری توافق گردد. استفاده از XID (0XAF یا 0XBF)، مجاز می باشد.
- فیلد PAD برای تنظیم بخش داده (فراتر از سرآیند محصورسازی) فریم برای قرار دادن اندازه آن در مضربی از ۳۲بیت، بکار می رود. در صورت امکان، PAD یک بایتی با مقدار صفر، خواهد بود.
- فیلد NLPID بوسیله ISO و ITU-T فراهم شده است.این فیلد حاوی مقادیری برای پروتکلهای متفاوت بسیاری،شامل IP، CLNP، و پروتکل دستیابی به زیر شبکه(SNAP[1]) IEEE، می باشد. این فیلد به دریافت کننده می گوید که چه پروتکلی در بسته ها محصور شده است. مقادیر این فیلد در ISO/IEC TR 9577، تعریف شده اند. مقدار 0X00 برای NLPID در ISO/IEC TR 9577، به عنوان یک لایه شبکه تهی یا مجموعه غیر فعال، تعریف شده است. بدلیل عدم تشخیص آن از یک

[1] - SubNetwork Access Protocol

فیلد PAD و بی معنـی بـودن آن در زمینـه طـرح محـصورسازی، مقـدار 0X00 بـرای 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 اسـت. یک شبکه باید حداقل طول ۲۶۲ بایت و حداکثر ۱۶۰۰ بایتی یا بیشتر (متناسب با تصمیمات تهیـه کننـده Frame Relay) را پشتیبانی کند. یک Frame Relay 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 وجـود دارنـد: بـسته هـای مـسیردهی شده[1] و بسته های پل شده[2]. این بسته ها فرمتهای مجزایی داشته و باید شامل یک شاخص که جهت تفـسیر صـحیح محتویات فریم در مقصد، مورد استفاده قرار می گیرد، باشد. این شاخص در اطلاعات سرآیند NLPID و SNAP، قـرار می گیرد.

ایستگاه های Frame Relay ممکن است جهت پشتیبانی از تبادل تعیین هویـت(XID[3])تعریـف شـده در ضمیمه ۳ Q.922، انتخاب گردند. این تبادل XID، اجازه می دهد تا پارامترهای زیر در ابتدای مقداردهی اولیه مـدار Frame Relay ، محاوره گردند: اندازه حداکثر طول فریم، زمان سنج انتقـال مجـدد و حـداکثر تعـداد فـریم هـای اطلاعات ارائه نشده. اگر این تبادل مورد استفاده قرار نگیرد، این مقادیر باید بصورت ثابـت ، بوسـیله توافـق دوجانبـه نقاط انتهایی اتصالات پیوند داده (DLC)، پیکربندی گردد و یا باید از مقادیر پیش فرض مشخص شده در بخش ۷-۹ در Q.922، استفاده شود.

ایستگاه هایی نیز هستند کـه مـی خواهنـد در مـورد یـک پروتکـل آدرس دهـی بـرروی کانالهـای مجـازی ثابت(VPC)، بصورت پویا تصمیم گیری کنند. این امر ممکن است بوسیله ARP محصور شده در یک بـسته Frame Relay کد شده SNAP، انجام گیرد.

بدلیل ناتوانی شبیه سازی Broadcast در یک محیط Frame Relay، یک نمونه تعیین آدرس تغییر یافتـه، توسعه یافته است که به آن ARP معکوس می گویند و شیوه ای را برای تصمیم گیری در مورد یـک آدرس پروتکـل در زمان وجود آدرس فیزیکی، توصیف می نماید. در یک شـبکه Frame Relay، آدرس سـخت افـزار هویـدا، 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 IP subnet یکسان، برای یک DLCI خاص، برروی 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 پهنای باند را برروی 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 فریمها قرارگیرد: مقدار NLPID[1]، نشان دهنده IP، و یا مقدار NLPID، نشاندهنده SNAP.

اگرچه هر دوی این محصورسازیها با تعاریف ارائه شده حمایت می شوند، استفاده از هرکدام از این مکانیزمها برای محصورسازی داده هایIP، 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 SNAP، ۴۸ بیت کمتر ارسال می کند و با محصورسازی IP در یک شبکه X.25 نیز سازگار می باشد.

ایجاد VPN با Frame Relay:

VPN،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 باشند و برای اینکه ظاهراً 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 سوئچینگ بسته ای است . اگر X.25 استفاده کنیم ، سربار 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 .

تصویر۷-۲۱: ایجاد VPN به کمک Frame Relay

FRAD[2] : یک نوع مسیریاب است با این تفاوت که مسیریابی انجام نمی شود و بلکه فقط بسته ها را انتقال می دهد.

خلاصه فصل:

ATM 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 برروی 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،

---

[1] - Network Level Protocol ID

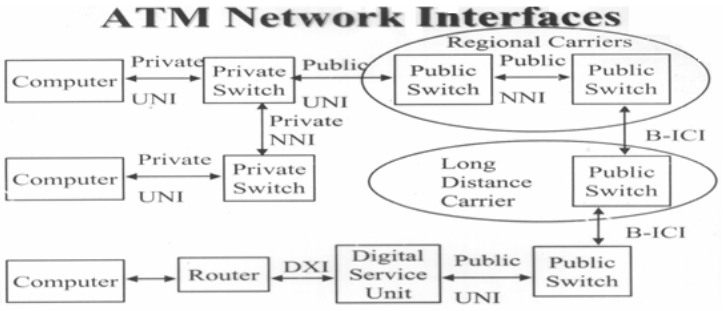
[2] - Frame Relay Access Device

اساس کار می باشد. گزینه دوم، قرار دادن سلولها در یک پوشش مالتی پلکس تقسیم زمان همزمان ، مـی باشـد. در این حالت، جریان بیتی در رابط، یک ساختار چهارچوب خارجی برروی 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 توانـد دامنه گسترده ای از دامنه ترافیک ، شامل جریانات TDM همزمان همانند T1، با استفاده از سرویسهای با نـرخ بیـت ثابت(CBR)، صوت و تصویر فشرده شده با استفاده از سرویس نرخ بیـت متغیـر زمـان واقعـی (rt-VBR)، ترافیـک بـا نیازمندیهای کیفیت سرویس مشخص، با استفاده از سرویس VBR غیر زمان واقعی(nrt-VBR) و ترافیـک مبتنـی بـر 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 بـر ATM را بوجود می آورد. لایه تطبیق ATM(AAL) اطلاعات AAL کاربر را در بسته های ۴۸ بایتی برای قرار دادن در سـلولهای ATM، بسته بندی می کند. این ممکن است شامل جمع نمودن بیتها از یک جریان بیتی و یا تقـسیم یـک فـریم بـه 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، مـشخص شده اند.



تصویر۷-۲۲: طرح رابط شبکه ATM

فصل ۸:

IntServ، DiffServ و MPLS

اجزا شبکه اینترنت به دو سرویس ISA[1] و DSA[2] (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[3]، 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 حداکثر تأخیر ۱ میلی ثانیه نیاز داریم . ISA , DSA به منظور ایجاد QoS در اینترنت بوجود 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 RSVP[4] 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 قبلاً 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 QoS Routing است یعنی مسیریابی براساس QoS (حمایت QoS بر روی IP توسط ISA).

انواع ترافیک :

- انعطاف پذیر[5] : 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[6] :در این نوع ترافیک ، مجبوریم که پارامترهای QoS را در حد خوبی انتظار داشته باشیم؛ یعنی حداقلهایی 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

---

[1] - Integrated Service Architecture
[2] - Differentiated Service Architecture
[3] - Jitter
[4] - Resource ReSerVation setup Protocol
[5] - Elastic
[6] - Inelastic

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 قبلاً 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 Flow، 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: Flow یک طرفه است و می تواند Multicast شود. بعلاوه یک بسته IP، به عنوان عضوی از یک Flow در پایه آدرسهای IP مبداء 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:

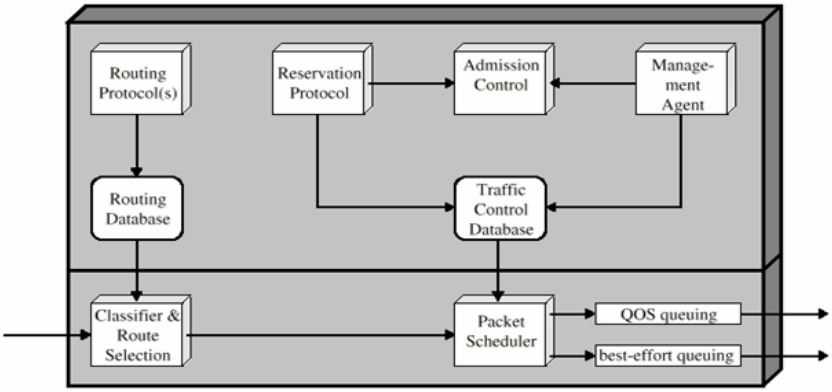
- کنترل پذیرش[1] : برای انتقال QoS، ISA نیازمند آنست که عملیات رزرو برای یک Flow جدید، صورت گیرد. اگر مسیریابها مجموعاً به این نتیجه رسیدند که منابع کافی برای تضمین QoS درخواستی وجود ندارد، Flow پذیرش نمی شود. پروتکل RSVP مسئول انجام این رزرو می باشد.
- الگوریتم مسیریابی: تصمیم مسیریابی ممکن است برپایه پارامترهای یک QoS متغیر باشد و تنها بر پایه تاخیر. برای مثال، پروتکل مسیریابی OSPF می تواند مسیرها را برپایه QoS انتخاب کند.
- سیاست صف گذاری[2] : یک عنصر حیاتی ISA، رویه صف بندی موثری است تا بتواند نیازمندیهای متفاوت Flow های متفاوت را در نظر بگیرد.
- رویه دورریختن[3] : یک رویه صف گذاری مشخص می کند که اگر چند بسته در صف 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 :

---

[1] - Admission Control
[2] - Queuing Discipline
[3] - Discard Policy



ISA Router Structure

RSVP هسته اصلی پروتکل ISA 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 . Mbone یک شبکه Multicast 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 .

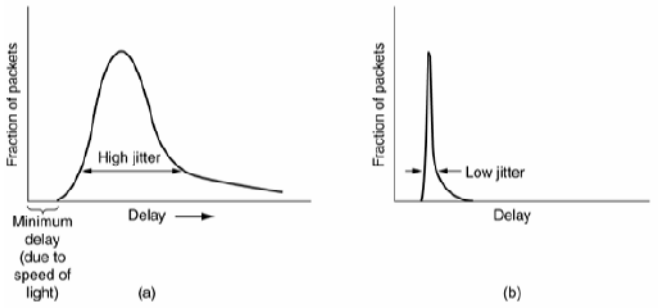
گروههای کاری :

۱- INTSERV (Integrated Service Over Specific Link Layer)

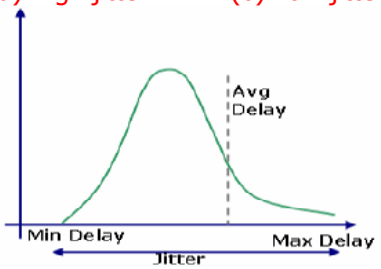
۲- ISSLL

۳- RSVP

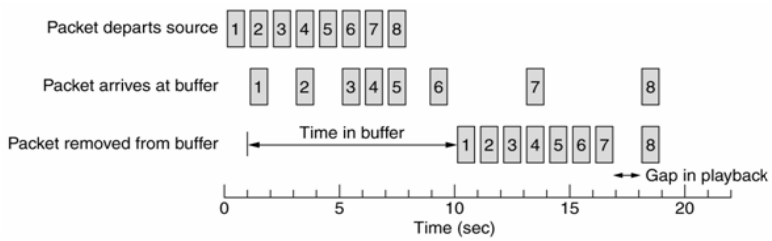
Read time application : یکی از پارامترهای QoS ، تأخیر (Delay) است .کاربردهایی که بصورت زمان واقعی هستند محدودیتی در زمینه تاخیر دارند .



(a) High jitter. (b) Low jitter.

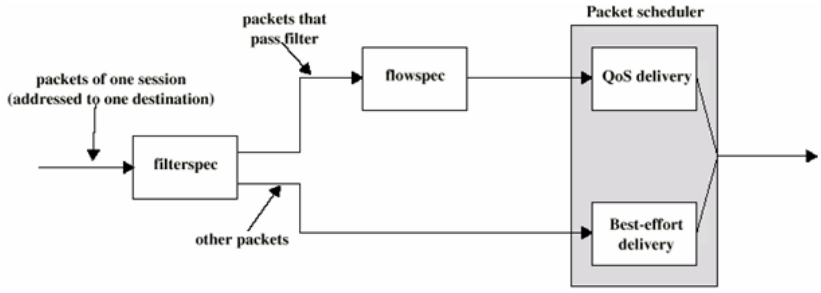


وقتی بسته ها ارسال می شوند (بسته از مبدأ بصورت منظم و با فواصل یکسان ارسال می شوند) ممکن است با همان فاصله بین بسته ها در گیرنده دریافت نشود (به دلیل تأخیر) . برای کارهای Real time می توان یک offset در نظر گرفت و بعد از این offset بسته ها به صورت منظم و پشت سرهم دریافت می شوند . با افزودن بافر هرچند 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 می گیرد . اگر شبکه توانست منابع را برای رسیدن به کارآیی مطلوب رزرو کند انتقال اطلاعات صورت می گیرد . بیشترین معیار QoS ، تأخیر بسته ها می باشد .



QoS ISA Router

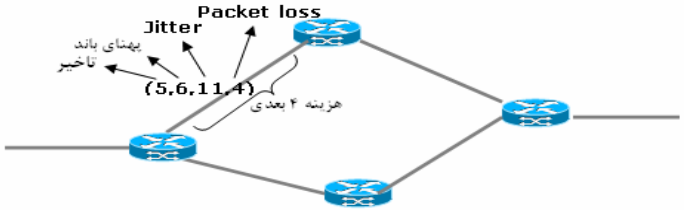
در ابتدا کاربر نیازهای خود را با Flow Identification مشخص می کند سپس بعد ازبیان نیازها مسیریاب دو کار انجام می دهد :

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 ی رزرو شده در جدول رزرواسیون قرار می گیرد . زمانی که بسته ای می آید واحد شناسائی Flow ، بسته ها را شناسائی می کند و نگاه می کند که آیا با Flow های رزرو شده مطابقت دارد یا خیر . اگر مطابقت داشته باشد آن را در صف قرار می دهد سپس packet scheduler بسته را بعد از اختصاص منابع به Flow ارسال می کند .

- QoS Routing (انتخاب مسیر) : مسیریابی های فعلی بر اساس مینیمم تأخیر در یک منطقه محلی کار می کنند 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 ماهواره ای) بتواند پهنای 25Mbps را حمایت کند در حالیکه از نظر تأخیر بهینه نیست . (یعنی پارامتر پهنای باند از پارامتر تأخیر در لینک ماهواره ای مهمتر است)



QoS Routing

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 می کنند یا یک سرور مرکزی بدین منظور اختصاص می دهند (این کار فقط node بعدی را می دهد) . این جملات به این معنی

است که پیاده سازی مسیریابی با چند پارامتر عملاً صورت نمی گیرد و با یک یا دو پارامتر صورت می گیـرد. بعـد از پیدا کردن نود بعدی باید حالتهای 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 مـسیر حالتهـــای رزرواسیون را نصب کند . پروتکل همچنین اطلاعاتی درباره مشخصات ترافیک و نیازهای منابع در رابطه با خصوصیات ترافیـــک و نیازهای منابع باید حمل کند تا مشخص شود کـه رزرواسـیون مـی توانـد صـورت گیرد یا خیر . این پروتکل در صورت خراب شدن یک لینک هم باید بتواند کار کند (تغییر توپولوژی) .

رزرو کردن منابع باید شامل مسائل مالی (مـادی) هـم باشـد: Authentication , Authonzation , billing .قبل از رزرو کردن منابع باید مشخص شود که چه کسی هزینـــه این کار را پرداخت خواهد کـرد (شناسـائی 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 تحقیقـاتی به خود گرفته است (Diffserv جای ISA را گرفته است) .

- کنترل پذیرش: این واحد بررسی می کند تا مشخص کند که آیا منابع کافی برای این فلـوی جدیـد وجـود دارد یا خیر . اگر منابع کافی نیستند جلوی ارتباط گرفته می شود .قبل از هر رزرواسیون باید از این تـست عبور کرد (قبول یا رد) . بنابراین هم قبول شدن رزرواسیون و هم انـدازه گیـری منـابع جـزء ایـن بخـش 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 تـصویر تغییـر مـی کنـد .(مـثلاً اگـر بـا دوربین بخواهیم تصویر یک نفر را ارسال کنیم حرکت کردن سر یا حرکت نکردن سر باعث تغییـر محتویـات ارسال می شود) .

-براساس اندازه گیری واقعی : در این روش شبکه اندازه گیری واقعی انجام می دهد . چنـد روش بـرای ایـن کار وجود دارد :

۱. Simplesum : اگر مجموعه پهنای باند برای node های جاری و جدید از ظرفیت لینک بیشتر شود ، منابع کافی نیست و A.C 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 بـرای یـک نـوع ترافیـک را بدست آورد .

Newestimate = (1- w) oldestimate +(w * new meusurement)
w = 0.1+0.1 (متوسط گیری نمائی)

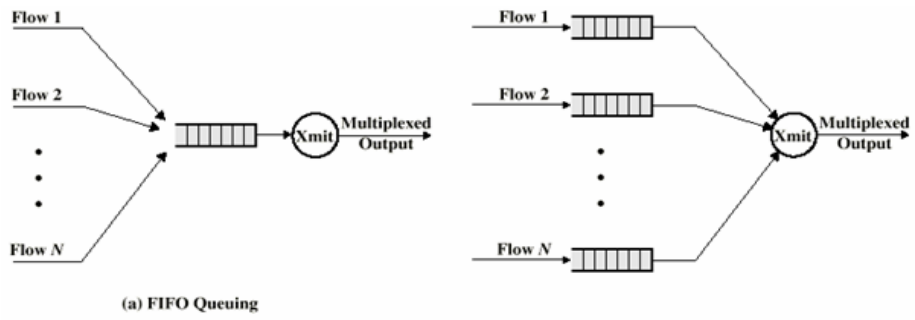
اگر w کم باشد یعنی به تغییرات لحظه ای بهای کمتری داده می شود و به تغییرات قدیمی (که قبلاً بـه دست آمده) ارزش بیشتری داده می شود (چون ضریب آن 1-w است) و اگر w زیاد باشد بـه تغییـرات لحظه ای بهای بیشتری داده می شود .

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

آدرس IP مبدأ ، آدرس IP مقصد ، پروتکـل ID (TCP , UDP,...) ، پـورت مقـصد ، پـورت مبـدأ .ایـن فیلدها از بسته ها استخراج می شوند و بررسی می شود که آیا قبلاً هم FLOW هایی با ایـن مشخـصـات وجود داشته است یا خیر . میلیونها FLOW می تواند در مسیریاب وجود داشته باشد .

Flow Identification باید در محدوده زمانی بسیار محدودی صورت گیـرد . بعـضی هـا بـرای ایـن کـار روشهای سخت افزاری را پیشنهاد کرده اند (مثل CAM) .

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



(a) FIFO Queuing

(b) Fair Queuing

Packet Scheduling

به همین دلیل به جای استفاده از یک صف برای تمام خروجیها می توان برای هر خروجی یک صف در نظـر گرفت . این روش Fair Queuing نامیده می شود . البته در این روش هم ممکن است بـسته بـزرگ وجـود 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 شـلوغتر است سرویس بیشتری می گیرد بدون آنکه برای دیگران مزاحمتی ایجاد کند (این بـسته بـین بـسته هـای دیگر ارسال می شود) .

- Packet scheduling یعنی اینکه بسته ها چگونه انتقال داده شود .

DiffServ[1]:

متدهای ISA و RSVP جهت حمایت از QoS در اینترنت و شبکه های خصوصی، مورد توجه هستند. اگرچـه 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 مقیاس پذیری خوب جهت مدیریت حجـم عظـیم ترافیـک ، بـدلیل وجـود سیگنالهای کنترلی مورد نیاز زیاد جهت هماهنگ سازی QoS یکپارچه پیشنهادی را بدلیل نیاز بـه حفـظ اطلاعـات وضعیت در مسیریابها، را ندارد.

همزمان با رشد اینترنت، کاربردهای مختلف نیز رشـد کـرده و ایـن موضـوع، یـک نیـاز فـوری بـرای ایجـاد لایه های متفاوت QoS برای Flow های ترافیکی مختلف، بوجود آورد. معماری DiffServ (RFC 2475) جهت ایجاد یک پیاده سازی راحت و آسان، با سربار ابزاری کم برای پشتیبانی از سرویسهای شـبکه بـا اجراهـای پایـه متفـاوت، 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 ، بوجود می آورد.
- DiffServ در مسیریابهای متفاوت بوسیله صف 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 DiffServ علامت گذاری می کند تا کلاس بسته مشخص گردد. تهیه کننده سرویس باید اطمینان دهد که مشتری حداقل QoS مورد 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.

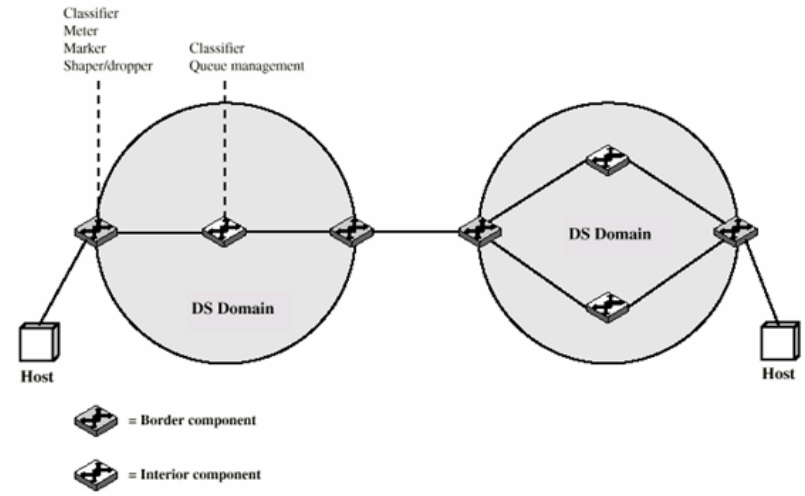
اگر یک مشتری بسته هایی را برای مقصدی در دامنه همان DiffServ، ارائه دهد، انتظار می رود DiffServ سرویس مورد توافق را ارائه دهد. اگر مقصد در خارج از دامنه DiffServ مشتری باشد، دامنه DiffServ سعی در انتقال بسته ها از طریق سایر دامنه های DiffServ یی که می توانند سرویس های مقتضی و مناسب با سرویس درخواستی را ارائه دهند، می نماید.

براساس RFC 1812، نیازمندیهای مسیریابهای IPV4، نیازمندیهای لازم برای ایجاد سیاست صف گذاری به دو دسته تقسیم می شوند:

- سرویس صف:
  - مسیریابها **باید** سرویسهای صف برپایه تقدم را ایجاد نمایند. سرویس صف 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 صف تقدم، ارسال گردد.
  - هر مسیریابی **ممکن است** سایر روالهای مدیریت گذردهی 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 بریزد.
  - یک مسیریاب **ممکن است** بسته ای را که به تازگی دریافت کرده دور بریزد؛ 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 صفهای عدالت(Fair) است که در آن دور ریختن از صفهای طویلتر 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 **نباید** بسته هایی را که اولویت بالاتری نسبت به سایر بسته ها دارد، را دور بریزد.
- یک مسیریاب **ممکن است** بسته هایی را که سرآیند آنها نیازمندی به حداکثر TOS را اعلام می کند، برخلاف قانون بالا حفظ نماید.
- یک مسیریاب **ممکن است** از بسته های تکه تکه شده محافظت نماید، زیرا در تئوری ، حذف یک قطعه می تواند بدلیل نیاز به ارسال مجدد همه قطعات توسط مبداء، 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 مبداء 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 بـه عنـوان رفتـار در هـر پـرش (PHB[1]) مطرح است. این PHB، باید در همه مسیریابها وجود داشته باشد و مخصوصاً PHB تنها بخشی از DiffServ است کـه در مسیریابهای درونی، پیاده سازی می گردد.

مسیریابهای مرزی نیز مکانیزم PHB را دارند، امـا مکانیزمهـای شـرایط پیچیـده تـر ترافیکـی لازم اسـت تـا سرویس های مورد نیـاز، فـراهم گـردد. بنـابراین مـسیریابهای دورنـی تابعیـت و سـربارکمتری بـرای فـراهم آوردن سرویس های DiffServ، دارند و این درحالیست که اکثر پیچیدگی بر روی مسیریابهای مرزی مـی باشـد. تـابع یـک گره مرزی نیز می تواند از طرف کاربردهای سیستم میزبان ، بوسیله سیستم میزبان متصل به دامنه، فراهم گردد.

تابع شرایط ترافیکی شامل ۵ عنصر می باشد:

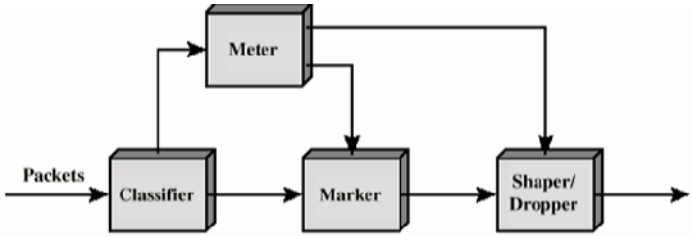
- طبقه بندی کننده[2]: طبقه بندی کننده ،جداکننده بسته ها بـه کلاسـهای مختلـف. طبقـه بنـدی کردن ، پایه ایجاد سرویسهای متفـاوت مـی باشـد. یـک طبقـه بنـدی کننـده ممکـن اسـت تنهـا ترافیکهای مختلف را برپایه مقدار DiffServ جدا کند (رفتـار طبقـه بنـدی کننـده متـراکم) و یـا براساس چندین فیلد در سرآیند بسته و یا حتی قسمت داده بسته، عمل کند(طبقه بنـدی کننـده چند فیلدی).
- پیمانه[3]: پیمانه وظیفه اندازه گیری ترافیـک بـرای پیـروی از یـک پروفایـل را دارد. پیمانـه تعیـین می نمایدکه آیا یک کلاس جریان بسته رسیده در سطح تـضمین شـده بـرای سـطح سـرویس آن کلاس است و یا از آن تجاوز کرده است.
- نشانه گذار[4]: نشانه گذار وظیفه نشانه گذاری مجدد بسته ها را با مقادیر DiffServ جدید برحـسب نیاز، به عهده دارد. این امر ممکن است برای بسته هایی اتفاق بیافتـد کـه از پروفایـل خـود تجـاوز نموده اند. برای مثال، برای یک گذردهی تضمین شده برای کلاس سرویس معین، هر بـسته ای در آن کلاس که از گذردهی در بازه های زمانی مشخص، تجاوز کنـد، ممکـن اسـت جهـت مـدیریت بهترین تلاش، دوباره نشانه گذاری گردد.

  همچنین نشانه گذاری مجدد در مرزهای بین دو دامنه DiffServ ، مورد نیاز باشد. برای مثال، اگـر یک کلاس ترافیکی با اولویت پشتیبانی بالا دریافت شود و مقدار آن در یکی ۳ و در دامنـه بعـدی ۷ باشد، بسته ها در دامنه اول با اولویت ۳ منتقل شده و در زمان ورود به دامنه بعـدی، مجـدداً بـا مقدار اولویت ۷ شماره گذاری می شوند.
- هشیار[5]: سیاست ترافیکیی که بوسیله به تاخیر انداختن بسته ها، در صورت لزوم ، زمینه جلوگیری از تخطی جریان یک کلاس خاص از نرخ ترافیکی مشخص شده در پروفایل آن را فراهم می آورد.
- دور انداز[6]: وظیفه دور انداختن بسته ها را در زمانیکه نرخ ترافیک بسته های یک کـلاس خـاص از معین شده در پروفایلش، تجاوز کرد را دارد.

تصویر زیر رابطه بین این ۵ عنصر را نشان می دهد.

---

[1] - Per-Hop Behavior
[2] - Classifier
[3] - Meter
[4] - Marker
[5] - Sharper
[6] - Dropper



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 توافقات 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 بریزد.

MPLS[1]:

استاندارد MPLS نشانگر تلاشهای جاری در زمینه تکامل سوئیچ لایه ای می باشد. هدف اولیه MPLS ترکیب کردن نمونه های تعویض برچسب[2] 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.

مروری بر MPLS:

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 تحویل 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.

مدل انتقال MPLS:

---

[1] - Multiprotocol Label Switching

[2] - Label swapping

در یک محیط MPLS، مسیر بهینه در طول شبکه بصورت پیشرفته مشخص می گردد. سپس با ورود بسته به شبکه MPLS، روترهای مرز ورود با استفاده از اطلاعات سرآیند لایه ۳، جهت تخصیص یکی از مسیرهای مشخص به بسته ها استفاده می نماید. این تخصیص برای افزودن یک **برچسب** ارجاعی به مسیر انتها به انتها به بسته ، بکار می رود. این برچسب به بسته داده در طول انتقال آن در شبکه پیوند می خورد. سایر مسیریابهای میانی مسیر از اطلاعات برچسب برای مشخص کردن مقصد پرش بعدی استفاده می نماید. بدلیل آنکه این مسیریابها تنها با اطلاعات برچسب کار می کنند، تجزیه و تحلیل ها و کلاس بندیهای پر CPU در سرآیند لایه ۳ تنها در نقاط ورودی اتفاق می افتد.

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

۱- مهندسی ترافیک[1]: مهندسی ترافیک فرایند انتخاب مسیرهای شبکه، بگونه ای که بهره برداری از تمام منابع شبکه با استفاده از الگوهای ترافیکی حاصل، به یک اندازه باشد.

مسیریابی بر پایه الگوریتمهای IGP متداول می تواند باعث انتخاب مسیری در شبکه گردد که بهره برداری نامتوازن از ابزارهای شبکه را باعث می گردد. در این محیط ها، برخی از ابزارهای شبکه بیش از حد بارگذاری دارند و درحالیکه برخی دیگر زیر حد بهره وری قرار دارند. یک حد پایین مهندسی می تواند با دستکاری معیارهای IGP مرتبط با پیوندهای شبکه، فراهم آید. اگرچه این تلاش برای مدیریت در محیطهای با تعداد بالای مسیرهای زائد، مشکل می باشد.

برای کسب مزایای مهندسی ترافیک، MPLS می تواند به همراه الگوریتمهای IGP مورد استفاده قرار بگیرد. استاندارد MPLS می تواند توانایی مسیرهای مشخص برای مسیردهی و عبور بسته های داده در شبکه را مشخص نماید. این مسیردهی صریح بسته های داده اطمینان می دهد که یک جریان مشخص از داده از مسیر مشخص شده استفاده می نماید. با نظارت و مدیریت این جریانات داده، بهره برداری موثر از منابع شبکه قابل حصول می باشد. مسیردهی صریح از طریق گزینه های مسیردهی مبداء در مسیریابی IP متداول، حاصل می گردد. 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 می گردد.

همچنین MPLS توانایی تجزیه و تحلیل فیلدهای خارج از سرآیند بسته IP را در زمان تعیین مسیر صریح برای بسته داده فراهم می آورد. برای مثال، مدیر شبکه می تواند سیاستهای جریان ترافیک را برپایه مکان و زمان ورود بسته به شبکه تعیین کند. در شبکه های مرسوم، این اطلاعات تنها در مبادی ورودی در دسترس می باشند. تجزیه و تحلیل اضافی زمینه ساز مدیریت با کنترل بالاتر و در نتیجه سطوح سرویس قابل پیش بینی بهتر می گردد.

۲-کیفیت سرویس مسیردهی: کیفیت سرویس مسیردهی، توانایی انتخاب یک مسیر برای یک جریان داده مشخص می باشد تا مسیر سطح سرویس مورد تقاضا را براورده نماید. این سطوح سرویس می توانند سطوح قابل قبول در پهنای 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، می باشد.

فراهم آوردن یک مسیر شبکه برای ارائه یک QoS مورد تقاضا، اغلب نیازمند استفاده از مسیردهی صریح می باشد. برای مثال، تخصیص یک مسیر برای یک جریان نیازمند تخصیص پهنای باند خاص، سرراست می باشد. اگرچه، این احتمال وجود دارد که ترکیب پهنای 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 گردند. این امر نیازمند سطح دانه بندی کوچکتر[2] می باشد که توسط استاندارد مهندسی ترافیک، فراهم می گردد.

---

[1] Traffic Engineering -

[2] finer level of granularity -

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 می تواند برای اولویت بندی هوشمند ترافیک در هر گره شبکه بکار رود.
- ☑ شبکه MPLS می تواند چندین مسیر بین نقاط ابتدایی و انتهایی پیش بینی کند. هر مسیر برای حصول سطوح مختلف سرویس مورد ارزیابی و مهندسی قرار می گیرد.

این دیدگاه بسادگی بسته ها را به یک کلاس از طبقه بندی سرویس دسته بندی می کند. سیاستهای مدیریت محلی شبکه تعیین کننده سرویسهای فراهم شده برای هر طبقه می باشد.

۳- پشتیبانی از چند پروتکلی: استاندارد MPLS پشتیبانی از پروتکلهای لایه شبکه موجود ، همانند IPV4، IPV6، IPX و AppleTalk را نیز به همراه دارد. استاندارد همچنین پشتیبانی از لایه پیوند در اترنت، Token-ring، FDDI، ATM، Frame relay و پیوندهای Point to Point را فراهم می آورد. 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 می گردد.

لغت شناسی:

- ☑ **کلاس هم ارزی ارسال(FEC[1]):** یک FEC گروهیست از بسته های لایه ۳ که بصورت مشابه انتقال می یابند. همه بسته ها در این گروه از مسیر یکسانی در شبکه منتقل می شوند و اولویت یکسانی دارند. بسته های FEC ممکن است اطلاعات سرآیند لایه ۳ متفاوتی را داشته باشند. اگرچه، برای ساده سازی تصمیم در مورد انتقال، ین بسته ها از هم جدا نمی شوند.

  نمونه های رایج FEC عبارتند از:
  - مجموعه ای از بسته ها که مسیر مشخص یکسانی را در جدول مسیردهی IP دارند.
  - مجموعه ای از بسته ها که مسیر مشخص یکسانی را در جدول مسیردهی IP و تنظیمات نوع سرویس یکسانی در سرآیند IP دارند.

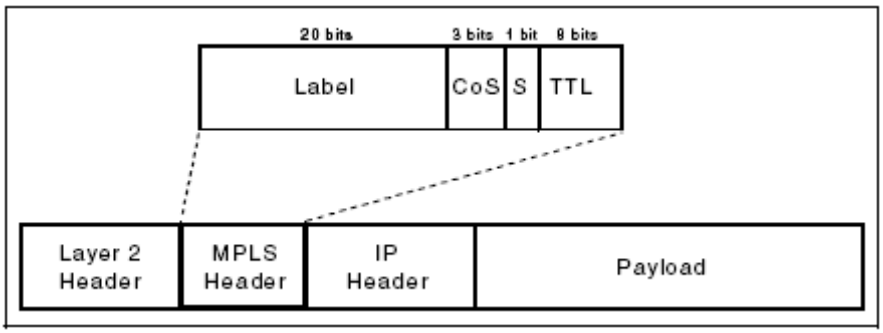
  در شبکه MPLS، یک FEC توسط یک برچسب مشخص می گردد.
- ☑ **برچسب و بسته های برچسب خورده:** براساس آنچه در بالا ذکر گردید، یک برچسب، یک FEC واحد را مشخص می نماید.

  یک برچسب بصورت محلی بین ۲ ابزار MPLS ارزشمند می باشد. این برچسب مبین یک توافق بین ۲ ابزار می باشد که توصیف کننده نگاشت بین یک برچسب و یک FEC می باشد. این حقیقت که برچسبها بصورت محلی دارای ارزشند زمینه ساز گسترش مقیاس پذیری MPLS در محیط های بزرگ گردیده است؛ زیرا نیازی به استفاده از برچسب مشابه در پرش وجود ندارد.

  برچسب MPLS می تواند 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 می گیرد. در یک شبکه ATM، فیلدهای VPI/VCI می توانند جهت ذخیره برچسب MPLS ذخیره بکار روند. در شبکه های Frame Relay نیز فیلد DLCI می تواند به این منظور مورد استفاده قرار گیرد.

[1] - Forwarding equivalency class

اگر فناوری لایه ۲ بصورت دورنی برچسب را مورد پشتیبانی قـرار ندهـد، برچـسب MPLS در یـک سرآیند گسترش یافته به این منظور قرار می گیرد. این سرآیند بین سرآیند لایـه ۲ و سـرآیند IP قرار می گیرد. به این ترتیب امکان استفاده از سرویس MPLS بر روی هر فناوری لایه ۲ ایی فراهم می گردد.



سرآیند ۳۲ بیتی MPLS

محتویات سرآیند MPLS عبارتند از:

- یک فیلد برچسب شامل مقدار واقعی برچسب MPLS.
- یک فیلد CoS که می توند برای تاثیر گذاری بر سیاستهای صف گذاری و دور ریختن در شبکه ای که بسته در حال عبور از آن می باشد، بکار رود.
- یک فیلد S (پشته) که می تواند یک پشته برچسب سلسله مراتبی[1] را حمایت کند.
- یک فیلد TTL[2] که IP TTL مرسوم را پشتیبانی می نماید.

