

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

شبکه های کامپیوتری

(Computer Networks)

تالیف :

دکتر محمد حسین یغمایی مقدم
دانشیار گروه مهندسی کامپیوتر
دانشگاه فردوسی مشهد

فصل اول

مفاهیم پایه شبکه های انتقال داده و شبکه های کامپیوتری

۱-۱- مقدمه ای بر شبکه های انتقال داده

در دنیای امروز، کامپیوترها در بسیاری از جنبه های زندگی انسان ها کاربرد پیدا کرده است. در مراکز تفریح از بازی های کامپیوتری که بسیار مورد علاقه جوانان است، استفاده می شود. در ادارات برای انجام امورتایپ و نامه نگاری، بایگانی پرونده ها و اطلاعات و ارائه سرویس اطلاع رسانی به مراجعه کنندگان از سیستم های کامپیوتری استفاده می گردد. در آژانس های مسافرتی برای رزرو و فروش بلیط پروازهای داخلی و خارجی و همچنین فروش بلیط قطار و اتوبوس از کامپیوترها استفاده می شود. در بیمارستان ها برای بایگانی و ضبط اطلاعات بیماران به طور وسیعی از سیستم های کامپیوتری استفاده می گردد. همچنین بسیاری از سیستم های پزشکی پیشرفته مثل دستگاه MRI^۱، دستگاه سونوگرافی و... از کامپیوتر استفاده می کنند. در مراکز صنعتی برای کنترل دستگاه های کارخانجات و افزایش بهره وری از کامپیوتر و ربات ها استفاده می گردد. دامنه استفاده از کامپیوترها آنقدر گسترش یافته است که امروزه اکثر خانه ها مجهز به حداقل یک کامپیوتر می باشند. یکی از موارد اصلی کاربرد کامپیوتر، دانشگاه ها و مراکز تحقیقاتی می باشد. در مراکز عملی پژوهشی، با استفاده از سیستم های کامپیوتری و نرم افزارها و سخت افزارهای مناسب، بسیاری از پروژه های تحقیقاتی انجام می شود. برای استفاده بهینه از اطلاعات موجود در کامپیوترها، لزوم تبادل داده ها بین آنها حس می گردد. یکی از ساده ترین روش های تبادل اطلاعات و جابجایی داده ها در کامپیوترها، استفاده از فلاپی دیسک، دیسک فشرد (CD^۲) و حافظه های USB^۳ می باشد. مسلماً استفاده از تجهیزات فوق در صورتی مناسب است، که اولاً حجم اطلاعات کم بوده و ثانیاً فاصله سیستم های کامپیوتری از یکدیگر زیاد نباشد. گسترش سیستم های کامپیوتری و افزایش حجم داده ها، متخصصین کامپیوتر را به فکر طراحی و پیاده سازی شبکه های انتقال داده انداخت. یکی از ساده ترین و اولین شبکه های انتقال داده، شبکه تلفن می باشد. با توجه به گستردگی و توسعه زیاد شبکه های تلفن، استفاده از آن برای تبادل داده های کامپیوتری بسیار مناسب است، به طوری که امروزه نیز از شبکه های تلفن به عنوان یک شبکه انتقال داده مناسب (برای سرعت های کم) استفاده می شود. افزایش میزان کامپیوترها در دنیا و حجم زیاد اطلاعات، باعث شد تا سیستم های انتقال داده جدید طراحی و پیاده سازی شود. به طور کلی در یک سیستم انتقال داده، باید سه مشخصه اصلی مد نظر باشد، این سه مشخصه عبارتند از: تحویل داده ها به مقصد درست و عدم اشتباه در تشخیص مقصد اصلی داده ها، حفظ صحت و درستی داده های تحویلی و تحویل به موقع داده ها با حداقل تأخیر به مقصد.

۱-۲- اجزای اصلی شبکه های انتقال داده

مطابق با شکل (۱-۱)، هر سیستم انتقال داده از چهار قسمت اصلی تشکیل شده است که عبارتند از:

- فرستنده و گیرنده
- داده های ارسالی

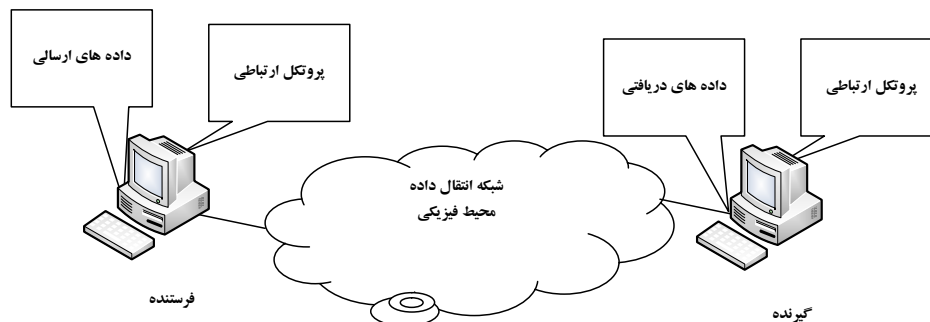
^۱ Magnitude Radiation Imaging

^۲ Compact Disk

^۳ Universal Serial Bus

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

- محیط فیزیکی برای تبادل داده ها
- پروتکل استفاده شده برای ارسال داده ها



شکل (۱-۱): اجزای یک سیستم انتقال داده

در یک شبکه انتقال داده، فرستنده با استفاده از تجهیزات ارسال، اقدام به تبدیل داده های ۱۰ و ۱ خام به سیگنال های الکتریکی یا نوری قابل ارسال در محیط فیزیکی می نماید. محیط های فیزیکی متعددی برای ارسال داده ها وجود دارند که در فصل دوم به بررسی آنها خواهیم پرداخت. در گیرنده نیز با استفاده از تجهیزات مناسب، سیگنال های دریافتی به صورت داده های اولیه تبدیل می شوند. برای مبادله صحیح داده ها بین فرستنده و گیرنده، هر دو باید از یک سری قوانین مشترک استفاده نمایند. این قوانین توسط پروتکل های ارتباطی مشخص می شود. هم فرستنده و هم گیرنده باید از پروتکل ارتباطی یکسانی برای ارسال و دریافت داده ها استفاده نمایند، در غیر این صورت تبادل داده ها میسر نمی باشد.

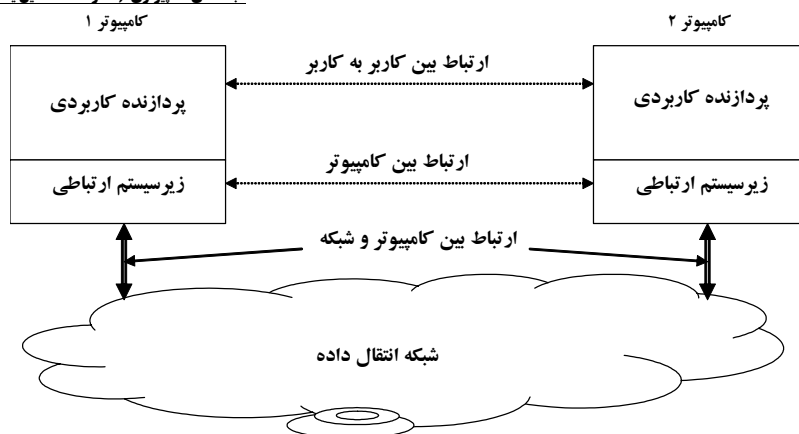
در شکل (۱-۲)، سه مورد از عملیات ارتباطی اصلی که باید در شبکه های انتقال داده در نظر گرفته شود، نشان داده شده است. هدف اصلی تمام شبکه های انتقال داده، فراهم سازی ارتباط لازم بین کاربران انتهایی شبکه می باشد. اما از آنجایی که فن آوری های مختلفی برای پیاده سازی شبکه های انتقال داده وجود دارد، ممکن است که کاربران انتهایی از زیرسیستم های مختلفی برای برقراری ارتباط با شبکه استفاده نمایند.

سه معیار اصلی در طراحی شبکه های انتقال داده وجود دارد که عبارتند از:

- عملکرد^۱
- قابلیت اطمینان^۲
- امنیت^۳

^۱ Performance
^۲ Reliability
^۳ Security

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۱-۲): مدل پایه یک سیستم انتقال داده

در شبکه های انتقال داده، موارد مختلفی برای ارزیابی عملکرد شبکه وجود دارد. برخی از این موارد عبارتند از:

- میزان تأخیر ارسال داده ها از مبدأ به مقصد
- میزان تغییرات تأخیر ارسال داده ها از مبدأ به مقصد
- میزان احتمال اتلاف داده های ارسالی از مبدأ به مقصد

عملکرد یک شبکه به عوامل متعددی بستگی دارد که به بررسی این عوامل می پردازیم. یکی از مهمترین عوامل تعیین کننده عملکرد یک شبکه انتقال داده، تعداد کاربران آن شبکه می باشد. از آنجایی که منابع موجود در شبکه محدود بوده و برای حجم مشخصی از ترافیک در نظر گرفته شده است، با افزایش تعداد کاربران شبکه، میزان ترافیک در شبکه نیز افزایش می یابد. افزایش ترافیک در شبکه باعث افزایش ازدحام و کاهش گذردهی شبکه می شود. یکی دیگر از عوامل عملکرد شبکه های انتقال داده، نوع محیط ارسال می باشد. در شبکه های انتقال داده محیط های ارسال متنوعی وجود دارد. مسلماً هر قدر محیط ارسال از سرعت بالا و کیفیت مطلوب تری برخوردار باشد، عملکرد شبکه افزایش می یابد. در فصل دوم، انواع محیط های ارسال در شبکه های انتقال داده بررسی خواهد شد. نوع سخت افزار و نرم افزار استفاده شده در کامپیوترهای شبکه انتقال داده نیز در میزان عملکرد شبکه دخالت دارد.

یکی دیگر از معیارهای انتخاب شبکه های انتقال داده، قابلیت اطمینان آن می باشد. فرکانس وقوع خطا، زمان بازیابی شبکه بعد از وقوع خطا و میزان مقاومت شبکه در برابر حوادث طبیعی نظیر سیل، رعدوبرق، آتش سوزی و زلزله، از موارد ارزیابی میزان اطمینان شبکه های انتقال داده می باشند.

امنیت، یکی دیگر از معیارهای انتخاب شبکه های انتقال داده است. دسترسی های غیرمجاز افراد به اطلاعات محرمانه شبکه و میزان مقاومت شبکه در مقابل نفوذ و ویروس از موارد ارزیابی امنیت شبکه های انتقال داده می باشد.

۳-۱- مراجع استاندارد گذاری شبکه های کامپیوتری

در ابتدای مطرح شدن شبکه های انتقال داده و شبکه های کامپیوتری، هر شرکت خصوصی از پروتکل های خاص خود استفاده می نمود. طبیعی بود که به علت عدم رعایت یک استاندارد مشخص، ارتباط بین شبکه های فوق و اتصال کاربران به آن به دلیل عدم برابری پروتکل های دو شبکه غیر ممکن بود. از این رو ایده های استفاده از استاندارد واحد در شبکه های کامپیوتری مطرح گردید. این کار نه تنها باعث امکان ارتباط و گسترش شبکه های کامپیوتری می شود، بلکه باعث رونق

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

محصولات مبتنی بر استاندارد در بازار کامپیوتر نیز می گردد. به طور کلی دو نوع استاندارد وجود دارد که عبارتند از استانداردهای اسمی^۱ و استانداردهای رسمی^۲. استانداردهای اسمی، استانداردهایی هستند که توسط شرکت های بزرگ کامپیوتری و مخابراتی برای گسترش محصولات خود وضع شده اند. در مقابل استانداردهای رسمی توسط مراجع بین المللی مورد تأیید و تصویب قرار گرفته است. طبیعی است به علت طولانی بودن نسبی تصویب استانداردها در مراجع بین المللی، معمولاً اکثر استانداردهای شبکه ابتدا به صورت اسمی می باشند و توسط شرکت های بزرگ ارائه می شوند و به تدریج با گسترش و کاربردی شدن استانداردهای مربوطه، تبدیل به استانداردهای رسمی می شوند. در ادامه به بررسی مهمترین مراجع استانداردگذاری در زمینه انتقال داده و شبکه های کامپیوتری می پردازیم.

۱-۳-۱ اتحادیه جهانی مخابرات (ITU^۳)

اتحادیه جهانی مخابرات موظف به تولید استانداردها و سرویس های مرتبط با ارتباطات و مخابرات می باشد. استانداردهای تولید شده این اتحادیه با عنوان توصیه نامه^۴ شناخته می شوند. در سال ۱۹۲۵ دو کمیته مشورتی به نام های CCIT و CCIF توسط اتحادیه جهانی مخابرات تعریف شدند. CCIF در رابطه با سرویس های تلفن و CCIT در زمینه سرویس های تلگراف فعال بودند. در سال ۱۹۵۶ این دو کمیته با یکدیگر ترکیب شده و کمیته مشورتی تلفن و تلگراف (CCITT^۵) ایجاد گردید. CCITT دارای اعضای مختلفی شامل: شرکت های تلگراف و تلفن کشورها، شرکت های خصوصی، سازمان های علمی و صنعتی، سایر سازمان های بین المللی دیگر و اعضای که رشته اصلی آنها چیز دیگری می باشد؛ ولی علاقه مند به فعالیت های CCITT هستند، می باشد. در بین این پنج نوع عضو، فقط شرکت های پست و تلگراف و تلفن کشورها حق رأی دارند. CCITT موظف به ارائه توصیه نامه هایی در زمینه شبکه تلفن و تجهیزات ارتباط داده می باشد. توصیه نامه های CCITT بعد از مدتی به صورت استانداردهای شناخته شده جهانی در می آیند. نمونه ای از استانداردهای CCITT می توان به V.24 و V.35, X.25, X.21, ... اشاره نمود. اتحادیه جهانی مخابرات در شهر ژنو سوئیس مستقر می باشد.

۱-۳-۲ سازمان جهانی استاندارد (ISO^۶)

این سازمان بین المللی در ۲۳ فوریه سال ۱۹۴۷ تأسیس گردید و اعضای آن سازمان های استاندارد ملی کشورهای مختلف می باشند. محل این سازمان در شهر ژنو سوئیس می باشد. این سازمان غیر دولتی بوده و ۱۵۷ کشور عضو آن می باشند. این سازمان دارای سه نوع عضویت مختلف می باشد که عبارتند از: اعضای بدنه سازمان^۷، اعضای وابسته^۸ و اعضای مشترک^۹. اعضای بدنه سازمان که تنها اعضای دارای حق رأی می باشند، معمولاً موسسات استاندارد هر کشور بوده که موظف به ارائه استاندارد در کشور می باشند. اعضای وابسته شامل کشورهایی هستند که دارای موسسات استاندارد کشوری نمی باشند. این اعضا فقط نسبت به استانداردهای ISO آگاهی پیدا کرده و در جریان تولید این استانداردها مشارکت ندارند. اعضای مشترک، مربوط به کشورهایی با اقتصاد کوچک می باشند که حق عضویت ناچیزی پرداخت کرده و فقط توسعه

^۱ By fact

^۲ By law

^۳ International Telecommunication Union

^۴ Recommendation

^۵ International Telegraph and Telephone Consultative Committee

^۶ International Standard Organization

^۷ Member bodies

^۸ Correspondent members

^۹ Subscriber members

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

استانداردهای ISO را پیگیری می کنند. اعضای اصلی این سازمان عبارتند از: ANSI از آمریکا، BSI از انگلیس، AFNOR از فرانسه و DIN از آلمان. توسط سازمان جهانی استاندارد، در زمینه های مختلفی استاندارد وضع شده است. این سازمان حدود ۲۰۰ کمیته فنی دارد که هریک موظف به یک زمینه خاصی می باشند. به عنوان مثال کمیته فنی شماره (۱) در زمینه استانداردسازی گام دنده پیچ و مهره ها فعال است و کمیته فنی شماره (۹۷) در زمینه کامپیوتر و پردازش اطلاعات کار می نماید. البته با توجه به گستردگی موضوعات هر کمیته فنی، معمولاً در هر کمیته چندین گروه کاری فعال در غالب زیرکمیته ها وجود دارد که کارهای مختلف بین آنها تقسیم می شود.

۱-۳-۳- انجمن مهندسان برق و الکترونیک (IEEE^۱)

انجمن مهندسان برق و الکترونیک یکی از بزرگترین سازمان های حرفه ای در سطح دنیا می باشد. این انجمن دارای حدود ۳۶۰ هزار عضو از ۱۷۵ کشور مختلف جهان می باشد. این انجمن در شهر نیویورک آمریکا ثبت شده است. این انجمن علاوه بر انتشارات بسیار زیادی که در زمینه های مختلف کامپیوتر و برق دارد. هر ساله چندین کنفرانس بین المللی در زمینه های مختلف مرتبط با فعالیت های خود برگزار می نماید. کنفرانس ها و مجلات انجمن مهندسان برق و الکترونیک از اعتبار و اهمیت بسیار زیادی در دنیا برخوردار می باشد. گروه کاری ۸۰۲ از انجمن مهندسان برق و الکترونیک در زمینه شبکه های محلی فعال می باشد.

۱-۴- شبکه های کامپیوتری

قرن حاضر، قرن ارتباطات نام دارد. با پیدایش کامپیوتر و فن آوری های ارتباطات، بسیاری از مشکلات زندگی انسان ها رفع شده است. شبکه های کامپیوتری که از اتصال چندین کامپیوتر در نقاط مختلف به وجود می آیند، نقش بسیار مهمی در انتقال اطلاعات و نزدیکی انسان ها به یکدیگر داشته اند. با استفاده از امکانات شبکه های کامپیوتری و اینترنت، امکان استفاده از سرویس زیادی نظیر: تبادل اطلاعات، ارسال نامه های الکترونیکی، انتقال فایل، کنفرانس های صوتی و تصویری، آموزش از راه دور، تبادل داده های تجاری و غیره فراهم شده است. شبکه های کامپیوتری جهت استفاده مشترک از منابع و برقراری ارتباط بین کاربران به وجود می آیند. در این بخش به ذکر مقدمات اولیه شبکه های کامپیوتری و معرفی مفاهیم اولیه و پایه ای آن می پردازیم.

۱-۴-۱- اهداف و مزایای شبکه های کامپیوتری

در اتصال کامپیوترها و ایجاد شبکه های کامپیوتری، اهداف زیر مدنظر می باشد:

- **به اشتراک گذاری منابع^۲:** یکی از مزایای عمده شبکه های کامپیوتری تقسیم منابع می باشد. در یک شبکه کامپیوتری، کلیه کاربران شبکه در صورتی که مجاز به استفاده از شبکه باشند، می توانند به منابع موجود در شبکه نظیر برنامه های کاربردی، بانک های اطلاعاتی و تجهیزات سخت افزاری نظیر چاپگر، مودم و غیره دسترسی پیدا نمایند.
- **قابلیت اطمینان بالا^۳:** یکی از مشکلات استفاده انفرادی از کامپیوترها این است که چنانچه بر روی یک کامپیوتر نرم افزار یا سخت افزار مهمی نصب شده باشد، اگر به هر دلیلی برای آن سیستم مشکلی پیش آید در این صورت کلیه اطلاعات و منابع موجود در آن غیر قابل دسترسی می باشد. به عبارت دیگر قابلیت اطمینان یک کامپیوتر به تنهایی

^۱ Institute of Electrical and Electronics Engineer

^۲ Resource sharing

^۳ High reliability

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

پایین است و این امر به خصوص در کاربردهای مهم نظیر کنترل و هدایت سیستم های نظامی پیشرفته نظیر هواپیما، موشک و غیره مشکل زا است. یکی از روش های افزایش قابلیت اطمینان، استفاده از شبکه های کامپیوتری و سیستم های توزیع شده می باشد. در این حالت منابع مهم بر روی چندین ایستگاه شبکه نصب می شوند تا در صورت خرابی یکی از سیستم ها، بتوان از طریق سایر ایستگاه های شبکه به منابع دسترسی پیدا نمود.

- **صرفه جویی مالی:** استفاده از شبکه های کامپیوتری، باعث صرفه جویی مالی نیز می شود. هرچند نصب و راه اندازی شبکه های کامپیوتری خود نیاز به هزینه و امکانات نرم افزاری و سخت افزاری خاص خود دارد، ولی در کل می توان به این نتیجه رسید که شبکه های کامپیوتری باعث صرفه جویی در هزینه ها می گردند. به عنوان مثال چنانچه در یک اداره، چندین کارمند به یک نرم افزار خاص نیاز داشته باشند، می توان به جای آن که برای تک تک آنها نرم افزار مربوطه را خریداری و نصب و راه اندازی نمود، یک نسخه از آن را تهیه کرد و در شبکه نصب کرد (به شرط آن که نرم افزار قابلیت نصب در شبکه را داشته باشد). در این حالت چندین کاربر می توانند به طور همزمان به شبکه متصل شوند و از امکانات آن نرم افزار بهره ببرند. همچنین به عنوان مثال دیگر می توان در شبکه، یک چاپگر نصب و راه اندازی نمود. در این حالت کاربران قادرند با استفاده از امکانات شبکه، از چاپگر به طور مشترک استفاده نمایند، که طبیعی است این امر باعث صرفه جویی در خرید چندین چاپگر برای کاربران شبکه می گردد.

- **ایجاد ارتباط بین مردم:** یکی دیگر از اهداف و مزایای عمده شبکه های کامپیوتری، ایجاد ارتباط بین مردم می باشد. این مسئله با گسترش سریع اینترنت و سرویس متنوع آن به خوبی مشاهده می شود. به عنوان مثال با کمک سرویس پست الکترونیکی^۱، کاربران مختلف در سطح شبکه اینترنت که ممکن است در فواصل بسیار دوری از هم قرار داشته باشند، قادر به ارسال نامه های الکترونیکی به یکدیگر می باشند. همچنین با استفاده از امکانات شبکه اینترنت، افراد مختلف می توانند در گروه های خبری و مباحثه ای گوناگون شرکت کرده و با استفاده از امکانات شبکه به مباحثه و تبادل نظر با یکدیگر بپردازند.

۱-۴-۲- انواع شبکه های کامپیوتری

از نظر وسعت، می توان شبکه های کامپیوتری را به سه نوع مختلف تقسیم بندی نمود که عبارتند از:

- **شبکه های محلی (LAN^۲):** این نوع شبکه ها دارای وسعت بسیار کمی می باشند و معمولاً در سطح یک ساختمان نظیر یک اداره کوچک و دانشکده های مختلف یک دانشگاه نصب و راه اندازی می شوند. شبکه های محلی جهت اشتراک منابع سخت افزاری (مثل چاپگر) و منابع نرم افزاری (مثل برنامه های کاربردی و بانک های اطلاعاتی)، بین کامپیوترهای شخصی و یا ایستگاه های کاری^۳ استفاده می شوند. در شبکه های محلی یکی از کامپیوترهای شبکه که معمولاً از سرعت بالا و حجم حافظه زیادی برخوردار است؛ به عنوان سرویس دهنده^۴ شبکه استفاده می شود. نرم افزارها و داده های لازم در سرویس دهنده شبکه ذخیره سازی می شود و سایر ایستگاه های شبکه که مشتری^۵ نام دارند، قادر به استفاده از آنها می باشند. سرعت انتقال اطلاعات در شبکه های محلی بسیار بالا می باشد. نوپذیری اطلاعات و احتمال

^۱ Electronic mail (E-mail)

^۲ Local Area Network

^۳ Workstations

^۴ Server

^۵ Client

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

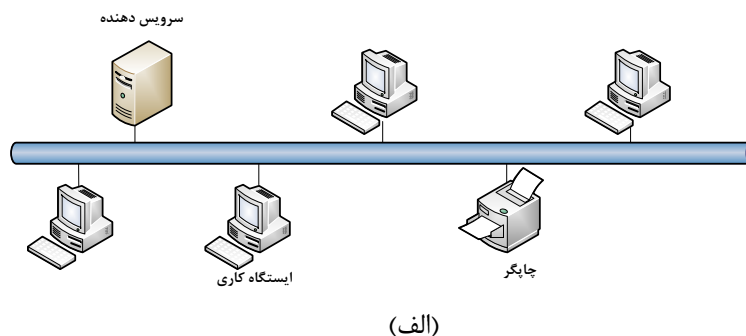
اتلاف داده ها در شبکه های محلی بسیار پایین است. شبکه های محلی معمولاً دارای تملک خصوصی می باشند. شبکه های اترنت، حلقه نشانه^۱ و گذرگاه نشانه^۲ مثال هایی از این نوع شبکه ها می باشند.

• **شبکه های شهری (MAN^۳)** : همانطوری که از نام این شبکه ها معلوم می شود، شبکه های شهری از نظر گستردگی در سطح یک شهر می باشند. از شبکه های شهری می توان برای اتصال شبکه های کوچکتر محلی به یکدیگر استفاده نمود. همچنین شبکه های انفرادی مثل شبکه تلویزیون کابلی که در سطح شهر گستردگی دارد نیز از این نوع شبکه ها می باشد. چنانچه شرکتی دارای چندین شعبه در سطح شهر باشد، با استفاده از امکانات شبکه های شهری، قادر به اتصال شبکه های محلی خود به یکدیگر است. شبکه های شهری می توانند به هر دو صورت خصوصی و یا عمومی اداره و مدیریت شوند. به عنوان مثال شبکه های DQDB^۴ و SMDS^۵ از نوع شبکه های شهری می باشند.

• **شبکه های گسترده (WAN^۶)** : این نوع شبکه ها دارای وسعت بسیار زیادی (در سطح یک کشور و یا حتی کل جهان) می باشند. به عنوان مثال شبکه های ملی هر کشور و یا شبکه جهانی اینترنت و شبکه تلفن، نمونه هایی از شبکه های گسترده هستند. برخلاف شبکه های محلی که به سخت افزار خاصی وابسته می باشند، در شبکه های گسترده امکان استفاده از تجهیزات متفاوتی که در فواصل طولانی به یکدیگر متصل شده اند، وجود دارد. شبکه های گسترده ای که توسط یک شرکت مدیریت و مورد استفاده قرار می گیرند، شبکه های enterprise نامیده می شوند. برخی از استانداردهای شبکه های گسترده عبارتند از: ATM, ISDN, MPLS^۷ و X.25. در شکل (۱-۳)، انواع شبکه های کامپیوتری شامل شبکه های محلی، شبکه های شهری و شبکه های گسترده نشان داده شده است.

۱-۴-۳ - ساختار شبکه های کامپیوتری

در شکل (۱-۴)، ساختار کلی شبکه های کامپیوتری نشان داده شده است. همانطور که در شکل دیده می شود، شبکه های کامپیوتری از دو قسمت اصلی تشکیل شده اند که عبارتند از زیر شبکه^۸ و کامپیوترهای میزبان^۹.



^۱ Token ring

^۲ Token bus

^۳ Metropolitan Area Network

^۴ Distributed Queue Dual Bus

^۵ Switched Multi-megabit Data Services

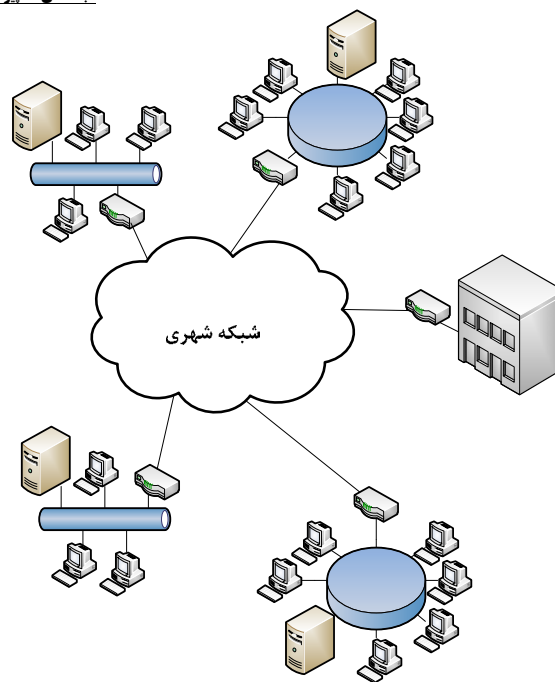
^۶ Wide Area Network

^۷ Multi-Protocol Label Switching

^۸ Subnet

^۹ Host

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



(ب)

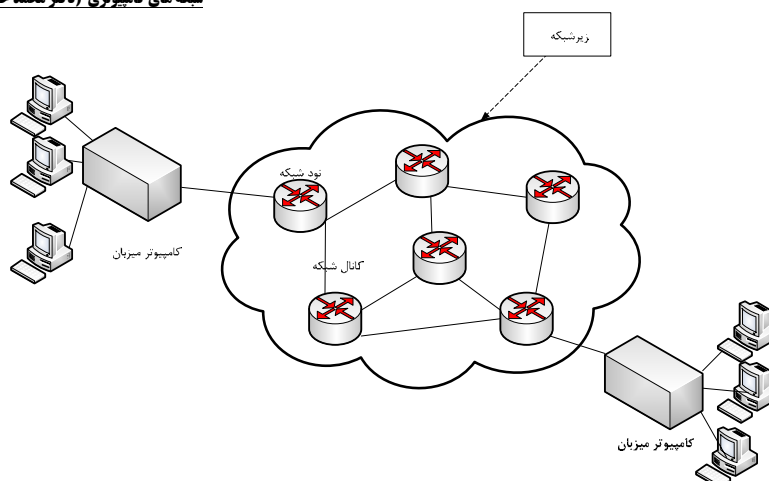


(ج)

شکل (۱-۳): انواع شبکه های کامپیوتری الف) شبکه محلی ب) شبکه شهری ج) شبکه گسترده

وظیفه اصلی زیرشبکه، انتقال و هدایت پیام ها و اطلاعات کاربران از مبدأ به مقصد می باشد. کاربران شبکه از طریق کامپیوترهای میزبان اطلاعات ارسالی خود را به زیرشبکه می فرستند و زیرشبکه نیز اطلاعات دریافتی را به سمت مقصد هدایت و مسیریابی می نماید.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۴-۱) : ساختار شبکه های کامپیوتری

زیر شبکه خود نیز از دو قسمت تشکیل می شود که عبارتند از: خطوط انتقال^۱ و نودهای شبکه. نودهای شبکه با نام های مرکز سوئیچ و IMP^۲ نیز شناخته می شوند. هر بسته ارسالی کامپیوترهای میزبان، بعد از ورود به زیر شبکه تحویل نودهای شبکه می شود و در آن جا منتظر می ماند تا عملیات سوئیچینگ یا مسیریابی بر روی آن انجام شود و کانال خروجی مناسب آن پیدا گردد. سپس از طریق کانال خروجی تحویل نود یا کامپیوتر میزبان بعدی می شود. به این دلیل در اصطلاح گفته می شود که شبکه های کامپیوتری به صورت "ذخیره و هدایت پیشرو"^۳ عمل می کنند.

در شبکه های کامپیوتری دو نوع کانال شبکه موجود است که عبارتند از:

- کانال های نقطه به نقطه^۴
- کانال های پخشی^۵

در شکل (۵-۱) این دو نوع کانال نشان داده شده است. همان طور که از شکل مشهود است، در کانال های نقطه به نقطه یک مسیر اختصاصی بین دو نقطه انتهایی وجود دارد. از کانال های نقطه به نقطه، فقط دواستگاهی که در انتهای کانال به آن متصل هستند، می توانند استفاده نمایند.

^۱ Channel

^۲ Interface Message Processor

^۳ Store and forward

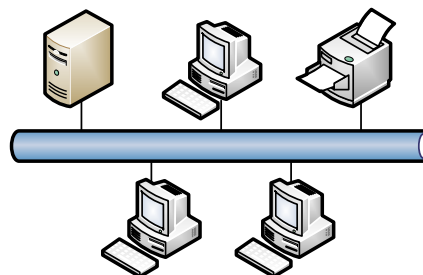
^۴ Point to point

^۵ Broadcast

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)



(الف)



(ب)

شکل (۱-۵): دو نوع مختلف کانال های شبکه (الف) کانال های نقطه به نقطه
(ب) کانال های پخش

در کانال های پخش، تمام کامپیوترهای متصل به کانال از یک مسیر مشترک برای ارسال و دریافت اطلاعات استفاده می نمایند. از آنجایی که در کانال های پخش تمام ایستگاه ها از طریق یک کانال مشترک اقدام به ارسال و دریافت بسته ها می کنند، این احتمال وجود دارد که بسته های ارسالی ایستگاه های مختلف با یکدیگر تداخل نموده و از بین بروند. بنابراین یکی از مهمترین مشکلات کانال های پخش، تصادم^۱ بسته ها می باشد.

در شبکه های کامپیوتری، نحوه اتصال کامپیوترها به یکدیگر از طریق کانال های انتقال، توپولوژی شبکه نامیده می شود. به طور کلی هفت نوع توپولوژی شبکه وجود دارد که عبارتند از:

- ستاره ای^۲
- حلقه^۳
- درخت^۴
- کامل^۵
- حلقه های متقاطع^۶
- نامنظم
- گذرگاه مشترک^۷

در شکل های (۱-۶) الی (۱۱-۱) توپولوژی های مختلف شبکه نشان داده شده است.

^۱ Collision

^۲ Star

^۳ Ring

^۴ Tree

^۵ Complete

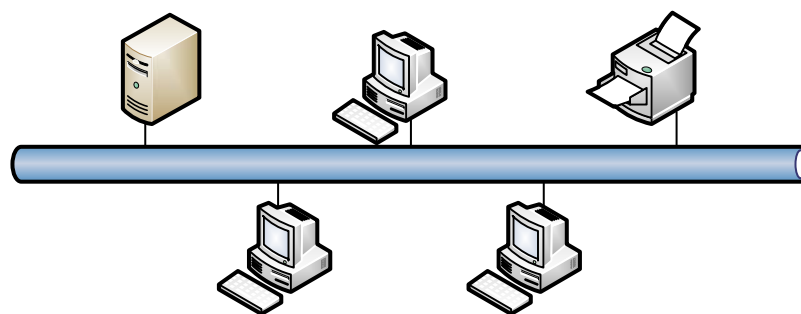
^۶ Interesting ring

^۷ Bus

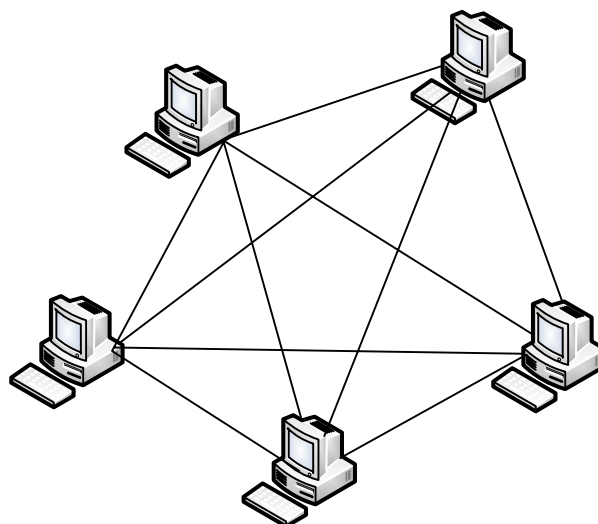
شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

همان طور که اشاره شد، یکی از مهمترین مشکلات و مسائلی که در کانال های پخششی وجود دارد، امکان تداخل اطلاعات ارسالی توسط ایستگاه های مختلف شبکه با یکدیگر می باشد. از آنجایی که در کانال های پخششی از یک محیط مشترک برای ارسال اطلاعات چندین کامپیوتر استفاده می شود (که این خود یک مزیت عمده کانال های پخششی است؛ زیرا تعداد کانال های مورد نیاز کاهش می یابد و باعث صرفه جویی مالی می شود). بنابراین باید کانال به طور مناسب در اختیار کاربران قرار داده شود. دو روش عمده تخصیص کانال به کاربران وجود دارد که عبارتند از: تخصیص کانال به صورت ایستا^۱ و تخصیص کانال به صورت پویا^۲.

در روش تخصیص کانال به صورت ایستا، از روش تقسیم زمانی استفاده می شود. به این ترتیب که زمان به برش های ثابتی تقسیم بندی می شود و هر ایستگاه اجازه دسترسی به کانال را در یک برش زمانی خاص دارد. هر برش زمانی به یک ایستگاه اختصاص دارد و سایر ایستگاه ها اجازه ارسال اطلاعات را ندارند، که این امر باعث عدم وجود تداخل می شود. یکی از مهمترین مشکلات تخصیص کانال به صورت ایستا این است که چنانچه ایستگاهی در یک برش زمانی اطلاعاتی برای ارسال نداشته باشد، در این صورت در آن برش زمانی کانال خالی می ماند و از ظرفیت آن به طور بهینه استفاده نمی شود. همچنین چنانچه تعداد ایستگاه ها زیاد باشد، زمان انتظار برای دستیابی به کانال برای هر ایستگاه نیز زیاد خواهد بود.



شکل (۱-۶): توپولوژی گذرگاه مشترک

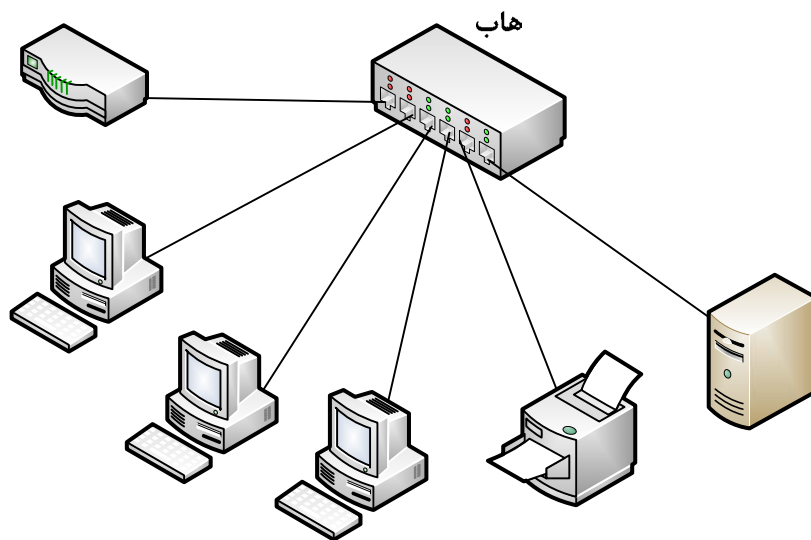


شکل (۱-۷): توپولوژی کامل

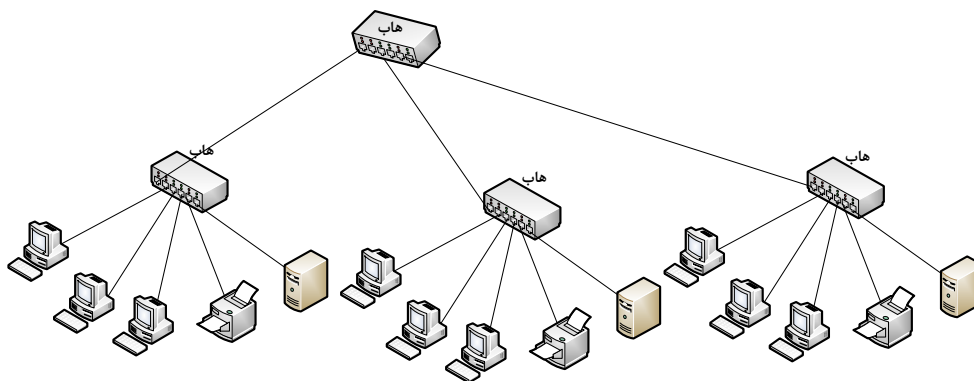
^۱ Static channel allocation

^۲ Dynamic channel allocation

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

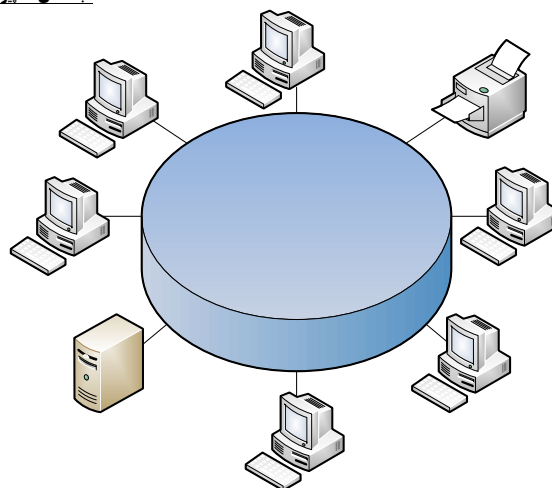


شکل (۸-۱): توپولوژی ستاره ای

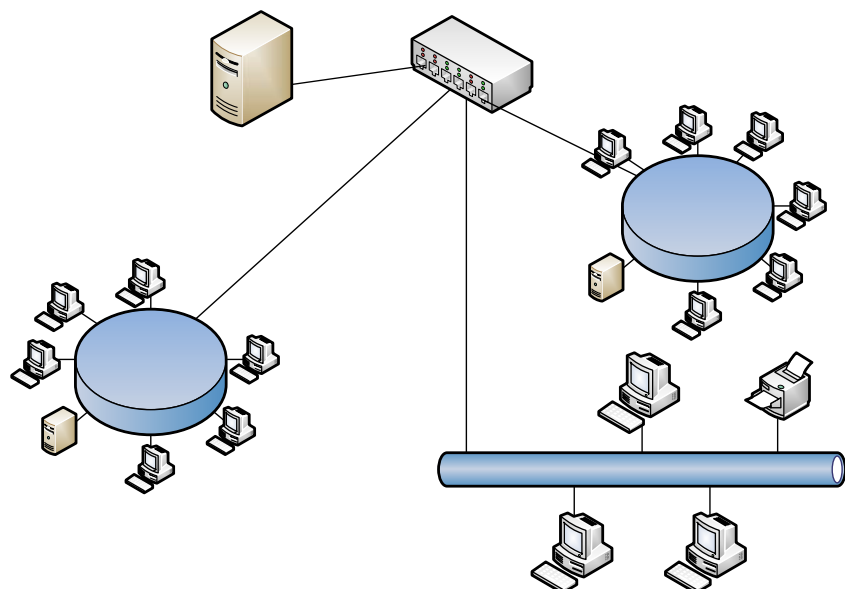


شکل (۹-۱): توپولوژی درخت

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۱-۱۰): توپولوژی حلقه



شکل (۱-۱۱): توپولوژی ترکیبی

روش تخصیص کانال به صورت پویا، خود به دو نوع تقسیم می شود که عبارتند از: تخصیص کانال به صورت مرکزی و تخصیص کانال به صورت غیرمرکزی. در روش تخصیص کانال به صورت مرکزی، یک ایستگاه مرکزی در شبکه وجود دارد که موظف به تصمیم گیری در مورد ارسال یا عدم ارسال سایر ایستگاه های شبکه می باشد. هر ایستگاه شبکه قبل از ارسال اطلاعات، ابتدا باید مجوز ارسال را از ایستگاه مرکزی دریافت دارد و بعد از آن که مجوز ارسال را دریافت نمود، قادر به ارسال اطلاعات می باشد. در روش غیرمرکزی، ایستگاه مرکزی در شبکه موجود نیست، بلکه خود ایستگاه ها در مورد ارسال یا عدم ارسال خود تصمیم گیری می نمایند. امروزه اکثر شبکه های محلی از کانال های پخش و تخصیص کانال به صورت پویا استفاده می کنند.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

۴-۴-۱ - ساختار لایه ای و معماری شبکه^۱

در شبکه های کامپیوتری جهت برقراری ارتباط و تبادل اطلاعات بین دو کامپیوتر میزبان، یک سری عملیات باید انجام شود. جهت کاهش پیچیدگی شبکه و افزایش انعطاف پذیری آن در مقابل تغییرات احتمالی، عملیات یک شبکه به صورت لایه های مختلفی تقسیم بندی می گردد. به طوری که هر لایه بر روی لایه دیگری قرار دارد و با آن در ارتباط است. هر لایه شبکه وظایف خاص خود را به عهده دارد و از لایه های دیگر مستقل می باشد. در مدل لایه ای شبکه، هر لایه از سرویس لایه پایین تر خود استفاده می نماید که به لایه بالاتر خود سرویس می دهد. هر لایه شبکه برای انجام وظایف خود از یک سری قواعد و قراردادهای استاندارد استفاده می نماید که به آن پروتکل گفته می شود. یک شبکه کامپیوتری ممکن است از چندین لایه برای انجام عملیات و وظایف خود استفاده نماید. به مرز بین دو لایه مجاور، واسط^۲ گفته می شود. تبادل اطلاعات بین لایه های مجاور از طریق واسطه های لایه ها انجام می گردد. در مدل لایه ای شبکه، کاربران شبکه از طریق بالاترین لایه شبکه، از سرویس و امکانات شبکه استفاده می نمایند. اطلاعات ایجاد شده در بالاترین لایه شبکه، برای ارسال به شبکه و تحویل به مقصد، باید از لایه های مختلف شبکه عبور نماید تا به پایین ترین لایه برسد و از طریق محیط فیزیکی وارد زیر شبکه گردد. در شکل (۱-۱۲) مثالی از مدل لایه ای شبکه آورده شده است.



شکل (۱-۱۲): مثالی از مدل لایه ای شبکه

مجموع لایه ها و پروتکل های یک شبکه را معماری شبکه می گویند. با استفاده از مشخصات و اطلاعات موجود از معماری یک شبکه می توان نرم افزارها و سخت افزارهای هر لایه را طراحی و تولید نمود. برای درک بهتر مدل لایه ای شبکه به یک مثال توجه نمایید. فرض کنید که مدیران عامل دو شرکت بین المللی می خواهند با یکدیگر ارتباط برقرار نمایند. چنانچه این دو مدیرعامل به زبان های یکدیگر آشنا نباشند، هر یک باید یک مترجم استخدام نماید. مترجمان نیز از طریق امکانات مخابراتی پیام و سخنان خود را به اطلاع یکدیگر می رسانند. در این حالت یک مدیرعامل متن پیام خود را به مترجم خود تحویل می دهد. مترجم نیز با استفاده از امکانات مخابراتی پیام را برای مترجم مقابل خود ارسال می دارد. در آن جا، مترجم متن پیام را به زبان اصلی برمی گرداند و تحویل مدیرعامل می دهد. طبیعی است در مثال اخیر دو مدیرعامل (بالاترین لایه) نمی توانند به طور مستقیم اطلاعات و پیام خود را ارسال دارند، بلکه باید از طریق مترجم و امکانات مخابراتی (لایه های پایین تر) این کار را انجام دهند. در ساختار لایه ای با مسائل و مشکلات مختلفی روبرو هستیم که در زیر به ذکر هر یک از این مسائل و روش حل آنها می پردازیم:

^۱ Network architecture
^۲ Interface

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

۱. **نیاز به مکانیسمی برای برقراری و قطع ارتباط:** از آنجایی که در یک شبکه کامپیوتری تعداد زیادی کامپیوتر موجود می باشد که هر یک نیز می تواند شامل چندین فرآیند مختلف در حال اجرا باشد، بنابراین هر لایه شبکه برای برقراری و قطع ارتباط با لایه متناظر خود در طرف مقابل باید مجهز به مکانیسم های خاصی باشد. برای این کار نیاز به نوعی آدرس دهی برای تعیین فرآیند طرف مقابل می باشد.
۲. **عدم تطابق سرعت لایه های فرستنده و گیرنده:** در یک مدل لایه ای شبکه این امکان وجود دارد که دو لایه متناظر با سرعت یکسان اطلاعات را برای یکدیگر ارسال نمایند. در این حالت چنانچه فرستنده با سرعتی به مراتب بیشتر از سرعت گیرنده اطلاعات را ارسال کند، امکان از بین رفتن اطلاعات وجود دارد. استفاده از بافر میانی و فیدبک ارسالی بین مبدأ و مقصد تا حدی مشکل فوق را حل می کند.
۳. **محدودیت اندازه بسته ها:** یکی دیگر از مشکلات موجود در مدل لایه ای این است که بسته های ارسالی هر لایه دارای حداکثر طول معینی می باشند. بنابراین هنگام ارسال بسته های یک لایه به لایه پایین تر، چنانچه حداکثر طول بسته های لایه پایین تر از طول بسته های دریافتی لایه بالا کمتر باشد، در این صورت امکان ارسال چنین بسته هایی وجود ندارد. یکی از روش های حل این مشکل، تکه سازی^۱ بسته ها به بسته های کوچکتر است. در گیرنده نیز بسته های تکه تکه شده بازسازی می گردند و بسته اولیه استخراج می شود.
۴. **وقوع خطا در بسته های دریافتی:** از آنجایی که بسته های ارسالی یک لایه در نهایت وارد زیر شبکه شده و از طریق کانال های مخابراتی به سمت مقصد ارسال می شوند، این امکان وجود دارد که ضمن ارسال بسته ها، خطاهایی در آنها اتفاق بیفتد. برای تشخیص و در صورت امکان تصحیح این خطاها باید چاره ای اندیشیده شود. یکی از روش های متداول، استفاده از مکانیسم های کنترل خطا می باشد. در این مکانیسم ها لایه فرستنده به اطلاعات ارسالی یک سری اطلاعات اضافه الحاق می نماید. لایه گیرنده با پردازش بر روی اطلاعات دریافتی، متوجه وقوع خطای احتمالی در اطلاعات می شود.
۵. **عدم رعایت ترتیب بسته ها:** چنانچه بین کامپیوتر میزبان مبدأ و مقصد چندین مسیر مختلف موجود باشد، در این صورت این امکان وجود دارد که بسته های ارسالی از مسیرهای مختلف به مقصد فرستاده شوند. از آنجایی که مسیرهای ارسالی بسته ها، الزاماً با یکدیگر یکسان نمی باشند، بنابراین ممکن است که بسته های ارسالی در مقصد به ترتیب دریافت نشوند. برای رفع این مشکل از شماره بسته^۲ استفاده می گردد. هر بسته ارسالی دارای یک شماره منحصر به فرد می باشد که به ترتیب ارسال بسته ها این شماره نیز یک واحد افزایش می یابد. در سمت گیرنده با بررسی شماره بسته، رعایت یا عدم رعایت ترتیب بسته ها مشخص می شود. در مدل لایه ای برای تعیین تعداد لایه ها باید نکات زیر را در نظر داشت:
 - یک لایه هنگامی ایجاد می شود که نیاز به سطح جدیدی از جداسازی عملیات داشته باشیم.
 - هر لایه، عملیات مشخص و تعریف شده ای را انجام می دهد.
 - عملیات هر لایه توسط پروتکل های استاندارد بین المللی مشخص می شود.
 - مرز بین لایه ها باید طوری انتخاب شود که جریان عبور اطلاعات از نقاط واسط حداقل گردد.
 - تعداد لایه ها باید به اندازه کافی بزرگ باشد که بتوان بین عملیات لایه ها تفاوت گذاشت. از طرف دیگر تعداد لایه ها نباید بیش از حد زیاد باشد که باعث پیچیدگی ساختار و معماری شبکه گردد.

۱-۴-۵- مدل مرجع OSI

^۱ Fragmentation

^۲ Sequence number

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

در سال ۱۹۸۳ از سوی سازمان جهانی استاندارد مدل مرجع OSI ارائه گردید. این مدل برای اتصال سیستم های باز به یکدیگر ارائه شده است. یک سیستم باز در حقیقت مجموعه ای از پروتکل هایی می باشد که امکان اتصال دو سیستم مختلف به یکدیگر را صرف نظر از معماری لایه های پایینی آنها فراهم می آورد. با استفاده از مدل مرجع OSI امکان اتصال سیستم های مختلف و برقراری ارتباط بین آنها بدون نیاز به اعمال تغییرات در منطق سخت افزار و نرم افزار پایینی آنها وجود دارد. مدل مرجع OSI به تنهایی یک پروتکل نمی باشد، بلکه یک مدل مرجع برای فهم بهتر طراحی یک معماری انعطاف پذیر برای شبکه های کامپیوتری است. این مدل دارای ۷ لایه می باشد که در شکل (۱-۱۳) نشان داده شده است. مطابق با شکل فوق در مدل لایه ای OSI لایه های زیر موجود می باشند:

۱-۴-۵-۱- لایه فیزیکی

وظیفه اصلی این لایه، ارسال بیت های خام ۰ و ۱ بر روی کانال ارتباطی شبکه می باشد. تعیین سطوح ولتاژ برای بیت های ۰ و ۱، از وظایف دیگر این لایه است. این لایه داده های دریافتی از لایه بالاتر خود را به صورت قابل حمل در کانال ارتباطی شبکه تبدیل می نماید و آنها را ارسال می دارد.

لایه کاربرد	لایه هفتم
لایه ارائه	لایه ششم
لایه جلسه	لایه پنجم
لایه حمل	لایه چهارم
لایه شبکه	لایه سوم
لایه پیوند داده	لایه دوم
لایه فیزیکی	لایه اول

شکل (۱-۱۳): مدل لایه ای OSI

در لایه فیزیکی مسائل مختلفی مطرح می باشد که عبارتند از :

- **ساختار کانال های اتصال:** همان طور که قبلاً نیز به آن اشاره گردید، کانال های ارتباطی در شبکه دارای دو نوع نقطه به نقطه و پخش می باشند.
- **ارسال داده ها در کانال:** برای ارسال داده ها بین دو سیستم کامپیوتری، سه روش ارسال وجود دارد که عبارتند از:
 - ارسال کاملاً یک طرفه^۱: در این نوع ارسال، یک طرف ارتباط همواره فرستنده و طرف دیگر همواره گیرنده می باشد.

^۱ Simplex

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

- ارسال یک طرفه^۱: در این نوع ارسال، در هر لحظه فقط یکی از دو سیستم کامپیوتری قادر به ارسال می باشند. به عبارت دیگر در هر لحظه از زمان، یک طرف ارتباط فرستنده و طرف مقابل گیرنده می باشد. البته برخلاف روش کاملاً یک طرفه، هر دو طرف ارتباط قادر به ارسال و دریافت اطلاعات می باشند (ولی در زمان های متفاوت).
- ارسال دو طرفه^۲: در این نوع ارسال، هر دو طرف ارتباط در هر لحظه توأم با هم قادر به ارسال و دریافت اطلاعات می باشند.

- **توپولوژی:** همان طور که قبلاً اشاره گردید، نحوه اتصال ایستگاه های شبکه به یکدیگر، توپولوژی شبکه نامیده می شود.
- **نوع سیگنال:** در لایه فیزیکی برای ارسال داده های منطقی ۰ و ۱، از دو نوع سیگنال آنالوگ و دیجیتال استفاده می شود. همچنین نحوه کدگذاری و تبدیل داده های ۰ و ۱ منطقی به سیگنال های مناسب، در این لایه مشخص می شود.
- **واسط ارتباطی:** در لایه فیزیکی نوع واسط ارتباطی که برای اتصال ایستگاه های شبکه به محیط ارسال استفاده می شود، مشخص می گردد.
- **محیط ارسال:** برای ارسال داده های ۰ و ۱ منطقی، به صورت سیگنال های مناسب در شبکه، محیط های ارسال متعددی وجود دارند که در فصل ۲ توصیف می شوند.

در این لایه استانداردهایی نظیر: CCITT V.24, EIA RS232, CCITT V.33, CCITT V.21, CCITT V.24 وجود دارد.

۱-۴-۵-۲- لایه پیوند داده^۳

در این لایه، اطلاعات ارسالی در قالب قاب هایی با طول مشخص ارسال می شوند. این قاب ها به ترتیب پشت سر یکدیگر ارسال می گردند. معمولاً گیرنده نیز با دریافت هر قاب، یک پیام گواهی مثبت یا منفی که نشان دهنده دریافت صحیح و یا دریافت نادرست قاب می باشد، به فرستنده ارسال می دارد. چنانچه پیام های گواهی مثبت یا منفی در بین راه گم شوند، این لایه باید قادر به رفع مشکلات احتمالی باشد. وظایف اصلی این لایه عبارتند از:

- کنترل خطا و اطمینان از دریافت صحیح قاب، از وظایف اصلی این لایه می باشد.
- چنانچه فرستنده با سرعت بیشتر از آنچه گیرنده قادر به دریافت است، ارسال نماید در این صورت بافر گیرنده به سرعت پر می شود و اطلاعات از بین می رود. لایه پیوند داده با استفاده از عملیات کنترل جریان قادر به تنظیم سرعت ارسال فرستنده با سرعت دریافت گیرنده می باشد. باید توجه داشت که عملیات کنترل خطا و کنترل جریان در لایه دوم، کانال به کانال انجام می شوند.
- در کانال های پخشی که چندین ایستگاه به طور مشترک از کانال استفاده می نمایند، برای جلوگیری از تداخل بسته ها با یکدیگر باید از مکانیسم های مناسبی در لایه پیوند داده استفاده نمود.

^۱ Half-duplex

^۲ Full-duplex

^۳ Data link layer

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

- در لایه پیوند داده هر ایستگاه، دارای یک آدرس منحصر به فرد می باشد که به آدرس فیزیکی مشهور است. از آنجائی که ایستگاه های مختلف در شبکه دارای آدرس فیزیکی متفاوت از یکدیگر می باشند، امکان ارسال و دریافت قاب ها بین آنها وجود دارد.
 - در لایه پیوند داده، اطلاعات ارسالی به صورت قاب های متوالی بین فرستنده و گیرنده مبادله می شود. یکی از مسائل مهم در این لایه تشخیص شروع و پایان هر قاب می باشد. بدین منظور از بایتهای خاصی در سرآیند^۱ و دنباله^۲ هر قاب استفاده می گردد.
- پروتکل هایی نظیر HDLC^۳ و SDLC^۴ مثال هایی از استانداردهای لایه دوم می باشند.

۱-۴-۵-۳- لایه شبکه^۵

لایه شبکه موظف به کنترل زیر شبکه می باشد. هنگامی که یک بسته اطلاعاتی از کامپیوتر میزبان مبدأ به کامپیوتر میزبان مقصد ارسال می شود، لایه شبکه موظف به مسیریابی^۶ و هدایت صحیح بسته درون زیر شبکه می باشد. چنانچه به طور ناگهانی تمام کاربران شبکه اقدام به ارسال بسته به درون زیر شبکه نمایند در این صورت شبکه با ازدحام^۷ روبرو می شود. ایجاد ازدحام در شبکه باعث کاهش کارایی و کیفیت سرویس می شود که امری نامطلوب است. کنترل ازدحام و رفع آن از وظایف اصلی لایه شبکه است. ارتباط بین شبکه ای^۸ یکی دیگر از وظایف لایه شبکه می باشد. هنگامی که بسته های ارسالی کاربران در راه رسیدن به مقصد از شبکه های میانی دیگری عبور نمایند، مشکلات و مسائل زیادی در ورود بسته به شبکه جدید به وجود می آید. برخی از این مشکلات عبارتند از: عدم تطابق نحوه آدرس دهی دوشبکه، عدم یکسان بودن اندازه بسته های دو شبکه و یا عدم تطابق پروتکل های دو شبکه. رفع مشکلات فوق و فراهم آوردن سرویس لازم برای اتصال شبکه ها به یکدیگر، از وظایف لایه شبکه است.

آدرس دهی منطقی، تبدیل آدرس های منطقی به آدرس های فیزیکی و تسهیم سازی کانال که به کمک آن امکان استفاده مشترک همزمان چندین وسیله از کانال فراهم می آید، از دیگر وظایف لایه سوم می باشد.

۱-۴-۵-۴- لایه حمل^۹

این لایه، بسته های لایه بالاتر را دریافت می دارد و آنها را در صورت لزوم به قطعات کوچکتری تقسیم می نماید و به لایه شبکه ارسال می کند. لایه حمل برای سرویس دهی به لایه جلسه، موظف به برقراری اتصال های مختلف با مقصد می باشد. عملکرد این لایه به صورت انتها به انتها است. این مطلب به این معنی می باشد که اتصال های موجود در لایه حمل

^۱ Header

^۲ Trailer

^۳ High level Data Link Control

^۴ Synchronous Data Link Control

^۵ Network layer

^۶ Routing

^۷ Congestion

^۸ Internetworking

^۹ Transport layer

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

فقط بین کامپیوترهای میزبان انتهایی ایجاد می شوند. برخلاف لایه شبکه که موظف به تحویل تک تک بسته های ارسالی به مقصد می باشد، لایه حمل موظف به تحویل سالم و بدون خطای کل پیام ارسالی به لایه همتای خود در مقصد است. از آنجائی که اکثر کامپیوترهای شبکه قادر به اجرای همزمان چندین نرم افزار مختلف می باشند، تحویل صحیح بسته ها از مبدأ به مقصد تنها به معنی سالم رساندن بسته ها به کامپیوتر مقصد نمی باشد، بلکه بسته هر نرم افزار اجرایی در سمت مبدأ باید به همان نرم افزار متناظر خود در سمت مقصد برسد. برای انجام این کار، لایه حمل در شبکه های کامپیوتری از آدرس خاصی به نام آدرس درگاه^۱ استفاده می نماید. لایه شبکه با استفاده از آدرس منطقی بسته ها، آنها را به کامپیوتر مقصد می رساند. در سمت مقصد، لایه حمل با استفاده از آدرس سوکت، هر بسته را به نرم افزار مربوط به آن تحویل می دهد. لایه حمل برای نیل به امنیت بیشتر در تبادل داده ها، اقدام به برقراری اتصال بین دو درگاه مبدأ و مقصد موجود در کامپیوترهای مبدأ و مقصد می نماید. هر اتصال درحقیقت یک مسیر منطقی می باشد که بین کامپیوترهای مبدأ و مقصد برای تبادل داده ها برقرار می شود. ایجاد هر اتصال در لایه حمل در طی سه مرحله انجام می شود که عبارتند از: برقراری اتصال، ارسال داده و قطع اتصال. با استفاده از مسیر منطقی ایجاد شده توسط هر اتصال، لایه حمل قادر به انجام عملیات مرتب سازی بسته ها، کنترل جریان و تشخیص و تصحیح خطا می باشد.

۱-۴-۵-۵- لایه جلسه^۲

با کمک امکانات این لایه، کاربران مختلف شبکه که بر روی کامپیوترهای میزبان متفاوتی قرار دارند، قادر به برقراری جلسه بین یکدیگر می باشند. ورود به یک کامپیوتر از راه دور و انتقال فایل بین دو ماشین شبکه، مثال هایی از جلسات این لایه می باشند. مدیریت نشانه^۳ از سایر وظایف این لایه به شمار می آید. چنانچه در برخی از پروتکل ها خواهیم که دو طرف جلسه همزمان اقدام به شروع به کار نمایند، در این صورت برای مدیریت این کار، لایه جلسه نشانه هایی بین دو کامپیوتر مبدأ و مقصد مبادله می نماید. کامپیوتری که این نشانه را در اختیار دارد قادر به انجام عملیات حساس مشخص شده می باشد.

یکی دیگر از وظایف این لایه، همزمانی است. برای درک بحث همزمانی، به ذکر یک مثال می پردازیم. فرض کنید که در حال ارسال یک فایل بسیار پر حجم از یک کامپیوتر به کامپیوتر دیگری می باشیم. چنانچه در حین ارسال ارتباط قطع شود، باید انتقال اطلاعات دوباره از سر گرفته شود. برای رفع این مشکل، لایه جلسه با کمک امکانات همزمانی قادر می باشد که در صورت قطع ارتباط فقط از همان نقطه قطع قبلی، دوباره اطلاعات را ارسال کند.

۱-۴-۵-۶- لایه ارائه^۴

یکی از وظایف لایه ارائه، تبدیل کدها به یکدیگر می باشد. چنانچه دو کامپیوتر که از کدهای متفاوتی برای ثبت و نمایش اطلاعات استفاده می نمایند (مانند کدهای ASCII^۵ و یا EBCDIC^۶) بخواهند با یکدیگر ارتباط برقرار کنند، با استفاده از امکانات لایه ارائه تبدیل کدها به یکدیگر انجام می شود. سایر وظایف این لایه عبارتست از:

^۱Port address

^۲Session layer

^۳Token management

^۴Presentation layer

^۵American Standard Code for Information Interchange

^۶Extended BCD Information Code

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

- رمزنگاری^۱: در این لایه برای افزایش امنیت در ارسال داده ها (به خصوص در کاربردهایی نظیر تجارت الکترونیکی) از روش های رمزنگاری استفاده می شود.
- فشرده سازی: برای کاهش زمان ارسال داده ها، و استفاده کارآمدتر از شبکه، از روش های فشرده سازی در این لایه استفاده می شود.
- امنیت: یکی دیگر از وظایف این لایه، تأمین امنیت ارتباط از طریق ایجاد شناسه کاربر و کلمه رمز عبور می باشد.

۱-۴-۵-۷- لایه کاربرد^۲

کاربران شبکه از طریق امکانات و پروتکل های این لایه قادر به استفاده از سرویس شبکه می باشند. در لایه کاربرد، نرم افزارهای کاربردی متنوع نظیر پست الکترونیکی، انتقال فایل، اتصال از راه دور به یک ماشین وغیره در اختیار کاربران قرار می گیرد. یکی دیگر از وظایف لایه کاربرد، ایجاد ترمینال مجازی^۳ است. ترمینال مجازی درحقیقت نسخه نرم افزاری ترمینال فیزیکی می باشد. بااستفاده از ترمینال مجازی، امکان اتصال به کامپیوتر میزبان راه دور فراهم می آید. بدین منظور برنامه کاربردی اقدام به ایجاد یک نسخه نرم افزاری از ترمینال کامپیوتر میزبان می کند.

۱-۴-۶- روند ارسال و دریافت اطلاعات در مدل OSI

در مدل لایه ای شبکه، اطلاعات ارسالی کاربر در بالاترین لایه ایجاد می شود و به ترتیب از لایه های شبکه عبور می کند تا وارد لایه فیزیکی گردد و از آنجا وارد شبکه می شود. در مدل لایه ای، هر لایه شبکه دارای وظایف خاصی می باشد که برای انجام وظایف خود به بسته های دریافتی از لایه بالاتر یک سری اطلاعات سرآیند اضافه می نماید و بسته ایجادشده را تحویل لایه پایین تر از خود می دهد. لایه پایین تر نیز این عمل را تکرار می نماید و به بسته دریافتی از لایه بالاتر خود، سرآیند اضافه می کند و آن را تحویل لایه پایین تر می دهد. البته در بعضی از لایه ها به خصوص در لایه دوم، علاوه بر سرآیند ممکن است که یک سری اطلاعات دنباله نیز به آخر بسته ها اضافه شود.

بنابراین با عبور بسته ها از لایه های مختلف شبکه، هر لایه برای انجام وظایف خود، یک سری اطلاعات به بسته ها اضافه می نماید که باعث افزایش طول بسته می شود. در پایین ترین لایه یعنی لایه فیزیکی، بسته های دریافتی بیت به بیت ارسال می شوند تا اینکه با عبور از شبکه و مسیریابی تحویل مقصد شوند. درسمت مقصد، بسته دریافتی از پایین ترین لایه تحویل لایه های بالاتر می شود. هر لایه موظف به پردازش برروی سرآیند ایجادشده توسط لایه متناظر در مبدأ می باشد. هر لایه در مقصد سرآیند یا دنباله ایجاد شده توسط مبدأ را حذف نموده و سپس بسته را تحویل لایه بالاتر خود می دهد. این عملیات درتمام لایه ها انجام می شود و هرلایه درمقصد درست همان سرآیندهایی را که لایه متناظر در مبدأ ایجاد کرده است جهت استفاده خود برمی دارد و آن را حذف می نماید تا این که داده های خالص تحویل بالاترین لایه شوند و کاربر قادر به استفاده از آنها می شود.

در شکل (۱-۱۴) مراحل ارسال و دریافت بسته ها در یک شبکه مبتنی بر مدل لایه ای OSI نشان داده شده است. در مدل OSI به سه لایه پایینی (فیزیکی، پیوند داده و شبکه) لایه های شبکه گفته می شود. همچنین چهار لایه بالایی (حمل، جلسه، ارائه و کاربرد)، لایه های کاربر نامیده می شوند. نودهای میانی شبکه تنها حداکثر تا لایه سوم را دارا می باشند،

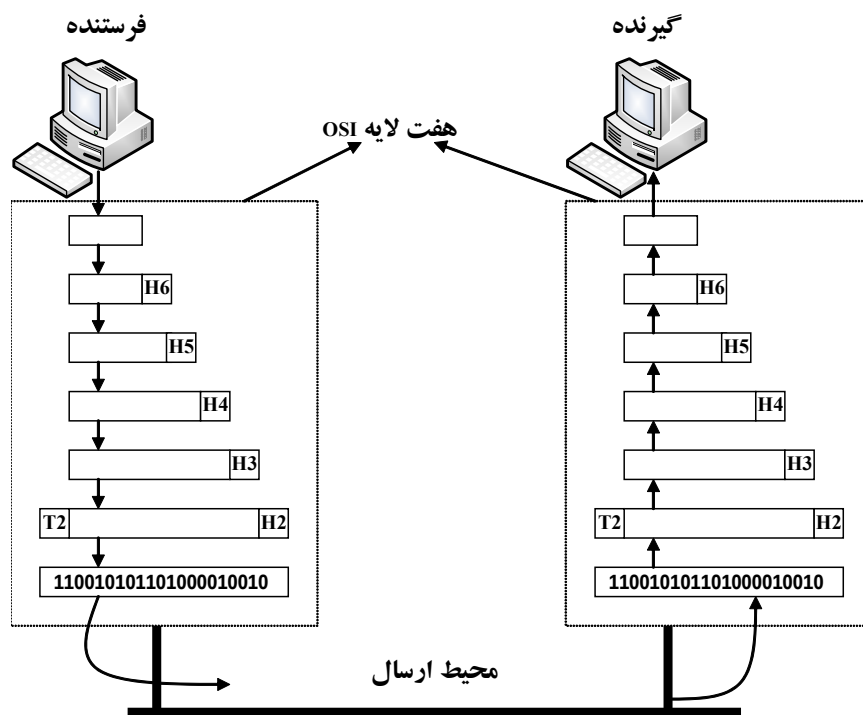
^۱ Encryption

^۲ Application layer

^۳ Virtual terminal

شبکه های کامپیوتری (دکتر محمد حسن یغمایی مقدم - دانشگاه فردوسی مشهد^۱)

ولی کامپیوترهای میزبان تمام هفت لایه را شامل می شوند. بسته های ارسالی هر لایه که شامل داده های لایه بالاتر و اطلاعات سرآیند همان لایه می باشند، در اصطلاح واحد داده ای پروتکل (^۱PDU) نام دارند.



شکل (۱-۱۴): مراحل ارسال و دریافت بسته ها در مدل مرجع OSI

همان طور که قبلاً اشاره شد، در مدل OSI هر لایه شبکه باید به لایه بالاتر از خود سرویس بدهد. هر لایه برای ارائه سرویس خود به لایه بالاتر، از عناصر فعال خود که موجودیت^۲ نام دارند استفاده می نماید. یک موجودیت در یک لایه شبکه می تواند یک فرآیند نرم افزاری و یا یک واحد سخت افزاری باشد. در هر دو سمت فرستنده و گیرنده و در هر لایه، موجودیت های متناظر وجود دارند که در اصطلاح به آنها موجودیت های همتا^۳ گفته می شود. سرویسی را که لایه N به لایه بالاتر از خود (لایه N+1) ارائه می دهد بوسیله موجودیت های آن لایه انجام می شود.

سرویس ارائه شده لایه از طریق نقاط دسترسی به سرویس (^۴SAP) در اختیار لایه بالاتر قرار می گیرد. هر نقطه دسترسی به سرویس در مدل لایه ای دارای آدرس مشخص و معینی می باشد. به عنوان مثال در یک شبکه تلفن، نقاط دسترسی به سرویس همان پریزهای تلفن است که از طریق اتصال تلفن به پریز امکان استفاده از سرویس شبکه تلفن برای کاربران فراهم می شود. شماره تلفن نیز آدرس نقطه دسترسی به سرویس تلفن می باشد. در سیستم عامل یونیکس، نقاط دسترسی به سرویس، سوکت می باشند و آدرس نقاط دسترسی به سرویس همان شماره سوکت ها هستند.

^۱ Protocol Data Unit

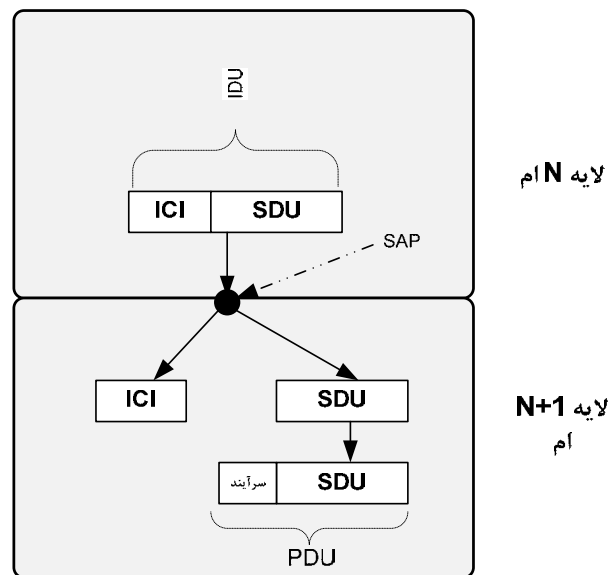
^۲ Entity

^۳ Peer entity

^۴ Service Access Point

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

قبل از ارسال اطلاعات بین دو لایه، آن دو باید به یک سری توافقات اولیه در مورد قواعد و ویژگی های هر لایه برسند. مطابق با شکل (۱-۱۵)، لایه $N+1$ ام شبکه از طریق یک نقطه دسترسی به سرویس، یک واحد داده ای به نام واحد داده ای واسط (IDU^1) را به موجودیت فعال لایه N ام ارسال می دارد. هر واحد داده ای واسط از دو قسمت تشکیل شده است که عبارتند از: واحد داده ای سرویس (SDU^2) و اطلاعات کنترلی واسط (ICI^3). از اطلاعات کنترلی واسط برای انجام امور کنترلی خاص استفاده می شود و جزو داده های ارسالی نمی باشد. هر لایه از اطلاعات کنترلی واسط لایه بالاتر خود استفاده می نماید و بعد از استفاده، آنها را از بین می برد. لایه N ام با دریافت واحد داده ای سرویس از لایه بالاتر خود، ممکن است که به خاطر محدودیت طول بسته های خود، آن را به قطعات کوچکتری تقسیم نماید. بعد از تکه سازی بسته، به هر تکه سرآیند مناسب اضافه می شود و کل بسته در قالب یک واحد داده ای پروتکل (PDU^4) ارسال می گردد.



شکل (۱-۱۵): مرز مشترک دو لایه

۱-۴-۷ - سرویس اتصال گرا و بی اتصال

هر لایه شبکه قادر به ارائه دو نوع سرویس مختلف به لایه بالاتر از خود می باشد. این دو نوع سرویس عبارتند از: سرویس اتصال گرا^۵ و سرویس بی اتصال^۶. یکی از کاربردهای بارز سرویس اتصال گرا، شبکه تلفن است. برای برقراری ارتباط و مکالمه صوتی بین دو کاربر، کاربر اولیه بعد از برداشتن گوشی تلفن و شنیدن بوق آزاد، اقدام به شماره گیری می نماید. در این مرحله شبکه تلفن درخواست کاربر را برای برقراری ارتباط دریافت می نماید و ارتباط کاربر را با مخاطب برقرار می سازد. بعد از آن که مخاطب گوشی تلفن خود را برداشت عملاً ارتباط برقرار می شود و دو طرف، قادر به صحبت با یکدیگر می باشند. در نهایت پس از اتمام مکالمه با گذاشتن گوشی، ارتباط قطع می شود.

^۱ Interface Data Unit
^۲ Service Data Unit
^۳ Interface Control Information
^۴ Protocol Data Unit
^۵ Connection oriented
^۶ Connectionless

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

در شبکه های کامپیوتری اتصال گرا نیز مشابه شبکه تلفن، کاربر ابتدا از شبکه می خواهد که یک مسیر اولیه بین کامپیوتر مبداء و مقصد برقرار نماید. پس از آن که این مسیر توسط شبکه بین کاربران مبداء و مقصد بوجود آمد، کاربران قادر به ارسال اطلاعات خود می باشند. پس از اتمام ارسال اطلاعات، مسیر بوجود آمده از بین می رود.

در سرویس بی اتصال، بدون آن که کاربر آمادگی گیرنده را بررسی نماید، اقدام به ارسال اطلاعات به شبکه می کند. طبیعی است که بسته های ارسالی کاربران در این نوع سرویس، به طور مستقل پردازش می شوند و از مسیرهای مختلف به مقصد می رسند. در این نوع سرویس، این احتمال وجود دارد که بسته ها به ترتیب به مقصد نرسند، زیرا ممکن است که بسته اول از یک مسیر طولانی تر نسبت به بسته دوم به مقصد برسد که این امر باعث دیرتر رسیدن بسته اول نسبت به بسته دوم در مقصد می شود. سیستم پست نمونه ای از سرویس بی اتصال است.

برای افزایش کیفیت و اطمینان از دریافت صحیح بسته ها در مقصد، این امکان وجود دارد که در هریک از این دو نوع سرویس، گیرنده با ارسال پیام تصدیق، دریافت صحیح بسته ورودی را به اطلاع فرستنده برساند. البته ارسال پیام تصدیق خود باعث افزایش تاخیر در سیستم می شود، ولی از طرف دیگر باعث افزایش اطمینان و کیفیت سرویس می گردد. به عنوان مثال پروتکل انتقال فایل (FTP¹) نوعی سرویس اتصال گرا همراه با پیام تصدیق می باشد. در سرویس پست الکترونیکی نیازی به ارسال پیام تصدیق از طرف گیرنده نمی باشد و این نوع سرویس از نوع بی اتصال بدون پیام تصدیق است. به سرویس بی اتصال به دلیل شباهت آن با سیستم تلگرام، سرویس داده گرام² نیز می گویند.

سرویس اتصال گرا همراه با پیام تصدیق خود به دو نوع تقسیم بندی می شوند. در نوع اول که جریان پیام ها³ نام دارد، حد و مرز پیام های ارسالی در گیرنده قابل تشخیص می باشد. به عنوان مثال اگر فرستنده، ۱۰ پیام یک کیلو بایتی ارسال دارد، در گیرنده نیز می توان این ۱۰ پیام یک کیلو بایتی را از یکدیگر تشخیص داد. ولی در نوع دوم که رشته بایت ها⁴ نام دارد، گیرنده قادر به تشخیص و تفکیک پیام ها از یکدیگر نمی باشد. در این حالت اگر فرستنده به طور مثال، ۱۰ پیام یک کیلو بایتی ارسال کند، گیرنده فقط یک پیام ۱۰ کیلو بایتی دریافت می نماید و نمی تواند تشخیص دهد که این ۱۰ کیلو بایت اطلاعات ورودی در اصل ۱۰ پیام یک کیلو بایتی متفاوت بوده است.

در بعضی از کاربردهای شبکه، که از سرویس بی اتصال استفاده می شود، ارسال پیام گواهی و تصدیق دریافت از طرف گیرنده ضروری و لازم به نظر می رسد. این نوع سرویس را در اصطلاح سرویس داده گرام همراه با پیام تصدیق می نامند. به عنوان مثال ارسال نامه های سفارشی در سیستم پستی که فرستنده می خواهد از دریافت نامه در گیرنده مطمئن شود، نمونه ای از این نوع سرویس می باشد. نوعی دیگر از سرویس موجود در شبکه های کامپیوتری، سرویس درخواست - پاسخ⁵ است. در این نوع سرویس، فرستنده با ارسال یک داده گرام، درخواست خود را برای گیرنده ارسال می دارد. گیرنده نیز در پاسخ به درخواست فرستنده یک داده گرام که حاوی پاسخ به درخواست فرستنده است ارسال می کند. به عنوان مثال جستجو در بانک های اطلاعاتی نوعی سرویس درخواست - پاسخ است.

در هر لایه شبکه، برای ارائه سرویس اتصال گرا یا بی اتصال از یک مجموعه عملیات پایه ای⁶ استفاده می شود. عملیات پایه ای به چهار نوع تقسیم بندی می شوند که عبارتند از:

¹ File Transfer Protocol
² Datagram
³ Message sequence
⁴ Byte stream
⁵ Request-reply
⁶ Service primitives

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۱

۱- **عملیات پایه ای درخواست^۱**: این عملیات برای اعلام درخواست انجام یک کار خاص مانند درخواست برقراری اتصال و یا درخواست ارسال داده ها در شبکه به کار می رود.

۲- **عملیات پایه ای اعلام^۲**: هنگامی که در موجودیت همتا در سمت گیرنده عملیات پایه ای درخواست دریافت گردید، برای اطلاع دادن به لایه بالایی، عملیات پایه ای اعلام ارسال می شود که کاربر را از ورود یک درخواست از سمت مقابل مطلع می سازد.

۳- **عملیات پایه ای پاسخ^۳**: هنگامی که موجودیت همتا از دریافت درخواست مطلع شد، برای پاسخ دادن به درخواست ورودی که از جانب همتای خود در فرستنده ارسال شده است، از عملیات پایه ای پاسخ استفاده می کند.

۴- **عملیات پایه ای تأیید^۴**: هنگامی که پاسخ موجودیت همتا به درخواست فرستنده ارسال شد، در سمت فرستنده اولیه این پاسخ به صورت عملیات پایه ای تأیید به اطلاع آن رسیده می شود. به این ترتیب فرستنده متوجه می گردد که آیا درخواستش مورد قبول واقع شده است یا خیر؟

عملیات پایه ای می تواند شامل مشخصه هایی باشد که به کمک این مشخصه ها می توان مشخصاتی نظیر: آدرس فرستنده درخواست کننده، نوع سرویس درخواستی و حداکثر طول بسته های ارسالی را به اطلاع طرف مقابل رساند.

از نظر نحوه ارسال عملیات پایه ای بین دو موجودیت همتا، سرویس شبکه را می توان به دو نوع تقسیم بندی نمود که عبارتند از: سرویس تأیید شده^۵ و سرویس بدون تأیید^۶. در سرویس تأیید شده، از هر چهار نوع عملیات پایه ای درخواست، اعلام، پاسخ و تأیید استفاده می شود، اما در سرویس بدون تأیید، فقط از عملیات پایه ای درخواست و اعلام استفاده می گردد.

برای درک بهتر مفاهیم عملیات پایه ای به یک مثال توجه می نماییم. فرض کنید در یک لایه برای ارائه سرویس اتصال گرا، هشت عملیات پایه ای زیر مورد استفاده قرار می گیرند:

- **CONNECT.request**: از این عملیات پایه ای برای ارسال درخواست برقراری اتصال فرستنده استفاده می شود (با مقایسه با یک ارتباط تلفنی برداشتن گوشی و گرفتن شماره تلفن مخاطب می باشد).
- **CONNECT.indication**: در سمت گیرنده، این عملیات پایه ای برای آگاه سازی لایه بالایی از ورود یک درخواست برقراری اتصال استفاده می شود (در ارتباط تلفنی زنگ زدن تلفن مخاطب می باشد).
- **CONNECT.response**: گیرنده، برای اعلام قبول یا رد درخواست ورودی و پاسخ دهی به آن از این عملیات پایه ای استفاده می نماید (در ارتباط تلفنی برداشتن گوشی توسط مخاطب می باشد).
- **CONNECT.confirm**: این عملیات پایه ای برای اطلاع دادن در مورد قبول یا رد درخواست به فرستنده که درخواست کننده اولیه بوده است، استفاده می شود (در ارتباط تلفنی قطع شدن صدای زنگ تلفن در سمت تماس گیرنده می باشد).
- **DATA.request**: از این عملیات پایه ای برای ارسال داده استفاده می شود (در ارتباط تلفنی صحبت های ارسالی بین تماس گیرنده و مخاطب می باشد).
- **DATA.indication**: برای مطلع ساختن گیرنده نسبت به ورود داده استفاده می شود (در ارتباط تلفنی شنیدن صحبت های یک طرف توسط طرف مقابل می باشد).

^۱ Request primitive

^۲ Indication primitive

^۳ Response primitive

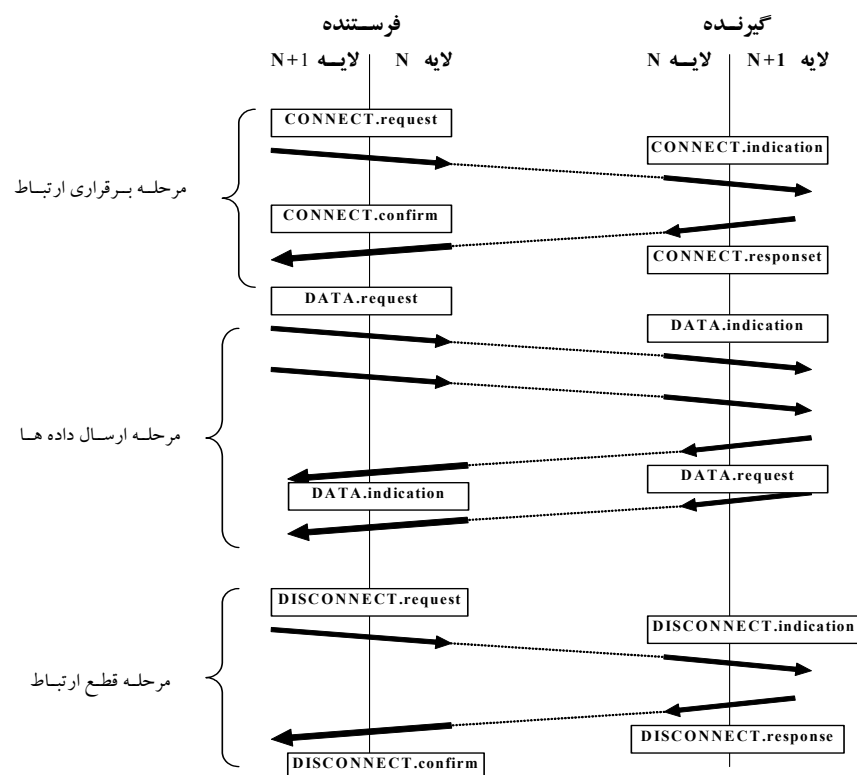
^۴ Confirm primitive

^۵ Confirm services

^۶ Unconfirmed services

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

- **DISCONNECT.request**: این عملیات پایه ای نشان دهنده درخواست قطع اتصال می باشد (در ارتباط تلفنی، قطع ارتباط و قرار دادن گوشی بر روی تلفن می باشد).
 - **DISCONNECT.indication**: از این عملیات برای مطلع ساختن موجودیت همتا در گیرنده از درخواست قطع اتصال، استفاده می شود (در ارتباط تلفنی شنیدن اتمام مکالمه و گذاشتن گوشی تلفن از جانب طرف مقابل می باشد).
- از آنجایی که در مثال فوق برای برقراری اتصال از هر چهار نوع عملیات پایه ای استفاده می گردد، ولی برای قطع اتصال فقط از دو عملیات پایه ای استفاده می شود، بنابراین می توان نتیجه گرفت که برقراری اتصال، یک نوع سرویس تأیید شده و قطع اتصال، یک نوع سرویس بدون تأیید می باشد. در شکل (۱-۱۶) دیاگرام زمانی و مراحل ارسال عملیات پایه ای فوق بین فرستنده و گیرنده نشان داده شده است. البته در این شکل برای مرحله قطع ارتباط از ۴ عملیات پایه ای استفاده شده است.



شکل (۱-۱۶): دیاگرام زمانی و مراحل ارسال عملیات پایه ای بین دو لایه همتای شبکه

۸-۴-۱ - سوئیچینگ

به طور کلی در شبکه های کامپیوتری دو نوع مختلف سوئیچینگ وجود دارد که عبارتند از: سوئیچینگ مداری^۱ و سوئیچینگ بسته ای^۲.

در سوئیچینگ مداری، یک مسیر فیزیکی با یک ظرفیت ثابت بین فرستنده و گیرنده ایجاد می شود. شبکه های سوئیچینگ مداری در حقیقت برای انتقال صوت طراحی شده اند. در شبکه های تلفن بعد از برقراری یک اتصال صوتی بین دو نقطه، این اتصال تا پایان ارتباط برقرار می باشد. شبکه های سوئیچینگ مداری برای ارسال داده ها مناسب نیست. یکی از مهمترین دلایل آن این است که بیشتر داده های کامپیوتری به صورت انفجاری^۳ می باشند. بدین معنی که در یک لحظه از زمان حجم زیادی از داده ها برای ارسال وجود دارد و در یک لحظه دیگر، ممکن است هیچ داده ای برای ارسال موجود نباشد. بنابراین چنانچه بخواهیم از سوئیچینگ مداری برای ارسال داده ها استفاده نماییم، در زمان عدم ارسال داده و عدم استفاده از پهنای باند ظرفیت شبکه بدون استفاده می ماند و از بین می رود.

یکی دیگر از دلایل نامناسب بودن شبکه های سوئیچینگ مداری برای ارسال داده های کامپیوتری آن است که در شبکه های داده نرخ ارسال متغیر می باشد. در شبکه های داده در لحظاتی که داده هایی برای ارسال وجود دارد سرعت ارسال باید به اندازه کافی زیاد باشد و در زمانی که داده ای برای ارسال وجود ندارد، سرعت ارسال کم یا صفر می باشد. از آنجایی که در شبکه های سوئیچینگ مداری ظرفیت اتصال ثابت است، بنابراین نمی توان از آن برای ارسال داده های کامپیوتری با نرخ ارسال متغیر استفاده نمود. عدم انعطاف پذیری شبکه های سوئیچینگ مداری نسبت به تغییرات، از دیگر دلایل نامناسب بودن شبکه های سوئیچینگ مداری برای تبادل داده های کامپیوتری می باشد. از دیگر معایب سوئیچینگ مداری، می توان به عدم قابلیت اولویت گذاری داده ها در آن اشاره نمود. برای ارسال داده های کامپیوتری باید مکانیسم هایی برای اولویت گذاری بسته ها وجود داشته باشد تا بتوان بین داده های مختلف فرق گذاشت.

در شبکه های سوئیچینگ بسته ای، داده های ارسالی به صورت بسته هایی به طول مشخص ارسال می شوند. شبکه های سوئیچینگ بسته ای دو نوع می باشند که عبارتند از:

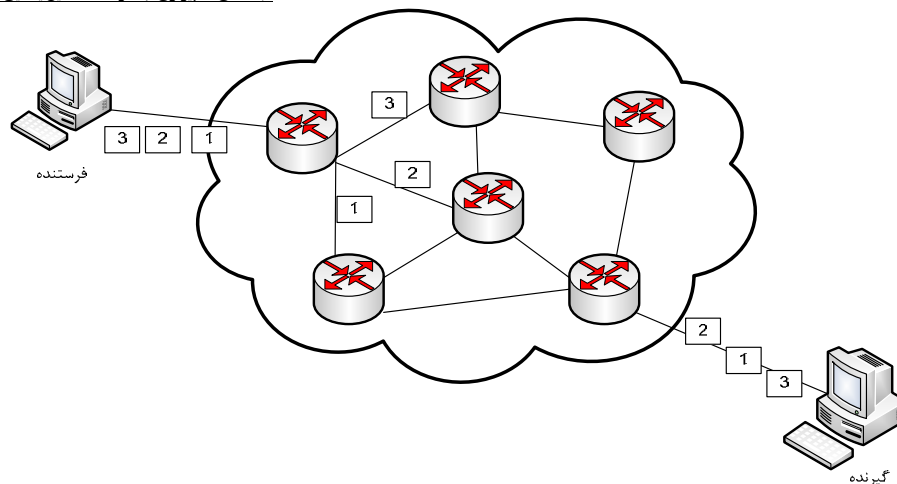
- شبکه های داده گرام
- شبکه های مدار مجازی^۴

شبکه های داده گرام از نوع بی اتصال می باشد. مطابق با آنچه که در شکل (۱-۱۷) نشان داده شده است، در شبکه های داده گرام بسته های ارسالی به طور مستقل از یکدیگر وارد نودهای شبکه می شود و مسیریابی می گردند. از آنجایی که هر بسته، مستقل از سایر بسته ها پردازش می شود، این احتمال وجود دارد که بسته های ارسالی از مسیره های مختلفی عبور نمایند و به ترتیب نادرست به مقصد برسند. بنابراین یکی از مهمترین مشکلات شبکه های داده گرام عدم رعایت ترتیب بسته ها می باشد.

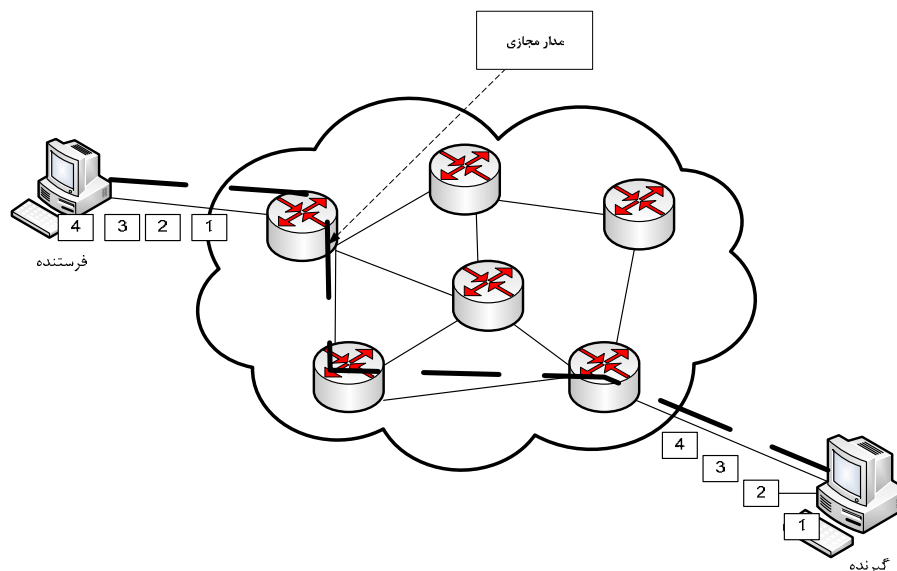
شبکه های سوئیچینگ بسته ای از نوع مدار مجازی، از روش اتصال گرا برای برقراری ارتباط بین مبدأ و مقصد استفاده می نماید. در این نوع شبکه ها قبل از ارسال داده ها، یک مدار مجازی بین فرستنده و گیرنده برقرار می شود و بسته های ارسالی بین مبدأ و مقصد از مسیر مجازی به وجود آمده عبور می نمایند و بنابراین تمامی بسته ها به ترتیب به مقصد می رسند. بعد از اتمام ارسال داده ها، مسیر مجازی به وجود آمده از بین می رود. در شکل (۱-۱۸) مثالی از یک شبکه مدار مجازی آورده شده است.

^۱ Circuit switching^۲ Packet switching^۳ Bursty^۴ Virtual circuit

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۲



شکل (۱-۱۷): شبکه های داده گرام



شکل (۱-۱۸): شبکه های مدار مجازی

در شبکه های مدار مجازی، دو نوع مدار مجازی وجود دارند که عبارتند از مدار مجازی سوئیچ شده (SVC^1) و مدار مجازی دائمی (PVC^2). مدارهای مجازی دائمی به طور دائم در اختیار فرستنده و گیرنده قرار دارند و نیازی به انجام عملیات برقراری و قطع ارتباط نمی باشد. در مدارهای مجازی سوئیچ شده، برای برقراری مدار مجازی بین فرستنده و گیرنده، باید روال های خاصی انجام شود. بعد از ارسال داده ها، مدار مجازی سوئیچ شده آزادی شود تا بتوان از ظرفیت آن برای سایر اتصال های موجود در شبکه استفاده نمود. شبکه های X.25 و ATM مثال هایی از سوئیچینگ بسته ای مدار مجازی هستند در حالی که پروتکل اینترنت از نوع داده گرام است.

پرسش های فصل

۱. حداقل ۱۰ مورد از کاربرد کامپیوتر در جامعه را نام ببرید.

^۱ Switched Virtual Circuit
^۲ Permanent Virtual Circuit

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

۲. سه مشخصه اصلی سیستم های انتقال داده را نام ببرید.
۳. اجزای اصلی یک سیستم انتقال داده را نام ببرید.
۴. مدل پایه یک سیستم انتقال داده را با رسم شکل توصیف نمایید.
۵. سه معیار اصلی در طراحی شبکه های انتقال داده را نام برده و عوامل مؤثر در هر یک را توضیح دهید.
۶. استانداردهای اسمی و نامی را توضیح داده و تفاوت آنها را بایکدیگر بنویسید.
۷. سه مرکز اصلی استانداردگذاری در شبکه های انتقال داده را نام برده و توضیح دهید.
۸. مفهوم مدل لایه ای را در شبکه های کامپیوتری توضیح دهید.
۹. مسائل و مشکلاتی را که در ساختار لایه ای با آن روبرو هستیم را عنوان نموده و راه حل هر یک را توضیح دهید.
۱۰. علت انجام عملیات تکه سازی و بازسازی در شبکه های کامپیوتری را توضیح دهید.
۱۱. نکاتی را که در مدل لایه ای در مورد انتخاب تعداد لایه ها و عملیات هر لایه با آن روبرو هستیم را تشریح نمایید.
۱۲. مدل مرجع OSI را توضیح دهید.
۱۳. وظایف لایه فیزیکی را در مدل OSI توضیح دهید.
۱۴. مسائل مختلفی که در لایه فیزیکی مدل OSI با آنها روبرو هستیم را توصیف نمایید.
۱۵. وظایف لایه پیوند داده را در مدل OSI توضیح دهید.
۱۶. وظایف لایه شبکه را در مدل OSI توضیح دهید.
۱۷. مفهوم ازدحام را در شبکه های کامپیوتری توضیح داده و روش مقابله با آن را تشریح نمایید.
۱۸. وظایف لایه حمل را در مدل OSI توضیح دهید.
۱۹. وظایف لایه جلسه را در مدل OSI توضیح دهید.
۲۰. وظایف لایه ارائه را در مدل OSI توضیح دهید.
۲۱. وظایف لایه کاربرد را در مدل OSI توضیح دهید.
۲۲. روند ارسال و دریافت بسته ها را در مدل مرجع OSI توصیف نمایید.
۲۳. در واسط ارتباطی بین دو لایه، نقطه دسترسی به سرویس را توضیح دهید.
۲۴. مفهوم موجودیت در لایه های شبکه و عملیات انجام شده توسط آنها را بنویسید.
۲۵. سرویس اتصال گرا را توضیح داده و برای آن مثالی ذکر کنید.
۲۶. سرویس بی اتصال را توضیح داده و برای آن مثالی ذکر نمایید.
۲۷. سرویس اتصال گرا و بی اتصال را بایکدیگر مقایسه کنید.
۲۸. سرویس تأیید شده و سرویس تأیید نشده را تعریف نموده و تفاوت آنها را بایکدیگر بنویسید.
۲۹. عملکرد سوئیچینگ مداری و سوئیچینگ بسته ای را توصیف نموده و با یکدیگر مقایسه نمایید.

فصل دوم

لایه فیزیکی

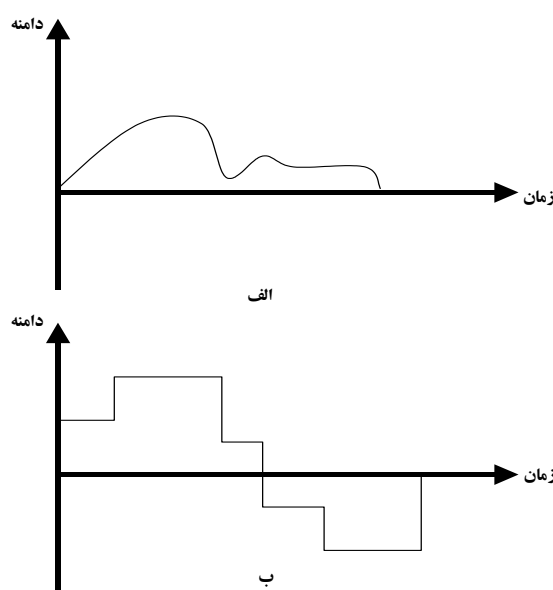
۱-۲- مقدمه

همان طور که در فصل قبل اشاره گردید، پایین ترین لایه در مدل لایه ای شبکه، لایه فیزیکی است. اطلاعات ارسالی کاربر بعد از عبور از لایه های شبکه، وارد لایه فیزیکی می شود. در این لایه اطلاعات از شکل منطقی خود خارج شده و به صورت سیگنال های الکتریکی وارد رسانه های فیزیکی مناسب شده و به سمت مقصد ارسال می گردد. در سمت مقصد لایه فیزیکی سیگنال های دریافتی را دوباره به صورت رشته بیت های منطقی در آورده و تحویل لایه های بالاتر می دهد. در این فصل به معرفی وظایف لایه فیزیکی در شبکه های کامپیوتری و استانداردهای مربوط به آن می پردازیم.

۲-۲- سیگنال های الکتریکی

یکی از مهم ترین وظایف لایه فیزیکی انتقال اطلاعات به صورت سیگنال های الکتریکی از طریق رسانه های ارسال می باشد. اطلاعات ارسالی فوق شامل صوت دیجیتال شده، تصویر، داده های عددی و کاراکترهای کامپیوتری می باشند. از آنجایی که اطلاعات ارسالی به صورت دیجیتال می باشد و شامل ۱ و ۰ منطقی است، برای ارسال در رسانه انتقال باید به سیگنال های الکتریکی تبدیل شوند.

سیگنال های الکتریکی به دو دسته کلی تقسیم بندی می شوند که عبارتند: از سیگنال های آنالوگ و سیگنال های دیجیتال. سیگنال های دیجیتال مقادیر مشخص و محدودی را اختیار می نمایند، در حالی که سیگنال های آنالوگ هر مقداری در محدوده تغییرات خود می توانند داشته باشند. در شکل (۱-۲) نمونه ای از سیگنال های آنالوگ و دیجیتال نشان داده شده است.



شکل (۱-۲): سیگنال های الکتریکی: الف) آنالوگ ب) دیجیتال

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

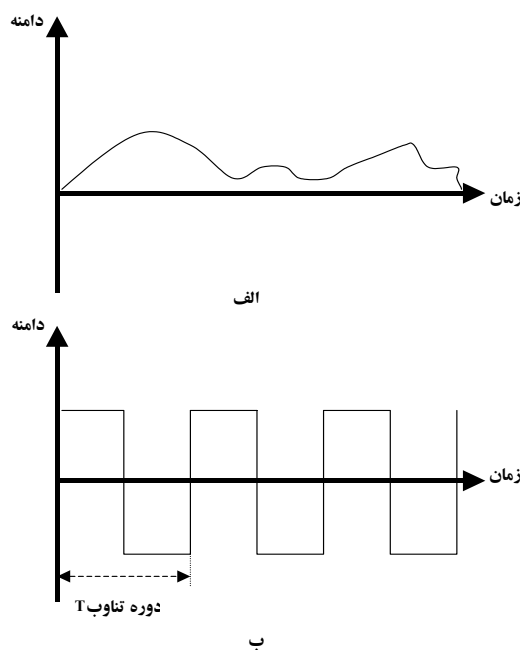
سیگنال های الکتریکی آنالوگ و دیجیتال به دو صورت متناوب و نامتناوب تقسیم بندی می شود. سیگنال های متناوب در فاصله های زمانی مشخص که دوره تناوب آن نامیده می شود، تکرار می گردد. طبق تعریف تعداد تکرارهای یک موج متناوب در واحد زمان فرکانس نامیده می شود. چنانچه دوره تناوب سیگنال را با T نمایش دهیم، در این صورت فرکانس سیگنال (f) به صورت $f=1/T$ محاسبه می شود.

در فرمول فوق چنانچه T برحسب ثانیه باشد در این صورت فرکانس برحسب هرتز خواهد بود. در جدول (۱-۲) واحدهای اصلی فرکانس و دوره تناوب نشان داده شده است.

جدول (۱-۲): واحدهای اصلی فرکانس و دوره تناوب

دوره تناوب	فرکانس
ثانیه	هرتز
میلی ثانیه	کیلوهرتز
میکروثانیه	مگاهرتز
نانو ثانیه	گیگاهرتز
پیکو ثانیه	تراهرتز

سیگنال های نامتناوب فاقد هرگونه تکرار منظم در فواصل زمانی معین می باشند. در شکل (۲-۲) نمونه ای از سیگنال های متناوب و نامتناوب نشان داده شده است.

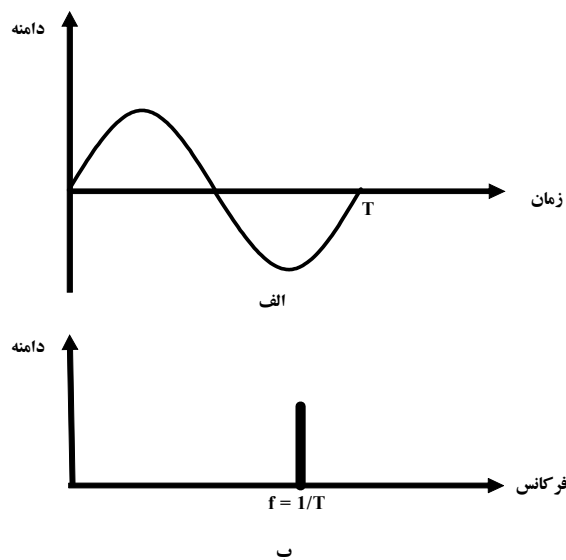


شکل (۲-۲): انواع سیگنال ها: الف) نامتناوب ب) متناوب

با استفاده از تبدیل فوریه، هر سیگنال نامتناوب را می توان به تعداد نامحدودی سیگنال متناوب تبدیل نمود. یکی از متداول ترین سیگنال های متناوب آنالوگ، سیگنال سینوسی می باشد. هر سیگنال سینوسی دارای ۳ مشخصه اصلی است که عبارتند از: دامنه، فاز اولیه و فرکانس زاویه ای. برای نمایش یک سیگنال از دو حوزه به نام های حوزه زمان و حوزه فرکانس استفاده می شود. هر سیگنال فرکانس پایین در حوزه زمان دارای دوره تناوب بالایی می باشد و بالعکس دوره تناوب هر

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۲

سیگنال فرکانس بالا، کم است. همان طور که در شکل (۳-۲) نشان داده شده است، یک موج سینوسی خالص در حوزه فرکانس فقط دارای یک مؤلفه است. چنانچه موج سینوسی دارای مؤلفه DC باشد، در این صورت در فرکانس صفر یک مؤلفه درحوزه فرکانس وجود دارد.



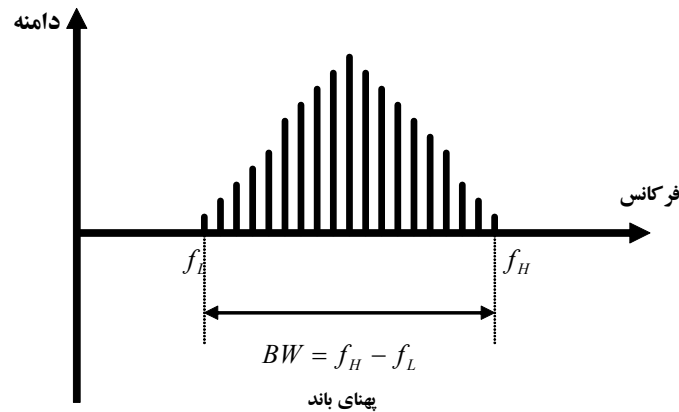
شکل (۳-۲): نمایش سیگنال سینوسی: الف) درحوزه زمان ب) درحوزه فرکانس

طبق تعریف، طیف فرکانسی^۱ هر سیگنال مجموعه ای از مؤلفه های فرکانسی سیگنال درحوزه فرکانس می باشد. فاصله بین کمترین و بالاترین مؤلفه فرکانسی درطیف فرکانسی سیگنال، پهنای باند^۲ نامیده می شود. در شکل (۴-۲) نمونه ای ازطیف فرکانسی سیگنال و پهنای باند آن نشان داده شده است.

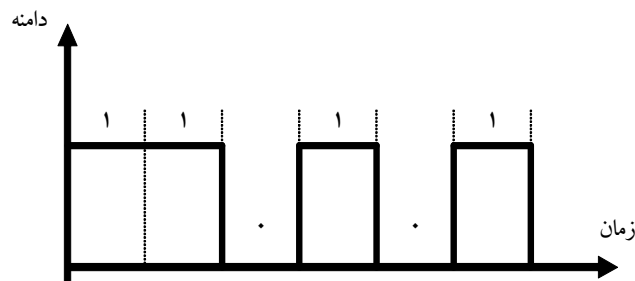
در شبکه های کامپیوتری برای تبادل داده ها از سیگنال های دیجیتال استفاده می شود. در شکل (۵-۲) نمونه ای از یک سیگنال دیجیتال نشان داده شده است. اغلب سیگنال های دیجیتال به صورت نامتناوب می باشند. طبق تبدیل فوریه، هر سیگنال دیجیتال قابل تجزیه به تعداد نامحدودی موج سینوسی با فرکانس و دامنه های متفاوت می باشد. بنابراین طیف فرکانسی یک سیگنال دیجیتال در تمام فرکانسها دارای مؤلفه می باشد و پهنای باند آن بی نهایت است. هنگام ارسال سیگنال های دیجیتال در رسانه انتقال، برخی از مؤلفه های فرکانسی آن حذف می شوند که این امر باعث وقوع اعوجاج در سیگنال خروجی می گردد. طبق تعریف، حداکثر نرخ بیت قابل ارسال در رسانه انتقال، ظرفیت کانال نامیده می شود. ظرفیت کانال به مشخصه هایی نظیر نسبت دامنه سیگنال به نویز و همچنین نوع کدینگ مورد استفاده بستگی دارد.

^۱ Spectrum
^۲ Bandwidth

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۲



شکل (۲-۴): طیف فرکانسی و پهنای باند سیگنال



شکل (۲-۵): نمونه ای از یک سیگنال دیجیتال

اغلب سیگنال های دیجیتال به صورت نامتناوب می باشند. طبق تعریف طول زمانی ارسال یک بیت ، فاصله بیت^۱ نامیده می شود. همچنین تعداد بیت های ارسالی در واحد زمان ، نرخ ارسال بیت^۲ نامیده می شود. براساس تبدیل فوریه، هر سیگنال دیجیتال قابل تجزیه به تعداد نامحدودی موج سینوسی با فرکانس و دامنه های متفاوت است.

۲-۳- روش های کدینگ

در سیستم های انتقال ، قبل از ارسال داده های کامپیوتری باید آنها را به صورت کدهای مناسبی تبدیل کرد. نحوه کد کردن اطلاعات به عواملی نظیر ساختار اصلی آنها و همچنین ساختار قابل ارسال در محیط بستگی دارد . همان طور که قبلاً اشاره گردید سیگنال های الکتریکی به دودسته آنالوگ و دیجیتال تقسیم می شوند. چهار روش مختلف کدینگ وجود دارد که عبارتند از :

- تبدیل سیگنال های دیجیتال به دیجیتال
- تبدیل سیگنال های دیجیتال به آنالوگ
- تبدیل سیگنال های آنالوگ به دیجیتال
- تبدیل سیگنال های آنالوگ به آنالوگ

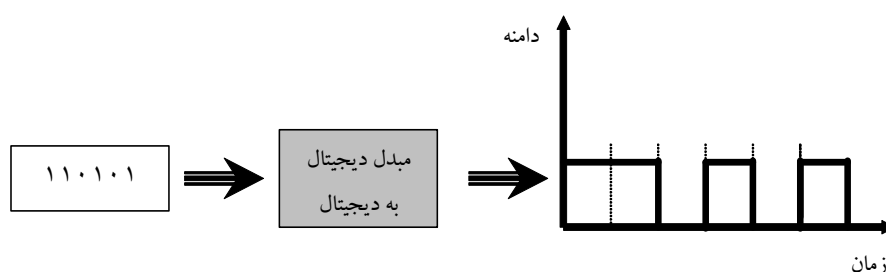
^۱ Bit interval
^۲ Bit rate

۲-۳-۱- تبدیل اطلاعات دیجیتال به دیجیتال

از این نوع کدینگ در ارسال اطلاعات دیجیتال بوسیله سیگنال های دیجیتال استفاده می شود. به عنوان مثال کامپیوتر برای مبادله داده های دیجیتال خود به چاپگر، آنها را به شکل سیگنال های دیجیتال تبدیل می نماید و ارسال می دارد. در شکل (۲-۶) ساختار کلی این نوع کدینگ نشان داده شده است. روش های مختلفی برای تبدیل اطلاعات دیجیتال به سیگنال های دیجیتال وجود دارند، که مهم ترین این روش ها که در شبکه های کامپیوتری و انتقال داده ها استفاده می شوند عبارتند از:

- روش تک قطبی^۱
- روش قطبی^۲
- روش دو قطبی^۳

در زیر به بررسی هر یک از این روش ها می پردازیم .



شکل (۲-۶): تبدیل دیجیتال به دیجیتال

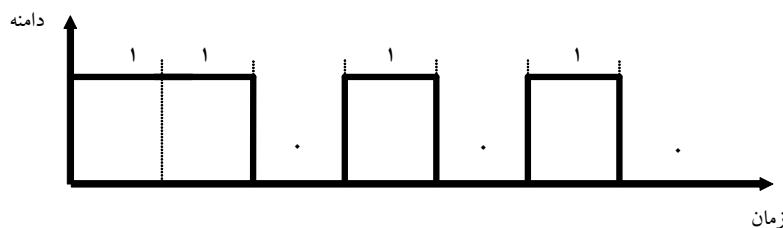
۲-۳-۱-۱- روش تک قطبی

در این روش، بیت ۰ با سیگنال الکتریکی با دامنه صفر ولت و بیت ۱ با سیگنال الکتریکی با سطح غیر صفر ارسال می شود. از آنجایی که در این روش فقط از یک سطح ولتاژ استفاده می شود، به آن روش تک قطبی گفته می شود. در شکل (۲-۷) مثالی از روش کدینگ تک قطبی آورده شده است.

روش تک قطبی دارای دو مشکل عمده می باشد که عبارتند از: وجود DC و حفظ همزمانی فرستنده و گیرنده. از آنجایی که متوسط ولتاژ سیگنال ارسالی در این روش غیر صفر است، در این صورت در سیگنال ارسالی قسمت DC مشاهده می شود. برخی از رسانه های ارسال مانند ترانسفورماتورها و سیستم های میکروویو قادر به انتقال سیگنال هایی که دارای متوسط غیر صفر هستند نمی باشند. یکی دیگر از مشکلات اصلی این روش عدم امکان همزمانی دقیق فرستنده و گیرنده است. چنانچه سیگنال دریافتی گیرنده تغییرات کمی داشته باشد، گیرنده قادر به تشخیص دقیق شروع و پایان هر بیت ارسالی نمی باشد.

^۱ Bit rate
^۲ Polar
^۳ Bipolar

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۷-۲): مثالی از کدینگ تک قطبی

چنانچه رشته بیت ارسالی در روش تک قطبی به طور ممتد حاوی ۰ و یا ۱ باشد در این صورت درسیگنال دیجیتال ارسالی تغییراتی وجود ندارد که این مسأله باعث عدم همزمانی دقیق گیرنده و فرستنده خواهد شد.

۲-۱-۳-۲- روش قطبی

روش کدینگ قطبی از دو سطح ولتاژ مثبت و منفی برای ارسال اطلاعات دیجیتال استفاده می نماید. با استفاده از این روش متوسط ولتاژ سیگنال ارسالی صفر خواهد بود. مشکل وجود DC که در روش قبلی مشاهده می شد، در این روش وجود ندارد. کدینگ قطبی دارای روش های متعددی می باشد که مهم ترین آنها عبارتند از:

- روش غیربازگشت به صفر (NRZ^1)

- روش بازگشت به صفر (RZ^2)

- روش دوفاز^۳

روش NRZ خود به دو روش دیگر تقسیم بندی می شود که عبارت است از: روش NRZ-L و روش NRZ-I. همچنین روش دو فاز به دو روش به نام های منچستر و روش منچستر تفاضلی تقسیم می گردد. از روش منچستر در شبکه محلی اترنت و از روش منچستر تفاضلی در شبکه های محلی حلقه نشانه استفاده می شود.

در روش NRZ سطح سیگنال ارسالی همواره مثبت و یا منفی می باشد. به عبارت دیگر در سیگنال ارسالی سطح صفر وجود ندارد. در روش NRZ-L برای بیت ۱، سطح سیگنال مثبت است و چنانچه بیت ارسالی ۰ باشد، سطح سیگنال ارسالی منفی خواهد بود. در روش NRZ-I چنانچه بیت ارسالی ۱ باشد، سطح سیگنال ارسالی معکوس می شود و چنانچه بیت ارسالی صفر باشد، سطح ارسالی بدون تغییر می ماند. در شکل (۸-۲) مثالی از روش های کدینگ NRZ-L و NRZ-I آورده شده است.

بادقت در روش NRZ مشاهده می شود که چنانچه رشته بیت ارسالی به طور ممتد حاوی ۰ و ۱ باشد، در این صورت سطح سیگنال ارسالی ثابت است و این مسأله باعث از بین رفتن همزمانی درگیرنده می گردد. برای اطمینان از همزمانی دقیق درگیرنده، در هر بیت باید سیگنال ارسالی دارای تغییراتی باشد که گیرنده با استفاده از این تغییرات قادر به همزمانی خود با فرستنده شود. در روش RZ برای نیل به همزمانی، از سه سطح مثبت، منفی و صفر استفاده می شود. در این روش در وسط فاصله زمانی ارسال هر بیت، سطح سیگنال ارسالی از مثبت یا منفی به صفر تغییر می کند. چنانچه بیت ارسال ۱ باشد در این صورت سطح سیگنال ارسالی در نیمه اول فاصله زمانی بیت مثبت و در نیمه دوم صفر است. در صورتی که بیت ۰

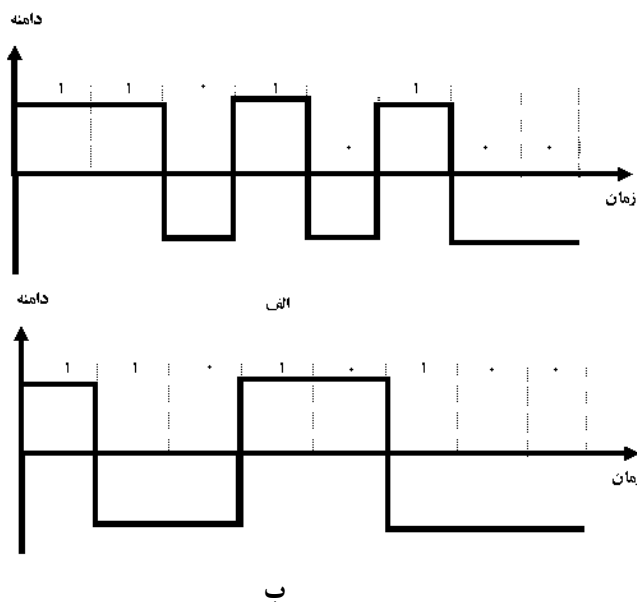
^۱ Non Return Zero

^۲ Return Zero

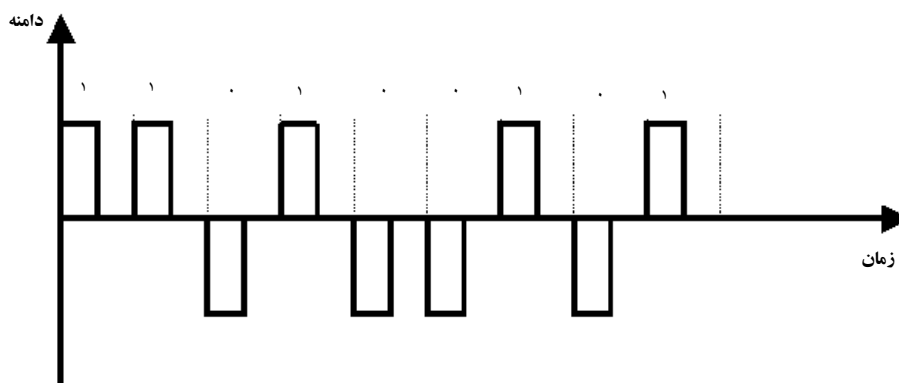
^۳ Biphas

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

ارسال گردد، سطح سیگنال ارسالی در نیمه اول منفی و در نیمه دوم صفر می باشد. یکی از مهم ترین مشکلات RZ نیاز به پهنای باند دو برابر نسبت به روش های قبلی است. در شکل (۲-۹) مثالی از روش RZ آورده شده است.