یک بست برچسب دار در بسته ای ذخیره می گردد که برچسب رمز شده دارد. بـرای پـشتیبانی از توابع پیشرفته MPLS، بسته ممکن است واقعاً بیش از یک برچسب داشت باشد. بـه ایـن وضـعیت **پشته برچسب** می گویند. پشته یک رابطه ترتیب یافته بین برچـسب هـای مجـزا را ایجـاد مـی نماید. پشته بصورت LIFO مدل شده است. این ویژگـی بعـداً در بخـش "پـشته برچـسب و سلـسه مراتب برچسب" مورد بحث قرار می گیرد.

☑ **مسیریاب پشته برچسب(LSR[3])**: یک مسیریاب برچسب پشته، یک گره MPLS است که علاوه بر آن قابلیت انتقال بسته های 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 اجـرای توابـع MPLS. ایـن گره وظیفه مدیریت ترافیک ورودی به شبکه MPLS را دارد.
- گره Egress متصل کنند ه شبکه MPLS با گره فاقد توانـایی اجـرای توابـع MPLS. ایـن گره وظیفه مدیریت ترافیک خروجی از شبکه MPLS را دارد.

☑ **مدخل برچسب ارسال پرش بعدی(NHLFE[1])**: یک NHLFE بوسیله یک گـره MPLS ، جهـت انتقال بسته ها بکار می رود. حداقل برای هر FEC منتقل شـده توسـط گـره، یـک NHLFE وجـود دارد. هر گره وظیفه نکهدارنده اطلاعات یک NHLFE را برپایه اطلاعات زیر دارد:

---

[1] - hierarchical label stack

[2] - time-to-live

[3] - Label stack router

- آدرس پرش بعدی بسته
- عملیات انجام شده برروی پشته
  - جانشین سازی برچسب بالای پشته با برچسب جدید
  - برداشتن برچسب قدیمی از بالای پشته
  - جانشین کرده برچسب بالای پشته با برچسب با مقدار جدید خاص و انتقال یک یا چند برچسب خاص به پشته برچسب. با خاتمه این فرایند، پشته حداقل شامل ۲ برچسب MPLS می باشد.

- محصورسازی پیوند داده[2] مورد استفاده برای انتقال بسته(اختیاری)
- رمزگذاری پشته داده مورد استفاده جهت انتقال بسته (اختیاری)
- هر داده مورد لزوم دیگر جهت پردازش صحیح بسته.

☑ **نگاشت برچسب ورودی(ILM[3])**: 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.

☑ **نگاشتFEC به NHLFE (FTN[4])**: 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 MPLS، به یک 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 محتوی 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 توسط 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 پشته 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 پشته می باشد. با استفاده از این اطلاعات، گره برچسب جدید را رمز کرده و بسته حاصل را منتقل می نماید.

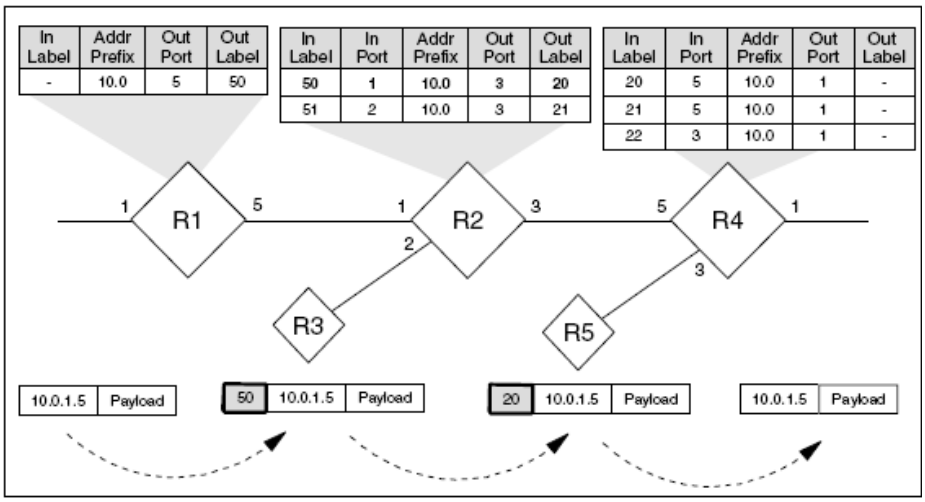
انتقال بسته بدون برچسب:

---

[1] - Next hop label forwarding entry
[2] - data link encapsulation
[3] - Incoming label map
[4] - FEC-to-NHLFE map

یک گره MPLS سرآیند لایه شبکه و هر گونه اطلاعات درخور و مورد نیاز جهت تعیین یـک FEC را ارزیـابی می کند. گره از FTN جهت نگاشت FEC به NHLFE استفاده می نماید. در این حالت پردازش بـسته هماننـد بـسته های برچسب دار می باشد. مقصد انتقال بسته و عملیات واقع شده بر روی پشته توسط NHLFE مشخص می گـردد. با استفاده از این اطلاعات، گره پشته برچسب جدید را رمز نموده و بسته حاصل را ارسال می نماید.

تصویر زیر نشاندهنده تعویض برچسب در یک محیط MPLS می باشد:



تعویض برچسب در محیط MPLS

توجه نمایید که در محیط تعویض برچسب، مسیریاب پرش بعدی همیشه توسط اطلاعات MPLS معین مـی گردد. این امر می تواند سبب گردد تا بسته از مـسیری متفـاوت از مـسیرهای مـشخص شـده توسـط الگوریتمهـای مسیریابی مرسوم، منتقل گردد.

برداشتن پرش یکی مانده به آخر:

یکی از توانایی های MPLS برداشتن یک برچسب MPLS در گره یکی مانده به آخر بجای گـره Egress مـی باشد. از دید ساختاری، چنین پردازشی مجاز می باشد. هدف برچـسب انتقـال یـک بـسته در شـبکه بـه یـک گـره Egress می باشد. زمانی که گره یکی مانده به آخر تصمیم گرفت تا بسته را به گره Egress منتقـل کنـد، برچـسب دیگر هیچ عملکردی را ندارد و دیگر در بسته مورد نیاز نیست.

گره ماقبل آخر برچسب را از پشته برداشته و بسته را براساس اطلاعـات آدرس بعـدی NHLFE منتقـل مـی 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 کـه گـره ماقبـل آخـر بـسته ای بـا حداقل ۲ برچسب را پردازش کرده باشد. در این حالت، برچسب بالای پشته، برچـسبی اسـت کـه گره Egress برای تصمیم گیری در مورد انتقال بسته ، باید آن را پردازش نماید.
- ☑ بسته فاقد برچسب می باشد. در ایـن حالـت، Egress LSP یـک بـسته لایـه شـبکه اسـتاندارد 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 ابتـدای لیـست بـه سـمت گـره انتهای 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 LSR egress 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:

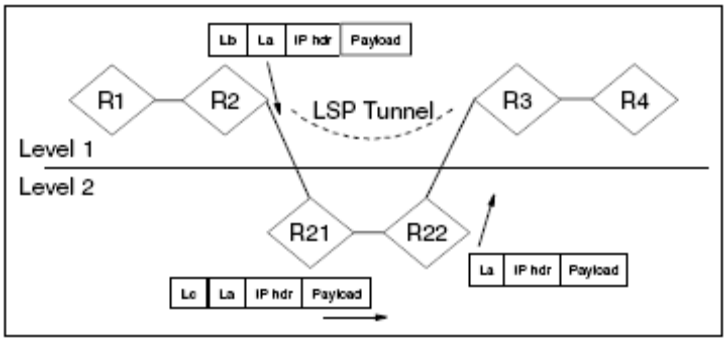
یک بسته برچسب دار می تواند شامل بیش از یک برچسب باشد. این برچسب ها بصورت پشته آخرین ورود-اولین خروج نگه داری می شوند. پشته، یک سری طبقات مرتب را بین مجموعه برچسب ها پیاده سازی می کند.

این طبقه بندی زمانی بکار می رود که یک گره MPLS یک بسته را به گره MPLS دیگری تحویل می دهد، اما این گرها، 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 منتسب 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 نقاط انتهایی یک تونل LSP می باشند. توالی 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:



تونلهای LSP

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 R2، R1 و R3 می باشند. از منظر دید سطح ۲، ابزار هم مرتبه R2، R21 می باشد.

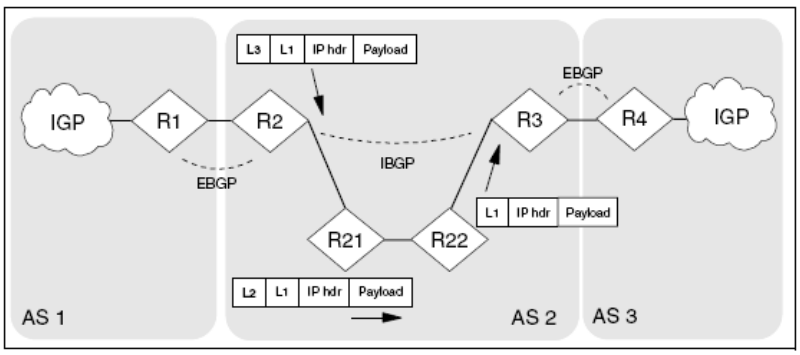
با استفاده از این دیاگرام، عملیات زیر در حین ارسال یک بسته از طریق تونل LSP رخ می دهد:

- ☑ 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 La 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 Lb نامیده می شود. اکنون پشته برچسب شامل ۲ مدخل می باشد.
- ☑ R2 بسته را به R21 ارسال می کند.
- ☑ R21 برچسب سطح ۲ (Lb) افزوده شده توسط R2 را بر می دارد و یک برچسب لایه ۲ قابل درک توسط R22 را جانشین آن می سازد. این برچسب Lc 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 (Lc) را برداشته 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 ارتبط در AS ها، اجرا می کند. برای مثال R2، R21، R22 و R3 ممکن است از OSPF برای حفظ مسیر در AS 2 استفاده می شود.
- ☑ هر سیستم Autonomous، BGP را برای حفظ ارتباط بین AS ها اجرا می کند. برای مثال ، مسیریابهای لبه R1، R2، R3 و R4 از BGP برای تبادل اطلاعات مسیردهی بین ASیی استفاده می کنند.



اتصال سیستم های Autonomous در یک محیط MPLS

در این شبکه ساده، خوشایند است تا از توزیع مسیرهای آموخته شده BGP برای ابزارهایی کـه مـسیریابهای BGP نیستند (برای مثال R21 و R22)، اجتناب گردد. این امر سبب کاهش پـردازش هـای CPU مـورد نیـاز جهـت نگهداری جدول مسیردهی IP در ابزارها می گردد. همچنین این امر زمینه سـاز حـذف اجـرای الگـوریتم مـسیریابی BGP در این ابزارها می باشد.

یک پشته LSP MPLS می تواند به این منظور مورد استفاده قرار گیرد. در این پیکربنـدی، مـسیرهای BGP تنها به BGP های همسان توزیع شده است و نه به مسیریابهای درونی که در مسیر Hop-by-Hop بین همـسان هـا وجود دارد. تونلهای LSP بگونه ای پیکربندی می شود تا:

- ☑ هر زوج یک برچسب را برای هر آدرس Prefix توزیع می نماید که از طریق BGP توزیع می گردد. این برچسب 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 درونـی، یک برچسب برای مسیر میزبان به هر IGP همسایه توزیع می نماید.

وضعیتی را در نظر بگیرید که R2 یک بسته فاقد برچسب برای یـک شـبکه متـصل شـده از طریـق AS 3 را دریافت می نماید. بسته ممکن است در ابتدا از یک LAN محلی متصل به R2 و یا LAN دیگری در AS 2 آمده باشـد. بسته در صورتیکه از AS 1 آمده باشد، قبلاً برچسب خورده است.

- ☑ R2 جدول ارسال IP محلی را جـستجو مـی نمایـد تـا بهتـرین مـسیر بـرای آدرس مقـصد مـورد درخواست را مشخص نماید. این مسیر از طریق BGP مشخص می گردد. پـرش بعـدی BGP، R3 خواهد بود.
- ☑ R3 قبلاً یک برچسب برای طولانی ترین تطبیق ممکن ارائه داده و آن را به R2 توزیع مـی نمایـد. این برچسب L1 نامیده می شود.
- ☑ بنابراین همه ابزارهای AS 2 در IGP شرکت می کنند، یک مسیر به R3 در جدول مسیریابی بـرای تمام ابزارهای موجود در AS 2 مشاهده می گردد:
  - ▪ R22 قبلاً یک برچسب را برای R3 ایجاد نموده و این برچسب را بـه R21 توزیـع مـی نمایـد. این برچسب L2 نامیده می شود.
  - ▪ R21 قبلاً یک برچسب را برای R3 ایجاد نموده و این برچسب را به R2 توزیع می نماید. ایـن برچسب L3 نامیده می شود.

- ☑ R2 یک بسته داده با مقصد AS 3 را با ایجاد یک پشته برچسب، فراهم می آورد. مـدخل اولیـه بـر روی پشته با ورود L1 به آن ایجاد می گردد. مدخل بالایی پشته بـرروی پـشته بـا ورود L3 بـه آن ایجاد می گردد. سپس بسته برچسب خورده به پرش بعدی ،R21 ، ارسال می گردد.
- ☑ R21 بسته برچسب دار را دریافت نموده و برچسب بالایی پشته را بررسی می نماید. بـا اسـتفاده از اطلاعات NHLEF، R21 برچسب L3 را با برچسبL2 جانشین می نمایـد. سـپس بـسته برچـسب خورده به پرش بعدی ،R22 ، ارسال می گردد.
- ☑ R22 بسته برچسب دار را دریافت نموده و مدخل بالایی را بررسـی مـی نمایـد. بـدلیل آنکـه R22 پرش ماقبل آخر در تونل R2-R3 می باشد، R22 برچسب L2 را از بالای پـشته برداشـته و بـسته داده را به R3 می فرستد. اکنون پشته برچسب در حیب انتقال به R3 تنها دارای یک برچسب مـی 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 LSP egress گره ایست 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 LSR دیگری 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 پرنماید. پروتکلهای توزیع برچسب این اطلاعات را جهت ایجاد برچسب ها بکار می برند. پس از اجرای یک پروتکل توزیع در هر گره، کل شبکه MPLS باید دارای یک مجموه 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:**پیشنهادات جدید برای فراهم آوردن امکان مبادله اطلاعات توزیع 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 پیشتر 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[1] 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 انتها به انتها 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 مواقعی 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.

---

[1] - 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 درخواست[1]: 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 جریان[2]

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 محییط مبتنی بر فریم، سرراست می باشد. ابزار انجام دهنده ادغام، چندین برچسب Upstream را به یک برچسب Downstream نگاشت می نماید. هیچ تغییری در روالهای تعویض برچسب MPLS 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. الزامی 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 MPLS، با مشکل موجه می شویم. در این حالت، سلول های ورودی از چند VC، در یک VC خروجی یکه، جاداده 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 VCخروجی 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

---

[1] - Unsolicited Downstream

[2] - Stream merge

ارسال، به تعویق می اندازد. با دریافت نشانگر خاتمه ارسال، فریم بعدی مـی توانـد بـصورت کامـل ارسال گردد. این نوع بافر کردن و توانایی ذخیـره و ارسـال، بطـور مـشخص در سـوئیچهای ATM موجود، وجود ندارد.

- ☑ ادغام VP اجازه می دهد تا چندین VP در یک VP خروجی یکه، ادغام گردد. VCI متفـاوت در VP ادغامی برای تشخیص فریمهای مبادی مختلف بکار می رود.

ادغام VP دارای این مزیت می باشد که با درصد بالایی از تجهیزات ATM موجـود در شـبکه هـای جـاری، سـازگار مـی باشـد. همچنـین تـاخیر روش قبلـی در نقـاط ادغـام را نـدارد و همچنـین نیازمندیهای بافرکردن جدید را نیز ندارد.

اصلی ترین ضعف این روش آنست که نیازمند تخصیص مختصات VCI در هر VP می باشد.

ویژگیهای معماری MPLS ، هر دو روش ادغـام VP و ادغـام VC را پـشتیبانی مـی نمایـد. سـوئیچهای ATM شرکت کننده در MPLS باید توانایی آن را داشته باشند تا تشخیص دهند که سوئیچهای همـسایه از ادغـام VP و یـا ادغام VC استفاده کرده اند و یا ادغامی انجام نداده اند.

سوئیچ Lambda چندپروتکلی

راه حلهای بهبود هزینه و مقیاس پذیری برای معماری، پیچیـدگیهای داده ای شـبکه را افـزایش مـی دهـد. همچنین این راه حلها باید ویژگیهای بهبود کارایی را نیز فراهم آورنـد. برخـی از ایـن نیازمنـدیها توسـط اسـتاندارد MPLS عنوان گردید. این نیازمندیهای تجاری، قابل اعمال بر شبکه های انتقالی نوری (OTN[1]) می باشد. در نتیجـه، تلاشها در جهت توسعه ویژگیهایی برای یکسان سازی توابع MPLS در ابزارهای OXC[2] در حال انجام است. نـام ایـن فعالیت MPλS می باشد.

توسعه توابع MPLS به شبکه های نوری مزیتهایی را به همراه دارد:

- ☑ این روند مـی توانـد بـه عنـوان اهرمـی در جهـت توسـعه تکنیکهـای MPLS بـرای فـراهم آوردن متدولوژیی برای فراهم آوردن کانالهای نوری بلادرنگ، بکار رود. ایـن زمینـه سـاز توسـعه و ترقـی سریعتر این فن آوریها می گردد.
- ☑ این روند می تواند دید واحدی را برای مدیریت شبکه برای هر دو محـیط داده ای و نـوری فـراهم آورد. این امر سبب ساده سازی تلاشهای کلی می گردد.
- ☑ این تلاش می تواند معماری واحدی را فراهم آورد که اجـاز مـی دهـد تـا یـک LSP از ترکیبـی از مسیریابها و ابزار OXC عبور نماید. این امر زمینه ساز آنست تا شـبکه در وضـعیتی قـرار بگیـرد تـا پهنای باند برحسب درخواست واقعی را فراهم آورد.
- ☑ این تلاشها مـسیریابهای IP را در مـوقعیتی قـرار مـی دهـد تـا توانـایی یکـسان سـازی احتمـالی 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 می باشد:

- ☑ در MPLS، یک LSP یک مسیر Point to Point را ارئه می دهد که توسـط مجموعـه ای از بـسته های برچسب دار مورد عبور واقع می شود. در MPλS ، یک کانال نـوری دنبالـه دار بـرای توصـیف اتصال نوری Point to Point بین دو نقطه دسترسی ، مورد استفاده قرار می گیرد.

---

[1] - Optical Transport Network

[2] - optical cross-connect

[3] - Dense Wave Division Multiplexing

- ☑ در یک شبکه MPLS، یک LSR 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 برعهده 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 برعهده 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 MPλS، این امکان وجود خواهد داشت تا فیبر در OTN به عنوان مجموعه ای از پیوندها بکار رودکه هر پیوند دربردارنده مجموعه ای از کانالهاست. 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، تفاوتهای مهمی بین یک شبکه MPLS و یک OTN قابل بیان است:

- ☑ در یک شبکه MPLS، اطلاعت 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.

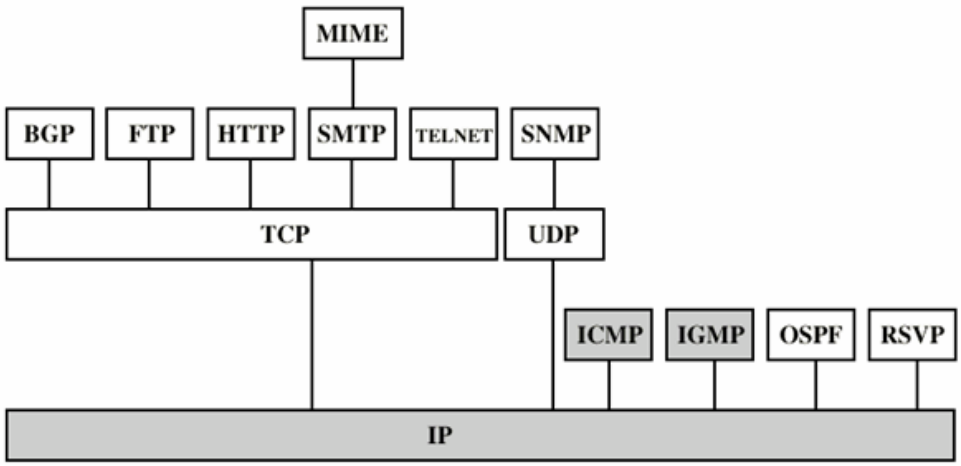
بخش ۴:
پروتکل های شبکه

فصل ۹: پروتکل IP
فصل ۱۰: پروتکل های IGMP و ICMP
فصل ۱۱: کنترل اتصالات در شبکه
فصل ۱۲: پروتکله های UDP و TCP

فصل ۹:

پروتکل IP

پروتکلIP بستر مناسبی برای تبادلات بین شبکه ای است ولی IP به صورت بدون اتصال است و TCP می تواند اتصال گرا است .



Internetworking Protocol in Context

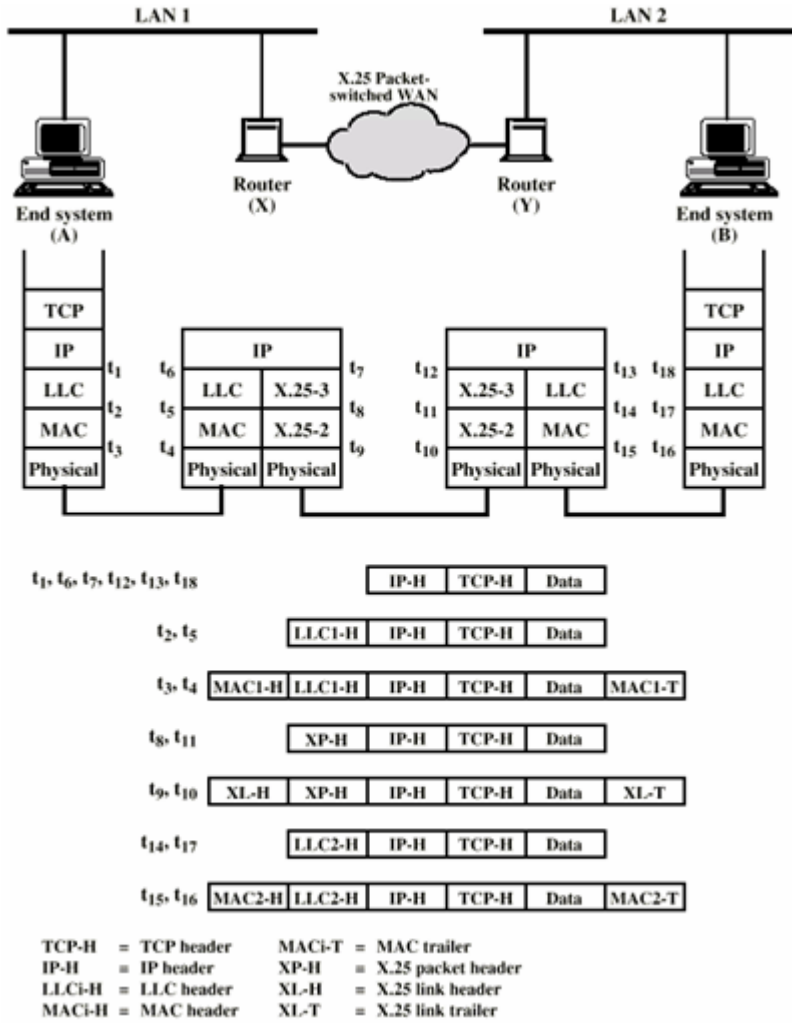
UDP: برای مواقعی که رسیدن Data به مقصد چندان مهم نیست.

OSPF: مسیریابی

RSVP : رزرو منابع برای تخصیص یک پهنای 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 INTERNETWORKINGمناسب است. باید بتواند موانع زیر را بر طرف کند . (موانعی که باعث مشکل شدن اتصال دو شبکه می شوند .)

- روشهای مختلف آدرس دهی در شبکه های مختلف
- تفاوت در اندازه بسته ها در شبکه های مختلف
- اختلاف در نحوه دسترسی به شبکه ها
- اختلاف در TIMEOUT ها .
- تفاوت در روشهای مختلف کنترل خطا .
- روشهای مسیریابی .
- روشهای مختلف کنترل دسترسی کاربران .
- اتصال گرا بدون اتصال بودن شبکه های فرعی .
- گزارش وضعیت ، (شامل اطلاعات آماری [مثلا 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 INTERNETWORNING کامل است .

آیا می توان گفت که اینترنت یک WAN است؟اینترنت هم یک WAN نیست . زیرا WAN بایید 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 رویLAN .

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 وداده.

(پارامتر های DELIVER هم به همین صورت است)

عملیات در مبدأ برای ارسال بسته های IP :

۱. 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 اگرنباشد به ROUTER داده شود .)
۴. انتقال دیتاگرام به پروتکل زیرین

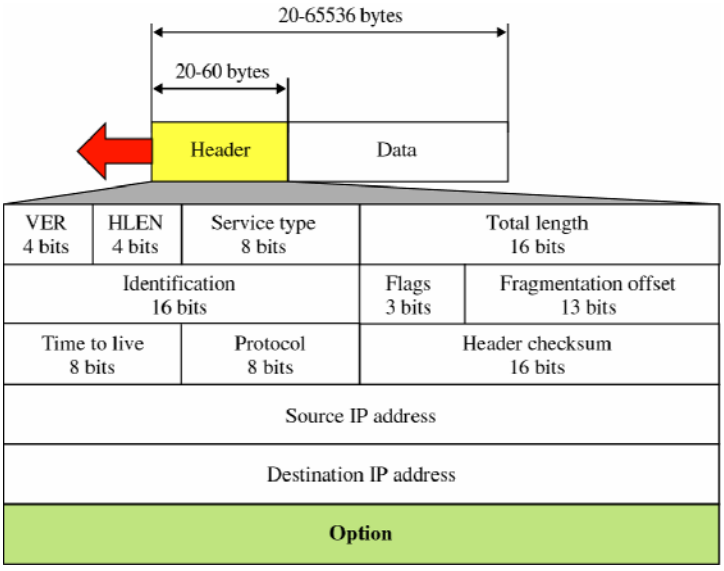
عملیات ROUTER :

- انجام عملیات Checksum (اگر Checksum محاسبه شده با 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 ازPADING استفاده میکند یعنی بیتهای اضافی 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:



IP Format

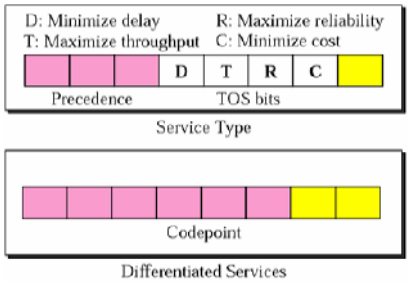
VER : version مربوط به Ip مورد استفاده را مشخص می کند . (مثلاً بسته توسط IP4 یـا IP6 فرسـتاده شده)

HLEN (Internet Header Length): طول Header را مشخص می کند (براساس ۳۲ بیتـی). از آنجـا کـه عدد مشخص شده در این قسمت عمدتاً در مبنای ۱۶ ذکر می شود ، باید در ۴ ضرب شود تا طـول سـرآیند بسته مشخص شود.

Service type :یعنی چه سرویسی باید به این بسته داده شود تا به مقصد برسد . شامل بیتهای زیر اسـت -
قابلیت اطمینان (کم یا زیاد) (۱ بیت).

- اولویت (سه بیت) : اگر دو بسته با هم برسند با توجه به این سه بیت تصمیم گرفته می شود .

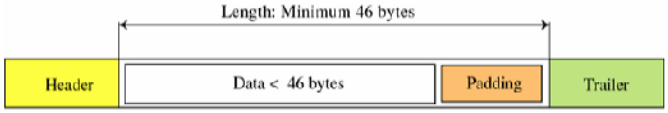
- گذردهی (۱ بیت) (کم یا زیاد) .
- تأ خیر (کم یا زیاد) .



ممکن است بجای نوع سرویس از Differentiated Sevices 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 2Bytes => 64kbyte 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.

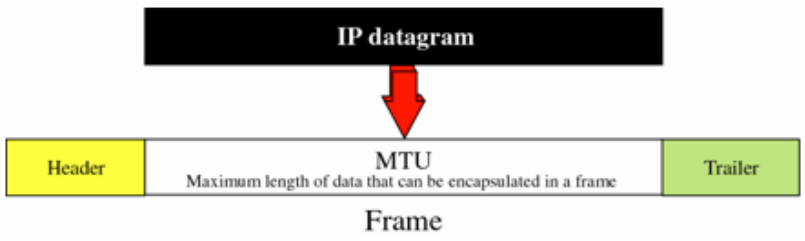


Identification : برای شناسائی بسته بکار می رود . باعث می شود که بسته بصورت یکتا باشد .

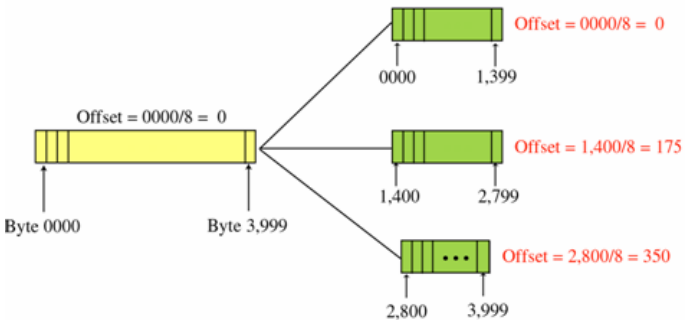
((id + آدرس مبدأ + آدرس مقصد) یک بسته یکتا می سازد)

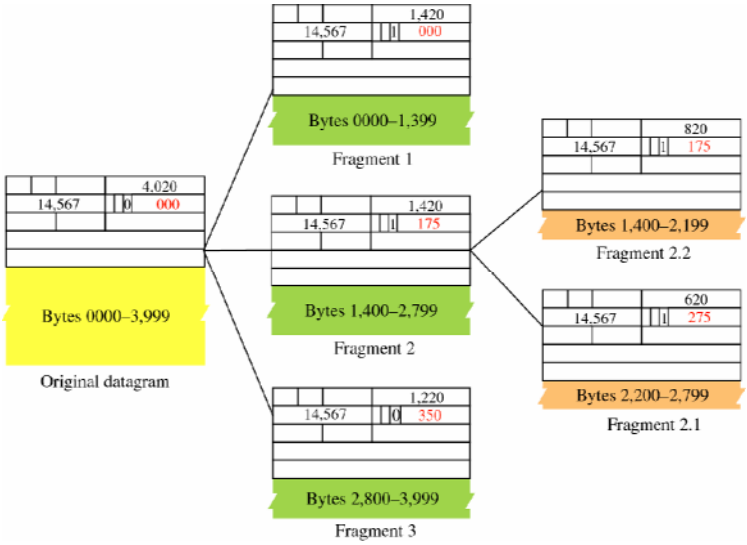
Flags : سه بیت است که از دو بیت ان استفاده می شود (یک بیت don 't fragment است و بیت دیگر more)

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 ، 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 اخرین قطعه است .

- offset نشان دهنده این است که این قطعه در کجای بسته اصلی قرار داشته است .

TTL : (Time to live) : 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 خطا برای خود header استفاده می شود .

برای کل بسته ، کنترل خطا وجود ندارد (درون بسته) .

source add & dest add : آدرسهای مبداء و مقصد را مشخص می کنند .

option padding : در این قسمت option های زیر می توانند قرارداده 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 نسخهIP می باشد و درست است. ۴ بیت بعد (0010) طول سرآیند را مشخص می کند که برابر با ۸=۴×۲ 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 دودویی دریافت می شود. تعداد بایتهای Option در این بسته چقدر است؟

مقدار HLEN، ۸ است. بنابراین طول کل سرآیند برابر با ۴×۸ یا ۳۲ است. سرآیند اصلی ۲۰ بایت اول را تشکیل می دهد و۱۲ بایت بعدی Option هستند.

مثال: یک بسته IP با HLEN 5_{16} و مقدار طول کلی فیلد 0028_{16} دریافت شده است. چند بایت داده در این بسته حمل می شود؟

مقدار HLEN ۵ است. بنابراین طول سرآیند ۲۰=۴×۵ بایت است و Option وجود ندارد. طول کلی ۴۰ بایت است که نشانگر آنست که ۲۰ بایت داده در این بسته حمل می شود(۲۰=۲۰-۴۰).

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، بایداز ۸ بایت اول(۱۶ عدد مبنای ۱۶) پرش کنیم. فیلد TTL در بایت نهم قرار دارد که مقدار 01 را دارد.این به این معناست که بسته قبل از دور ریخته شدن تنها می تواند یک پرش داشته باشد. فیلد پروتکل ، بایت بعدی است(02) که مشخص می کند این بسته به پروتکل IGMP مربوط می شود.

مثال: یک بسته با بیت M با مقدار صفر دریافت می شود. این بسته اولین قطعه، قطعه میانی و یا قطعه آخری می باشد؟ آیا می توانید 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 می باشد. اگرچه نمی توانیم بگوئیم که بسته اصلی تکه تکه شده است یا نه. یک بسته بدون تکه تکه شدن به عنوان آخرین قطعه درنظر گرفته می شود.

مثال: یک بسته با بیت M با مقدار یک دریافت می شود. این بسته اولین قطعه، قطعه میانی و یا قطعه آخری می باشد؟ آیا می توانید بگوئید بسته تکه تکه شده است یا نه؟

بیت M با مقدار یک نشانگر آنست که حداقل یک قطعه دیگر، وجود دارد. قطعه دریافتی می تواند قطعه اول و یا یک قطعه میانی باشد؛ اما قطعه آخر نخواهد بود. اما نمی توانیم 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 می توانیم بگوئیم که بسته تکه تکه شده است.

مثال: یک بسته با مقدار یک برای M و یک آفست قطعه صفر دریافت می شود. آیا این قطعه، اولین قطعه، قطعه میانی و یا قطعه آخری می باشد؟

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 می باشد.

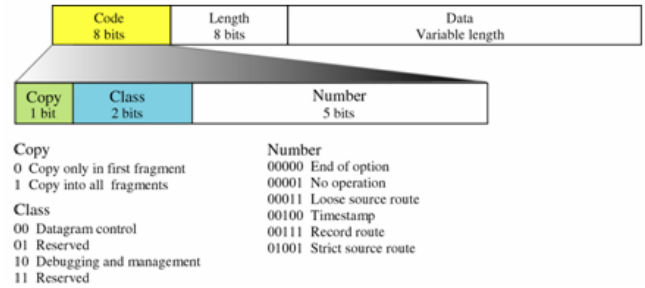
مثال: یک بسته با آفست ۱۰۰ دریافت می شود. شماره اولین و آخرین بایت آن چیست؟

برای یافتن شماره بایت اول قطعه، کافی است تا مقدار آفست را در ۸ ضرب کنیم. بنابراین شماره بایت اول برابر ۸۰۰ می باشد. بدلیل عدم اطلاع از طول داده ها، نمی توانیم شماره آخرین بایت قطعه را مشخص کنیم.

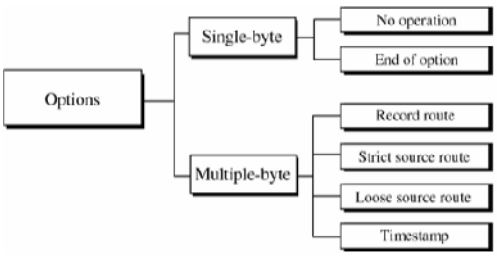
مثال: یک بسته با آفست ۱۰۰ ، HLEN ۵ و با مقدار ۱۰۰ برای فیلد کل طول ، دریافت شده است. شماره اولین و آخرین بایت آن چیست؟

شماره اولین بایت ۸۰۰=۸×۱۰۰ است. طول کل بسته ۱۰۰ بایت و طول سرآیند ۲۰ بایت (۲۰=۴×۵) می باشد؛ بنابراین طول بخش داده ۸۰ بایت است. اگر شماره بایت اول ۸۰۰ باشد، شماره بایت آخر ۸۷۹ می باشد.

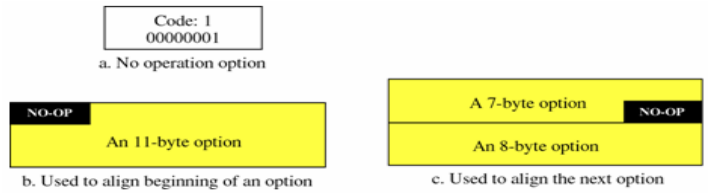
فرمت Option های بسته IP:



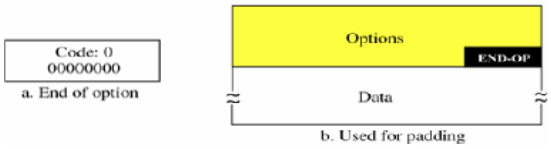
طبقه بندی Option های IP:



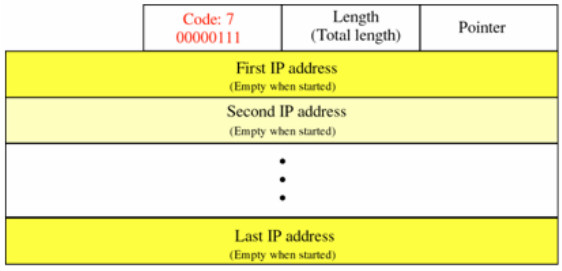
موارد استفاده از No Operation Option:



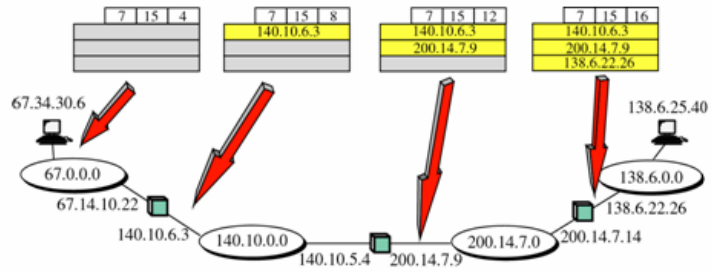
موارد استفاده از End of Option:



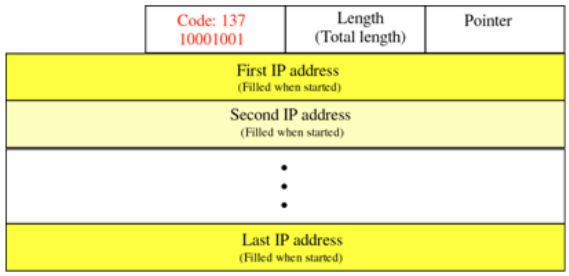
فرمت بسته Record Route Option:



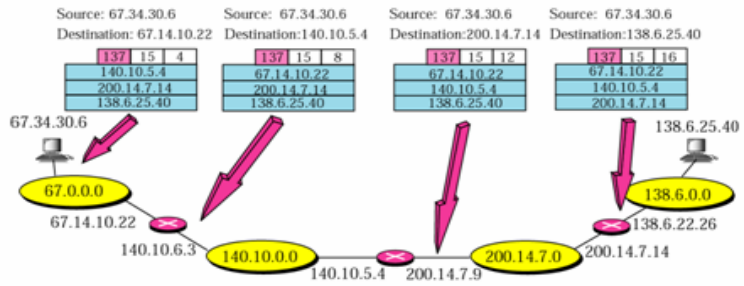
پس از عبور از هر مسیریاب،IP رابط خروجی آن مسیریاب در بسته نوشته می شود. قسمت آدرسها از ابتدا خالی است.



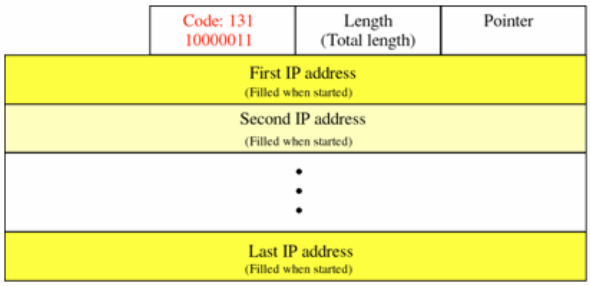
فرمت بسته Strict Source Route:



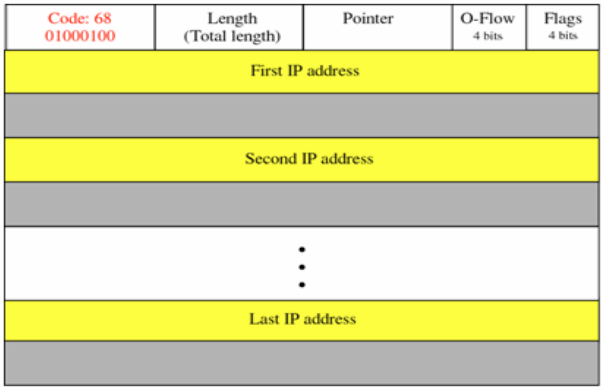
ابتدا IP رابط ورودی از مسیریاب دوم تا مقصد، در بسته ثبت شده است. هر مسیریاب ، IP رابط مسیریاب بعدی را برداشته و IP رابط ورودی خودش را جانشین آن می کند.



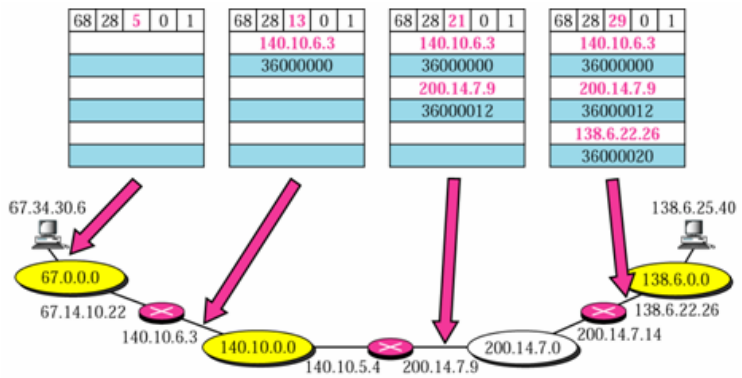
فرمت بسته loose Source Route:



فرمت بسته Timestamp:



در Timesatmp، هر مسیریاب زمان خود را در بسته مـی نویـسد. اطلاعـات ثبـت شـده در هـر مـسیریاب بوسیله Flag مشخص می گردد.



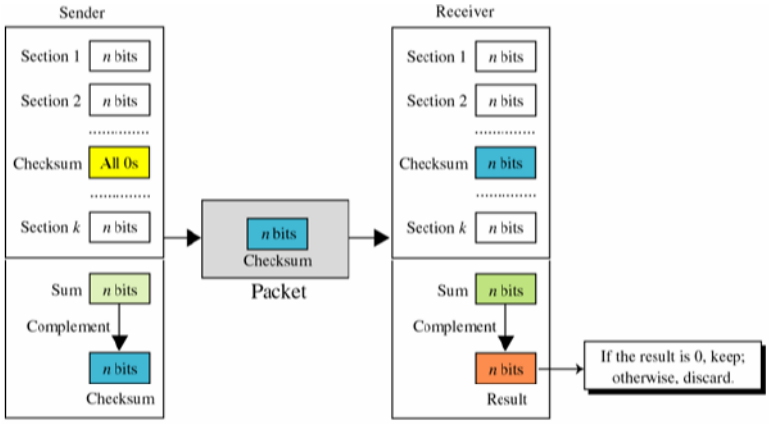
با توجه به فرمت Option ها، تنهـا Option هـای Strict source route و Loose source route بایـد در همه قطعات کپی شوند و نیازی به کپی کردن سایر Option ها در قطعات، بجز قطعه اول، نمی باشد. همچنین تنهـا Timestamp Option جهت دیباگ و اشکالزدایی مورد استفاده قرار می گیرد و سایرین جهت مقاصد کنترلی مـورد استفاده قرار می گیرند.

نحوه محاسبه Checksum:

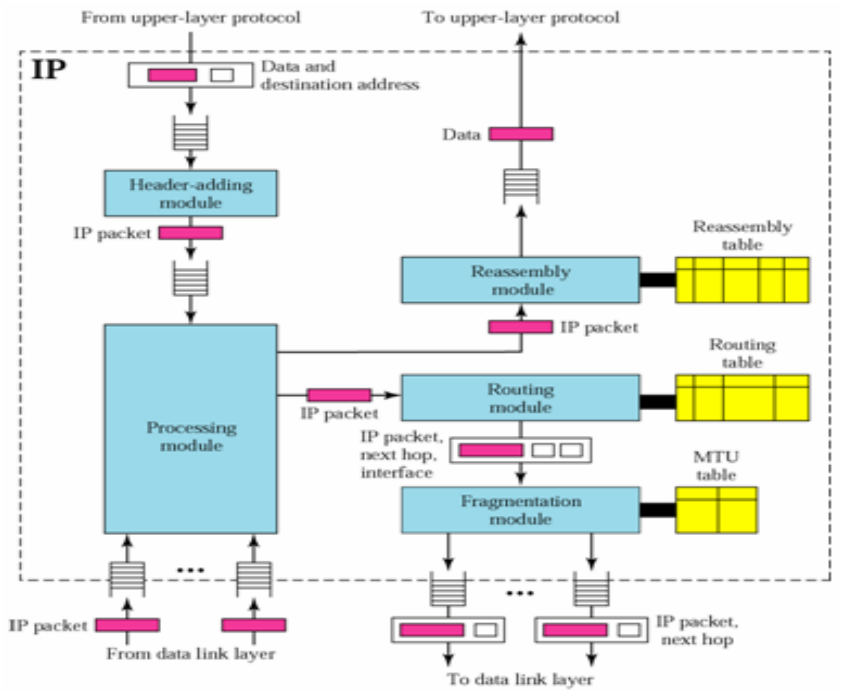
۱. تقسیم بسته به k قسمت n بیتی
۲. جمع تمام قسمتها با یکدیگر بصورت مکمل یک

۳. مکمل کردن جواب

در ابتدا در سمت فرستنده، مقدار صفر به Checksum تخصیص داده شده و مقدار Checksum براساس این مقدار بدست می آید و در فیلد Checksum قرار می گیرد. در گیرنده ، دوباره Checksum محاسبه شده و این بار باید پس از مکمل گیری نهایی ، حاصل صفر گردد تا اطمینان حاصل شود که بسته سالم است.



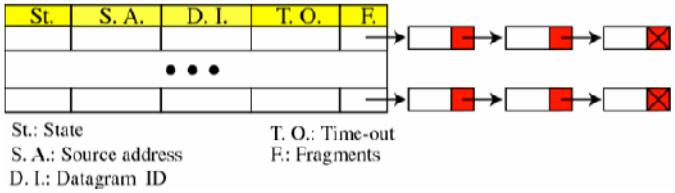
ساختار IP بصورت زیر می باشد:



جدول MTU، حداکثر 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 نمی کند .(چند بیت از این ۳۲ بیت هم برای HEADER و ... استفاده می شود) مثلاً در زمینه موبایلها هم که می خواهند از اینترنت استفاده کنند، تخصیص آدرس IP به این گوشیها فعلاً برآورده نمی شود .

مزایای IPV6 :

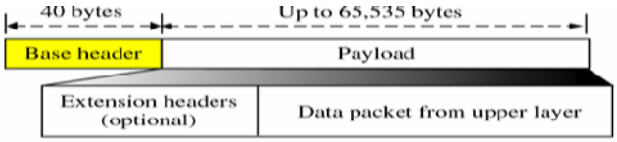
-آدرس ۱۲۸ بیتی است ۱۰ به توان ۲۳ ضرب در ۶ آدرس برای هر متر مربع از کره زمین یعنی برای هر مولکول یک آدرس می تواند اختصاص یابد !!!

- OPTION های زیاد و امکان سریعتر پردازش شدن بسته های IPV6

-امکان آدرسهای Multi cast

-دادن آدرسهای IPV6 به صورت Automatic

-پشتیبانی اختصاصی منبع (و ICMP V6 = ICMP V4 + IGMP V6)

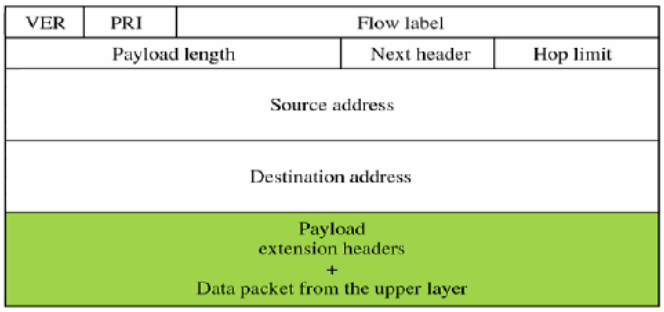


IPV6 Format

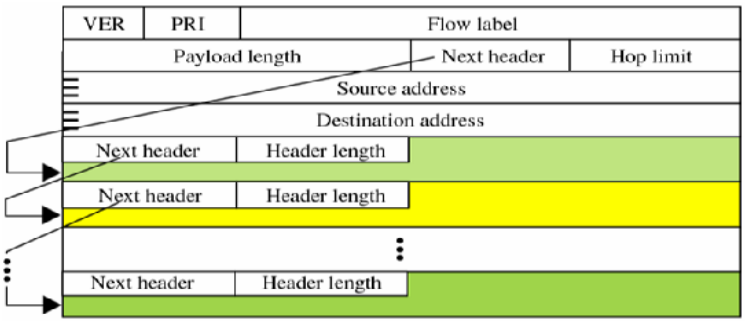
HEADER های زیادی در IPV6 می تواند وجود داشته باشد :

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 می شوند این است که سرآیندهای مختلفی در این بسته ها قرار دارد و با توجه به اطلاعات درون سرآیندها می توان 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



Version : 4 بیت است (برای نمایش عدد 6 و ...).

Traffic class : کلاس بسته را مشخص می کند (به خاطر اولویت) (8 بیت است) .

Flow lable : 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 64 k 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 خطا در 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 processing مهمتر از packet processing است .

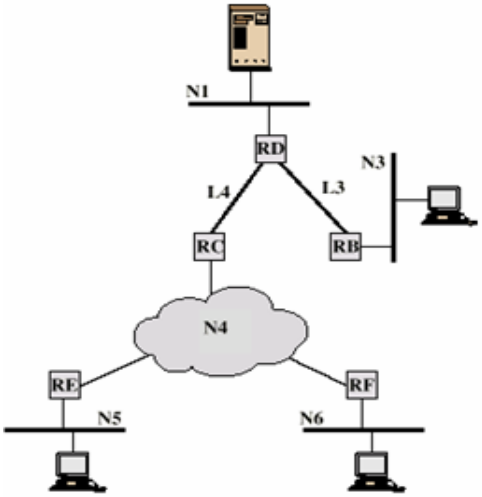
• مثلاً برای انجام یک chat تصویری online ممکن است سه flow وجود داشته باشد flow تصویری : که تصویر را ارسال می کند . flowصوتی : که صوت را ارسال می کند . flow (text) : عبارات type شده .هرچند که هر سه دارای آدرسهای مشابه هستند .

مهمترین مسأله در این مورد شناسائی نوع flow است . مسأله packet classitication درباره این موضوع است .در IPV6 یک فیلد برای flow وجود دارد (flow lable) . مسیریاب با نگاه کردن به این فیلد ، سرویس مورد نظر را به آن می دهد .

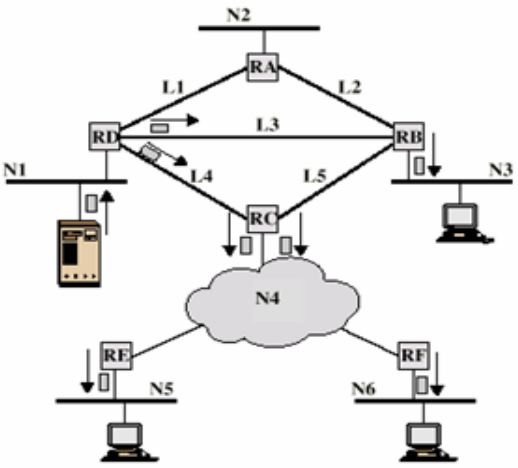
• Traffic class : کمی با موضوع flow lable تفاوت دارد . مثلاً مشخص می کند که چه مقدار delay یا Throughput یا ... مورد نیاز است .

• Multicasting : بدون اینکه بسته copy شود ، چگونه می توان بسته را به مقصدهای 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 ها یا Data base ها یا ... استفاده می شود) برای اینکار باید شبکه را بعنوان یک Spanning Tree ببینیم . 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

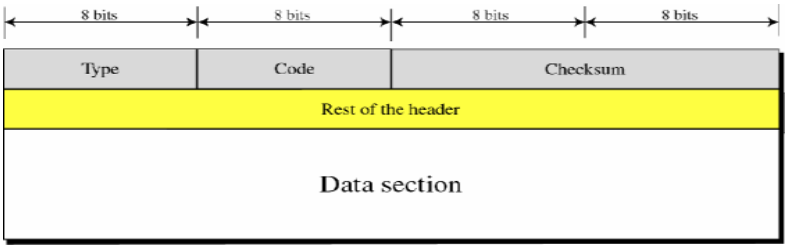
فصل ۱۰:

پروتکل های IGMP و ICMP

پروتکلهای ICMP و IGMP در لایه شبکه قرار دارند:

ICMP[1]:

این پروتکل وظیفه دارد که چنانچه اتفاقی غیر منتظره در شبکه اینترنت رخ دهد ، آن را گزارش دهد . ایـن پروتکل مستقیماً با IP کار می کند و FORMAT آن بصورت زیر است :



ICMP Format

TYPE : ۸ بیت است و نوع پیغام را مشخص میکند .

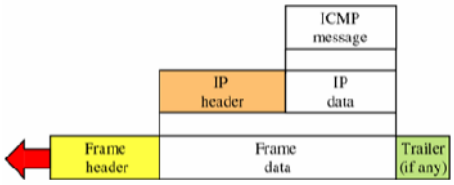
CODE : هشت بیت است و دربرخی از پیغام ها پیغام را مشخص تر میکند .

Checksum : ۱۶ بیت است که برای کنترل خطا 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 خطا

۸- پرسوجو(Query)

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 خطا ارسال می گـردد و بـرای سـایر قسمتها پیامی ارسال نمی گردد.

۳- پیام خطا برای بسته های با آدرس Multicast ارسال نمی گردد.

۴- پیام خطا برای آدرسهای خاص همانند 127.0.0.0 و یا 0.0.0.0 ارسال نمی گردد.

ICMP همیشه پیامهای خطا را به مبداء گزارش می نماید. انواع این پیام ها عبارتند از:

۱- مقصد در دسترس نیست(Destination Unreachable)

۲- خاموش شدن منبع(Source Quench)

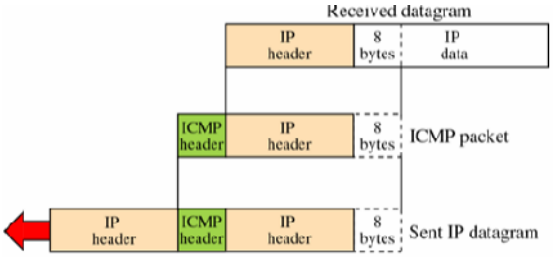
۳- تخطی زمانی(Time Exceeded)

۴- مشکلات پارامتر(Parameter Problems)

[1] - Internet control message protocol

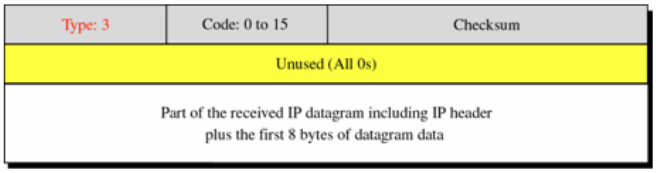
۵- تعیین مسیر دوباره(Redirection)

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.



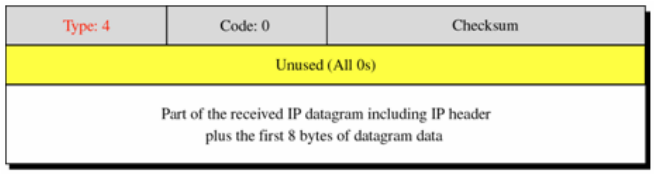
فرمت بسته های مختلف ICMP در ادامه ارائه شده است:

۱- مقصد در دسترس نیست:



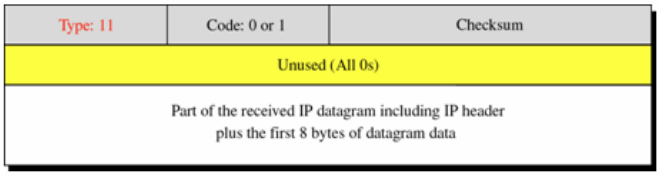
این پیام با کد ۲ و ۳ فقط بوسیله میزبان و با سایر کدها فقط بوسیله مسیریاب ایجاد می شود. مسیریابها توانایی تشخیص تمام مشکلاتی که مانع از تحویل بسته می شود را ندارد و از سوی دیگر مکانیزم کنترل جریان در پروتکل IP وجود ندارد.

۲- خاموش شدن منبع:



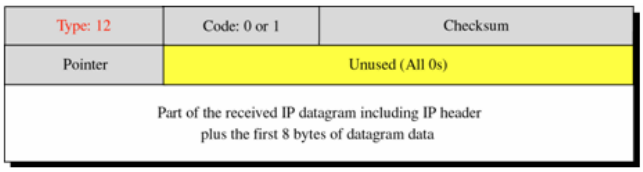
این پیام می تواند جهت هر Datagramیی که در اثر تراکم، چه در مسیریاب و چه در میزبان، دور ریخته می شود، تولید گردد. منبع به این ترتیب در جریان دور ریخته شدن بسته ها بدلیل تراکم شده و باید سرعت ارسال Datagramها را تا برطرف شدن تراکم، کاهش دهد.

۳- تخطی زمانی:



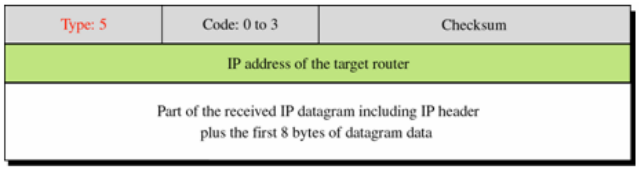
این پیام در مسیریاب برای بسته هایی ارسال می گردد که فیلد TTL آنها صفر شده است(کد صفر) و باید دور ریخته شوند. همچنین اگر مقصد در بازه زمانی مشخص، همه قسمتهای یک داده تقسیم شده را دریافت نکند، داده های دریافتی را دور ریخته و یک پیام تخطی زمانی به مبداء ارسال می کند(کد یک).

۴- مشکلات پارامتر:

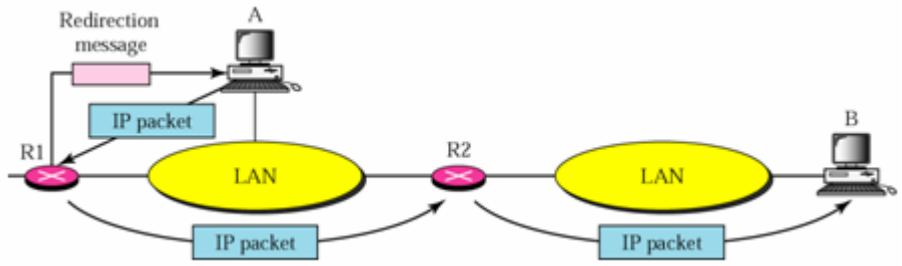


این پیام می تواند توسط یک مسیریاب یا مقصد تولید گردد. کد صفر نشانگر مشکل در سرآیند و کد یک نشانگر مشکل در فیلد Option می باشد. در این پیام یک اشاره گر در فیلد بدون استفاده پیام قرار می گیرد.

۵- تعیین مسیر دوباره:



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 اشتباهی 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 اشتباه بودن مسیر انتخابی را متذکر می شود.



کد ۱:Network Specific

کد ۲:Host Specific

کد ۳:Network Specific(Specified Service)

کد ۴:Host Specific(Specified Service)

مسیریاب این پیام را فقط برای میزبانهای شبکه محلی خودش می فرستد.

پیامهای پرسوجوی ICMP شامل موارد زیر می باشد:

۱- درخواست و پاسخ Echo

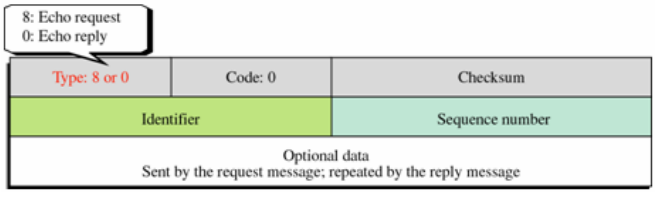
۲- درخواست و پاسخ Time Stamp

۳- درخواست و پاسخ Mask آدرس

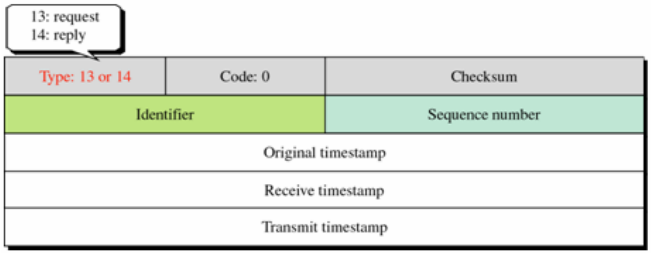
۴- تقاضای مسیریاب و اعلان (Solicitation & Advertisement)

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.



۲- پیام درخواست و پاسخ Time Stamp می تواند جهت محاسبه RTT بین یک مبداء و یک مقصد حتی در حالت عدم همزمانی بین آنها بکار رود.



جهت محاسبه RTT بشکل 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)

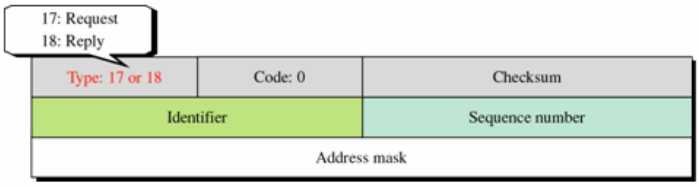
برای نمونه مقادیر زیر را در نظر بگیرید:

Value of original timestamp: 46
Value of receive timestamp: 59
Value of transmit timestamp: 60
Time the packet arrived: 67

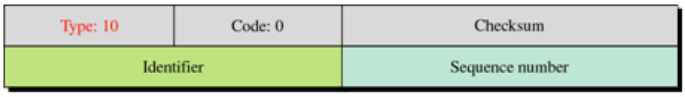
Sending time = 59 - 46 = 13 milliseconds
Receiving time = 67 - 60 = 7 milliseconds
Round-trip time = 13 + 7 = 20 milliseconds

Time difference = 59 - (46 + 10) = 3

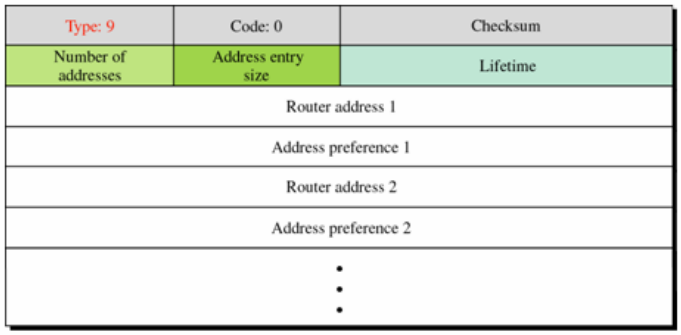
۳- درخواست و پاسخ Mask آدرس:



۴- تقاضای مسیریاب:



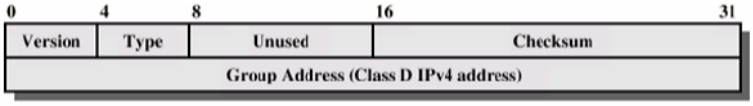
۵- اعلان :



IGMP[1] :

[1] - Internet Group Message Protocol

• پروتکل IGMP، یک پروتکل مدیریت گروه است که به مسیریابهای Multicastکمک می کند تـا لیـستی از اعضای ثابت مرتبط با هر رابط مسیریاب را ایجاد و بروز رسانی نماید. فرمت کلی پیام های این پروتکـل بـشکل زیر می باشد:



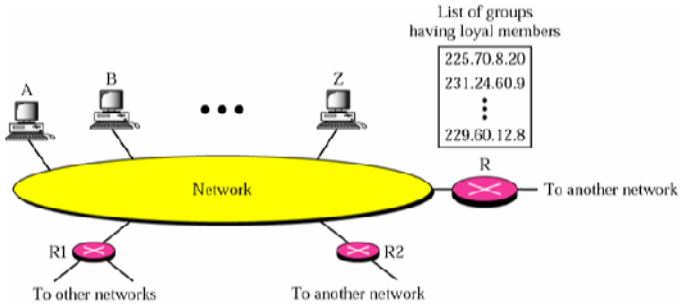
IGMP Format

- Version=1
- Type مقدار صفر دارد اگر Host گزارش بدهد و یک است اگر مسیریاب یک درخواست ارائه نماید.
- Group Address برای پیام های درخواست صفر و در غیر این صورت آدرس یک گروه معتبر است.

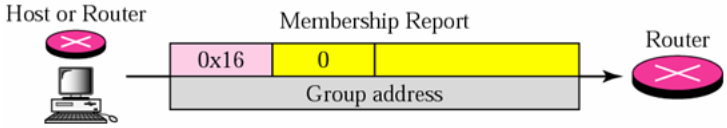
انواع پیامهای IGMP:

۱. گزارش عضویت(Membership Report)
۲. گزارش ترک(Leave Report)
۳. پرسوجو: شامل دو نوع عام(General) و خاص(Special). وجه تمایز این دو پیام در آن اسـت کـه در نوع عام مقدار فیلد آدرس گروه صفر است.

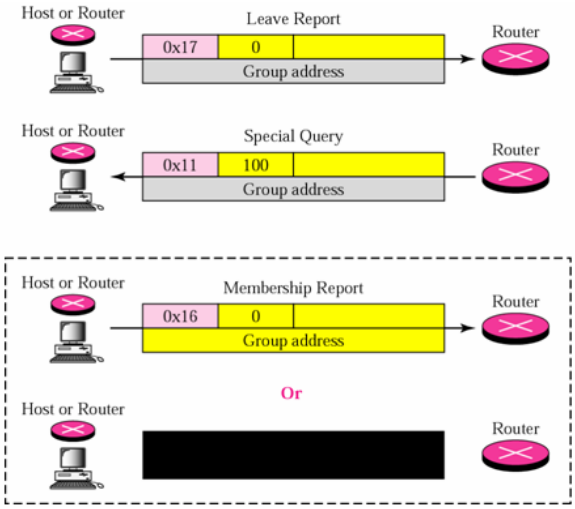
عملکرد کلی IGMP بصورت زیر می باشد:



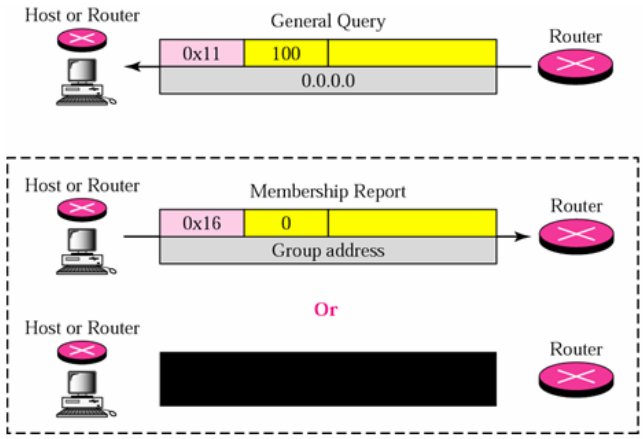
- میزبان برای افزوده شدن به یک گروه، پیام های گزارش عضویت را ارسال می نماینـد. ایـن پیـام دو بـار و پشت سرهم ارسال می گردد.
  - آدرس گروه مورد درخواست جهت افزوده شدن.
  - در IP Datagram این آدرس همانند آدرس مقصد multicast است.
  - همه host های در یک گروه پیام را دریافت می کنند.
  - مسیریابها برای دریافت تمام گزارش ها، به همه آدرسهای multicast گوش می کنند.



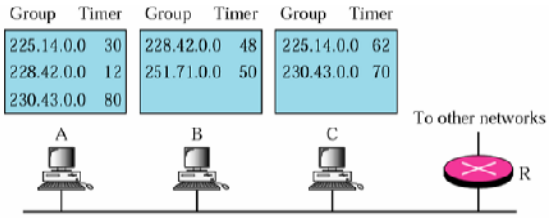
- میزبان برای حذف شدن از گروه از پیام ترک گروه استفاده می کند. سرور جهت اطمینان از صـحت پیـام ترک دریافتی، یک پیام پرسوجوی خصوصی به میزبان می فرستد و میزبان در صورت نیاز بـه مانـدن در گـروه یک پیام عضویت را ارسال خواهد کرد؛ وگرنه از گروه حذف خواهد شد.



- مسیریابها بصورت دوره ای پیام های پرسوجوی 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 پرسوجو 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.



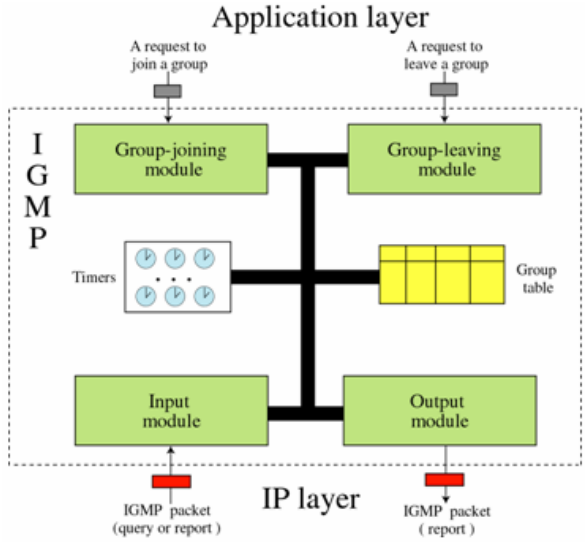
زمان ۱۲: تایمر آدرس 228.42.0.0 در میزبان A به پایان رسیده است و این میزبان یک پیام عضویت را ارسال می کند که بوسیله مسیریاب و همه میزبانها دریافت می گردد. میزبان B تایمر خود برای این آدرس را لغو می نماید.

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 بوسیله مسیریاب و همه میزبانها دریافت می گردد. میزبان C تایمر 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 تایمر خود برای این آدرس را لغو می نماید.

بسته IP حامل پیام IGMP دارای مقدار ۲ در فیلد پروتکل و مقدار ۱ در فیلد TTL خود می باشد. ساختار IGMP بشکل زیر می باشد:



ساختار جدول گروه نیز بشکل زیر می باشد:

State	Interface No.	Group Address	Reference Count
.....	.....	.....	.....
.....	.....	.....	.....
.....	.....	.....	.....

State: Free, Delaying, Idle
Reference Count: Number of processes interested

ICMP V6 = IGMP V4+ ICMP V4 .یعنی در IPV6 دیگر IGMP وجود ندارد و ICMP کار هر دو را انجام می دهد .

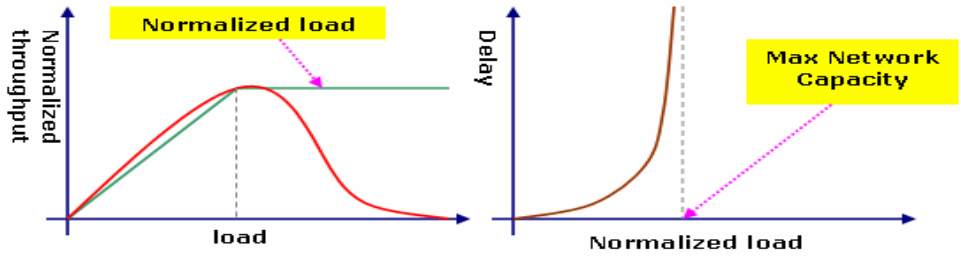
فصل ۱۱:

کنترل اتصالات در شبکه

استفاده بهینه از شبکه ها :

الگورتیم مسیریابی نقش مهمی در استفاده در از شبکه ها دارد ولی کنترل ترافیک هم از موارد مورد توجه است. باید مواظب 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 تواند کم شود .



Network Load Behavior

یعنی 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 شود . خود 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 بیتهای BECN/FECN در شبکه Frame RELAY) .

در هر لایه تصمیات می تواند باعث کنترل تراکم شود و می توان کنترل ترافیک انجام داد (یعنی 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 پـاک کـرد بلکـه ممکـن 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 ACKفرستاد . 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 طـول عمـر نبایـد زیاد کوچک باشد . روش ارسال بسته ها ROUND ROBIN و روش DISCARD کردن بسته ها مهم است .

پروتکل های دسترسی به محیط انتقال مشترک:

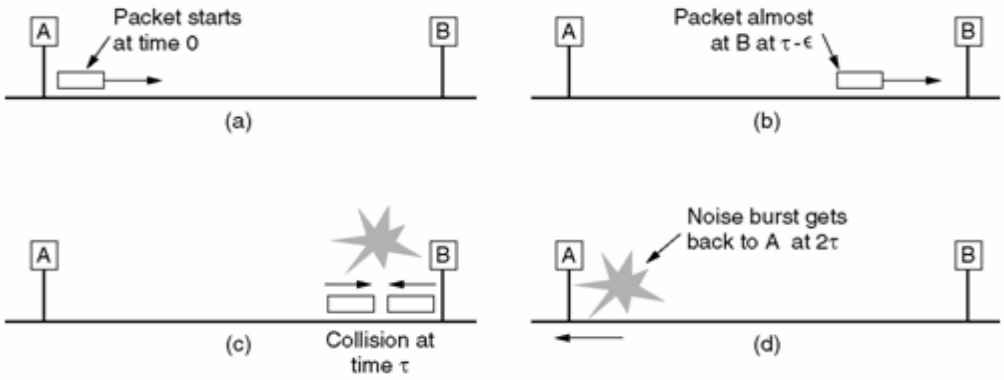
در شبکه های 100BASE از ۴ سیم به جای یک سیم استفاده می شود (در T4). این کار به خـاطر افـزایش سرعت انجام می شود .یک روش برای افزایش سرعت این است که در یک سیگنال تعداد بیت های بیـشتری ارسـال شود تا از پهنای باند موجود بیتهای بیشتری ارسال شود . روش دیگر استفاده از چند سیم به جای یک سـیم اسـت . در T4 یک سیم مخصوص رفت است و یک سیم مخصوص برگشت و دو سیم دیگر به صورت رفت و برگـشت اسـت 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 (a) که باید در محدوده قابل قبولی باشد .

$$\alpha = \frac{T_{Propagation}}{T_{Transmission}}$$

$T_{Propagation} = v/d$: برای شبکه های سیمی v برابر با ۲/۳ سرعت نور می باشد و d فاصله انتقال است.