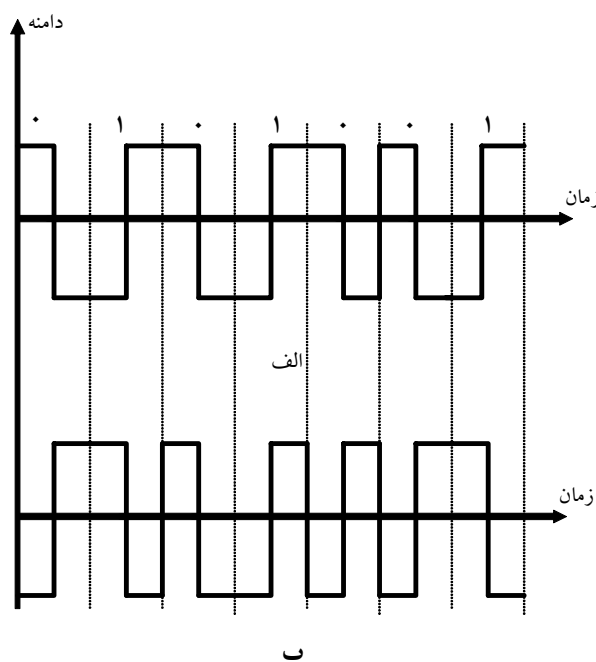
شکل (۲-۸): مثالی از کدینگ NRZ (الف) روش NRZ-L (ب) روش NRZ-I



شکل (۲-۹): مثالی از روش RZ

یکی از بهترین روش های حل مشکل همزمانی، روش دو فاز می باشد. در این روش سیگنال در وسط فاصله زمانی هر بیت، تغییر قطبیت داده و از منفی به مثبت و یا بالعکس از مثبت به منفی می رود. دو روش عمده دو فاز عبارتند از: روش منچستر و روش منچستر تفاضلی. در روش منچستر برای ارسال بیت های ۱، قطب سیگنال ارسالی در وسط فاصله زمانی هر بیت از منفی به مثبت تغییر می نماید. در حالی که برای بیت های ۰ قطب سیگنال ارسالی در وسط فاصله زمانی هر بیت از مثبت به منفی تغییر می کند. قدرت همزمانی این روش مشابه روش RZ می باشد، در حالی که در این روش فقط از دو سطح مثبت و منفی استفاده می شود. در روش منچستر تفاضلی، چنانچه بیت ارسالی صفر باشد، سطح سیگنال ارسالی در شروع فاصله زمانی بیت تغییر می کند. در حالی که چنانچه بیت ارسالی ۱ باشد سطح سیگنال ارسالی بدون تغییر می ماند. در شکل (۲-۱۰) مثالی از عملکرد روش منچستر و منچستر تفاضلی آورده شده است.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۲



شکل (۲-۱۰): کدینگ دوفاز: (الف) روش منچستر (ب) روش منچستر تفاضلی

۲-۳-۱-۳ روش دو قطبی

یکی دیگر از روش های ارسال سیگنال های دیجیتال روش دوقطبی می باشد. در این روش مشابه روش RZ از سه سطح مثبت، منفی و صفر استفاده می شود. ولی برخلاف روش RZ، در روش دو قطبی بیت ۰ با سیگنال صفر و بیت ۱ با سیگنال هایی با سطح مثبت و یا منفی ارسال می شوند. سطح سیگنال ارسالی برای بیت های ۱ به طور متناوب مثبت و منفی می شود.

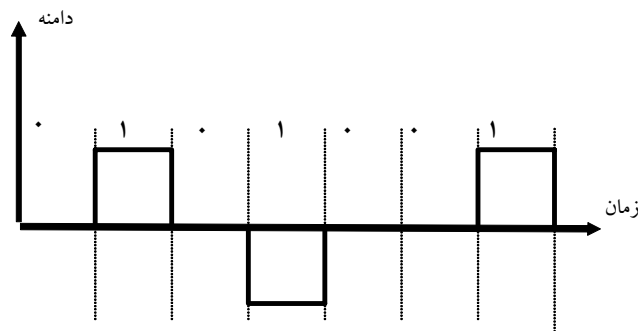
کدینگ دوقطبی به سه روش ^۱AMI، ^۲B8ZS و ^۳HDB3 تقسیم می شود. روش AMI ساده ترین روش دو قطبی می باشد. در این روش بیت ۰ با سیگنال با سطح ولتاژ صفر و بیت ۱ با سیگنالی با سطوح ولتاژ مثبت یا منفی ارسال می شود. سطح ولتاژ سیگنال ارسالی برای بیت ۱ به طور متناوب مثبت و یا منفی می شود. در شکل (۲-۱۱) مثالی از روش AMI آورده شده است. در روش AMI به دلیل تغییر متناوب سطح سیگنال ارسالی بیت های ۱، مشکل وجود DC حل می شود و همچنین همزمانی هنگام ارسال یک رشته متوالی بیت ۱ حفظ می شود، ولی یکی از نقاط ضعف عمده این روش مشکل بودن همزمانی در گیرنده هنگام ارسال متوالی چندین بیت ۰ می باشد. برای رفع این مشکل دو روش B8ZS و HDB3 ارائه شده است. در روش B8ZS برای ارسال ۸ بیت متوالی ۰ بر اساس قطبیت بیت ۱ قبلی از یکی از الگوهای نشان داده شده در شکل (۲-۱۲) استفاده می شود. تفاوت اصلی AMI با B8ZS هنگام ارسال متوالی ۸ بیت صفر مشاهده می شود. در روش B8ZS گیرنده با مشاهده تخلف از سطح ولتاژ دریافتی قادر به تشخیص بیت ۰ و ۱ می باشد.

^۱ Alternative Mark Inversion

^۲ Bipolar 8-Zero Substitution

^۳ High Density Bipolar 3

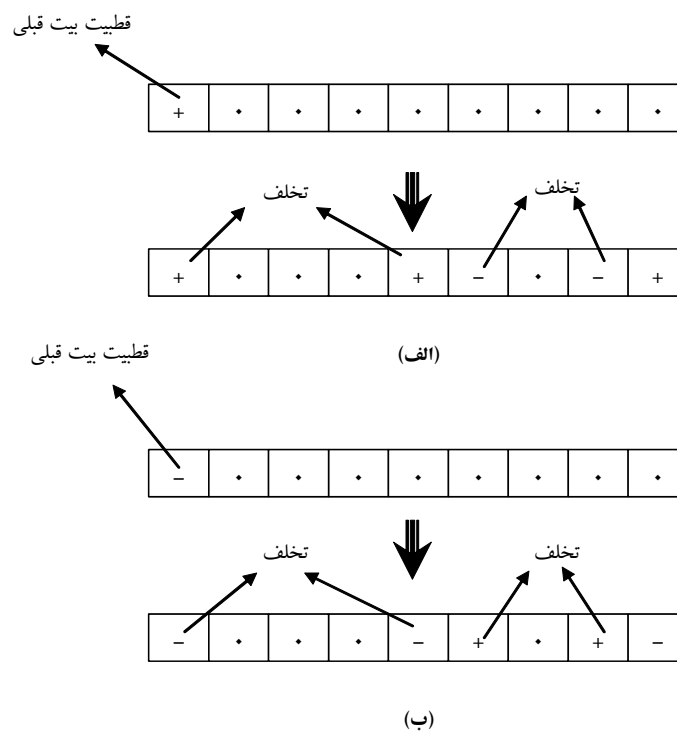
شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۱۱-۲): مثالی از روش AMI

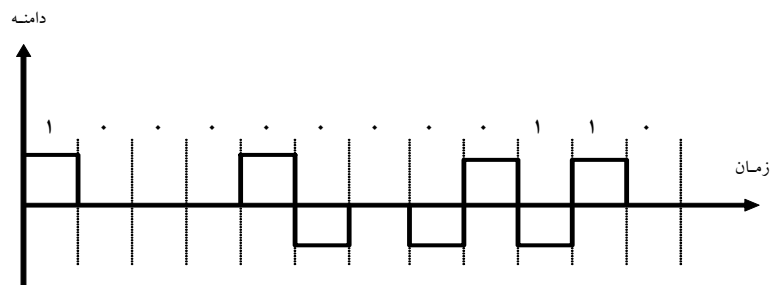
در شکل (۱۳-۲) مثالی از روش B8ZS آورده شده است .

از روش فوق در آمریکا برای حل مشکل همزمانی ارسال چندین بیت ۰ متوالی استفاده می شود، در حالی که در اروپا و ژاپن برای حل مشکل فوق از روش HDB3 استفاده می گردد. در روش HDB3 برای ارسال ۴ بیت متوالی صفر بر اساس تعداد اهای ارسالی بعد از آخرین جایگزینی و همچنین بر اساس قطبیت آخرین بیت ۱ از یکی از الگوهای نشان داده شده در شکل (۱۴-۲) استفاده می شود .

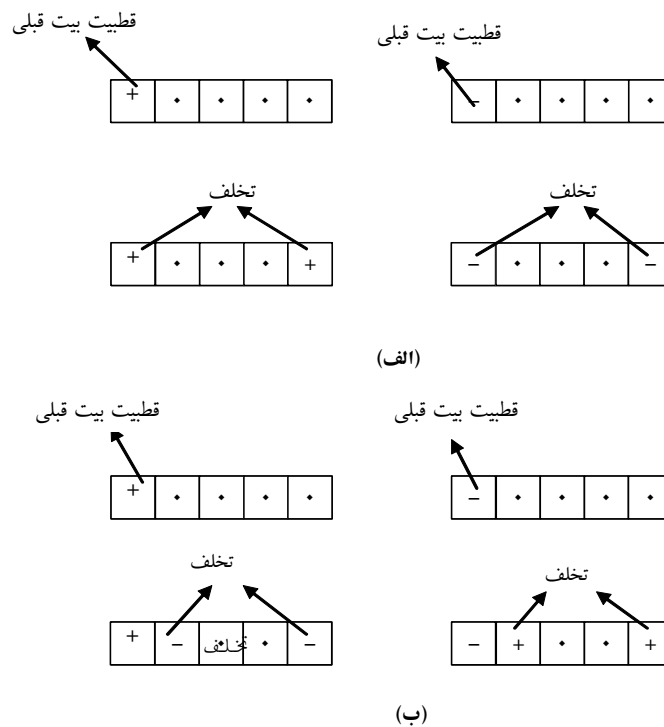


شکل (۱۲-۲): الگوهای مختلف روش B8ZS
الف) قطبیت بیت ۱ قبلی + است ب) قطبیت بیت ۱ قبلی - است

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

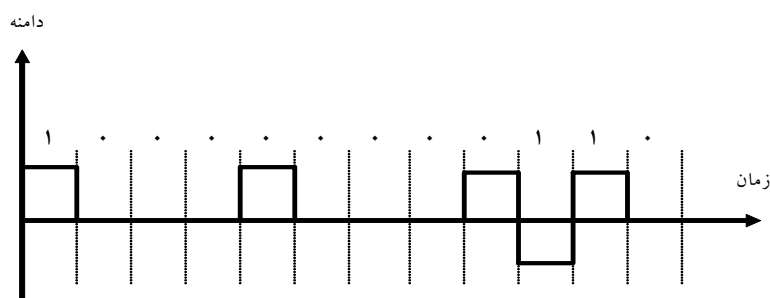


شکل (۲-۱۳): مثالی از روش B8ZS



شکل (۲-۱۴): الگوهای مختلف روش HDB3
 (الف) تعداد ۱ های قبل از آخرین جابجائی فرد است
 (ب) تعداد ۱ های قبل از آخرین جابجائی زوج است

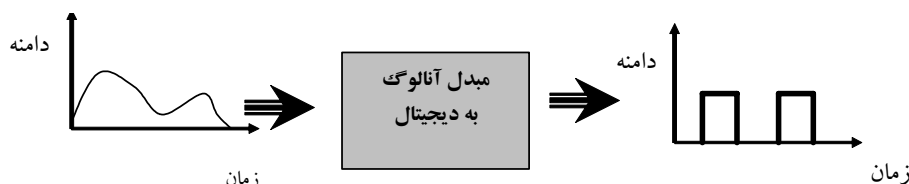
در شکل (۲-۱۵) مثالی از روش HDB3 آورده شده است .



شکل (۲-۱۵): مثالی از روش HDB3

۲-۳-۲ - تبدیل اطلاعات آنالوگ به دیجیتال

از تبدیل آنالوگ به دیجیتال در کاربردهایی نظیر ذخیره سازی اطلاعات در CD و ارسال صوت در شبکه های تلفن دیجیتال که اطلاعات اولیه آنالوگ می باشد ولی رسانه انتقال دیجیتال است، استفاده می شود. در شکل (۲-۱۶) مثالی از مبدل آنالوگ به دیجیتال آورده شده است. مطابق با شکل فوق، موج پیوسته آنالوگ به یک سری پالس های دیجیتال که نشان دهنده بیت های ۱ و ۰ می باشند تبدیل می گردند.



شکل (۲-۱۶): تبدیل آنالوگ به دیجیتال

اولین مرحله در تبدیل اطلاعات آنالوگ به دیجیتال مدولاسیون دامنه پالس (PAM^1) می باشد. در این روش اطلاعات آنالوگ دریافت می شوند و بعد از نمونه برداری از آنها یک سری پالس های دیجیتال ایجاد می گردد. منظور از نمونه برداری، اندازه گیری دامنه سیگنال در فواصل زمانی معین می باشد. از روش PAM در سیستم های مدولاسیون کد پالس (PCM^2) که یکی از روش های اصلی تبدیل اطلاعات آنالوگ به دیجیتال در شبکه های کامپیوتری است استفاده می گردد. مطابق با شکل (۲-۱۷) در فواصل زمانی معین از سیگنال آنالوگ ورودی نمونه برداری می شود و مقدار این نمونه تا نمونه برداری بعدی نگهداری می گردد. سیگنال های خروجی از عملیات PAM به تنهایی قابل ارسال نمی باشند و هنوز ماهیت آنالوگ دارند. برای تبدیل این سیگنال های آنالوگ به سیگنال های دیجیتال از روش PCM استفاده می شود. در سیستم های PCM بعد از نمونه برداری از سیگنال به روش PAM سیگنال های به دست آمده به سطوح مشخصی تقسیم بندی می شوند که این عملیات سطح بندی ^{3} نام دارد.

در شکل (۲-۱۸) نمونه ای از سیگنال سطح بندی شده که از ۲۵۵ سطح مثبت و منفی استفاده می نماید، نشان داده شده است. بعد از عملیات سطح بندی هر یک از سطوح به دست آمده به معادل باینری تبدیل می شوند. تعداد بیت های مورد استفاده در این روش به تعداد سطوح انتخاب شده بستگی دارد. به عنوان مثال چنانچه از ۲۵۵ سطح مختلف برای عملیات سطح بندی استفاده شود، به ۸ بیت برای ارسال هر یک از سطوح نیاز می باشد.

در آخرین مرحله یک سیستم PCM رشته بیت های به دست آمده با استفاده از یکی از روش های تبدیل دیجیتال به دیجیتال که در قسمت قبلی توضیح داده شد، به سیگنال های دیجیتال مناسب تبدیل شده و ارسال می گردند. بنابراین هر سیستم PCM از چهار قسمت اصلی تشکیل شده است که عبارتند از: عملیات PAM، سطح بندی، تبدیل سطوح به معادل باینری ^{4} و تبدیل اطلاعات دیجیتال به دیجیتال. در شکل (۲-۱۹) قسمت های تشکیل دهنده یک سیستم PCM نشان داده شده است.

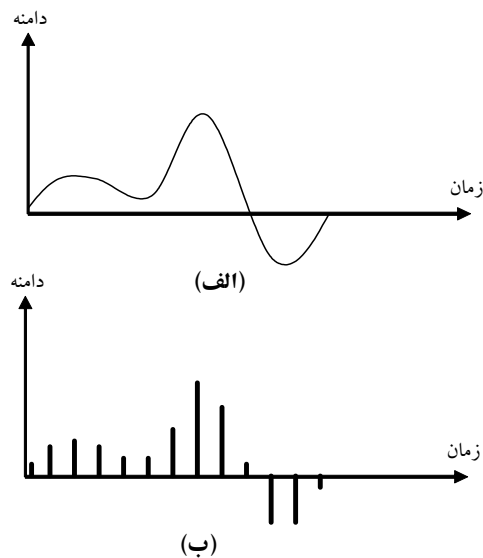
^۱ Pulse Amplitude Modulation

^۲ Pulse Cod Modulation

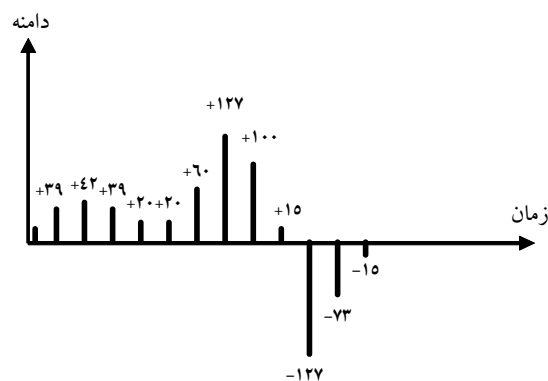
^۳ Quantization

^۴ Binary encoding

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)



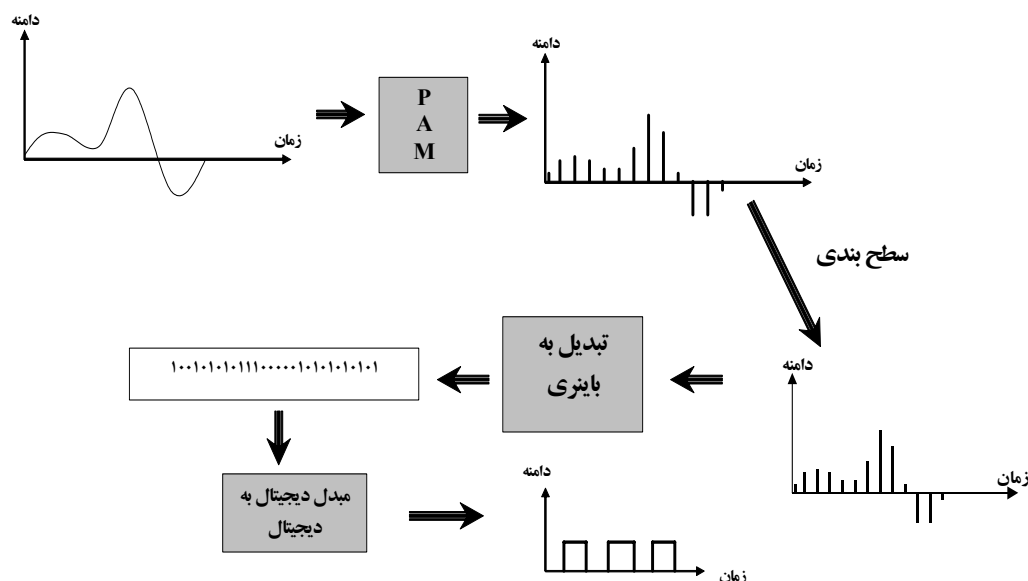
شکل (۲-۱۷): عملکرد PAM : (الف) سیگنال اولیه (ب) سیگنال نمونه برداری شده



شکل (۲-۱۸): یک سیگنال سطح بندی شده به ۲۵۵ سطح

یکی از عوامل مهم در دقت عملیات تبدیل آنا لوگ به دیجیتال، نرخ نمونه برداری و تعداد سطوح مورد استفاده می باشد. مطابق با قضیه نا یکوئیست، برای بازسازی سیگنال نمونه برداری شده PAM، باید نرخ نمونه برداری حداقل دو برابر بالاترین فرکانس سیگنال آنا لوگ اولیه باشد. به عنوان مثال در انتقال صوت انسان به وسیله سیستم PCM، از آنجایی که بالاترین فرکانس صوت انسان حدود ۳۳۰۰ هرتز است، بنابراین به تعداد ۶۶۰۰ نمونه در هر ثانیه نیاز است که در عمل برای دقت بیشتر در هر ثانیه ۸۰۰۰ نمونه برداشته می شود.

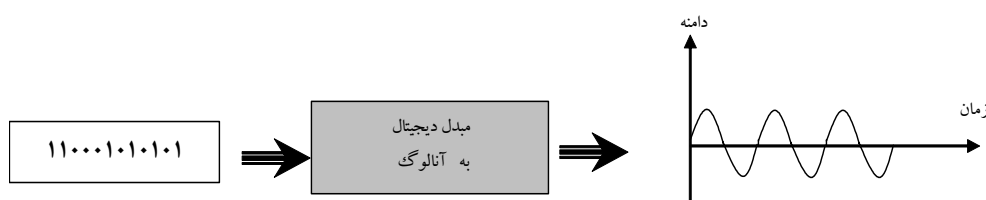
شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۲-۱۹): نمونه ای از یک سیستم PCM

۲-۳-۳- تبدیل اطلاعات دیجیتال به آنالوگ

از این نوع تبدیل، هنگام ارسال اطلاعات دیجیتال بر روی رسانه های آنالوگ استفاده می شود. به عنوان مثال چنانچه دو کامپیوتر از طریق خط تلفن آنالوگ به یکدیگر متصل شوند، در این صورت از آنجایی که اطلاعات کامپیوترها دیجیتال بوده و خطوط آنالوگ تلفن قادر به ارسال آنها نمی باشند، از مبدل های دیجیتال به آنالوگ استفاده می شود. در شکل (۲-۲۰) نمونه ای از یک سیستم تبدیل دیجیتال به آنالوگ آورده شده است.

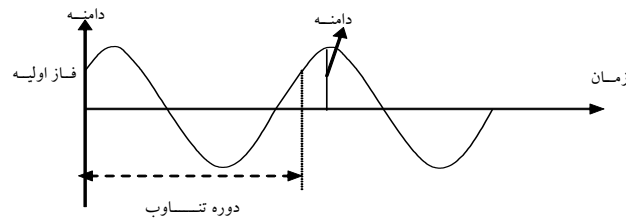


شکل (۲-۲۰): تبدیل دیجیتال به آنالوگ

روش های متعددی برای تبدیل اطلاعات دیجیتال به آنالوگ وجود دارد که در این قسمت به بررسی مهم ترین آنها که در شبکه های انتقال داده استفاده می شوند می پردازیم.

به طور کلی یک سیستم آنالوگ سینوسی به وسیله سه مشخصه اصلی که عبارتند از: دامنه، فرکانس و فاز مشخص می شود. در شکل (۲-۲۱) مثالی از یک موج سینوسی که مشخصه های فوق در آن نشان داده شده آورده شده است. چنانچه بخواهیم بیت های ۰ و ۱ دیجیتال را در یک موج سینوسی مدوله نماییم، باید یکی از سه مشخصه نامبرده فوق را تغییر دهیم.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



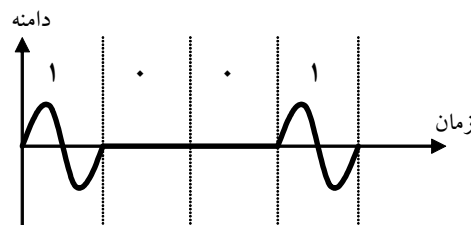
شکل (۲-۲۱): یک موج سینوسی

چهار روش اصلی تبدیل دیجیتال به آنالوگ که در سیستم های انتقال داده استفاده می شوند عبارتند از:

- مدولاسیون فرکانس (FSK^1)
- مدولاسیون دامنه (ASK^2)
- مدولاسیون فاز (PSK^3)
- مدولاسیون (QAM^4)

۲-۳-۱- مدولاسیون ASK

در روش ASK دامنه موج سینوسی ارسالی (موج حامل) متناسب با صفر یا یک بودن بیت ارسالی تغییر می کند. در شکل (۲-۲۲) مثالی از مدولاسیون ASK آورده شده است.



شکل (۲-۲۲): مثالی از مدولاسیون ASK

یکی از بزرگ ترین معایب مدولاسیون ASK، حساسیت زیاد آن به نویز می باشد. در ASK سیگنال های نویز که از پدیده های مختلفی نظیر گرما و یا القای الکترومغناطیسی ناشی می شوند، دامنه موج ارسالی را تغییر می دهند، به طوری که گیرنده ممکن است در تشخیص بیت ۰ و ۱ دچار اشکال شود. در روش متداول ASK که کلیدزنی قطع و وصل (OOK^5) نام دارد، برای ارسال بیت صفر سیگنال صفر ولت ارسال می شود. در شکل (۲-۲۳) طیف فرکانسی سیگنال ASK نشان

^۱ Frequency Shift Keying

^۲ Amplitude Shift Keying

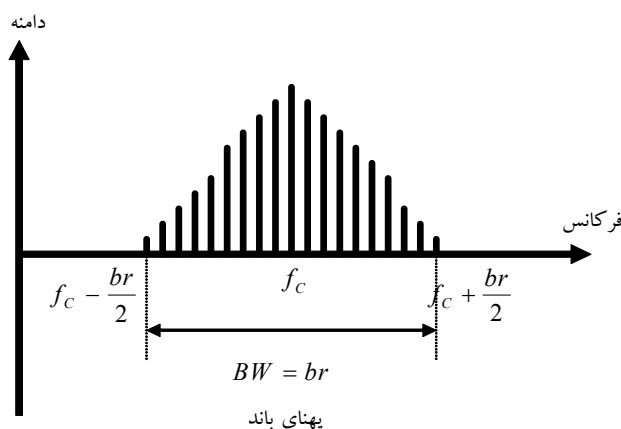
^۳ Phase Shift Keying

^۴ Quadrature Amplitude Modulation

^۵ On-Off Keying

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

داده شده است. در این شکل f_c فرکانس سیگنال حامل^۱ که همان فرکانس موج سینوسی ارسالی است، می باشد. همچنین br نشان دهنده نرخ ارسال سمبل در ASK است.

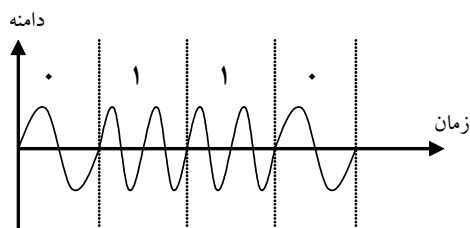


شکل (۲-۲۳): طیف فرکانسی سیگنال ASK

از آنجایی که در این مدولاسیون برای هر بیت، یک سمبل (موج سینوسی با دامنه مشخص) ارسال می شود، نرخ ارسال سمبل با نرخ ارسال بیت برابر می باشد.

۲-۳-۳-۲- مدولاسیون FSK

در مدولاسیون FSK فرکانس سیگنال سینوسی ارسالی متناسب با ۰ و ۱ بودن بیت ارسالی تغییر می کند. در این مدولاسیون دامنه و فاز موج ارسالی ثابت بوده ولی فرکانس آن متغیر است. در شکل (۲-۲۴) مثالی از مدولاسیون FSK نشان داده شده است. مطابق با شکل فوق در مدولاسیون FSK برای ارسال بیت صفر، یک موج سینوسی با فرکانس f_{c0} و برای ارسال بیت ۱، یک منبع سینوسی با همان دامنه و فاز قبلی ولی با فرکانس f_{c1} ارسال می گردد.



شکل (۲-۲۴): مثالی از مدولاسیون FSK

معمولاً فرکانس منبع ارسالی برای بیت ۱ از فرکانس موج ارسالی بیت ۰ بیشتر است.

مهم ترین برتری FSK به ASK، مصونیت آن در مقابل نویز می باشد. نویزهای کانال های مخابراتی فقط دامنه سیگنال را تغییر می دهند و فرکانس آن بدون تغییر می ماند، بنابراین گیرنده قادر به تشخیص فرکانس موج دریافتی می باشد و نویز کانال در آن اثری ندارد. در شکل (۲-۲۵) طیف فرکانسی سیگنال FSK نشان داده شده است. مطابق با

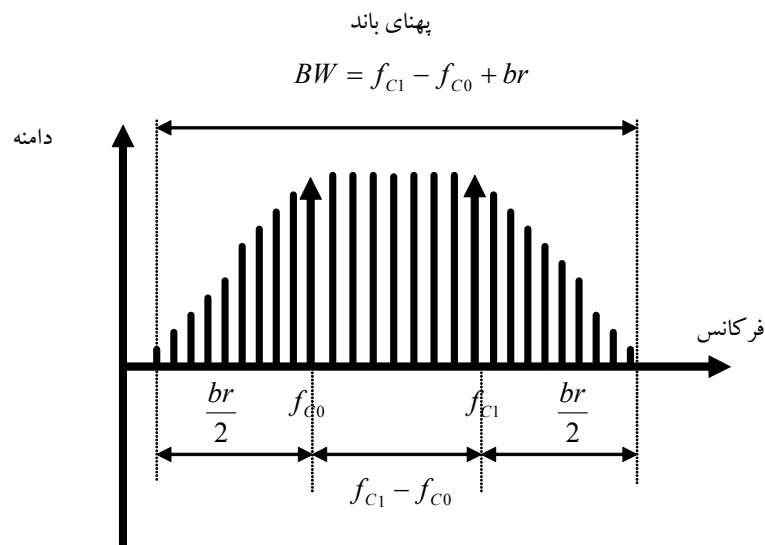
^۱ Carrier

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

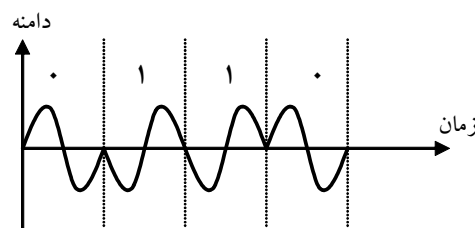
شکل فوق ، پهنای باند FSK برابر با $f_{c1} - f_{c0} + br$ می باشد که در آن br نرخ ارسالی سمبل در مدولاسیون FSK است که با نرخ ارسال بیت برابر است .

۲-۳-۳-۲ مدولاسیون PSK

در مدولاسیون PSK ، فاز سیگنال سینوسی ارسالی متناسب با ۰ و یا ۱ بودن بیت ارسالی تغییر می کند. در مدولاسیون PSK دامنه و فرکانس موج سینوسی ارسالی ثابت می باشد. در شکل (۲-۲۶) مثالی از مدولاسیون PSK آورده شده است .



شکل (۲-۲۵): طیف فرکانسی مدولاسیون FSK

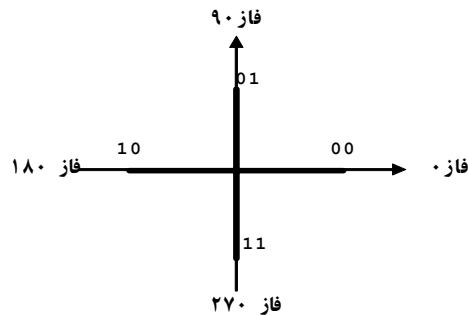


شکل (۲-۲۶): مثالی از مدولاسیون PSK

مطابق با شکل فوق، در مدولاسیون PSK برای ارسال بیت ۰ موج سینوسی با فاز صفر و برای ارسال بیت ۱، یک منبع سینوسی با فاز ۱۸۰ درجه ارسال می شود. از آنجایی که در این روش از دو فاز صفر و ۱۸۰ درجه استفاده می گردد، به این روش PSK یا PSK۲ باینری نیز گفته می شود . همانند FSK، سیگنال های PSK نیز در مقابل نویز از مصونیت بالایی برخوردار می باشند . چنانچه از ۴ فاز ۰، ۹۰، ۱۸۰ و ۲۷۰ درجه برای ارسال سیگنال PSK استفاده شود. در این صورت می توان هر دو بیت متوالی را به وسیله یک سمبل PSK ارسال نمود که باعث افزایش سرعت ارسال می شود. همچنین با افزایش فازهای ارسالی می توان به سرعت های بالاتر نیز دسترسی پیدا کرد. در شکل (۲-۲۷) دیاگرام فازی مدولاسیون های PSK 4- و PSK 8- که به ترتیب از ۴ و ۸ فاز متفاوت برای ارسال بیت ها استفاده می کنند نشان داده شده است.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

در شکل (۲-۲۸) طیف فرکانسی سیگنال PSK نشان داده شده است. مطابق با شکل فوق، پهنای باند PSK مشابه ASK بوده و برابر br می باشد. البته در مدولاسیون های 4-PSK و 8-PSK، مقدار br به ترتیب دو برابر و سه برابر نرخ ارسال بیت است.



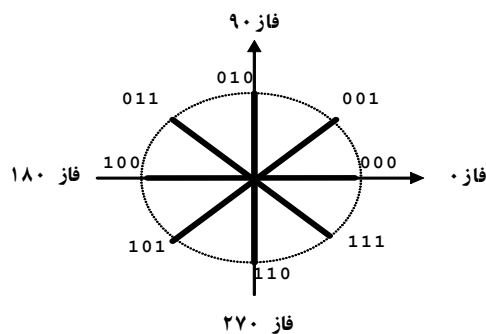
(الف)

شکل (۲-۲۷): دیگرام

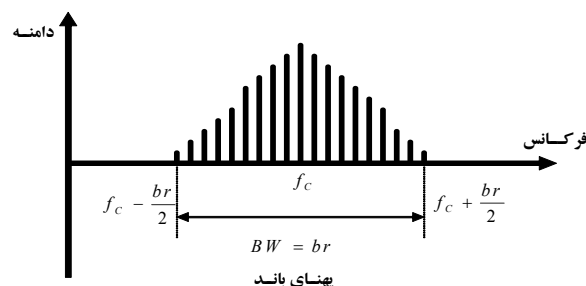
فازی: الف (مدولاسیون 4-

PSK ب) مدولاسیون 8-

PSK



(ب)



شکل (۲-۲۸): طیف فرکانسی سیگنال PSK

۲-۳-۳-۴ - مدولاسیون QAM

در مدولاسیون ASK، FSK و PSK فقط یکی از مشخصه های سیگنال سینوسی (به ترتیب دامنه، فرکانس و فاز) تغییر می نماید و دو مشخصه دیگر ثابت می باشند. چنانچه مدولاسیون های ASK و PSK با یکدیگر ترکیب شوند، مدولاسیون جدیدی به نام QAM ایجاد می شود. در QAM اطلاعات ارسالی هم در فاز و هم در دامنه می باشد. در شکل (۲-۲۹) مثالی از دیگرام فازی می باشد. حالت های مختلف QAM آورده شده است. حداقل پهنای باند لازم برای QAM

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

مشابه ASK و PSK می باشد. در جدول (۲-۲) رابطه بین نرخ ارسال بیت و نرخ ارسال سمبل در مدولاسیون های مختلف نشان داده شده است.

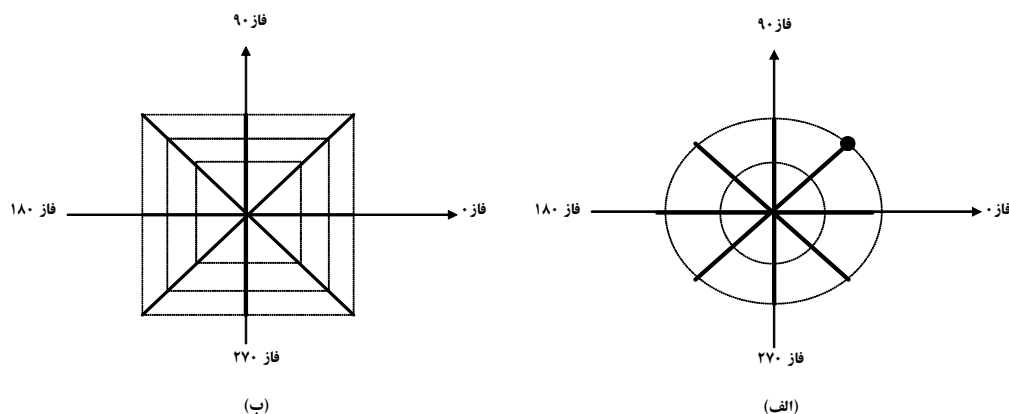
جدول (۲-۲): رابطه بین نرخ ارسال بیت و نرخ ارسال سمبل در مدولاسیون های مختلف

نوع مدولاسیون	نرخ بیت	نرخ سمبل
ASK, FSK و PSK-۲	N	N
4-PSK, 4-QAM	2N	N
8-PSK, 8-QAM	3N	N
16-QAM	4N	N
32-QAM	5N	N
64-QAM	6N	N
128-QAM	7N	N
256-QAM	8N	N

۲-۳-۴ تبدیل اطلاعات آنالوگ به سیگنال های آنالوگ

برای ارسال اطلاعات آنالوگ بر روی رسانه های انتقال آنالوگ، از مدولاسیون های آنالوگ به آنالوگ استفاده می شود. در شکل (۲-۳۰) نمونه ای از یک سیستم تبدیل آنالوگ به آنالوگ نشان داده شده است. سه روش اصلی برای تبدیل اطلاعات آنالوگ به سیگنال های آنالوگ وجود دارد که عبارتند از:

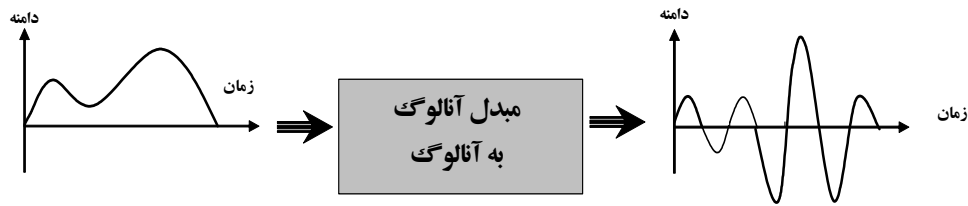
- مدولاسیون دامنه (AM^1)
- مدولاسیون فرکانس (FM^2)
- مدولاسیون فاز (PM^3)



شکل (۲-۲۹): دیاگرام فازی QAM (الف) ۲ دامنه و ۸ فاز (ب) ۴ دامنه و ۸ فاز

^۱ Amplitude Modulation
^۲ Frequency Modulation
^۳ Phase Modulation

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

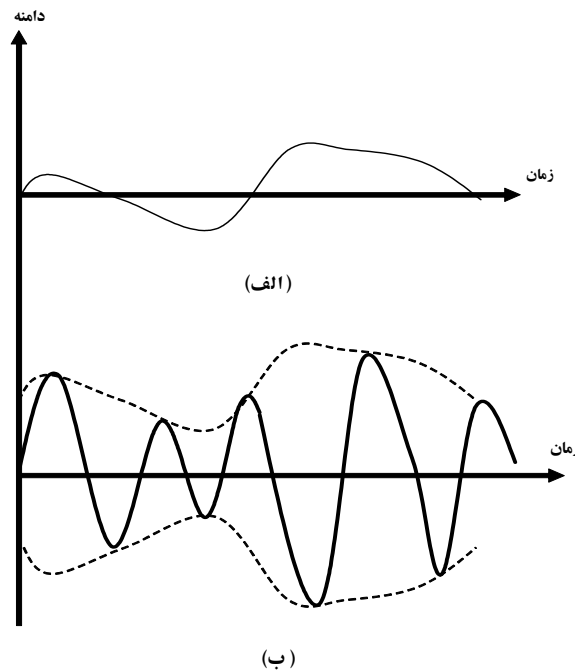


شکل (۲-۳۰): تبدیل آنالوگ به آنالوگ

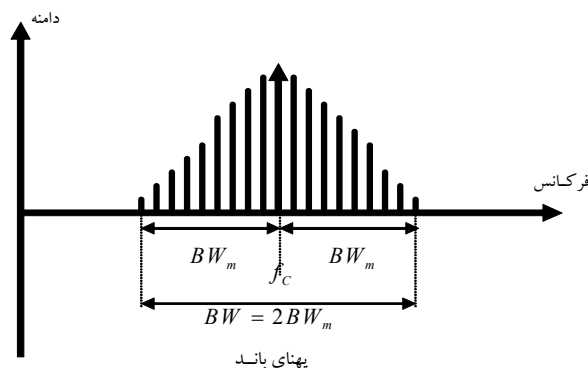
۲-۳-۴-۱- مدولاسیون AM

در ارسال AM، سیگنال حامل طوری مدوله می شود که دامنه آن متناسب با سیگنال پایه ارسالی تغییر می کند. فرکانس و فاز سیگنال حامل ثابت می باشد و فقط دامنه آن متناسب با دامنه موج پایه ارسالی تغییر می کند. در شکل (۲-۳۱) مثالی از مدولاسیون AM آورده شده است.

در شکل (۲-۳۲)، طیف فرکانسی سیگنال AM نشان داده شده است.



شکل (۲-۳۱): مثالی از مدولاسیون AM (الف) سیگنال پایه (ب) سیگنال مدوله شده



شکل (۲-۳۲): طیف فرکانسی سیگنال AM

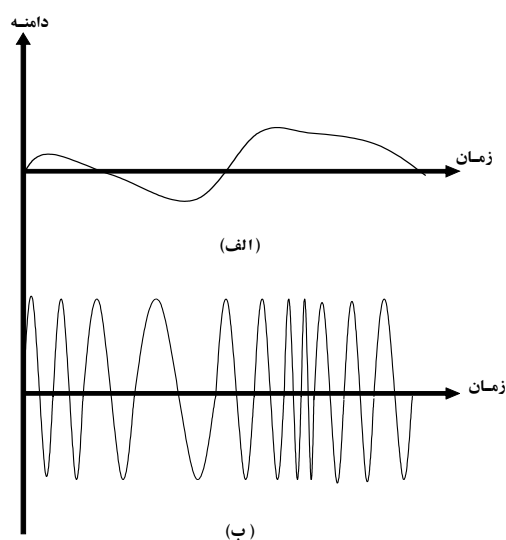
شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

مطابق با شکل فوق، پهنای باند سیگنال AM دو برابر پهنای باند سیگنال پایه ارسالی (BW_m) می باشد. به عنوان مثال پهنای باند سیگنال های صوتی، معمولاً حدود ۵ کیلو هرتز است. بنابراین یک ایستگاه رادیویی AM به پهنای باند حدود ۱۰ کیلو هرتز نیاز دارد. در ایستگاه های رادیویی AM از فرکانسهای بین ۵۳۰ کیلو هرتز تا ۱۷۰۰ کیلو هرتز استفاده می شود. هر ایستگاه AM به حدود ۱۰ کیلو هرتز پهنای باند نیاز دارد، بنابراین در محدوده فرکانسی فوق حدود ۱۱۸ ایستگاه رادیو AM قابل استفاده می باشد.

۲-۴-۳-۲- مدولاسیون FM

در مدولاسیون FM فرکانس موج حامل، متناسب با سیگنال ارسالی باند پایه تغییر می نماید. در شکل (۲-۳۳) مثالی از مدولاسیون FM آورده شده است. همان طور که در شکل (۲-۳۳) مشاهده می شود، در سیگنال ارسالی دامنه و فاز ثابت می ماند و فقط فرکانس موج حامل متناسب با سیگنال پایه ارسالی تغییر می نماید.

در شکل (۲-۳۴) طیف فرکانسی سیگنال FM نشان داده شده است. سیگنال FM دارای پهنای باند ۱۰ برابر پهنای باند سیگنال پایه ارسالی می باشد. به عنوان مثال پهنای باند سیگنال صوت استریو حدود ۱۵ کیلو هرتز است، بنابراین هر ایستگاه FM به پهنای باند حدود ۱۵۰ کیلو هرتز نیاز دارد. البته برای جلوگیری از تداخل فرکانسی ایستگاه های مجاور FM، ۵۰ کیلو هرتز پهنای باند محافظ نیز در هر ایستگاه FM در نظر گرفته می شود؛ که در نتیجه هر ایستگاه FM حدود ۲۰۰ کیلو هرتز پهنای باند نیاز دارد. در ایستگاه های رادیویی FM از محدوده فرکانسی ۸۸ مگاهرتز تا ۱۰۸ مگاهرتز استفاده می شود. از آنجایی که هر ایستگاه FM به ۲۰۰ کیلو هرتز پهنای باند نیاز دارد، بنابراین در محدوده فرکانسی فوق حدود ۱۰۰ ایستگاه FM قابل استفاده است.

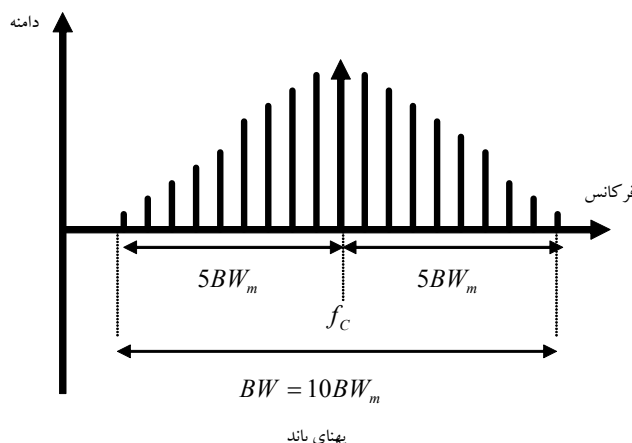


شکل (۲-۳۳): مثالی از مدولاسیون FM: (الف) سیگنال پایه (ب) سیگنال مدوله شده

۲-۴-۳-۳- مدولاسیون PM

در مدولاسیون PM، فاز موج ارسالی متناسب با سیگنال پایه ارسالی تغییر می نماید. دامنه و فرکانس موج ارسالی PM ثابت می باشد. پهنای باند PM مشابه FM است.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۲-۳۴): طیف فرکانسی FM

۲-۴- واسطه های دیجیتال

برای انتقال اطلاعات دیجیتال کامپیوترها بر روی کانال های ارتباطی، نیاز به واسطه های دیجیتال می باشد. به عنوان مثال چنانچه بخواهیم اطلاعات دیجیتال یک کامپیوتر را بر روی خطوط آنالوگ تلفن ارسال کنیم، نیاز به واسطه مشخص و همچنین وسیله ای به نام مودم برای انتقال اطلاعات کامپیوتر به خط تلفن داریم.

جهت ارسال اطلاعات در کامپیوترها دو روش موازی و سری وجود دارد. در روش ارسال موازی، داده های ۰ و ۱ باینری به صورت گروه های چندبیتی درآمده و یکجا ارسال می گردند، که باعث افزایش نرخ ارسال بیت می شود. حداکثر ارسال داده ها به روش موازی ۲۵ فوت است. در روش ارسال سری، داده های ارسالی بیت به بیت یکی پس از دیگری ارسال می گردند. بنابراین در این روش تنها به یک کانال ارتباطی نیاز می باشد که از مزایای عمده روش ارسال سری است. ارسال اطلاعات سری به روش غیرهمزمان^۱ و همزمان صورت می گیرد که به بررسی هر یک از این روش ها می پردازیم.

۲-۴-۱- روش غیر همزمان

در این روش زمان بندی سیگنال ارسالی مهم نمی باشد و داده های ارسالی به صورت بایت به بایت ارسال می گردند. از آنجایی که در روش غیر همزمان سیگنال ساعت^۲ عملاً بین فرستنده و گیرنده مبادله نمی شود، برای جداسازی و تشخیص داده های ارسالی در گیرنده، فرستنده یک سری بیت هایی به هر بایت ارسالی اضافه می نماید. بدین منظور در ابتدای هر بایت یک بیت صفر به عنوان بیت شروع^۳ و در پایان هر بایت، ۱ یا ۱/۵ و یا ۲ بیت ۱ به عنوان بیت پایان^۴ اضافه می شود. با استفاده از بیت های شروع و پایان، عملاً گیرنده قادر به جداسازی بایت های ارسالی از یکدیگر می باشد. علاوه بر بیت های فوق، معمولاً بین هر دو بایت متوالی، کانال ارسال در حالت بی کار^۵ به سر می برد. در شکل (۲-۳۵) نمونه ای از ارسال غیرهمزمان نشان داده شده است.

^۱ Asynchronous

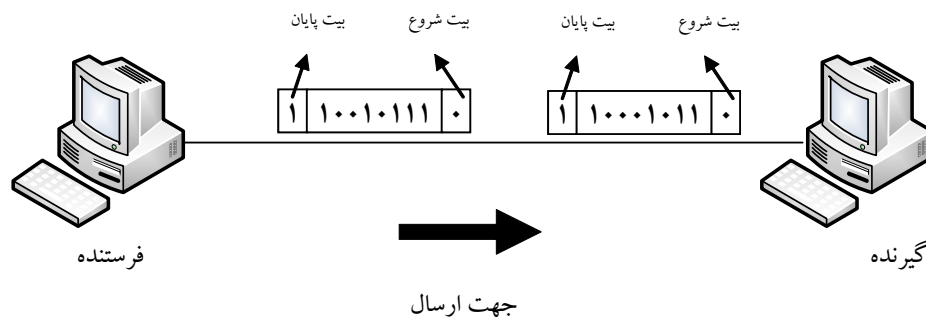
^۲ Clock

^۳ Start bit

^۴ Stop bit

^۵ Idle

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۲-۳۵): مثالی از ارسال غیرهمزمان

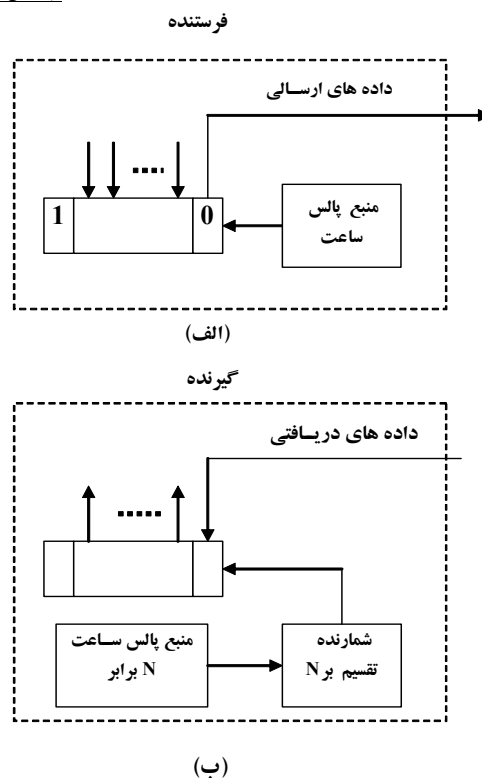
در روش غیرهمزمان، فرستنده و گیرنده از مولد پالس ساعت مستقل از یکدیگر و به طور محلی استفاده می نمایند. این روش برای سرعت های پایین و در مواردی که ارسال کاراکترها به صورت تصادفی (مثل تایپ کردن بر روی صفحه کلید) می باشد، استفاده می گردد. اضافه کردن بیت های شروع و پایان، باعث افزایش بالا سری و کاهش سرعت ارسال روش غیر همزمان می گردد.

ساختار فرستنده و گیرنده روش غیرهمزمان در شکل (۲-۳۶) نشان داده شده است. مطابق با این شکل، داده های ارسالی فرستنده داخل یک شیفت رجیستر ¹PISO به صورت موازی قرار می گیرند و به صورت سری با هر پالس ساعت بیت به بیت از آن خارج می شوند. در سمت گیرنده، برای اطمینان از صحت دریافت بیت ها، از یک منبع پالس ساعت با فرکانس N برابر فرکانس منبع پالس ساعت فرستنده استفاده می شود. (معمولاً $N = 16$ اختیار می گردد).

گیرنده از یک شیفت رجیستر ²SIPO، برای دریافت اطلاعات به صورت سری و تبدیل آنها به صورت موازی استفاده می نماید. از یک شمارنده تقسیم بر N برای تبدیل فرکانس منبع پالس ساعت گیرنده به مقداری مساوی با فرکانس پالس ساعت فرستنده استفاده می شود.

¹ Parallel-In, Serial-Out
² Serial-In, Parallel-Out

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۲-۳۶): ساختار روش غیرهمزمان (الف) فرستنده (ب) گیرنده

۲-۴-۲ روش همزمان

در روش همزمان رشته بیت های ارسالی به صورت قاب هایی به طول مشخص که شامل چندین بیت می باشد، ارسال می گردند. در این روش بین بایت های ارسالی موجود در قاب هیچ گونه فاصله زمانی (که در روش غیر همزمان وجود داشت) وجود ندارد. در شکل ۲-۳۷ نمونه ای از ارسال همزمان نشان داده شده است. از این روش برای ارسال حجم زیادی از داده ها با سرعت بالا استفاده می شود.

در این روش در آغاز و پایان هر قاب از یک یا چند کاراکتر کنترلی خاص که منحصر به فرد بوده و در ناحیه داده های کاربران وجود ندارد، برای تعیین شروع و پایان هر قاب استفاده می شود.



شکل (۲-۳۷): مثالی از ارسال همزمان

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

از آنجایی که در روش همزمان ازبیت شروع و پایان درهربایت استفاده نمی شود و همچنین با توجه به سرعت بالای ارسال در این روش، برای همزمانی بیت و استخراج صحیح اطلاعات ازهرقاب، نیاز به حفظ همزمانی پالس ساعت درفرستنده و گیرنده حس می گردد. بدین منظور ازروش های کدینگ دیجیتال به دیجیتال نظیر روش منچستر وهمچنین مدار $DPLL^1$ برای همزمان سازی پالس ساعت گیرنده با فرستنده استفاده می شود.

۲-۴-۳- واسط DTE به DCE

در شبکه های کامپیوتری به تجهیزاتی نظیر کامپیوترها، چاپگرها و ماشین های فاکس، تجهیزات پایانه داده (DTE^2) گفته می شود. همچنین تجهیزاتی مثل مودم که برای ارسال داده های DTE ها به کار می روند؛ تجهیزات مخابره داده یا تجهیزات پایان دهنده مدار (DCE^3) نام دارند. برای ارتباط بین DTE و DCE باید از استانداردهای خاصی استفاده نمود. مطابق با شکل (۲-۳۸)، اتصال DTE به DCE توسط استانداردهای مشخصی صورت می گیرد. هر استاندارد مدل خاصی را برای مشخصات مکانیکی، الکتریکی و عملیاتی تعریف می نماید. در این راستا سازمان جهانی ITU-T استانداردهای سری V (مثل V.24) و سری X را وضع نموده است. همچنین از سوی سازمان EIA نیز استانداردهایی نظیر EIA-232، EIA-449 و EIA-442 برای ارتباط بین DTE و DCE وضع شده است. یکی از متداول ترین و مهم ترین استانداردهای واسط DTE به DCE، استاندارد EIA-232 می باشد. این استاندارد که تا حد زیادی مشابه استاندارد CCITT V.24 است، برای ارتباط یک DTE مثل کامپیوتر به یک DCE نظیر مودم به کار می رود که به بررسی آن می پردازیم. لازم به توضیح است که مودم وسیله ای می باشد که امکان انتقال اطلاعات دیجیتال کامپیوترها را از طریق خطوط آنالوگ تلفن فراهم می آورد که درقسمت های بعدی به توصیف عملکرد آنها خواهیم پرداخت.



شکل (۲-۳۸): واسط DTE به DCE

۲-۴-۳-۱- واسط EIA-232

استاندارد EIA-232 (که با نام قبلی آن یعنی RS-232 نیز شناخته شده می باشد)، دارای دو نوع کانکتور مختلف ۲۵ پین (DB-25) و ۹ پین (DB-9) است. هریک از کانکتورهای فوق نیز دو نوع می باشند که عبارتند: از کانکتور نری ⁴ و کانکتور مادگی ⁵. در شکل (۲-۳۹) نمونه ای از کانکتورهای DB-25 و DB-9 آورده شده است.

¹ Digital Phase Lock Loop

² Data Terminal Equipment

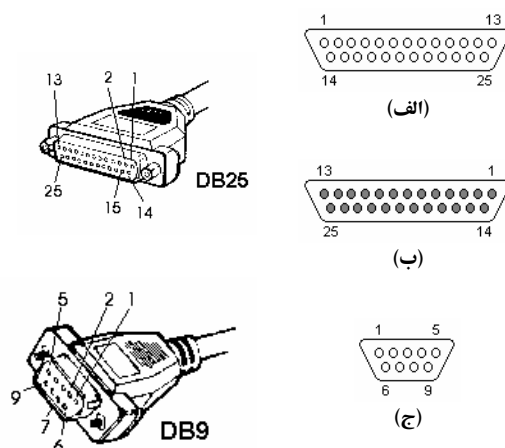
³ Data Circuit Terminating Equipment

⁴ Male connector

⁵ Female connector

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

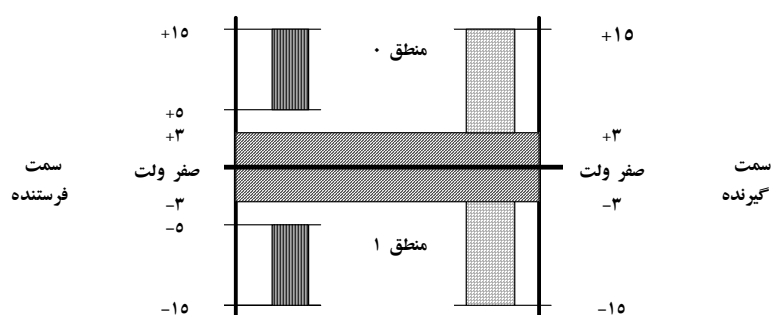
در کانکتور نوع DB-25، از ۲۵ رشته سیم برای تبادل اطلاعات و سیگنال های کنترلی استفاده می شود. برای ارسال داده ها از طریق این کانکتور، بیت ۱ با سطح ولتاژ بین ۳- تا ۱۵- و بیت ۰ با سطح ولتاژ بین ۳+ و ۱۵+ نشان داده می شوند. ناحیه بین ۳- تا ۳+ ناحیه غیرمجاز و تعریف نشده می باشد. در DB-25 فقط از چهار پین آن برای ارسال و دریافت داده ها استفاده می شود و ۲۱ پین باقی مانده برای عملیات کنترلی نظیر کنترل DTE و DCE، زمان بندی^۱، تعیین سطح ولتاژ صفر و عملیات تست استفاده می گردد.



شکل (۲-۳۹): انواع کانکتورهای EIA 232

الف) کانکتور DB25 نری (ب) کانکتور DB25 مادگی (ج) کانکتور DB9

در شکل (۲-۴۰) سطوح ولتاژ منطق ۰ و ۱ در استاندارد RS232 نشان داده شده است.



شکل (۲-۴۰): سطوح ولتاژ منطق ۰ و ۱ در استاندارد RS232

حداکثر نرخ بیت ارسالی در استاندارد EIA-232، ۲۰ کیلو بیت بر ثانیه می باشد. مهم ترین پین های DB-25 به شرح زیر است:

- پین شماره (۲)، داده های ارسالی^۲: توسط این پین داده های ارسالی DTE تحویل DCE می شود، تا آنها را ارسال کند.

^۱Timing

^۲Transmitted data

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

- **پین شماره (۳)، داده های دریافتی^۱** : این پین حاوی داده های دریافتی DCE می باشد که از طریق آن به DTE ارسال می شود.
 - **پین شماره (۴)، درخواست ارسال DTE (RTS^۲)** : با فعال شدن این پین، درخواست ارسال داده از طرف DTE به اطلاع DCE رسانده می شود.
 - **پین شماره (۵)، آمادگی ارسال DCE (CTS^۳)** : هنگامی که DCE درخواست ارسال DTE را دریافت نماید و آماده انتقال اطلاعات DTE باشد، با فعال کردن این پین آمادگی خود را به اطلاع DTE می رساند.
 - **پین شماره (۶)، آمادگی DCE^۴** : هنگامی که DCE آماده کار باشد، این پین فعال می شود. معمولاً با روشن شدن DCE این پین نیز فعال می گردد.
 - **پین شماره (۷)، زمین مشترک سیگنال^۵** : برای آن که دو وسیله الکترونیکی را به یکدیگر متصل نماییم؛ طوری که قادر به تبادل اطلاعات با یکدیگر باشند، در اولین قدم باید سطح مرجع ولتاژ صفر (زمین) آنها را یکسان کنیم. از طریق این پین زمین مشترک DTE و DCE یکسان می شود.
 - **پین شماره (۸)، آشکارساز سیگنال دریافتی از خط^۶** : هنگامی که DCE متوجه وجود سیگنال در خط شود، با فعال کردن این پین به اطلاع DTE می رساند که داده های دریافتی در خط وجود دارند.
 - **پین شماره (۲۰) آمادگی DTE^۷** : DTE با فعال کردن این پین به اطلاع DCE می رساند که آماده کار می باشد. معمولاً با روشن شدن DTE این پین نیز فعال می شود.
- البته به غیر از پین های فوق که شرح مختصری از آنها آورده شد، پین های دیگری نیز وجود دارد که از اهمیت کمتری برخوردارند. به همین دلیل با کاهش پین های کم مصرف DB-25، کانکتور DB-9 که فقط ۹ سیم دارد، ساخته شده است. مراحل کار در ارتباط یک DTE مثل کامپیوتر به یک DCE مثل مودم به شرح زیر است:
- مرحله ۱- تهیه مقدمات:** در اولین مرحله برقراری ارتباط بین دو کامپیوتر از طریق دو مودم، مقدمات اولیه که اتصال دو زمین کامپیوتر و مودم به یکدیگر است انجام می شود. |||| آمادگی h hhh HH
- مرحله ۲- آمادگی:** در این مرحله، آمادگی هر ۴ وسیله (دو کامپیوتر و دو مودم)، در طرف فرستنده و گیرنده بررسی می شود. بدین منظور هر دو کامپیوتر فرستنده و گیرنده اعلام آمادگی خود را از طریق پین شماره ۲۰ به اطلاع مودم می رسانند. مودم ها نیز در پاسخ به ارسال پیام فوق، با فعال کردن پین شماره ۶، اعلام آمادگی متقابل خود را به کامپیوترها می رسانند.
- مرحله ۳- برقراری ارتباط:** در این مرحله یک اتصال فیزیکی بین مودم های فرستنده و گیرنده برقرار می شود. بدین منظور ابتدا کامپیوتر فرستنده از طریق پین شماره ۴، اعلام درخواست خود را برای مودم ارسال می دارد و به دنبال آن مودم فرستنده نیز یک سیگنال حامل برای مودم طرف مقابل ارسال می کند. وقتی که مودم مقابل سیگنال حامل فوق را دریافت کرد، از طریق پین شماره ۸، وقوع احتمالی ارسال داده را به کامپیوتر متصل به خود اطلاع می دهد. کامپیوتر گیرنده نیز با فعال سازی پین شماره ۴ اعلام آمادگی خود را به مودم ارسال می دارد و مودم نیز یک سیگنال حامل برای

^۱ Received data

^۲ Request To Send

^۳ Clear To Send

^۴ DCE ready

^۵ Signal ground common return

^۶ Received Line Signal Detector

^۷ DTE ready

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

مودم فرستنده ارسال می کند . در پاسخ به درخواست ارسال هر دو کامپیوتر، مودم های فرستنده و گیرنده نیز از طریق پین شماره ۵، اعلام آمادگی ارسال خود را به اطلاع کامپیوتر می رسانند .