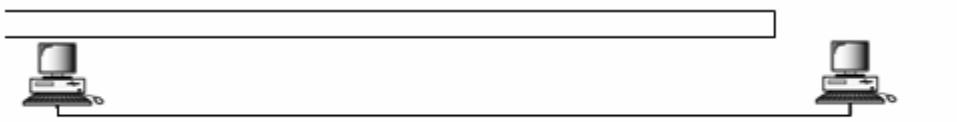
$T_{Transmission} = R/L$: R نرخ داده و یا پهنای باند است و L طول فریم است.



Collision detection can take as long as 2τ.

اگر a بسیار بزرگ باشد به خاطر مسأله حداقل طول فریم ، ممکن است در شبکه اشکال رخ دهد .

در شکل فوق ممکن است اشکال رخ دهد زیرا اگر B به کانال گوش کند می بیند که خط اشغال نیـست (در B) بنابراین می تواند بسته بفرستد و در صورت ارسال بسته ممکن است با بسته ارسـالی از طـرف A برخـورد کنـد . ولی در شکل زیر مشکلی به وجود نمی آید .

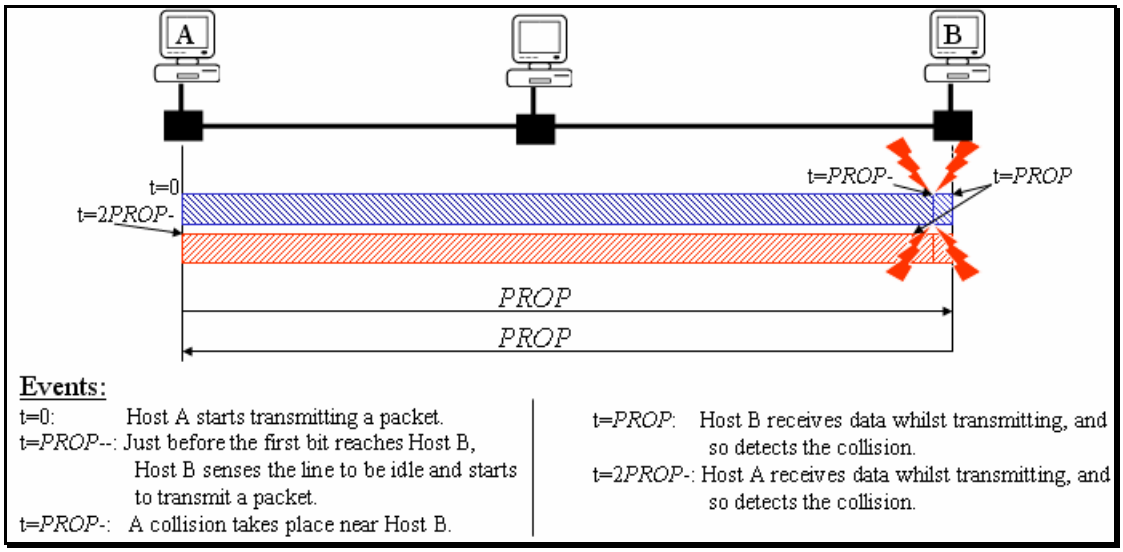


Terminator

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 TOKEN RING یک 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 .

UTILIZATION در شبکه های LAN بستگی به a(که قبلاً توضیح داده شد.) دارد:U=1/ (a +1) .هر چه aکمتر باشد Uبیشتر است ، و یا aبرای 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 مثال در تصویر بالا برای اینکه سیستم میزبان بتواند قبل از اتمام ارسال بسته، تصادم را تشخیص بدهد نیازمند آنیم 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 ۲×۱۰^{۸} تا $۲/۵\times۱۰^{۸}$ متر بر ثانیه درنظر گرفته می شود. به عنوان نمونه برای یک فاصله ۱۵۰۰ متری و سرعت شبکه ۱۰ مگا بیت بر ثانیه ای ، حداقل طول بسته بصورت زیر محاسبه می شود:

$PROP_{max}=d/c=1500/2.5*10^{8}=6\mu s$

TRANSP > 2PROP = 12μs

Packet Size ≥ (12μs) * 10Mb/s =120 bits

زمان ارسال داده ها نیز بصورت زیر محاسبه می شود:

Transmission Time =TRANSP + wasted time between packets

اگر P را احتمال تصمیم گیری یک نود برای انتقال بسته یا عدم ارسال بسته در یک بازه زمانی فرض کنیم، بهترین توان کاری (a(p)) برای شبکه بصورت زیر محاسبه می گردد:

$$\alpha(p) = \binom{N}{1} p(1-p)^{N-1}$$

$$\frac{d\alpha}{dp} = N(1-p)^{N-1} - pN(N-1)(1-p)^{N-2}$$

$a_{max} \approx 36\% \approx 40\%$ When $p=1/N$

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

Transmission Time = TRANSP + 1.5 (2 * PROP)

Transmission Time ≈ PROP=d /c (1)

از سوی دیگر زمان انتقال را می توان بصورت نسبت پهنای باند شبکه بـه طـول بـسته هـای ارسـالی نیـز تعریف نمود:

Transmission Time = Network Bandwidth / Frame Length (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 پهنای 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 :

- Connection-Less : Datagram و سر بار کم . در کاربردهایی که سرعت بـالا مـورد نظـر اسـت استفاده دارد . مانند UDP و چند رسانه ای .
- Connection -Oriented (سه فاز دارد) :
  ۱. ایجاد اتصال
  ۲. انتقال داده ها
  ۳. اتمام اتصال

  که در انتقال Reliable داده مورد نیاز است .مانند TCP ، E-mailو FTP .

۲-کیفیت سرویس (QoS):QoS هم در Connection-Less است و هم در Connection –Oriented.

- خطا و میزان از دست دادن آن (در Connection -Less)
- تأخیر ماکزیمم و متوسط مطلوب
- گذردهی 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 (Resilence)

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

۴-Interface با کاربر :

-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 انتها 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 تایمرهای 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 (سایتهای تجاری بیشتر به این موضوع نیاز دارند).

مکانیزمهای پروتکل در مورد شبکه های مطمئن (lan 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) :

ID کاربر: پورت یا TSAP (Transport Service Accses Point)

ID حمل و نقل (TCP, UDP ,...)

آدرس ایستگاه (آدرس Host)

شماره شبکه (آدرس شبکه)

چگونه لایه حمل و نقل مبدأ آدرس لایه حمل ونقل مقصد را پیدا می کند ؟

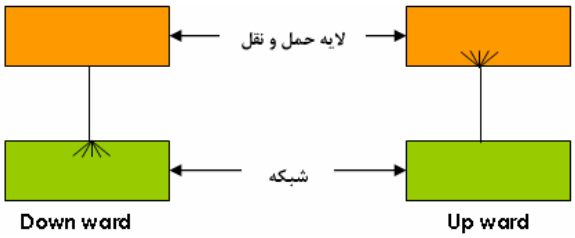
۱-لایه حمل ونقل قبل از ارسال آدرس مقصد را کاملاً داشته باشد .

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 سروررا داشته باشد .

مالتی پلکس :

به دو صورت upward و Downward می تواند وجود داشته باشد .

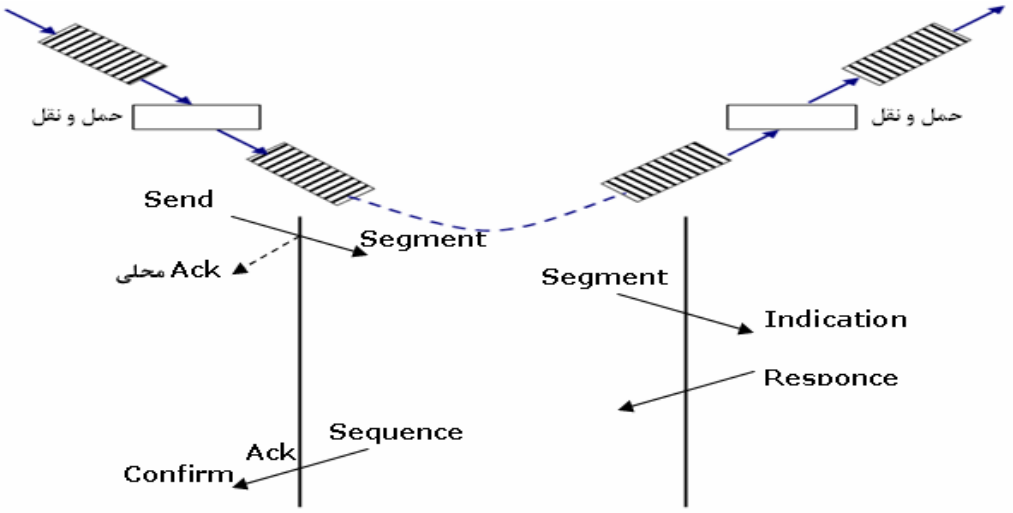


DownWard/UpWard Multiplexing

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 صف های زیادی در لایه حمل و نقل وجود دارد که در صورت تراکم باید با آنها برخورد مناسب صورت بگیرد .



Flow Control Plane

-حداقل ۴ صف وجود دارد .

چهار روش برای رفع نیاز کنترل Flow در لایه حمل و نقل می تواند وجود داشته باشد :

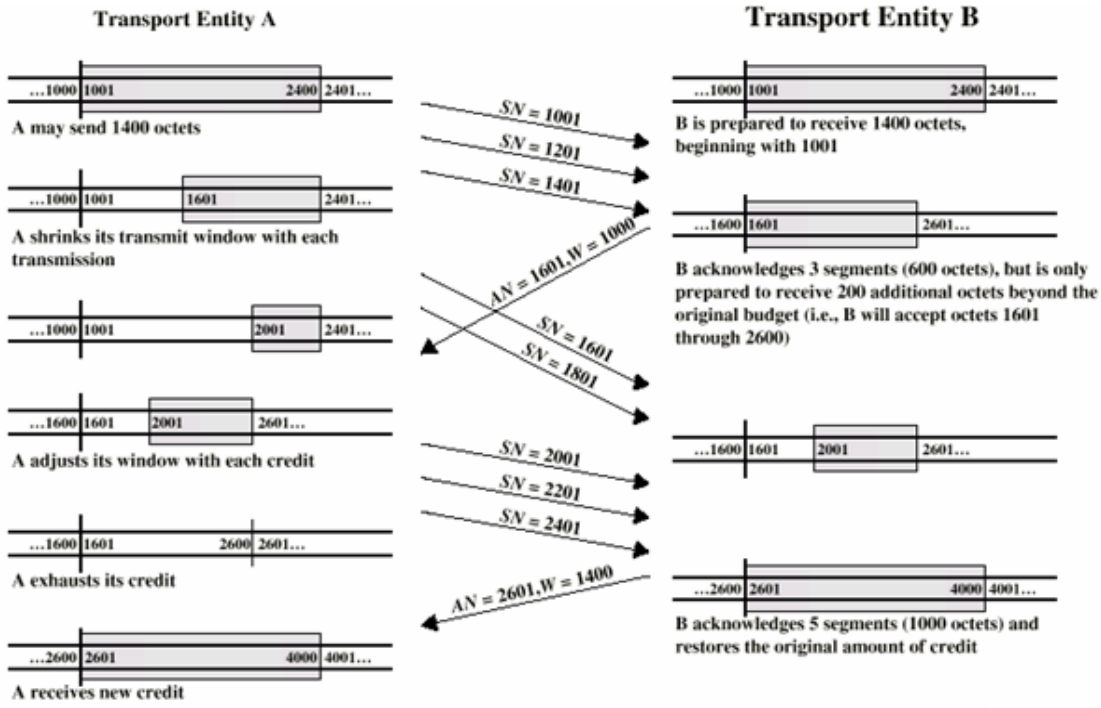
۱-کاری انجام نگیرد (قطعه های زیادی از بافرها دور ریخته می شوند و ارسال کننده چون ACK دریافت نمی کند دوباره بسته را می فرستد)(به جای قطعه های جدید ، قطعه های قدیمی ارسال می شوند) .

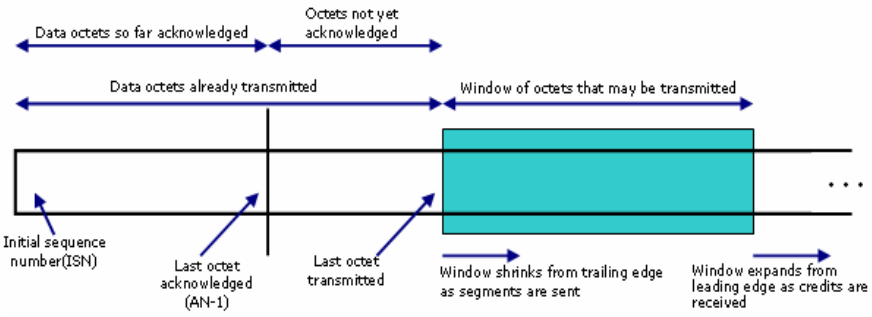
۲-جلوی دریافت قطعه های بعدی را بگیرد (وقتی بافر پر است دریافت قطعه های جدید صورت نمی گیرد).

۳-پروتکل ثابت پنجره های افزان (Sliding Window):

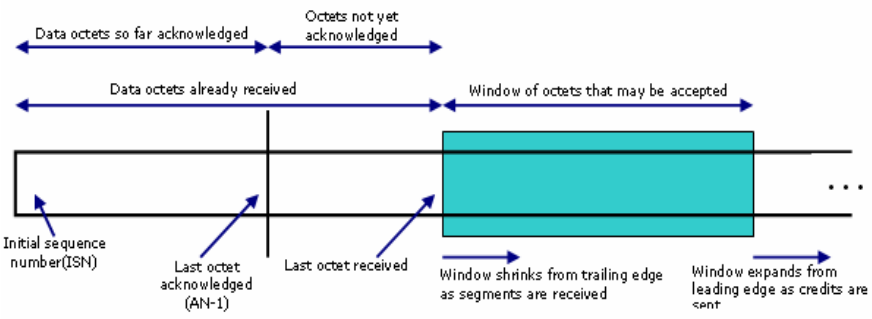
- استفاده از seqno
- استفاده از ACK برای جلو بردن پنجره
- استفاده از پنجره

۴-روش Credit :



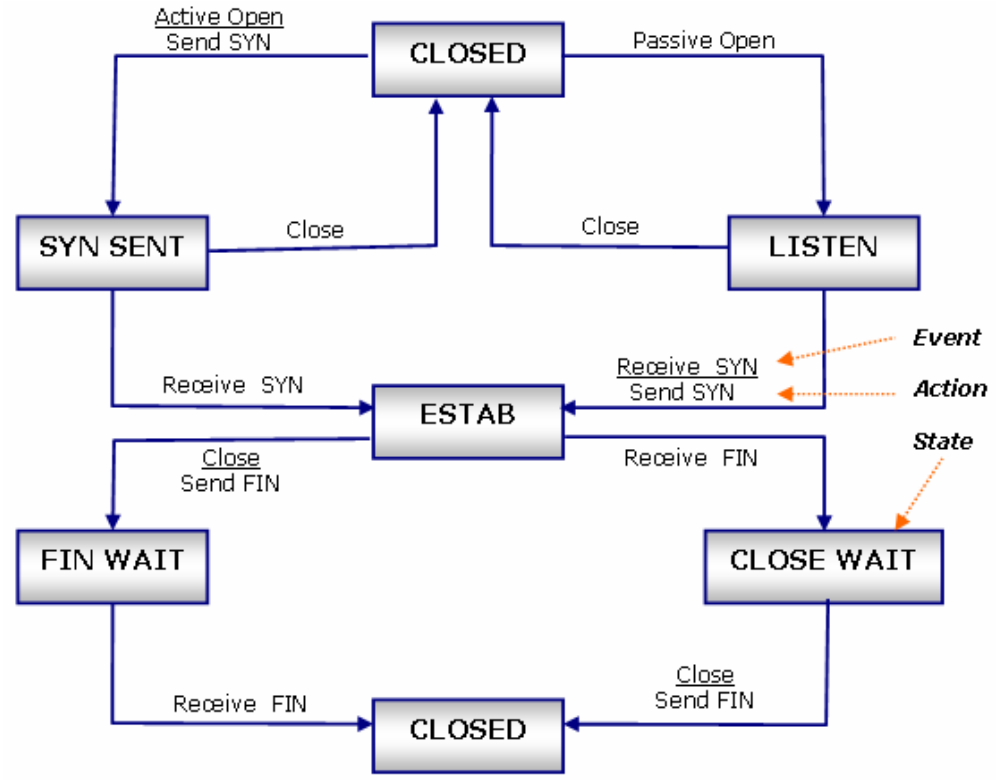


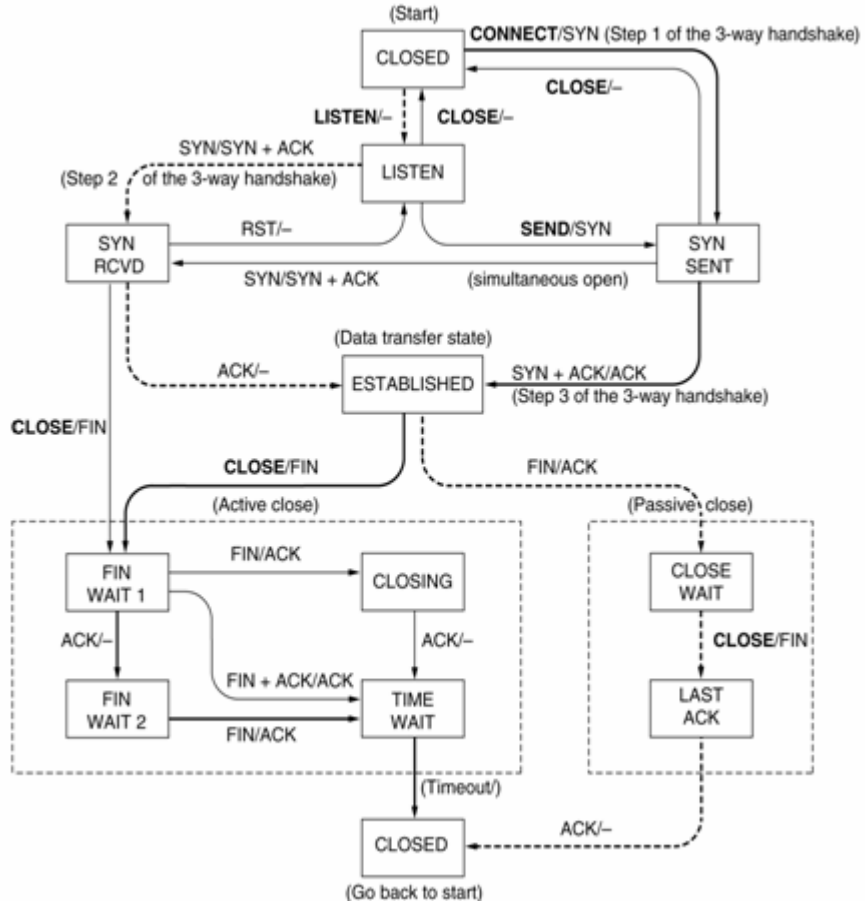
(a) Send sequence space



(b) Receive sequence space

-ایجاد واتمام 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....
- تریگر 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) . کاربرممکن 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 قطعهSYNC 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 تأئید 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 : Abroupt , graceful .

در شبکه Reliable به صورت graceful است :

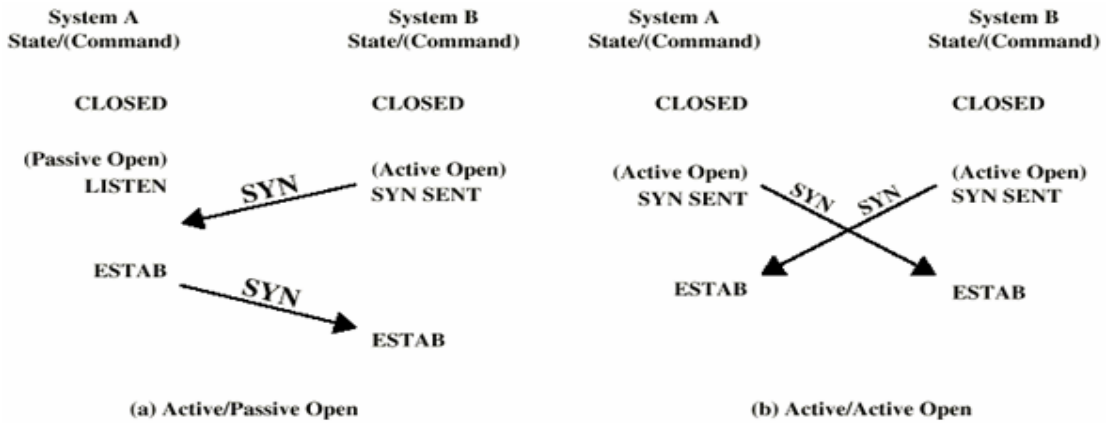
- طرف Client : در پاسخ به فرمان close کاربر یک قطعه بنام Fin به طرف دیگر ارسال می کند . بعد از ارسال Fin وضعیت به Finwait تغییر می کند (در این حالت لایه حمل و نقل کماکان دریافت داده ها را قبول می کند (graceful).

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 کابر 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 B,A در وضعیت CLOSE هستند .



ب – در ابتدا B,A در وضعیت Active باشند (هر دو به صورت همزمان می خواهند در ایجاد اتصال به صورت فعال شرکت کنند)

یعنی دراین حالت هردو به حالت syncsent می روند و حالت Listen وجود ندارد .

یه حمل و نقل برای لایه شبکه Unreliable , Connection-Less :

(مثلاً لایه شبکه ، IP باشد)در این حالت بسته ها به صورت نامرتب می رسند .

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 (ACK گروهی) .

تایمرهای مختلف(مدیریت تایمرهای مختلف بسیار پیچیده است) :

تایمر انتقال مجدد

تایمر اتصال مجدد

تایمر پنجره

تایمر انتقال مجدد Sync

تایمر غیر فعال کننده

تایمر حضور

زمان تایمرها یا به صورت ثابت است و یا به صورت پویا . در تایمر پویا ، تغییرات شبکه (مانند ترافیک و عوامل دیگر) باعث می شود که تنظیم آن صورت گیرد . تنظیم تایمر در لایه حمل ونقل 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 ACK 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 کپی مجدد وجود نداشته باشد) .

کنترل Flow : تقریباً مثل روش Connection-Oriented است (روش Credit)

CreditAckn : یعنی N فریم رسیده است و قطعه های N+1 تا N+M می تواند ارسال شود :

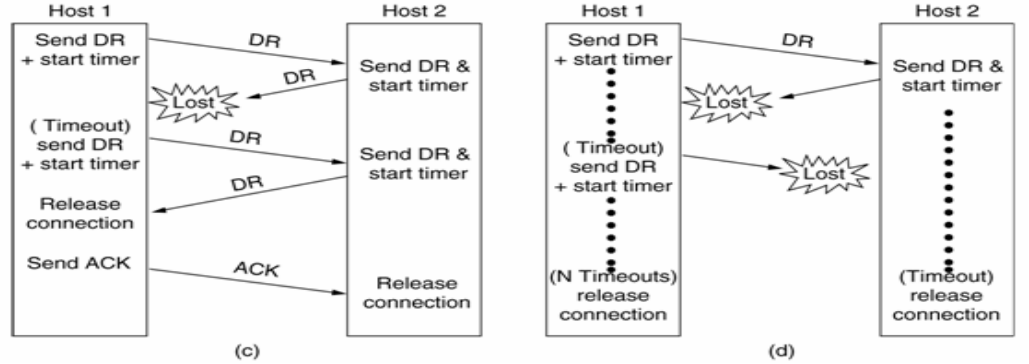
-ایجاداتصال

-قطع اتصال

-رفع خرابی

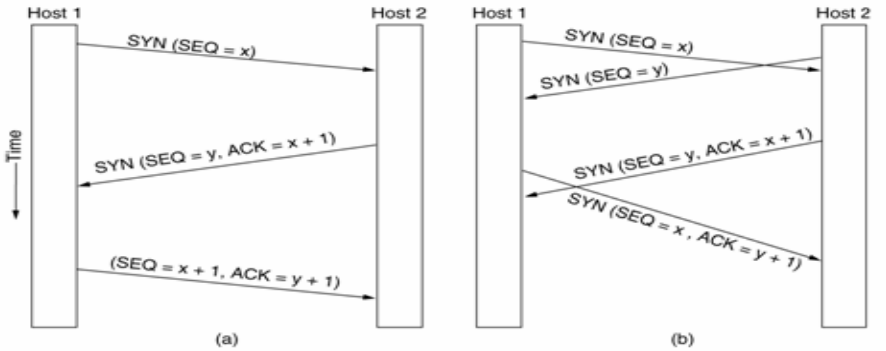
ایجاد اتصال در شبکه های نامطمئن :

با رد و بدل کردن فریمهای Syn اتصال برقرار می شود . A 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 دوطرفه ممکن است اشکالاتی بوجود آید . ممکن است Syn گم شود . یا Syn از یک اتصال قدیمی وارد سیستم شود و اتصال مخدوش شود .

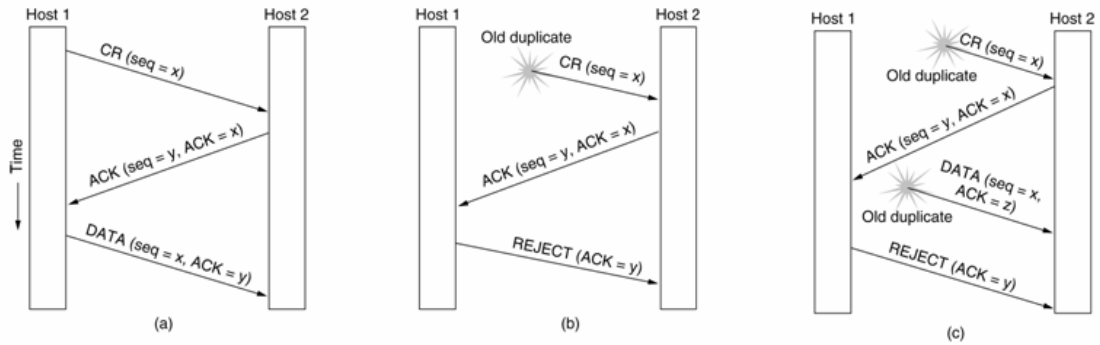


یک راه حل این است که درخواستها شماره گذاری شوند . Synj , Syni این هم اشکالاتی دارد که ممکن است Synk برسد و اتصال مخدوش شود .

قطع اتصال : (B,A همزمان درخواست اتصال می کنند) و سپس A با فرض اینکه اتصال برقرار است شروع به ارسال اطلاعات می کند Snr+1 که B آن را نمی پذیرد زیرا برای Syni B اتصال است و داده باید Sni+ 1 باشد .



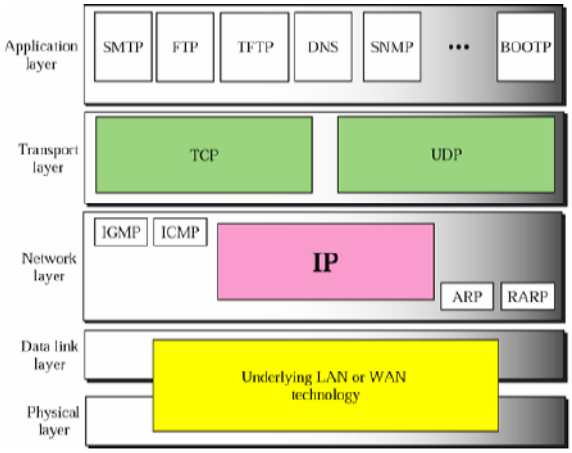
راه حل این است که که هر طرف شماره Syn و ترتیب داده ها (SN) از طرف قبل را مجزا جواب دهند که این روش بنام 3- Way hand shake می باشد حالتهای جدید در دیاگرام حالت پروتکل حمل و نقل ایجاد می شود و قطعه های کنترلی جدید مانند RST (Reset) افزوده می شود .



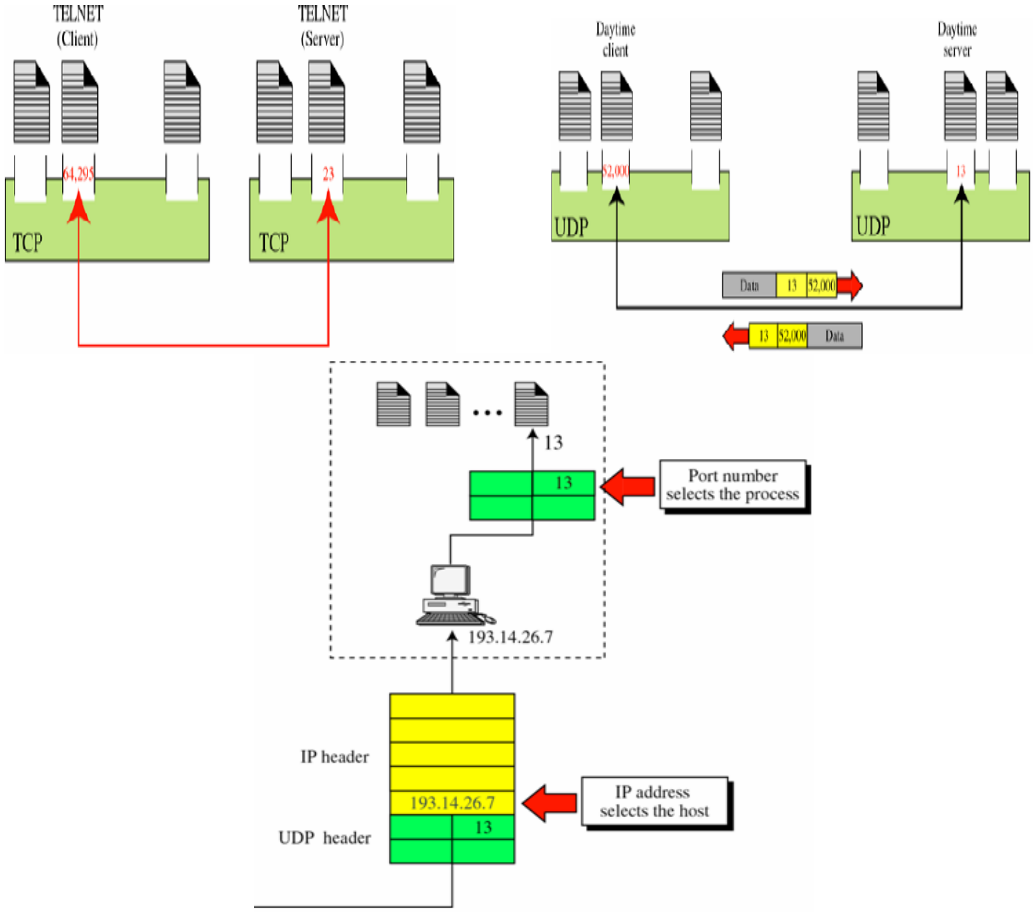
فصل ۱۲:

پروتکل های UDP و TCP

UDP وTCP در لایه حمل و نقل قرار دارد:



برخلاف IP که بصورت میزبان به میزبان می باشد، UDP و TCP بصورت پردازش به پـردازش مـی باشـد. در UDP و TCP از شماره پورت جهت مشخص کردن پردازش استفاده می کننـد. شـماره پـورت یـک مقـدار ۱۶ بیتـی می باشد و شماره پورت TCP و UDP از یکدیگر جدا هستند.

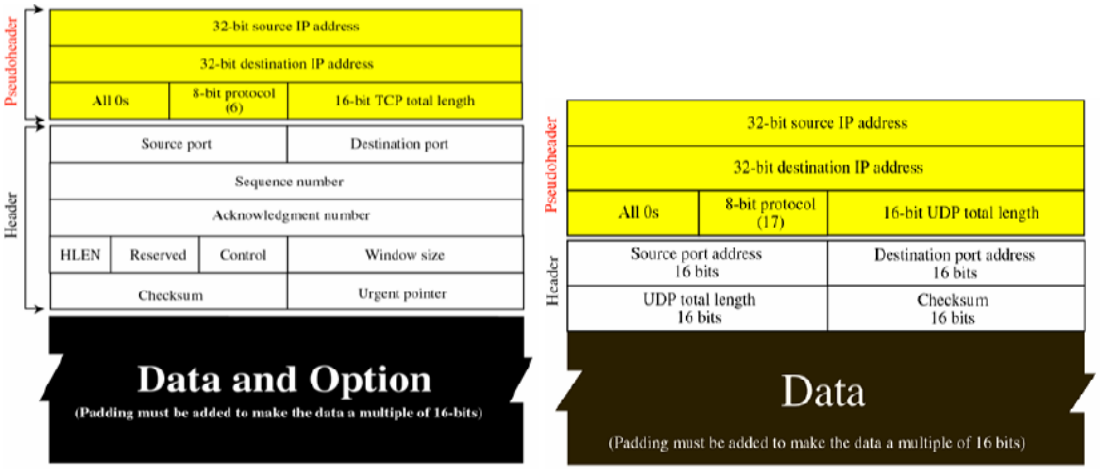


شماره پورتها در دامنه IANA بصورت زیر می باشد:

۱. شماره پورتهای مشهور (۰-۱۰۲۳)
۲. شماره پورتهای ثبت شده (۱۰۲۴-۴۹۱۵۱)
۳. شماره پورتهای پویا (۴۹۱۵۲-۶۵۵۳۵)

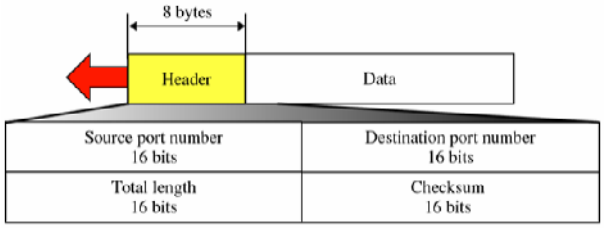
آدرس سوکت عبارت است از آدرس IP و آدرس پورت.

در بسته های UDP و TCP از شبه سرآیند(Pseudoheader) جهت کمک به CheckSum استفاده می شود. این شبه سرآیندها اطلاعاتی همچون آدرس IP مبداء و مقصد، شماره پروتکل و طول بسته UDP ویا TCP قرار گرفته است. همچنین اگر طول قسمت داده این بسته ها کمتر از حد مجاز باشد(مضربی از ۱۶ نباشد)، با استفاده از Padding طول آن تا حد مجاز افزایش می یابد.

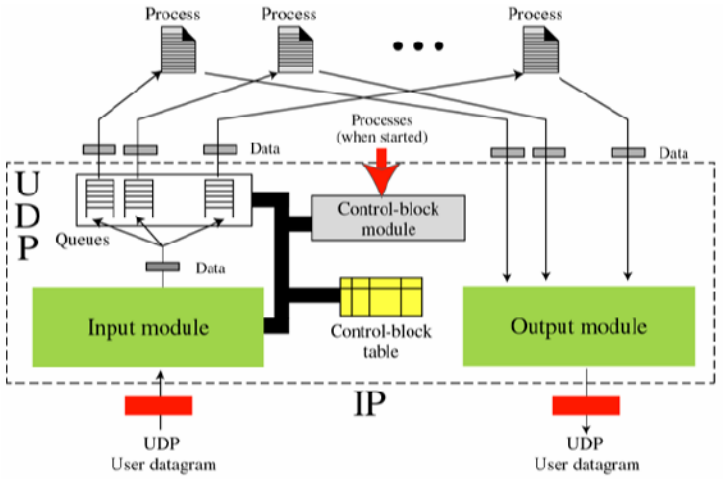


UDP[1]:

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:

[1] User Datagram Protocol -

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. ماژول ورودی جدول کنترل بلاک را برای این شماره پورت جستجو کرده و آن را پیدا می کند. صف شماره ۳۸ به این پورت اختصاص یافته است که این به معنی آن است که این پورت قبلاً مورد استفاده قرار گرفته است. ماژول ورودی داده را به صف 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 ماژول کنترل بلاک ارسال می کند و این ماژول نیز یک مدخل را در جدول ایجاد می نماید. ماژول صفی را در این لحظه به مدخل تخصیص نمی دهد، زیرا هیچ Datagram یی 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. ماژول ورودی جدول را چک کرده متوجه می شود که هیچ صفی برای این مقصد تخصیص داده نشده است، زیرا این اولین بسته Datagram کاربر می باشد که برای این مقصد دریافت می گردد. ماژول یک صف 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. ماژول ورودی جدول را چک کرده و مدخلی را برای این مقصد پیدا نمی کند. Datagram دور ریخته می شود و یک درخواست به ICMP برای ارسال یک پیام "در دسترس نبودن پورت" به مبداء ، ایجاد می شود.

پس از چند ثانیه یک پردازش می خواهد یک Datagram ارسال نماید. پردازش داده ها را به ماژول خروجی تحویل داده و این ماژول پس از افزودن سرآیند UDP، آن را ارسال می کند.

TCP[1]:

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 سگمنتهایی قرار گرفته و سپس ارسال می گردد. بایتهای داده ارسالی در هر اتصال بوسیله TCP شمرده می شود. شمارش با یک عدد تصادفی آغاز می شود.

[1] - Transmission Control Protocol

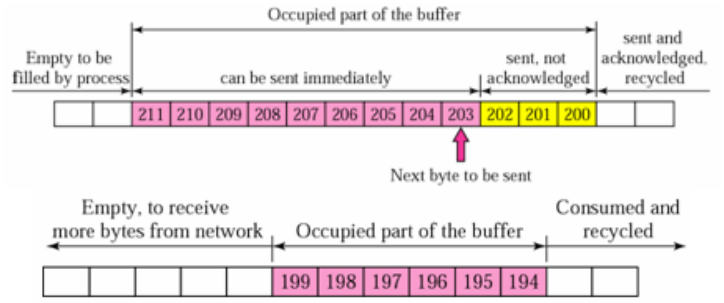
مثال: یک اتصال TCP قصد ارسال یک فایل ۶۰۰۰ بایتی را دارد. اولین بایت با 10010 شماره گـذاری شـده است. شماره توالی هر سگمنت با فرض ارسال ۴ سـگمنت ۱۰۰۰ بـایتی و یـک سـگمنت ۲۰۰۰ بـایتی در پایـان، را مشخص کنید.

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)

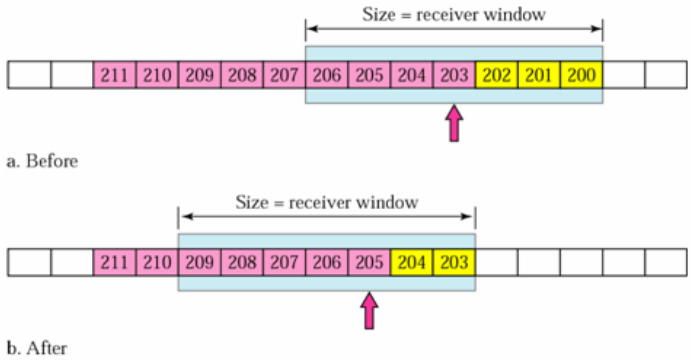
مقدار شماره توالی در هر سگمنت، شماره بایت اول داده موجود در هر سگمنت را مشخص می کنـد. مقـدار فیلد Acknowledgment در یک سگمنت، شماره بایت بعدی یک دسته را که انتظار دریافت آن می رود را مشخص می نماید. شماره Acknowledgment بصورت تجمعی می باشد.

پنجره لغزان:

پنجره لغزان(Sliding Window) برای کارایی بیشتر ارسال و کنترل جریان داده بکار مـی رود تـا مقـصد در داده ها غوطه ور نمی شود. پنجره لغزان TCP بایت گرا است. طرح بافر فرستنده و پنجره دریافت کننـده در تـصاویر زیر آمده است:

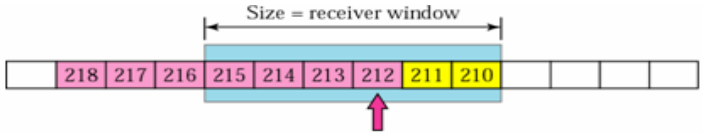


اندازه پنجره لغزان بوسیله پنجره دریافت کننده معین می گردد. اگرچه اندازه واقعی پنجره می توانـد بـدلیل تراکم در شبکه کوچکتر شود.



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 داده های ممکن در اندازه کامل پنجره را ارسال کند.

۲. اندازه پنجره 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 Time out) Ackیی دریافت ننماید، فرستنده مجدداً داده های ارسالی پس از آخرین Ack دریافتی را ارسال می نماید. همچنین از آنجاییکه گیرنده در ارسال Ack محدودیتی ندارد، اگر یک Ack 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.

تایمرهای TCP عبارتند از:

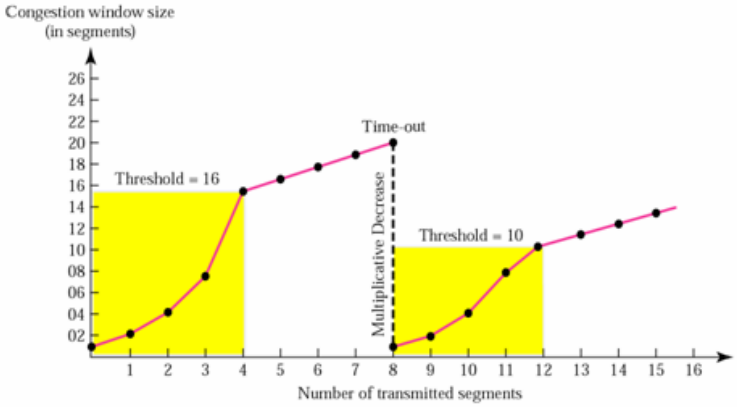
۱. Retransmission: پس از برقراری یک ارتباط، وقتی فرستنده بسته ای برای پردازش به مقصد ارسال میکند، ضمن نگهداری موقت آن در یک بافر، برای آن یک زمان سنج را تنظیم و فعال می نماید و اگر در مهلت مقرر،پیام تایید آن دریافت نشد، آن بسته دوباره ارسال می گردد. این زمان سنج در ابتدا به یک مقدار پیش فرض تنظیم می 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 شبکه های محلی سریع، بسیار کوتاه و در حد هزارم ثانیه می باشد و برای شبکه های WAN طولانی و در حد چند ثانیه می باشد. بنابراین اگر زمان سنج مقدار پیش فرض کوتاهی داشته باشد، برای انتقالات فواصل دور، قبل از آنکه بسته به مقصد برسد و تایید ارسال شده آن به مبداء 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 شبکه های محلی و سریع، هنگام بروز یک خطا، تاخیر زیادی بوجود آید. بهترین راه حل، تنظیم زمان سنج بصورت پویا، با استفاده از روشهای تطبیقی و پویا، می باشد؛ چرا که بازده TCP بشدت به آن وابسته است.

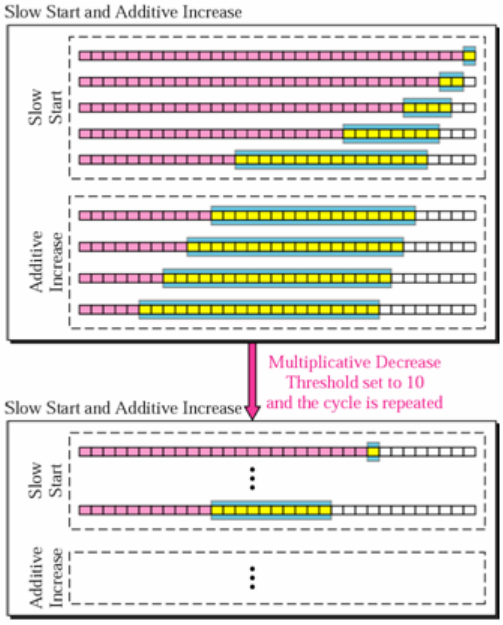
۲. Persistence: در پروتکل TCP وقتیکه یکی از طرفین ارتباط، مقدار بافر آزاد خود را در فیلد اندازه پنجره صفر اعلام کند، ناگزیر است تا پردازش طرف مقابل را مسدود نماید. در چنین حالتی پس از آنکه مقداری از فضای بافر پرشده، تخلیه گردید، این موضوع به طرف مقابل اعلام می گردد تا سیستم عامل ، پردازش مسدود شده را 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 پروسه 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 داده ای 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 بازه های 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.

۴. Time-Waited: 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 ، برحسب ثانیه، بین ۳۰ تا ۱۲۰ ثانیه، می باشد. به این زمان سنج، زمان سنج Quiet نیز گفته می شود.

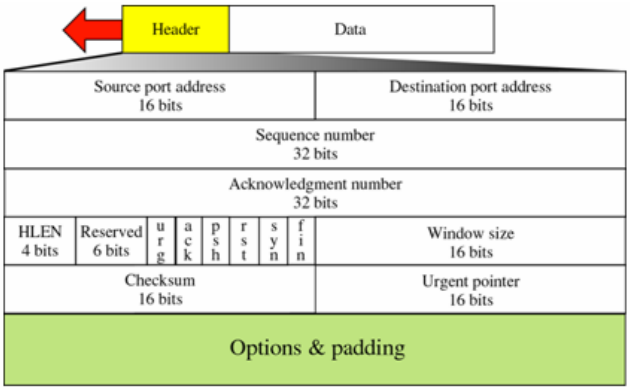
TCP دلیل گم شدن بسته ها را تراکم در شبکه می داند و حال آنکه در صورت صحیح بودن این فرض ارسال دوباره سگمنت گم شده، نه تنها عامل تراکم را حذف نمی کند، بلکه آن را تشدید می نماید. در تصویر زیر مکانیزم تعیین اندازه پنجره تراکم در TCP امده است. این مکانیزم جهت کنترل تراکم در TCP بکار می رود.



ابتدا TCP اقدام به ارسال بسته می نماید تا آنجا که بر اثر تراکم Ackیی 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 ساختارسگمنت TCP در ادامه آمده است.



فیلدهای کنترلی در سگمنت TCP عبارتند از:

- URG: اشاره گر فوری معتبر است. درصورتیکه این بیت مقدار ۱ داشته باشد معین می کند که در فیلد اشاره گر فوری مقداری قابل استناد و معتبر قرار دارد و بایستی مورد پردازش قرار گیرد. درصورتیکه 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 تحویل 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 درحقیقت 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.

Optionها در TCP:

- تک بیتی

۱. No Operation
   - No Operation
   - تنظیم ابتدای یک Option
   - تنظیم Option بعدی

۲. End of Option
   - پایان option ها

- استفاده در Padding

- چند بیتی

۱. ماکزیمم اندازه سگمنت

۲. ضریب مقیاس پنجره

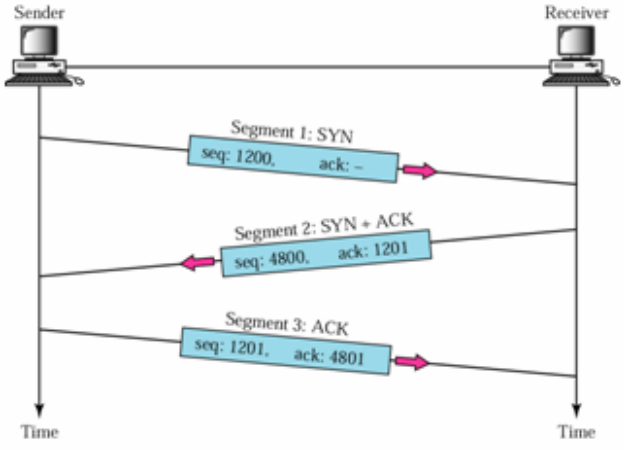
۳. Time Stamp

TCP برای آغاز یک اتصال از "دست دهی" سه طرفه استفاده می کند. روند این عمل بصورت زیر می باشد:

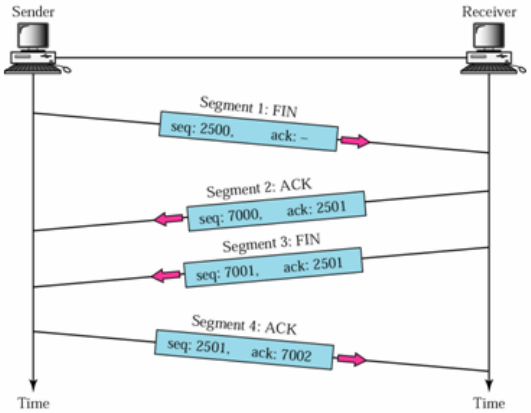
۱. شروع کننده ارتباط، یک بسته TCP بدون داده و با تنظیمات بیتهای SYN=1، ACK=0، برای طرف مقابل ارسال می کند. در حقیقت ارسال چنین بسته ای به معنی تقاضا برای برقراری ارتباط می باشد.

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 متذکر می شود.

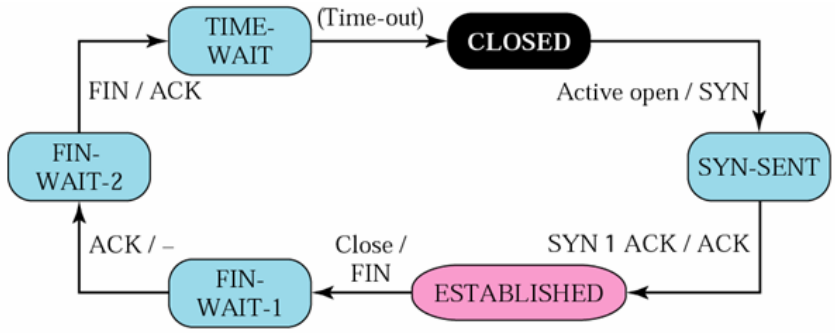
۳. فرستنده اقدام به ارسال اطلاعات می نماید(بیت SYN=1 و بیت ACK=1).

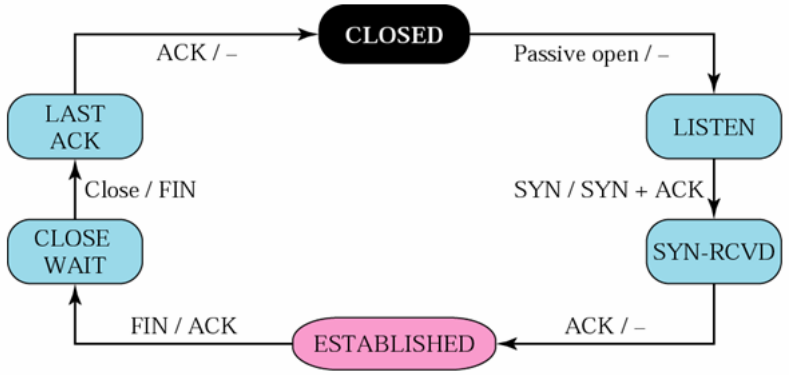


و برای خاتمه اتصال از دست دهی چهار طرفه استفاده می کند.

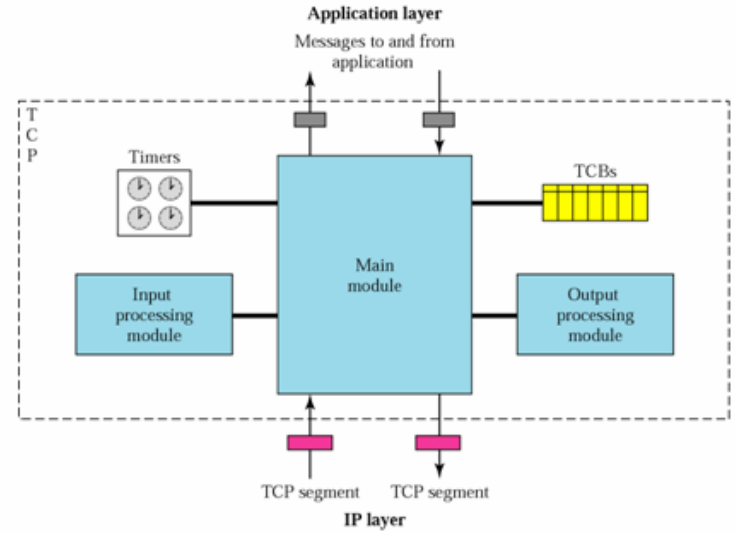


براین اساس نمودارهای گذر حالت زیر را می توان برای فرستنده و گیرنده ارائه داد:

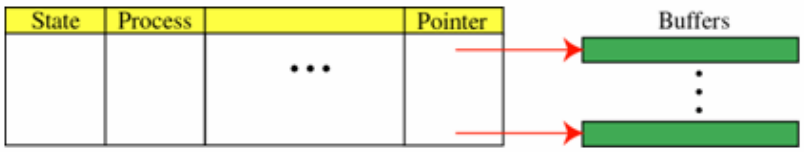




در فصل بعد در مورد این نمودارها بیشتر توضیح داده می شود. ساختار داخلی TCP بصورت زیر می باشد:



ساختار TCB[1] بصورت زیر می باشد:



[1] - Transmission Control Block

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.

Internet Architecture Borard (IAB)، RFC 1052 را ارائه داد که در بردارنده ۲ شیوه می باشد:

- ☑ پروتکل ساده مدیریت شبکه (SNMP[1])
- ☑ پروتکل سرویس اطلاعات متعارف/ اطلاعات مدیریت متعارف (CMIS/CMIP[2]) ISO.

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.

۱۳-۱: پروتکل ساده مدیریت شبکه و مروری بر MIB[3]

چهارچوب مدیریت شبکه SNMP عبارتست از:

- ☑ تعداد زیادی گره های مدیریت شده، که هر کدام یک موجودیت (یا SNMP Agent) دارند. یک SNMP Agent سروریست 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. SNMP Agent 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 برروی یک ایستگاه مدیریتی اجرا شده و درخواست اطلاعات مدیریتی را از یک SNMP Agent، 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 [4] (RFC 1028) و MIB-I (RFC 1156)، جهت استفاده توصیه نشده اند. SNMP 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 دارد اطلاعات آن را می توان در RFC 1213 مدیریت شبکه های مبتنی بر TCP/IPبرپایه مدیریت اطلاعات پایه:MIB-II پیدا نمود. اطلاعات بیشتر را می توان در RFC 1155 (SMI)، RFC 1213 (MIB-II)و RFC 1157 (SNMP) یافت.

۱۳-۲: ساختار و هویت اطلاعات مدیریت(SMI[5])

---

[1] - Simple Network Management Protocol

[2] - Common Management Information Services/Common Management Information Protocol

[3] - Management Information Base

[4] - Simple Gateway Monitoring Protocol

[5] - Structure and identification of management information

SMI قوانین نحوه توصیف اشیاء مدیریتی و نحوه دستیابی پروتکلهای مدیریتی به این اشیاء را ارائه می دهد. مفهوم اشیاء مدیریت شده در یک زیر مجموعه از ASN.1[1] ارائه شده است نوع شئی تعریفی از ۵ فیلد تشکیل شده است:

- ☑ **شئی:** یک نام متنی که توصیفگر شئی نامیده می شود، به همراه یک نوع شئی همراه با شناسه شئی.
- ☑ **Syntax**: دستورالعمل خلاصه برای نوع شئی. می تواند از نوع SimpleSyntax انتخاب شود (Integer, Octet String, Object Identifier, Null) یا ApplicationSyntax (Network Address, Counter, Gauge, Timeticks, Opaque) و یا انواع گسترده دیگر کاربرد باشد (به RFC 1155).
- ☑ **تعریف:** توصیف متنی از معنی شناسی نوع شئی.
- ☑ **دسترسی:** یکی از Read-only، Read-Write، Write-only و یا Not-Accessible.
- ☑ **وضعیت:** یکی از Mandatory، Optional و یا Obsolete.

به عنوان یک نمونه وضعیت زیر را ببینند:

```
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 می دهد. نام آن sysDescr است و به گروه system تعلق دارد (۱۳-۳ را ببینید).

یک شئی مدیریت شده علاوه بر توصیف شامل شناسه نیز می باشد. این امر با کمک شناسه شئی ASN.1 ، همانند یک شماره تلفن، انجام می گیرد و شماره گروه ها برای مناطق مختلف رزرو می گردد. در مدیریت شبکه های مبتنی بر TCP/IP شماره های تخصیصی 1.3.6.1.2 بوده و SMI از این به عنوان پایه ای برای تعریف اشیاء جدید استفاده می نماید.

شماره 1.3.6.1.2 بوسیله ادغام گروه هایی با شماره های با معانی زیر بکار می رود:

- ☑ اولین گروه، معرف گره Administartor می باشد:
  - (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 می نماید، بنابراین انجمن اینترنت مقدار (۱) را برای آن فرض نموده است.

[1] - Abstract Syntax Notation 1, ISO standard 8824

☑ 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 1}" 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.

۱۳-۳: MIB

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:

گروه	اشیاء برای	#
System	اطلاعات پایه سیستم	۷
Interfaces	الحاقات شبکه	۲۳
AT	ترجمه آدرس	۳
IP	پروتکل اینترنت	۴۲
ICMP	پروتکل پیام کنترل اینترنت	۲۶
TCP	پروتکل کنترل انتقال	۱۹
UDP	پروتکل داده گرام کاربر	۷
EGP	پروتکل دروازه خروجی	۱۸
SNMP	موجودیتهای کاربردهای SNMP	۳۹
# = تعداد اشیاء در گروه		

جدول ۱۳-۱: 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 مکانیزمهای توسعه پذیریی 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، RFC 2012 و 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 مقداردهی اولیه مجدد
- sysContact : نام شخص تماس گیرنده
- sysServices : سرویس ارائه شده توسط سیستم

☑ گروه واسط

- ifIndex : شماره واسط
- ifDescr : توصیف واسط
- ifType : نوع واسط
- ifMtu : اندازه بزرگترین داده گرام IP
- ifAdminisStatus : 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

- atTable : deprecated (MIB-I)
- atEntry : deprecated (MIB-I)
- atIfIndex : شماره واسط ifIndex
- atPhysAddress : آدرس فیزیکی وابسته به محیط انتقال
- atNetAddress : آدرس شبکه منطبق با آدرس فیزیکی وابسته به محیط انتقال
- media

☑ گروه IP

- 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

☑ گروه ICMP

- icmpInMsgs : تعداد پیام ICMP دریافتی
- icmpInDestUnreachs : تعداد پیام ICMP عدم در دسترس بودن مقصد دریافتی
- icmpInTimeExcds : تعداد پیام ICMP تخطی از بازه زمانی دریافتی
- icmpInSrcQuenchs : تعداد پیام ICMP خاموش بودن منبع دریافتی
- icmpOutErrors : تعداد پیام ICMP ارسال نشده بدلیل مشکلات در ICMP

☑ گروه TCP

- tcpRtoAlgorithm : الگوریتم تعیین انقضاء بازه زمانی برای ارسال دوباره هشت تاییهای بدون تایید
- tcpMaxConn : محدودیت تعداد اتصالات TCP مورد حمایت موجودیت

- tcpActiveOpens : تعداد دفعات رفتن مستقیم اتصالات TCP از حالت CLOSED به 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

☑ گروه UDP

- udpInDatagrams : تعداد داده گرام UDP تحویل 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 تحویل به دلایلی بجز عدم وجود کاربرد در پورت مقصد
- udpOutDatagrams : تعداد داده گرام UDP ارسالی برای این موجودیت

☑ گروه EGP

- 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 EGP
- 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 ماژولها 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 درختMIB با استفاده از نماد ASN.1 بوسیله 1.3.6.1.2.1.2.2.1.3 تعریف 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-specific در IMB

IMB اشیاء زیر را به پایگاه داده MIB-II افزوده است:

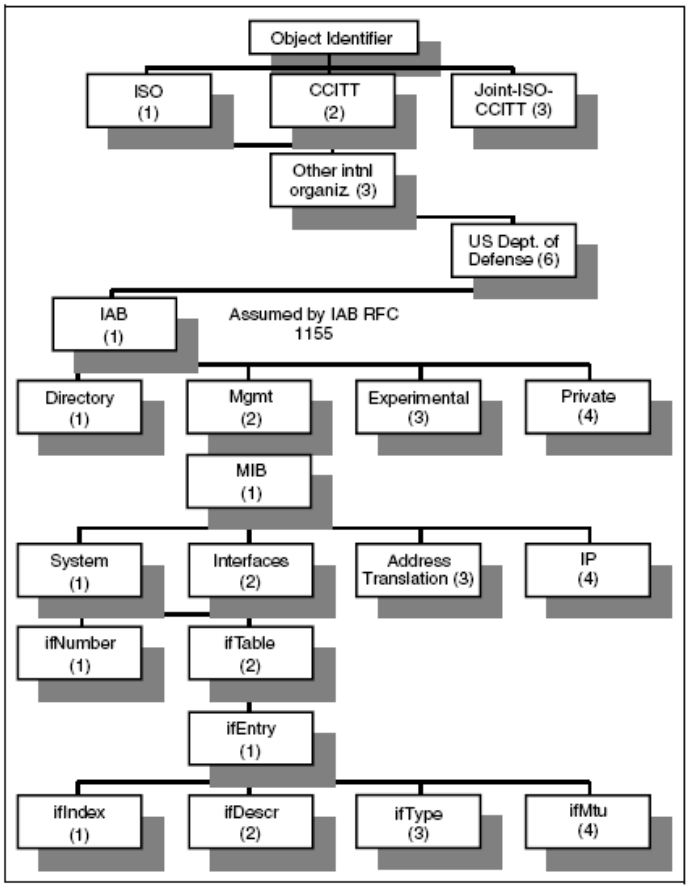
```
* IBM SNMP agent DPI UDP port
DPI_port 1.3.6.1.4.1.2.2.1.1. number 2

* 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 Agent و subAgent را بر می گرداند.

☑ *RTT* اجازه 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 ۱۳-۱: MIB-II- شناسه شئی تخصیصی برای شبکه مبتنی بر TCP/IP

SNMP :۴-۱۳

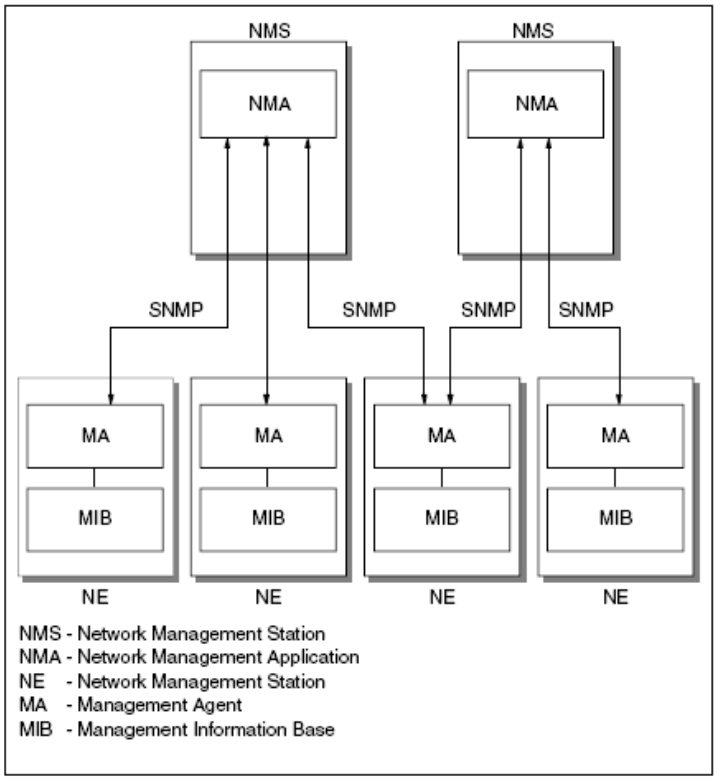
Snmp حاصل بهبودهای سالها تجربه SGMP را در بردارد و مجاز است تا با اشیاء تعریف شده در MIB با توصیفات ارائه شده در SIM کار کند.

RFC 1157 ایستگاه مدیریت شبکه (NMS[1]) را به عنوان یک مجری کاربردهای مدیریت شبکه(NMA[2]) که عناصر شبکه (NE[3]) همانند میزبانها، دروازه ها و پایانه های سرور را تحت نظارت و کنترل دارد. این عناصر شبکه از یک Agent مدیریتی(MA[4]) جهت اجرای توابع مدیریت شبکه مورد درخواست بوسیله ایستگاه های مدیریت شبکه،

---

[1] Network Management Station -
[2] Network Management Applications -
[3] Network Elements -
[4] Management Agent -

استفاده می نمایند. SNMP جهت تبادل اطلاعات مدیریت شبکه بین ایستگاه های مـدیریت شـبکه و Agent هـا در عناصر شبکه بکار می رود.



شکل ۱۳-۲: اجزاء SNMP

توابع مدیریت Agent شامل دو دسته متغیرهای تغییر دهنده (set) و یا بررسی کننده (get) می باشـند کـه توابع اصلی مدیریت را ب دو دسته محدود می سازند و از پروتکلهای پیچیده بیشتر جلـوگیری مـی کننـد. از سـوی دیگر، از NE به NMS، از تعداد محدودی پیام های ناخواسته(یا Trap)، جهت تعیین رویـدادهای ناهمزمـان اسـتفاده می شود. به همین شکل در جهت حفظ سادگی، تبادل اطلاعات تنها نیازمند یک سرویس داده گـرام نـامطمئن مـی باشد و هر پیام بصورت کاملاً مجزا توسط یک داده گرام انتقالی، ارائه می گردد. همچنین این شیوه به معنی مناسـب بودن SNMP برای استفاده با دامنه وسیعی از پروتکلهای انتقالی مـی باشـد. RFC 1157، تبـادل اطلاعـات از طریـق 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 ارتبـاط دارنـد را موجودیتهای کاربرد SNMP[1] می نامند. زوج پردازشهای ایجاد کننـده آن، موجودیتهـای پروتکـل[2] مـی باشـند. یـک SNMP Agent با مجموعه دلخواهی از موجودیتهای کاربرد SNMP یک انجمن SNMP[3] نامیده مـی شـود کـه هـر کدامشان برای مشخص بودن در زمان حضور در انجمن، بوسیله یک رشته ۸ تایی مشخص می گردند.

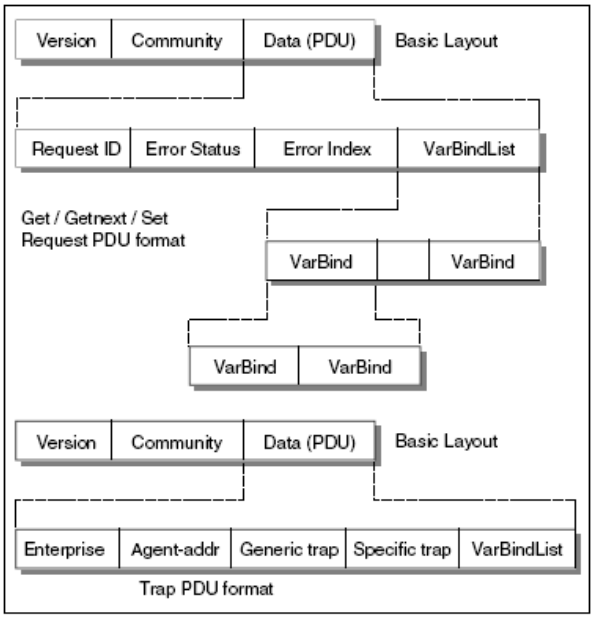
یک پیام در پروتکل SNMP شامل شناسه نسخه، نام انجمن SNMP و یک PDU می باشد. لازم است تا تمـام پیاده سازیهای SNMP از ۵ نوع PDU حمایت نمایند:

- ☑ **GetRequest** : بازگرداننده مقادیر یک شئی مشخص از MIB
- ☑ **GetNextRequest** : حرکت در میان بخشی از MIB
- ☑ **SetRequest** : تغییر مقادیر یک شئی خاص از MIB

[1] - SNMP application entities
[2] - protocol entities
[3] - SNMP community

- ☑ **GetResponse** : پاسخ یک GetRequest، یک GetNextRequest و یک SetRequest
- ☑ **Trap** : توانایی اجزاء شبکه برای ایجاد رویدادهایی برای ایستگاه های مدیریت شبکه، همانند مقداردهی اولیه Agent، Agent restart و خطای پیوند. ۷ نوع Trap در RFC 1157 معرفی گردیده است: coldStart، warmStart، linkDown، linkUp، authenticationFailure، egpNeighborLoss و enterpriseSpecific.

فرمت این پیامها به شکل زیر می باشد:



شکل ۱۳-۳: فرمت پیام SNMP- Request، set و trap PDU

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[1]، 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[2])، 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[3]) 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.

۱۳-۵: SNMPv2

[1] - community-based security model
[2] - user-based security model
[3] - view-based access control model

ساختار SNMPv2 در آوریل ۱۹۹۳ ارائه گردید و مشتمل بر RFC۱۲ می باشد کـه اولـین آنهـا RFC 1441 می باشد که یک مقدمه است. در آگوست ۱۹۹۳، همه ۱۲ RFC در قالب یک استاندارد با وضعیتهای انتخـابی، ارائـه گردید.

این ساختار دارای سیاستهای زیر می باشد:

- ☑ **ساختار اطلاعات مدیریتی (SMI[1])**: تعاریف زیر مجموعه OSI ASN.1 بـرای ایجـاد ماژولهـای MIB(به RFC 2578 مراجعه شود).
- ☑ **قراردادهای متنی[2]** : تعاریف مجموعه اولیه قراردادهای متنی موجود در همـه ماژولهـای MIB (بـه RFC 2579 مراجعه شود).
- ☑ **اعمال پروتکل:** تعاریف عملکرد پروتکل با توجـه بـه ارسـال و دریافـت PDUهـا (بـه RFC 1905 مراجعه شود).
- ☑ **نگاشت انتقال:** تعاریف نگاشت SNMPv2 به یک مجموعـه اولیـه از دامنـه هـای انتقـال، بـدلیل استفاده از آن در شرایط مختلف. نگاشت به UDP ارجح ترین نگاشـت مـی باشـد. همچنـین RFC، OSI، DDP، IPX و ... را نیز تعریف نموده است (به RFC 1906 مراجعه گردد).
- ☑ **تجهیزات پروتکل:** تعاریف MIB برای SNMPv2 (به1907 RFC مراجعه شود).
- ☑ **ساختار مدیریتی:**تعاریف ساختار مدیریتی SNMPv2، مدل مبتنـی بـر کـاربر بـرای SNMPv2 و مدل مبتنی بر انجمن SNMPv2 (به RFC های ۱۹۰۹، ۱۹۱۰ و ۱۹۰۱ مراجعه شود).
- ☑ **توضیحات تطبیق :** تعاریف توانایی های Agent ها(به RFC 2578 مراجعه شود).

موجودیت SNMPv2

یک موجودیت SNMPv2 یک پردازش واقعیست که اعمال مدیریت شبکه را تولید و/یا پاسـخ بـه پیـام هـای پروتکل SNMPv2 با استفاده از عملیاتهای پروتکل SNMPv2، انجام می دهـد. همـه اعمـال ممکـن یـک موجودیـت می تواند توسط یک زیر مجموعه از اعمال ممکن متعلق به دسته تعریف شده مدیریتی خاص، محـدود گـردد(بخـش "دسته SNMPv2[3]" را ببینید). یک موجودیت SNMPv2 می تواند عضو چند دسته SNMPv2 باشد. پایگـاه داده هـای محلی زیر توسط یک موجودیت SNMPv2 نگهداری می شود:

- ☑ یک پایگاه داده برای تمام دسته های 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 مـدیریت شـده آشـنا بـرای آن موجودیـت SNMPv2 را در بردارد.
- ☑ و حداقل یک پایگاه داده دیگر کـه ارائـه دهنـده یـک سیاسـت کنتـرل دسترسیـست کـه حقـوق دسترسی متناسب با دسته های 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 محرمانگی و پارامترهای مرتبط، بگونه ای که تمام پیامهای پروتکل دریافتی دسته را در برابر افشا شدن، محافظت نماید.

GetBulkRequest

GetBulkRequest در RFC 1905 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. اهدف GetBulkRequest، جهت درخواست انتقال یک حجم بالقوه زیاد از اطلاعات، شامل ، اما نه محدود به ، بازیابی کارامد و سریع جداول بزرگ، می باشد. GetBulkRequest از GetNextRequest 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:

- ☑ **RequestedObjectName1,2,3:** 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 برده شده در بین پرانتزها، می خواهید. این همانند عملکرد GetNextRequest می باشد.
- ☑ **M:** مقدار حداکثر بازتکرارها[1] را که به معنی درخواست شما از باقیمانده (تعداد درخواست شده اشیاء N) اشیاء محتوی 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 متغییر 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 کزده 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 مرزهای دسته ها) بکار می رود. دو متغیر اول در لیست متغیرهای یک InformRequest از نوع sysUpTime.0 و snmpEventID.i می باشند.

۱۳-۶: MIB برای SNMPv2

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:

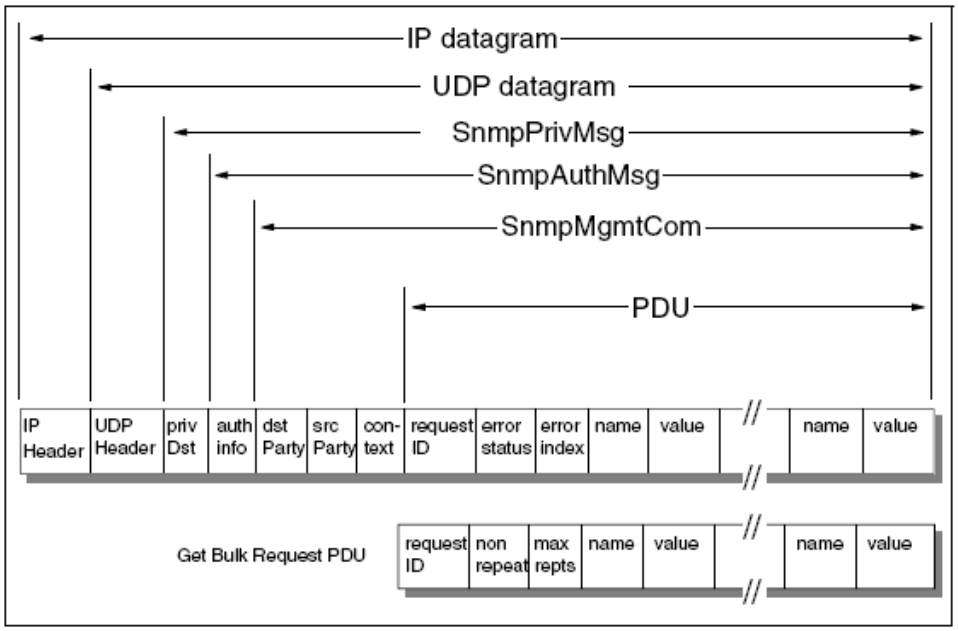
```
sysName OBJECT-TYPE
       SYNTAX       DisplayString (SIZE (0..255))
       MAX-ACCESS    read-write
       STATUS       current
```

```
        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 }
```

۱۳-۷: 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 انجمن در SNMPv1 صرفه نظر شده است. با تعریف بدون ابهام مبداء و نامزد دریافت کننده هر پیام SNMPv2، این استراتژی جدید برپایه طرح انجمنی قدیمی برای هر دو با حمایت از یک مدل کنترل دسترسی مناسب تر به همراه اجازه استفاده موثر از پروتکلهای امنیتی نامتقارن (کلید عمومی) در آینده، بهبود می یابد. تصویر زیر فرمت پیام جدید را نشان می دهد.