مرحله ۴ - ارسال داده ها : در این مرحله داده های دیجیتال بین دو کامپیوتر فرستنده و گیرنده مبادله می شود. بدین منظور کامپیوتر فرستنده از طریق پین شماره ۲ داده های ارسالی خود را برای ارسال به مودم تحویل می دهد . همچنین از طریق پین شماره ۲۴، سیگنال زمان بندی بین کامپیوتر و مودم ارسال می شود . داده های ارسالی توسط مودم به صورت سیگنال های آنالوگ دریافتی به دیجیتال تبدیل می شوند و از طریق پین شماره ۳ تحویل کامپیوتر می گردند .

مرحله ۵ - قطع ارتباط : بعد از ارسال داده ها توسط دو طرف و اتمام داده های ارسالی، هر دو کامپیوتر پین درخواست خود را غیر فعال می سازند و به این ترتیب مودم ها نیز سیگنال حامل ارسالی را خاموش کرده و پین های شماره ۸ و ۵ خود را غیر فعال می سازند.

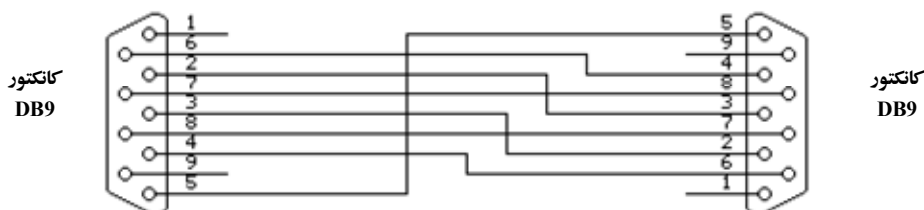
در شکل (۲-۴)، مراحل برقراری ارتباط، ارسال داده ها و قطع ارتباط در یک مودم یک طرفه نشان داده شده است.



شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

شکل (۲-۴۱): مراحل کار یک ارتباط در مودم های یک طرفه

چنانچه بخواهیم دو DTE را به طور محلی بدون استفاده از مودم به یکدیگر متصل نماییم، در این صورت نیاز به کابل نال مودم داریم. در شکل (۲-۴۲) نمونه ای از یک کابل نال مودم با استفاده از کانکتور DB9 نشان داده شده است.



شکل (۲-۴۲): کابل نال مودم

۲-۴-۴ - مودم

یکی از تجهیزات ارتباطی در شبکه های کامپیوتری مودم می باشد. با استفاده از این وسیله امکان تبادل فایل ها بین کامپیوترها، اتصال به اینترنت و ارسال و دریافت فاکس فراهم می آید. مودم در حقیقت ترکیبی از دو کلمه مدولاتور^۱ و دی مدولاتور^۲ می باشد. اطلاعات دیجیتال کامپیوترها توسط مودم تبدیل به سیگنال های آنالوگ قابل ارسال در شبکه تلفن می گردد. در سمت گیرنده نیز، اطلاعات آنالوگ دریافتی تبدیل به اطلاعات دیجیتال می شود و تحویل کامپیوتر می گردد. بنابراین برای استفاده از مودم نیاز به یک خط تلفن می باشد.

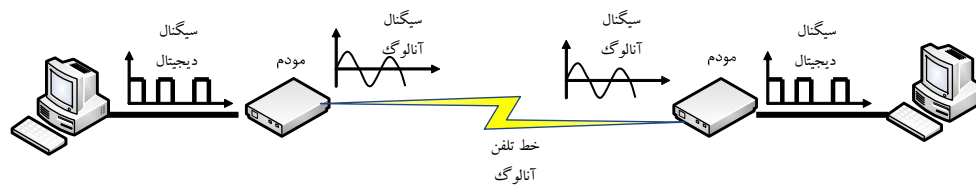
مودم ها به دو دسته داخلی و خارجی تقسیم می شوند. مودم های داخلی، در داخل کامپیوتر بر روی یکی از اسلات های آن نصب می شوند. مودم های خارجی، خارج از کامپیوتر می باشند و مستقل عمل می کنند. این مودم ها از طریق کابل سریال RS 232 به کامپیوتر متصل می شوند. سرعت مودم ها متفاوت می باشد و در حدود ۳۰۰۰ تا بالاتر از ۵۶۰۰۰ بیت بر ثانیه است. به غیر از مودم های تلفنی، مودم های دیگری نیز وجود دارند که بر روی خطوط استیجاری^۳ فعال می باشند.

علاوه بر عملیات تبدیل اطلاعات دیجیتال به آنالوگ و بالعکس، هر مودم عملیات دیگری نظیر کنترل خطا و فشرده سازی اطلاعات را نیز بر عهده دارد. در شکل (۲-۴۳) نمونه ای از عملیات یک مودم نشان داده شده است.

مودم ها از تکنیک های تبدیل دیجیتال به آنالوگ نظیر ASK, FSK, PSK و QAM استفاده می کنند. پهنای باند خطوط تلفن برای انتقال داده های دیجیتال حدود ۲۴۰۰ هرتز می باشد که بسته به نوع عملکرد مودم (یک طرفه و یا کاملاً دوطرفه) و همچنین با توجه به روش تبدیل دیجیتال به آنالوگ مورد استفاده در مودم، سرعت های متفاوتی برای عملکرد مودم ها وجود دارد. در جدول (۲-۳) نرخ بیت ارسالی مودم ها بر اساس نوع مدولاسیون و نحوه عملکرد آنها آورده شده است. امروزه اکثر استانداردهای مودم های موجود، براساس ITU-T می باشند. در جدول (۲-۴) مشخصات برخی از مودم های ITU-T آورده شده است.

^۱ Modulator
^۲ Demodulator
^۳ leased line

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)



شکل (۲-۴۳): عملیات

مودم

جدول (۲-۳): نرخ ارسال مودمها برحسب نوع مدولاسیون آنها

نوع مدولاسیون	سرعت ارسال یک طرفه (بیت بر ثانیه)	سرعت ارسال دو طرفه (بیت بر ثانیه)
ASK,FSK,2-PSK	۲۴۰۰	۱۲۰۰
4-PSK , 4-QAM	۴۸۰۰	۲۴۰۰
8-PSK , 8-QAM	۷۲۰۰	۳۶۰۰
16- QAM	۹۶۰۰	۴۸۰۰
32- QAM	۱۲۰۰۰	۶۰۰۰
64- QAM	۱۴۴۰۰	۷۲۰۰
128- QAM	۱۶۶۰۰	۸۴۰۰

جدول (۲-۴): مشخصات برخی از مودمهای ITU-T

استاندارد	نوع عملکرد مودم	نرخ ارسال (بیت بر ثانیه)
V.21	دوطرفه	۳۰۰
V.22	دوطرفه	۱۲۰۰
V.22bis	دوطرفه	۲۴۰۰
V.29	یک طرفه	۹۶۰۰
V.32	دوطرفه	۹۶۰۰
V.32bis	دوطرفه	۱۴۴۰۰
V.32terbo	دوطرفه	۱۹۲۰۰
V.34	دوطرفه	۲۸۸۰۰
V.34bis	دوطرفه	۳۳۶۰۰
V.42bis	دوطرفه	۳۴۰۰۰
V.90	دوطرفه	۵۶۰۰۰
V.92	دوطرفه	۵۶۰۰۰

۲-۴-۴-۱- مودمهای هوشمند

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

بسیاری از مودم های امروزه مجهز به نرم افزاری می باشند که به وسیله آن قادر به پشتیبانی از قابلیت های مختلفی هستند. این نوع مودم ها که به نام مودم های هوشمند معروف می باشند، برای اولین بار توسط شرکت میکرو کامپیوتری Hayes معرفی گردیدند. امروزه مودم های سازگار با Hayes توسط شرکت های کامپیوتری متعددی وارد بازاری می شوند. مودم های هوشمند توسط دستورات AT کنترل و برنامه ریزی می شوند. شکل کلی این دستورات به شرح زیر است:

... , [مشخصه ها] دستور [مشخصه ها] دستور AT

مهم ترین دستورات AT در جدول (۲-۵) آورده شده است.

جدول (۲-۵): مهم ترین دستورات AT

دستور	مفهوم دستور	مشخصه ها
A	مودم را در حالت پاسخ گویی قرار می دهد	-----
B	مودم را در حالت کاری V.22bis در سرعت ۱۲۰۰ بیت بر ثانیه قرار می دهد	-----
D	شماره گیری	شماره مورد نظر
E	فعال سازی / غیر فعال سازی حالت اکو	۰ یا ۱
H	مودم را در حالت on/off hook قرار می دهد	۰ یا ۱
L	تنظیم شدت صدای بلندگو	N
P	استفاده از شماره گیری پالس	-----
T	استفاده از شماره گیری تن	-----

۲-۵- معرفی رسانه های انتقال

در این قسمت، رسانه های مختلفی که در انتقال داده و شبکه های کامپیوتری برای ارسال اطلاعات استفاده می شوند توصیف می گردند. در حالت کلی دو نوع رسانه انتقال در شبکه های کامپیوتری وجود دارد که عبارتند از: رسانه های هدایت شونده^۱ و رسانه های غیرهدایت شونده^۲. چنانچه دو کامپیوتر توسط رسانه های هدایت شونده به یکدیگر متصل شوند، در این صورت یک کانال بین دو کامپیوتر متصل شده به یکدیگر وجود دارد. رسانه هایی نظیر زوج سیم به هم تابیده شده^۳، کابل هم محور^۴ و فیبر نوری^۵ مثال هایی از رسانه های هدایت شونده می باشند. رسانه های غیرهدایت شونده یا بی سیم، از امواج الکترومغناطیسی و بدون استفاده از هادی های فیزیکی برای انتقال اطلاعات استفاده می نمایند. امواج رادیویی، مایکروویو، مخابرات سلولی (موبایل) و مخابرات ماهواره ای نمونه ای از رسانه های غیرهدایت شونده می باشند. در زیر به معرفی چند رسانه هدایت شونده می پردازیم.

۲-۵-۱- زوج سیم به هم تابیده شده

^۱ Guided

^۲ Unguided

^۳ Twisted-pair cable

^۴ Coaxial

^۵ Optical fiber

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

یک زوج سیم به هم تابیده شده شامل دو رشته سیم مسی روپوش دار می باشد که ضخامت تقریبی هر رشته سیم حدود یک میلی متر است. برای کاهش تداخل الکتریکی زوج سیم با زوج سیم های مشابه که در نزدیکی آن قرار دارند، این دو رشته سیم به صورت مارپیچ دور هم پیچیده می شوند. از این نوع سیم ها معمولاً در شبکه های تلفن استفاده وسیعی می شوند. می توان اطلاعات موجود در زوج سیم ها را تا چندین کیلومتر ارسال نمود، ولی چنانچه فاصله بیش از حد زیاد باشد باید در بین راه از تقویت کننده های مناسب استفاده شود.

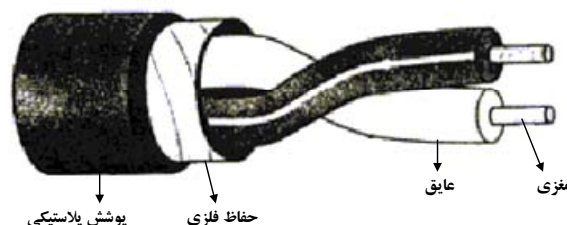
در مراکزی که به چندین زوج سیم نیاز است؛ مانند تلفن کشی مجتمع های مسکونی، چندین زوج سیم به هم تابیده به صورت دسته هایی جمع می شوند و در یک غلاف محافظ قرار می گیرند. طیف فرکانسی زوج سیم به هم تابیده شده در محدوده ۱۰۰ هرتز تا ۵ مگا هرتز می باشد. دو نوع زوج سیم به هم تابیده شده وجود دارد که عبارتند از:

□ **زوج سیم به هم تابیده شده بدون حفاظ، (UTP¹)** : این نوع زوج سیم که متداولترین نوع در شبکه های انتقال داده امروزه نیز می باشد بدون حفاظ و حفاظ خارجی است. ارزانی، انعطاف پذیری و نصب آسان این نوع زوج سیم از مزایای عمده آن می باشند. از سوی سازمان EIA، ۵ رده مختلف از کاربردهای UTP تعیین شده است که برای انتقال اطلاعات در سرعت های بسیار پایین (رده یک) تا سرعت های بالا در حدود ۱۰۰ مگا بیت در ثانیه (رده پنج) به کار می روند. متداولترین کانکتورهای UTP، RJ45 می باشد که دارای ۸ رشته سیم (۴ زوج UTP) است و در شبکه های کامپیوتری کاربرد فراوان دارد.

□ **زوج سیم به هم تابیده شده حفاظ دار (STP²)** : همانطور که از نام این نوع زوج سیم نیز مشخص می باشد، در STP یک حفاظ فلزی به همراه یک پوشش پلاستیکی در اطراف زوج سیم به هم تابیده شده قرار می گیرد. وجود این حفاظ باعث کاهش نویز پذیری سیم می گردد و همچنین از القای متقابل^۳ یک سیم بر روی سیم دیگر جلوگیری می نماید. به خاطر وجود همین حفاظ در STP، قیمت این نوع رشته سیم از UTP بیشتر می باشد. در شکل (۲-۴۴) زوج سیم های UTP و STP نشان داده شده اند.



(الف)



(ب)

^۱ Unshielded Twisted-Pair

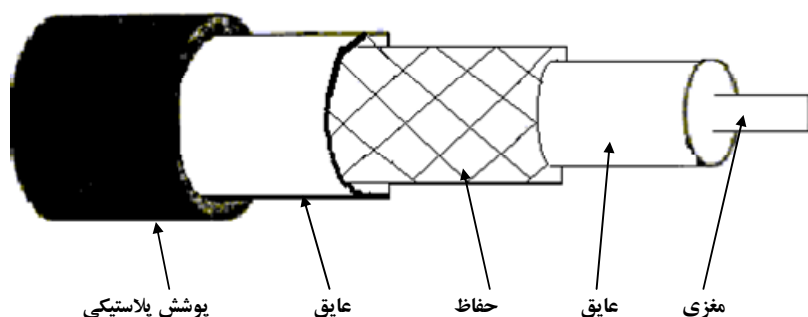
^۲ Shielded Twisted-Pair

^۳ Crosstalk

شکل (۲-۴۴): زوج سیم‌های به هم تابیده: (الف) UTP (ب) STP

۲-۵-۲- کابل هم‌محور

یکی دیگر از متداول‌ترین رسانه های هدایت شونده، کابل هم‌محور می‌باشد. این نوع کابل شامل یک مغزی سخت از جنس مس است که دور یک ماده عایق قرار گرفته است و یک توری ریزبافت فلزی به صورت یک هادی استوانه‌ای اطراف عایق مغزی قرار گرفته است. هادی استوانه‌ای نیز توسط یک محافظ پلاستیکی پوشانده شده است. در شکل (۲-۴۵) یک کابل هم‌محور نشان شده است.



شکل (۲-۴۵): ساختار کابل هم‌محور

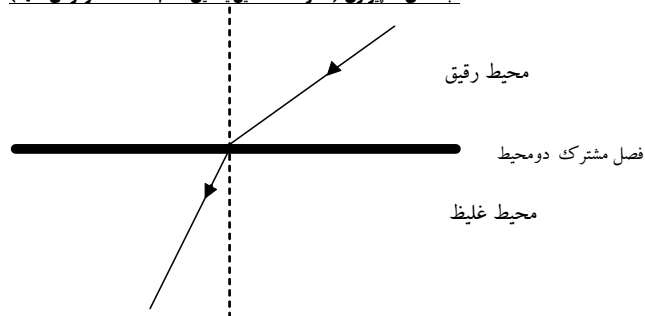
کابل هم‌محور دارای پهنای باند زیادی می‌باشد که در محدوده فرکانسی ۱۰۰ کیلوهرتز تا ۵۰۰ مگاهرتز قرار دارد. البته هرچه طول کابل افزایش یابد، حداکثر سرعت انتقال داده‌ها در کابل کم می‌شود. ۵ نوع متداول از کابل هم‌محور وجود دارند که عبارتند از: RG-8, RG-9, RG-11 (مورد استفاده در شبکه‌های اترنت سخت)، RG-58 (مورد استفاده در شبکه‌های اترنت نرم) و RG-75 (جهت انتقال سیگنال‌های تلویزیونی).

۲-۵-۳- فیبر نوری

با گسترش سیستم‌های انتقال و افزایش سرعت، نیاز به رسانه های انتقال با پهنای باند و اطمینان بالا حس گردید. بدین منظور فیبر نوری به عنوان یک رسانه هدایت شونده مناسب مطرح است. نور یک نوع موج الکترومغناطیسی است که با سرعت ۳۰۰ هزار کیلومتر در ثانیه در خلاء انتشار می‌یابد. در سایر محیط‌ها، سرعت نور به چگالی محیط بستگی دارد؛ طوری که با افزایش چگالی محیط سرعت نور کاهش می‌یابد. مسیر حرکت نور بر روی یک خط مستقیم می‌باشد. هنگامی که نور از یک محیط وارد محیط دیگری با ضریب شکست متفاوت با محیط اول می‌شود، امتداد خود را از دست می‌دهد که در اصطلاح به این پدیده شکست^۱ نور می‌گویند. چنانچه غلظت محیط دوم از محیط اول بیشتر باشد، پرتوی نور شکست یافته در محیط دوم به خط قائم نزدیکتر می‌شود. در شکل (۲-۴۶) نمونه‌ای از پدیده شکست نور نشان داده شده است.

^۱ Refraction

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

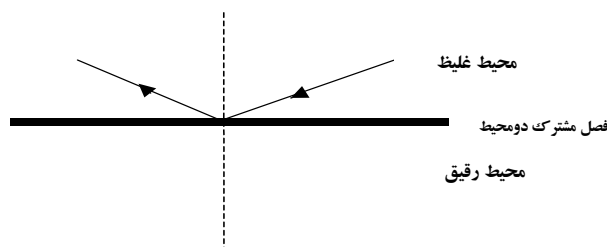


شکل (۲-۴۶):

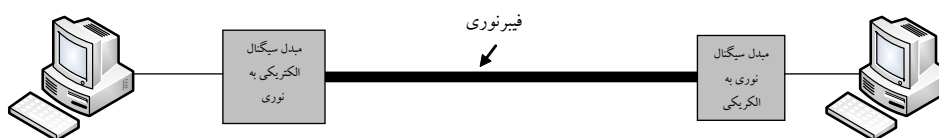
پدیده شکست نور

هنگامی که نور از یک محیط غلیظ وارد یک محیط رقیق می گردد، زاویه پرتوی نور خروجی نسبت به خط قائم افزایش می یابد. در حالت حدی چنانچه نور از یک محیط غلیظ طوری به یک محیط رقیق تابیده شود که زاویه پرتوی خروجی نسبت به خط قائم ۹۰ درجه باشد، در این صورت زاویه تابش زاویه بحرانی^۱ نامیده می شود. چنانچه زاویه تابش از زاویه بحرانی بیشتر شود، در این صورت پرتوی نور تابیده شده به درون محیط اول انعکاس می یابد. در این حالت مطابق با شکل (۲-۴۷) زاویه تابش پرتوی نور با زاویه انعکاس برابر می باشد. فیبر نوری از پدیده انعکاس برای انتقال نور استفاده می کند. اطراف فیبر نوری یک بافر مخصوص قرار دارد که آن را در مقابل رطوبت و نم محافظت می نماید. در اطراف بافر نیز یک پوشش محافظ قرار می گیرد.

در شکل (۲-۴۸) ساختار کلی یک سیستم انتقال نوری نشان داده شده است. در فرستنده از دیودهای نوری (LED^۲) (و لیزر برای تبدیل سیگنال های الکتریکی به سیگنال های نوری استفاده می شود. در سمت گیرنده نیز از گیرنده های نوری مخصوص جهت تبدیل سیگنال نوری به سیگنال الکتریکی استفاده می گردد.



شکل (۲-۴۷): پدیده بازتابش کلی



شکل (۲-۴۸): یک سیستم انتقال نوری

در فیبر نوری برای ارسال اطلاعات ۰ و ۱ از پالس های نور مرئی استفاده می گردد.

^۱ Critical angle

^۲ Light Emitting Diode

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

مطابق با شکل (۲-۴۸)، یک سیستم انتقال نوری از سه قسمت اصلی تشکیل شده است که عبارتند از: سیستم مبدل سیگنال های الکتریکی به پالس های نوری (با استفاده از دیودهای نوری یا لیزری)، فیبر نوری و مبدل پالس های نوری به سیگنال های الکتریکی (با استفاده از فتودیود).

فیبر نوری از دو قسمت اصلی تشکیل شده است که عبارتند از: مغزی^۱ و غلاف^۲. هم مغزی و هم غلاف هر دو از جنس شیشه می باشند. ضریب شکست مغزی بیشتر از ضریب شکست غلاف است که این امر باعث پدیده بازتابش کلی در فیبر نوری می شود. مطابق با شکل (۲-۴۹) سه نوع مختلف فیبر نوری وجود دارند که عبارتند از:

□ **فیبر نوری چند مود با ضریب شکست پله ای^۳:** در این نوع فیبر، مغزی و غلاف دارای دو ضریب شکست مختلف می باشند. قطر مغزی نسبتاً زیاد می باشد و این باعث می شود که چندین پرتوی نوری مختلف با زاویه های تابش گوناگون وارد فیبر شوند. این پرتوهای نوری از مسیرهایی با طول مختلف به مقصد می رسند. از آنجایی که سرعت انتشار در محیط برای تمام این پرتوها یکسان می باشد، بنابراین پرتوی نوری که مسیر کمتری را طی کرده است زودتر از پرتوی نوری که مسیر طولانی را طی نموده است به مقصد می رسد. این مسئله باعث اعوجاج در پالس نوری دریافتی در مقصد می شود که آشکارسازی آن را با مشکل مواجه می سازد.

□ **فیبر نوری چند مود با ضریب شکست تدریجی^۴:** در این نوع فیبر نیز قطر مغزی نسبتاً زیاد می باشد که باعث می شود تا پرتوهای نوری مختلف با زوایای تابش گوناگون وارد فیبر شوند. برخلاف فیبر نوری با ضریب شکست پله ای، در این نوع فیبر ضریب شکست به طور ناگهانی تغییر نمی کند بلکه هر چه از محور مرکزی فیبر فاصله می گیریم، ضریب شکست به طور تدریجی کاهش می یابد. این امر باعث می شود که پرتوهای نوری که از محور مرکزی فیبر دور هستند و فاصله بیشتری را طی می کنند عملاً با سرعت بیشتر منتقل شوند (زیرا سرعت انتشار نور با ضریب شکست محیط ارتباط معکوس دارد) و پرتوهای نوری که از نزدیکی مرکز فیبر عبور می کنند و مسیر کوتاهتری را طی می کنند با سرعت کمتری به مقصد برسند. بنابراین تدریجی بودن ضریب شکست فیبر، باعث همزمان رسیدن تمام پرتوهای نوری ارسالی فرستنده در گیرنده می شود و این امر باعث کاهش اعوجاج پالس نوری در گیرنده می شود.

□ **فیبر تک مود^۵:** در این نوع فیبر، قطر فیبر تا حد طول موج نور کاهش یافته است و این کاهش باعث می شود که پرتوی نور بدون انعکاس و بر روی یک خط مستقیم منتشر شود و به مقصد برسد. بنابراین در فیبر نوری تک مود، پالس نوری در مقصد با کمترین اعوجاج دریافت می شود و آشکارسازی آن آسان می باشد.

نوع فیبر نوری، با توجه به نسبت قطر مغزی آن به قطر غلاف شناخته می شود. در جدول (۲-۶) انواع فیبر نوری آورده شده است. از نقطه نظر حفاظت فیبر از نیروهای خارجی، فیبر نوری به دو نوع Loos Buffer و Tight Buffer تقسیم می شوند. در ساخت Loos Buffer، فیبر داخل یک لوله پلاستیکی که قطر درونی آن به طور قابل ملاحظه ای بزرگتر از خود فیبر است قرار می گیرد و درون لوله پلاستیکی و اطراف فیبر معمولاً با یک ماده ژلی پر می شود که فیبر داخل این ژل آزاد است. Loos Buffer تا حدودی فیبر را در برابر نیروهای مکانیکی خارجی محافظت می کند و همچنین به دلیل وجود ژل در اطراف فیبر، در برابر گرما، سرما و در نتیجه انبساط و انقباض به طور

^۱ Core

^۲ Cladding

^۳ Multimode step- index

^۴ Multimode graded- index

^۵ Single mode

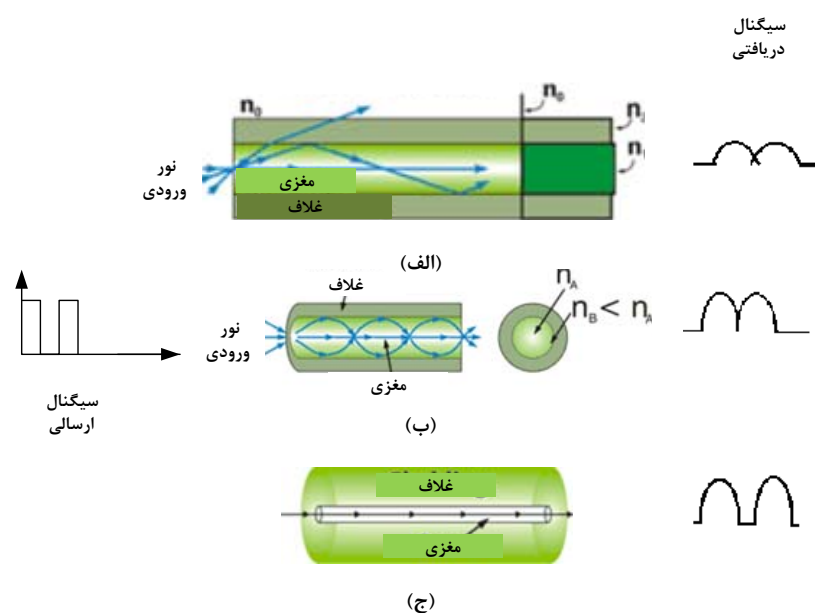
شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

قابل ملاحظه ای ایمن است. این کابل معمولاً برای نصب در محیط های بیرونی، کاربردهای هوایی، کانالی و در زیر خاک استفاده می شود.

در فیبر نوری Tight Buffer یک روکش پلاستیکی چسبیده به فیبر وجود دارد و مانع از آزاد بودن فیبر می شود. این نوع روکش برای اتصال به اجزای شبکه بسیار مناسب است زیرا این روکش از شکستن فیبر جلوگیری می کند. فیبرهای Tight Buffer اغلب برای کاربردهای داخل ساختمان، منابع تغذیه ساختمان های مرکزی و کاربردهای عمومی به کار برده می شوند.

فیبر نوری به خاطر سرعت بسیار بالای خود که از مرز یک گیگا بیت بر ثانیه نیز فراتر است، برای انتقال داده ها با سرعت بسیار بالا مفید می باشد. علاوه بر شبکه های محلی، از فیبر نوری می توان در شبکه های مخابراتی راه دور و شبکه تلفن نیز استفاده کرد. به طور خلاصه مزایای فیبر نوری را می توان نوپذیری کم، تضعیف کم و پهنای باند بسیار بالا دانست. البته فیبر نوری دارای معایبی نیز می باشد که مهم ترین آنها عبارتند از: هزینه بالا (به خصوص در مورد فیبرهای تک مود)، نیاز به تخصص بالا در نصب و نگهداری آن و همچنین شکنندگی زیاد.

علاوه بر رسانه های ارسال هدایت شونده فوق که به آنها اشاره شد، نوع دیگری از رسانه های ارسال وجود دارند که با عنوان رسانه های ارسال غیر هدایت شونده یا بدون سیم شناخته می شوند. در رسانه های ارسال غیر هدایت شونده، امواج الکترومغناطیسی بدون این که از یک هادی فیزیکی استفاده نمایند، در محیط اطراف انتشار می یابند. در زیر به بررسی انواع رسانه های ارسال غیر هدایت شونده می پردازیم.



شکل (۲-۴۹): سه نوع فیبر نوری

الف) فیبر چند مود با ضریب شکست پله ای (ب) فیبر چند مود با ضریب شکست تدریجی (ج) فیبر تک مود

جدول (۲-۶): انواع فیبر نوری

نوع فیبر	قطر مغزی (میکرون)	قطر غلاف (میکرون)

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

۱۲۵	۶۲/۵	۶۲/۵ ۱۲۵ (چندمود با ضریب شکست تدریجی)
۱۲۵	۵۰	۵۰ ۱۲۵ (چندمود)
۱۴۰	۱۰۰	۱۰۰ ۱۴۰ (چندمود با ضریب شکست تدریجی)
۱۲۵	۸۵	۸۵ ۱۲۵ (چند مود با ضریب شکست تدریجی)
۲۴۰	۲۰۰	۲۰۰ ۲۴۰ (چند مود با ضریب شکست پله ای)
۱۲۵	۸/۳	۸/۳ ۱۲۵ (تک مود)

۲-۵-۴ - امواج رادیویی

امواج رادیویی که بخشی از طیف امواج الکترومغناطیسی می باشند، بر اساس فرکانس به ۸ دسته عمده تقسیم می شوند که عبارتند از :

_ امواج با فرکانس بسیار پایین ($VLFF^1$) (۳ الی ۳۰ کیلوهرتز)

_ امواج با فرکانس پایین (LF^2) (۳۰ الی ۳۰۰ کیلوهرتز)

_ امواج با فرکانس متوسط (MF^3) (۳۰۰ کیلوهرتز الی ۳ مگاهرتز)

_ امواج با فرکانس بالا (HF^4) (۳ الی ۳۰ مگاهرتز)

_ امواج با فرکانس بسیار بالا (VHF^5) (۳۰ الی ۳۰۰ مگاهرتز)

_ امواج با فرکانس مافوق بالا (UHF^6) (۳۰۰ مگاهرتز الی ۳ گیگاهرتز)

_ امواج با فرکانس بسیار مافوق بالا (SHF^7) (۳ الی ۳۰ گیگاهرتز)

_ امواج با فرکانس شدیداً بالا (EHF^8) (۳۰ الی ۳۰۰ گیگاهرتز)

امواج رادیویی که نام برده شد، از ۵ نوع انتشار مختلف استفاده می نمایند که عبارتند از :

• انتشار سطحی⁹

• انتشار در قسمت پایین هوای کره (تروفوسفوریک)¹⁰

• انتشار یونوسفریک¹¹

• انتشار در خط مستقیم¹²

• انتشار فضایی¹³

در انتشار سطحی، امواج رادیویی از طریق سطح پایینی اتمسفر جو انتقال می یابند. امواج VLF و LF از این نوع انتشار استفاده می کنند.

¹Very Low Frequency

²Low Frequency

³Medium Frequency

⁴High Frequency

⁵Very High Frequency

⁶Ultra High Frequency

⁷Super High Frequency

⁸Extremely High Frequency

⁹Surface propagation

¹⁰Tropospheric propagation

¹¹Ionospheric propagation

¹²Line of sight Propagation

¹³Space propagation

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

در انتشار تروفسفوریک، امواج ارسالی با سطح پایین جو برخورد کرده و منعکس می شوند. البته می توان فرستنده و گیرنده را نیز در یک مسیر و در دید یکدیگر قرار داد و امواج رادیویی را ارسال نمود. سیگنال های رادیویی MF از این نوع انتشار استفاده می کنند.

در انتشار یونوسفوریک امواج رادیویی فرکانس بالا HF به سطح میانی جو برخورد کرده و در آن جا به سمت زمین منعکس می گردند. از این نوع انتشار در حالتیکه توان ارسال کم می باشد و فاصله فرستنده و گیرنده زیاد است استفاده می گردد.

در انتشار در خط مستقیم، سیگنال های رادیویی بسیار فرکانس بالای VHF و UHF مستقیماً در یک خط راست، بین فرستنده و گیرنده منتقل می شوند. در این حالت آنتن های فرستنده و گیرنده باید دقیقاً در معرض دید مستقیم یکدیگر قرار داشته باشند.

در انتشار فضایی که در مخابرات ماهواره ای استفاده می شود، امواج رادیویی VHF، SHF و EHF از جو زمین عبور کرده و به وسیله آنتن ماهواره دوباره به سمت زمین منعکس می شوند.

۲-۵-۵- امواج مایکروویو

امواج مایکروویو قادر به پیمودن انحنای کره زمین نمی باشند، بلکه ارسال و دریافت آنها بر روی خطوط مستقیم و در دید یکدیگر می باشد. فاصله مستقیمی که امواج مایکروویو قادر به پیمودن آن می باشند، بستگی به ارتفاع آنتن دارد، به طوری که هرچه آنتن بزرگتر باشد فاصله بیشتری می تواند طی شود. معمولاً آنتن های مایکروویو در نقاط بلند، نظیر برج ها و کوهستان قرار می گیرند. امواج مایکروویو در هر لحظه در یک جهت انتشار می یابند. بنابراین برای برقراری ارتباط دوطرفه نیاز به دو فرکانس متفاوت می باشد و برای هر فرکانس فرستنده و گیرنده مخصوصی نیاز می باشد. البته می توان هر دو فرستنده و گیرنده را در یک دستگاه به نام فرستنده/گیرنده ادغام نمود.

برای افزایش برد امواج مایکروویو از تکرار کننده های مناسب استفاده می شود. هر تکرار کننده، امواج مایکروویو را دریافت می نماید و پس از تقویت با استفاده از آنتن های مناسب امواج را به تکرار کننده بعدی ارسال می کند. فاصله بین تکرار کننده ها بستگی به فرکانس امواج مایکروویو و همچنین شرایط محیطی دارد. براساس نوع سیستم به کار گرفته شده، هر تکرار کننده می تواند سیگنال دریافتی را با همان فرکانس و یا با فرکانس متفاوت ارسال دارد. سیستم های مایکروویو دارای دو نوع آنتن به نام های آنتن های سهموی^۱ و شیپوری^۲ می باشند.

۲-۵-۶- مخابرات ماهواره ای

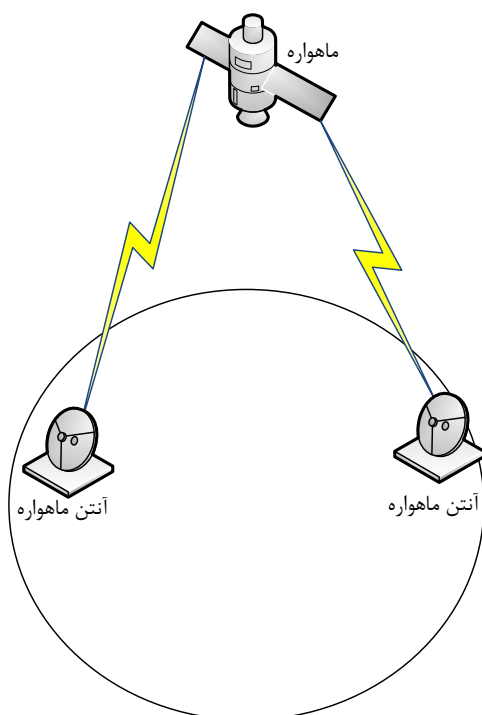
انتشار امواج در سیستم های مخابرات ماهواره ای شبیه ارسال امواج مایکروویو، بر روی مسیر مستقیم صورت می گیرد که در آن یک ایستگاه زمینی اطلاعات را برای یک ماهواره که دور زمین می چرخد ارسال می دارد. اصول سیستم های ماهواره ای نیز مشابه سیستم های مایکروویو می باشد که در آن ماهواره مانند یک تکرار کننده عمل می کند. در شکل (۲-۵۰) نمونه ای از یک سیستم ماهواره نشان داده شده است.

با استفاده از سیستم های ماهواره ای از هر نقطه زمین می توان برای هر نقطه دیگر از زمین اطلاعات را ارسال کرد. بنابراین سیستم های مخابرات ماهواره ای از کیفیت ارتباطی بالایی برخوردار هستند. ماهواره به تنهایی قیمت بالایی دارد اما اجاره کردن فرکانسهای ماهواره ای و یا اجاره کردن زمانی آن قیمت نسبتاً مناسبی دارد.

^۱ Parabolic
^۲ Horn

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

برای ارسال مستقیم امواج، باید آنتن های فرستنده و گیرنده در دید یکدیگر قرار داشته باشند، در غیر این صورت امکان برقراری ارتباط وجود ندارد. بنابراین ماهواره هایی که سریعتر و یا کندتر از زمین حرکت می کنند، فقط برای دوره زمانی کوتاهی در طول روز قابل استفاده می باشند. برای آن که ارتباط دائمی برقرار باشد، ماهواره باید با همان سرعت زمین دور زمین گردش نماید، طوری که نسبت به زمین ثابت باشد. به این نوع ماهواره ها، ماهواره های ژئوسنکرون^۱ می گویند.



شکل (۲-۵۰): نمونه ای از یک سیستم ماهواره ای

از آنجایی که سرعت مداری حرکت ماهواره ها به فاصله آنها از زمین بستگی دارد، بنابراین فقط یک مدار ژئوسنکرون وجود دارد. این مدار در فاصله تقریبی ۳۵۷۸۰ کیلومتر از سطح زمین قرار دارد. یک ماهواره ژئوسنکرون به تنهایی نمی تواند کل کره زمین را پوشش دهد؛ بلکه حداقل به ۳ ماهواره ژئوسنکرون که در زاویه ۱۲۰ درجه از یکدیگر قرار دارند برای پوشش کل زمین نیاز می باشد. فرکانسهای مورد استفاده در مخابرات ماهواره ای در محدوده گیگاهرتز می باشد. هر ماهواره در دو باند فرکانسی متفاوت اقدام به ارسال و دریافت اطلاعات می نماید. ارسال امواج از زمین به ماهواره، کانال بالا^۲ و ارسال امواج از ماهواره به زمین، کانال پایین^۳ نام دارد. در جدول (۲-۷) باند فرکانسی مورد استفاده در ماهواره ها نشان داده شده است.

جدول (۲-۷): باندهای فرکانسی مورد استفاده در ماهواره ها

باند	کانال پایین	کانال بالا
فرکانسی	(بر حسب گیگا هرتز)	(بر حسب گیگا هرتز)

^۱ Geosynchronous

^۲ Up link

^۳ Down link

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

C	۴/۲ الی ۳/۷	۵/۹۲۵ الی ۶/۴۲۵
Ku	۱۱/۷ الی ۱۲/۲	۱۴ الی ۱۴/۵
Ka	۱۷/۷ الی ۲۱	۲۷/۵ الی ۳۱

۲-۵-۷- تلفن سلولی

از تلفن سلولی برای برقراری ارتباط مطمئن و پایدار بین دو وسیله متحرک و یا بین یک وسیله متحرک و یک وسیله ثابت استفاده می شود. در سیستم تلفن های سلولی پس از شناسایی و ردگیری محل کاربر، یک کانال فرکانسی خاص برای مکالمه ایجاد می گردد و به کاربر تخصیص داده می شود. چنانچه کاربر از محدوده کانال اختصاص یافته به آن خارج شود، سیگنال آن از کانال قبلی به کانال جدیدی منتقل می شود.

برای ردگیری کاربران در شبکه های تلفن سلولی، سطح شهر به مناطق کوچکی به نام سلول تقسیم می شوند. هر سلول شامل آنتن خاصی می باشد و توسط یک دفتر کوچکی اداره می شود. هر یک از دفترهای فوق به نوبت توسط یک دفتر مرکزی به نام دفتر سوئیچینگ تلفن موبایل (MTSO^۱) کنترل می شوند.

هر MTSO وظیفه ایجاد هماهنگی لازم بین دفاتر سلولی و اداره مرکزی تلفن را به عهده دارد. اندازه سلول ها ثابت نیست و متناسب با تراکم جمعیتی منطقه، قابل افزایش و یا کاهش هستند. شعاع معمولی هر سلول بین ۱ تا ۱۲ مایل است. مناطقی که از چگالی جمعیتی بالایی برخوردار هستند، از سلول های کوچکتری نسبت به سایر مناطق استفاده می کنند. برای جلوگیری از تداخل بین سلول های مجاور توان ارسالی هر سلول به اندازه کافی کم در نظر گرفته می شود. تلفن های سلولی از روش آنالوگ FM برای برقراری ارتباط بین تلفن متحرک و اداره سلولی استفاده می کنند. دو باند فرکانسی ۸۲۴ الی ۸۴۹ مگاهرتز برای ارتباط هایی که با تلفن موبایل شروع می شود و باند فرکانسی ۸۶۹ الی ۸۹۴ مگاهرتز برای ارتباط هایی که توسط تلفن های ثابت آغاز می شود، اختصاص یافته است. فرکانسهای حامل به فاصله ۳۰ کیلوهرتز از یکدیگر قرار دارند، بنابراین هر باند قادر به پشتیبانی از ۸۳۳ فرکانس حامل می باشد. از آنجایی که برای هر ارتباط دوطرفه به دو فرکانس حامل نیاز است، در نتیجه در هر باند فرکانسی فقط ۴۱۶ کانال وجود دارد. البته برخی از این کانال ها برای عملیات کنترل و برقراری ارتباط رزرو شده اند. علاوه بر این برای جلوگیری از تداخل، کانال های فوق طوری بین سلول ها توزیع شده اند که دو سلول مجاور از کانال یکسان استفاده نمایند. بدین ترتیب هر سلول معمولاً فقط به ۴۰ کانال دسترسی دارد.

برای برقراری یک ارتباط توسط تلفن موبایل، کاربر یک کد ۷ الی ۱۰ رقمی (شماره تلفن مخاطب) را وارد می نماید. به دنبال آن تلفن موبایل کل باند فرکانسی را جاروب نموده و به دنبال یک کانال خالی کنترلی می گردد. سپس شماره تلفن مخاطب را با استفاده از کانال کنترلی به نزدیکترین اداره سلول ارسال می دارد. اداره سلول نیز داده های دریافتی را به MTSO ارسال می دارد و MTSO نیز داده ها را به اداره مرکزی تلفن ارسال می کند. چنانچه مخاطب در دسترس باشد، اداره مرکزی تلفن اتصال را برقرار می کند و آن را به MTSO ارسال می کند. MTSO نیز یک کانال خالی صوتی پیدا نموده و به دنبال آن ارتباط برقرار می شود. تلفن موبایل به طور اتوماتیک خود را به کانال جدید وفق می دهد و ارتباط صوتی برقرار می شود. هنگامی که یک تلفن ثابت مایل به برقراری ارتباط با یک تلفن موبایل می باشد، اداره مرکزی تلفن شماره مخاطب را برای MTSO ارسال می کند. MTSO نیز با ارسال پیام های جستجو برای هر سلول به دنبال محل تلفن موبایل مخاطب می گردد.

^۱ Mobile Telephone Switching Office

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

هنگامی که MTSO محل تلفن موبایل مخاطب را پیدا کرد، برای آن یک سیگنال زنگ ارسال می‌دارد و پس از آن که مخاطب به سیگنال زنگ ورودی جواب داد، یک کانال صوتی برای مکالمه تخصیص داده می‌شود و مکالمه صوتی شروع می‌شود. این احتمال وجود دارد که در طی مکالمه، کاربر تلفن موبایل از یک سلول به سلول دیگر تغییر مکان دهد. در این حالت سیگنال دریافتی ضعیف می‌شود. برای حل این مشکل MTSO هر چند ثانیه سطح سیگنال دریافتی را اندازه گیری می‌کند و چنانچه سطح سیگنال دریافتی از حدی کمتر باشد به دنبال یک سلول جدیدی که با سطح انرژی مطلوب قادر به سرویس دهی به کاربر باشد می‌گردد و به دنبال آن MTSO کانال مکالمه را از کانال جدید تغییر می‌دهد. انتقال به طریقی انجام می‌گیرد که کاربر متوجه آن نشود (شفافیت). به این عملیات در اصطلاح hand off گفته می‌شود. امروزه تلفن‌های سلولی در حال گسترش به سمت یکپارچه سازی آن با سیستم‌های مخابرات ماهواره‌ای می‌باشند. با مجتمع سازی تلفن‌های موبایل و سیستم‌های مخابرات ماهواره‌ای، امکان برقراری ارتباط بین هر دو نقطه در سطح دنیا وجود خواهد داشت. همچنین با توسعه این سیستم امکان ارسال و دریافت داده، صوت و تصویر فراهم می‌شود.

۲-۵-۸ - کارآیی سیستم‌های انتقال

برای مقایسه سیستم‌ها و رسانه های ارسال از ۵ مشخصه کارآیی استفاده می‌شود، این مشخصه‌ها عبارتند از :

- **هزینه :** شامل هزینه سرمایه‌گذاری و همچنین هزینه ارسال و نگهداری سیستم .
- **سرعت :** حداکثر تعداد بیت‌های ارسالی در ثانیه، که با اطمینان بالا در محیط قابل ارسال می‌باشند. سرعت ارسال با فرکانس تغییر می‌کند و فرکانسهای بالاتر امکان ارسال با سرعت بیشتر را فراهم می‌آورند .
- **تضعیف :** سیگنال‌های الکترومغناطیسی با عبور از رسانه انتقال دچار تضعیف می‌گردند.
- **تداخل الکترو مغناطیسی:** تداخل الکترو مغناطیسی نشان‌دهنده میزان تاثیر سایر امواج الکترومغناطیسی بر روی رسانه انتقال می‌باشد.
- **امنیت :** منظور از امنیت، جلوگیری از دسترسی غیر مجاز افراد به اطلاعات موجود در رسانه انتقال می‌باشد . بعضی از رسانه ها نظیر امواج رادیویی و کابل UTP به راحتی قابل شنود می‌باشند. در حالی که فیبر نوری از امنیت بیشتری برخوردار می‌باشد.

در جدول (۸-۲) کارآیی رسانه های ارسال گوناگون آورده شده است.

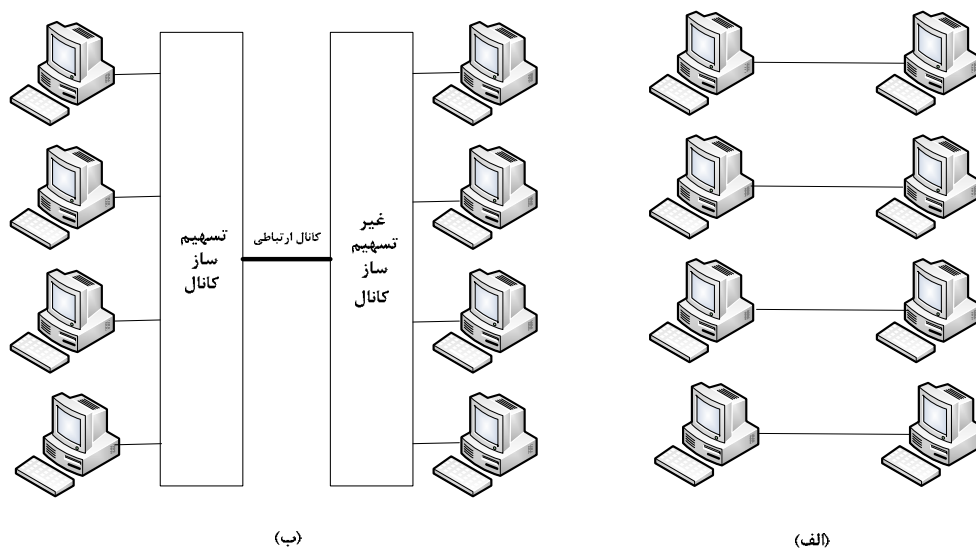
جدول (۲-۸): کارآیی رسانه های ارسال

رسانه انتقال	هزینه	سرعت	تضعیف	تداخل الکترومغناطیسی	امنیت
کابل UTP	کم	۱۱ الی ۱۰۰ مگابیت بر ثانیه	زیاد	زیاد	کم
کابل STP	متوسط	۱ الی ۱۵۰ مگابیت بر ثانیه	زیاد	متوسط	کم
کابل هم محور	متوسط	۱ مگابیت الی ۱ گیگا بیت بر ثانیه	متوسط	متوسط	کم
فیبر نوری	زیاد	۱۰ مگا بیت الی ۲ گیگا بیت بر ثانیه	کم	کم	زیاد
امواج رادیویی	متوسط	۱ الی ۱۰ مگابیت بر ثانیه	کم - زیاد	زیاد	کم
مایکروویو	زیاد	۱ مگابیت الی ۱۰ گیگا بیت بر ثانیه	متغیر	زیاد	متوسط
ماهواره	زیاد	۱ مگابیت الی ۱۰ گیگا بیت بر ثانیه	متغیر	زیاد	متوسط
تلفن سلولی	زیاد	۹۶۰۰ الی ۱۹۲۰۰ بیت بر ثانیه	کم	متوسط	کم

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

یکی دیگر از وظایف لایه فیزیکی، تسهیم سازی می باشد. هنگامی که ظرفیت کانالی که دو وسیله کامپیوتری را به یکدیگر متصل می نماید، از ظرفیت مورد نیاز برای ارسال بیشتر باشد، در این صورت می توان از کانال به طور مشترک استفاده نمود و چندین وسیله کامپیوتری را از طریق آن به همدیگر متصل کرد. با استفاده از تسهیم سازی، امکان ارسال همزمان چندین کامپیوتر بر روی یک کانال فیزیکی مشترک فراهم می آید.

طبیعی است که استفاده از تسهیم سازی، و استفاده مشترک از یک کانال باعث کاهش تعداد کانال های مورد نیاز می شود و هزینه ارتباطی نیز کاهش می یابد. در شکل (۲-۵۱)، نمونه ای از یک تسهیم کننده^۱ کانال آورده شده است. در این مثال، چهار کامپیوتر از طریق یک تسهیم کننده کانال که به اختصار به آن MUX گفته می شود، به یک کانال مشترک متصل شده اند. در سمت گیرنده از یک DEMUX جریان اطلاعاتی هریک از کامپیوترها از کانال جدا می شود و تحویل گیرنده مربوطه می گردد.



شکل (۲-۵۱): نمونه ای از کاربرد یک تسهیم کننده کانال
الف) اتصال مستقیم بدون تسهیم کننده کانال ب) اتصال با استفاده از تسهیم کننده کانال

دو نوع روش مختلف تسهیم سازی وجود دارند که عبارتند از:

- تسهیم سازی به صورت زمانی (TDM^2)
- تسهیم سازی به صورت فرکانسی (FDM^3)

تسهیم سازی به صورت زمانی خود به دو نوع مختلف، همزمان و غیرهمزمان تقسیم بندی می شوند. در زیر به بررسی هر یک از روش های مختلف فوق می پردازیم.

۲-۶-۱- تسهیم سازی فرکانسی (FDM)

این روش یک تکنیک آنالوگ می باشد و در مواقعی که پهنای باند کانال از پهنای باند سیگنال های ارسالی بیشتر است استفاده می شود. در روش FDM هریک از سیگنال های ارسالی در فرکانس های مختلف حامل مدوله می شوند که این

^۱ Multiplexer

^۲ Time Division Multiplexing

^۳ Frequency Division Multiplexing

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

فرکانس های حامل به اندازه کافی از یکدیگر فاصله دارند تا تداخلی در سیگنال ها به وجود نیاید. در شکل (۲-۵۲) مثالی از عملیات تقسیم فرکانسی کانال نشان داده شده است.

به عنوان مثال، یکی از کاربردهای متداول FDM در تلویزیون های کابلی می باشد. کابل های هم محور که در سیستم تلویزیون های کابلی استفاده می شوند دارای پهنای باندی در حدود ۵۰۰ مگاهرتز می باشند. هر کانال تلویزیون در حدود ۶ مگاهرتز پهنای باند نیاز دارد. با این حساب هر کابل هم محور در حدود ۸۳ کانال تلویزیون را سرویس می دهد. اما در عمل با توجه به این که مقداری از پهنای باند به عنوان باند محافظ استفاده می شود، تعداد کانال هایی که توسط هر کابل هم محور سرویس داده می شود به مراتب کمتر از ۸۳ می باشد.

با گسترش تکنولوژی فیبر نوری از روش WDM^۱ که مشابه FDM برای ارسال سیگنال های نوری است، استفاده می شود.

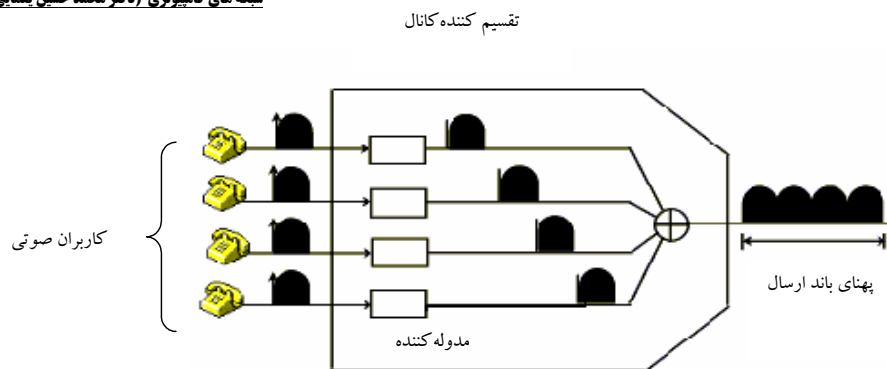
۲-۶-۲ - تسهیم سازی زمانی (TDM)

روش TDM یک تکنیک دیجیتال برای تسهیم سازی زمانی کانال بین کاربران می باشد و در مواقعی که نرخ ارسال داده کانال، از نرخ ارسال مورد نیاز هریک از تجهیزات کامپیوتری متصل به کانال بیشتر است، استفاده می گردد. در روش TDM همزمان، زمان به برش های ثابتی تقسیم بندی می شود و هر برش زمانی در اختیار یک کاربر قرار می گیرد. هر ایستگاه متصل به کانال، فقط در مواقعی که برش زمانی مخصوص آن برسد، اجازه ارسال داده ها در کانال را دارد و در سایر زمان ها اجازه ارسال از آن سلب می شود. در روش TDM همزمان، چنانچه ایستگاهی هیچ داده ای برای ارسال در برش زمانی خود نداشته باشد، در این صورت آن برش زمانی بدون استفاده می ماند که این امر باعث اتلاف ظرفیت کانال می شود که از معایب عمده این روش است.

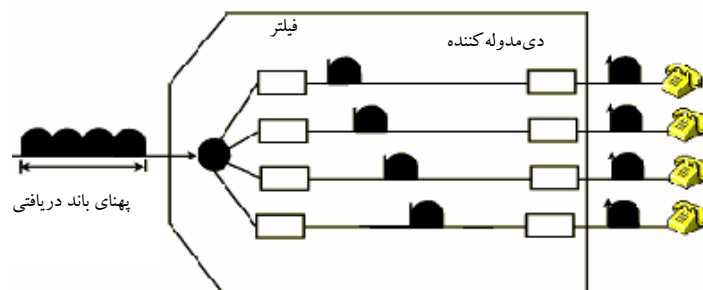
چنانچه N ایستگاه مختلف به کانال متصل باشند و هریک برش زمانی خاص خود را در اختیار داشته باشند، یک سیکل کامل ارسال حداقل شامل N برش زمانی می باشد. در صورتی که همه ایستگاه های متصل به کانال دارای سرعت ارسال یکسان باشند، به هریک از آنها در هر قاب یک برش زمانی ثابت می رسد. هنگامی که نرخ ارسال یک ایستگاه بیشتر از سایر ایستگاه ها باشد، آن ایستگاه می تواند برش های زمانی بیشتری در یک قاب را اشغال کند. به عنوان مثال اگر سرعت پایه یک سیستم TDM همزمان ۱۲۰۰ بیت بر ثانیه باشد، چنانچه ایستگاهی دارای سرعت ارسال ۴۸۰۰ بیت بر ثانیه باشد، در این صورت آن ایستگاه ۴ برش زمانی را در هر قاب به خود اختصاص می دهد. در شکل (۲-۵۳) مثالی از عملکرد یک سیستم تقسیم زمانی همزمان آورده شده است.

^۱Wavelength Division Multiplexing

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

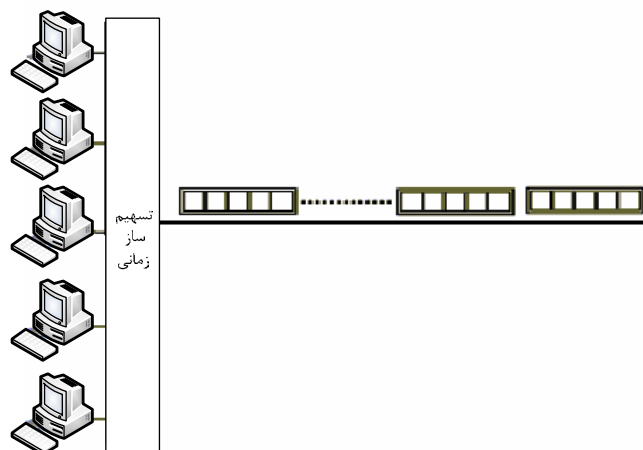


فرستنده



گیرنده

شکل (۲-۵۲): نمونه‌ای از عملیات تقسیم فرکانسی کانال

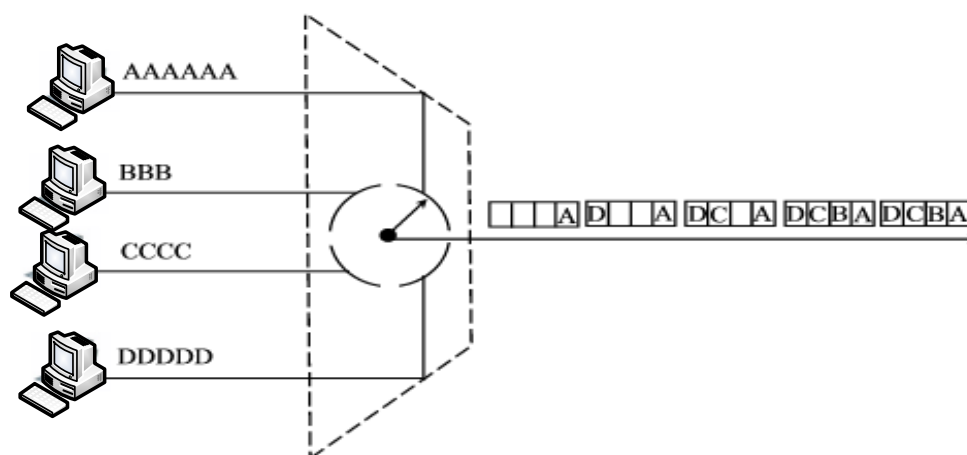


شکل (۲-۵۳): مثالی از یک سیستم TDM همزمان

یکی از مشکلات و معایب روش TDM همزمان آن است که این روش در مورد استفاده کامل از ظرفیت کانال هیچ‌گونه تضمینی به کاربران خود نمی‌دهد. در شکل (۲-۵۴) مثالی از یک سیستم TDM همزمان آورده شده است، که در آن برخی از برش‌های زمانی به دلیل عدم وجود ترافیک ارسالی خالی مانده است.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

برای رفع این مشکل، روش TDM غیر همزمان ارائه شده است. در این روش، مجموع سرعت همه ایستگاه های متصل به کانال ممکن است که از سرعت کانال بیشتر باشد. در روش TDM غیرهمزمان، چنانچه N ایستگاه داشته باشیم که به یک کانال مشترک متصل می باشند، برخلاف روش TDM همزمان تعداد برش های زمانی در هر قاب به مراتب از N کمتر می باشد. به عبارت دیگر در یک سرعت یکسان کانال، تعداد ایستگاه های متصل شونده به کانال در روش TDM غیرهمزمان از روش TDM همزمان بیشتر می باشد. تعداد برش های زمانی موجود در هر قاب، به وسیله آنالیز آماری ترافیک ورودی هر ایستگاه تعیین می شود، از اینرو به این روش، TDM آماری^۱ نیز گفته می شود.