۱۳-۵: فرمت پیام SNMPv2

☑ **PDU :** شامل یکی از PDU هی زیر می باشد:

- GetNextRequest
- GetRequest
- Inform
- Report
- Response
- SNMPv2-Trap
- SetRequest

GetBulkRequest دارای فرمت PDU متفاوتی است که قبلاً تشریح گردید. SNMP Trap در حال حاضر فرمتی مشابه با سایر درخواستها دارد.

- ☑ **snmpMgmtCom** : ID دسته مبداء(srcParty)، ID دسته مقصد(dstParty) و محتویات PDU را اضافه می کند. محتویات شامل اطلاعات مدیریتی مورد ارجاع در ارتباط می باشد.
- ☑ **snmpAuthMsg** : این فیلد به عنوان اطلاعات تایید اعتبار از پروتکل تایید اعتبار مورد استفاده بوسیله آن دسته، بکار می رود. snmpAuthMsg براساس ASN.1 BER[1] سریال گذاری 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 این 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 SNMP
- ☑ 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.

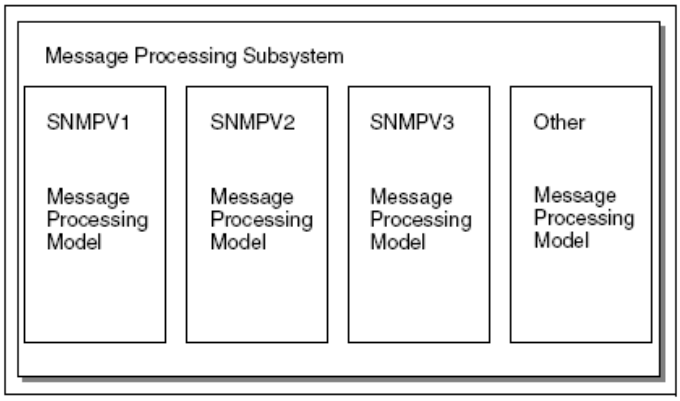
مدل کنترل دسترسی مبتنی بر View در RFC 2575، نحوه تعریف View ها به عنوان زیر مجموعه هایی از درخت کامل MIB را نشان می دهد. سپس کنترل دسترسی برای این View ها در دسترس می باشد.

به دلیل ساختار ماژولار SNMP، تغییر ماژولهای مجزا، تغییر مستقیمی بر سایر ماژولها ندارد. این امر امکان تعریف SNMPv3 را بر روی مدل موجود فراهم می سازد. برای مثال، برای افزودن فرمت جدید پیام SNMP، کافیست تا مدل پردازش پیام بروز گردد. بعلاوه، به دلیل نیاز به پشتیبانی از SNMPv1 و SNMPv2، می توان ماژول جدید پیام 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 عمده 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[1]
- ☑ تغییر جریان پیام
- ☑ افشاء شدن

سرویسهای امنیتی زیر حفاظت لازم در برابر رفتارهای بالا فراهم می آورند:

- ☑ **جامعیت داده:** بوسیله الگوریتم digest پیام DM5 فراهم می گردد. یک digest ۱۲۸ بیتی برروی بخش طرح شده یک پیام SNMPv3 محاسبه شده و به عنوان بخشی از پیام، به گیرنده ارسال می گردد.
- ☑ **تایید اعتبار داده در مبداء**: به وسیله 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 می گردد. این پروتکل با الگوریتم رمز نگاری متقارن، در مد بلاک سرّی زنجیره ای، که بخشی از DES است، بکار می رود. بخش مشخص شده یک پیام SNMPv3 رمز نگاری شده و به عنوان بخشی از پیام ارسالی به مقصد، به آن افزوده می گردد.

[1] - Masquerade

بخش ۵:
شبکه های بی سیم

فصل ۱۴: شبکه های محلی بی سیم

فصل ۱۴:

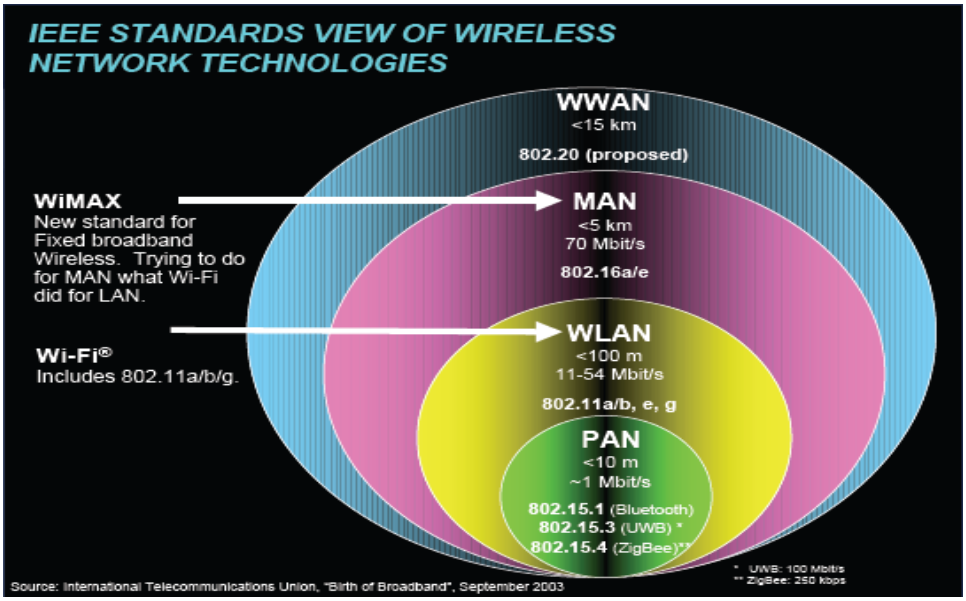
شبکه های محلی بی سیم

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 آغازگردیده 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 پیچیده‌یی چون شبکه‌های بی‌سیم سلولی - که اغلب برای تلفن‌های همراه استفاده می‌شود- و شبکه‌های محلی بی‌سیم (WLAN) گرفته تا انوع ساده‌یی چون 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 این‌گونه شبکه‌ها و هم‌چنین امکان ایجاد تغییر در ساختار مجازی آن‌هاست. از نظر ابعاد ساختاری، شبکه‌های بی‌سیم به سه دسته تقسیم می‌گردند : WWAN، WLAN و WPAN.

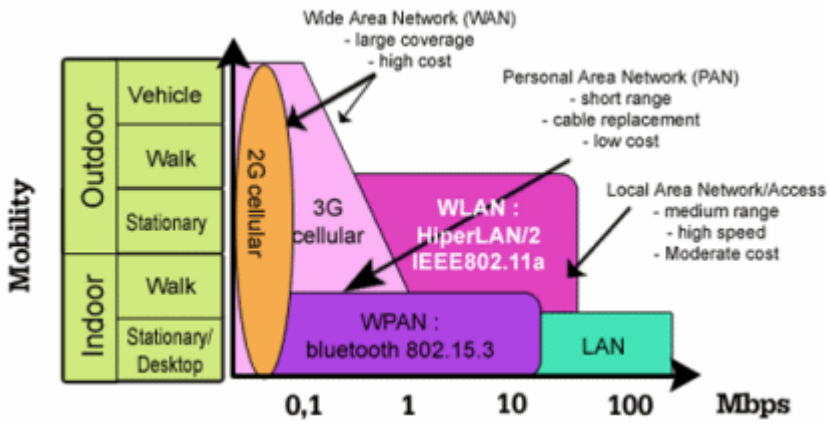
مقصود از WWAN، که مخفف Wireless WAN است، شبکه‌هایی با پوشش بی‌سیم بالاست. نمونه‌یی از این شبکه‌ها، ساختار بی‌سیم سلولی مورد استفاده در شبکه‌های تلفن همراه است. WLAN پوششی محدودتر، در حد یک ساختمان یا سازمان، و در ابعاد کوچک یک سالن یا تعدادی اتاق، را فراهم می‌کند. کاربرد شبکه‌های WPAN[1] یا برای موارد 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 قرارگرفتن 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. به‌عبارت دیگر، ساختار مجازی شبکه‌های محلی بی‌سیم بر پایه‌ی طرحی ایستاست درحالی‌که شبکه‌های Ad hoc از هر نظر پویا هستند.



تصویر ۱۴-۱: انواع متفاوت شبکه های بی سیم

[1] - Wireless Personal Area Network



تصویر ۱۴-۲: نمودار سرعت انواع مختلف شبکه های بی سیم

۱۴-۱: شبکه های محلی بی سیم

اولین شبکه محلی بی‌سیم 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 مقرون به‌صرفه نبود. از همان زمان به بعد، در اوایل دهه‌ی ۹۰ میلادی، پروژه‌ی استاندارد 802.11 در IEEE شروع شد. پس از نزدیک به ۹ سال کار، در سال ۱۹۹۹ استانداردهای 802.11a و 802.11b توسط IEEE نهایی شده و تولید محصولات بسیاری بر پایه این استانداردها آغاز شد. نوع a، با استفاده از فرکانس حامل 5GHz، پهنای باندی تا 54Mbps را فراهم می‌کند. در حالی‌که 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 802.11b است.

WLAN (LAN بی‌سیم) 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 بعهده 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 شبکه ها بصورت پویا می باشد و به دلایلی همچون نیاز به مصرف توان پایین، این شبکه ها عمدتاً بصورت اتصال کامل تمام گره ها به آن قرار ندارد. انتشار امواج در این شبکه ها، متقارن نیست و بدلیل کار برخی انواع آنها در فرکانس 2.4 GHz امواج رادیوی، امکان تداخل امواج این شبکه ها با شبکه های بی سیم دیگر، تلفن های بی سیم، و امواج مایکرویو، وجود دارد.

ساختار و اجزای شبکه محلی بی سیم:

در یک WLAN ، عمدتاً، یک دستگاه فرستنده و گیرنده مرکزی به نام نقطه دسترسی(AP[1]) 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 بعهده دارد. AP با آنتنی که به آن متصل است، می‌تواند در

[1] 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[1]، به WLAN متصل شود. این کارت‌ها به صورت استاندارد برای رایانه‌های شخصی و کیفی ساخته می‌شوند. کارت WLAN به عنوان واسطی بین سیستم عامل شبکه کاربر و امواج دریافتی از آنتن عمل می‌کند.سیستم عامل شبکه عملاً درگیر چگونگی ارتباط ایجاد شده نخواهد بود.

WLANها از دو توپولوژی حمایت می‌کنند:

- توپولوژی Ad hoc
- توپولوژی ساختاردار[2]

در توپولوژی Ad hoc کامپیوترها به شبکه بی‌سیم مجهز هستند و مستقیماً با یکدیگر به شکل نظیر به نظیر[3]، 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.

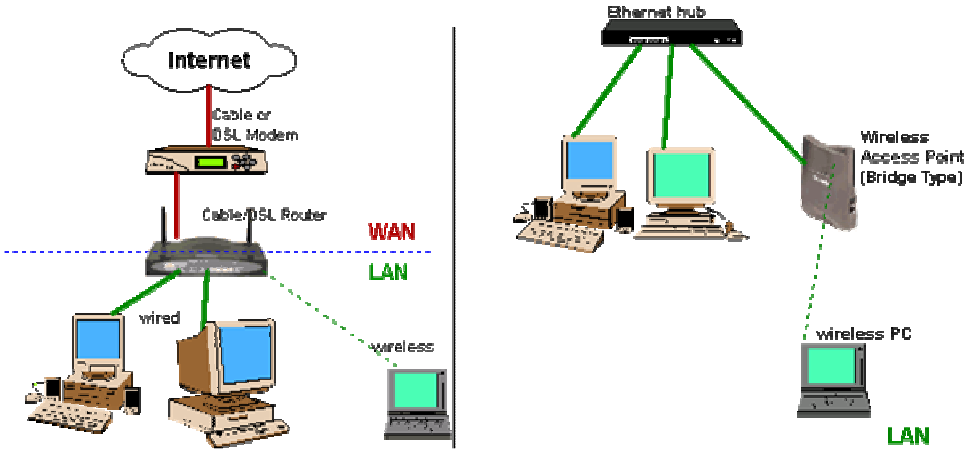
این نوع شبکه که به شبکه Mesh نیز معروف است، شبکه‌ای پویا از دستگاههای بی‌سیم است که به هیچ نوع زیرساخت موجود یا کنترل مرکزی وابسته نیست. در این شرایط، دستگاههای شبکه همچنین به مانند گرههایی عمل می‌کنند که کاربران از طریق آنها می‌توانند داده‌ها را انتقال دهند، به این معنی که دستگاه هر کاربر بعنوان مسیریاب و تکرارکننده، عمل می‌کند. این شبکه نوع تکامل‌یافته شبکه Point-to-Multipoint است که در آن همه کاربران می‌بایست برای استفاده از شبکه دسترسی مستقیم به نقطه دستیابی مرکزی داشته باشند. در معماری Mesh کاربران می‌توانند بوسیله چند پرش[4] ، 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.

AP اساساً بعنوان 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.

---

[1] - Wireless Adapter
[2] - Infrastructure
[3] - Peer to Peer
[4] - Multi-Hop

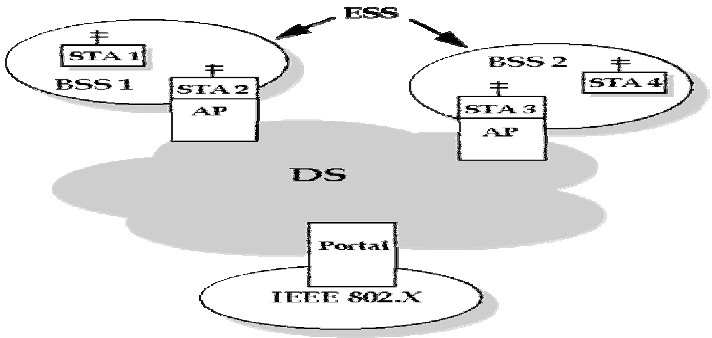


تصویر ۱۴-۳: شیوه های اتصال شبکه بی سیم به شبکه سیمی و اینترنت

در شکل فوق یک AP از طریق یک کابل به شبکه LAN متصل شده است. در اینجا وظیفه یک AP دریافت اطلاعات از سرویس گیرنده‌ها 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.

ناحیه‌ای که توسط یک AP تحت پوشش قرار می‌گیرد BSS[1] (و در برخی موارد سلول) نامیده می‌شود. هر ایستگاه در داخل BSS می‌تواند به AP دسترسی پیدا کند. وظیفه یک AP ایجاد هماهنگی بین سرویس گیرندگان شبکه WLAN و یک شبکه LAN می‌باشد.

به منظور گسترش بخش بی‌سیم و تحت پوشش قرار دادن سرویس گیرندگان بیشتر، می‌توان از AP های متعدد در مناطق مختلف استفاده کرد، و یا اینکه یک نقطه توسعه(EP[2]) را بکار گرفت. EP، یک تقویت کننده سیگنال‌های بی‌سیم است که به عنوان ایستگاهی بین سرویس گیرندگان بی‌سیم و AP عمل می‌کند. اگر شبکه از چند BSS استفاده کند، BSS ها بوسیله یک ستون فقرات بنام سیستم توزیع(DS[3]) به هم اتصال می‌یابند. DS معمولاً یک شبکه کابلی است، اما می‌توان آن را بی‌سیم هم در نظر گرفت. همچنین به چنین طرحی که شامل چند BSS می باشد، ESS[4] ، می گویند.



تصویر۱۳-۴: یک شبکه محلی بی سیم چند بخشی

شعاع پوشش شبکه بی‌سیم بر اساس استاندارد ۸۰۲،۱۱ به فاکتورهای بسیاری بستگی دارد که برخی از آنها به شرح زیر هستند :

- پهنای باند مورد استفاده

---

[1] Basic Service Set -
[2] Extension point -
[3] Distribution System -
[4] Extended Service Set -

- منابع امواج ارسالی و محل قرارگیری فرستنده‌ها و گیرنده‌ها
- مشخصات فضای قرارگیری و نصب تجهیزات شبکه‌ی بی‌سیم
- قدرت امواج
- نوع و مدل آنتن

شعاع پوشش از نظر تئوری بین ۲۹متر (برای فضاهای بسته‌ی داخلی) و ۴۸۵متر (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 کلیی که برای استفاده از این پروتکل (802.11b) ذکر می‌شود چیزی میان ۵۰ تا ۱۰۰متر 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] (ETS,[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 ۱۴-۱: سطوح پهنای باند و توان مصرفی در شبکه های محلی بی سیم

۱۴-۲: شبکه های بی سیم، مزایا و معایب

در این قسمت به برخی مزایای یک WLAN نسبت به یک شبکه کابلی می‌پردازیم. از WLAN ها 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 مداوم 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 بپردازند و بدین شکل امکان دسترسی سریع به اطلاعات را فراهم کنند.

با وجود تمام این مزایا، می توان موارد زیر را جزء معایب شبکه های بی سیم نامید:

- محدودیت پهنای باند: علاوه بر محدودیتهای پهنای باند ISM، در نقاط مختلف دنیا، محدودیتهای دیگر پهنای باند نیز وضع می گردد که خود عاملی جهت کاهش پهنای باند می باشد.
- محدودیت توان مصرفی: بدلیل سیار بودن ایستگاه ها در این شبکه، آنها باید از انرژی ذخیره شده در باتریهای خود استفاده نمایند. این موضوع نیازمندی به شیوه های کاهش توان مصرفی در ابزارهای متحرک را شدیداً تحت تاثیر قرار می دهد.
- توان خروجی محدود: توان خروجی محدود IEEE 802.11، زمینه کاهش برد امواج را فراهم می آورد. به همین دلیل، جهت افزایش برد شبکه، نیازمند استفاده از سخت افزار اضافی هستیم که این خود باعث افزایش هزینه های ایجاد ونگهداری شبکه می گردد.
- امنیت فیزیکی محدود: نویز پذیری این شبکه ها بالا می باشد 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 داده های ارسالی در شبکه، وجود ندارد.
- توپولوژی پویا: وجود ساختارهای پویا، زمینه ساز ایجاد شیوه های مدیریتی پیچیده گره های شبکه، می باشد.
- 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 می باشد.

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، اشیای موجود در ساختمان مانعی 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 توپولوژی 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 بحساب می‌آیند. بعنوان 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 دقیقا 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 کـه از فناوری FHSS استفاده کند نمی‌تواند با سیستمی با فناوری DSSS کار کند.
- اگر فرکانس کار دو سیستم با یکدیگر یکسان نباشـد، حتـی در صـورت اسـتفاده از فنـاوری 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 ایجاب می‌کند تا سیستمهای مختلف که دارای طیفهای فرکانسی یکسانی هستند، بر روی یکدیگر اثر تداخل داشـته باشـند. بـا این وجود اغلب تولیدکنندگان در تولیـد محـصولات خـود تمهیـداتی را بـرای مقابلـه بـا آن بکـار می‌گیرند، به نحوی که وجود چند سیستم WLAN نزدیک به یکدیگر، تداخلی در دیگـر سیـستمها بوجود نمی‌آورد.
۵. ملاحظات مجوز فرکانسی: در اغلب کشورها ارگانهای ناظر بر تخصیص فرکانس رادیـویی، محـدوده فرکانس شبکه‌های WLAN را مشخص کرده‌اند. این محدوده ممکن است در همه کشورها یکـسان نباشد. معمولا سازندگان تجهیزات WLAN فرکانس سیستم را در محدوده مجاز قرار مـی‌دهنـد. در نتیجه کاربر نیاز به اخذ مجوز فرکانسی ندارد. این محدوده فرکانس به ISM معروف است. محـدوده بـین‌المللـی ایـن فرکانـسها ۹۲۸-۹۰۲ مگـاهرتز،۲/۴۸۳-۲/۴ گیگـاهرتز، ۵۳۵-۵/۱۵ گیگـاهرتز و ۵/۸۷۵-۵/۷۲۵ گیگاهرتز است. بنابراین تولیدکنندگان تجهیزات WLAN باید این محـدوده مجـوز فرکانسی را در سیستمهای خود رعایت کنند.
۶. سادگی و سهولت استفاده: اغلـب کـاربران در مـورد مزیتهـای WLAN هـا اطلاعـات کمـی دارنـد. می‌دانیم که سیستم عامل اصولاً به نحوه اتصال سیمی و یا بی‌سیم شبکه وابستگی ندارند. بنـابراین 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. مـدیران شـبکه به سادگی می‌توانند نصب و راه‌اندازی سیستم را با توجه به توپولوژی شبکه موردنظر انجـام دهنـد. در WLAN کلیه کاربران بدون نیاز به کابل‌کشی می‌توانند با یکدیگر ارتباط برقرار کنند. عـدم نیـاز به کابل‌کشی موجب می‌شود که تغییرات، جابجایی و اضافه کردن در شبکه به آسانی انجـام شـود. در نهایت به موجب قابلیت جابجایی آسان تجهیزات WLAN مدیر شـبکه مـی‌توانـد قبـل از اینکـه تجهیزات شبکه را در مکان اصلی خود نصب کند، ابتدا آنها را راه‌انـدازی کنـد و تمـامی مـشکلات احتمالی شبکه را برطرف سازد و پس از تایید نهـایی در محـل اصـلی جایگـذاری نمایـد و پـس 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 نظـامی بـوده اسـت، امنیـت از جملـه مقولات مهم در طراحی سیستمهای بی‌سیم بشمار می‌رود. بحث امنیت هم در سـاختار تجهیـزات WLAN به نحو مطلوبی پیش‌بینی شده است و این امـر شـبکه‌هـای بـی‌سـیم را بـسیار امـن‌تـر از شبکه‌های سیمی کرده است. برای گیرنده‌هایی که دستیابی مجاز به سـیگنالهای دریـافتی ندارنـد، دسترسی به اطلاعات موجود در WLAN بسیار مشکل است. به دلیل تکنیکهای پیشرفته رمزنگاری برای اغلب گیرنده‌های غیرمجاز دسترسی به ترافیک شبکه غیـرممکن اسـت. عمومـاً گیرنـده‌هـای 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 شـامل دو بخـش اسـت: هزینـه‌هـای زیرسـاختار شبکه مانند APهای شبکه و نیـز هزینـه کارتهـای شـبکه جهـت دسترسـی کـاربران بـه WLAN.

هزینه‌های زیرساختار شبکه به تعداد APهای موردنیاز شبکه بستگی دارد. قیمت یک AP بین ۱۰۰۰ تا۲۰۰۰ دلار می‌باشد. تعداد APهای شبکه به شعاع 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 توپولوژی بسیار ساده تا بسیار پیچیده را طراحی کرد. در شبکه‌های بی‌سیم با افزایش تعداد AP ها ، می‌توان محدوده فیزیکی تحت پوشش و تعداد کاربران موجود در شبکه را تا حد بسیار زیادی گسترش داد. شعاع 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 مستهلک می‌گردند و در عین حال، افرادی را که در محدوده تشعشع انرژی 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 شبکه های بی سیم:

در حال حاضر عملاً تنها پروتکلی که امنیت اطلاعات و ارتباطات را در شبکه‌های بی‌سیم بر اساس استاندارد 802.11 فراهم می‌کند WEP[1] است. 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 به‌خاطر 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 دهنده‌ی اشتراکی هرچند جزءیی 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.

[1] - Wired Equivalent Privacy

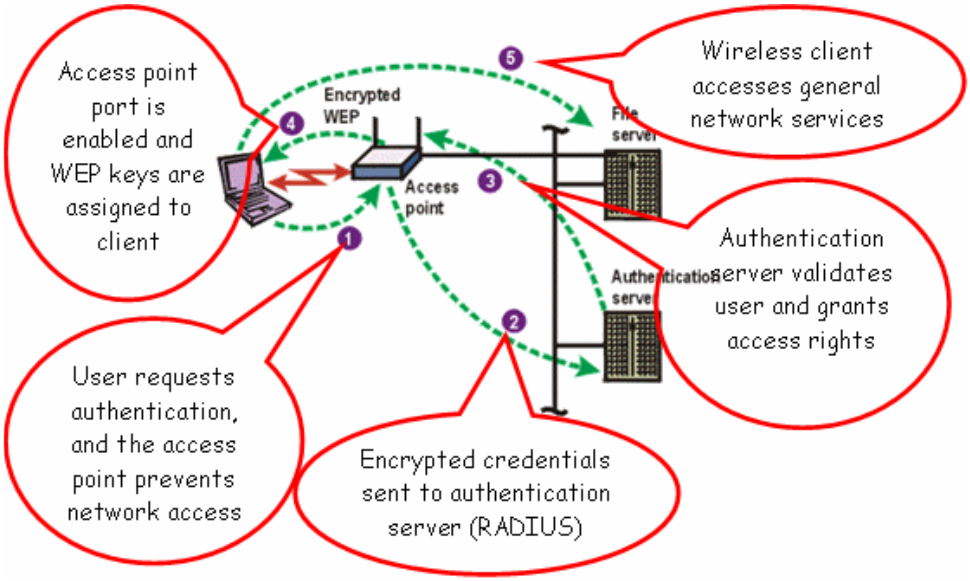
- محرمانه‌گی[1]: محرمانه‌گی هدف دیگر WEP است. این بُعد از سرویس‌ها و خدمات WEP با هدف ایجاد امنیتی در حدود سطوح شبکه‌های سیمی طراحی شده است. سیاست این بخش از WEP جلوگیری از سرقت اطلاعات در حال انتقال بر روی شبکه‌ی محلی بی‌سیم است.
- جامعیت: هدف سوم از سرویس‌ها و قابلیت‌های WEP طراحی سیاستی است که تضمین 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 کم‌وبیش 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 گره های استفاده کننده از WEP فقط با وجود کلید WEP قابل دسترس می باشد.

WEP دارای ۲ نمونه می باشد:

- رمزگذاری ۶۴ بیتی که تنها ۴۰ بیت آن واقعاً استفاده می شود.
- رمزگذاری ۱۲۸ بیتی که ۱۰۴ بیت آن مورد استفاده قرار می گیرد.

نمونه ۶۴ بیتی، طرح استاندارد و پیش فرض رمز گذاری می شود، وای براتی شکسته مـی شـود. طـرح ۱۲۸ بیتی مطمئن تر می باشد، 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[2]
  - بعنوان WEP2 شناخته می شود.
  - ایجاد جریان رمز RC4 بوسیله امنیت RSA

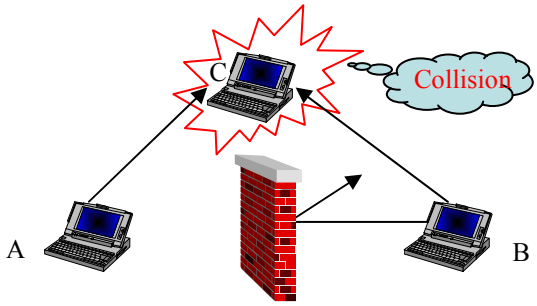
[1] Confidentiality -
[2] Temporal Key Integrity Protocol -

- کلید ۱۲۸ بیتی موقت ترکیب شده با آدرس MAC کامپیوتر مشتری
- تغییر کلید در هر ۱۰,۰۰۰ بسته

- AES[1]
  - 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.

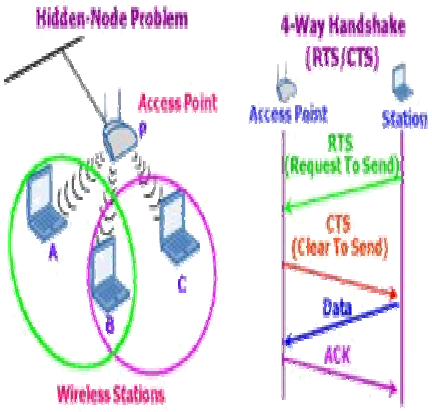


تصویر ۱۴-۶: مشکل گره های پنهان

بعنوان نمونه مثال ، تصویر زیر را درنظر بگیرید. ایستگاه های A، B و C 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(هوا) 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، وگرنه فرستنده باید دوباره سعی در ارسال داده ها بنماید.

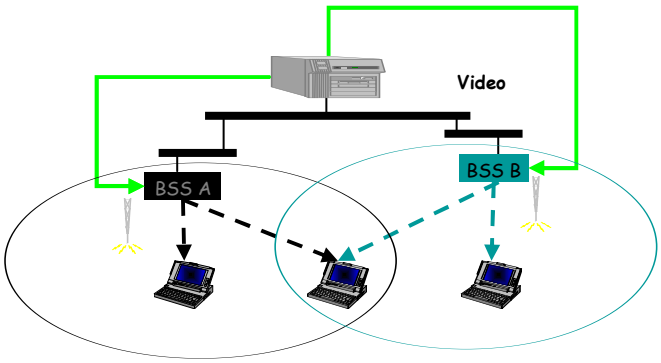
[1] - Advanced Encryption Standard



تصویر ۱۴-۷: گره های پنهان و دست دهی ۴ طرفه

سرگردانی[1]:

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 این BSS انجام می شود. همین حالت در مورد BSS B عیناً تکرار می گردد. این مشکل بدلیل متحرک بودن ایستگاه های ۸۰۲،۱۱، رخ می دهد.



تصویر ۱۴-۸: سرگردانی گره در شبکه بی سیم

۱۴-۳: مدیریت مصرف توان

از آنجا که بخش عمده کاربران شبکه های بی سیم را کاربران ابزارهای موبایل تشکیل می دهند، ۸۰۲،۱۱ 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 MP=PS، ایستگاه در وضعیت ذخیره توان(PS[2]) 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.

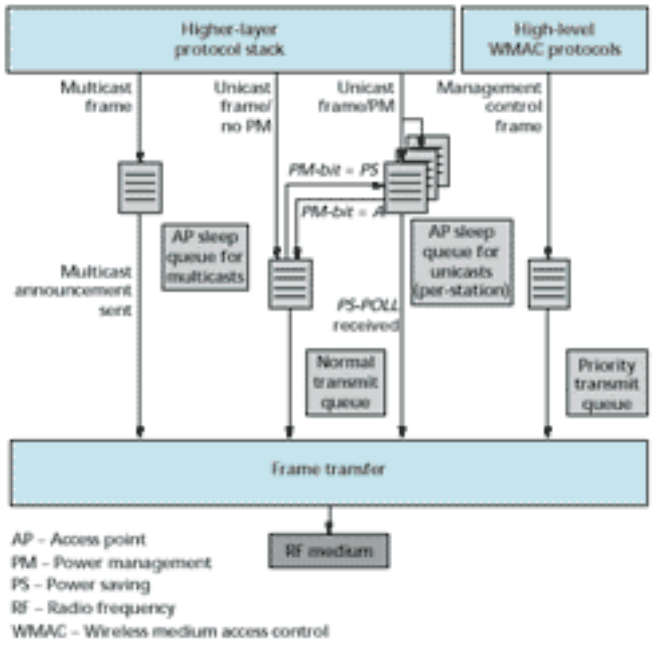
---

[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[1]، 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[2] 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 Beacon جهت نمایش بافرشدن پیامهای Multicast ، بکار می رود. ، بکار می رود. زمانیکه یک Multicast Beacon دریافت گردد، پیامهای Multicast بلافاصله ارسال می گردد. زمانیکه یک ایستگاه یک فریم Beacon پیام Multicast 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 ۱۴-۹: طرح مدیریت توان یک AP

بلاک 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 صفهای Unicast مجزا برای هر ایستگاه نیز وجود دارد.

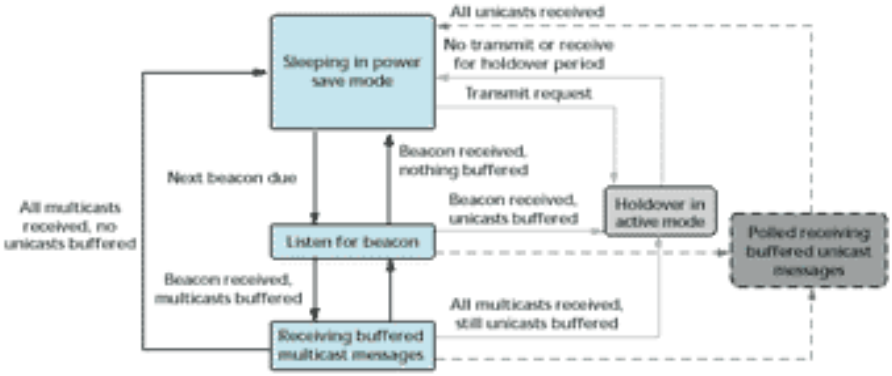
---

[1] Doze

[2] Awake

هر زمان که یک ایستگاه **اجازه** ارسال فریم را بدهد، پیام جلوی صف Unocast ایستگاه ، به انتقال فریم با انتقال با اولویت بالا، تحویل می گردد. زمانیکه یک ایستگاه در وضعیت PS (PM=PS) باشد، پیامی را به AP می فرستد، که نشان می دهدکه در حالت A(PM=A) قرار دارد(دیگر اجازه دادن مطرح نیست)، همه پیامهای Unicast بافر شده به صف انتقال نرمال، انتقال می یابد. زمانیکه یک ایستگاه در وضعیت فعال، پیامی را به AP می فرستد که بوضعیت خواب (PM=PS) رفته است، همه پیامهای آن از صف انتقال نرمال به صف خواب Unicast ایستگاه ها، انتقال می یابد.

نمودار زیر یک بلاک دیاگرام از دو طرح مدیریت توان را نشان می دهد: طرح استاندارد ۸۰۲،۱۱ و یک طرح پیشرفته توسعه داده شده برای The Wave LAN.



State diagram for two different power management schemes.

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 می کنند. زمان سنج ایستگاه، ایستگاه را برای یک فریم Beacon بیدار می کند. اگر پیامی بافر نشده باشد، ایستگاه بلافاصله به وضعیت خواب برمی گردد. این چرخه در هر دو طرح استاندارد ۸۰۲،۱۱(با رنگ آبی و خاکستری روشن) و طرح پیشرفته The Wave LAN (با رنگ آبی و خاکستری تیره)، وجود دارد و اجازه می دهد تا ایستگاه در ۹۹٪ زمانش در وضعیت خواب، قرار داشته باشد.

در طرح استاندارد، زمانیکه پیام بافر شده تشخیص داده شد، ایستگاه در وضعیت بیدار باش قرار می گیرد و منتظر دریافت پیامهای Multicast ویا سرکشی فعال AP جهت پیامهایش می ماند. طرح پیشرفته یک وضعیت HoldOver را اضافه کرده است که در موقعیتهای تشخیص انتقال و یا وجود پیامهای بافر شده ، استفاده می شود. این وضعیت HoldOver بصورت موقت ایستگاه را از وضعیت خواب به وضعیت فعال در می آورد و PM را به A تنظیم می کند. سپس AP اقدام به ارسال همه پیامهای بافر شده می کند و صف Unicast ایستگاه را متوقف می کند. این ایستگاه تا پایان دوره HoldOver، فعال می ماند (معمولاً بین ۳ تا ۵ ثانیه) و در این مدت ایستگاه بدون هرگونه فعالیت ارسال و یا دریافت می باشد.

مزیت این وضعیت HoldOver در آنست که اکثر فعالیتهای LAN بصورت انفجاری می باشد. انفجاری دوره هایست که در آن در دوره های زمانی، هیچ ترافیکی بوسیله دوره های ترافیک سنگین، جریان نمی یابد. با فعال نگه داشتن ایستگاه در دوره HoldOver ، نیازی به تشکیل صف نمی باشد. همچنین، سیستم نمونه برداری پیام ، مورد استفاده برای دریافت پیامهای بافر شده، نسبتاً ناکارا می گردد. سرانجام، اگر ایستگاه برای مدتی در وضعیت خواب قرار داشته باشد، می توان بصورت دستی ایستگاه را برای هرکاربردی 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

- 802.11a: با وجود آنکه 802.11b بیشتر به عنوان پایه استانداردهای اصلی ۸۰۲،۱۱ تعریفی IEEE ، مطرح می گردد، 802.11a یک جابجایی فناوری مهیج سریعتر به قلمرو جدید را ارائه می دهد. این پروتکل از OFDM در لایه فیزیکی خود، بعنوان مکانیزم انتقال داده خود استفاده می نماید. مهمترین پیشرفت در 802.11a را می تواند نرخ انتقال داده بغایت سریع آن دانست. با سرعت تئوری 54Mbps، اگر کاربران در یک محیط بدون مانعی 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 36 Mbps – 20 را بدست آورند. بدلیل استفاده از دامنه فرکانس 5GHz در لایه فیزیکی، می توان از تداخل امواج با سایر ابزارها، صرفه نظر کرد. این بزرگترین مزیت 802.11a در برابر 802.11b می باشد که بصورت بسیار گسترده مستعد انواع تداخلات می باشد.
- 802.11b: با در نظرگرفتن اسلاف استاندارد شبکه های بی سیم ۸۰۲،۱۱، 802.11b هنوز هم در باند فرکانس رادیویی 2.4GHz و فروسرخ، عمل می نماید. پیشرفتهای این پروتکل در رشد نرخ انتقال آن از 5.5-11Mbps و بهبود دامنه آن، می باشد. دقت کنید که این تنها یک نرخ نظری سرعت انتقال ، تحت شرایط بهینه شبکه و محیط می باشد. نرخ گذردهی واقع بینانه 802.11b ، درحدود 4-5Mbps می باشد.
- 802.11c: 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[1]، بهره می برند.
- 802.11d: بعد از شروع کار، ۸۰۲،۱۱ مقداری درمورد توجه جهت رفتن به رفتن به سمت سایر طرحهای مشهور، نگران بود. مقدمه گروه کاری استاندارد ۸۰۲،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 بدنبال 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 5GHz بعنوان فرکانس متفاوت مهیج از یک کشور تا کشور دیگر، استفاده شده است.
- 802.11e: استانداردی است که جهت افزایش بهره وری انتقال بی سیم صوت و تصویر پیوسته برپایه یک تاخیر، 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 802.11e، برروی ترقی و بهبود کیفیت سرویس برای صوت وتصویر 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 به بهبود شدید انتقال و ارائه داده، کمک می کند.

---

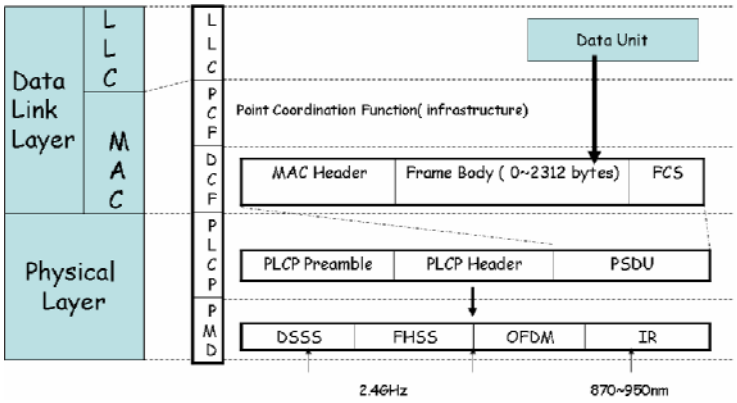
[1] - Bridged Communication

- 802.11f: هدف اصلی گروه کاری استاندارد 802.11f، کمک به هدف همسازی درونی بین AP های فروشنده های مختلف، می باشد. پروتکل ۸۰۲،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 فروشندگان، زمینه نیاز به ایجاد یک استاندارد جهت مجاز نمودن کاربران به حداکثر کردن قدرت جابجاییشان را فراهم آورد. توجه گروه کاری 802.11f، کمک به ترقی ۸۰۲،۱۱ و مجاز ساختن آن به سازگاری بیشتر بین تولیدکنندگان بی سیم مختلف و تولیداتشان، می باشد.
- 802.11g: این پروتکل از یک فرکانس کاری مشابه 802.11b در دامنه 2.4GHz استفاده نموده و از کلید کد تعریفی(CCK) 802.11b، جهت اطمینان از انطباق و سازگازی با شبکه های عقب مانده کار کننده با نرخ انتقال 5.5-11Mbps ، بهره می برد. این استاندارد با 802.11a در زمینه های حداکثر سرعت نظری 54Mbps و متوسط گذردهی مشابه با آن، رقابت می نماید. این عقل سلیم 802.11g را می رساند که فناوری OFDM از 802.11a را مورد استفاده قرار داده تا سرعت آن را بدست آورد و هنوز هم در دامنه فرکانس 2.4GHz، عمل می کند. 802.11g امروزه در زمینه های مختلف، در سطح ثابتی قرار دارد
- 802.11h: این پروتکل جهت انطباق با قوانین عملکرد 5GHz در اروپا(802.11a)، ارائه شده است. مزیت این پروتکل در کنترل انتقال و انتخاب پویای فرکانس می باشد. به این ترتیب کاربران 802.11a 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.
- 802.11i: پس از موفقیت رمزگذاری WEP در آگوست ۲۰۰۱، گروه کاری 802.11i، بیشتر مورد توجه قرار گرفت؛ بویژه آنکه هدف اصلی آن بهبود امنیت بی سیم بود. 802.11i یک گروه استاندارد ۲ سطحیست که هردو به اهداف مرتبط با 802.1x(بخشی از استاندارد ۸۰۲،۱۱ نیست) و امنیت شبکه و همچنین نگاهی عمیق تر به امنیت ثابت WEP بنام جامعیت کلید موقت(TKI[1])، توجه نموده است.
- 802.11n: این استاندارد به عنوان پاسخ سریع به کمبود سرعتهای شبکه های بی سیم موجود، مطرح شده است. با سرعت عملکرد 100 Mbps، این پروتکل براحتی سرعتی ۲ برابر سرعت انتقال شبکه های بی سیم کنونی دارد و در عین حال قابلیت انطباق با مدلهای 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 برپایه پیش نویسهای اولیه آن نموده اند.
- 802.11ng: این استاندارد را می توان نسل بعدی استاندارد ۸۰۲،۱۱ نامید. از ویژگیهای آن می توان به سرعت انتقال بالاتر و مدولاسیون Ultera-Wideband، اشاره نمود.

۱۴-۵: لایه فیزیکی

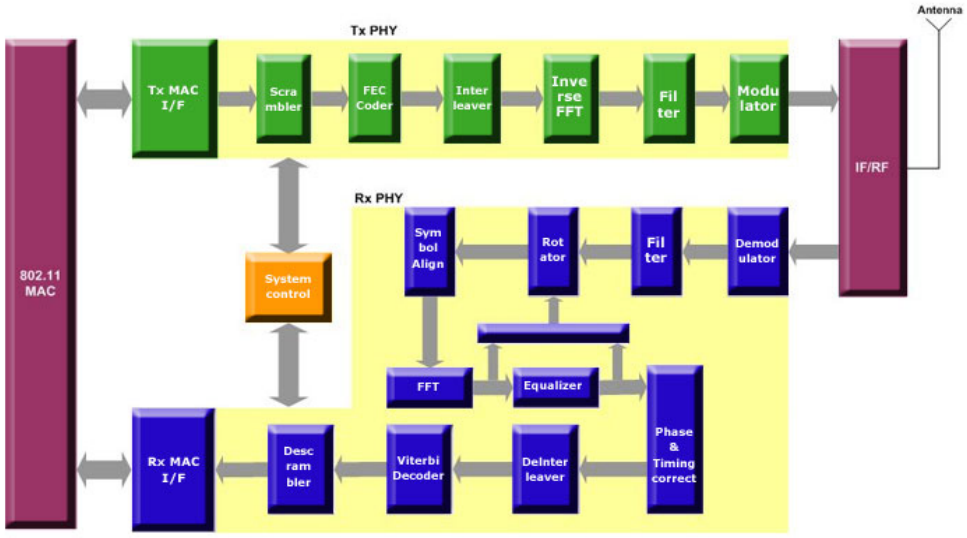
همانطور که دیدیم، باند 2.4GHz تنها باند مورد استفاده در دنیا نیست. استاندارد ۸۰۲،۱۱ تنها به لایه های MAC و فیزیکی شبکه های بی سیم می پردازد.

[1] - Temporal Key Integrity



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[1])، OFDM، FHSS[2] و DSSS[3]. طرح IR از اشعه فروسرخ جهت انتقال داده استفاده می کند، همانند کنترل تلوزیون، و سایر طرح ها از فرکانسهای رادیویی (FR)، استفاده می کنند. طرح های DSSS و FHSS بر مبنای طیف گسترده[4] عمل می کنند که در سال ۱۹۴۰ توسط Hedy Lamarr، هنرپیشه زن هالیود(استرالیایی الاصل)، در سن ۲۶ سالگی، در خلال جنگ جهانی دوم ابداع گردیده است.



تصویر ۱۴-۱۱: بلاک دیاگرام لایه فیزیکی 802.11a

FHSS:

سیستم FHSS تمام پهنای باند را به تعدادی زیر باند با پهنای کم ، کانال، 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 کانال 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 300 msec می باشد.

---

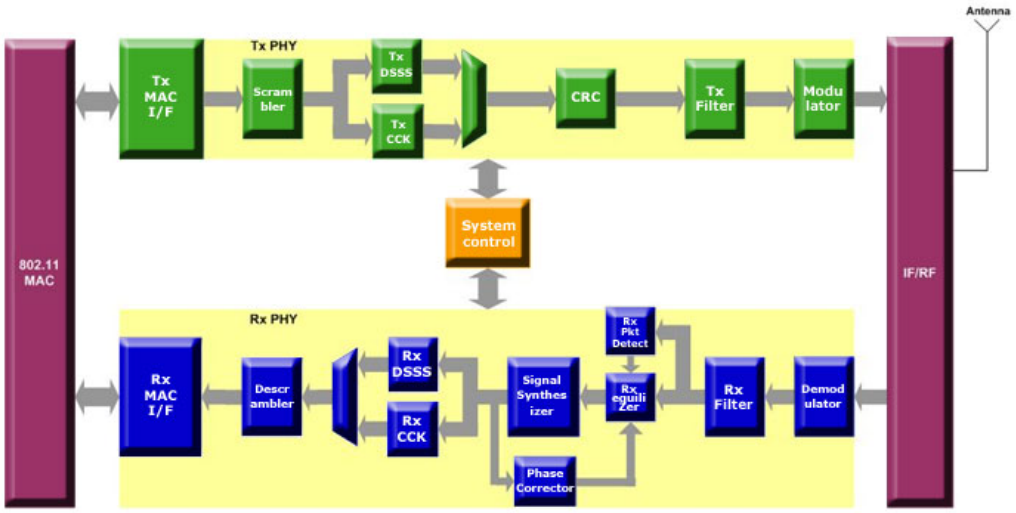
[1] - Infrared

[2] - Frequency Hopping Spread Spectrum

[3] - Direct-Sequence Spread Spectrum

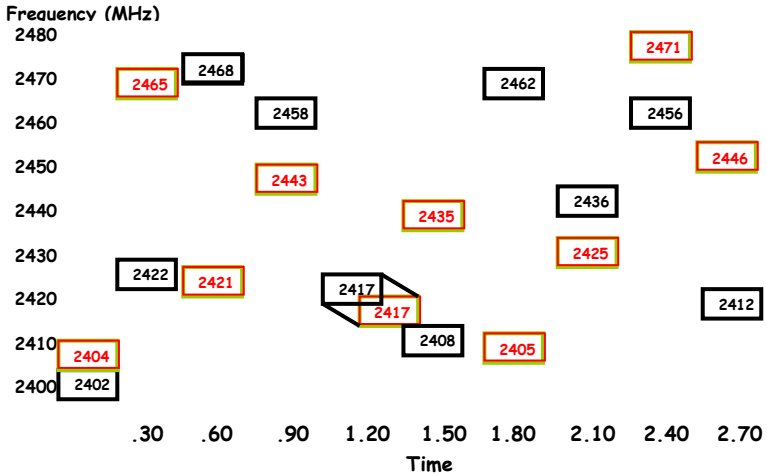
[4] - Spread Spectrum

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 ۱۴-۱۲: بلاک دیاگرام لایه فیزیکی 802.11b

از مزایای پرش فرکانس می توان به تاثیر جانبی آن در کمک به اجتناب از تصادم، اشاره نمود. بدلیل ارسال سیگنال، تنها در بازه کوتاه در هر کانال، تصادم بسیار کمتر رخ می دهد. با نرخ 1 MHz برای پهنای هر کانال، تعداد آنها بازهم به موقعیت شبکه بستگی دارد. در ژاپن، ۲۳ کانال بین 2.473 GHz تا 2.495 GHz تعریف شده است ودر آمریکا ۷۹ کانال بین 2.402 GHz تا 2.48 GHz ، تعریف شده است.



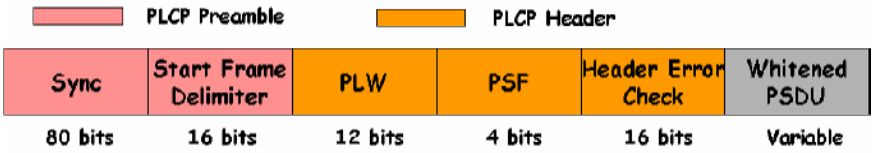
تصویر ۱۴-۱۳: کاهش امکان تصادم با استفاده از طرح پرش فرکانس

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 قبل 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[1])، انطباق را

[1] - 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 کع 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.



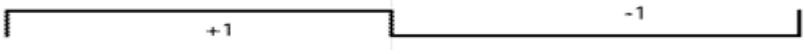
تصویر ۱۳-۱۴: ساختار فریم FHSS

- Sync: ترکیبی از صفر و یک متناوب جهت آگاه سازی دریافت کننده.
- حائل شروع فریم: تعیین کننده آغاز یک فریم:0000110010111101
- PLW[1]: طول PSDU را مشخص می کند.
- PSF[2]: نرخ داده Whitend PSDU را مشخص می کند.
- کنترل خطای سرآیند: CRC ۱۶ بیتی کنترل خطا.
- 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 پهنای باند به کانالهایی و سپس سوئیچ کردن بین آنها، DSSS سیگنال را در تمام پهنای باند می گستراند و به این ترتیب بهره وروی پهنای 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[3] مورد استفاده، مشخص می گردد. البته برخلاف FHSS، DSSS تلفیق خودش را برمبنای قطع متناوب شیفت مرحله ای(PSK[4])، بنیان نهاده است. جریان نمادهای تلفیق PSK به یک سیگنال مقادیر مختلط، تبدیل می گردد که پس از آن به یک تراشه منتشرکننده، داده می شود. تراشه منتشر کننده، یک سیگنال شبه نویز[5] ، 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[6]، 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:



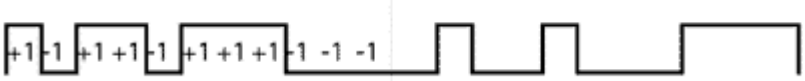
تصویر ۱۴-۱۵: یک پالس نمونه

[1] PSDU Length Word -
[2] PLCP Signaling Field -
[3] Modulation -
[4] Phase Shift Keying -
[5] Pseudo-Noise -
[6] Eleven-Chip Barker Sequence -

اگر این پالس را با توالی زیر تلفیق دهیم:

+1-1+1+1-1+1+1+1-1-1-1

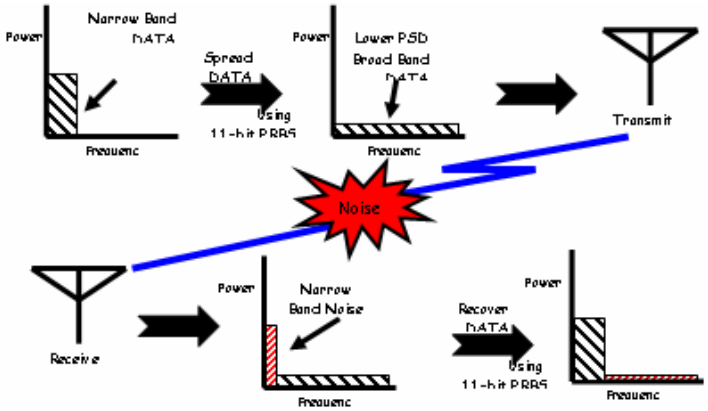
و سپس پالس را در هر انتقال تغییر دهیم(بالا اگر پایین بود و پایین اگـر بـالا بـود)، و یـا موقیعـت آن را در حالات بدون درخواست ارسال حفظ نمائید، پالس تلفیق یافته ای همانند تصویر زیر، خواهید داشت:



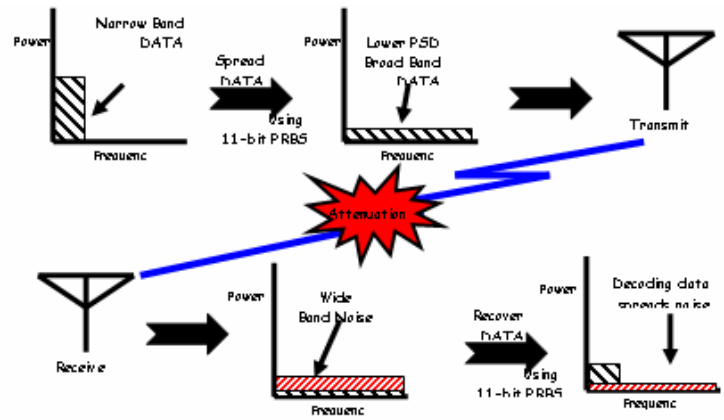
تصویر ۱۴-۱۶: پالس تلفیق یافته نمونه

اگرچه پالسها ، برای نیمه دوم پالس، خارج از توالی هستند، توالی پس ۱۱امین قطع مـورد اسـتفاده ، تکـرار می گردد. بنابراین با اینکه آخرین قطع a-1 است و اولین قطع a+1 است، این حالت مانند یک بازنـشانی و نـه یـک گذار ، عمل می کند. مرحله ای در قطع دوم ،a-1، صورت می پذیرد، که یک گـذار مـی باشـد. گـستراندن سـیگنال برمبنای این توالی، پهنای باند مورد استفاده را گسترش مـی دهـد و پنهـای بانـد مـوثر را از 1 MHz بـه 11 MHz ، افزایش می دهد و این درحالیست که هنوز می توان، در صورت نیاز، آن را به ۵/۵، ۲ و یا 1 Mbps کاهش داد.

گسترش سیگنال همچنین زمینه کاهش تاثیر پذیری آن در برابر تداخل را فراهم مـی آورد؛ بطوریکـه بـرای 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 تـصاویر زیـر نشان داده شده است. در ین تصویر محور y، توان سیگنال و محور x، فرکانس ارسال داده می باشد.

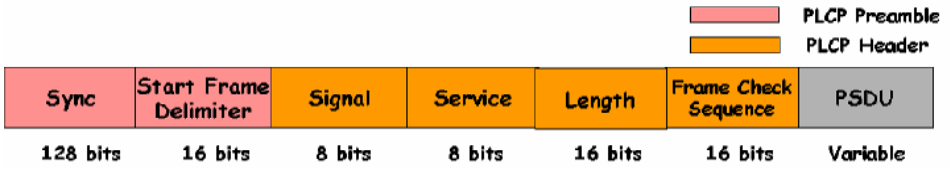


تصویر ۱۴-۱۷: تاثیر نویز بر داده های ارسال شده



تصویر ۱۴-۱۸: تاثیر میرایی بر داده های ارسال شده

سپس خروجی گسترش دهنده به یک تلفیق دهنده تربیع[1] منتقل می شود . سپس تحویل انتقال دهنده نهایی می گردد. ۸۰۲،۱۱ مبتنی بر DSSS، ۲ نرخ بیت دارد: 1 Mbps با استفاده از PSK و BPSK و 2 Mbps با استفاده از تربیع PSK (QPSK).



تصویر ۱۴-۱۹: ساختار فریم DSSS

- 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 میکروثانیه های مورد نیاز جهت انتقال فریم، است.
- تست توالی فریم: CRC ۱۶ بیتی جهت تست خطا.
- PSDU: MSDU ی ارسالی

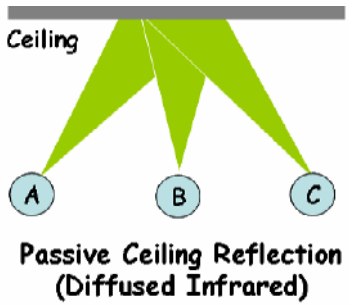
مادون قرمز :

۸۰۲،۱۱ از امواج منتشر شونده IR استفاده می نماید. برخلاف فرستنده و دریافت کننده های متداول خطی فروسرخ ، همانند تلوزیون و کنترل از راه دور، ابزار ۸۰۲،۱۱ 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 دهند. این عمل در مورد داده های دریافتی نیز صورت می گیرد. در ارتباطات مادون قرمز از فرکانسهای بالا - دقیقاً زیر طیف نور مرئی- استفاده می‌شود. در این روش سیگنالها نمی‌توانند از اشیاء و دیوارها عبور کنند. این امر بکارگیری تکنولوژی مادون قرمز را محدود می‌سازد. بطور کلی در ارتباطات داخل ساختمان که فاصله ایستگاهها کم باشد از این روش استفاده می‌شود. بعلاوه در داخل ساختمان نیازمند سقفی جهت بازتاباندن طول موجهای دامنه ۸۵۰ تا ۹۵۰ نانومتری فرو سرخ، لازم است. علاوه بر نیازمندی به سقف، وجود برد تقریباً ۱۰ متری، آن را مناسب اتاقهای کوچک، همانند یک اطاق کاری دارای یک چاپگر فروسرخ، نموده است.

۸۰۲،۱۱ فروسرخ از دون نرخ داده پشتیبانی می کند: 1Mbps و 2Mbps . در سرعت 1Mbps، هر جریان داده به ۴ بخش[2] تقسیم می شود. امواج رادیویی بخاطر برد، پهنای 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[3] 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



تصویر ۱۴-۲۰: استفاده ازIR در ۸۰۲،۱۱

OFDM :

استاندارد IEEE 802.11a از طرح لایه فیزیکی OFDM استفاده می نماید که در آن سیگنالهای داده به ۵۲ زیرحمل کننده[1] مجزا، جهت تهیه نرخ انتقال داده ۶، ۹، ۱۲، ۱۸، ۲۴، ۳۶، ۴۸ و یا 54 Mbps ، استفاده می کند. نرخ داده های ۶، ۱۲ و 24 Mbps اجباری هستند. ۴ زیرحمل کننده، 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 شبه توالی 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، 0.3125 MHz (برای 20 MHz با ۶۴ بازه فرکانس زیرحمل کننده)، می باشد.

هدف اولیه لایه فیزیکی OFDM، هدایت انتقال واحدهای داده پروتکل MAC(MPDUها)، توسط لایه MAC ۸۰۲،۱۱ می باشد. لایه فیزیکی OFDM به بخش تقسیم می شود: پروتکل همگرایی لایه فیزیکی (PLCP[2]) و زیر لایه های وابسته فیزیکی (PMD[3]).

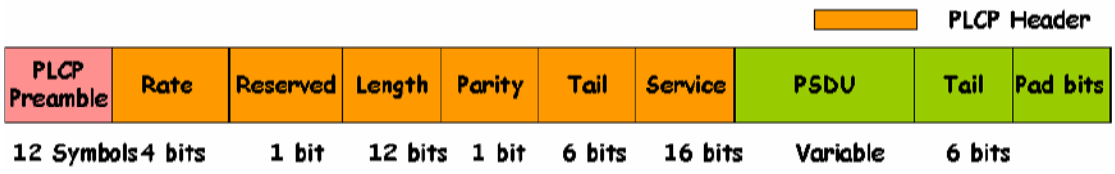
لایه MAC با PLCP از طریق ویژگیهای اصلی از طریق سرویس فیزیکی AP، ارتباط برقرار می کند. با اشاره لایه MAC، PLCP ، MPDU ها رابرای انتقال، مهیا می سازد. همچنین PLCP فریمهای وارد شده از طریق رسانه بی سیم، به لایه MAC تحویل می دهد. زیر لایه PLCP، وابستگی لایه MAC به زیرلایه PMD را بوسیله نگاشت MPDU ها بدورن یک ساختار فریم مناسب برای انتقال بوسیله PMD ، را کاهش می دهد.

با توجه به جهت PLCP، PMD 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 سرویسهای ابتدایی استفاده می نمایند.

تصویر زیر فرمت فریم یک فریم 802.11a را نمایش می دهد. فیلد مقدمه[4]، به دریافت کننده ، رسیدن یک سیگنال OFDM ورودی و همگام سازی بازیاب فریم را اطلاع می دهد. مقدمه، حاوی ۱۲ نماد می باشد. ۱۰ نماد کوتاه بود و جهت برپاسازی کنترل بهره خودکار (AGC[5]) و احتمال دریافت فرکانسهای 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.

---

[1] - Subcarrier
[2] - Physical Layer Convergence Protocol
[3] - Physical Medium Dependent
[4] - Preamble
[5] - Automatic Gain Control



تصویر۱۳-۲۱: ساختار فریم OFDM

فیلد سیگنال، حاوی ۲۴ بیت می باشد که نرخ داده و طول فریم را دربردارد. نسخه 802.11a از OFDM، از ترکیب قطع متناوب شیفت مرحله ای دودویی(BPSK)، PSK جهار بخشی (QPSK) و تلفیق دامنه ۴ بخشی (QAM[1])، براساس نرخ داده مورد نیاز ، نشان داده شده در جدول ۱۴-۲، استفاده می نماید. فیلد طول، طول فریم برحسب بایت را نشان می دهد. مقدمه PLCP و فیلد سیگنال، با BPSK تبدیل و با سرعت 6 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 ۱۴-۲: تکنیک های تلفیق

فیلد سرویس، ۱۶ بیتی است که ۶ بیت اول آن ، جهت همزمانی بازیاب بسته، صفر می باشد و سایر ۹ بیت باقیمانده، جهت استفاده های آتی، رزرو شده می باشند(تنظیم شده به صفر). .احد داده سرویس PLCP(PSDU)، Payload ارسال شده از لایه MAC می باشد. فیلد Pad ، حداقل حاوی ۶ بیت است، اما در واقع تعداد بیتهای آن به اندازه ایست که فیلد داده، بصورت مضربی از تعداد بیتهای کد در یک نماد OFDM (۴۸، ۹۶، ۱۹۲ و یا ۲۸۸)،گردد. یک Scrambler داده، با استفاده از یک مولد توالی ۱۲۷ بیتی، همه بیتهای فیلد داده را با الگوهای بیتی تصادفی ، جهت جلوگیر از جریانهای طولانی صفر یا یک، تغییر می دهد.

با شیوه انطباق OSDM در 802.11a، 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 مختلط، در می آیند. برای مثال، اگر نرخ داده 24 Mbps انتخاب گردد، PLCP بیتهای داده را به 16 QAM، نگاشت می نماید.

پس از نگاشت، PLCP مقادیر مختلط را نرمالسازی می کند تا میانگین توان مصرفی یکسانی برای تمام نگاشتها حاصل گردد. PLCP ، هر نماد، با دوره تناوب ۴ میکروثانیه ای، را به زیرحمل کننده خاصی، انتساب می دهد. یک تغییر شکل عکس فوریه سریع (IFFT[2])، قبل از انتقال، با زیرحمل کننده ها ترکیب می گردد.

همانند سایر طرحهای لایه فیزیکی 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.

فرکانسهای کاری برای لایه OFDM در ۸۰۲،۱۱، به سه باند بدون مجوز 100 MHz تقسیم می گردد: 5.15-5.25 MHz، 5.25-5.35 MHz و 5.725-5.825 MHz. ۱۲ کانال 20 MHz 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.

[1] Quadrature Amplitude Modulation -
[2] Inverse Fast Fourier Transform -

استاندارد 802.11a نیازمند آنست که دریافت کنندگان، یک دامنه محدود dBm 65-82 را بـر اسـاس نـرخ داده انتخابی، داشته باشند.

IEEE شبکه های بی سیم 802.11a و 802.11b را در سال ۱۹۹۹ استاندارد نمود تا فناوری اسـتانداردی را بوجود آورد تا بین شیوه های رمزگذاری فیزیکی مختلف، فرکانسها و کاربردهـایی هماننـد اسـتاندارد اترنـت ۸۰۲،۳ عمل کننده با سرعتهای ۱۰، ۱۰۰ و 1000 Mbps، برروی فیبر نوری و کابلهای مختلف، ارتباط برقرار کند.

استاندارد 802.11b برای کار در باند 2.4 GHz با استفاده از تکنیـک DSSS، طراحـی شـده اسـت. از سـوی دیگر، استاندارد 802.11a، بـرای کـار در بانـد 5 GHz، طراحـی شـده اسـت. اسـتاندارد 802.11a از طـرح OFDM استفاده می کند.

استاندارد 802.11a، که نرخ سرعتهایی تا 54 Mbps را پشتیبانی می کند، شبکه های سریعتری نـسبت بـه 802.11b، که از سرعتهای حـداکثر 11 Mbps پـشتیبانی مـی کنـد، مـی باشـد. هماننـد اترنـت و اترنـت سـریع، 802.11b و 802.11a از یک MAC یکسان، استفاده می نمایند. اگرچه اترنت سریع از طرح لایه فیزیکی یکسانی بـا اترنت استفاده می کند(فقط سریعتر است)، 802.11a از یک طرح کاملاً متفاوت استفاده مـی نمایـد، بنـام OFDM ، استفاده می نماید.

FCC[1] ، طیف موج 300 MHz را برای کاربردهای بدون مجوز در بـلاک 5 GHz، 200 MHz در دامنـه 5.15 GHz تا 5.35 GHz، و 100 MHz دیگر در 5.725 MHz تا 5.825 MHz، تخـصیص داده اسـت. ایـن طیـف بـه سـه ناحیه کاری تقسیم شده است. اولین 100 MHz، در پایین ترین بخش، با توان خروجـی حـداکثر 50 Mw ، محـدود شـده اسـت. 100 MHz دوم، تـوان خروجـی 250 mW را دارد و بـالاترین 100 MHz، جهـت کاربردهـای بیـرون ساختمان، نامزد می باشد و حداکثر توان خروجی آن 1 W است. در مقام مقایسه، کارتهای 802.11b، می تواننـد بـا توان خروجی 1 W در آمریکا، عمل کنند. اگرچه بسیاری از کارتهای مدرن امروزی، به دلایلی همچون حفظ باتری و گرما، تنها بخشی از حداکثر توان خورجی موجود (30 mW) را استفاده می نمایند.

استاندارد 802.11a، برخی از معیارهای کارایی را بواسطه فرکانس کاری بالاتر، بدسـت مـی آورد. افـزایش طیف از 2.4 GHz به 5 GHz، باعث کم شدن برد می گردد. 802.11a برای غلبه براین کـاهش بـرد مقـدار EIRP [2] خود را تا حداکثر 50 Mw افزایش می دهد.

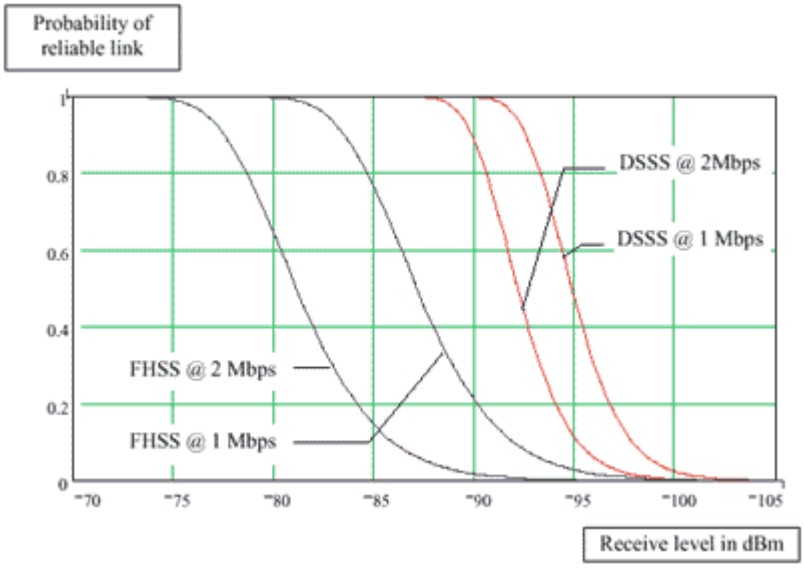
OFDM در اصل جهت اهداف درون ساختمانی بی سیم، توسعه یافته اسـت و کـارایی بـالاتری را نـسبت بـه راه حلهای طیف گسترده ، ارائه می دهد. OFDM با تقسیم یک حامل داده با سرعت بالا به چندین زیرحمـل کننـده با سرعت پایین تر، که آنها به شیوه DMT انتقال موازی ،همانند روش مورد استفاده در مـودم هـای ADSL، را انجـام می دهند، کار می کند. هر حامل سرعت بالا، پهنای 20 MHz داشته و به ۵۲ زیرکانـال ،هرکـدام تقریبـاً 300 KHz، تقسیم می گردد. OFDM از ۴۸ زیرکانال، جهت انتقال داده استفاده می نماید.

هر زیر کانال پیاده شده در OFDM، تقریبـاً 300 KHz پهنـا دارد. بـا کمتـرین حـد سـرعت، BPSK جهـت رمزگذاری 125 Kbps برای هر کانال مورد استفاده قرار می گیرد و در نتیجه ، سرعت به 6,000 Kbps یا 6 Mbps می رسد. با استفاده از قطع متناوب شیفت فاز ۴ گانه(QPSK)، می توان به سـرعت ۲ برابـر بـرای هـر کانـال (250 Kbps) و سرعت کل 12 Mbps دست یافت. با استفاده از ۱۶ سطح تلفیق دامنه ای ۴ بخـشی (4QAM)، ۴ بیـت در هرتز 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 FHSS با DSSS:

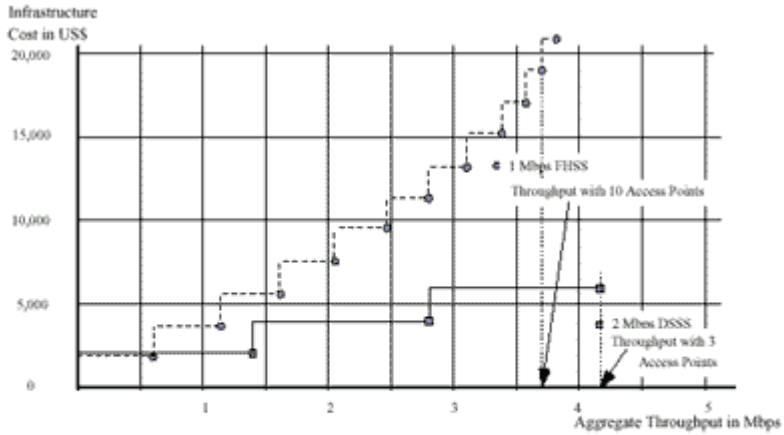
[1] - Federal Communications Commission
[2] - Equivalent Isotropic Radiated Power

در مقایسه FHSS با DSSS، 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 برابر 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 ۱۴-۲۲:مقایسه FHSS با DSSS

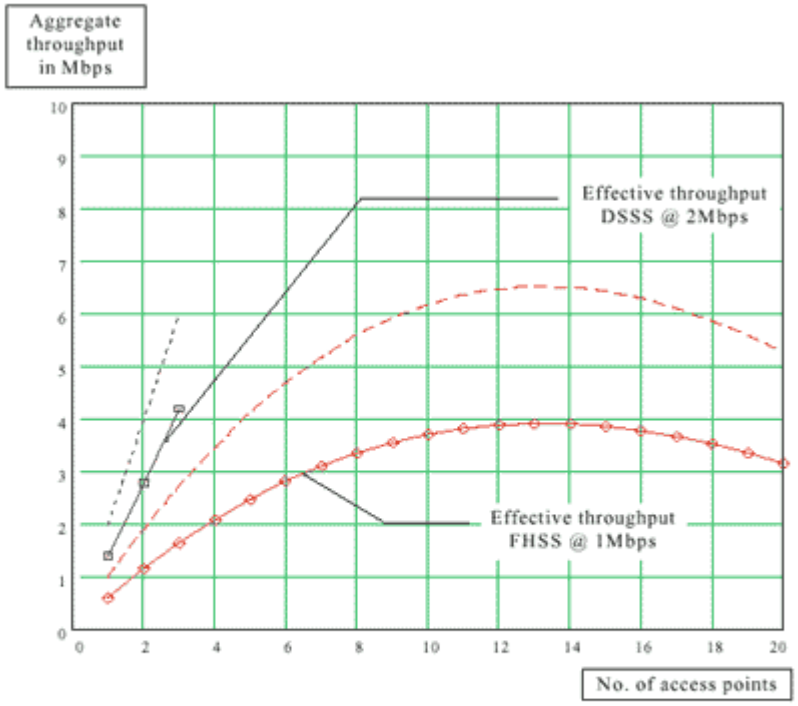
مزیت دیگر DSSS، بازده آن می باشد. DSSS قادر به ارائه کارایی بهتر با تعداد AP کمتر نسبت به FHSS ، می باشد. بعلاوه، FHSS ، همانطور که در تصویر زیر دیده می شود، نقاط تنزل سریعتری را نسبت به DSSS دارد.



Cost of Access points as a function of required throughput
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.

تصویر ۱۴-۲۳:مقایسه هزینه AP بعنوان تابعی از گذردهی مورد نیاز در FHSS و DSSS

بعلاوه،DSSS از تعداد بیشتری AP استفاده می نماید که یک پهنای باند متراک بالاتر سراسری را نسبت بـه FHSS، فراهم می آورد.



Aggregate throughput vs. number of collocated access points
Dotted lines give the gross capacity.
Solid lines with boxes and diamonds gives effective net throughput.
The difference between gross and net throughput comes form overhead in frame headers, the requirement for transmission of acknowledgement frames, and losses due to collisions.

تصویر ۱۴-۲۴: مقایسه نسبت گذردهی با تعداد AP در FHSS و DSSS

بعلاوه در کنار هم گذاشتن شبکه ها، DSSS سرعت بالاتری را با AP کمتر نسبت به FHSS، ارائه می دهد.

۱۴-۶: لایه MAC

پس از بررسی لایه فیزیکی، اجازه بدهید به لایه بالاتر این استاندارد ، لایه MAC، نگاهی بیاندازیم. بـه عنـوان یک استاندارد شبکه بی سیم، MAC استاندارد ۸۰۲،۱۱، با MAC شـبکه هـای سـیمی ، هماننـد اترنـت، فـرق دارد. نمونه ای از این تفاوت آنست که AP در ۸۰۲،۱۱ بعنوان یک پل بین شبکه سیمی و شبکه بی سیم، عمل می کنـد، که در شبکه های سیمی فرض نشده است. بعلاوه فریمهای ۸۰۲،۱۱ ، دارای ویژگیهـای یکتـایی مـی باشـد کـه بـه ارسال و دریافت داده در شبکه بی سیم ، کمک می کند.

هر فریم دارای کنترل توالی و فیلرهای سعی مجدد است که برای به حـداقل رسـاندن تـداخل بـین فریمهـا، مورد استفاده قرار می گیرد. از آنجاکه RF همه جهته می باشد، صرفه نظر از AP یـی کـه ایـستگاه نهـایی بـا 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 تصمیم گیری در مورد این موضوع بکار رود. عطف به فیلد کنترل توالی، می توانید فیلـدهای نوع/زیر نوع و دوره نیز به منظور کمک به ارتبطات 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 برپاسـازی و اسـتفاده از کانال تنهای بی سیم Backbone ، بکار می رود.