شکل (۲-۵۴): مثالی از یک سیستم TDM همزمان

۲-۶-۳- کاربردهای تسهیم سازی کانال

هر دو نوع تسهیم سازی به صورت زمانی و فرکانسی از مدت ها قبل در شبکه های تلفن به طور وسیعی مورد استفاده قرار گرفته است. به طور کلی شبکه های تلفن به دو دسته آنالوگ و دیجیتال تقسیم بندی می شوند که در زیر به بررسی آنها می پردازیم.

۲-۶-۳-۱- سرویس سوئیچینگ آنالوگ

در شبکه های سوئیچینگ آنالوگ از دو سیم (در مواردی چهار سیم) از نوع به هم تابیده شده برای اتصال تلفن مشترک به مرکز تلفن شبکه استفاده می شود.

به این نوع اتصال در اصطلاح حلقه محلی^۲ گفته می شود. این سیستم ها، شبکه های تلفن سوئیچینگ محلی (PSTN^۳ نامیده می شوند. سیگنال ارسالی در حلقه محلی از نوع آنالوگ می باشد و پهنای باند آن معمولاً از فرکانس صفر تا ۴ کیلو هرتز می باشد. در خطوط سوئیچینگ هنگامی که یک مشتری اقدام به شماره گیری می کند، مکالمه مورد نظر به

^۱ Statistical TDM

^۲ local loop

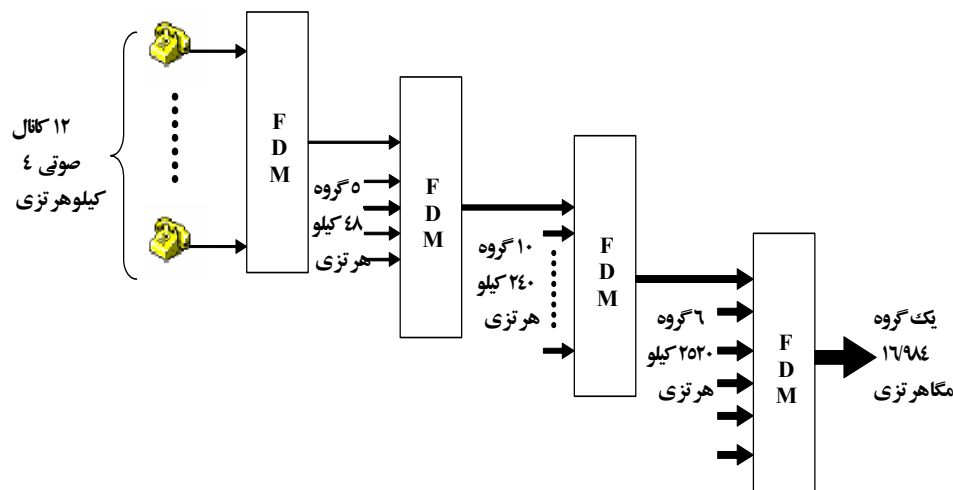
^۳ Public Switched Telephone Network

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

سمت یک یا چند سوئیچ هدایت می شود. بعد از انتخاب سوئیچ مناسب، ارتباط بین دو طرف مکالمه از طریق کانال های ارتباطی بین سوئیچ ها برقرار می شود.

- سرویس خطوط استیجاری آنالوگ

در این نوع سرویس بین دو مشترک یک کانال اختصاصی از نوع استیجاری وجود دارد، بنابراین هر مشترک به طور مستقیم و دائمی با مشترک دیگر متصل است. در این نوع سرویس نیازی به شماره گیری نمی باشد. برای استفاده بهینه از ظرفیت شبکه تلفن، شرکت هایی تلفن با استفاده از تسهیم سازها سیگنال های ورودی را از خطوط پهنای باند پایین به خطوط پهنای باند بالاتر تسهیم سازی می نمایند. معمولاً در خطوط آنالوگ از روش تسهیم سازی FDM استفاده می شود. نمونه ای از سیستم سلسله مراتبی آنالوگ^۱ که AT&T از آن استفاده می نماید در شکل (۲-۵۵) نشان داده شده است.



شکل (۲-۵۵): نمونه ای از سیستم سلسله مراتبی آنالوگ AT&T

مطابق با شکل فوق، ۱۲ کانال صوتی با یکدیگر تسهیم سازی شده و تشکیل یک گروه با پهنای باند ۴۸ کیلوهرتز می دهند. در سطح بعدی، ۵ گروه با یکدیگر تسهیم سازی می شوند و تشکیل یک ابرگروه با ظرفیت ۲۴۰ کیلوهرتز می دهند. هر ابرگروه شامل ۶۰ کانال ۴ کیلوهرتز صوتی می باشد. در سطح بعدی ۱۰ ابرگروه با یکدیگر تسهیم سازی شده و تشکیل یک گروه بزرگ^۲ می دهند.

هر گروه بزرگ دارای پهنای باند ۲/۵۲ مگاهرتز می باشد که می تواند ۶۰۰ کانال صوتی را پشتیبانی نماید. مقداری از پهنای باند هر گروه بزرگ (۱۲۰ کیلوهرتز) به عنوان محافظ بین کانال های صوتی استفاده می شود. در آخرین مرحله، ۶ گروه بزرگ با یکدیگر ترکیب می شوند و تشکیل یک گروه بسیار بزرگ^۳ می دهند.

هر گروه بسیار بزرگ دارای پهنای باند ۱۵/۱۲ مگاهرتز می باشد، اما با در نظر گرفتن باندهای محافظ، هر گروه بسیار بزرگ دارای پهنای باند ۱۶/۹۸۴ مگاهرتز می باشد، که قادر به پشتیبانی از ۳۶۰۰ کانال صوتی ۴ کیلوهرتز است.

^۱ Analog hierarchy

^۲ Master group

^۳ Jumbo group

۲-۳-۶-۲ - سرویس سوئیچینگ دیجیتال

امروزه اکثر شرکت‌هایی تلفن از سرویس دیجیتال برای سرویس‌دهی به مشترکین خود استفاده می‌کنند. یکی از مزایای عمده سرویس دیجیتال، حساسیت کم آن به نویز و تداخل می‌باشد. در شبکه های آنالوگ، نویز و سیگنال ارسالی هردو آنالوگ بوده و به آسانی از یکدیگر قابل جداسازی نیستند. اما در سیستم‌های دیجیتال از آنجایی که سیگنال ارسالی از نوع دیجیتال است جداسازی آن از نویز آسانتر می‌باشد. یکی دیگر از مزایای ارسال دیجیتال هزینه کم آن است. از آنجایی که در سیستم‌های دیجیتال از دو یا سه سطح ولتاژ استفاده می‌شود در مقایسه با تجهیزات آنالوگ که یک محدوده پیوسته از ولتاژ استفاده می‌نمایند، تجهیزات دیجیتال ارزانتر می‌باشد. سرویس دیجیتال به سه نوع تقسیم بندی می‌شوند که عبارتند از:

۱- سرویس سوئیچ شده ۵۶/۱

۲- سرویس داده دیجیتال DDS^۲

۳- سرویس سیگنال دیجیتال DS^۳

سرویس سوئیچ شده ۵۶/۱: این سرویس درحقیقت نسخه دیجیتال از خطوط سوئیچ شده آنالوگ می‌باشد. در این نوع سرویس حداکثر نرخ ارسال ۵۶ کیلو بیت بر ثانیه است. برای برقراری ارتباط از طریق این سرویس، هر دو طرف ارتباط باید مشترک سرویس باشند. بنابراین یک کاربر شبکه تلفن معمولی، حتی با داشتن مودم قادر به برقراری ارتباط با مشترک سرویس سوئیچ شده ۵۶/۱، نمی‌باشد. از آنجایی که در این نوع سرویس خطوط ارتباطی دیجیتال می‌باشند، مشترکین برای ارسال داده های دیجیتال نیازی به استفاده از مودم ندارند، بلکه در عوض مشترکین فوق از یک وسیله خاصی به نام واحد سرویس دیجیتال (DSU^۴) استفاده می‌نمایند. واحد سرویس دیجیتال وظیفه تنظیم سرعت داده های ارسالی کاربر، به ۵۶ کیلو بیت بر ثانیه و قالب بندی آنها به نحوی که قابل ارسال در شبکه باشد را دارد. هرچند واحد سرویس دیجیتال به مراتب از مودم گرانتر است اما به خاطر سرعت بیشتر، کیفیت بالاتر و نویز پذیری کمتر خطوط دیجیتال، استفاده از این سرویس به مراتب بر سرویس آنالوگ ترجیح داده می‌شود. در این سرویس کاربران با استفاده از بیشتر از یک خط ارتباطی قادر به دستیابی به سرعت‌های بالاتر می‌باشند. با استفاده از این ویژگی، کاربران قادر به تخصیص پهنای باند درخواستی خود برای ارائه سرویسی نظیر کنفرانسهای ویدئویی، فاکس سریع، سرویس چند رسانه ای و ارسال داده با سرعت بالا می‌باشند.

سرویس DDS: این سرویس درحقیقت یک نسخه دیجیتال از خطوط استیجاری آنالوگ می‌باشد. بنابراین می‌توان به آن خطوط استیجاری دیجیتال گفت. حداکثر سرعت سرویس DDS مشابه سرویس سوئیچ شده ۵۶/۱ برابر با ۵۶ کیلو بیت بر ثانیه است. البته در این سرویس کاربران قادر به انتخاب یکی از نرخ‌های ارسال ۲/۴، ۴/۸، ۹/۶، ۱۹/۲، و یا ۵۶ کیلو بیت بر ثانیه می‌باشند. مشابه سرویس سوئیچ شده ۵۶/۱ در سرویس DDS نیز از واحد سرویس دیجیتال استفاده می‌شود. واحد سرویس دیجیتال برای سرویس DDS به دلیل آنکه نیازی به پانل شماره گیری نمی‌باشد، ارزانتر از سیستم سوئیچ شده ۵۶/۱ است.

سرویس DS: بعد از ارائه سرویس سوئیچ شده ۵۶/۱ و DDS، شرکت‌هایی تلفن به دنبال ارائه سرویسی بودند تا مشابه سرویس آنالوگ بتوان در آنها از سیستم سلسله مراتبی استفاده نمود. بدین منظور سرویس DS که یک سیستم

^۱ Switched/56

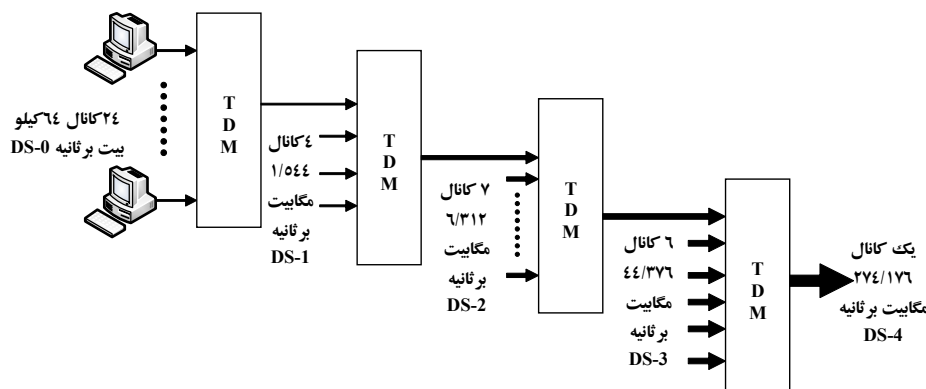
^۲ Digital Data Service

^۳ Digital Signal Service

^۴ Digital Service Unit

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

سلسله مراتبی سیگنال های دیجیتال است ارائه گردید . در شکل (۲-۵۶) یک سیستم سلسله مراتبی DS نشان داده شده است . مطابق با شکل فوق ۲۴ کانال DS-0 که هر کدام دارای سرعت ۶۴ کیلو بیت بر ثانیه می باشند با یکدیگر با استفاده از تسهیم سازی زمانی TDM ترکیب شده و تشکیل یک کانال DS-1 با سرعت ۱/۵۴۴ مگابیت بر ثانیه می دهند . در هر کانال DS-1 ، ۸ کیلو بیت بر ثانیه به عنوان بالاسری استفاده می شود. در مرحله بعدی ۴ کانال DS-1 (۹۶ کانال DS-0) با یکدیگر ترکیب می شوند و تشکیل یک کانال DS2 با سرعت ۶/۳۱۲ مگابیت بر ثانیه می دهند. در مرحله بعدی ۷ کانال DS-2 (۶۷۲ کانال DS-0) با یکدیگر ترکیب می شوند و تشکیل یک کانال DS-3 با سرعت ۴۴/۳۷۶ مگابیت بر ثانیه می دهند . در هر کانال DS-3 ، ۱/۳۶۸ مگابیت بر ثانیه به عنوان بالاسری استفاده می شود . در مرحله بعدی ۶ کانال DS-3 (۴۰۳۲ کانال DS-0) با یکدیگر ترکیب می شوند و تشکیل یک کانال DS-4 با سرعت ۲۷۴/۱۷۶ مگابیت بر ثانیه می دهند. در هر کانال DS-4 ، ۱۶/۱۲۸ مگابیت بر ثانیه به عنوان بالاسری استفاده می شود . معمولاً برای پیاده سازی سرویس DS شش رکت های تلفنی از خط T و متناظر آن در سرویس DS آورده شده است . (T1 تا T4) استفاده می کنند . در جدول (۲-۹) نرخ ارسال خطوط T و متناظر آن در سرویس DS آورده شده است .



شکل (۲-۵۶): یک سیستم سلسله مراتبی DS

جدول (۲-۹): نرخ ارسال خطوط T و متناظر آن در سرویس DS

تعداد کانال های صوتی معادل	نرخ ارسال (مگابیت بر ثانیه)	خط T	سرویس DS
۲۴	۱/۵۴۴	T1	DS-1
۹۶	۶/۳۱۲	T2	DS-2
۶۷۲	۴۴/۳۷۶	T3	DS-3
۴۰۳۲	۲۷۴/۱۷۶	T4	DS-4

خطوط T از نوع دیجیتال می باشند و برای ارسال داده های دیجیتال و یا سیگنال های صوت و تصویر دیجیتال شده به کار می روند. در مواردی می توان از آنها برای ارسال آنالوگ نیز استفاده نمود. بدین منظور سیگنال های آنالوگ ابتدا باید نمونه برداری شوند و سپس با روش تسهیم سازی زمانی به اطلاعات دیجیتال تبدیل گردند. کشورهای اروپایی از خطوط E که نسخه ای از خطوط T می باشد استفاده می نمایند . هر دو سیستم از نظر مفهومی مشابه یکدیگر می باشند، ولی سرعت های ارسال آنها با یکدیگر متفاوت است .

جدول (۲-۱۰) نرخ ارسال خطوط E را نشان می دهد .

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

جدول (۲-۱۰): نرخ ارسال خطوط E

خط E	نرخ ارسال (مگابیت بر ثانیه)	تعداد کانال های صوتی معادل
E1	۲/۰۴۸	۳۰
E2	۸/۴۴۸	۱۲۰
E3	۳۴/۳۶۸	۴۸۰
E4	۱۳۹/۲۶۴	۱۹۲۰

علاوه بر سرویس دیجیتال فوق، امروزه شرکت هایی تلفن از سرویس دیگری نظیر^۱ ISDN، NET^۲ و ATM^۳ استفاده می نمایند که در فصل های بعدی آنها را توضیح خواهیم داد.

۲-۷- فن آوری خط دیجیتال نامتقارن مشترکین (ADSL^۴)

روش های موجود فعلی برای ارسال و دریافت داده ها در سرعت بالا تقریباً پر هزینه می باشد. شرکت هایی بزرگ برای اتباط های راه دور خود معمولاً از خطوط مایکروویو و ماهواره استفاده می کنند و برای انتقال داده ها و اتباط های تلفنی از خطوط گران قیمت T1 و E1 به صورت اجاره ای بهره می برند. به علت هزینه بالای اشتراک خطوط فوق، شرکت هایی متوسط و کوچک قادر به استفاده از فن آوری های فوق برای اتباط های خود نمی باشند. بدین منظور فن آوری ADSL ارائه شده است. با استفاده از خطوط تلفن موجود و با بهره بردن از فن آوری ADSL شرکت های و فراهم کنندگان سرویس اینترنت قادر به برقراری ارتباط خصوصی با سرعت بالا می باشند.

خطوط سیم مسی تلفن برای حمل صوت و یا سیگنال های مودم در محدوده فرکانسی صفر تا ۳۴۰۰ هرتز با حداکثر سرعت ۵۶ کیلوبایت ثانیه طراحی شده است. این خطوط باند باریک و فرکانس پایین امکان انتقال بدون تضعیف زیاد سیگنال تا حداکثر ۵۵۰۰ متر را فراهم می آورد. متأسفانه ارسال سیگنال های فرکانس بالا بر روی خطوط مسی باعث تضعیف انرژی و تداخل می گردد که این امر موجب اختلال در ارسال داده می شود. به خاطر عدم وجود تضعیف زیاد، فیبر نوری برای ارسال سریع داده های کامپیوتری در فواصل طولانی بسیار مناسبتر از سیم های مسی می باشد، اما باید توجه نمود که فیبرهای نوری به مراتب گران قیمت تر از سیم های مسی می باشند. با استفاده از فن آوری ADSL امکان افزایش ظرفیت خطوط مسی برای پشتیبانی از ارسال داده های سرعت بالا مانند کنفرانس های ویدئویی، سرویس محیط چند رسانه ای و دسترسی سریع به اینترنت فراهم می آید. در حقیقت ADSL نوع مهمی از خانواده فن آوری خط دیجیتال مشترکین (DSL^۵) می باشد. هنگامی که مودم و منشعب کننده^۶ با هم استفاده می شوند، فن آوری ADSL مطابق با شکل (۲-۵۷) امکان ارائه توأم با هم سرویس تلفن و ارسال داده های سرعت بالا را از طریق خطوط تلفن فراهم می سازد. در فن آوری ADSL از یک زوج سیم به هم تابیده شده مسی برای مصارف زیر استفاده می شود:

الف) اتباط های تلفنی معمولی در فاصله فرکانسی صفر تا ۳۴۰۰ هرتز

ب) ارسال داده ها از طرف مشتری در فاصله ۳۰ تا ۱۳۸ کیلو هرتز

^۱ Integrated Services Digital Network

^۲ Synchronous Optic Network

^۳ Asynchronous Transfer Mode

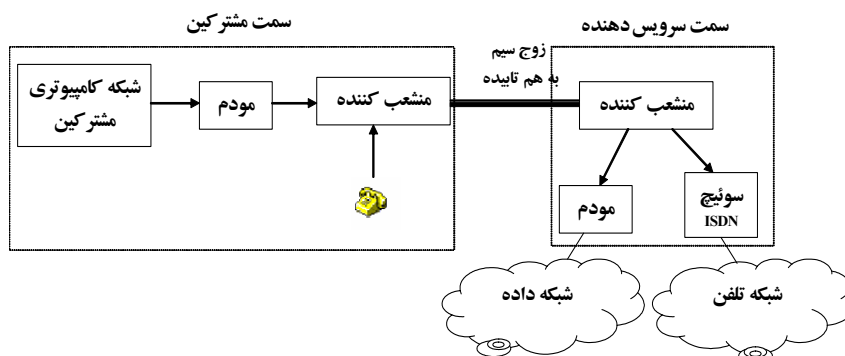
^۴ Asymmetric Digital Subscriber Line

^۵ Digital Subscriber Line

^۶ Splitter

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

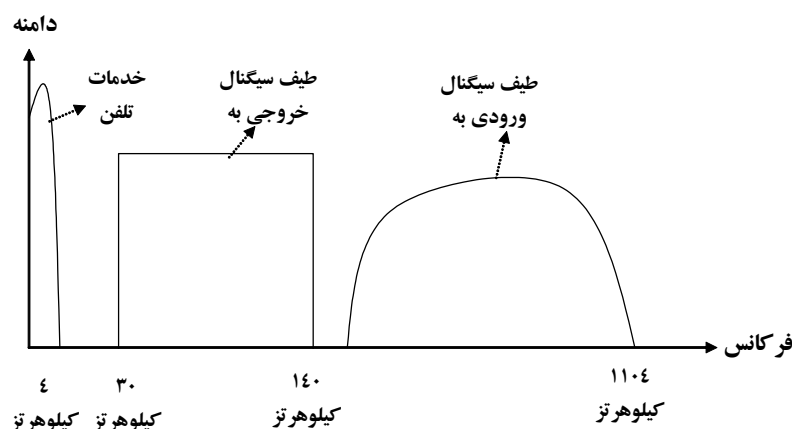
ج) انتقال داده ها به سمت مشتری در حداکثر فرکانس ۱۱۰۴ کیلوهرتز



شکل (۲-۵۷): پیکره بندی ADSL

در شکل (۲-۵۸) طیف فرکانسی ADSL نشان داده شده است. از آنجایی که در ADSL سیگنال های خروجی در محدوده فرکانسی ۳۰ کیلوهرتز تا ۱۴۰ کیلوهرتز و سیگنال های ورودی در محدوده فرکانسی تا حداکثر ۱۱۰۴ کیلوهرتز قرار دارند، بنابراین ظرفیت ارسال داده در جهت ارسال ۶۴۰ کیلو بیت بر ثانیه و در جهت دریافت ۶۱۴۴ کیلو بیت بر ثانیه می باشد. به خاطر تفاوت نرخ ارسال و دریافت در ADSL به این فن آوری ارسال نامتقارن گفته می شود. دلیل نامتقارن بودن سرعت ارسال و دریافت در ADSL کاهش القای متقابل می باشد.

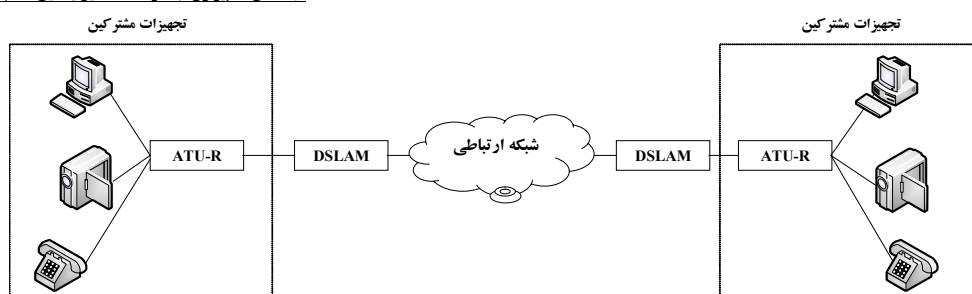
در سمت مشترکین ADSL یک واحد فرستنده گیرنده ADSL به نام ATU-R قرار می گیرد. در سمت شبکه ارتباطی نیز یک تسهیم ساز دسترسی به خطوط دیجیتال مشترکین (DSLAM^۱) وجود دارد. با استفاده از یک تسهیم ساز فوق؛ امکان جابجایی و هدایت ترافیک های ورودی چندین ATU-R وجود دارد. از شبکه های ارتباطی موجود برای ارتباط بین تسهیم کننده های دسترسی به خطوط مشترکین دیجیتال استفاده می شود. در شکل (۲-۵۹) نمونه ای از پیکربندی شبکه نقطه به نقطه ADSL نشان داده شده است که در آن امکان ارائه سرویس باند وسیع به مشترکین فراهم می آید.



شکل (۲-۵۸): طیف فرکانسی سیگنال های ADSL

^۱ Digital Subscriber Line Access Multiplexer

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۲-۵۹): پیکربندی نقطه به نقطه ADSL

از آنجایی که سیم کشی تلفن در اغلب ساختمان ها وجود دارد نیازی به کانال کشی برای پیاده سازی سرویس ADSL نمی باشد. در سرویس ADSL امکان دریافت داده ها در سرعت حداکثر ۶۱۴۴ کیلو بیت بر ثانیه وجود دارد که با مقایسه سرعت مودم های استاندارد ۵۶ کیلو بیت بر ثانیه به مراتب بیشتر می باشد. فن آوری ADSL در مقایسه با سایر فن آوری های موجود نظیر ISDN و خطوط T و E دارای مزایای زیر است:

الف) هزینه نصب و بهره برداری از تجهیزات ADSL بسیار پایین است.

ب) سرعت ارسال و دریافت در ADSL برای سرویسی نظیر ارسال داده های سریع و کنفرانس های ویدئویی بالا می باشد.

ج) استفاده از ADSL ساده است. اتصال به اینترنت از طریق ADSL نیاز به هیچ گونه شماره گیری ندارد.

در جدول (۲-۱۱) جدیدترین استانداردهای موجود ADSL آورده شده است.

جدول (۲-۱۱): جدیدترین استانداردهای موجود ADSL

نام استاندارد	نام متعارف	سرعت دریافت	سرعت ارسال
ANSI T1.413-1998 Issue 2	ADSL	۸ مگابیت بر ثانیه	۱ مگابیت بر ثانیه
ITU G.992.1	ADSL (G.DMT)	۱۲ مگابیت بر ثانیه	۱/۳ مگابیت بر ثانیه
ITU G.992.1 Annex A	ADSL over POTS	۱۲ مگابیت بر ثانیه	۱/۳ مگابیت بر ثانیه
ITU G.992.1 Annex B	ADSL over ISDN	۱۲ مگابیت بر ثانیه	۱/۸ مگابیت بر ثانیه
ITU G.992.2	ADSL Lite (G.Lite)	۴ مگابیت بر ثانیه	۰/۵ مگابیت بر ثانیه
ITU G.992.3/4	ADSL2	۱۲ مگابیت بر ثانیه	۱ مگابیت بر ثانیه
ITU G.992.3/4 Annex J	ADSL2	۱۲ مگابیت بر ثانیه	۳/۵ مگابیت بر ثانیه
ITU G.992.3/4 Annex L	RE-ADSL2	۵ مگابیت بر ثانیه	۰/۸ مگابیت بر ثانیه
ITU G.992.5	ADSL2+	۲۴ مگابیت بر ثانیه	۱ مگابیت بر ثانیه
ITU G.992.5 Annex L ^[1]	RE-ADSL2+	۲۴ مگابیت بر ثانیه	۱ مگابیت بر ثانیه
ITU G.992.5 Annex M	ADSL2+M	۲۴ مگابیت بر ثانیه	۳/۵ مگابیت بر ثانیه

پرسش‌های فصل

- [illegible]

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

۲۹. ویژگی های واسط RS232 را توضیح داده و پین های مهم آن را بنویسید.
۳۰. مودم را تعریف کرده و کاربرد آن را توصیف نمایید.
۳۱. مراحل برقراری یک ارتباط مودمی را با رسم شکل توصیف نمایید.
۳۲. موارد استفاده کابل نال مودم را نوشته و ساختار آن را رسم کنید.
۳۳. مودم های هوشمند را توضیح دهید.
۳۴. مهم ترین دستورات AT را نام برده و مورد کاربرد هر دستور را بنویسید.
۳۵. زوج سیم به هم تابیده و انواع آن را توضیح دهید.
۳۶. ساختمان یک کابل هم محور را توصیف نموده و انواع آن را نام برید.
۳۷. اساس کار فیبر نوری و انواع آن را توصیف نمایید.
۳۸. یک سیستم انتقال فیبر نوری از چه قسمت هایی تشکیل شده است؟ وظیفه هر قسمت را توضیح دهید.
۳۹. امواج رادیویی از نظر فرکانس به چند دسته تقسیم می شوند؟
۴۰. انواع انتشار امواج رادیویی را توضیح دهید.
۴۱. مورد کاربرد سیستم های میکروویو را بنویسید.
۴۲. اساس کارمخابرات ماهواره ای و قسمت های تشکیل دهنده آن را توصیف نمایید.
۴۳. اصول کار سیستم های تلفن سلولی را توضیح دهید.
۴۴. مشخصه های کارآیی رسانه های انتقال را نام برده و هر مشخصه را توضیح دهید.
۴۵. رسانه های انتقال موجود را با یکدیگر مقایسه نموده و نقطه ضعف و برتری هر رسانه را با سایر رسانه های دیگر توصیف نمایید.
۴۶. تسهیم سازی را توضیح داده و انواع آن را تشریح نمایید.
۴۷. بلوک دیاگرام عملیاتی یک سیستم FDM را رسم کرده و وظایف قسمت های مختلف آن را بنویسید.
۴۸. روش TDM همزمان و TDM غیرهمزمان را با یکدیگر مقایسه نمایید.
۴۹. سیستم سلسله مراتبی آنالوگ AT&T را رسم نمایید.
۵۰. عملکرد و موارد کاربرد سرویس سوئیچ شده/۵۶ را تشریح نمایید.
۵۱. عملکرد سرویس داده دیجیتال (DDS) را نوشته و تفاوت آن را با سرویس سوئیچ شده/۵۶ بنویسید.
۵۲. سیستم سلسله مراتبی DS را تشریح نمایید.
۵۳. فن آوری ADSL را توضیح داده و مزایای آن را بنویسید.
۵۴. نمودار پهنای باندی سیستم های ADSL را رسم نمایید.

فصل سوم

لایه پیوند داده

۳-۱- مقدمه

در این فصل به بررسی لایه پیوند داده و وظایف مهم آن می پردازیم. در لایه فیزیکی که در فصل قبل به بررسی آن پرداختیم، داده های ارسالی در قالب رشته بیت های ۱ و ۰ به سیگنال های الکتریکی مناسب تبدیل می شوند و وارد محیط انتقال می گردند. حال برای کنترل داده ها و تعیین این که کدام یک از کامپیوترهای متصل به کانال باید داده های ارسالی را دریافت دارند، از مکانیسم های کنترلی لایه دوم استفاده می شود. لایه پیوند داده براساس وضعیت کانال و نحوه اتصال ایستگاه ها به یکدیگر، عملیات خود را انجام می دهد. مثلاً در کانال های دو طرفه امکان ارسال همزمان داده در طرفین کانال وجود دارد، درحالی که در کانال های یک طرفه چنانچه همزمان ایستگاه ها اقدام به ارسال نمایند، تداخل به وجود می آید. بنابراین لایه دوم باید براساس نوع کانال طراحی شود. لایه پیوند داده دو وظیفه عمده زیر را به عهده دارد:

- **کنترل جریان:** جهت جلوگیری از اتلاف داده ها در گیرنده، کنترل سرعت ارسال فرستنده و تنظیم آن با سرعت دریافت گیرنده مهم می باشد. این عملیات کنترل جریان نام دارد.
- **کنترل خطا:** لایه پیوند داده با استفاده از مکانیسم های کنترل خطا، متوجه وقوع خطا در کانال ارسالی می شود و در این صورت اقدامات لازم برای تصحیح خطا و یا درخواست ارسال مجدد داده ها را از گیرنده انجام می دهد. در کنترل خطا دو مسئله متفاوت مطرح است که عبارتند از: تشخیص خطا و تصحیح خطا.

۳-۲- کنترل جریان

یکی از وظایف بسیار مهم لایه پیوند داده، کنترل جریان می باشد. برای پی بردن به اهمیت مسئله فوق به مثالی توجه نمایید. فرض کنید که دو کامپیوتر به طور مستقیم از طریق یک کانال نقطه به نقطه به یکدیگر متصل شده اند. چنانچه کامپیوتر فرستنده با سرعتی بیشتر از آنچه کامپیوتر گیرنده قادر به دریافت آن است، اقدام به ارسال داده های خود بنماید، در این صورت طبیعی است که بعد از مدتی بافر گیرنده سرریز می شود و بعد از آن تمامی داده های ارسالی از بین خواهد رفت. یکی از روش های معمول برای رفع مشکل فوق، استفاده از روال های کنترل جریان می باشد. هنگامی که بافر گیرنده در آستانه پر شدن است، کامپیوتر گیرنده با ارسال پیامی از فرستنده درخواست می نماید که دیگر اطلاعاتی ارسال ننماید تا این که دوباره بافر آن خالی شود. در این لحظه گیرنده با ارسال پیام مناسبی به فرستنده از او می خواهد که دوباره ارسال اطلاعات را از سر بگیرد. معمولاً گیرنده با دریافت هریک یا هرچند قاب، اقدام به ارسال پیام تصدیق (ACK^1) مبنی بر دریافت صحیح قاب ها به فرستنده می نماید. با دریافت این پیام تصدیق، فرستنده از دریافت صحیح قاب توسط گیرنده اطمینان حاصل می نماید و قادر است سایر قاب ها را ارسال کند. در صورتی که قاب های دریافتی در سمت گیرنده معیوب باشد و گیرنده قادر به شناسایی و پردازش آنها نباشد، در این صورت پیام عدم تأیید (NAK^2) برای فرستنده ارسال می شود. دو روش کلی برای کنترل جریان وجود دارد که عبارتند از :

^۱ Acknowledge

^۲ Not-Acknowledge

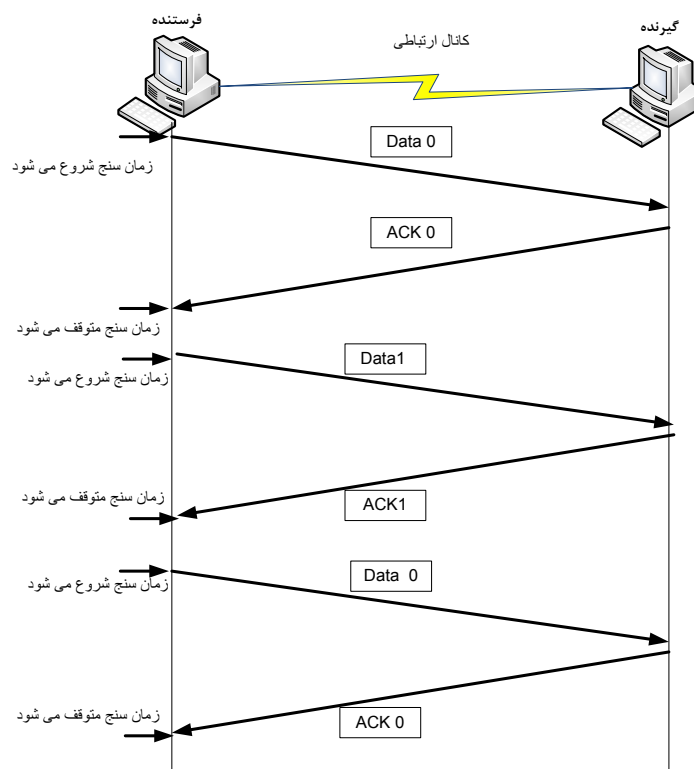
شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

- روش توقف و انتظار^۱
- روش پنجره لغزان^۲

در ادامه به بررسی هریک از دو روش فوق می پردازیم.

۳-۲-۱- روش توقف و انتظار

در این روش با ارسال هر قاب فرستنده منتظر دریافت پیام تصدیق از طرف گیرنده می ماند و هنگامی که پیام تصدیق قاب قبلی را دریافت نمود، قادر به ارسال قاب جدید می باشد. در شکل (۳-۱) مثالی از عملکرد روش توقف و انتظار آورده شده است. از آن جایی که در این روش، قبل از این که قاب بعدی ارسال شود، قاب قبلی بررسی می شود و از دریافت صحیح آن در گیرنده اطمینان حاصل می گردد، این امر باعث سادگی پیاده سازی پروتکل می شود که از مزایای عمده روش توقف و انتظار می باشد. عیب عمده این روش، بهره وری کم آن است. از آن جایی که با توجه به این که هر قاب باید مسیر فرستنده تا گیرنده را طی نماید و گیرنده نیز باید در جواب به قاب ارسالی پیام تصدیق ارسال نماید، بنابراین دیده می شود که در روش فوق، فرستنده باید مدت زیادی بی کار بماند که باعث کاهش سرعت و بهره وری کانال می گردد. نام دیگر روش فوق، ARQ^3 بی کار می باشد.



شکل (۳-۱): مثالی از روش توقف و ارسال

در روش توقف و انتظار با ارسال هر قاب یک زمان سنج خاص نیز فعال می گردد. چنانچه قبل از اتمام زمان زمان سنج، پیام تصدیق قاب ارسالی دریافت شود، در این صورت زمان سنج قطع می شود و قاب بعدی ارسال می گردد. ولی چنانچه

^۱ Stop and wait

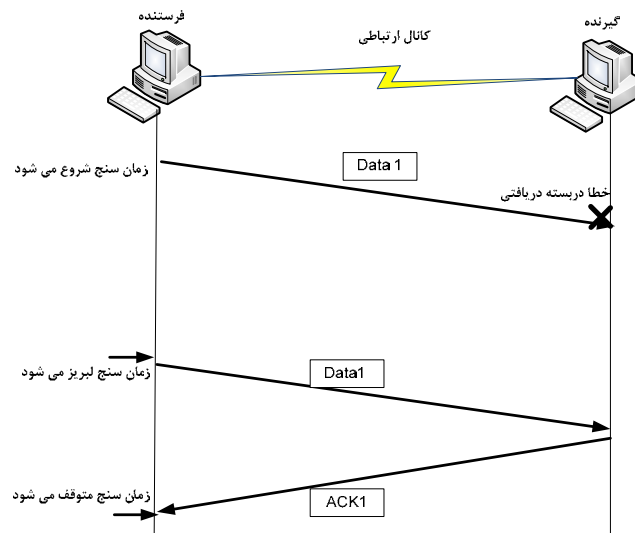
^۲ Sliding window

^۳ Automatic Repeat reQuest

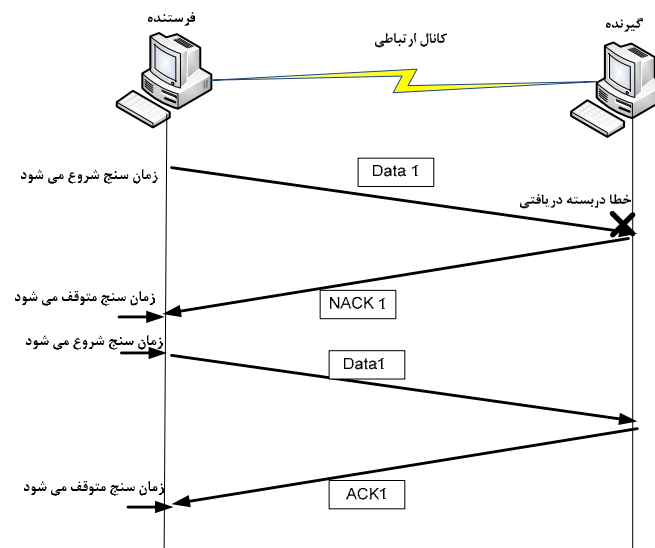
شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد^۱)

زمان سنج به پایان رسیده و پیام تصدیق قاب ارسالی دریافت نشود، در این صورت فرستنده متوجه بروز مشکلی در سیستم می شود و دوباره قاب قبلی را ارسال می کند. در این روش تنها به دو شماره قاب (۰ و ۱) نیاز می باشد.

برای پیاده سازی این روش دو راه حل وجود دارد. روش ضمنی و روش صریح. در روش ضمنی مقصد تنها برای دادهای صحیح تصدیق می فرستد و مبدا در صورت عدم دریافت تصدیق به بطور ضمنی نتیجه می گیرد داده قبلی خراب شده است. و در روش صریح گیرنده با تشخیص قاب خراب یک پیام عدم تصدیق می دهد تا درخواست کپی مجدد نماید. در شکل (۳-۲) الف و ب مثالی از عملکرد روش توقف و انتظار آورده شده است.



(الف)



(ب)

شکل (۳-۲): (الف) روش توقف و ارسال با ارسال مجدد ضمنی (ب) روش توقف و ارسال با ارسال مجدد صریح

۳-۲-۱-۱- بهر وری کانال^۱

¹ Channel utilization

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

در این قسمت بهره وری ظرفیت قابل دسترس کانال را در پروتکل توقف و انتظار بدست می آوریم. بهره وری کانال (U) بصورت حاصل تقسیم دو زمان از لحظه ارسال قاب می باشد و بصورت زیر تعریف می شود:

$$U = \frac{T_{ix}}{T_t}$$

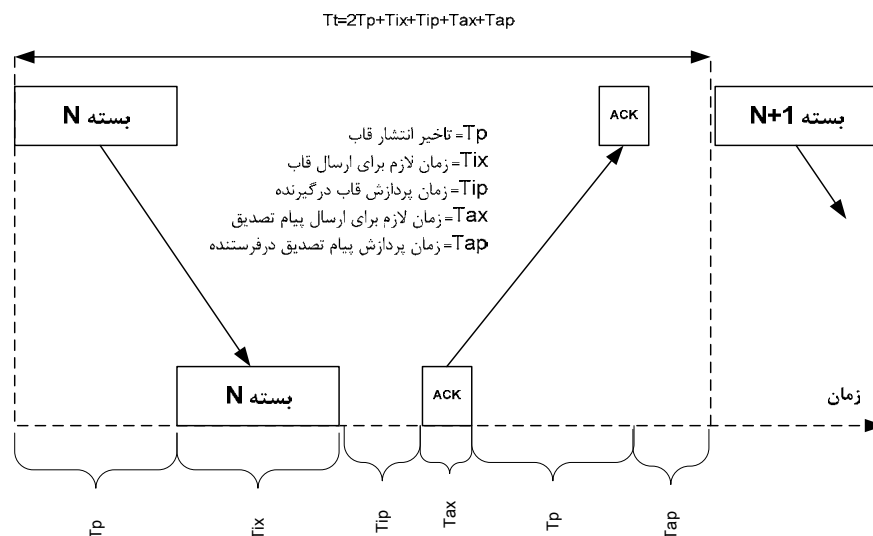
که T_{ix} زمان مورد نیاز فرستنده برای ارسال قاب و T_t برابر T_{ix} بعلاوه مقدار زمانی است که فرستنده برای دریافت پیام تصدیق منتظر می ماند.

برای محاسبه بهره وری کانال در روش توقف و انتظار، در شکل (۳-۳) یک دیاگرام ترتیب قاب با عناصر مختلف زمانی نشان داده شده است. در عمل و در بیشتر شرایط، زمان پردازش یک قاب اطلاعاتی T_{ip} و قاب تصدیق مربوط به آن T_{ap} هردو نسبت به زمان ارسال T_{ix} و T_{ax} کوچک هستند. همچنین از آنجائیکه یک قاب تصدیق بسیار کوتاهتر از یک قاب اطلاعاتی است، T_{ax} نسبت به T_{ix} قابل چشم پوشی است. از اینرو حداقل زمان کلی قبل از ارسال قاب بعدی تقریباً معادل $T_{ix} + 2T_p$ است. از اینرو یک رابطه تخمینی برای U بصورت زیر است:

$$U = \frac{1}{1 + 2T_p / T_{ix}} \quad \text{یا} \quad U = \frac{T_{ix}}{T_{ix} + 2T_p}$$

نسبت T_p / T_{ix} معمولاً با a نشان داده می شود و از اینرو:

$$U = \frac{1}{1 + 2a}$$



شکل (۳-۳): شمای بهره وری کانال در روش توقف و انتظار

برای کانال های نسبتاً کوتاه که مقدار a کمتر از ۱ است، بهره وری کانال با تقریباً خوب برابر با ۱۰۰٪ بوده و مستقل از نرخ داده است. به عبارت دیگر پروتکل توقف و انتظار برای کانال های کوتاه و نرخ داده متوسط کافی است. برای مثال شبکه هایی مبتنی بر مودم و تلفن عمومی آنالوگ را می توان نام برد. در خطوط طولانی تر زمینی، بهره وری خط برای نرخ های داده پایین (و از اینرو مقادیر کم a) بالا است اما با افزایش نرخ داده (و از اینرو a) بطور قابل ملاحظه ای کاهش می یابد. بهره وری کانال برای خطوط ماهواره حتی با نرخ داده پایین ضعیف است. می توان نتیجه گرفت که پروتکل توقف و انتظار

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

برای این قبیل کاربردها و خطوط زمینی با سرعت بالا مثل شبکه های محلی و اکثر شبکه های گسترده عمومی مناسب نیست.

در محاسبات بهره وری کانال که در بالا اشاره شد، فرض براین بود که هیچ خطای ارسالی وجود ندارد. در عمل مقدار نرخ خطای بیت (BER^1) مربوط به خط غیر صفر است. از اینرو برای ارسال موفقیت آمیز یک قاب، متوسط تعداد ارساله های مجدد N_r لازم است. با اصلاح رابطه بهره وری کانال می توانیم عبارت زیر را بدست آوریم:

$$U = \frac{T_{ix}}{N_r T_{ix} + 2N_r T_p} = \frac{1}{N_r (1 + \frac{2T_p}{T_{ix}})}$$

مقدار N_r با توجه به مقدار BER موجود در کانال که با P نمایش داده می شود، بدست می آید. اگر P احتمال خرابی بیتی باشد، با فرض خطاهای تصادفی، احتمال اینکه قابی بطول N_i بیت بدون خطا دریافت شود برابر است با:

$$P_f = 1 - (1 - P)^{N_i}$$

از اینرو احتمال دریافت قابی با خطا برابر است با: اگر $N_i P \ll 1$ ، $N_i P \approx 1 - (1 - P)^{N_i} \approx P_f$. حال اگر P_f احتمال خرابی یک قاب باشد، $(1 - P_f)$ احتمال این است که یک قاب سالم دریافت شود. از اینرو:

$$N_r = \frac{1}{1 - P_f}$$

برای مثال اگر $P_f = 0.5$ و $N_r = 2$ ، یعنی اگر بطور متوسط ۵۰٪ قابها خراب شوند، هر قاب باید دوبار ارسال شود. این مقدار زیاد است چرا که با فرض عدم خرابی قابهای تصدیق ۵۰٪ قابهای دوباره ارسال شده نیز خراب خواهند شد. بدلیل طول کوتاه نسبت به قابهای اطلاعاتی، این یک فرض معقولی است. در عمل همه مقادیر کارایی خط باید تقسیم بر N_r شوند. یعنی:

$$U = \frac{1 - P_f}{1 + 2a}$$

مزیت بزرگ پروتکل توقف و انتظار حداقل بافر مورد نیاز آن است، چرا که هردو فرستنده و گیرنده فضای کافی برای تنها یک قاب را دارند. بعلاوه، S باید شناسه ای از آخرین قاب دریافتی صحیح را داشته باشد تا بتواند از قابهای تکراری را تشخیص دهد. از آنجائیکه توقف و انتظار فضای کمی نیاز دارد، بطور گسترده در کاربردهایی بکار می رود که از دستگاههای ساده (مثل پایانه یا کامپیوتر شخصی) در یک طرف خط استفاده می کنند.

۳-۲-۲- روش پنجره لغزان

چنانچه فاصله فرستنده و گیرنده از یکدیگر زیاد باشد، در این صورت طولانی بودن این فاصله باعث افزایش تأخیر بین ارسال قابها و کاهش بهره وری از کانال می شود. به عنوان مثال یک کانال ماهواره با سرعت ۵۰ کیلوبیت بر ثانیه را در نظر بگیرید که تأخیر انتشار رفت و برگشت در آن ۵۰۰ میلی ثانیه است. چنانچه فرستنده یک قاب ۱۰۰۰ بیتی را ارسال دارد با توجه به سرعت کانال ماهواره، ۲۰ میلی ثانیه بعد، ارسال قاب تمام شده است و ۲۷۰ میلی ثانیه بعد قاب به طور کامل به گیرنده می رسد. در صورتی که گیرنده همان لحظه پیام تصدیق ارسال دارد ۵۲۰ میلی ثانیه بعد فرستنده متوجه سالم رسیدن قاب ارسالی خود در گیرنده می شود. با این حساب اگر از روش توقف و انتظار استفاده شود، فرستنده در حدود ۹۶ (۵۲۰/۵۰۰) درصد از کانال را از دست داده است و فقط از ۴ درصد ظرفیت کانال استفاده می نماید. با این مثال متوجه

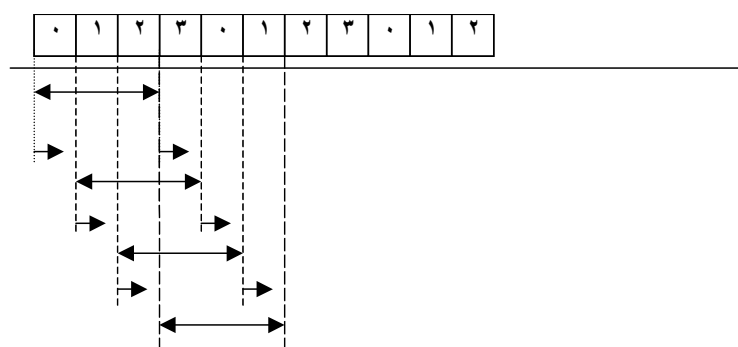
¹ Bit Error Rate

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

می‌شویم که چنانچه فاصله فرستنده تا گیرنده زیاد باشد و یا سرعت ارسال زیاد باشد و یا طول قاب ارسالی کوتاه باشد در این صورت کارایی سیستم به شدت پایین می‌آید و میزان بهره‌وری از کانال نیز کاهش می‌یابد.

یکی از دلایل بروز مشکل فوق آن است که فرستنده بعد از ارسال هر قاب باید مدتی صبر نماید تا پیام تأیید قاب ارسالی قبلی را دریافت نماید و سپس دوباره اقدام به ارسال قاب جدید کند. برای رفع مشکل فوق، می‌توان این محدودیت را از فرستنده برداشت و به آن این اجازه را داد که به‌طور مداوم و پشت سر هم اقدام به ارسال قاب نماید. این کار در روش پنجره لغزان صورت می‌گیرد.

روش پنجره لغزان که با نام ARQ پیوسته نیز نامیده می‌شود، از نظر سرعت و بهره‌وری از کانال به مراتب بهتر از روش قبل می‌باشد. در این روش فرستنده بدون آن که منتظر دریافت پیام تصدیق قاب‌های ارسالی قبلی خود باشد، اقدام به ارسال پیوسته قاب‌ها می‌نماید. گیرنده نیز به‌طور دسته جمعی با دریافت چندین قاب، اقدام به ارسال پیام تصدیق می‌نماید. کلمه پنجره در روش پنجره لغزان، نشان‌دهنده استفاده از بافر به طول مشخص (طول پنجره) در سمت فرستنده و گیرنده برای نگه‌داری قاب‌های ارسالی و دریافتی می‌باشد. طول پنجره نشان‌دهنده حداکثر تعداد قاب‌هایی می‌باشد که فرستنده بدون دریافت پیام تصدیق قادر به ارسال آنها است. البته در سمت گیرنده الزاماً نباید همه قاب‌های موجود در پنجره کامل شوند و بعد گیرنده پیام تصدیق ارسال نماید. قاب‌های ارسالی فرستنده به‌صورت پیمانه N (از شماره 0 تا $N-1$) شماره‌گذاری می‌شوند. در این حالت طول پنجره ارسال $N-1$ می‌باشد. به‌عنوان مثال چنانچه $N=8$ باشد، در این صورت قاب‌های ارسالی به‌صورت $0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 3, 4, 5, 6, 7, \dots$ شماره‌گذاری و ارسال می‌گردند. هنگامی که گیرنده پیام تصدیق مبنی بر دریافت صحیح یک قاب را ارسال می‌دارد، در پیام فوق شماره قاب بعدی را که انتظار دریافت آن را از گیرنده دارد، ذکر می‌نماید. حداکثر تعداد قاب‌هایی که هنوز پیام تصدیق آنها دریافت نشده است برابر با $N-1$ می‌باشد. در آغاز ارسال، پنجره فرستنده شامل $N-1$ قاب است. شماره ردیف موجود در پنجره ارسال، نمایشگر قاب‌هایی که فرستاده شده‌اند، ولی هنوز پیام تصدیق آنها نیامده است، می‌باشد. هرگاه لایه دوم فرستنده، یک قاب جدید از لایه شبکه دریافت نماید در این صورت، چنانچه پنجره ارسال به حداکثر مقدار خود نرسیده باشد، لایه بالایی پنجره یک واحد اضافه می‌شود. هنگامی که فرستنده پیام تصدیق مربوط به قاب‌های ارسالی قبلی خود را دریافت کرد، در این حالت لایه پایینی پنجره، یک واحد به جلو حرکت می‌کند. در شکل (۳-۴) مثالی از عملکرد پنجره لغزان آورده شده است. در این مثال طول پنجره ارسال برابر با ۳ می‌باشد (۴-۳). ($N=$

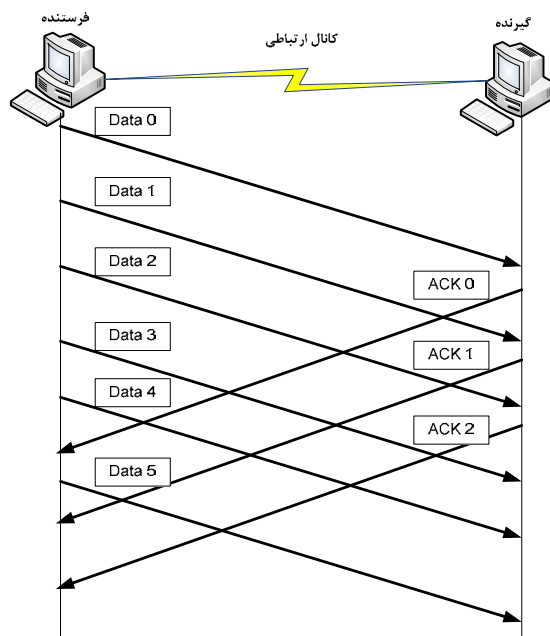


شکل (۳-۴): عملکرد پنجره لغزان

در روش پنجره لغزان این احتمال وجود دارد که قاب‌های موجود در پنجره ارسال در بین راه دچار اشکال شوند و از بین بروند. در این صورت فرستنده باید دوباره قاب‌های معیوب را ارسال کند. بنابراین فرستنده نیاز به یک بافر به اندازه طول

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

پنجره ارسال دارد تا قادر به نگهداری قاب‌های ارسالی باشد. هنگامی که قابی ارسال می‌شود یک کپی از آن در بافر ارسال نگهداری می‌گردد تا اگر برای آن مشکلی پیش آمد بتواند دوباره آن را ارسال کند. با دریافت پیام تصدیق هر قاب، فرستنده قاب را از بافر خود حذف می‌نماید. در سمت گیرنده نیز پنجره دریافت وجود دارد که طول آن می‌تواند با پنجره ارسال متفاوت باشد. هنگامی که طول پنجره دریافت گیرنده ۱ باشد، این بدان معنی است که در سمت گیرنده قاب‌ها باید به ترتیب دریافت شوند و اگر قابی خارج از ترتیب دریافت گردد، آن قاب باید از بین برود. برای جلوگیری از اتلاف ظرفیت کانال، در روش پنجره لغزان مشابه روش توقف و انتظار نیز با ارسال هر قاب یک زمان سنج فعال می‌شود و چنانچه در مدت زمان فعال بودن زمان سنج پیام تصدیق قاب ارسالی دریافت نشود، قاب قبلی دوباره ارسال می‌گردد. در شکل (۳-۵) مثالی از روش پنجره لغزان آورده شده است.



شکل (۳-۵): مثالی از روش پنجره لغزان

در پروتکل پنجره لغزان، دو استراتژی مختلف در مواجهه با خطا وجود دارد که عبارتند از: روش بازگشت به عقب به عقب به اندازه N ^۱ و روش تکرار انتخابی.^۲ در زیر به بررسی هریک از این دو روش می‌پردازیم.

۱-۲-۲-۳ روش بازگشت به عقب به اندازه N

در این روش چنانچه ضمن ارسال قاب‌ها خطایی به وجود آید و یکی از قاب‌ها معیوب شود، گیرنده از پذیرش همه قاب‌های دریافتی بعد از قاب معیوب خودداری می‌کند و هیچ پیام تصدیق ارسال نمی‌دارد و منتظر دریافت صحیح قاب معیوب می‌ماند. بنابراین دیده می‌شود که این روش نوعی روش پنجره لغزان با طول پنجره دریافت برابر با ۱ می‌باشد. در شکل (۳-۶) مثالی از عملکرد این روش آورده شده است.

در این مثال فرض بر آن است که قاب شماره ۲، ضمن ارسال دچار خطا شده است. گیرنده تمامی قاب‌های دریافتی بعدی را نادیده می‌گیرد و منتظر می‌ماند تا قاب شماره ۲ را دوباره دریافت کند. هنگامی که زمان سنج مربوط به قاب شماره

^۱ Go back N

^۲ Selective repeat

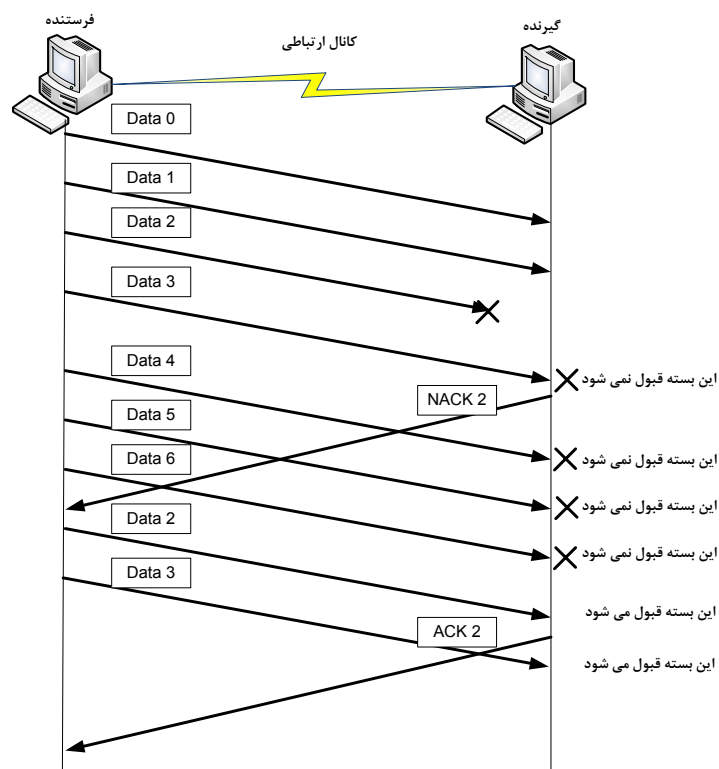
شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

۲ در سمت فرستنده منقضی شود و یا فرستنده پیام NACK دریافت کند، دوباره اقدام به ارسال قاب شماره ۲ و قاب های بعد از آن می نماید.