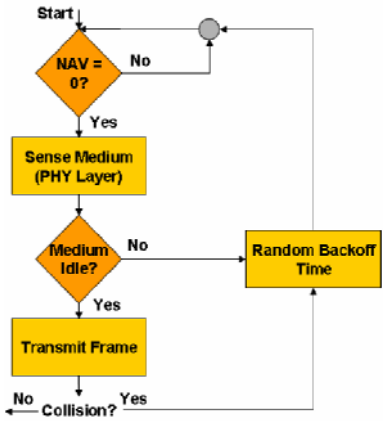
CSMA/CA[1]:

۸۰۲،۱۱ از یک طرح MAC مشابه طرح CSMA/CD اترنت، بنام CSMA/CA، استفاده می کند. مهمترین تفاوت بین این دو در آنست که ۸۰۲،۱۱ بدنبال اجتناب از تصادم می باشد (CA) و درحالیکه در اترنت تشخیص خطا 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 شانس تصادم در طی دوره زمانی که احتمال بالایی 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[2] اتفاقی، استفاده می نماید.

بازه های زمانی مورد استفاده در این تکنیک، بترتیب اندازه شان از کوچک به بزرگ، به شرح زیر می باشند:

- SIFS[3]: جهت یک ACK، CTS، قطعات دیگر MPDU بجز قطعه اول و در پاسخ به نمونه برداری PCF، مورد استفاده قرار می گیرد.
- PISF[4]: در زمان کار با PCF[5] ، جهت کسب اولویت دسترسی به رسانه انتقال بکار می رود.
- DIFS[6]: در زمان کار با DCF[7]، 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.

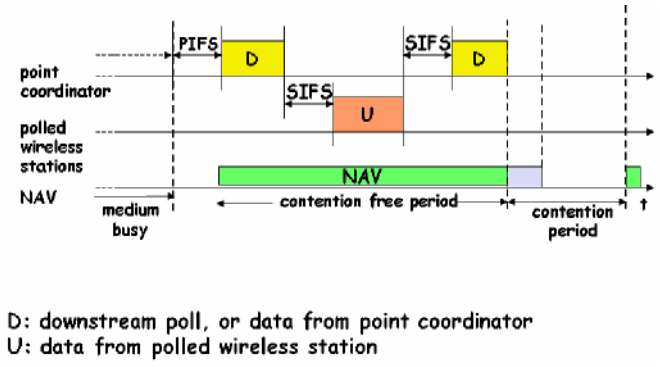
CSMA جهت جلوگیری از تصادم برروی رسانه انتقال، از تابع هماهنگی توزیع شده (DCF) و الگوریتم بازیابی معکوس اتفاقی، استفاده می نماید. DCF یک پروتکل مبتنی بر مجادله می باشد. NAV[8] یک شمارنده است که با مقدار رزرو در فیلد دوره آخرین فریم دریافتی، مقداردهی می گردد. این زمان بیانگر مدت زمانیست که یک ایستگاه جهت انتقال داده های خود، نیازمند می باشد.



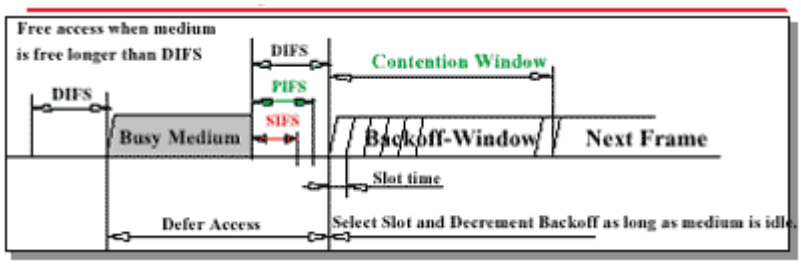
تصویر ۱۴-۲۵: فلوچارت عملکرد CA

[1] Carrier Sense Multiple Access/ Collision Avoidance
[2] BacK-off
[3] Short Interframe space
[4] PCF Interframe space
[5] Point Coordination Function
[6] DCF Interframe space
[7] Distributed Coordination Function
[8] Network Allocation Vector

CSMA/CA همچنین دارای یک تابع هماهنگی نقطه (PCF) اختیاری می باشد که جهت برپاسازی یـک AP به عنوان یک نقطه هماهنگ ساز، بکار می رود. در این تابع، نقطه هماهنگ کننده، اولویتهایی را به هـر متقاضـی، در یک فریم ارسالی، می دهد . گزینه PCF بسیار قدرتمند است؛ زیـرا مـی توانـد جهـت سرویـسهای دارای محـدودیت زمانی همچون صوت، صوت برروی IP(VoIP) و ترافیکهای چند رسانه ای، بکار رود.



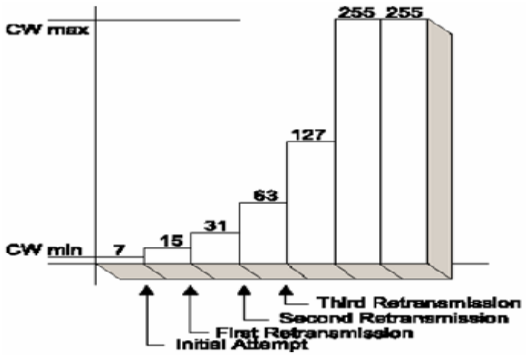
تصویر ۱۴-۲۶: عملکرد PCF



تصویر ۱۴-۲۷: نمودار زمانی عملکرد CA

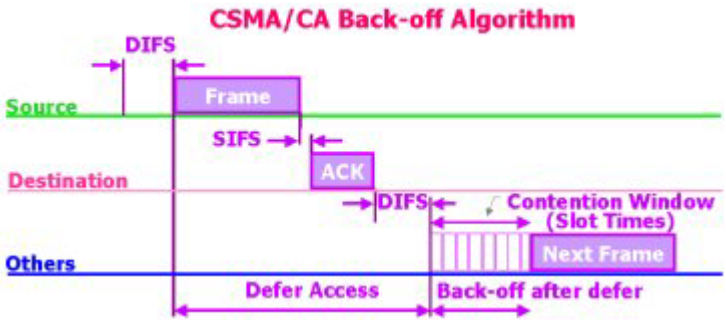
همانطور که در تصویر بالا مشاهده می شود، پس از دوره اشغال بودن رسـانه انتقـال، یـک دوره فـضای بـین فریم (IFS[1])، که برای ۸۰۲،۱۱ 50 µsec است، قرار دارد. همه ابزارهای باید به اندازه دوره IFS، صبر نمایند. پـس از IFS، ابزارها یک زمان اتفاقی اضافی از بازه های 20 µsec ، کـه بوسـیله یـک الگـوریتم بازیـابی معکـوس نمـایی 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، مقـادیر از پـیش تعیـین شـده ای هـستند کـه تعیین صحیح آنها، تاثیر زیادی در ارسال بموقع بسته های داده، دارد. در 802.11e ، جهت بهبود کیفیـت سـرویس 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 شانس ارسال داده های با اولویـت بـالاتر و محـدودیتهای زمـانی سخت تر، بیشتر می گردد. پس از گذشته این زمان، رسانه انتقال آزاد بوده (هنوز هیچ ایستگاهی انتقال داده نـدارد)، و ایستگاه می تواند سعی در انتقال داده بنماید. هر ایستگاه از مقادیر تصادفی (در واقع شـبه تـصادفی) خـودش، بـه عنوان زمان انتظار استفاده می کند. این طرح شانس تصادم را کاهش می دهد. اگر یک تصادم مشخص شود ، ابزارها به وضعیت بازه های زمانی انتظار، برمی گردند تا زمانیکه رسانه انتقال دوباره آزاد گردد.

[1] - Interframe spacing period



تصویر ۱۴-۲۸: 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 ۸۰۲،۱۱، برخی نیازمندیهای یکتا را در این زمینه، تحمیل می دارد. همانند سایر LANها، ۸۰۲،۱۱ تمام تایید فریمهای خود را در پایان دریافت، انجام می دهد. اگرچه برخلاف اکثر LAN ها، ۸۰۲،۱۱ این کار را در لایه MAC خود مدیریت می کند و این درحالیست که سایر LANها این کار را در لایه های بالاتر انجام می دهد. دلیل این امر نیازمندیهای زمانی تحمیل شده در ۸۰۲،۱۱ می باشد. با زمان انتظارIFS به اندازه 50 µsec ، دریافت کننده باید یک تایید را در 10 µsec، پس از تایید CRC برای فریم، ارسال کند. با انجام تمام این توابع در 10 µsec پس 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:



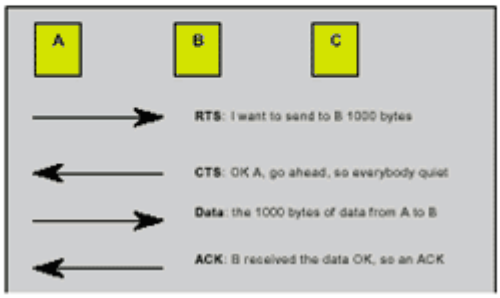
تصویر ۱۴-۲۹: نمودار کلی عملکرد تایید در ۸۰۲،۱۱

در بتدای بخش MAC، به تفاوتهای موجود در فیلدهای فریم ۸۰۲،۱۱، 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/از DS و استفاده از فریمهای ارسال/آماده جهت ارسال در ۸۰۲،۱۱ می باشد. فیلدهای به/از DS، مسیر فریم ارسال شده را مشخص می کند ، برخلاف اترنت که تنها آدرسهای MAC مبداء و مقصد بکار می رود. در سیستم CTS/RTS، C یک فریم RTS را به AP می فرستد، که به AP نشان می دهد که C آماده ارسال یک فریم می باشد. دراین فریم یک مقدار زمانی وجود دارد که نشانگر زمانی است که C جهت ارسال فریم داده خود ، به آن نیاز دارد. فیلدی که این داده را نگهداری می کند، فیلد طول می باشد.

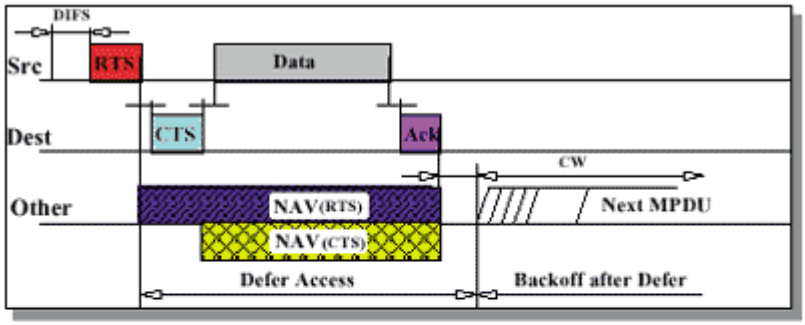
گره C می تواند پس از این به حالت انتظار برود. بلافاصله پس از خاتمه IFS و دوره بازیابی معکوس، AP یک فریم CTS برای C را Broadcast می کند که توسط همه ایستگاه های تحت پوشش AP دریافت می گردد. این فریم CTS همان مقدار زمانی موجود در فریم RTS را دارد. سایر ایستگاه های دریافت کننده این فریم، به اندازه مقدار زمان مشخص شده در فریم CTS، انتقالشان را متوقف می کند. زمانیکه C فریم CTS را دریافت می کند، شروع به انتقال داده می کند. اولین نمودار زیر این فرایند را به شیوه پایه، تشریح می کند و نمودار بعدی برخی جنبه های ساختار RTS/CTS ، ترکیب شده با رفتار بازیابی معکوس CSMA/CA، را نشان می دهد.

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



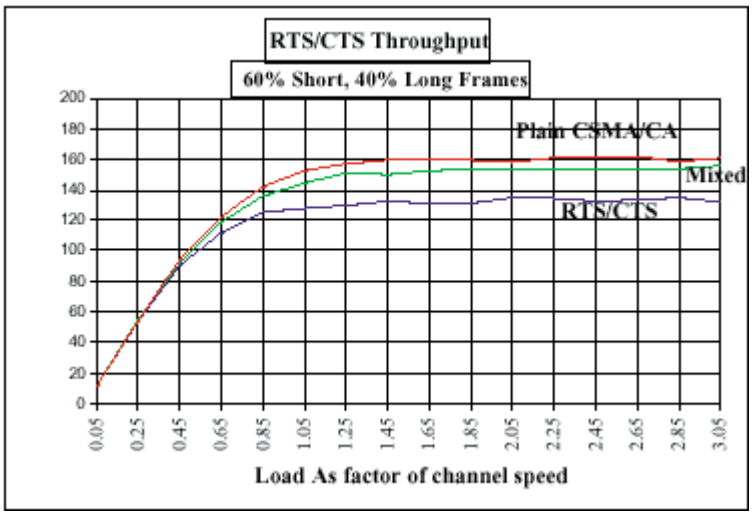
تصویر ۱۴-۳۰:انتقال داده CSMA/CA



- *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 ارسال داده با CTS/RTS و بازیابی معکوس CSMA/CA

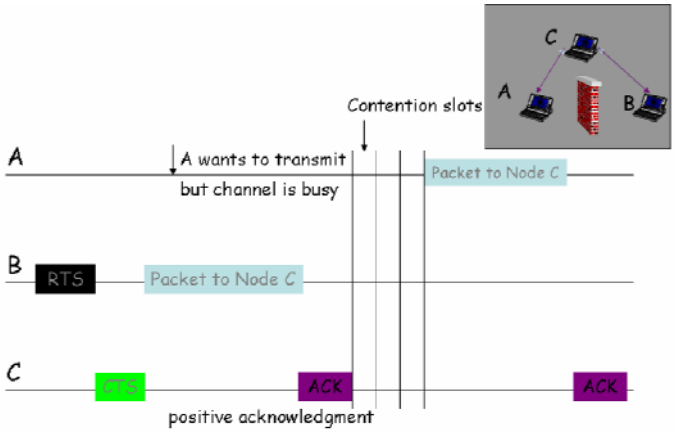
یکی دیگر از مزایای RTS/CTS، جلوگیری از تراکم می باشد که این موضوع باعث تحمیل سربار کمی به ۸۰۲،۱۱ می گردد. در مثال زیر، حتی در یک محیط خالص RTS/CTS، گذردهی در مقایسه با محیطهای بدون RST/CTS، تقریباً ۱۳٪ کاهش یافته است.



تصویر ۱۴-۳۲: مقایسه گذردهی ۸۰۲،۱۱ با/بدون RTS/CTS

تاثیر محدود RTS/CTS بر گذردهی، دربرابر توانایی کاهش تصادم آن، آن را بـه خصیـصه ای بـسیار جـذاب برای محصولات ۸۰۲،۱۱، تبدیل نموده است. باوجود آنکـه خصیـصه RTS/CTS یـک گزینـه اختیـاری در ۸۰۲،۱۱ می باشد ، جهت کاهش هزینه می توان از آن صرفه نظر نمود.

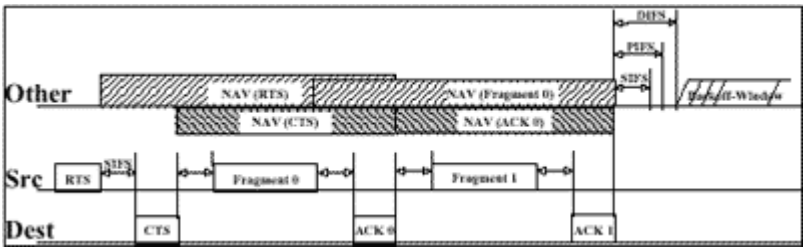
مثال: تصویر زیر نمونه یک محیط عملیاتی شبکه ۸۰۲،۱۱ است. در این تصویر A بدلیل مشغول بودن رسانه انتقال و کنترل آن توسط B، اجازه ارسال داده را ندارد. پس از پایان اتصال B به C، A مـی توانـد جهـت ارسـال داده خود به C اقدام نماید.



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 باشـد، کـه یـک تکنیـک بـرای شـرایط ارسـال ضـعیف 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 تلوزیون موبایل، مورد بحث قرار گیـرد. بـرای غلبـه بـر تـداخل، 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 تواند بسیار سریعتر انتقال و دریافت را انجام دهند. بعلاوه، 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 100 msec، به همه گره های موجود در دامنه خود، ارسال می نماید. در Beacon، داده هایی همچون TimeStampکنونی، 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.

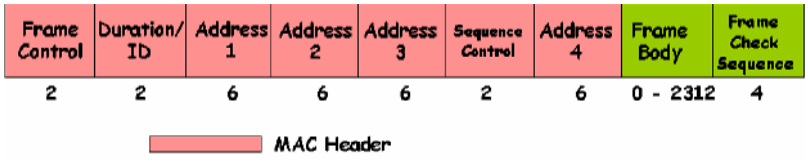
در حالت بالا و همچنین حالت سرگردانی، گره انتهایی ، نه AP، کیفیت ارتباط(QC) سیگنال AP را تعیین می نماید و از سطح QC جهت تعیین AP مناسب اتصال، استفاده می نماید. اگر CQ سیگنال یک AP متصل شده، به زیر حد معینی نزول نمود، که بوسیله تعدادی از فاکتورها همانند طراحی، کاربرد، سرعت و غیره، تعیین می گردد، به دلایلی همچون تداخل، قطع برق و یا سرگردانی گره، گره فعال، به دنبال یک AP جدید می گردد. زمانیکه AP جدید یافت شد، گره نهایی به وضعیت جدید، منتقل می شود و با AP جدید متحد 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 تحویل و تحولات و سرگردانی گره های نهایی، استفاده می نمایند.

این موضوع به ۸۰۲،۱۱ اجاز می دهد تا از آدرس MAC، برای تحویل 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:

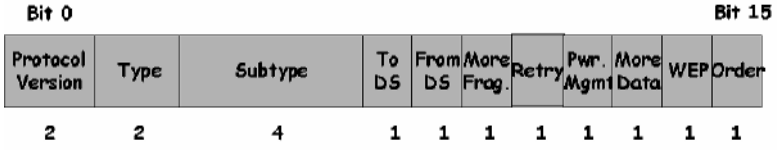
فریمهای MAC در ۸۰۲،۱۱ را می توان به سه دسته تقسیم نمود:

- فریمهای داده: بوسیله مسیر سرویس داده MAC ، مدیریت می گردند و حاوی داده های کاربر مـی باشد.



تصویر ۱۴-۳۵: ساختار فریم داده ۸۰۲،۱۱

- فیلد کنترل فریم: حاوی اطلاعات کنترلی ارسال شده بین ایـستگاه هـا مـی باشـد. ایـن فیلد، خود دارای ساختار زیر می باشد:

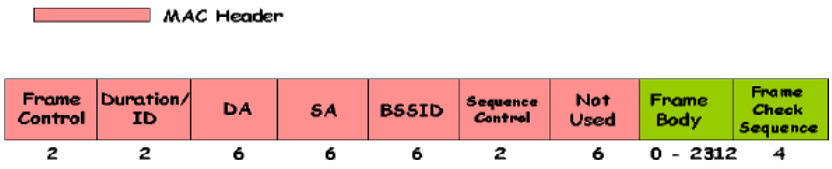


تصویر ۱۴-۳۶: ساختار فیلد کنترل فریم

  - 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 ادامـه 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 فریمهـا مـی باشد.

- دوره/ID: حاوی اطلاعات زمانی مورد نیاز جهت ارسال فریمهای بعدی است.
- آدرسهای ۱ تا ۴: آدرسهای خاص که متناسب با نوع فریم ارسـالی از آنهـا اسـتفاده مـی گردد.
- کنترل توالی: حاوی ۴ بیت شماره قطعه و ۱۲ بیت ، شماره توالی می باشد.
- کنترل توالی فریم: حاوی نتیجه CRC جهت تشخیص خطا، می باشد.

- فریم های مدیریتی: بوسیله مسیر داده سـرویس مـدیریت MAC، مـدیریت مـی شـود. در مـواردی همچون تایید اعتبار، درخواست و ... بکار می رود. این فریمها جهت برپاسازی و حفظ ارتبـاط بـین ایستگاه ها و AP ها، بکار می روند.

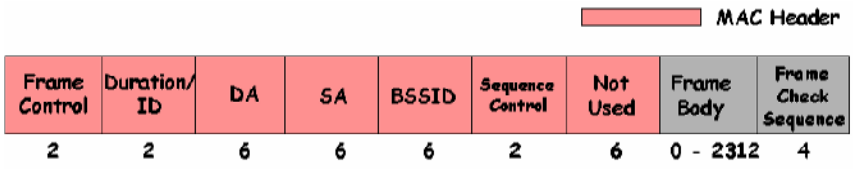


تصویر ۱۴-۳۷: ساختار فریم مدیریتی ۸۰۲،۱۱

انواع زیر نوع در این فریم ، بشرح زیر می باشد:

- وابستگی درخواست و پاسخ
- وابستگی مجدد درخواست و پاسخ
- بررسی درخواست و پاسخ
- Beacon
- ATIM [1]
- فسخ همکاری
- تایید و عدم تایید

- فریمهای کنترلی: RTS، CTS، ACK، سرکشی در وضعیت ذخیره توان. این فریمها، جهت کمک به تحویل فریمها، بکار می رود.



تصویر ۱۴-۳۸: ساختار فریم کنترلی ۸۰۲،۱۱

انواع زیر نوع در این فریم ، بشرح زیر می باشد:

- TRS
- CTS
- ACK
- PS Poll [2]
- CF End [3]
- CF End + CF-ACK

[1] Announcement Traffic Indication Message -

[2] Power-Save Poll -

[3] Contention-Free End -

بخش ۶:
امنیت در شبکه

فصل ۱۵: امنیت در شبکه

فصل ۱۵:

امنیت در شبکه

یک شبکه در معرض چهار نوع حمله قرار می گیرد:

۱-وقفه : باعث توقف کار شبکه می شود .

۲-استراق سمع

۳-دستکاری داده

۴-حمله از نوع افزودن اطلاعات

دونوع حمله داریم :

فعال : حمله ای که اختلال در کار شبکه ایجاد کند .

غیرفعال : حمله ای که اختلالی در کار شبکه ایجاد نمی کند و به تدریج داده ها را نابود می کند .

دیوار آتش[1] :

دیواری است که برای امنیت در شبکه بکار می رود . که در سر راه ارتباط شبکه با دنیای خارج قرار دارد . مثلاً بسته ها را پردازش کرده و اجازه عبور یا عدم عبور را به بسته می دهد . می تواند ردیابی کند . یکسری قوانین یا rol دارد که به دیوار آتش اعمال می شود . دیوار آتش هم می تواند به صورت لایه لایه طراحی شود (مثل شبکه) .

اگر در لایه شبکه باشد ، بسته های IP را پردازش می کند (سرآیند IP)

اگر در لایه انتقال و حمل ونقل باشد سرآیندهای بسته را سرویس می دهد (امکان دادن Ftp و ... را می توان کنترل کرد)

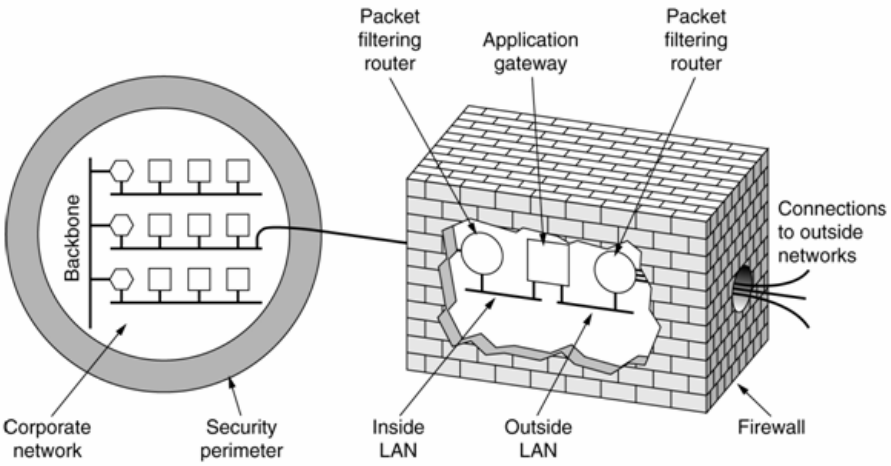
اگر در لایه کاربرد باشد باید به داده های داخل آن حساس باشد .

با استفاده از دیوار آتش می توانیم سرویسها را کنترل کنیم . اگر بخواهیم اجازه دسترسی به آدرسهای مختلف را ندهیم از دیوار آتش در لایه IP استفاده می کنیم .آدرس مبدأ و مقصد و ... را در IP بررسی می کند .

در لایه حمل و نقل جلوی بعضی از سرویسها را می گیریم مانند : FTP, Telnet و ...

در لایه کاربرد ،داده ها و محتوای آنها توسط دیوار آتش انجام می شود .

اعضای جانبی دیوار آتش :



A firewall consisting of two packet filters and an application gateway

[1] - Fire Wall

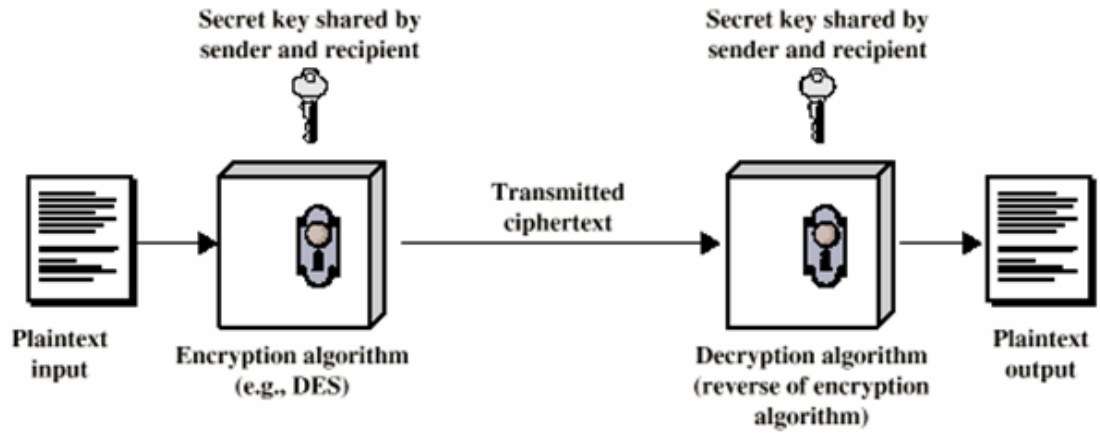
۱-سیستم رابط با کاربر : مدیر شبکه از طریق Interface مربوطه FireWall رولهای خاص را به شبکه اعمال می کند .

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 دیکر جـــــایگزین می شود . این روش می تواند یک جابجائی ساده باشد. امـا امروزه هر جدولی برای رمزگذاری در نظر گرفته شود به راحتی با برنامه های کامپیوتری آشکار می شود . روش این کـــار چنین است که از آنتروپی حروف لاتین استفـاده 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[1] : ترتیب قرار گرفتن حروف تغییر می کند مانند this که شود itsh .

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
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

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

۳-Data Eneviption Standard :

[1] permutation -

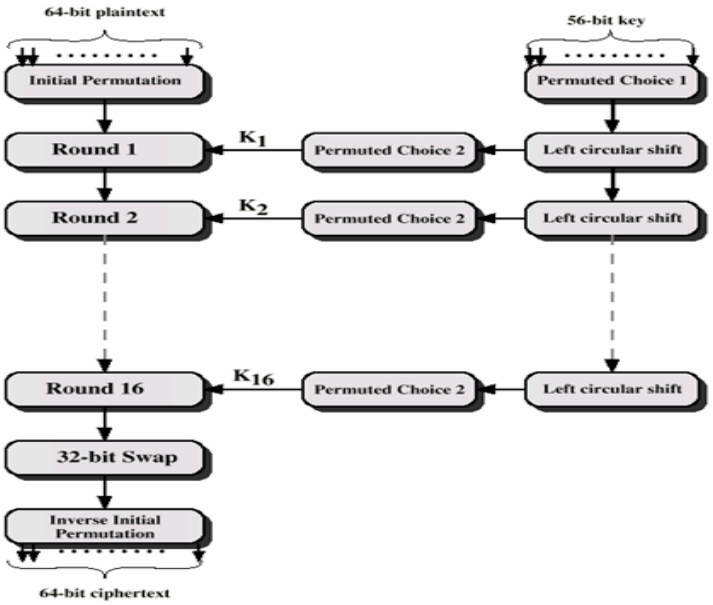
در ۱۶ مرحله عمل رمز نگاری انجام می شود یک کلید دارد که روی متن در هر مرحله اجرا مـی شـود و در هر مرحله توابع خاصی روی آن انجام می شود . توسط IBM در اوایل دهه ۷۰ ایجـاد شـد . ایـن رمـز نگـاری در دو حالت استفاده می شود :

۱-سیستمهای End – to –End (در لایه application)

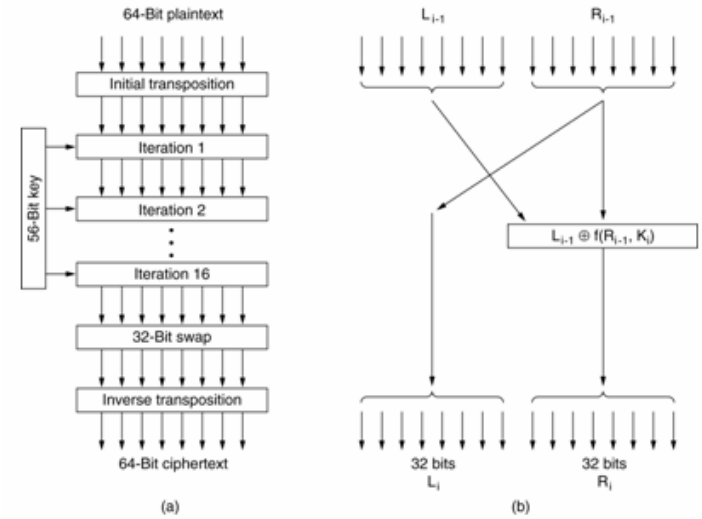
۲-روش پیوندی در نودها و مسیریابها عمل رمز نگاری و کشف آن انجام می شود .

الگوریتم DES [1] :

در اوایل دهه هفتاد توسط IBM توسعه یافت . اطلاعات بصورت بسته های ۶۴ بیتی در مـی آیـد و در ابتـدا یک جایگشت روی داده ها اعمال می شود .

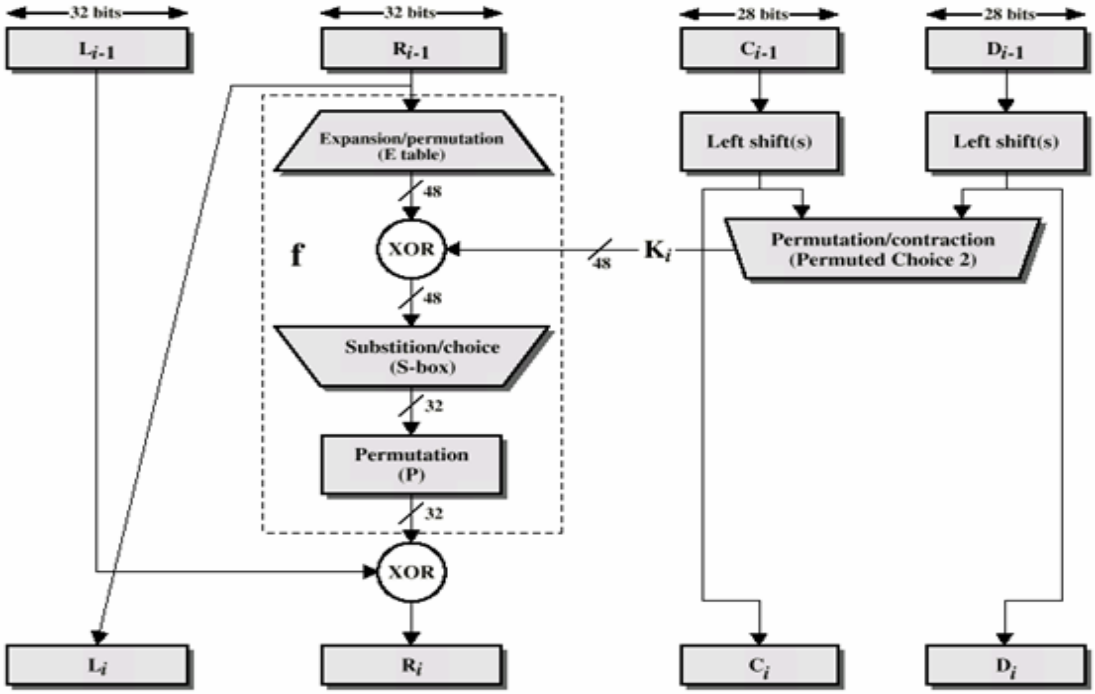


جزئیات تابع F : ابتدا رشته ۳۲ بیتی به یک دیتای ۴۸ بیتی تبدیل می شود . سپس عمـل XOR بـا کلیـد ۴۸ بیتی انجام می شود و نتیجه باید به ۳۲ بیت تبدیل شود . یک کلید ۵۶ بیتی داریم که در تمام مراحل ۱۶ کلیـد ۴۸ بیتی از روی آن ساخته می شود . البته در ابتدا نیز خود داده با داده رمزنگاری قبلی XOR می شود .



The Data encryption standard. (a) General outline.
(b) Detail of one iteration. The circled + means exclusive OR.

[1] - Data Eneryptum Standard



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 رمزگشائی همان مراحل تکرار می شود و کلیدهای بالا مشخص می شود . اشکال این روش این است که کلید بین رمزنگاری و رمزگشائی مشترک است .

رمزنگاری کلید عمومی (RSA) :

یک کلید برای رمزنگاری (عمومی) و یک کلید برای رمزگشائی (خصوصی).یعنی همه کلید رمزنگاری دارند ولی کلید رمز گشائی ندارند . البته کلید رمزگشائی از روی کلید رمزنگاری ساخته می شود و کار هر کسی نیست . در سال ۱۹۷۸ الگوریتم RAS بوجود آمد در ابتدا داده ها به عدد تبدیل می شوند.

Key Generation

Select p, q	p and q both prime
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d = e^{-1} \bmod \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

یک داده به صورت مقابل داریم

ID ES OF

MA RC HX

0803 0418

0779 1983

ابتدا داده ها را به قسمت های دو کاراکتری تقسیم می کنیم

0 طبق قرارداد هر کاراکتر را به عدد تبدیل می کنیم مـثلاً: A:01

B:01

C:02

در مرحله بعد یک هفت عدد انتخاب می شود : کلید عمومی (e,n)

کلید خصوصی (d,n)

ci = pi mod n رمزنگاری

pi = ci mod n و رمز گشائی

باید عددی مثل d پیدا کرد تا بتوان رمز گشائی را با آن انجـام داد . در روش RSA انتخـاب کلیـد عمـومی 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 کنبد که نسبت به z اول باشد .

د : بر اساس d عدد e به گونه ای انتخاب می شود که رابطه زیر برقرار باشد :

exd mod z = 1

مثال : فرض کنید که suzanne را بخواهیم رمز کنیم :

q,p را انتخاب می کنیم : q = 11 , p= 3

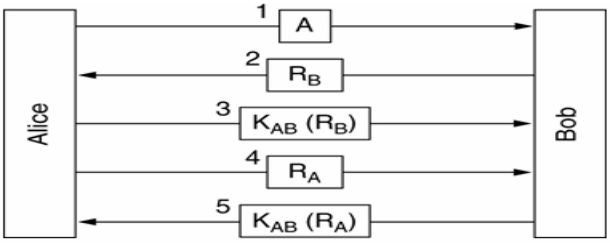
z = 20 , n = 33 : یک عدد اول که نسبت به z اول است انتخاب می شود: d = 7

و e را بدست می آوریم به گونه ای که 7 * e mod 20 = 1 : e = 3 یا e = 23

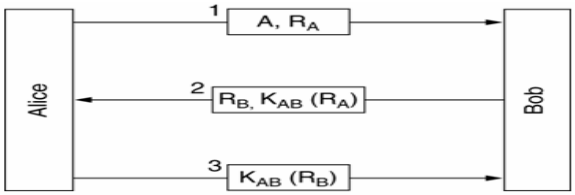
Plaintext (P)			Ciphertext (C)		After decryption	
Symbolic	Numeric	P^3	$P^3 \pmod{33}$	C^7	$C^7 \pmod{33}$	Symbolic
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E
		Sender's computation		Receiver's computation		

احراز هویت :

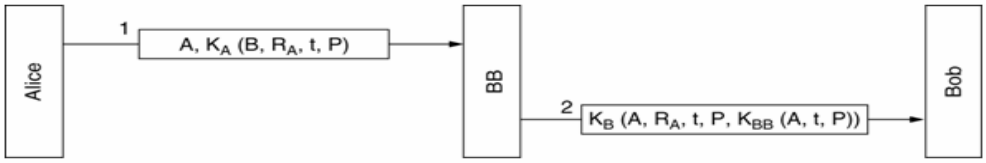
شکل روبرو مربوط به احراز هویت با استفاده از کلید مشترک می باشد .



عیب روش فوق این است که افشای 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 (CA[1])) که تمام شرکت کنندگان برای نگهداری و مدیریت کلیدها با CA توافق کرده اند . CA عهده دار انتشار ، ایجاد و امضاء گواهی ها و توزیع آنها می باشد .فیلدهای 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 : پیغام + الگوریتم Hash = Message digest

[1] - Certificate Authority

Message digest + senderprira tekey = Encrypted digest (ED)

گیرنده گواهی پیغام امضاء شده را چک می کند .

گیرنده: ED + Senderpmbdiekey = Recorer of message digest (I)

پیغام اولیه + Hash الگوریتم= 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