۳-۲-۲- روش تکرار انتخابی

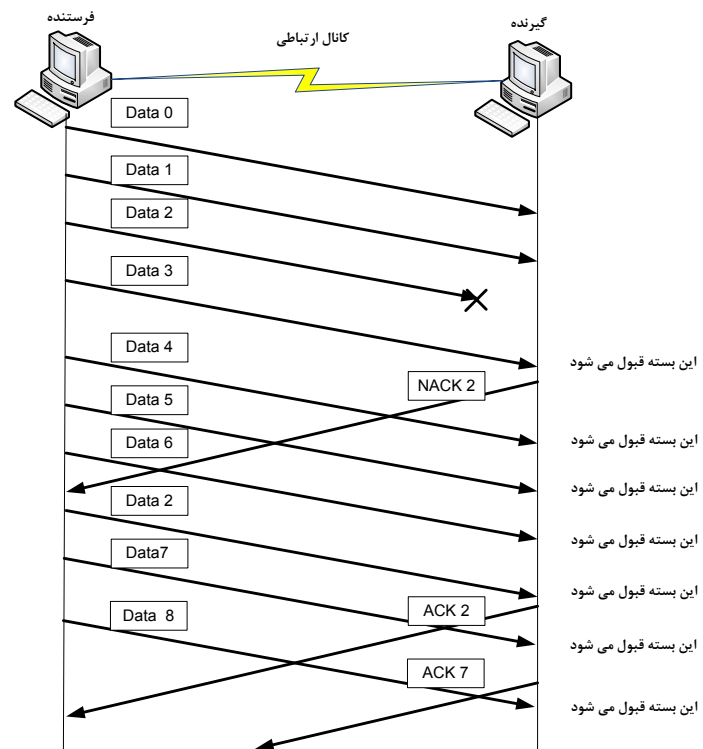
یکی دیگر از استراتژی های موجود در هنگام مواجهه با خطا در روش پنجره لغزان، تکرار انتخابی قاب های معیوب می باشد. در این روش چنانچه قابی با خطا مواجه شود و گیرنده آن را دریافت نکند، گیرنده تمامی قاب های ورودی بعد از قاب معیوب را دریافت می کند و در بافر خود ذخیره می نماید و برای قاب معیوب پیام عدم تصدیق ارسال می نماید. با دریافت این قاب، فرستنده اقدام به ارسال مجدد قاب معیوب می کند و برخلاف روش بازگشت به عقب به اندازه N ، نیازی به ارسال مجدد قاب های سالم ارسالی بعد از قاب معیوب نمی باشد. در شکل (۳-۷) مثالی از نحوه عملکرد روش تکرار انتخابی آورده شده است.

طبیعی است که در این روش، طول پنجره دریافت در سمت گیرنده بزرگتر از ۱ می باشد. با مقایسه دو روش تکرار انتخابی و بازگشت به عقب به اندازه N ، به این نتیجه می رسیم که در روش تکرار انتخابی میزان استفاده از ظرفیت کانال زیاد می باشد و به عبارتی اتلاف پهنای باند کمتری وجود دارد، ولی در مقابل به فضای بافر زیادی در گیرنده نیاز می باشد. روش بازگشت به عقب به اندازه N ، دارای میزان بهره وری کمتری از کانال نسبت به روش تکرار انتخابی است، ولی در مقابل گیرنده فقط به یک بافر به اندازه یک قاب نیاز دارد.



شکل (۳-۶): مثالی از عملکرد روش بازگشت به عقب به اندازه N

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۳-۷): مثالی از عملکرد روش تکرار انتخابی

۳-۲-۲-۳ بهره وری کانال

در بخش مربوط به پروتکل توقف و انتظار دیدیم که با تقریب نسبتاً خوبی بهره وری کانال، U ، تابعی از زمان T_{ix} برای ارسال یک قاب اطلاعاتی و تاخیر انتشاری خط T_p می باشد. بهر حال در کانال هایی با T_p بزرگتر از T_{ix} ، بهره وری کانال تحت تاثیر پنجره ارسال K قرار می گیرد. بطور کلی بهره وری کانال برای پنجره ای به اندازه $k \geq 1 + 2a$ برابر است با:

$$U=1$$

و اگر $k < 1 + 2a$ باشد برابر است با:

$$U = \frac{KT_{ix}}{T_{ix} + 2T_p} = \frac{K}{1 + \frac{2T_p}{T_{ix}}} = \frac{K}{1 + 2a}$$

در فرمول فوق، فرض بر این است که خطای ارسال وجود نداشته باشد. هر خطایی بهره وری کانال را کم می کند چرا که برخی از قابها باید دوباره ارسال شوند. بهر حال، تاثیرات تاحدودی برای دو روش ارسال مجدد تفاوت دارند. برای مثال برای روش تکرار انتخابی، مقدار U بر اساس تعداد ارسال های مجدد هر قاب N_r کاهش می یابد چرا که تنها قاب خراب ارسال مجدد می شود. اگر P_f نرخ خرابی قاب در لینک باشد آنگاه با فرض خطاهای تصادفی:

$$N_r = \frac{1}{1 - P_f}$$

مقدار اصلاح شده U برای مقادیر $K < 1 + 2a$ بدین صورت است:

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

$$U = \frac{K}{1+2a} = \frac{K(1-P_f)}{1+2a}$$

برای $K \geq 1+2a$ با جایگزینی $K=1+2a$ در این عبارت U بدست می آید چرا که $1+2a$ حداکثر تعداد قابهایی است که می تواند قبل از دریافت یک تصدیق در زمان $T_{tx} + 2T_p$ ارسال شود. از اینرو برای $K \geq 1+2a$:

$$U = \frac{(1+2a)(1-P_f)}{1+2a} = 1-P_f$$

در روش بازگشت به عقب به اندازه N ، بهره وری کانال کمتر نیز می شود، چرا که اگر یک قاب خراب شود، بیش از یک قاب باید ارسال مجدد شود. دوباره تعداد قابهای اضافی ارسالی بوسیله اندازه K نسبت به $1+2a$ تعیین می شود.

برای $K < 1+2a$ ، تعداد بارهایی $(K-1)$ که قاب باید ارسال مجدد شود، $P_f(K-1)$ است. برای هر اتفاقی، یک تاخیر $1+2a$ نیز رخ می دهد. عبارت اصلاح شده برای $K < 1+2a$ بدین صورت است:

$$U = \frac{K(1-P_f)}{(1+2a) + (1+2a)P_f(K-1)} = \frac{K(1-P_f)}{(1+2a)(1+P_f(K-1))}$$

و برای $K \geq 1+2a$:

$$U = \frac{(1+2a)(1-P_f)}{(1+2a)(1+P_f(K-1))} = \frac{1-P_f}{1+P_f(K-1)}$$

توجه داشته باشید که این فرمولها تخمینی بوده و اگر تخمین های قبلی در دسترس باشند مفهوم بهتری خواهند داشت. علارغم این، راهنمای خوبی برای سطح کارایی مورد انتظار و کارایی نسبی هر روش می باشند.

۳-۳- لایه پیوند داده در شبکه های محلی

همان طور که در فصل ۱ به آن اشاره شد، کانال های انتقال را می توان به دو نوع عمده تقسیم بندی نمود که عبارتند از: کانال های نقطه به نقطه و کانال های پخش. شبکه های محلی عمدتاً از کانال های پخش برای انتقال اطلاعات کاربران استفاده می نمایند. در کانال های پخش، چندین کاربر به طور مشترک از یک کانال استفاده می کنند. مهمترین مسئله در کانال های پخش، تخصیص مناسب کانال به کاربران و جلوگیری از تداخل قاب های ارسالی هر ایستگاه می باشد. در شبکه های محلی، لایه پیوند داده به دو زیرلایه مختلف تقسیم می شود که عبارتند از: زیرلایه کنترل دسترسی به محیط (MAC^1) و زیرلایه کنترل اتصال منطقی (LLC^2) . در زیر به بررسی هریک از دو زیرلایه فوق می پردازیم.

۳-۳-۱- زیرلایه کنترل دسترسی به محیط

همان طور که گفته شد، یکی از مسائل بسیار مهم در شبکه های محلی که از کانال های پخش استفاده می نمایند، کنترل دسترسی به محیط می باشد. این کار توسط زیرلایه کنترل دسترسی به محیط انجام می شود. در طراحی مکانیسم های دسترسی به محیط عوامل مختلفی نظیر توپولوژی شبکه و نوع کنترل محیط دخالت دارند. در کنترل دسترسی به محیط سه روش مختلف وجود دارد که عبارتند از:

^۱ Medium Access Control

^۲ Logical Link Control

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۱

- **کنترل مرکزی^۱**: در این روش، یک کنترل کننده مرکزی در شبکه وجود دارد که برکل شبکه نظارت دارد. هر ایستگاه قبل از ارسال اطلاعات نیاز به اخذ مجوز از کنترل کننده مرکزی دارد. از آنجایی که تمام ایستگاه ها تا اجازه کنترل کننده مرکزی را دریافت نکنند، حق ارسال اطلاعات به شبکه را ندارند، بنابراین در این روش احتمال تداخل وجود ندارد. پروتکل های سوئیچینگ مداری، سرکشی^۲ و TDMA^۳ از روش کنترل مرکزی استفاده می کنند.
 - **کنترل توزیعی^۴**: در این روش هر ایستگاه برای ارسال اطلاعات نیاز به دریافت نشانه دارد. نشانه در بین ایستگاه ها توزیع می شود. هنگامی که ایستگاهی نشانه را در اختیار دارد، اطلاعات خود را ارسال می دارد و سپس نشانه را آزاد کرده و آن را به داخل شبکه می فرستد تا سایر ایستگاه های شبکه با دریافت آن اقدام به ارسال اطلاعات بنمایند. پروتکل هایی نظیر حلقه نشانه و گذرگاه نشانه از روش کنترل توزیعی استفاده می نمایند.
 - **کنترل تصادفی^۵**: در این نوع کنترل، هر ایستگاهی در شبکه قادر به ارسال در هر لحظه دلخواه می باشد و نیازی به اخذ نشانه و یا دریافت اجازه از یک ایستگاه مرکزی در شبکه ندارد. پروتکل هایی نظیر ALOHA^۶، CSMA/CD^۷، حلقه برش بندی شده^۸ و درج ثبات^۹ از این روش کنترل استفاده می نمایند.
- در زیر به بررسی برخی از مهمترین پروتکل های ارسال در شبکه های پخش می پردازیم.

۳-۱-۱- پروتکل ALOHA

این پروتکل در سال ۱۹۷۰ توسط آقای نورمن آبرامسون و همکارانش در دانشگاه هاوایی ارائه گردید و به دنبال آن توسط سایر محققین بسط و توسعه یافت. سیستم های اولیه ALOHA بر روی سیستم های پخش رادیویی زمینی پیاده سازی گردید ولی بر روی هر محیط دیگری نیز قابل پیاده سازی می باشد.

پروتکل ALOHA به دو نوع تقسیم می شود که عبارتند از:

- **پروتکل ALOHA خالص^۱**: در این پروتکل کاربران شبکه اجازه دارند که در هر لحظه دلخواه اقدام به ارسال اطلاعات نمایند. البته مسلماً در این روش امکان تداخل داده های ارسالی وجود دارد. برای رفع مشکل تداخل، در این روش هر کاربر بعد از ارسال قاب، کانال را بررسی می نماید تا متوجه وقوع تداخل در کانال شود. چنانچه قاب ارسالی با تداخل مواجه شود، فرستنده با بررسی کانال متوجه وقوع تداخل می شود و سپس یک زمان تصادفی صبر می نماید و دوباره قاب را ارسال می دارد. طبیعی است برای کاهش احتمال تداخل دوباره قاب ارسالی، فرستنده باید یک زمان تصادفی منتظر بماند و سپس دوباره قاب را ارسال دارد چون در غیر این صورت دوباره تداخل به وجود خواهد آمد. به سیستم هایی که چندین کاربر برای دسترسی به یک کانال مشترک با یکدیگر به رقابت می پردازند، سیستم های رقابتی^۹ گفته می شود. در شکل (۳-۸) دیاگرام زمانی ارسال قاب ها در یک شبکه ALOHA خالص با ۴ کاربر نشان داده شده است. مطابق با این شکل هرگاه دو یا چند قاب همزمان کانال را اشغال نمایند، در این صورت تداخل روی خواهد داد و اطلاعات

^۱ Centralized control

^۲ Polling

^۳ Time Division Multiple Access

^۴ Distributed control

^۵ Random control

^۶ Carrier Sense Multiple Access/ Collision Detect

^۷ Slotted ring

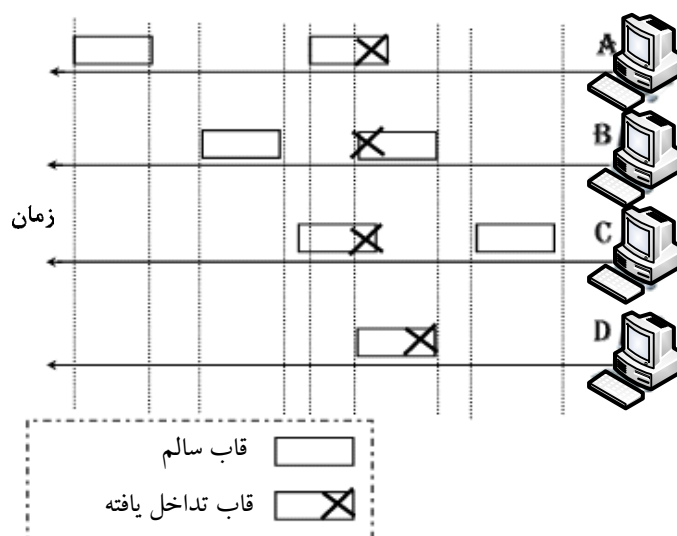
^۸ Register insertion

^۹ Contention system

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

از بین می رود. حتی اگر اولین بیت یک قاب با آخرین بیت قاب دیگری بر روی هم قرار بگیرد، در این صورت باز هم تداخل روی داده است و باید دوباره دو قاب ارسال شود.

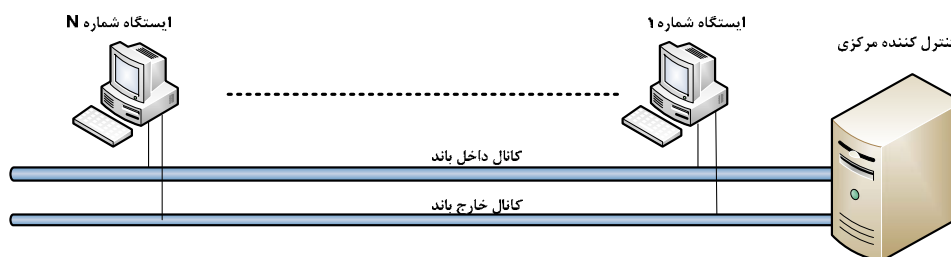
- **پروتکل ALOHA برش بندی شده:** در سال ۱۹۷۲ جهت افزایش ظرفیت و بهره وری بیشتر از کانال، توسط روبرتس، پروتکل ALOHA برش بندی شده ارائه گردید. در این پروتکل زمان به فواصل معین و ثابتی به نام برش تقسیم بندی می شود. برخلاف روش ALOHA خالص که هر ایستگاه در هر لحظه از زمان قادر به ارسال می باشد، در این روش ایستگاه ها فقط در لحظات خاصی که همان شروع هر برش می باشد، اجازه ارسال اطلاعات را دارند. با آنالیز ریاضی می توان ثابت نمود که حداکثر میزان استفاده از کانال در روش ALOHA خالص برابر با ۱۸ درصد و در ALOHA برش بندی شده برابر با ۳۶ درصد می باشد.



شکل (۳-۸): مثالی از یک سیستم ALOHA خالص

۳-۱-۲- روش سرکشی

در این روش که از نوع کنترل مرکزی کانال می باشد، ایستگاه های شبکه از طریق دو کانال به یک ایستگاه مرکزی که در حکم کنترل کننده کانال می باشد متصل می شوند. در شکل (۳-۹) مثالی از یک سیستم سرکشی آورده شده است.



شکل (۳-۹): مثالی از پروتکل سرکشی

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۱

مطابق شکل فوق، بین ایستگاه ها و کنترل کننده مرکزی، دو کانال وجود دارد. این دو کانال عبارتند از : کانال خارج باند^۱ و کانال داخل باند^۲. از کانال داخل باند برای تبادل اطلاعات و داده های ارسالی بین ایستگاه ها استفاده می شود. برای ارسال پیام های کنترلی و نشانه بین ایستگاه ها از کانال خارج باند استفاده می گردد. پروتکل سرکشی به دو نوع تقسیم می شود که به بررسی هریک می پردازیم.

- **پروتکل سرکشی چرخشی^۳** : در این روش کنترل کننده مرکزی به ترتیب به تک تک ایستگاه ها از طریق کانال خارج باند خود سرکشی می نماید. اگر ایستگاهی که به آن سرکشی شده است، اطلاعاتی برای ارسال داشت، آن را از طریق کانال داخل باند ارسال می دارد و پایان ارسال اطلاعات خود را به کنترل کننده مرکزی گزارش می دهد. چنانچه ایستگاهی که به آن سرکشی شده است، داده هایی برای ارسال نداشته باشد، کنترل کننده مرکزی به دنبال ایستگاه بعدی می رود. سرکشی به ایستگاه ها در این روش منظم و چرخشی می باشد. روش کار این پروتکل به این صورت است که در ابتدا ایستگاه مرکزی با ارسال پیام خاصی به اولین ایستگاه از آن می خواهد که داده های خود را ارسال دارد. ایستگاهی که به آن سرکشی شده است، چنانچه داده ای برای ارسال داشته باشد، آنها را از طریق کانال داخل باند ارسال می کند و در پایان دوباره نشانه را به کنترل کننده مرکزی ارسال می دارد. کنترل کننده مرکزی با دریافت نشانه، آن را برای ایستگاه دوم ارسال می دارد و ایستگاه دوم نیز در پایان ارسال داده های خود دوباره نشانه را به کنترل کننده مرکزی ارسال می کند. این کار به طور چرخشی ادامه دارد و به تمام ایستگاه ها از طریق کانال خارج باند سرکشی می شود.
- **پروتکل سرکشی هاب^۴** : یکی از معایب روش سرکشی چرخشی، آن است که در پایان ارسال هر ایستگاه نشانه دوباره به ایستگاه مرکزی ارسال می شود و از آن طریق در اختیار ایستگاه بعدی قرار می گیرد. این مسئله باعث افزایش تاخیر بین ارسال دو ایستگاه متوالی می گردد، که این امر نیز باعث کاهش میزان استفاده از کانال و اتلاف ظرفیت کانال می شود. برای رفع این مشکل از روش سرکشی هاب استفاده می شود. در این روش ایستگاه مرکزی ابتدا نشانه را به بالاترین ایستگاه (ایستگاه شماره N) تحویل می دهد. چنانچه ایستگاه شماره N اطلاعاتی برای ارسال داشت، اطلاعات خود را ارسال می دارد و در پایان ارسال، نشانه را به ایستگاه مجاور خود (ایستگاه N-1) ارسال می کند. این روند آن قدر ادامه پیدا می کند تا دوباره نشانه به ایستگاه مرکزی برسد و یک سیکل ارسال کامل شود. طبیعی است که در مقایسه با روش سرکشی چرخشی، در این روش میزان تأخیر انتظار برای در اختیار گرفتن کانال کاهش می یابد و میزان بهره وری از کانال افزایش می یابد.

۳-۱-۳- پروتکل تشخیص سیگنال حامل با دسترسی چندگانه (CSMA^۵)

چنانچه پروتکلی بتواند ابتدا وجود سیگنال حامل در خط را بررسی نماید و سپس با استفاده از آن اقدام به ارسال یا عدم ارسال اطلاعات خود بنماید، در آن صورت به آن پروتکل تشخیص سیگنال حامل گفته می شود. یکی از متداولترین پروتکل های تشخیص سیگنال حامل، پروتکل CSMA است. پروتکل های CSMA خود به چندین نوع تقسیم می شوند که عبارتند از: پروتکل CSMA صد درصد مضر^۶ و پروتکل CSMA غیر مضر^۷.

^۱ Outband line

^۲ Inband line

^۳ Roll call polling

^۴ Hub polling

^۵ Carrier Sense Multiple Access

^۶ 1-persistent CSMA

^۷ Nonpersistent CSMA

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

در پروتکل CSMA صددرصد مصّر، هنگامی که ایستگاهی اطلاعاتی برای ارسال دارد، ابتدا کانال را بررسی می نماید تا مطمئن شود کانال مشغول است یا خیر؟ چنانچه کانال مشغول باشد، تا لحظه آزاد شدن کانال، صبر می نماید و بعد از آن اقدام به ارسال یک قاب می کند. اگر قاب ارسالی با تداخل مواجه شود، در این صورت ایستگاه مدت زمانی تصادفی صبر می نماید و دوباره اقدام به ارسال قاب می کند. از آنجایی که در این پروتکل هرگاه ایستگاهی کانال را خالی ببیند با احتمال ۱ اقدام به ارسال قاب می نماید، به آن پروتکل CSMA صددرصد مصّر گفته می شود.

در کارایی این پروتکل، تأخیر انتشار تأثیر مهمی دارد. چنانچه دو ایستگاه همزمان اقدام به بررسی کانال بنمایند، در این صورت هر دو متوجه خالی بودن کانال می شوند. چنانچه یکی از آنها اقدام به ارسال اطلاعات نماید، این احتمال وجود دارد که قبل از آن که سیگنال ارسالی ایستگاه اول به ایستگاه دوم برسد، ایستگاه دوم نیز متوجه خالی بودن کانال شده و آن هم اقدام به ارسال اطلاعات کند. طبیعی است که در این صورت هر دو قاب ارسالی با تداخل مواجه می شوند و از بین می روند. هرچه تأخیر انتشار بیشتر باشد (فاصله ایستگاه ها از همدیگر زیاد باشد)، در این صورت احتمال وقوع تداخل نیز زیاد می شود و کارایی سیستم کاهش می یابد.

در پروتکل CSMA غیرمصّر، اشتهای کمتری برای ارسال قاب نسبت به پروتکل CSMA مصّر وجود دارد. در این پروتکل نیز ایستگاه قبل از ارسال از وضعیت کانال آگاهی کسب می نماید و چنانچه ایستگاه دیگری در حال ارسال نباشد، شروع به ارسال قاب می نماید. ولی در صورتی که کانال مشغول باشد، آنگاه ایستگاه به طور پیوسته وضعیت کانال را بررسی نمی نماید تا به محض این که کانال آزاد شد اقدام به ارسال قاب کند بلکه در صورتی که کانال مشغول باشد، یک زمان تصادفی صبر نموده و بعد دوباره وضعیت کانال را بررسی می نماید. ثابت می شود که کارایی این روش نسبت به روش CSMA مصّر به مراتب بهتر است.

نوع دیگری از پروتکل CSMA با نام P CSMA درصد مصّر^۱ نیز وجود دارد. از این پروتکل در کانال های برش بندی شده استفاده می شود. روش کار آن به این صورت است که ایستگاهی که می خواهد اطلاعاتی ارسال دارد، ابتدا کانال را بررسی می کند و بعد از آن چنانچه متوجه خالی بودن کانال گردید، با احتمال P ارسال می دارد و با احتمال 1-P ارسال خود را به برش بعدی موکول می نماید. اگر برش بعدی نیز آزاد باشد با احتمال P ارسال می کند و با احتمال 1-P ارسال خود را به برش بعدی می اندازد. این فرآیند تا زمانی که قاب ارسال نشود و یا تا زمانی که ایستگاه دیگری شروع به ارسال ننماید، ادامه پیدا می کند. با کاهش P، کارایی سیستم افزایش می یابد و احتمال تداخل کم می شود.

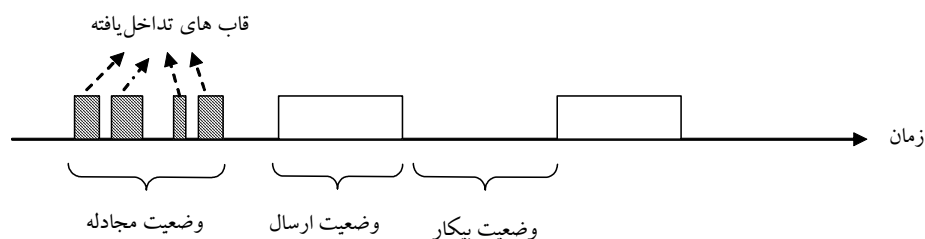
۳-۱-۴- پروتکل CSMA با قابلیت کشف تداخل (CSMA/CD)

از آنجایی که در پروتکل های CSMA، هیچ ایستگاهی وقتی که کانال مشغول است ارسال نمی نماید، بنابراین میزان کارایی آن نسبت به روش ALOHA به مراتب بیشتر می باشد. در پروتکل CSMA/CD، هرگاه دو ایستگاه همزمان شروع به بررسی وضعیت کانال بنمایند، متوجه آزاد بودن کانال می شوند و هر دو با هم اقدام به ارسال قاب می کنند. مسلماً قاب های ارسالی با تداخل مواجه می شود و از بین می روند. چنانچه قاب ارسالی در اولین بیت های آن و یا در آخرین بیت های آن با تداخل مواجه شود، امکان بازسازی آن وجود ندارد و آن قاب از بین می رود. در پروتکل CSMA/CD چنانچه حین ارسال ایستگاهی متوجه وقوع تداخل گردد، بلافاصله ارسال قاب را قطع می نماید. قطع سریع ارسال قاب های آسیب دیده باعث صرفه جویی در زمان و پهنای باند می گردد. در پروتکل CSMA/CD هر ایستگاه مطابق با شکل (۳-۱۰) در یکی از سه وضعیت زیر قرار دارد:

^۱ P-persistent CSMA

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

- **وضعیت ارسال:** در این وضعیت بدون آن که تداخلی گزارش داده شود، ایستگاه در حال ارسال قاب خود می باشد و در نهایت با موفقیت این کار را به پایان می رساند.
- **وضعیت مجادله:** در این وضعیت چند ایستگاه در حال رقابت برای دسترسی به کانال می باشند. قاب ارسالی ایستگاه ها با یکدیگر تداخل می نماید و ایستگاه ها یک مدت زمان تصادفی صبر می کنند و دوباره اقدام به ارسال قاب می نمایند. این کار آن قدر ادامه پیدا می کند که بالاخره ایستگاه ها موفق به ارسال صحیح قاب شوند.
- **وضعیت بی کار:** در این وضعیت ایستگاه ها قابی برای ارسال ندارند و کانال بلا استفاده و بی کار می ماند. چنانچه تاخیر انتشار در شبکه برابر با T باشد، در این صورت هر ایستگاه در بدترین حالت $2T$ ثانیه باید صبر نماید تا متوجه وقوع تداخل در شبکه شود. چنانچه بعد از گذشت $2T$ ثانیه هیچ سیگنالی مبنی بر وقوع تداخل گزارش نشود، طبیعی است اطلاعات ارسالی با صحت به مقصد رسیده است.



شکل (۳-۱۰): سه وضعیت کاری پروتکل CSMA/CD

۳-۴- استانداردهای IEEE برای شبکه های محلی

یکی از مراجع معتبر استانداردگذاری در زمینه های مرتبط با برق و کامپیوتر، انجمن IEEE می باشد. گروه کاری ۸۰۲ وابسته به انجمن IEEE در زمینه استانداردگذاری شبکه های محلی فعال است. توسط این گروه استانداردهای متعددی در زمینه شبکه های کامپیوتری محلی ارائه شده است که عبارتند از:

- شبکه محلی اترنت (IEEE 802.3)
- شبکه محلی گذرگاه نشانه (IEEE 802.4)
- شبکه محلی حلقه نشانه (IEEE 802.5)
- پروتکل زیرلایه پیوند منطقی، (IEEE 802.2)

در شکل (۳-۱۱) مدل لایه ای شبکه های محلی IEEE 802 نشان داده شده است. در زیر به بررسی هر یک از شبکه های فوق می پردازیم.

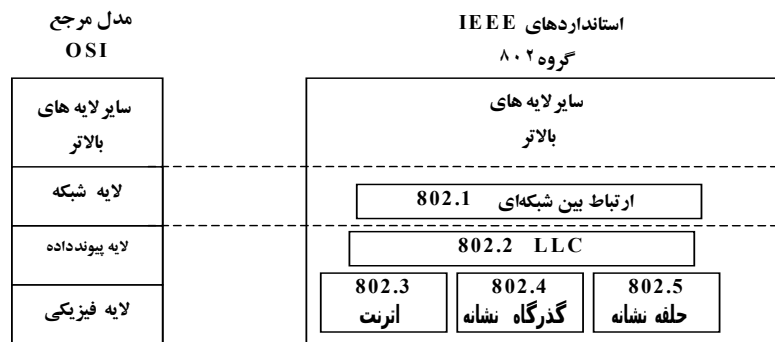
۳-۴-۱- شبکه های محلی اترنت

شبکه های محلی اترنت از روش CSMA/CD صددرصد مضر استفاده می نمایند. در این شبکه ها هنگامی که ایستگاه قابی برای ارسال دارد، ابتدا وضعیت کانال را بررسی می نماید و چنانچه کانال مشغول باشد تا آزاد شدن کانال صبر می کند و در صورتی که کانال آزاد شد اقدام به ارسال قاب می نماید. ایستگاه فرستنده، همزمان با ارسال قاب وقوع تداخل در قاب ارسالی را نیز بررسی می کند و چنانچه متوجه وقوع تداخل در قاب ارسالی شود، ارسال قاب را قطع می نماید و یک زمان تصادفی صبر می کند و دوباره اقدام به ارسال قاب می نماید.

پایه استاندارد اترنت، سیستم ALOHA آقای آبرامسون که در بخش های قبلی به بررسی آن پرداختیم می باشد که به مرور زمان به آن قابلیت تشخیص حامل نیز اضافه شده است.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

اولین سیستم عملی شبکه مبتنی بر CSMA/CD توسط شرکت زیراکس با سرعت ۲/۹۴ مگابیت بر ثانیه طراحی و ساخته شد. در این شبکه ۱۰۰ ایستگاه کاری بر روی یک کابل به طول یک کیلومتر به هم متصل شدند. شبکه پیشنهادی شرکت زیراکس که اترنت نام گرفت، آن قدر موفق عمل نمود که توسط سه شرکت معتبر زیراکس، DEC و اینتل استاندارد اترنت با سرعت ۱۰ مگابیت بر ثانیه ارائه شد. این استاندارد مبنای استاندارد IEEE 802.3 قرار گرفت.



شکل (۳-۱۱): مدل لایه های شبکه های محلی IEEE 802

کلمه اترنت از اتر به معنای کابل مشتق شده است. علت انتخاب این نام برای این نوع شبکه آن است که در این نوع شبکه ها از کابل به عنوان محیط هادی برای انتقال امواج الکترومغناطیسی استفاده می شود. در شبکه های اترنت دو نوع کابل موجود است که با نام های کابل نرم و کابل سخت شناخته می شوند. کابل های اترنت نرم بسیار نازک و انعطاف پذیر هستند و نسبت به کابل سخت ارزانتر نیز می باشند. از این نوع کابل ها فقط می توان در فواصل کوتاه استفاده نمود. امکان اتصال این دو نوع کابل نیز به یکدیگر وجود دارد.

یکی از مشکلات اساسی در شبکه های اترنت، وقوع خرابی و قطعی در کابل می باشد. چنانچه کابل شبکه دچار قطعی شود و یا یکی از اتصال دهنده های آن از محل خود خارج شود، سیگنال های ارسالی منعکس می شود و شبکه قادر به ادامه فعالیت خود نمی باشد. یکی از روش های متداول تشخیص قطعی در کابل شبکه آن است که یک پالس الکتریکی در کابل ارسال گردد. هنگامی که پالس ارسالی به مانعی برخورد نماید، منعکس می شود. با اندازه گیری دقیق زمان ارسال پالس و زمان دریافت انعکاس آن، می توان دقیقاً محل انعکاس را تعیین نمود و بدین ترتیب متوجه محل قطعی کابل شد. به این روش، انعکاس سنجی زمانی^۱ گفته می شود.

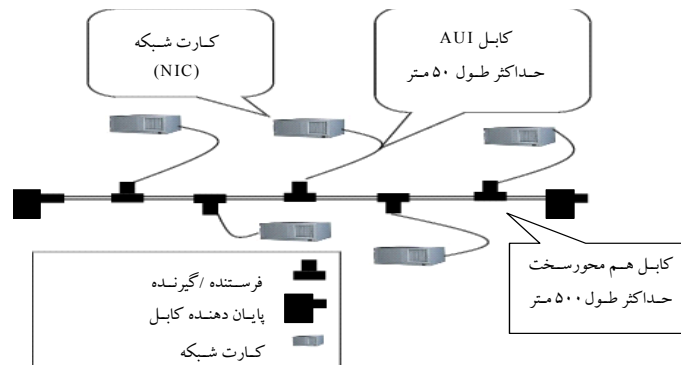
در شکل (۳-۱۲) نحوه کابل کشی شبکه های اترنت با استفاده از کابل های سخت RG-8 نشان داده شده است. همان طور که در این شکل نیز دیده می شود، هر کامپیوتر شبکه از طریق یک کابل که حداکثر طول آن ۵۰ متر است از طریق وسیله ای به نام فرستنده/گیرنده^۲ به کابل اصلی شبکه متصل است. در فرستنده/گیرنده تجهیزات الکترونیکی وجود دارد که به وسیله آن امکان تشخیص وضعیت سیگنال حامل در کانال و کشف تداخل فراهم می آید. هنگامی که فرستنده/گیرنده متوجه وقوع تداخل در کابل شبکه می شود، سیگنال مشخصی را روی کانال قرار می دهد و بدین وسیله به همه فرستنده/گیرنده های دیگر از وقوع تداخل اطلاع می دهد. کابلی که ایستگاه را به فرستنده/گیرنده متصل می نماید حاوی پنج زوج سیم به هم تابیده شده روکش دار است. دو زوج سیم فوق برای ورود و خروج داده ها به کار می روند و دو زوج دیگر به

^۱ Time domain reflectometry

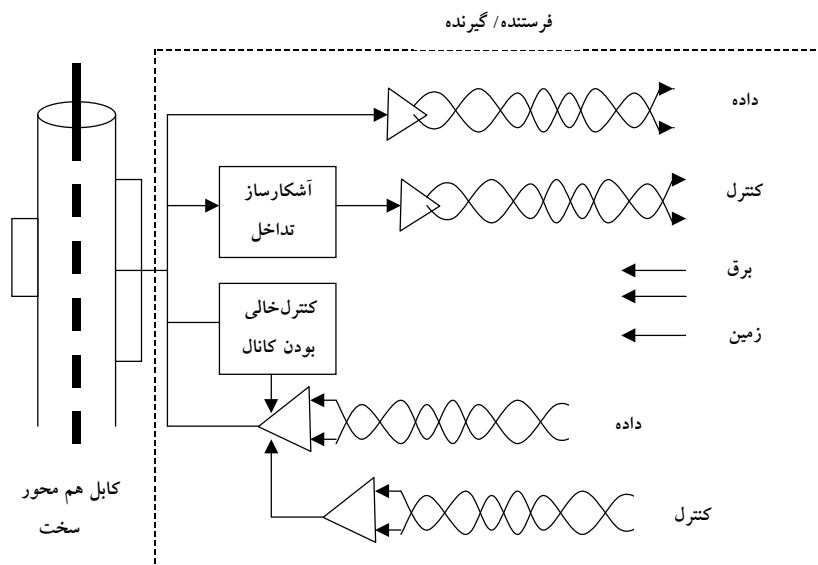
^۲ Transceiver (Transceiver مخفف کلمات Transmitter و Receiver می باشد)

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۱

ورود و خروج سیگنال های کنترلی اختصاص دارند. از پنجمین زوج سیم استفاده زیادی نمی شود و می توان در مواردی از آن برای تغذیه فرستنده/گیرنده استفاده نمود. برای کاهش تعداد فرستنده/گیرنده ها، در برخی از آنها امکان اتصال ۸ کامپیوتر به یک فرستنده/گیرنده وجود دارد. در شکل (۳-۱۳) اجزای داخلی فرستنده/گیرنده نشان داده شده است.



شکل (۳-۱۲): نمونه ای از شبکه اترنت از نوع اترنت سخت



شکل (۳-۱۳): اجزای داخلی فرستنده/گیرنده

هر کامپیوتر متصل به شبکه از طریق یک برد الکترونیکی که کارت واسط شبکه^۱ (NIC) نام دارد، امکان اتصال به شبکه را دارد. کارت شبکه حاوی یک پردازنده الکترونیکی است که به وسیله آن عملیات ارسال و دریافت قاب ها انجام می شود. همچنین عملیاتی نظیر: تشکیل و ایجاد قاب های ارسالی و محاسبه مجموع مقابله ای برای قاب های ارسالی و دریافتی توسط پردازنده انجام می شود. برخی از کارت های شبکه دارای قابلیت های اضافی دیگر نظیر اتصال به کامپیوتر از طریق DMA^۲ و

^۱ Network Interface Card

^۲ Direce Memory Access

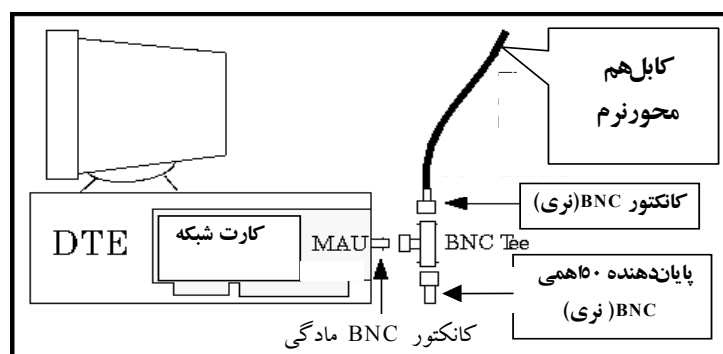
شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

انجام عملیات مدیریت شبکه می باشند. هر کارت شبکه از طریق یک واسطه اتصال (AUI^۱) که یک کانکتور DB-15 می باشد، به کابل اترنت سخت متصل می شود.

حداکثر طول مجاز کابل اترنت سخت برابر با ۵۰۰ متر می باشد. چنانچه بخواهیم شبکه محلی خود را به فواصل طولانی تری گسترش دهیم، می توان چندین کابل شبکه را از طریق تکرارکننده^۲ به یکدیگر متصل نمود. تکرارکننده ها در لایه فیزیکی عمل می نمایند و وظیفه آنها دریافت و تقویت و ارسال دوباره قاب های دریافتی از یک طرف به طرف مقابل می باشد. با استفاده از تکرارکننده ها می توان طول فیزیکی یک شبکه اترنت را افزایش داد، ولی باید توجه نمود که بیشترین فاصله بین فرستنده و گیرنده در یک شبکه اترنت نباید از ۲/۵ کیلومتر بیشتر باشد، بدین ترتیب در یک شبکه حداکثر می توان از ۴ تکرارکننده استفاده نمود.

به شبکه های اترنت کابل سخت، 10Base5 نیز اطلاق می شود که در آن 10 نشان دهنده سرعت ارسال ده مگابیت بر ثانیه است و 5 بیانگر حداکثر طول ۵۰۰ متری کابل شبکه می باشد. قطر کابل در شبکه های 10Base5 حدود نیم اینچ است. علاوه بر کابل های سخت برای شبکه های اترنت، می توان از کابل های نرم نیز برای کابل کشی شبکه استفاده نمود. طبیعی است که این نوع کابل های شبکه، دارای انعطاف پذیری بالا و قیمت پایین تری می باشند. قطر کابل های نرم حدود ۲۵ صدم اینچ می باشد. همان طور که در شکل (۳-۱۴) نشان داده شده است، در شبکه های اترنت نرم هر کارت شبکه مستقیماً به کابل نرم متصل است. در شکل (۳-۱۵) مثالی از نحوه کابل کشی شبکه اترنت نرم آورده شده است. یکی از معایب عمده این روش این است که حداکثر طول کابل شبکه برابر با ۱۸۵ متری باشد و بنابراین تعداد کاربران آن نسبت به شبکه کابل سخت کمتر است.

با توجه به ساختار شبکه های اترنت نرم، دیده می شود که در این نوع شبکه ها، فرستنده/گیرنده حذف شده است. از کابل های هم محور RG-58 در شبکه های اترنت نرم استفاده می شود. هر کارت شبکه از طریق یک کانکتور BNC-T به کابل شبکه متصل می گردد. به شبکه های اترنت نرم، شبکه های 10Base2 نیز گفته می شود. این نوع شبکه ها نیز مشابه شبکه های 10Base5 که از کابل های سخت استفاده می کنند دارای سرعت ۱۰ مگابیت بر ثانیه می باشند. برای رفع مشکل محدودیت طول کابل در شبکه های اترنت نرم، از تکرار کننده استفاده می گردد. با استفاده از تکرار کننده امکان افزایش طول شبکه اترنت نرم وجود دارد. در شکل (۳-۱۶) مثالی از گسترش یک شبکه اترنت با استفاده از تکرار کننده آورده شده است.

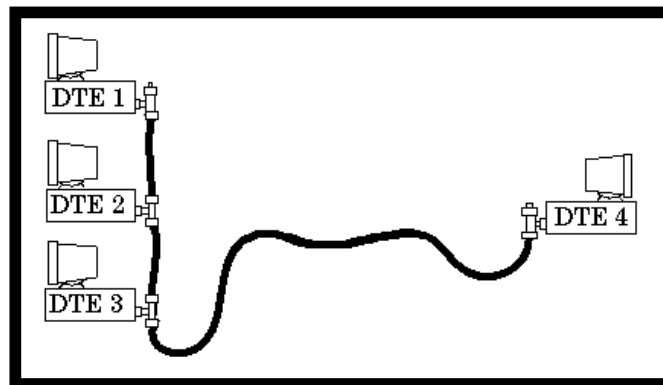


شکل (۳-۱۴): اجزای شبکه اترنت نرم

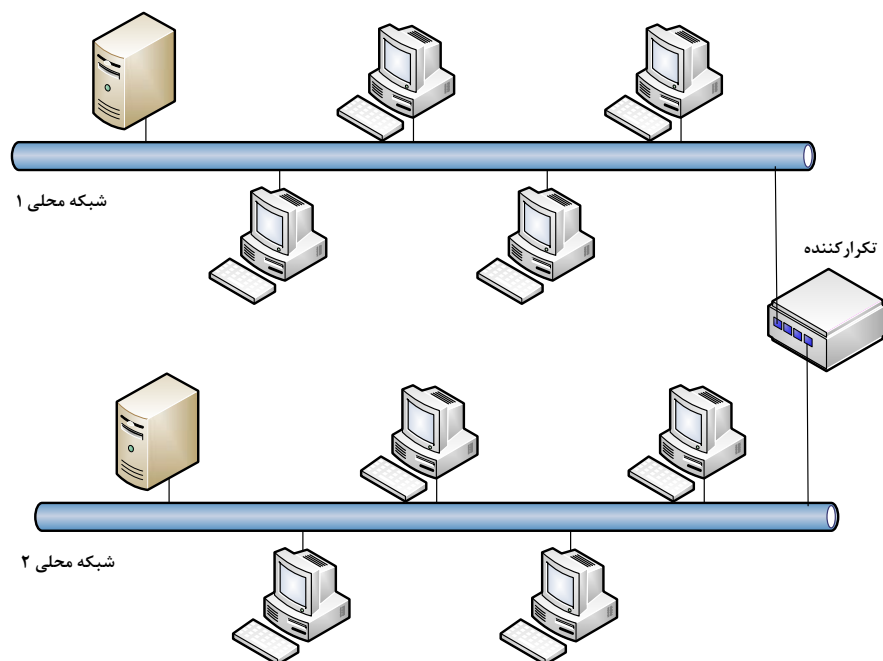
^۱ Attachment Unit Interface

^۲ Repeater

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



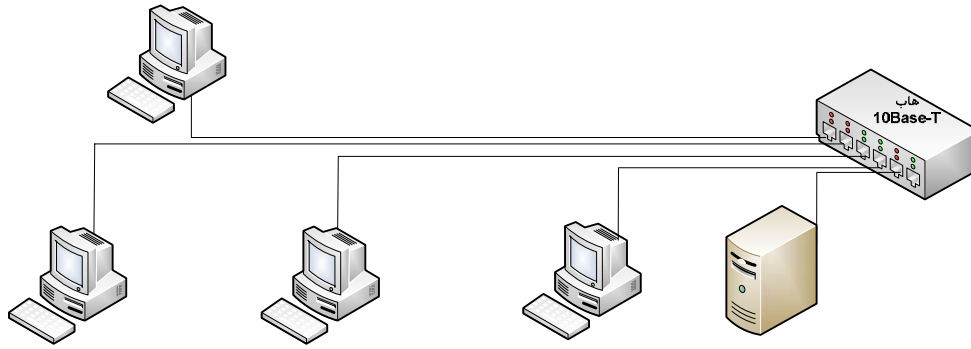
شکل (۳-۱۵): مثالی از کابل کشی شبکه اترنت نرم



شکل (۳-۱۶): گسترش یک شبکه اترنت با استفاده از تکرار کننده

امروزه شبکه های 10Base5 و 10Base2 به تدریج از رده خارج شده اند و شبکه های اترنت ستاره ای (10Base-T, 100Base-T) جایگزین آنها گردیده اند. در این نوع شبکه ها از زوج سیم های UTP استفاده می شود. سرعت های متداول این نوع شبکه ها ۱۰ مگابیت بر ثانیه (10Base-T) و ۱۰۰ مگابیت بر ثانیه (100Base-T) می باشد. تمام ایستگاه های شبکه از طریق یک کابل RJ-45 (که شامل ۴ زوج سیم UTP است) به یک ایستگاه مرکزی که هاب نام دارد متصل می شوند. چنانچه یکی از ایستگاه های متصل شده به هاب قابی را ارسال دارد، در این صورت هاب آن را دریافت می کند و آن را به تمام درگاه های خروجی خود ارسال می دارد. بدین ترتیب قاب ارسالی هر ایستگاه توسط هاب به تمام ایستگاه های دیگر نیز ارسال می شود. در شکل (۳-۱۷)، نمونه ای از یک شبکه ستاره ای با استفاده از هاب نشان داده شده است.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

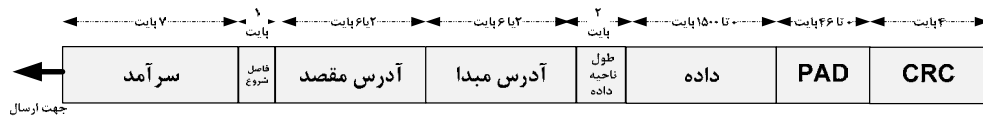


شکل (۳-۱۷): یک شبکه محلی ستاره ای از نوع 10Base-T

در شبکه های ستاره ای حداکثر طول کابل RJ-45 که ایستگاه های شبکه را به هاب متصل می نماید، برابر با ۱۰۰ متر می باشد. یکی از مهمترین مزایای شبکه های محلی ستاره ای این است که چنانچه خرابی در یکی از کابل های RJ-45 رخ دهد، فقط همان ایستگاه از کار می افتد و سایر ایستگاه های شبکه به کار خود ادامه می دهند.

۳-۴-۱- ساختار زیرلایه MAC در اترنت

در شکل (۳-۱۸) ساختار قاب های اترنت نشان داده شده است .



شکل (۳-۱۸): ساختار قاب های MAC استاندارد اترنت

همان طور که در این شکل دیده می شود، فیلدهای زیر در ساختار قاب های اترنت وجود دارند.

- **فیلد سرآمد:** این فیلد ۷ بیتی حاوی الگوی بیتی ۱۰۱۰۱۰۱۰ می باشد و برای همزمان سازی ساعت فرستنده با ساعت گیرنده مورد استفاده قرار می گیرد.
- **فیلد فاصل شروع (SFD):** این فیلد که حاوی بایت ۱۰۱۰۱۰۱۱ است نشان دهنده شروع قاب می باشد.
- **فیلد آدرس های مقصد و مبدأ:** توسط این فیلدهای ۲ یا ۶ بیتی آدرس های فرستنده و گیرنده قاب مشخص می شود. معمولاً استاندارد اترنت با سرعت ۱۰ مگابیت بر ثانیه از آدرس های ۶ بیتی استفاده می نماید. توسط بالاترین بیت در فیلد آدرس گیرنده، نوع آدرس مشخص می گردد. چنانچه آدرس از نوع گروهی باشد این بیت حاوی ۱ است و برای آدرس های معمولی بیت فوق صفر می باشد. به وسیله مکانیسم آدرس دهی گروهی این امکان وجود دارد که به چندین ایستگاه که در یک گروه قرار گرفته اند، قاب هایی را ارسال نمود. چنانچه تمام بیت های فیلد آدرس مقصد حاوی بیت ۱ باشد، در این صورت تمامی ایستگاه های شبکه، قاب ارسالی را دریافت می نمایند که به این حالت، آدرس دهی داده پراکنی گفته می شود. از دومین بیت بالا (بیت شماره ۴۶) برای تفکیک آدرس های

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

محلی از آدرس های جهانی استفاده می شود. آدرس های محلی توسط مدیران شبکه تعیین می شود و در خارج از شبکه اهمیت و معنایی ندارند. ولی آدرس های جهانی در دنیا واحد بوده و از سوی سازمان IEEE تعیین می شوند. با ۴۶ بیت باقیمانده از فیلد آدرس، می توان تعداد 2^{46} آدرس جهانی تولید نمود که هر ایستگاه در جهان به طور انحصاری قابل آدرس دهی یکتا می باشد.

- **فیلد طول ناحیه داده:** از این فیلد برای تعیین دقیق طول ناحیه داده که می تواند صفر تا ۱۵۰۰ بایت باشد، استفاده می شود.
- **فیلد PAD:** برای آن که بتوان قاب های سالم را از قاب های آشغال که از تداخل قاب های دیگر به وجود می آیند، جداسازی نمود، باید حداقل طول قاب های ارسالی ۶۴ بایت باشد. چنانچه طول قاب های ارسالی از ۴۶ بایت کمتر باشد به تعداد بایت کمتر از ۴۶ در ناحیه PAD بایت صفر اضافه می گردد تا طول قاب به حداقل مقدار خود برسد.
- **فیلد داده:** این فیلد متغیر که دارای طول ۰ تا ۱۵۰۰ بایت می باشد، حاوی اطلاعات لایه بالاتر است که باید در قالب قاب هایی به درون شبکه ارسال شود.
- **فیلد CRC:** این فیلد که دارای ۴ بایت طول می باشد، برای اطمینان از صحت قاب دریافتی به کار می رود. چنانچه ضمن ارسال قاب در شبکه برخی از بایت های فیلد داده از بین بروند، در این صورت گیرنده با بررسی فیلد CRC دریافتی با CRC ای که خود بدست می آورد، متوجه وقوع خطا در قاب دریافتی می شود. از کدهای CRC 32 برای این فیلد استفاده می شود.

همان طور که قبلاً نیز اشاره شد، بعد از هر بار تداخل در قاب ارسالی، ایستگاه فرستنده مدت زمان تصادفی صبر می نماید و دوباره قاب را ارسال می دارد. الگوریتم کار به این صورت است که در اولین تداخل، ایستگاه به طور تصادفی یکی از اعداد 0, T, 2T را انتخاب می کند و به آن اندازه صبر می نماید و سپس دوباره اقدام به ارسال قاب می کند. چنانچه برای بار دوم تداخل رخ دهد، ایستگاه فرستنده یکی از اعداد 0, T, 2T, 3T را انتخاب می کند و به آن اندازه صبر می نماید و سپس اقدام به ارسال مجدد قاب می کند. به طور کلی بعد از i بار تداخل، فرستنده یکی از زمان های $0, T, 2T, \dots, (2^i - 1)T$ را انتخاب نموده و به آن اندازه صبر می کند و دوباره اقدام به ارسال قاب می نماید. البته بعد از رسیدن به ۱۰ تداخل، دیگر دامنه اعداد تصادفی افزایش نمی یابد و یکی از زمان های بین $0, T, 2T, \dots, 1023T$ انتخاب می شود. پس از ۱۶ بار تداخل فرستنده تسلیم می شود و دیگر از ارسال قاب صرف نظر می نماید. به این الگوریتم، الگوریتم عقب گرد توانی دودویی^۱ می گویند. طبیعی است که با افزایش محدوده اعداد تصادفی که ایستگاه باید به اندازه آن صبر نماید، احتمال بروز تداخل کاهش می یابد. متغیر زمانی T نشان دهنده حداکثر تأخیر انتشار در کانال می باشد.

۳-۴-۱-۲- اترنت سریع^۲

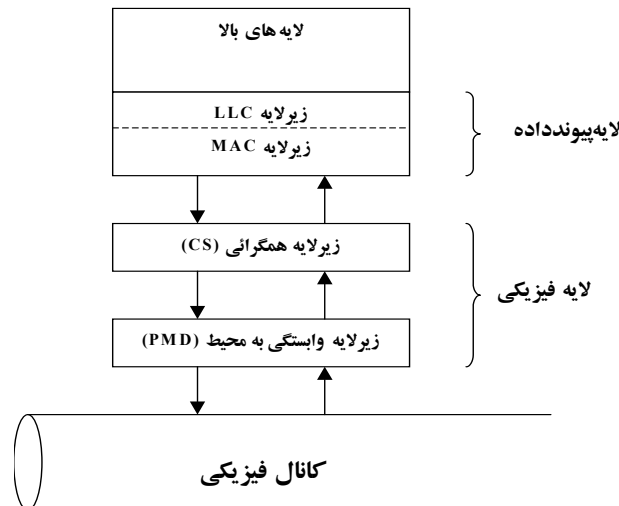
با پیشرفت خدمات جدید در شبکه های کامپیوتری، سرعت شبکه های اترنت معمولی برای تبادل اطلاعات کافی به نظر نمی رسد. تعدادی از شرکت های کامپیوتری معتبر با ارائه توافق نامه ای و تصویب IEEE در سال ۱۹۹۵ استاندارد اترنت سریع (IEEE 802.3U) را تصویب کردند. در این استاندارد که توسعه یافته اترنت معمولی است، سرعت مبادله داده ها، ۱۰۰ مگابیت بر ثانیه می باشد. در شکل (۳-۱۹) ساختار لایه ای پروتکل اترنت سریع نشان داده شده است. باتوجه به این شکل، در

^۱ Binary exponential backoff

^۲ Fast Ethernet

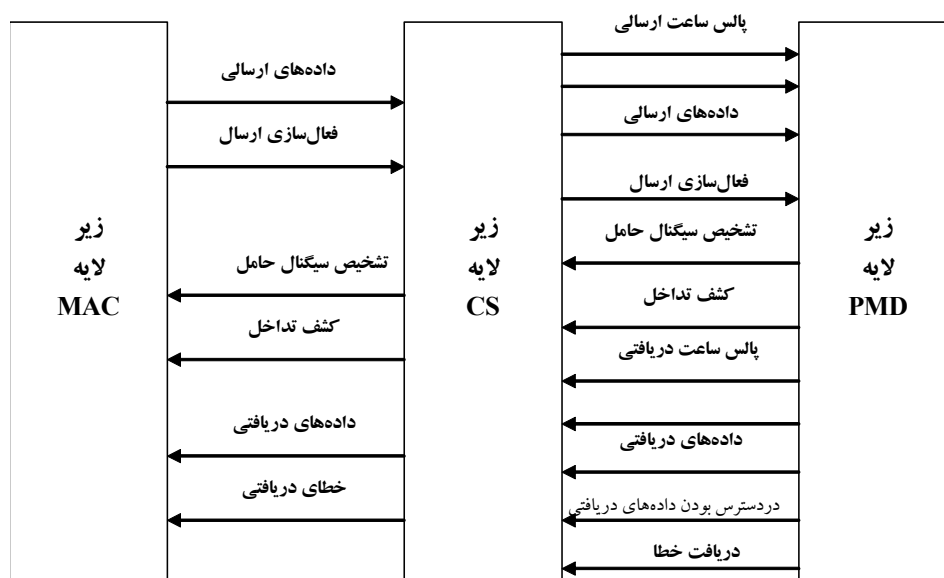
شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

شبکه های اترنت سریع، لایه فیزیکی به دو زیرلایه به نام های زیرلایه همگرایی (CS^1) و زیرلایه وابسته به محیط فیزیکی (PMD^2) تجزیه می شود.



شکل (۳-۱۹): ساختار لایه ای اترنت سریع

زیرلایه همگرایی موظف به فراهم آوری واسط لازم بین زیرلایه MAC و زیرلایه PMD می باشد. با استفاده از این زیرلایه، می توان با شفافیت لازم در MAC برای استفاده از کانال های مختلف در لایه فیزیکی دستیابی داشت. در شکل (۳-۲۰)، سیگنال های موجود در واسط زیرلایه CS با زیرلایه MAC و همچنین زیرلایه PMD با زیرلایه CS نشان داده شده است.



شکل (۳-۲۰): سیگنال های موجود در واسط زیرلایه CS با زیرلایه MAC و زیرلایه PMD با زیرلایه CS

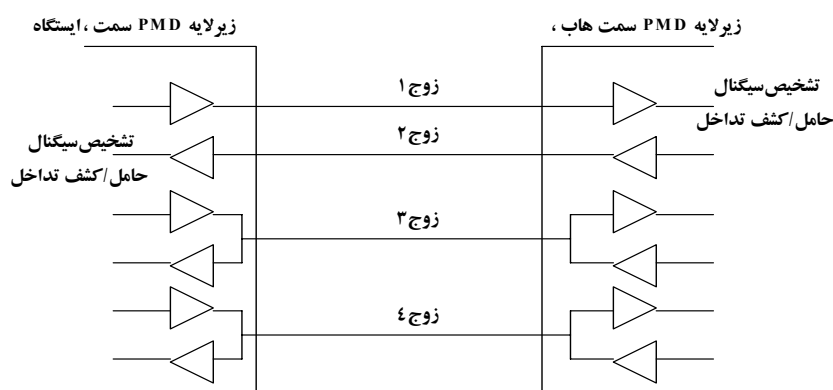
^۱ Convergence Sublayer

^۲ Physical Medium-dependent Sublayer

شبکه های کامپیوتری (دکتر محمد حسین یغمایی، مقدم - دانشگاه فردوسی مشهد)

در شبکه های اترنت سریع، هر ایستگاه شبکه از طریق دو کانال مجزا به هاب متصل شده است، که یک کانال برای ارسال و یک کانال برای دریافت استفاده می شود. استاندارد اترنت سریع دارای انواع مختلفی می باشد که عبارتند از:

- **100Base-T4** : در این نوع شبکه از ۴ زوج سیم UTP بین هر ایستگاه و هاب استفاده می شود. از زوج سیم های شماره ۳ و ۴ برای ارسال و دریافت داده ها استفاده می گردد. در هر یک از زوج سیمهای به کاررفته، ارسال به صورت یک طرفه انجام می شود. یک رشته سیم از زوج سیم شماره ۱ و یک رشته سیم از زوج شماره ۲ برای انجام عملیات تشخیص حامل و تشخیص وقوع تداخل استفاده می شود. در شکل (۳-۲۱)، زوج سیم های مورد استفاده در 100Base-T4 نشان داده شده است.
- **100Base-TX** : در این نوع شبکه از دو زوج سیم UTP و یا STP بین هر ایستگاه و هاب استفاده می گردد.
- **100Base-FX** : در این استاندارد از دو رشته فیبر نوری برای اتصال هر ایستگاه به هاب استفاده می شود. استاندارد 100Base-FX از فیبر نوری چند مد با قطر مغزی ۶۲/۵ میکرون و قطر غلاف ۱۲۵ میکرون استفاده می نماید. در این استاندارد از پروتکل کد گذاری NRZ-I استفاده می شود.



شکل (۳-۲۱): زوج سیم های مورد استفاده در 100Base-T4

۳-۴-۱-۳- گیگابیت اترنت

با پیشرفت فن آوری ساخت کامپیوترها و ارائه پردازنده های سریع با گذرگاه های PCI، امکان مبادله داده ها با سرعت بیش از یک گیگابیت بر ثانیه درون کامپیوتر وجود دارد. به عنوان مثال در یک باس ۶۴ بیتی که با سرعت ۱۰۰ مگاهرتز کار می نماید می توان داده ها را با سرعت ۶/۴ گیگابیت بر ثانیه مبادله نمود.

استاندارد گیگابیت اترنت قادر به مبادله اطلاعات با سرعت ۱ گیگابیت بر ثانیه که صد برابر سریع تر از اترنت پایه است، می باشد. این استاندارد با اترنت سریع و اترنت پایه سازگاری دارد، و می توان از آن به عنوان شبکه شالوده در اتصال شبکه های محلی استفاده نمود.

توسط سازمان IEEE استاندارد IEEE 802.3Z برای شبکه های گیگابیت اترنت تصویب گردید. گیگابیت اترنت برای اتصال سوئیچ های شبکه های اترنت پایه و سریع به یکدیگر و برقراری یک شبکه شالوده سریع به کار می رود. ساختار قاب های این استاندارد مشابه اترنت پایه است و از پروتکل CSMA/CD استفاده می نماید. استاندارد گیگابیت اترنت از عملکرد یک طرفه و دوطرفه پشتیبانی می کند. در این استاندارد از فیبر نوری و زوج سیم UTP برای مبادله اطلاعات استفاده می گردد. زیر لایه سری کننده/غیرسری کننده که در مدل لایه ای گیگابیت اترنت دیده می شود، وظیفه تبدیل اطلاعات موازی لایه بالاتر به اطلاعات سری و بالعکس را به عهده دارد.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

در شبکه های اترنت گیگابیت از روش کد گذاری B8/B10 استفاده می شود. در این روش کد گذاری که برای ارسال اطلاعات در محیط فیبر نوری به کار می رود اطلاعات از ۸ بیت به ۱۰ بیت تبدیل شده و ارسال می گردند. همان طور که گفته شد استاندارد گیگابیت اترنت هر دو عملکرد یک طرفه و دو طرفه را پشتیبانی می نماید. در حالت یک طرفه از پروتکل CSMA/CD و در حالت دو طرفه از پروتکل IEEE 802.3X استفاده می شود. در گیگابیت اترنت حداقل طول قاب های ارسالی ۵۱۲ بایت می باشد. برخی از پروتکل های فیزیکی گیگابیت اترنت عبارتند از 1000Base-LX، 1000Base-SX، 1000Base-T و 1000Base-CX. در جدول (۳-۱) استانداردهای متداول گیگا بیت اترنت نشان داده شده است.

جدول (۳-۱): استانداردهای گیگا بیت اترنت

استاندارد گیگا بیت اترنت	واسط لایه فیزیکی	نوع محیط ارسال	فاصله	تاریخ استاندارد
IEEE802.3z	1000 Base-SX	فیبر نوری چند مود	۲ تا ۵۵۰ متر	۱۹۹۸
	1000 Base-LX	فیبر نوری تک مود یا چند مود	۲ متر تا ۵ کیلومتر	
	1000 Base-CX	سیم مسی	۲۵ متر	
IEEE 802.3ab	1000 Base-T	کاتگوری ۵ و 5E سیم UTP	۱۰۰ متر	۱۹۹۹

از استاندارد گیگابیت اترنت جهت افزایش سرعت اتصال به خدمات دهنده های شبکه، اتصال سوئیچ ها به یکدیگر و اتصال سوئیچ ها به خدمات دهنده ها استفاده می شود. همچنین با استفاده از گیگابیت اترنت می توان برنامه های کاربردی نظیر مدل سازی ۳ بعدی، انیمیشن سازی CAD/CAM، تصویربرداری پزشکی، پیاده سازی خدمات محیط های چندرسانه ای و بسیاری از کاربردهای دیگر اینترنت و اینترنت را که پهنای باند زیادی نیاز دارند، پیاده سازی نمود.

۳-۴-۱-۴- ده گیگابیت اترنت

از ۲۷ سال پیش که فن آوری اترنت ارائه شد، این فن آوری تاکنون تحول های زیادی جهت برآورده کردن نیازهای شبکه های سوئیچ بسته ای یافته است. به خاطر مزایایی نظیر هزینه پیاده سازی کم، قابلیت اطمینان بالا و نصب و نگهداری آسان، فن آوری اترنت به شدت مورد استقبال قرار گرفته است. با افزایش سرعت شبکه ها و ارائه خدمات جدیدتر، فن آوری اترنت نیز تکامل یافته است و خود را با سرعت های بالا وفق داده است.

استاندارد گیگابیت اترنت که در بالا به آن اشاره شد، در شبکه های خصوصی و همچنین شبکه های عمومی استفاده می شود. با توسعه این فن آوری، استفاده اترنت از شبکه های محلی به شبکه های شهری توسعه یافته است. اخیراً استاندارد اترنت ۱۰ گیگابیت برثانیه ارائه شده است. با استفاده از این استاندارد امکان ارسال ترافیک داده ای سریع و همچنین خدمات جدیدی نظیر ویدئوی متحرک فراهم شده است. استاندارد اترنت ۱۰ گیگا بیت از چند جنبه با استاندارد اترنت پایه متفاوت است. در این استاندارد فقط از فیبر نوری استفاده می شود و همچنین عملیات ارسال به صورت کاملاً دوطرفه است. بنابراین در این استاندارد هیچ گونه تداخلی بین قاب ها به وجود نمی آید. هر چند اترنت ۱۰ گیگا بیت از سرعت بسیار بالایی نسبت به اترنت پایه برخوردار است، اما از نظر ساختار قاب ها تا حد زیادی مشابه آن می باشد. سرمایه گذاری بر روی اترنت ۱۰ گیگابیت بر ثانیه و استفاده وسیع از آن هنوز مطمئن نمی باشد. قابلیت ارتباط اترنت ۱۰ گیگابیت با سایر فن آوری های شبکه نظیر SONET در حال بررسی است.

برای وفق دادن اترنت ۱۰ گیگابیت بر ثانیه، از سوی گروه مطالعاتی ۸۰۲I سازمان IEEE معیارها و اهداف زیر در استاندارد فوق در نظر گرفته شده است:

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

۱. این فن آوری باید قادر به پشتیبانی از برنامه های کاربردی مختلف که توسط فروشندگان گوناگونی ارائه شده است، باشد.
 ۲. این استاندارد باید با سایر استانداردهای اترنت و همچنین با مدل OSI و قابلیت های مدیریتی SNMP سازگار باشد.
 ۳. این استاندارد باید با سایر استانداردهای اترنت طوری متفاوت باشد که بتوان از آن برای توسعه شبکه ها به عنوان یک راه حل واحد و منحصر به فرد و نه به عنوان یک راه حل ثانویه استفاده نمود.
- از نظر اقتصادی، باید نصب و توسعه شبکه های اترنت ۱۰ گیگابیت برای مشتریان مقرون به صرفه باشد. از سوی سازمان IEEE استاندارد IEEE 802.3ae جهت شبکه های اترنت ۱۰ گیگابیت وضع شده است. در این شبکه ها، لایه فیزیکی که مطابق با لایه اول مدل مرجع OSI است، برای اتصال محیط ارسال (فیبر نوری یا زوج سیم) به لایه MAC که مطابق با لایه دوم مدل مرجع OSI می باشد استفاده می شود.
- در این استاندارد، مشابه استاندارد اترنت سریع، لایه فیزیکی به دو زیر لایه PMD و CS تجزیه می شود. فرستنده/گیرنده های نوری نمونه ای از PMD می باشند. توسط زیر لایه CS نحوه کدگذاری و عملیات تسهیم سازی توصیف می شود. در استاندارد 802.3ae دو نوع لایه فیزیکی پیشنهاد شده است که عبارتند از: لایه فیزیکی برای شبکه های محلی^۱ و لایه فیزیکی برای شبکه های گسترده^۲.
- در شبکه های اترنت ۱۰ گیگابیت از واسط XAUI استفاده می شود. کلمه AUI از استاندارد اترنت پایه گرفته شده است. همچنین حرف X نشان دهنده سرعت ۱۰ گیگابیت بر ثانیه می باشد. علاوه بر واسط XAUI واسط XGMII در شبکه های اترنت ۱۰ گیگابیت استفاده می گردد. این واسط دارای ۷۴ پین می باشد که برای اتصال کارت شبکه به محیط فیزیکی استفاده می شود.
- در اترنت ۱۰ گیگابیت فقط از کانال های فیبر نوری از نوع چند مد یا تک مد استفاده می شود. با استفاده از این کانال ها می توان حداکثر تا ۴۰ کیلومتر را بدون نیاز به تکرار کننده اطلاعات ارسال نمود. هر دو واسط موجود برای شبکه های محلی و گسترده از یک زیر لایه PMD یکسان استفاده می کنند.

کاربردهای اترنت ۱۰ گیگابیت

فن آوری اترنت، متداول ترین و کاملترین فن آوری در شبکه های محلی می باشد. با توسعه فن آوری اترنت و پیدایش ۱۰ گیگابیت اترنت، امکان استفاده از برنامه های کاربردی با پهنای باند بالا در شبکه های محلی فراهم می شود.

مشابه فن آوری اترنت ۱ گیگابیت، در اترنت ۱۰ گیگابیت نیز امکان استفاده از کانال های فیبر نوری تک مد و چند مد وجود دارد. در شبکه های اترنت ۱۰ گیگابیت در حالتی که از فیبر تک مد استفاده می شود، حداکثر فاصله بین ایستگاه های شبکه ۴۰ کیلومتر می باشد در حالی که در شبکه های اترنت ۱ گیگابیت این فاصله ۵ کیلومتر است. به این دلیل استفاده از اترنت ۱۰ گیگابیت برای اتصال شبکه های محلی شرکت ها که دارای چندین شبکه محلی در سطح شهر می باشند مناسب تر از اترنت ۱ گیگابیت می باشد.

با استفاده از این نوع شبکه ها امکان استفاده از خدماتی نظیر ویدئوی متحرک، تصویر برداری پزشکی و کاربردهای گرافیکی با دقت بالا وجود دارد. همچنین به علت سرعت بالای شبکه های اترنت ۱۰ گیگابیت، تأخیر ارسال بسیار پایین است، بنابراین از آن می توان برای ارسال ترافیک داده ای انفجاری استفاده نمود. همچنین از اترنت ۱۰ گیگابیت بر ثانیه

^۱ LAN PHY
^۲ WAN PHY

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

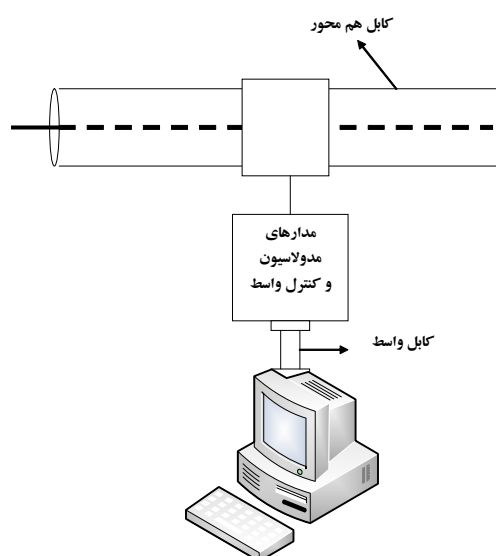
می توان برای پیاده سازی شالوده شبکه های شهری استفاده کرد. با استفاده از این فن آوری می توان همان طور که گفته شد، فاصله کانال های شبکه را تا ۴۰ کیلومتر افزایش داد. از فن آوری اترنت ۱۰ گیگابیت در شبکه های گسترده نیز استفاده می شود. به عنوان مثال فراهم کنندگان خدمات اینترنت، از شبکه های اترنت ۱۰ گیگابیت برای اتصال سریع و نسبتاً ارزان به شبکه اینترنت استفاده می کنند. همچنین می توان از این فن آوری برای اتصال شبکه های محلی دور از هم از طریق شبکه گسترده استفاده نمود.

۳-۴-۲- شبکه گذرگاه نشانه (IEEE 802.4)

با وجود این که امروزه استاندارد اترنت به طور وسیعی در مراکز دانشگاهی و ادارات استفاده می شود، ولی یک عیب عمده در آن وجود دارد. در شبکه های اترنت امکان اولویت گذاری در قاب های ارسالی وجود ندارد؛ از این رو نمی توان از آن برای کاربردهای زمان حقیقی^۱ استفاده نمود. در این راستا از سوی شرکت جنرال موتور که در زمینه اتوماسیون کارخانجات فعال است، استاندارد گذرگاه نشانه مطرح گردید. در شکل (۳-۲۲)، نحوه اتصال ایستگاه ها در شبکه گذرگاه نشانه به کابل هم محور نشان داده شده است.

واحد مدولاسیون و واسط فیزیکی که در شکل فوق نشان داده شده است، موظف به انجام عملیات زیر است:

- کدینگ داده های ارسالی (مدولاسیون)
- بازگشایی کد داده های دریافتی (دی مدولاسیون)
- تولید پالس ساعت



شکل (۳-۲۲): نحوه اتصال ایستگاه ها در شبکه گذرگاه نشانه به کابل هم محور

شبکه های گذرگاه نشانه در دو حالت کاری عمل می نمایند که عبارتند از: حالت کاری باند پهن^۲ و باند حامل^۱. در حالت کاری باند حامل، داده های ارسالی با استفاده از مدولاسیون FSK به صورت سیگنال های سینوسی تبدیل می شوند. بسامد سیگنال حامل برای بیت ۰، دوبرابر بسامد حامل برای بیت ۱ می باشد.

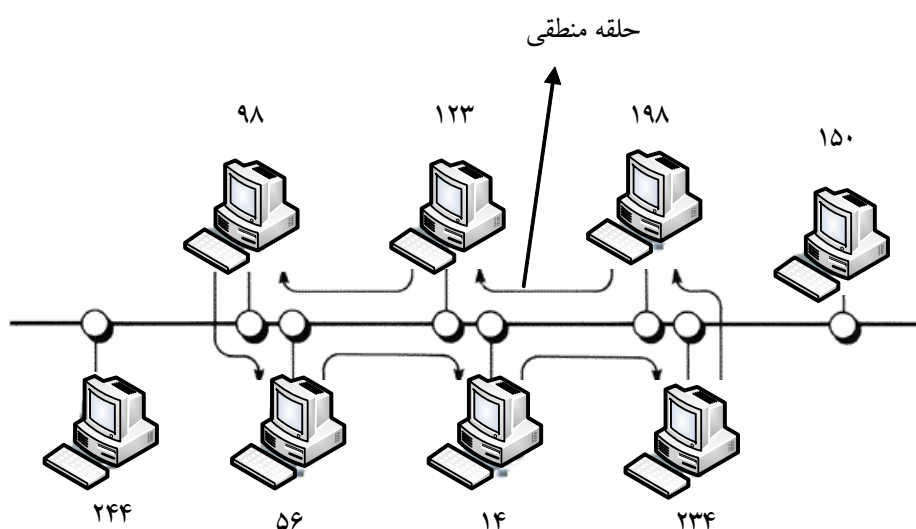
^۱ Real time

^۲ Broadband

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

در این استاندارد، ایستگاه های شبکه از طریق یک گذرگاه مشترک به یکدیگر متصل می شوند. ایستگاه های شبکه تشکیل یک حلقه منطقی می دهند به طوری که هر ایستگاه آدرس ایستگاه سمت چپ خود را می داند. هنگامی که حلقه منطقی به وجود می آید، ایستگاهی که دارای بالاترین آدرس است قادر به ارسال قاب می باشد. پس از آن که ارسال قاب های ایستگاه فرستنده پایان یافت، ایستگاه مزبور با ارسال یک قاب کنترلی خاص به نام نشانه، امکان ارسال را در اختیار همسایه اش بر روی حلقه منطقی می گذارد. بعد از آن که ایستگاه، نشانه را به همسایه منطقی خود ارسال نمود، برای اطمینان از دریافت صحیح آن توسط همسایه، برای مدت زمان معینی به کانال گوش فرامی دهد و چنانچه در این مدت عبور قاب سالمی از کانال را تشخیص ندهد، متوجه خراب شدن و یا گم شدن نشانه شده و دوباره آن را برای همسایه منطقی خود ارسال می دارد.

بدین ترتیب نشانه در سراسر شبکه در حرکت می باشد و فقط ایستگاهی که نشانه را در اختیار دارد، قادر به ارسال می باشد. بنابراین امکان بروز تداخل در این استاندارد وجود ندارد. شکل (۳-۲۳) نمونه ای از یک شبکه گذرگاه نشانه را نشان می دهد. همچنین در این شکل حلقه منطقی نیز نشان داده شده است.



شکل (۳-۲۳): شبکه گذرگاه نشانه

همان طور که در شکل فوق نیز دیده می شود، در شبکه های گذرگاه نشانه، ترتیب فیزیکی قرار گرفتن ایستگاه ها در روی گذرگاه مشترک اهمیتی ندارد. هنگامی که یک ایستگاه، قابی را ارسال می کند، آن قاب در هر دو طرف کانال منتشر می شود و تمام ایستگاه های دیگر آن را دریافت می دارند، ولی تنها ایستگاهی که آدرس گیرنده قاب ارسالی با آدرس آن مطابقت دارد قاب را دریافت می کند. در پایان ارسال هر ایستگاه، قاب در اختیار همسایه منطقی ایستگاه قرار می گیرد. احتمال این که در یک حلقه منطقی تمام ایستگاه های شبکه عضویت نداشته باشند وجود دارد. به عنوان مثال در شکل (۳-۲۳)، فقط ایستگاه های به آدرس ۱۹۸، ۱۲۳، ۹۸، ۵۶، ۱۴ و ۲۳۴ داخل حلقه منطقی می باشند. هنگامی که حلقه منطقی فعال می شود، می توان یک ایستگاه جدید به حلقه افزود و یا ایستگاهی را از حلقه خارج ساخت.

پروتکل گذرگاه نشانه از پیچیدگی بسیار بالایی برخوردار است. هر ایستگاه دارای ۱۰ زمان سنج و ۱۲ متغیر داخلی می باشد. در شبکه های فوق کابل های هم محور ۷۵ اهمی که بیشتر در سیستم های تلویزیون کابلی کاربرد دارند استفاده می شود. سرعت های متداول این نوع شبکه ها عبارتند از ۱،۵ و ۱۰ مگابیت بر ثانیه.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

هنگامی که برای اولین بار حلقه منطقی تشکیل می شود، ایستگاه ها به ترتیب آدرس فیزیکی (کارت شبکه) خود در حلقه قرار می گیرند. مبادله نشانه نیز از ایستگاه های با آدرس بالا به سمت ایستگاه های با آدرس کم صورت می گیرد. هرگاه ایستگاهی نشانه را در اختیار قرار گرفت، فقط برای مدت محدودی اقدام به ارسال قاب می نماید و بعد از آن که مدت زمان آن تمام شد، باید نشانه را در اختیار ایستگاه دیگر قرار دهد. چنانچه ایستگاهی که نشانه را در اختیار دارد داده هایی برای ارسال نداشته باشد، آنگاه به سرعت نشانه را آزاد می کند و به ایستگاه مجاور خود بر روی حلقه منطقی تحویل می دهد.

در شبکه های گذرگاه نشانه، هریستگاه به طور داخلی به چهار زیر ایستگاه دیگر تقسیم بندی می شود. هر زیر ایستگاه داخلی قادر به ارسال یک کلاس خاص ترافیک می باشد. چهار کلاس ترافیک با اولویت های ۰، ۲، ۴ و ۶ در شبکه های گذرگاه نشانه وجود دارند که کلاس صفر کمترین اولویت و کلاس ۶ بالاترین اولویت را در اختیار دارد. نحوه استفاده از ۴ کلاس ترافیکی فوق به صورت زیر می باشد:

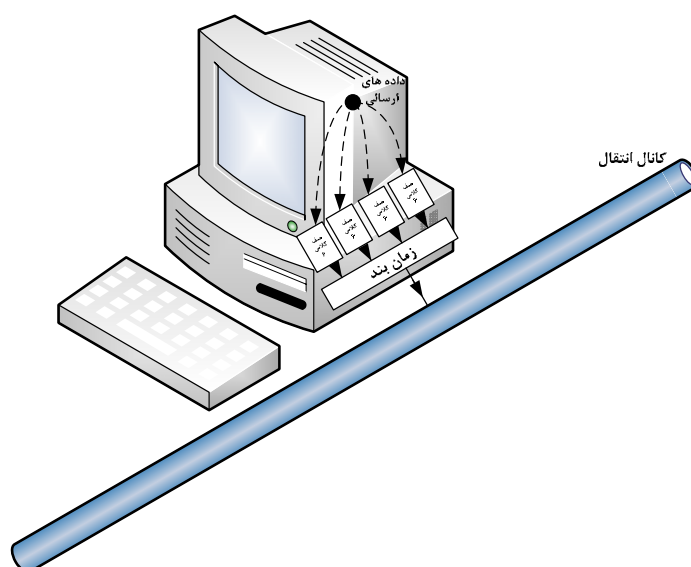
□ **کلاس ۶:** پیام های اورژانسی و بسیار مهم نظیر آلام های هشدار دهنده و عملیات کنترلی حساس از کلاس ۶ که بالاترین اولویت را دارا می باشد، استفاده می کنند.

□ **کلاس ۴:** پیام های مربوط به مدیریت حلقه منطقی و کنترل طبیعی شبکه از این کلاس ترافیکی استفاده می نمایند.

□ **کلاس ۲:** پیام های مربوط به روتین های گردآوری داده ها به منظور واقع نگاری^۱ از کلاس اولویت ۲ استفاده می نمایند.

□ **کلاس ۰:** پیام های مربوط به انتقال فایل دارای کمترین اولویت بوده و از کلاس اولویت ۰ استفاده می کنند.

هنگامی که از لایه بالاتر (زیر لایه LLC) قابی برای ارسال تحویل زیر لایه MAC می گردد، ابتدا قاب دریافتی از نظر اولویت بررسی می شود و سپس به یکی از زیر ایستگاه های ۰ تا ۶ ارسال می گردد و در آنجا در یک صف قرار می گیرد تا نوبت ارسال آن فرا برسد. در شکل (۳-۲۴) زیر ایستگاه های موجود در یک ایستگاه شبکه گذرگاه نشانه نشان داده شده است.



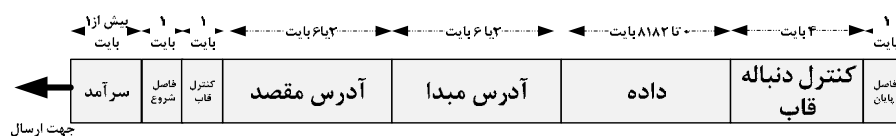
شکل (۳-۲۴): زیر ایستگاه های موجود در یک ایستگاه شبکه گذرگاه نشانه

^۱ Logging

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

هرایستگاه برای کنترل ارسال قاب ها دارای دو زمان سنج می باشد که عبارتند از: زمان سنج نگه داری نشانه (THT^1) و زمان سنج نگه داری نشانه برای کلاس اولویت بالا ($HP-THT^2$). هنگامی که یک ایستگاه شبکه نشانه را در اختیاری می گیرد، آنرا به زیرایستگاه شماره ۶ تحویل می دهد. این زیرایستگاه حداکثر به اندازه مدت زمان زمان سنج $HP-THT$ ، قادر به ارسال قاب های با اولویت بالا می باشد. حداکثر مدت زمانی که ایستگاه قادر به نگه داری نشانه و ارسال قاب های خود می باشد توسط زمان سنج THT مشخص می شود. بنابراین در شبکه های گذرگاه نشانه، هر زیرایستگاه برای مدت زمان معینی قادر به ارسال داده ها می باشد و هنگامی که زمان سنج هر زیرایستگاه لبریز شد، نشانه از آن سلب می شود و به زیرایستگاه بعدی داده می شود. از آنجایی که کلاس های ۶ و ۴ به ترتیب دارای اولویت بیشتری نسبت به کلاس های دیگر می باشند، مدت زمانی که زمان سنج در اختیار کلاس ۶ است بیشتر از سایر کلاس ها می باشد. بدین ترتیب زیر کلاس صفر کمترین فرصت ارسال قاب های خود را پیدا می نماید.

چنانچه زیر ایستگاهی تمام قاب های خود را ارسال دارد، دیگر نیازی به نشانه ندارد و زمان باقی مانده خود را تحویل زیرایستگاه بعدی می دهد. با توجه به اولویت بالایی که زیر کلاس ۶ دارد، از آن می توان برای ارسال داده های زمان حقیقی مثل صوت و تصویر استفاده کرد. در شکل (۳-۲۵) ساختار قاب های گذرگاه نشانه نشان داده شده است.



شکل (۳-۲۵): ساختار قاب های گذرگاه نشانه

همان طور که در این شکل نیز دیده می شود، در قاب های گذرگاه نشانه فیلدهای زیر موجود است:

- **فیلد سرآمد:** حداقل طول این فیلد یک بایت می باشد و مشابه استاندارد اترنت از آن برای همزمان سازی ساعت های فرستنده و گیرنده استفاده می شود.
- **فیلدهای فاصل شروع و فاصل پایان:** از این فیلدها برای تعیین محدوده شروع و پایان قاب ها استفاده می گردد.
- **فیلد کنترل قاب:** برای جداسازی قاب های داده ای از قاب های کنترل شبکه از این فیلد تکبایتی استفاده می شود. توسط این فیلد اولویت قاب های داده ای قابل تعیین می باشد. همچنین چنانچه بیت خاصی در این فیلد فعال باشد، گیرنده قاب ملزم به ارسال پیام تصدیق مبنی بر دریافت صحیح یا نادرست قاب است. نوع قاب های کنترلی توسط این فیلد مشخص می شود. انواع مختلف قاب های کنترلی عبارتند از: قاب های واگذاری نشانه و قاب های نگه داری حلقه که به وسیله آن امکان ورود و خروج ایستگاه جدید به حلقه وجود دارد.
- **فیلدهای آدرس مبدا و آدرس مقصد:** توسط این فیلدها مشابه آنچه که در استاندارد اترنت گفته شد، آدرس های مبدا و مقصد قاب ارسالی مشخص می شود.
- **فیلد داده:** این فیلد حاوی داده های زیر لایه LLC است که باید توسط قاب های MAC تحویل مقصد شود. طول این فیلد متغیر می باشد و چنانچه از آدرس های دو بایتی استفاده شود، این فیلد حداکثر دارای طول ۸۱۸۲ بایت خواهد بود ولی در صورت استفاده از آدرس های ۶ بایتی حداکثر طول این فیلد ۸۱۷۴ بایت است.

¹ Token Hold Timer

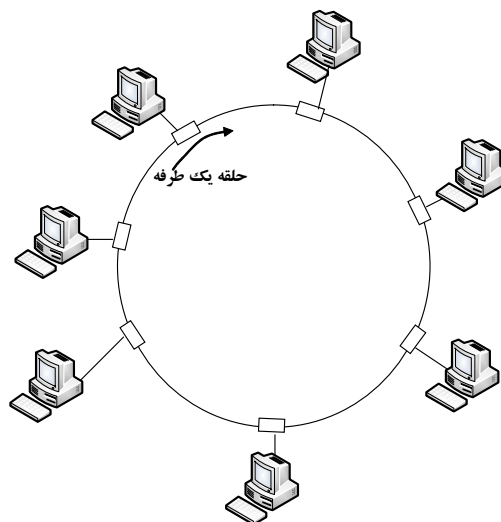
² High-Priority Token Hold Timer

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

□ **فیلد کنترل دنباله قاب:** این فیلد که مشابه فیلد کد افزونگی چرخشی (CRC) استاندارد اترنت می باشد، برای تشخیص و رفع خطاهای احتمالی در انتقال قاب ها به کار می رود.

۳-۴-۳- شبکه حلقه نشانه (IEEE 802.5)

در این استاندارد مطابق با شکل (۳-۲۶)، تمام ایستگاه ها از طریق یک حلقه مشترک به یکدیگر متصل می شوند. البته یک حلقه را می توان به صورت مجموعه ای از کانال های نقطه به نقطه تصور نمود و برای پیاده سازی آن از محیط هایی نظیر زوج سیم به هم تابیده شده، کابل هم محور و فیبر نوری استفاده کرد. هنگامی که تمام ایستگاه های موجود در حلقه بی کار هستند، یک نشانه در حلقه در حال چرخش می باشد. وقتی که ایستگاهی قصد ارسال یک قاب را داشته باشد، ابتدا نشانه را تصرف می نماید و آن را از حلقه خارج می سازد و سپس اقدام به ارسال اطلاعات می کند. از آن جایی که فقط یک نشانه در شبکه به صورت آزاد وجود دارد، بنابراین امکان تداخل از بین می رود. طول فیزیکی حلقه و سرعت آن باید طوری باشد که حداقل یک قاب نشانه به طور کامل در حلقه جریان داشته باشد.



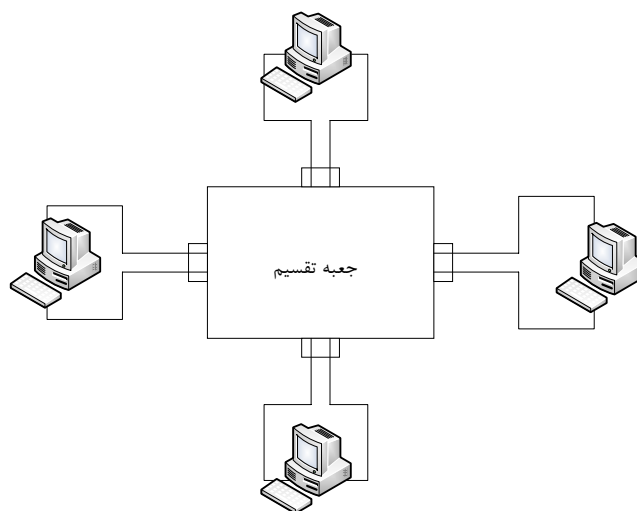
شکل (۳-۲۶) : شبکه حلقه نشانه

در شبکه های حلقه نشانه، از کانال های فیزیکی از نوع زوج سیم های STP در سرعت های ۱.۴ و ۱۶ مگابیت بر ثانیه استفاده می شود. یکی از مشکلات اصلی شبکه های حلقه نشانه این است که چنانچه کابل شبکه در محلی قطع شود، کل شبکه از کار می افتد. برای رفع این مشکل از جعبه تقسیم استفاده می شود. در این روش ایستگاه ها از نظر منطقی تشکیل یک حلقه می دهند ولی از نظر فیزیکی هر ایستگاه به وسیله دو زوج سیم STP که یکی برای ارسال و یکی برای دریافت است به جعبه تقسیم متصل می شوند. در شکل (۳-۲۷)، نمونه ای از شبکه حلقه نشانه با استفاده از جعبه تقسیم نشان داده شده است.

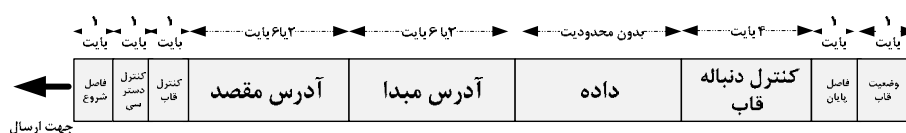
در داخل جعبه چندین کلید وجود دارد که وظیفه آنها اتصال یا قطع اتصال یک ایستگاه از حلقه می باشد. چنانچه حلقه قطع شود و یا ایستگاهی از کار بیفتد، کلید آزاد می شود و در نتیجه ایستگاه از حلقه خارج می گردد. می توان کلیدهای فوق را به وسیله نرم افزار کنترل نمود، که در این صورت امکان عیب یابی اتوماتیک شبکه فراهم می آید. هنگامی که حلقه از هرگونه ترافیکی خالی باشد، یک نشانه ۳ بیتی به طور مداوم در حلقه می چرخد تا این که ایستگاهی نشانه را دریافت دارد و آن را تصرف کند. در شبکه های حلقه نشانه هر ایستگاهی که قاب را ارسال نموده است، خود موظف به خارج نمودن آن

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

از حلقه می باشد. بدین ترتیب هر قاب ارسالی یک دور در حلقه می چرخد و سپس توسط خود فرستنده از حلقه حذف می شود. هر ایستگاهی که نشانه را در اختیار دارد، قادر به ارسال قاب به مدت ۱۰ میلی ثانیه می باشد. البته این زمان قابل تغییر است. بعد از اتمام ارسال قاب ها، نشانه دوباره توسط ایستگاه تولید می شود و وارد شبکه می گردد. در شبکه های حلقه نشانه، هر شبکه دارای یک ایستگاه ناظر^۱ می باشد که از آن برای نظارت بر حلقه استفاده می شود. از ایستگاه ناظر برای پاک سازی حلقه از قاب های مخدوش و انجام اقدامات لازم در هنگامی که حلقه قطع می شود، استفاده می گردد. جهت اطمینان از گم شدن احتمالی نشانه، هر ناظر شبکه دارای یک زمان سنج می باشد که در صورت لبریز شدن آن، متوجه گم شدن نشانه می شود. در شکل (۳-۲۸)، ساختار قاب های حلقه نشانه نشان داده شده است.



شکل (۳-۲۷): نمونه ای از یک شبکه حلقه نشانه با استفاده از جعبه تقسیم



شکل (۳-۲۸): ساختار قاب های حلقه نشانه

همان طور که در این شکل نیز دیده می شود، در قاب های حلقه نشانه فیلدهای زیر موجود می باشد:

- **فیلد فاصل شروع^۲ و فاصل پایان^۳:** از این فیلدها برای نشان دادن شروع و پایان هر قاب استفاده می شود.
- **فیلد کنترل دسترسی^۴:** این فیلد شامل بیت هایی برای رزرو نشانه و نظارت بر حلقه می باشد.
- **فیلد کنترل قاب:** برای جداسازی قاب های داده ای از قاب های کنترلی از این فیلد استفاده می شود.
- **فیلدهای آدرس مبدا و مقصد:** این فیلدها مشابه فیلدهای موجود در استانداردهای اترنت و گذرگاه نشانه برای تعیین آدرس فرستنده و گیرنده قاب ها به کار می روند.

^۱ Monitoring station

^۲ Start delimiter

^۳ End delimiter

^۴ Access control

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

- **فیلد داده:** این فیلد حاوی داده های لایه بالاتر می باشد. در طول این فیلد هیچ گونه محدودیتی وجود ندارد.
- **فیلد کنترل دنباله قاب:** این فیلد مشابه با فیلد موجود در قاب های اترنت و گذرگاه نشانه برای بررسی و اطمینان از صحت قاب دریافتی در مقصد به کار می رود. از روش CRC برای کنترل خطا استفاده می شود.
- **فیلد وضعیت قاب^۱:** در این فیلد دو بیت به نام های بیت های A و C موجود است که از آنها برای اطمینان از دریافت صحیح قاب ارسالی توسط مبدأ در گیرنده استفاده می شود. چنانچه مقصد در شبکه موجود نباشد و یا هنوز ایستگاه خاموش باشد، دو بیت A و C صفر می باشند. در صورتی که $A=1$ و $C=0$ باشد، مقصد موجود بوده است ولی قاب پذیرفته نشده است. چنانچه $A=C=1$ باشد، مقصد وجود داشته است و قاب را هم به طور صحیح دریافت نموده است. بدین ترتیب فرستنده با بررسی وضعیت بیت های فوق، هنگامی که قاب ارسالی خود را دوباره دریافت می کند، متوجه دریافت ویا عدم دریافت صحیح قاب در مقصد می شود.

۳-۵- پروتکل DQDB

توسط گروه ۸۰۲ سازمان IEEE، استاندارد 802.6 که با نام DQDB نیز شناخته می شود، برای استفاده در شبکه های شهری ارائه گردید. همان طور که از نام این استاندارد شناخته می شود DQDB از ساختار متشکل از دو گذرگاه مشترک استفاده می نماید. هر ایستگاه در شبکه به دو گذرگاه مشترک متصل می باشد. نحوه دسترسی به گذرگاه مشترک فوق به وسیله مکانیسمی بنام صف های توزیع شده انجام می گیرد.

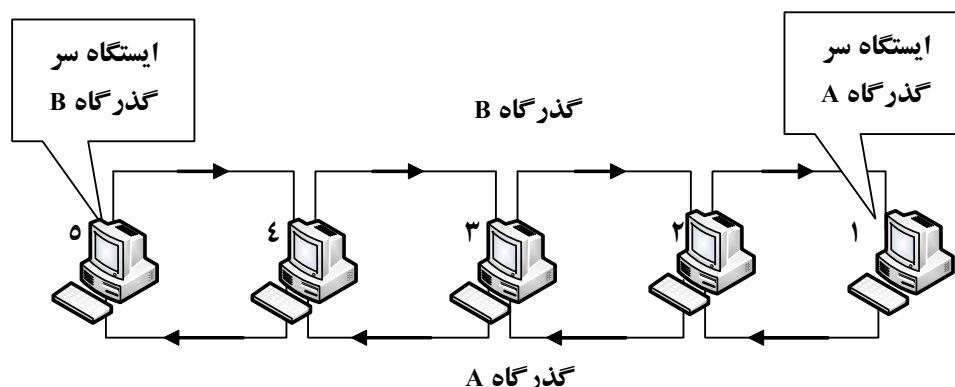
در شکل (۳-۲۹) توپولوژی یک شبکه DQDB نشان داده شده است. مطابق با شکل فوق دو گذرگاه مشترک یک طرفه به نام A و B در شبکه وجود دارند. تمام ایستگاه های شبکه به طور مستقیم به هر دو گذرگاه مشترک A و B متصل می باشند. ترافیک ارسالی در گذرگاه های مشترک فوق یک طرفه می باشد. جهت ترافیک در یک گذرگاه مشترک بر خلاف جهت ترافیک در گذرگاه مشترک دیگر می باشد. ارتباط بین ایستگاه ها در شبکه های DQDB به وسیله جریان ترافیکی در گذرگاهها مشخص می شود. به عنوان مثال در گذرگاه A شکل (۳-۲۹) ایستگاه های ۱ و ۲ نسبت به ایستگاه ۳ بالا جریانی^۲ و ایستگاه های ۴ و ۵ نسبت به ایستگاه ۳، پایین جریانی^۳ می باشند. همچنین در گذرگاه مشترک B نیز ایستگاه های ۱ و ۲ نسبت به ایستگاه ۳ پایین جریان و ایستگاه ۴ و ۵ نسبت به ایستگاه ۳، بالا جریانی می باشند.

۳-۵-۱- ارسال برش های زمانی

در شبکه های DQDB ارسال اطلاعات از طریق برش های زمانی ۵۳ بیتی انجام می گیرد. ایستگاه سر گذرگاه مشترک موظف به ایجاد برش زمانی خالی برای استفاده در گذرگاه مشترک می باشد. نرخ ارسال ایستگاه ها بستگی به تعداد برش های زمانی ایجاد شده در ثانیه دارد. برش زمانی خالی در گذرگاه مشترک به سمت پایین حرکت می نماید تا این که یک ایستگاه فرستنده داده ها را درون برش زمانی قرار دهد. گیرنده نیز با توجه به آدرس خود اقدام به برداشتن داده از برش زمانی می نماید.

^۱ Status field
^۲ Upstream
^۳ Downstream

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۳-۲۹): مثالی از شبکه DQDB

همان طور که گفته شد از آنجایی که در شبکه DQDB از دو گذرگاه مشترک استفاده می شود، ایستگاه فرستنده باید از طریق گذرگاه مشترکی داده های خود را ارسال نماید که ایستگاه گیرنده نسبت به آن پایین جریان باشد. به عنوان مثال اگر ایستگاه ۳ بخواهد برای ایستگاه ۲ در شکل (۳-۲۹) داده هایی را ارسال نماید، از گذرگاه مشترک B استفاده می کند.

۳-۵-۲- رزرو برش های زمانی

برای ارسال داده ها در شبکه های DQDB هر ایستگاه باید منتظر ورود یک برش زمانی خالی باشد. از آنجایی که برشهای زمانی خالی از طرف ایستگاه سرگذرگاه مشترک به سمت پایین تولید می گردد، بنابراین ایستگاه هایی که نزدیکتر به ایستگاه سر می باشند شانس بیشتری برای دسترسی به برشهای زمانی خالی در گذرگاه مشترک دارند. چنانچه برای مشکل فوق راه حل مناسبی ارائه نگردد، کیفیت خدمات در ایستگاه های پایین جریان به شدت کاهش می یابد.

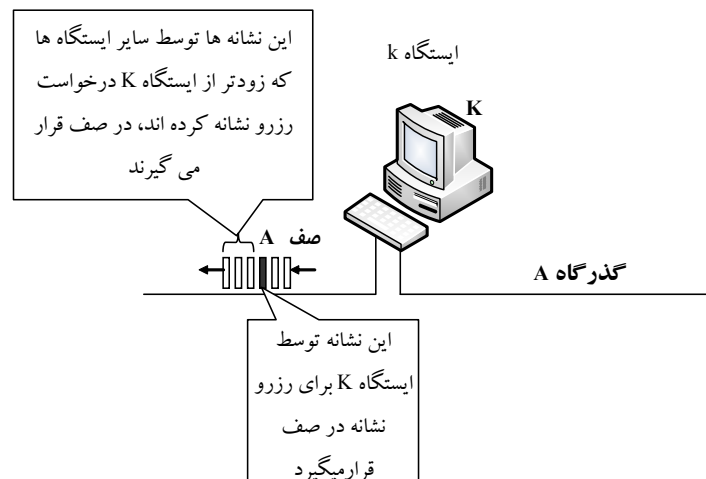
برای حل مشکل فوق از عملیات رزرو برش زمانی استفاده می شود. هر ایستگاه در صورتی اجازه استفاده از برش زمانی خالی را دارد که قبلاً آن را رزرو کرده باشد. از آنجایی که جهت ارسال در گذرگاههای مشترک یک طرفه می باشد، هر ایستگاه برای رزور یک برش زمانی در یک گذرگاه مشترک از گذرگاه مشترک دوم استفاده می نماید. با فعال نمودن یک بیت مشخص در هر برش زمانی عملیات رزرو انجام می گیرد.

۳-۵-۳ - صف های توزیع شده

برای انجام عملیات رزرو برش زمانی و ردگیری عملیات رزرو سایر ایستگاه ها، در هر گذرگاه مشترک در شبکه های DQDB، هر ایستگاه به دو صف نیاز دارد. برای گذرگاه مشترک A، صف A و برای گذرگاه مشترک B، صف B در نظر گرفته می شود. عملکرد صف ها به صورت FIFO می باشند.

هنگامی که ایستگاهی درخواست رزرو برش زمانی را ارسال می کند، تمام ایستگاه های دیگر که درخواست فوق را دریافت می دارند، آن را به صف خود اضافه می نمایند. با عبور هر برش زمانی خالی یکی از محتویات صف کاهش می یابد. چنانچه خود یک ایستگاه بخواهد داده هایی را ارسال نماید، ابتدا درخواست رزرو برش زمانی خود را از طریق گذرگاه مشترک دوم ارسال می کند و سپس در صف یک علامت که نشان دهنده درخواست رزرو خود ایستگاه می باشد قرار می دهد. شکل (۳-۳۰) عملیات رزرو در صف را نشان می دهد.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

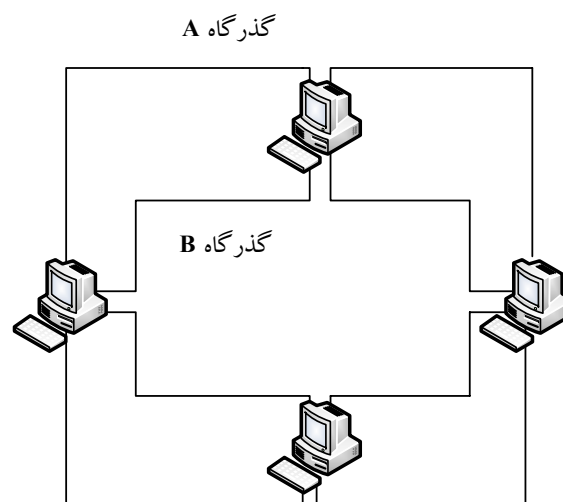


شکل (۳-۳۰): مثالی از رزرو نشانه در شبکه DQDB

با عبور هر برش زمانی خالی یکی از محتویات صف کم می شود. چنانچه نشانه مشخص کننده رزرو ایستگاه در صف به ابتدای صف رسید، نوبت ارسال خود ایستگاه فرا رسیده است. در این حالت با عبور اولین برش زمانی خالی، ایستگاه داده های خود را در آن قرار می دهد و آن را ارسال می دارد.

۳-۵-۴ - ساختار حلقه

می توان پروتکل DQDB را به صورت حلقه نیز پیاده سازی نمود که در شکل (۳-۳۱) نمونه ای از این ساختار نشان داده شده است. در این حالت یک ایستگاه نقش هر دو ایستگاه شروع و پایان را عمل می نماید. یکی از مزایای این ساختار، قدرت آن در مواجهه با خرابی در کانال است.



شکل (۳-۳۱): ساختار حلقه ای DQDB

۳-۵-۵- لایه های DQDB

توسط سازمان IEEE زیرلایه های MAC و لایه فیزیکی برای DQDB تعریف شده است. زیرلایه MAC موظف به تجزیه قاب های ورودی از زیرلایه LLC به تکه های ۴۸ بیتی می باشد. این زیر لایه به هر تکه ۵ بایت سرآیند اضافه می نماید و قاب های ۵۳ بیتی ایجاد می کند.

در سرآیند قاب های DQDB که طول آن ۵ بایت است، ۵ فیلد زیر وجود دارد:

- **فیلد دسترسی:** از این فیلد که دارای طول ۸ بیت می باشد برای کنترل دسترسی به گذرگاه مشترک استفاده می شود. این فیلد به ۵ زیر فیلد زیر تجزیه می شود.
- **بیت B:** چنانچه این بیت ۱ باشد، نشان دهنده وجود داده در برش زمانی است. در صورتی که این بیت صفر باشد برش زمانی خالی می باشد.
- **بیت ST:** توسط این بیت دو نوع برش زمانی مشخص می گردد که یکی از آنها برای ارسال قاب های داده و دیگری برای ارسال اطلاعات همزمانی به کار می رود.
- **بیت R:** از این بیت برای رزرو برش زمانی استفاده می شود.
- **فیلد PRS:** این فیلد دو بیتی هنگامی که ایستگاه مقصد محتویات برش زمانی ورودی خود را خواند صفر می گردد.
- **فیلد RQ:** این فیلد سه بیتی توسط ایستگاهی که می خواهد عملیات رزرو برش زمانی را انجام دهد مقدار دهی می شود. توسط این سه بیت می توان ۸ سطح اولویت تعریف نمود.
- **فیلد آدرس:** این فیلد ۲۰ بیتی حاوی مشخص کننده کانال مجازی (VCI^1) که در شبکه های شهری و گسترده استفاده می شود، می باشد. هنگامی که از شبکه های DQDB به صورت شبکه های محلی استفاده می شود، تمام بیت های این فیلد ۱ است. برای حمل آدرسهای فیزیکی، سرآیندهای دیگری به قابها اضافه می شود.
- **فیلد نوع:** این فیلد دو بیتی نوع داده های موجود در قاب را مشخص می نماید. داده های موجود در ۴۸ بایت قاب های DQDB می تواند داده های کاربر، داده های مدیریت و نظیر آن باشد.
- **فیلد اولویت:** توسط این فیلد دو بیتی اولویت برش زمانی مشخص می شود.
- **فیلد CRC:** این فیلد حاوی کد افزونگی چرخشی می باشد که از آن برای تشخیص یک یا چند بیت خطا و تصحیح یک بیت خطا در سرآیند استفاده می شود.

۳-۶- شبکه SMDS

یکی دیگر از استانداردهای شبکه های شهری، SMDS می باشد که از آن برای برقراری ارتباط با سرعت بالا استفاده می شود. یکی از موارد استفاده SMDS، اتصال شبکه های محلی سازمانها که در نقاط مختلف یک شهر قرار دارند به یکدیگر است. قبل از پیدایش SMDS اتصال بین شبکه های محلی فوق به سختی انجام می شد و اغلب از خدمات شبکه تلفن سوئیچ شده و DDS استفاده می گردید. از آنجایی که اکثر شبکه های محلی دارای نرخ ارسال بالای ۱۰ مگابایت بر ثانیه می باشند، استفاده از شبکه تلفن و خدمات آن برای اتصال شبکه های محلی به یکدیگر راه حل مناسبی نمی باشد. یکی دیگر از روش های مناسب، استفاده از خطوط T1 با سرعت ۱/۵۴۴ مگابایت بر ثانیه و یا خطوط T3 با سرعت ۴۴/۷۳۶ مگابایت بر ثانیه می باشد. استفاده از این خطوط تا حدی مشکل سرعت اتصال شبکه های محلی به یکدیگر را حل می نماید ولی باید

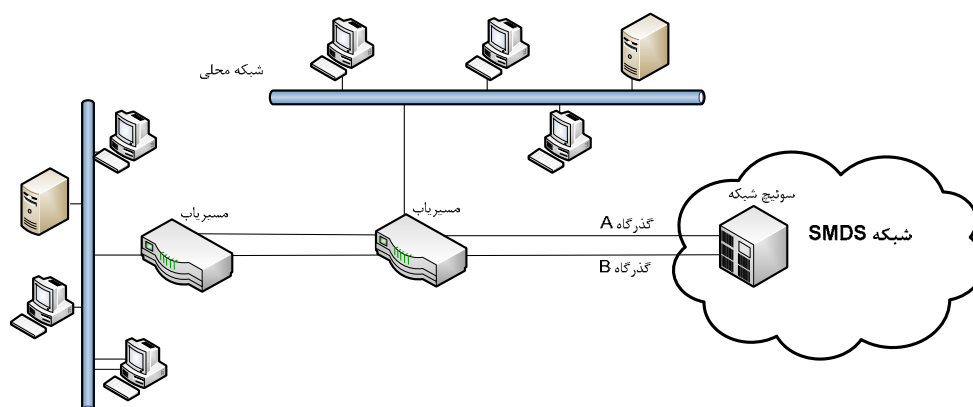
¹Virtual Channel Identifier

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

توجه نمود که هزینه خطوط فوق بسیار زیاد است. از طرف دیگر ترافیک داده ارسالی شبکه های محلی شرکتها به طور دائمی وجود ندارد و بنابراین از تمامی ظرفیت خطوط بهره برداری کامل نمی شود.

برای حل مشکلات فوق از فن آوری SMDS استفاده می گردد. SMDS از نوع سوئیچینگ بسته ای داده گرام می باشد که برای حمل ترافیکهای شبکه شهری با سرعت بالا بسیار مفید است. این فن آوری به وسیله یک سری استانداردهایی که توسط مرکز تحقیقاتی Bellcore پیشنهاد گردید و توسط خدمات دهنده های شبکه های مخابراتی به طور مناسب تغییر و توسعه یافت، توصیف می شود.

اتصال شبکه های محلی به شبکه SMDS از طریق مسیریابها صورت می پذیرد. دسترسی به شبکه SMDS از طریق پروتکل واسط SMDS (SIP^۱) که مبتنی بر DQDB است انجام می پذیرد. شبکه های محلی کاربران از طریق مسیریاب و دو گذرگاه مشترک مطابق با آنچه که در شکل (۳-۳۲) نشان داده شده است، به شبکه SMDS متصل می شوند.



شکل (۳-۳۲): اتصال شبکه محلی کاربران به شبکه SMDS

چنانچه مشتریان فقط یک شبکه محلی خود را به شبکه SMDS اتصال دهند، در این صورت مکانیسم DQDB ساده می باشد و نیازی به صف ندارد. ولی در صورتی که چندین شبکه محلی مشتریان به شبکه SMDS متصل شود، در این حالت به تمامی قابلیت های DQDB نیاز می باشد.

استانداردهای SMDS به روشنی نحوه پیاده سازی شبکه را مشخص نمی کند، بلکه فراهم کنندگان خدمات SMDS در انتخاب فن آوری شبکه برای حمایت از خدمات مورد نیاز خود آزاد می باشند. پیش بینی می شود که در آینده نزدیک نرخ ارسال در شبکه های SMDS به بالاتر از ۶۰۰ مگابیت بر ثانیه برسد.

۳-۷- شبکه FDDI

شبکه FDDI یک پروتکل شبکه محلی می باشد که توسط سازمان های ANSI و ITU-T استاندارد شده است. نرخ ارسال شبکه های FDDI، ۱۰۰ مگابیت بر ثانیه می باشد، که به مراتب بالاتر از نرخ شبکه های اترنت و گذرگاه نشانه و حلقه نشانه است. در هنگام ارائه FDDI فقط کانال فیبر نوری قادر به تامین سرعت ارسال ۱۰۰ مگابیت بر ثانیه بود، ولی امروزه با کمک زوج سیم های مسی نیز می توان به این سرعت دسترسی پیدا نمود. به نسخه سیم مسی از شبکه های FDDI، CDDI^۲ گفته می شود.

^۱SMDS Interface Protocol

^۲Copper Distributed Data Interface

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

شبکه FDDI مبتنی بر مبادله نشانه می باشد. در شبکه های حلقه نشانه هر ایستگاه فقط هنگامی که نشانه را دریافت نمود، قادر به ارسال یک قاب می باشد. اما در شبکه های FDDI دسترسی به شبکه محدود به زمان می باشد و هر ایستگاه تا هنگامی که محدودیت زمانی به آن اجازه می دهد، قادر به ارسال چندین قاب است. برای پیاده سازی این نوع مکانیسم دسترسی، دو نوع قاب داده در شبکه FDDI وجود دارند که عبارتند از: قاب همزمان و قاب غیرهمزمان. کلمه همزمان در FDDI اشاره به اطلاعاتی دارد که به زمان حساس می باشند و در مقابل، کلمه غیرهمزمان به اطلاعاتی اشاره می کند که به زمان حساس نمی باشند. هر ایستگاهی که نشانه را در اختیار می گیرد ابتدا قاب های همزمان خود را ارسال می دارد و چنانچه از زمان ارسال آن چیزی باقی مانده باشد، قاب های غیرهمزمان ارسال می شوند.

۳-۷-۱- رجیسترهای FDDI

در FDDI برای کنترل چرخش نشانه و دسترسی عادلانه ایستگاه های شبکه به کانال، از سه رجیستر زمانی استفاده می گردد. بنابراین هر ایستگاه در FDDI دارای سه رجیستر زمانی می باشد که برای کنترل حلقه به کار می رود. مقادیر این رجیسترها با راه افتادن حلقه تنظیم می گردد و در تمام مدت کارکرد شبکه ثابت می مانند. این سه رجیستر عبارتند از: رجیستر تخصیص همزمان (SA^1)، رجیستر زمان چرخش نشانه هدف ($TTRT^2$) و رجیستر زمان حداکثر مطلق (AMT^3). رجیستر SA مدت زمان مجاز برای هر ایستگاه که اجازه ارسال داده های همزمان را دارد مشخص می نماید. مقدار این رجیستر برای ایستگاه های شبکه متفاوت می باشد و در هنگام راه اندازی حلقه مقداردهی می گردد.

رجیستر TTRT مشخص کننده زمان متوسط مورد نیاز برای یک دور چرخش نشانه می باشد. مقدار این رجیستر برای تمام ایستگاه ها یکسان است که در هنگام راه اندازی حلقه تعیین می شود. از آنجایی که این رجیستر مقدار متوسط زمان چرخش یک دور نشانه در حلقه را مشخص می کند، ممکن است مقدار واقعی بیشتر یا کمتر از محتوای این رجیستر باشد. مقدار رجیستر AMT دو برابر مقدار رجیستر TTRT است. زمان چرخش نشانه در حلقه نباید بیشتر از این مقدار باشد. چنانچه زمان چرخش نشانه بیشتر از مقدار رجیستر AMT باشد، در این صورت حلقه باید دوباره راه اندازی شود.

۳-۷-۲- زمان سنج های FDDI

در شبکه FDDI هر ایستگاه برای مقایسه زمان واقعی با مقادیر موجود در رجیسترهای فوق نیاز به یک سری زمان سنج دارد. زمان سنج های فوق قابل مقداردهی و آغاز دوباره می باشند که مقدار آنها توسط ساعت سیستم کم می شود. دو زمان سنج در شبکه FDDI به کار می روند که عبارتند از: زمان سنج TRT و زمان سنج THT. زمان سنج TRT مقدار زمانی یک دور چرخش نشانه در حلقه را اندازه گیری می کند. هر ایستگاه مدت زمان سپری شده بین دو مشاهده متوالی نشانه در شبکه را با استفاده از زمان سنج TRT اندازه گیری می نماید. باید توجه نمود که زمان فوق شامل مدت زمان لازم برای ارسال قاب های ایستگاه هایی که نشانه را در اختیار می گیرند نیز می باشد. طبیعی است که در صورتی که در شبکه بار ترافیکی کمی موجود باشد، در این صورت مقدار زمان سنج TRT بسیار کم است.

در صورتی که ایستگاهی قاب هایی برای ارسال داشته باشد، با دریافت نشانه مقدار جاری TRT را از مقدار موجود در رجیستر TTRT کم نموده و حاصل را در زمان سنج THT قرار می دهد. مقدار حاصل در زمان سنج THT نشان دهنده حداکثر زمان مجاز برای ایستگاه که قادر به ارسال قاب های منتظر خود است، می باشد. در صورتی که مقدار THT مثبت باشد، ایستگاه قادر به ارسال قاب های منتظر خود است؛ ولی چنانچه مقدار THT منفی باشد، ایستگاه قادر به ارسال قاب های منتظر

^۱ Synchronous Allocation

^۲ Target Token Rotation Time

^۳ Absolute Maximum Time

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

خود نمی باشد و باید به سرعت نشانه را آزاد نماید. تا زمانی که THT مثبت است، ایستگاه قادر به ارسال قاب های غیرهمزمان می باشد. هنگامی که زمان سنج فوق صفر شد، ایستگاه باید نشانه را رها نماید.

۳-۷-۳- مشخصات الکتریکی FDDI

FDDI از یک مکانیسم کدگذاری ویژه به نام 4B/5B استفاده می کند. در این سیستم هر ۴ بیت داده تبدیل به یک کد ۵ بیتی می شوند و سپس با استفاده از روش کد گذاری NRZ-I ارسال می گردند. دلیل استفاده از کدگذاری 4B/5B این است که چنانچه یک رشته بیت طولانی صفر ارسال گردد، این احتمال وجود دارد که همزمانی فرستنده، گیرنده از بین برود. مکانیسم کدگذاری 4B/5B هر بخش ۴ بیتی داده را به ۵ بیت تبدیل می کند؛ طوری که بیشتر از ۲ بیت صفر متوالی در آن نباشد. در جدول (۲-۳) کدگذاری 4B/5B نشان داده شده است. از سایر کدهای ۵ بیتی باقی مانده که در جدول (۲-۳) وجود ندارند، برای مصارف کنترلی که در جدول (۳-۳) نشان داده شده است استفاده می شود.

جدول (۲-۳): کدگذاری 4B/5B در FDDI

رشته بیت ورودی	رشته بیت رمز شده
۰۰۰۰	۱۱۱۱۰
۰۰۰۱	۰۱۰۰۱
۰۰۱۰	۱۰۱۰۰
۰۰۱۱	۱۰۱۰۱
۰۱۰۰	۰۱۰۱۰
۰۱۰۱	۰۱۰۱۱
۰۱۱۰	۰۱۱۱۰
۰۱۱۱	۰۱۱۱۱
۱۰۰۰	۱۰۰۱۰
۱۰۰۱	۱۰۰۱۱
۱۰۱۰	۱۰۱۱۰
۱۰۱۱	۱۰۱۱۱
۱۱۰۰	۱۱۰۱۰
۱۱۰۱	۱۱۰۱۱
۱۱۱۰	۱۱۱۰۰
۱۱۱۱	۱۱۱۰۱

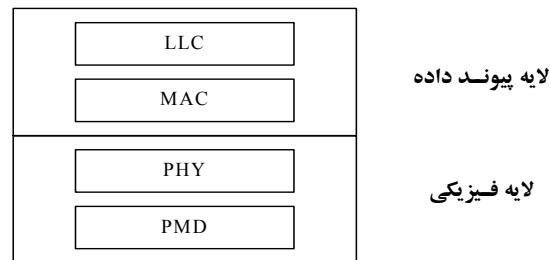
جدول (۳-۳): سمبل های کنترلی در کدگذاری 4B/5B

رشته بیت کد شده	سمبل کنترلی
۰۰۰۰۰	Q (خروج)
۱۱۱۱۱	I (حالت بی کار)
۰۰۱۰۰	H (حالت درنگ ^۱)
۱۱۰۰۰	J (مورد استفاده در فاصل شروع)
۱۰۰۰۱	K (مورد استفاده در فاصل شروع)
۰۱۱۰۱	T (مورد استفاده در فاصل پایان)
۱۱۰۰۱	S (تنظیم)
۰۰۱۱۱	R (آغاز دوباره)

^۱ Halt

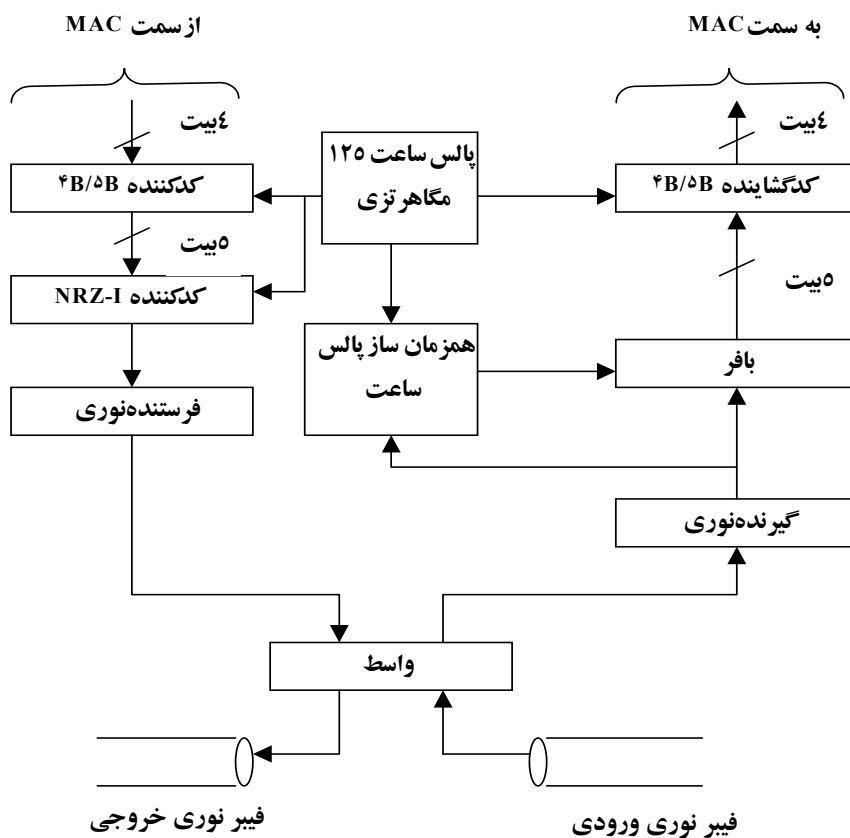
شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

در شکل (۳-۳۳) ساختار لایه ای FDDI نشان داده شده است. همان طور که در شکل دیده می شود. لایه فیزیکی FDDI به دو زیر لایه PHY و PMD تجزیه می شود. همچنین لایه پیوند داده، در FDDI، از دو زیر لایه LLC و MAC تشکیل شده است. زیر لایه LLC در FDDI، مشابه زیر لایه LLC تعریف شده در پروتکل IEEE 802.2 است. همچنین زیر لایه MAC در FDDI مشابه زیر لایه فوق در شبکه حلقه نشانه است، با این تفاوت که ساختار قاب های FDDI با قاب های حلقه نشانه متفاوت است.



شکل (۳-۳۳) : ساختار لایه ای FDDI

در شکل (۳-۳۴) بلوک دیاگرام واسط فیزیکی در FDDI نشان داده شده است.

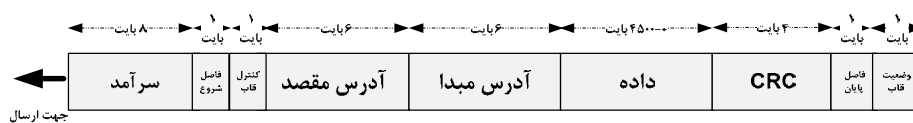


شکل (۳-۳۴) : ساختار واسط فیزیکی FDDI

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

در شکل (۳-۳۵) ساختار قاب های MAC ، در شبکه FDDI نشان داده شده است. مطابق شکل فوق در قاب های FDDI فیلدهای زیر موجود می باشد.

- **فیلد سرآمد:** این فیلد ۸ بیتی برای همزمانی پالس ساعت گیرنده با فرستنده به کار می رود.
- **فیلد فاصل شروع:** این فیلد نشان دهنده شروع قاب FDDI می باشد که به صورت کدهای متوالی J و K که در جدول (۳-۳) آورده شده است، می باشد.
- **فیلد کنترل قاب:** این فیلد نشان دهنده نوع قاب است.
- **فیلد آدرس مبدأ و مقصد:** این دو فیلد که طول هر یک ۶ بایت است، نشان دهنده آدرس مبدأ و آدرس مقصد قاب می باشند.
- **فیلد داده:** این فیلد حاوی داده های ارسالی می باشد که حداکثر طول آن ۴۵۰۰ بایت است .
- **فیلد CRC:** از این فیلد برای کنترل خطا در قاب های FDDI استفاده می شود .
- **فیلد فاصل پایان:** طول این فیلد در قاب های داده نیم بایت و در قاب های نشانه یک بایت کامل می باشد. هنگام ارسال قاب های FDDI فیلد فوق در قاب های داده به یک کد T و در قاب های نشانه به دو کد T تبدیل می شود. کد T در جدول (۳-۳) نشان داده شده است.
- **فیلد وضعیت قاب:** این فیلد مشابه فیلد فوق در شبکه های حلقه نشانه می باشد، که طول آن ۱/۵ بایت است و فقط در قاب های داده وجود دارد.

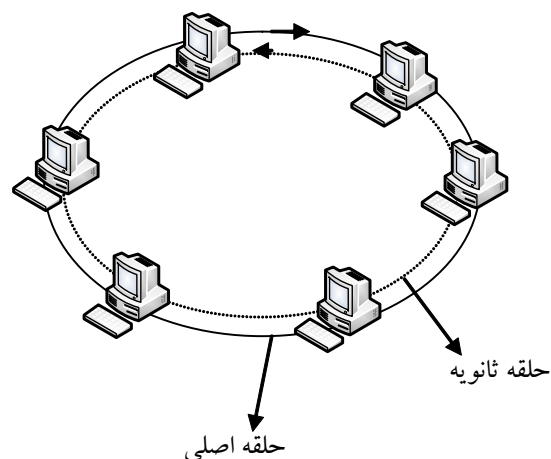


شکل (۳-۳۵): ساختار قاب های لایه MAC در FDDI

۳-۷-۳-۱- زیر لایه PMD

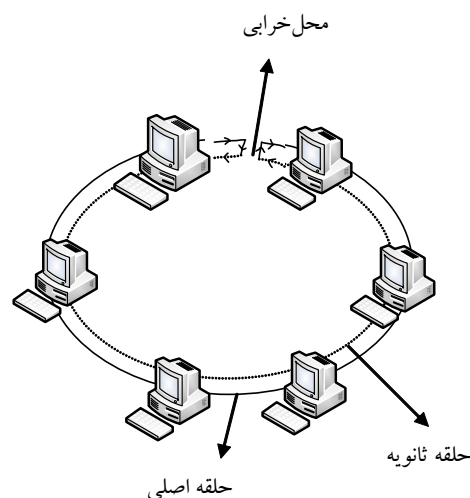
توسط زیر لایه PMD ، اتصال های لازم و تجهیزات الکترونیکی شبکه FDDI تعریف می گردد . مشخصات این زیر لایه، براساس این که محیط ارسال فیبرنوری و یا کابل مسی باشد، تعیین می شود. همان طور که در شکل (۳-۳۶) دیده می شود، FDDI از دو حلقه به نام های حلقه اصلی و حلقه ثانویه استفاده می کند. چنانچه حلقه اصلی دچار اشکال گردد، از حلقه ثانویه استفاده می شود.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۳-۳۶): حلقه ها در شبکه های FDDI

شکل (۳-۳۷) ساختار حلقه FDDI بعد از وقوع خرابی در حلقه اصلی را نشان می دهد. هر ایستگاه شبکه از طریق دو درگاه فیبرنوری که بر روی کانکتور واسط محیط (MIC^۱) نصب می شود، به حلقه های اصلی و ثانویه متصل می گردد.



شکل (۳-۳۷): ساختار حلقه های FDDI بعد از وقوع خرابی

در FDDI، سه نوع ایستگاه وجود دارد که عبارتند از: ایستگاه های DAC^۲، DAS^۳ و SAS^۴. در شکل (۳-۳۸) این نوع ایستگاه ها نشان داده شده است. ایستگاه های از نوع DAS، دارای دو MIC می باشند که از طریق آنها به هر دو حلقه اصلی و ثانویه متصل می باشند. چنانچه خطایی در حلقه اصلی به وجود آید، ایستگاه های DAS به طور اتوماتیک ارسال اطلاعات را از

^۱ Medium Interface Connector

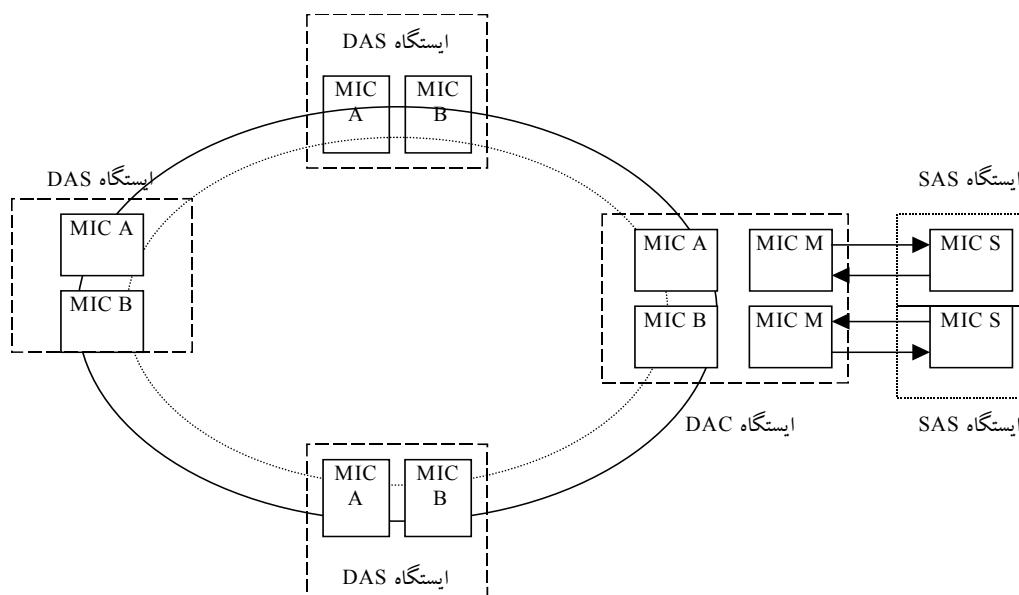
^۲ Dual Attachment Concentrator

^۳ Dual Attachment Station

^۴ Single Attachment Station

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

طریق MIC دوم خود که به حلقه ثانویه متصل است ادامه می دهند. اکثر ایستگاه های کاری، خدمات دهنده های شبکه و میکرو کامپیوترهای شبکه FDDI به صورت DAS عمل می کند. ایستگاه های SAS فقط یک MIC دارند و بنابراین فقط می توانند به یک حلقه متصل شوند. این ایستگاه ها به جای آن که مستقیماً به حلقه FDDI وصل شوند، به نودهای میانی DAC متصل می گردند. ایستگاه DAC موظف به فراهم سازی اتصال به هر دو حلقه شبکه می باشد. چنانچه ایستگاهی معیوب گردد، برای جلوگیری از قطع حلقه، ایستگاه از حلقه کنار زده می شود.



شکل (۳-۳۸): انواع اتصال ایستگاه ها در شبکه FDDI

۳-۷-۲- مقایسه FDDI با اترنت و حلقه نشانه

سه استاندارد مهم شبکه های محلی عبارتند از: شبکه اترنت، شبکه حلقه نشانه و شبکه FDDI. در جدول (۳-۴)، سه استاندارد فوق با یکدیگر مقایسه شده اند.

جدول (۳-۴): مقایسه انواع فن آوری های شبکه های محلی با یکدیگر

شبکه	روش دسترسی به کانال	طول آدرس	نوع کد گذاری	نرخ ارسال	قابلیت کنترل خطا
اترنت پایه	CSMA /CD	۶ بایت	منچستر	۱۰ مگابیت بر ثانیه	خیر
حلقه نشانه	عبور نشانه	۶ بایت	منچستر تفاضلی	۱۰ و ۱۶ مگابیت بر ثانیه	بله
FDDI	عبور نشانه	۶ بایت	4B/5B	۱۰۰ مگابیت بر ثانیه	بله

۳-۱۰- پروتکل های لایه پیوند داده

پروتکل های لایه پیوند داده به دو دسته تقسیم می شوند که عبارتند از: پروتکل های همزمان و پروتکل های غیرهمزمان. در پروتکل های غیرهمزمان هر بایت به همراه بیت های شروع و پایان، در رشته بیت ارسالی انتقال می یابد؛ اما در

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

پروتکل های همزمان کل رشته بیت ارسالی در قالب قاب هایی با طول مشخص ارسال می گردد. اکثر مودم های امروزی از پروتکل های غیرهمزمان استفاده می کنند، که برخی از مهمترین این پروتکل ها عبارتند از Zmodem, Ymodem, Xmodem, Kermit و Blast. پروتکل های غیرهمزمان از پیچیدگی زیادی برخوردار نمی باشند و پیاده سازی آنها نسبتاً ساده و کم خرج می باشد. در این پروتکل ها همان طور که قبلاً اشاره گردید هر بایت ارسالی به همراه بیت شروع، بیت پایان و بیت توازن ارسال می شود. در پروتکل های غیرهمزمان، گیرنده باید شروع و پایان هر بایت را با کمک بیت های شروع و پایان تشخیص دهد.

پروتکل های همزمان از سرعت بسیار بالایی نسبت به پروتکل های غیرهمزمان برخوردار می باشند. بدین علت از این پروتکل ها اغلب در شبکه های محلی، شبکه های شهری و شبکه های گسترده استفاده می شود. پروتکل های همزمان به دو دسته مختلف به نام پروتکل های کاراکتر گرا^۱ و پروتکل های بیت گرا^۲ تقسیم بندی می شوند. تفاوت عمده دو روش فوق، در نحوه همزمانی در کاراکتر و قاب می باشد. پروتکل های کاراکتر گرا برای ارسال حجم زیادی از اطلاعات نظیر فایل های اسکی استفاده می شوند. از آنجایی که در پروتکل های ارسال همزمان، به اول و آخر هر بایت، بیت های شروع و پایان اضافه نمی شود، بنابراین برای نیل به همزمانی کاراکتر و قاب، از کاراکترهای خاصی در اول و آخر قاب برای نشان دادن شروع و پایان هر قاب استفاده می شود. در شکل (۳-۳۹) نمونه ای از پروتکل کاراکتر گرا نشان داده شده است.

ETX	داده	STX	SYN	SYN

شکل (۳-۳۹) : نمونه ای از یک قاب پروتکل کاراکتر گرا

مطابق با شکل فوق، در پروتکل های کاراکتر گرا، در ابتدای قاب از دوبایت SYN برای همزمان سازی گیرنده با شروع قاب ارسالی استفاده می گردد. کاراکتر STX^۳ برای تعیین شروع قاب و کاراکتر ETX^۴ برای مشخص سازی پایان قاب استفاده می شوند. گیرنده با تشخیص کاراکتر SYN، وارد مد شکار شده و منتظر دریافت کاراکتر STX می شود. بعد از تشخیص کاراکتر STX، گیرنده تا دریافت کاراکتر ETX، بایت به بایت اطلاعات موجود در قاب را دریافت می کند. یکی از مشکلات این روش، امکان وجود بایت ETX در قسمت داده قاب می باشد. با توجه به این که اطلاعات موجود در ناحیه داده قاب پروتکل های کاراکتر گرا از لایه های بالاتر دریافت می شود، این امکان وجود دارد که در این ناحیه کاراکتری با کد مشابه با ETX وجود داشته باشد. در این صورت گیرنده آن را با کاراکتر ETX پایان قاب اشتباه تشخیص داده، که موجب عدم تشخیص درست اطلاعات می شود. برای حل این مشکل، مطابق با آنچه که در شکل (۳-۴۰) نشان داده شده است، در ابتدا و انتهای هر قاب، قبل از کاراکترهای کنترلی STX و ETX، از کاراکتر DLE استفاده می گردد. همچنین چنانچه در ناحیه داده های قاب، کاراکتر DLE جزو اطلاعات ارسالی باشد، قبل از آن نیز یک DLE دیگر اضافه می شود. به این روش، میان گذاری بایت^۵ گفته می شود.

ETX	DLE	داده	STX	DLE	SYN	SYN

^۱ Character oriented

^۲ Bit oriented

^۳ Start of Text

^۴ End of Text

^۵ Character stuffing

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

شکل (۳-۴۰) : استفاده از DLE برای عملیات میان گذاری بایت

با توجه به این که در روش کاراکترگرا از عملیات میان گذاری بایت برای جلوگیری از اشتباه گیرنده در تشخیص نادرست انتهای قاب استفاده می شود، این روش برای ارسال فایل های باینری چندان از کارایی بالایی برخوردار نمی باشد. برای حل مشکل فوق، پروتکل های بیت گرا ارائه گردیدند. این پروتکل ها هم برای ارسال فایل های اسکی و هم برای ارسال فایل های باینری مناسب می باشند. در این پروتکل ها شروع و پایان هر قاب، بایک کاراکتر خاص به نام کاراکتر پرچم^۱ مشخص می گردد. در شکل (۳-۴۱) نمونه ای از ساختار قاب در پروتکل های بیت گرا نشان داده شده است.

پرچم پایان	داده	پرچم شروع

شکل (۳-۴۱) : نمونه ای از ساختار قاب در پروتکل های بیت گرا

دلیل نام گذاری این پروتکل به بیت گرا، این است که در این پروتکل رشته بیت دریافتی بیت به بیت برای تشخیص کاراکتر پرچم شروع، کاراکترهای ناحیه داده قاب و پرچم پایان جستجو می گردد. برای کمک به عملیات همزمان سازی درست گیرنده، فرستنده قبل از ارسال قاب، اقدام به ارسال بایت های idle (با کد ۰۱۱۱۱۱۱) می نماید. بعد از تشخیص پرچم شروع، گیرنده اقدام به خواندن هشت بیت به هشت بیت داده ها تا هنگام تشخیص پرچم پایان می نماید. یکی از مهمترین مشکلات این روش، امکان وجود کاراکتر پرچم در بین داده های کاربر می باشد. در این صورت این امکان وجود دارد که گیرنده آن را با پرچم نشان دهنده پایان قاب اشتباه بگیرد. برای حل این مشکل از روش درج صفر استفاده می شود که در ادامه این فصل هنگام توصیف پروتکل HDLC توضیح داده خواهد شد.

دو پروتکل متداول همزمان عبارتند از: پروتکل ارتباط همزمان باینری (BSC^۲) و پروتکل HDLC. پروتکل BSC از نوع کاراکترگرا می باشد و پروتکل HDLC به صورت بیت گرا عمل می نماید.

۳-۱-۱-۳- پروتکل BSC

پروتکل BSC، یکی از متداولترین پروتکل های کاراکترگرا می باشد که در سال ۱۹۶۴ توسط شرکت IBM ارائه گردید. از این پروتکل در اتصالهای نقطه به نقطه و نقطه به چند نقطه می توان استفاده نمود. پروتکل BSC به صورت ارسال یک طرفه عمل می کند و از روش کنترل جریان توقف و انتظار استفاده می نماید. از پروتکل BSC معمولاً برای کاربردهای چند نقطه ای که در آن یک ایستگاه خادم^۳ با چندین ایستگاه مخدوم^۴ در ارتباط است استفاده می شود. در شکل (۳-۴۲) دو نمونه از شبکه گذرگاه مشترک BSC نشان داده شده است.

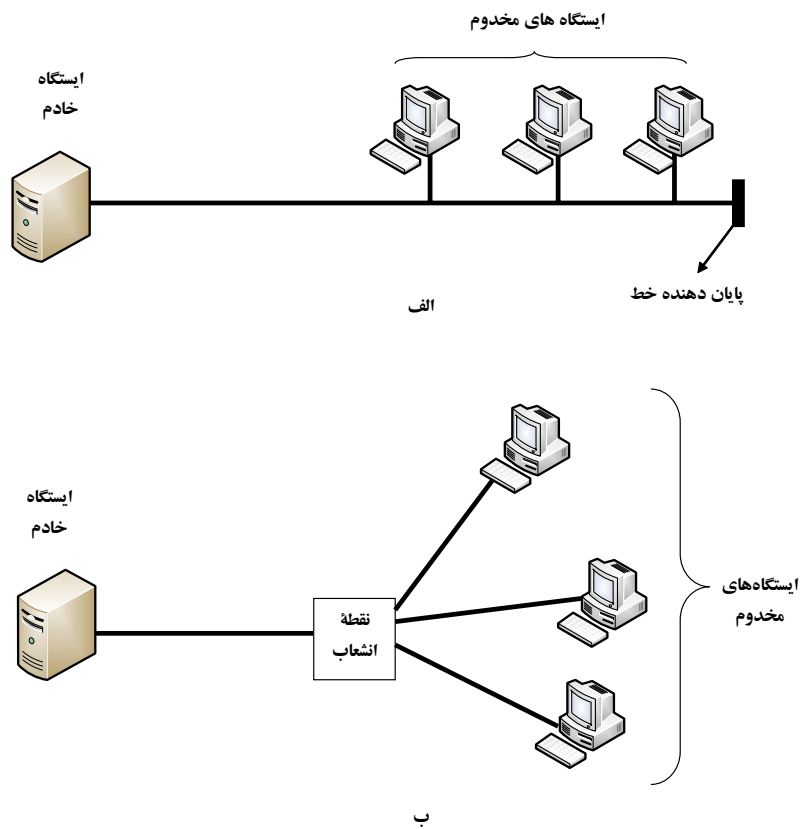
^۱ Flag

^۲ Binary Synchronization Communication

^۳ Master

^۴ Slave

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۳-۴۲): مثالی از شبکه گذرگاه مشترک BSC (الف) اتصال multidrop (ب) اتصال چند نقطه ای

بنابراین باید توجه نمود که پروتکل BSC ارسال دوطرفه و همچنین پروتکل کنترل جریان پنجره لغزان را پشتیبانی نمی کند. در جدول (۳-۵) لیست کاراکترهای کنترلی که در پروتکل BSC استفاده می شود آورده شده است.

جدول (۳-۵): لیست کاراکترهای کنترلی در پروتکل BSC

عملیات	کاراکتر
اعلام دریافت صحیح قاب‌های زوج یا اعلام آمادگی دریافت	ACK0
اعلام دریافت صحیح قاب‌های فرد	ACK1
نشانه شفافیت داده ها	DLE
درخواست پاسخ	ENQ
اعلام خاتمه فرستنده	EOT
اعلام انتهای ارسال بلوک (به پیام تصدیق نیاز دارد)	ETB
نشان دهنده پایان ناحیه متن در پیام	ETX
پایان بلوک میانی درحالت ارسال چندبلوکی	ITB
اعلام دریافت قاب نادرست یا اعلام عدم وجود داده ای برای ارسال	NAK
کاراکتر پرکننده	NUL
پیام اورژانسی از جانب گیرنده	RVI
شروع ناحیه اطلاعات سرآیند	SOH
شروع ناحیه متن	STX
اعلام ورود آتی قاب ها به گیرنده (برای همزمانی گیرنده با فرستنده به کار می رود)	SYN
فرستنده درحالت خاموشی، است اما هنوز خط را واگذار نکرده است	TTD
قاب سالم و خوب دریافت شده است، اما دیگر آمادگی دریافت قاب‌های بیشتری وجود ندارد	WACK

در پروتکل BSC دو نوع قاب وجود دارد که عبارتند از: قاب‌های کنترل و قاب‌های داده. قاب‌های کنترل برای انجام عملیات کنترلی مانند مبادله اطلاعات کنترلی بین تجهیزات ارتباطی به کار می‌روند. به عنوان مثال برای برقراری و قطع اتصال اولیه، کنترل جریان و تصحیح خطا از قاب‌های کنترلی استفاده می‌گردد. از قاب‌های داده برای مبادله اطلاعات کاربران استفاده می‌شود، ولی در مواردی از آنها نیز می‌توان برای تبادل اطلاعات کنترلی استفاده نمود.

در شکل (۳-۴۳) ساختار قاب‌های داده نشان داده شده است. مطابق با شکل فوق هر قاب، با دو یا چند کاراکتر همزمانی (SYN) شروع می‌شود. از کاراکترهای همزمانی برای اعلام ورود قاب جدید استفاده می‌گردد. بعد از دو کاراکتر همزمانی در قاب‌های داده یک کاراکتر شروع متن (STX) استفاده می‌شود. این کاراکتر نشان دهنده پایان ناحیه کنترلی و شروع ناحیه داده می‌باشد. ناحیه داده می‌تواند دارای هر طول متغیری باشد که در پایان این ناحیه از کاراکتر پایان متن (ETX) استفاده می‌گردد. در انتهای قاب داده یک یا دو بایت شمارش بررسی صحت بلوک (BCC) وجود دارد. از BCC برای کنترل خطا در قاب ارسالی استفاده می‌شود. ناحیه سرآیند شامل آدرس فرستنده و گیرنده و شماره قاب ارسالی است.

SYN	SYN	STX	داده	ETX	BCC

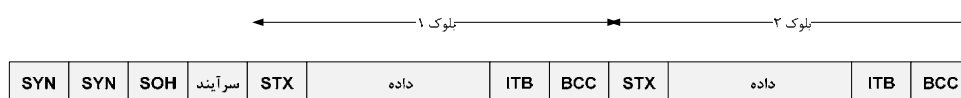
شکل (۳-۴۳): ساختار قاب‌های داده در پروتکل BSC

احتمال خرابی متن داخل یک بلوک اطلاعاتی با افزایش طول متن، زیاد می‌شود. بدین علت می‌توان متن موجود در پیام ارسالی را به

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

چندین بلوک کوچکتر تقسیم بندی نمود. هر بلوک به جز آخرین آن، با کاراکتر STX شروع می شود و با کاراکتر بلوک متنی میانی (ITB) خاتمه می یابد. آخرین بلوک با STX شروع می شود و با ETX خاتمه می یابد. بعد از هر ITB یا ETX فیلد BCC قرار دارد.

گیرنده با استفاده از فیلد BCC، وقوع خطای احتمالی را در هر بلوک بررسی می نماید. چنانچه در یکی از بلوک های قاب خطایی مشاهده شود، فرستنده باید کل قاب ارسالی را دوباره ارسال کند. در شکل (۳-۴۴) ساختار قاب های چند بلوکه نشان داده شده است.



شکل (۳-۴۴): ساختار قاب های چند بلوکه در پروتکل BSC

با توجه به این که پروتکل BSC از روش یک طرفه استفاده می کند، بعد از پایان ارسال قاب، کنترل کانال از فرستنده به گیرنده منتقل می شود. چنانچه پیام ارسالی بسیار طولانی باشد به طوری که در داخل یک قاب به تنهایی گنجانده نشود، می توان پیام ارسالی را به چندین قاب کوچکتر تجزیه نمود و آنها را ارسال کرد. همان طور که اشاره گردید از قاب های کنترلی برای تبادل اطلاعات کنترلی نظیر برقراری و حذف ارتباط، کنترل جریان و کنترل خطا بین دو طرف ارتباط استفاده می شود. در شکل (۳-۴۵) ساختار قاب های کنترلی در BSC نشان داده شده است.

SYN	SYN	سایر کاراکترهای کنترلی	BCC

شکل (۳-۴۵): ساختار قاب های کنترلی در پروتکل BSC

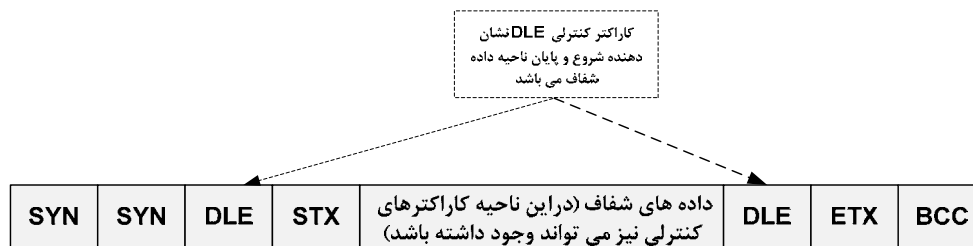
۳-۱-۱-۲- شفافیت داده ها^۱

در ابتدا از پروتکل BSC برای تبادل داده های متنی استفاده می گردید. امروزه در بسیاری از کاربردها، داده های ارسالی از نوع باینری می باشند. چنانچه داده های ارسالی باینری باشند، این احتمال وجود دارد که یک یا چند بیت در داده های ارسالی مطابق با کاراکترهای کنترلی BSC باشند. در این حالت گیرنده در تشخیص و جدا سازی کاراکترهای کنترلی با کاراکترهای داده دچار اشتباه می شود. به عنوان مثال چنانچه در رشته بیت ارسالی فرستنده بیت ۰۰۰۰۰۰۰۱ قرار داشته باشد، گیرنده آن را با کاراکتر کنترلی ETX اشتباه خواهد گرفت. از طرفی دیگر یک پروتکل خوب و موفق باید به صورت شفاف عمل کند و هیچ گونه محدودیتی در رشته بیت ارسالی وضع ننماید. بدین منظور همان طور که قبلاً توضیح داده شد، برای حفظ شفافیت داده های ارسالی در BSC از روش میان گذاری بیت استفاده می شود. در این روش چنانچه در داده های ارسالی بیت های کنترلی موجود باشد، قبل از کاراکتر STX و ETX دو کاراکتر کنترلی DLE قرار داده می شود. گیرنده با مشاهده اولین کاراکتر DLE متوجه می شود که در داده های ارسالی بیت های کنترلی وجود دارد و بدین ترتیب تا دریافت دومین

^۱Data transparency

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

کاراکتر DLE از تمام بایت های کنترلی دریافتی صرف نظر می کند. در شکل (۳-۴۶) نمونه ای از عملیات میان گذاری بایت نشان داده شده است.



شکل (۳-۴۶) : عملیات میان گذاری بایت در پروتکل BSC

۳-۱-۲ - پروتکل HDLC

در پروتکل های کاراکتر گرا بیت های ارسالی به صورت الگوهای از قبل تعریف شده گروه بندی می شوند و تشکیل کاراکتر می دهند. در مقایسه با پروتکل های کاراکتر گرا، پروتکل های بیت گرا قادر به گنجاندن اطلاعات بیشتر در قاب های کوتاه تر و اجتناب از مشکل شفافیت داده می باشند. در طی چند سال گذشته پروتکل های بیت گرای متعددی ارائه شده است که از میان آنها می توان به پروتکل های SDLC، HDLC، پروتکل های LAP و پروتکل های شبکه های محلی اشاره نمود. اغلب پروتکل های بیت گرا توسط شرکت های خصوصی جهت پشتیبانی از محصولات آنها ارائه شده است.

یکی از مهمترین پروتکل های بیت گرا، HDLC می باشد که توسط سازمان ISO طراحی گردیده است و به عنوان پایه اغلب پروتکل های بیت گرای امروزی شناخته می شود. در سال ۱۹۷۵ شرکت IBM پروتکل SDLC را به سازمان ISO ارائه داد و درخواست تایید استاندارد ISO را نمود. ۴ سال بعد در سال ۱۹۷۹ سازمان جهانی ISO پروتکل HDLC را که بر پایه پروتکل SDLC می باشد تایید کرد. با تایید استاندارد HDLC توسط ISO، سایر مراجع استاندارد گذاری نظیر ITU-T اقدام به تصویب پروتکل هایی نظیر پروتکل های LAP (LAPB، LAPD، LAPM و LAPX) نمودند. تمامی این پروتکل ها توسعه یافته پروتکل HDLC می باشند. همچنین پروتکل های Frame relay و PPP که توسط ITU-T و ANSI توسعه یافتند، بر اساس HDLC طراحی شده اند. بنابراین با توجه به اهمیت HDLC به بررسی این پروتکل می پردازیم.

پروتکل استاندارد HDLC، یک پروتکل اتصال گرا می باشد که قادر به عملکرد یک طرفه و دو طرفه بر روی خطوط نقطه به نقطه و چند نقطه می باشد. ایستگاه ها در پروتکل HDLC، به سه دسته اولیه^۱ ثانویه^۲ و ترکیبی^۳ تقسیم بندی می شوند. ایستگاه اولیه در HDLC اقدام به ارسال پیام های دستور به ایستگاه های ثانویه می نماید. ایستگاه های ثانویه نیز در جواب به پیام دستور اقدام به ارسال پیام پاسخ می نمایند. به عنوان مثال ارتباط کامپیوتر با پایانه، نمونه ای از ارتباط ایستگاه اولیه به ایستگاه ثانویه در HDLC می باشد. ایستگاه ترکیبی قادر به ارسال پیام های دستور و پاسخ های آنها نیز می باشد.

بر اساس جهت مبادله اطلاعات، ایستگاه های ترکیبی در HDLC می توانند هم به صورت ایستگاه اولیه و هم به صورت ایستگاه ثانویه عمل نمایند. در HDLC ایستگاه های اولیه، ثانویه و ترکیبی به سه صورت مختلف پیکره بندی می شود این سه ترکیب مختلف عبارتند از غیر بالانس، متقارن و بالانس. در شکل (۳-۴۷) این سه نوع پیکره بندی HDLC نشان داده شده

^۱ Primary
^۲ Secondary
^۳ Combined

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

است. در پیکره بندی غیربالانس که به پیکره بندی خدمات دهنده/ خدمات گیرنده نیز نامیده می شود، یک ایستگاه به صورت اولیه و سایر ایستگاه ها به صورت ثانویه عمل می نمایند. پیکره بندی غیربالانس هم به صورت نقطه به نقطه و هم به صورت نقطه به چند نقطه عمل می کند.

در پیکره بندی متقارن، هر ایستگاه فیزیکی به طور منطقی از دو ایستگاه اولیه و ثانویه تشکیل شده است. کانال های مجزایی ایستگاه های اولیه و ثانویه را به یکدیگر متصل می نمایند. این نوع پیکره بندی مشابه پیکره بندی غیربالانس می باشد. با این تفاوت که کنترل کانال و جهت ارسال پیام های دستور و پاسخ می تواند بین دو ایستگاه فیزیکی تغییر نماید. در پیکره بندی بالانس هر دو ایستگاه در اتصال های نقطه به نقطه از نوع ایستگاه ترکیبی می باشند. برخلاف پیکره بندی متقارن در این نوع پیکره بندی فقط از یک کانال برای اتصال ایستگاه ها استفاده می شود. جهت ارسال پیام در کانال توسط هر دو ایستگاه قابل کنترل می باشد. پروتکل HDLC قادر به پشتیبانی از پیکره بندی بالانس چند نقطه ای نمی باشد، ولی سایر انواع پیکره بندی که اشاره گردید توسط HDLC پشتیبانی می شود. برای کنترل کانال در HDLC سه مد ارتباطی متفاوت بین ایستگاه ها وجود دارند که عبارتند از:

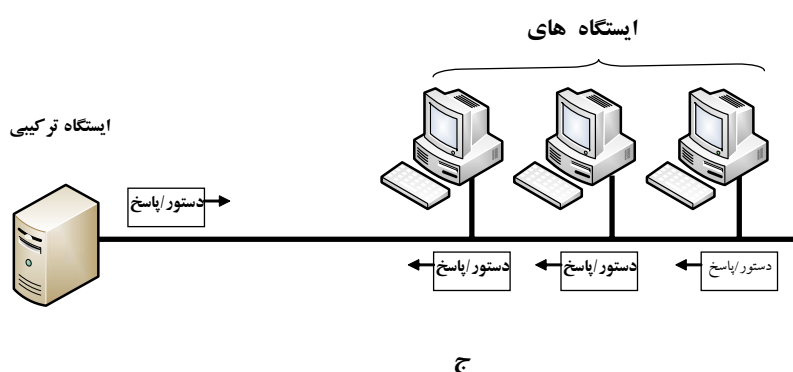
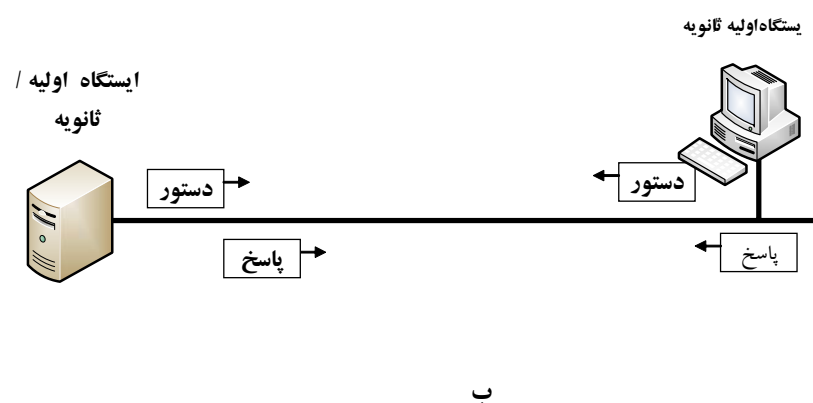
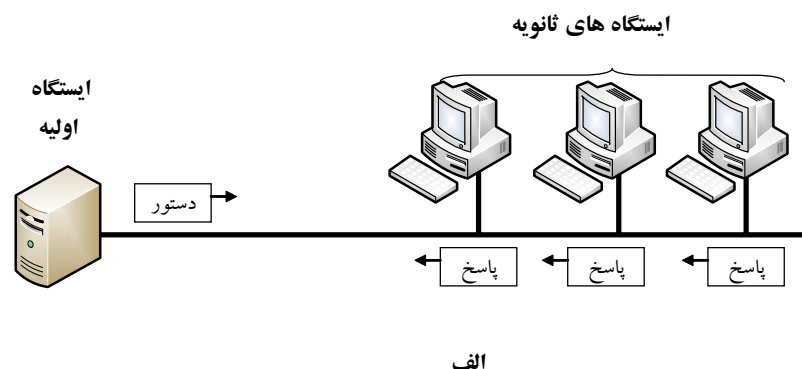
- مد پاسخ طبیعی (NRM^1)
- مد پاسخ غیرهمزمان (ARM^2)
- مد بالانس شده غیرهمزمان (ABM^3)

¹ Normal Response Mode

² Asynchronous Response Mode

³ Asynchronous Balance Mode

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۳-۴۷): انواع پیکره بندی در پروتکل HDLC

(الف) غیربالانس (ب) متقارن (ج) بالانس

- **NRM**: این مدل ارتباطی در پیکره بندی غیربالانس به کار می رود. در این مدل، ایستگاه ثانویه برای ارسال اطلاعات، باید از قبل اجازه ارسال را از ایستگاه اولیه کسب نماید و پس از کسب مجوز، ایستگاه ثانویه قادر به ارسال یک یا چندین قاب پاسخ حاوی اطلاعات می باشد. از کانال های نقطه به نقطه و یا چند نقطه در این مدل ارتباطی استفاده می شود.
- **ARM**: این مدل ارتباطی در پیکره بندی غیربالانس به کار می رود. در این مدل، ایستگاه ثانویه هنگامی که کانال خالی می باشد، قادر به ارسال اطلاعات بدون مجوز از ایستگاه اولیه است. در این حالت تمام اطلاعات ارسالی ایستگاه های ثانویه، حتی بین خودشان باید از طریق ایستگاه اولیه عبور داده شود. در این مدل ارتباطی از کانال های دوطرفه نقطه به نقطه استفاده می شود.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

- **ABM:** در مد ABM تمام ایستگاه ها یکسان می باشند و بنابراین ایستگاه های ترکیبی که به صورت نقطه به نقطه به یکدیگر متصل شده اند، استفاده می شوند. هر کدام از ایستگاه های ترکیبی بدون نیاز به کسب مجوز قادر به ارسال می باشند. در این مدل ارتباطی از کانال های دوطرفه نقطه به نقطه استفاده می شود. در جدول (۳-۶) ارتباط بین مدهای فوق و انواع ایستگاه های HDLC نشان داده شده است.

جدول (۳-۶): مدهای مختلف HDLC و ارتباط بین آنها

ABM	ARM	NRM	
ترکیبی	اولیه و ثانویه	اولیه و ثانویه	نوع ایستگاه
هر کدام	اولیه	یکی از دو ایستگاه اولیه/ثانویه	آغاز کننده

۳-۱-۲-۱-۱-۱ HDLC

جهت فراهم سازی انعطاف پذیری لازم برای پشتیبانی انواع مدهای HDLC، سه نوع قاب به نامهای قاب های اطلاعاتی، قاب های نظارتی و قاب های بدون شماره وجود دارد. در شکل (۳-۴۸) انواع قاب های HDLC نشان داده شده است. از قاب های اطلاعاتی برای ارسال داده های کاربر و اطلاعات کنترلی مربوط به داده های کاربر استفاده می شود. از قاب های نظارتی برای مبادله اطلاعات کنترلی، کنترل جریان و کنترل خطا استفاده می گردد. قاب های بدون شماره برای مدیریت سیستم به کار می روند.

پرچم	FCS	داده های کاربر	کنترل	آدرس	پرچم

(الف)

پرچم	FCS	کنترل	آدرس	پرچم

(ب)

پرچم	FCS	اطلاعات مدیریت شبکه	کنترل	آدرس	پرچم

(ج)

شکل (۳-۴۸): انواع قاب ها در پروتکل HDLC

الف) قاب های اطلاعاتی (ب) قاب های نظارتی (ج) قاب های بدون شماره

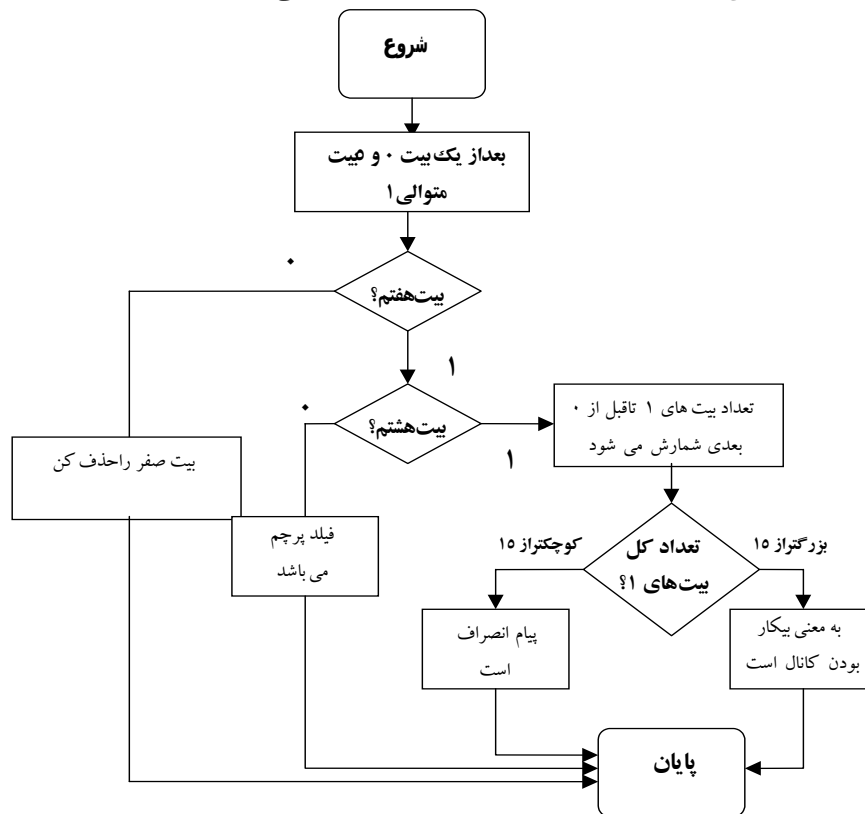
همان طور که در شکل ۳-۴۸ دیده می شود قاب های HDLC از فیلدهای زیر تشکیل شده اند:

- **فیلد پرچم:** فیلد پرچم در HDLC، که شامل رشته بیتی ۰۱۱۱۱۱۱۰ می باشد، شروع و پایان قاب را مشخص می کند و برای همزمانی فرستنده با گیرنده استفاده می شود. برای تضمین عدم وجود فیلد پرچم در بخش داده قاب های HDLC، از عملیات درج صفر استفاده می شود. در سمت فرستنده، بعد از هر ۵ بیت ۱ متوالی یک بیت ۰ اضافه می گردد. به عنوان مثال رشته بیت ۰۱۰۱۱۱۱۱۰۱۰ تبدیل به رشته بیت ۰۱۰۱۱۱۱۱۰۱۰۱۰ می شود. در سمت گیرنده نیز ۰ بعد از ۵ بیت ۱ حذف می شود. در شکل (۳-۴۹)

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

فلوچارت عملیات درج صفر درست گیرنده HDLC نشان داده شده است.

- فیلد آدرس: دومین فیلد در قاب های HDLC، مشخص کننده آدرس ایستگاه که می تواند ایستگاه اولیه یا ایستگاه ثانویه باشد، است. درحالتی که فرستنده قاب، ایستگاه اولیه باشد، فیلد آدرس مشخص کننده آدرس ایستگاه ثانویه که باید پیام را دریافت نماید، است؛ ولی درحالتی که ایستگاه ثانویه فرستنده قاب است، فیلد آدرس، مشخص کننده آدرس ایستگاه ثانویه که فرستنده قاب است، می باشد.



شکل (۳-۴۹): فلوچارت درج بیت صفر درست گیرنده HDLC

- **فیلد کنترل:** از این فیلد که دارای یک یا دو بایت است، برای مدیریت جریان ترافیکی استفاده می شود. بر اساس نوع قاب، محتویات فیلد کنترل متفاوت است. چنانچه اولین بیت فیلد کنترل صفر باشد، قاب از نوع اطلاعاتی است. در صورتی که دو بیت اول فیلد کنترل ۱۰ باشند، قاب از نوع نظارتی می باشد و چنانچه دو بیت اول در فیلد کنترل ۱۱ باشند، قاب از نوع بدون شماره می باشد. فیلد کنترل در هر سه نوع قاب HDLC، شامل بیتی به نام بیت P/F^1 می باشد. این بیت برای دو منظور متفاوت استفاده می شود و در صورتی معتبر است که مقدار آن ۱ باشد. هنگامی که قاب از سمت ایستگاه اولیه به سمت ایستگاه ثانویه ارسال می گردد، این بیت مفهوم سرکشی می دهد و در صورتی که قاب از سمت ثانویه به اولیه ارسال شود، مفهوم آن پایان است. فیلد کنترل در قاب های اطلاعاتی شامل دو فیلد سه بیتی $N(S)$

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

و $N(R)$ می باشد. این دو فیلد برای کنترل جریان استفاده می شوند. $N(S)$ نشان دهنده شماره قاب ارسالی و $N(R)$ نشان دهنده شماره قابی که ایستگاه، انتظار دریافت آن را از طرف مقابل دارد، می باشد. با توجه به این که در قاب های نظارتی، هیچ گونه داده ای مبادله نمی شود، بنابراین فیلد کنترل در قاب های نظارتی فقط حاوی فیلد $N(R)$ می باشد. در قاب های نظارتی فیلد کنترل شامل دو بیت فیلد کد نیز می باشند که از این دو بیت برای حمل اطلاعات کنترل خطا استفاده می شود. قاب های بدون شماره نه حاوی $N(S)$ و نه حاوی $N(R)$ می باشند بنابراین از آنها نه برای ارسال داده و نه برای ارسال پیام تصدیق استفاده می شود. در عوض قاب های بدون شماره حاوی دو فیلد دو بیتی و سه بیتی به عنوان کد می باشند که از آنها برای مشخص نمودن نوع قاب بدون شماره و عملیات آن استفاده می شود.

- **فیلد اطلاعات:** یکی دیگر از فیلدهای موجود در قاب های HDLC، فیلد اطلاعات می باشد که برای حمل داده های کاربر در قاب های اطلاعاتی و داده های مدیریت شبکه در قاب های بدون شماره استفاده می شود. طول فیلد اطلاعات در شبکه های مختلف، متغیر می باشد ولی معمولاً در هر شبکه طول این فیلد ثابت است. باید توجه نمود که قاب های نظارتی شامل هیچ گونه فیلد اطلاعاتی نمی باشند.
- **فیلد کنترل ترتیب قاب (FCS):** از این فیلد دو یا چهار بیتی به منظور تشخیص خطا در قاب های HDLC استفاده می شود.

۳-۲-۲- انواع قاب های HDLC

همان طور که اشاره شد HDLC دارای سه نوع قاب اطلاعاتی، نظارتی و بدون شماره می باشد. از قاب های نظارتی برای ارسال پیام تصدیق، کنترل جریان و کنترل خطا استفاده می گردد. نوع هر قاب نظارتی توسط دو بیت کد مشخص می شود. در جدول (۳-۷) انواع قاب های نظارتی آورده شده اند.

جدول (۳-۷): انواع قاب های نظارتی در HDLC

قاب	کد	عملیات
RR	۰۰	آمادگی دریافت
REJ	۰۱	رد
RNR	۱۰	عدم آمادگی دریافت
SREJ	۱۱	رد انتخابی

مطابق با جدول ۳-۷ انواع قاب های نظارتی در HDLC عبارتند از:

- **قاب RR:** از این قاب برای چهار عمل متفاوت استفاده می شود که عبارتند از:

الف) تصدیق: هنگامی که گیرنده هیچ داده ای برای ارسال نداشته باشد، برای تصدیق دریافت سالم قاب های ورودی از این قاب استفاده می کند. در این حالت فیلد $N(R)$ در قسمت کنترل قاب نشان دهنده شماره قاب بعدی که گیرنده منتظر دریافت آن است می باشد.

ب) سرکشی: هنگامی که ایستگاه اولیه اقدام به ارسال قاب RR که در آن بیت P/F برابر ۱ است می کند عملاً از ایستگاه ثانویه سؤال می نماید که آیا داده ای برای ارسال دارد یا خیر؟

ج) پاسخ منفی به سرکشی: هنگامی که قاب RR توسط ایستگاه ثانویه با بیت P/F مساوی ۱ ارسال شود، به وسیله آن ایستگاه ثانویه به ایستگاه اولیه اعلام می دارد که هیچ داده ای برای ارسال ندارد.

د) پاسخ مثبت به انتخاب: هنگامی که ایستگاه ثانویه قادر به دریافت اطلاعات از ایستگاه اولیه باشد، یک قاب RR

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

که در آن بیت P/F ، ۱ است ارسال می دارد.

- **قاب RNR :** از این قاب ها برای سه منظور متفاوت به صورت زیر استفاده می شود:

الف) تصدیق: چنانچه قاب RNR توسط گیرنده برای ایستگاه فرستنده ارسال شود، در این صورت دریافت سالم تمام قاب ها تا قبل از $N(R)$ اعلام می شود. همچنین از فرستنده درخواست می شود که ارسال را متوقف نموده تا این که دوباره گیرنده برای فرستنده یک قاب RR ارسال دارد.

ب) انتخاب: هنگامی که ایستگاه اولیه بخواهد داده ای را برای ایستگاه ثانویه ارسال دارد با ارسال یک قاب RNR که بیت P/F آن ۱ می باشد، ایستگاه ثانویه را مطلع می سازد. با ارسال این قاب عملاً به ایستگاه ثانویه گفته می شود که داده های خود را برای ایستگاه اولیه ارسال نکند.

ج) پاسخ منفی به انتخاب: هنگامی که یک ایستگاه ثانویه انتخاب شده، قادر به دریافت اطلاعات نباشد، یک قاب RNR که در آن بیت P/F ، ۱ است برای ایستگاه اولیه ارسال می دارد.

- **قاب REJ :** سومین نوع قاب های نظارتی قاب REJ می باشد. گیرنده هنگامی که هیچ داده ای برای ارسال نداشته

باشد، از این قاب به عنوان یک پیام تصدیق منفی در حالت کنترل خطا به صورت بازگشت به عقب به اندازه N استفاده می کند. در این قاب، $N(R)$ نشان دهنده شماره فیلد معیوب است که فرستنده از آن به بعد را باید دوباره برای گیرنده ارسال دارد.

- **قاب $SREJ$:** از این قاب به عنوان یک پیام تصدیق منفی در روش کنترل خطا به صورت رد انتخابی استفاده

می شود. این قاب توسط گیرنده به فرستنده ارسال می شود و نشان دهنده این است که یک قاب مشخص که شماره آن در فیلد $N(R)$ معلوم شده است با خطا دریافت گردیده و باید دوباره ارسال گردد.

قاب های بدون شماره

از این قاب ها برای مبادله اطلاعات مدیریت جلسه و اطلاعات کنترلی بین ایستگاه ها استفاده می شود. برخلاف قاب های نظارتی، قاب های بدون شماره، حاوی فیلد اطلاعات می باشند؛ اما از این اطلاعات فقط برای مدیریت سیستم استفاده می شود و هیچ گونه داده کاربر در آن وجود ندارد. انواع قاب های بدون شماره توسط فیلدهای ۵ بیتی کد مشخص می شود. حداکثر می توان ۳۲ قاب بدون شماره مشخص نمود. از این قاب ها برای عملیاتی نظیر تنظیم مد، مبادله بدون شماره، قطع اتصال، مقدار دهی اولیه و سایر موارد دیگر استفاده می شود. در جدول (۳-۸) انواع قاب های بدون شماره آورده شده است.

در شکل (۳-۵) مثالی از ارتباط همتا به همتا بین دو ایستگاه A و B با استفاده از پروتکل HDLC آورده شده است. مطابق با این شکل، ابتدا ایستگاه A برای برقراری ارتباط در حالت بالانس غیرهمزمان (ABM) یک قاب بدون شماره ($SABM$) برای ایستگاه B ارسال می دارد. در قاب ارسالی بیت P برابر ۱ می باشد که نشان دهنده این است که ایستگاه A خواهان کنترل جلسه و ارسال زودتر است. در پاسخ، ایستگاه B با ارسال قاب بدون شماره از نوع UA که بیت F آن ۱ می باشد، درخواست A را می پذیرد. از آنجایی که با توافق دو طرف حالت ارسال به صورت بالانس غیرهمزمان است، بنابراین هر دو ایستگاه از نوع ترکیبی می باشند و بیت P/F اعتبار خود را از دست می دهد. بعد از تنظیم حالت ارتباط، دوا ایستگاه برای یکدیگر قاب های اطلاعاتی ارسال می دارند.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

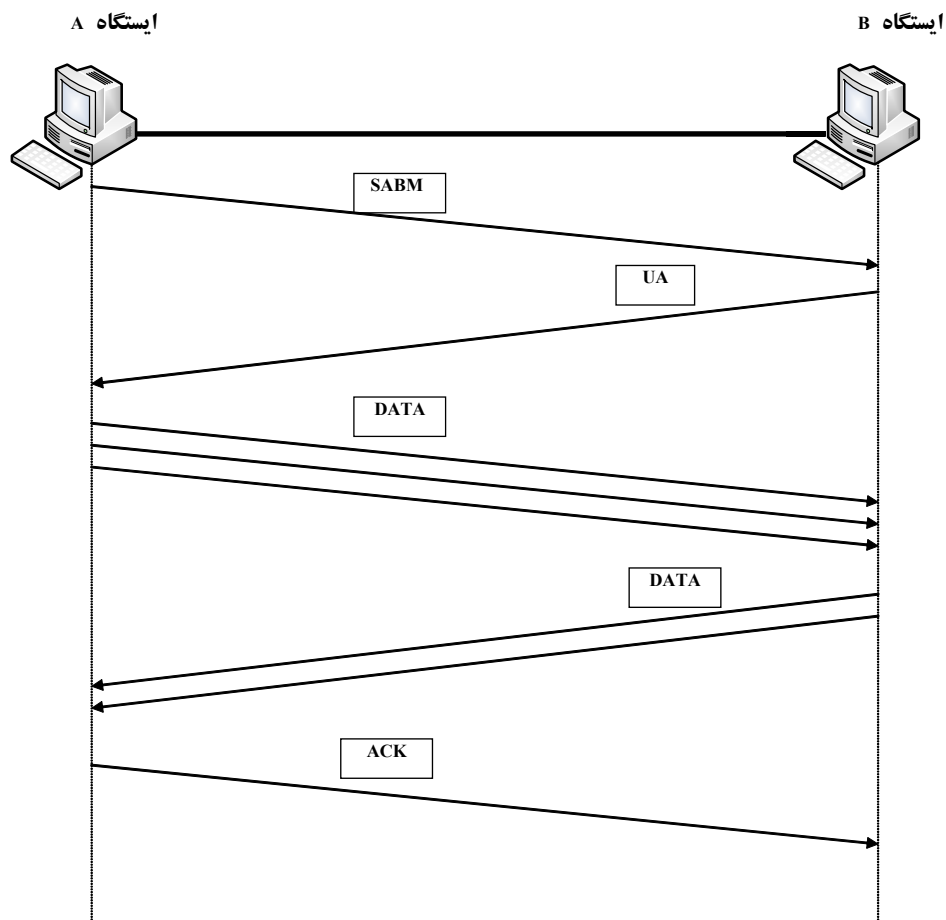
جدول (۳-۸): پیام های دستور و پاسخ قاب های بدون شماره

دستور/ پاسخ	عملیات
SNRM	تنظیم حالت NRM
SNRME	تنظیم حالت NRM (توسعه یافته)
SARM	تنظیم حالت ARM
SARME	تنظیم حالت ARM (توسعه یافته)
SABM	تنظیم حالت ABM
SABME	تنظیم حالت ABM (توسعه یافته)
UP	سرکشی بدون شماره
UI	اطلاعات بدون شماره
UA	پیام تصدیق بدون شماره
RD	درخواست قطع ارتباط
DISC	قطع ارتباط
DM	حالت قطع
RIM	درخواست حالت اطلاعات
SIM	تنظیم حالت آماده سازی اولیه
RSET	آغاز دوباره

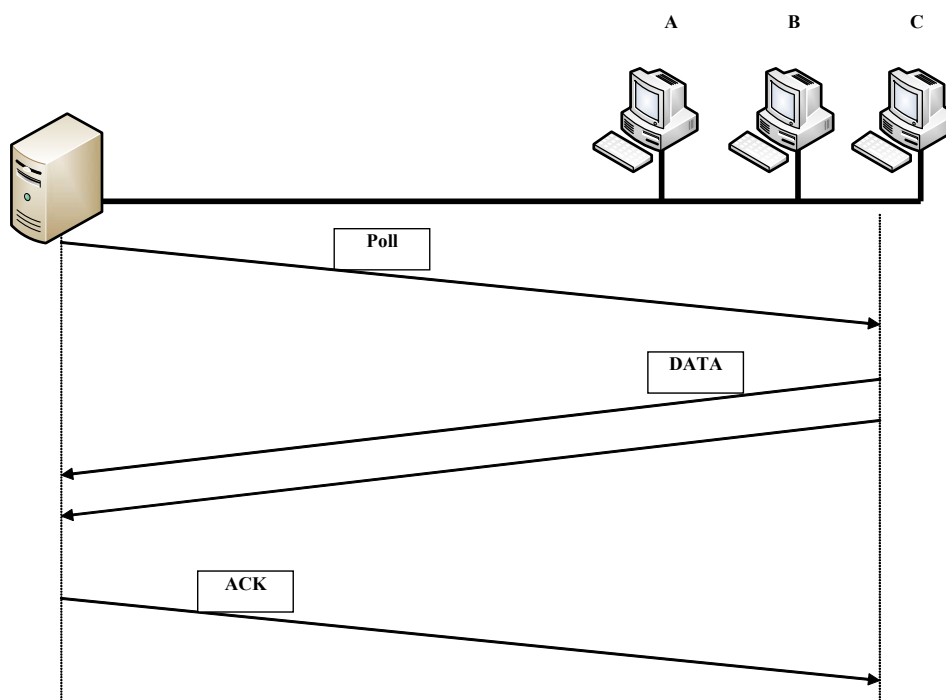
در شکل (۳-۵۱) یک ارتباط نقطه به چند نقطه نشان داده شده است که در آن یک ایستگاه اولیه به چندین ایستگاه ثانویه متصل شده است.

ایستگاه اولیه با ارسال یک قاب نظارتی از نوع سرکشی به مقصد ایستگاه A ، از آن می خواهد که داده های خود را ارسال دارد. ایستگاه A دو قاب به شماره های ۰ و ۱ برای ایستگاه اولیه ارسال می کند. در آخرین قاب ارسالی بیت F مساوی ۱ می باشد که نشان دهنده پایان ارسال اطلاعات است. ایستگاه اولیه با ارسال یک قاب نظارتی از نوع RNR به ایستگاه A اعلام می دارد که قاب های شماره ۰ و ۱ آن را دریافت نموده است.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۳-۵۰): مثالی از برقراری ارتباط همتا به همتا در حالت ABM در HDLC



شکل (۳-۵۱): مثالی از عملیات سرکشی در اتصالات نقطه به چند نقطه در HDLC

پرسش های فصل

۱. وظایف اصلی لایه پیوند داده را نام برده و توصیف نمایید.
۲. روش توقف و انتظار را توضیح دهید.
۳. علت استفاده از زمان سنج در روش توقف و انتظار توضیح دهید.
۴. معایب و مزایای روش توقف و انتظار را بنویسید.
۵. روش پنجره لغزان را با ذکر مثالی توصیف نمایید.
۶. تفاوت روش های بازگشت به عقب به اندازه N و روش تکرار انتخابی را توضیح دهید.
۷. علت استفاده از زمان سنج برای هر قاب در روش پنجره لغزان را بنویسید.
۸. برتری و نقاط ضعف روش پنجره لغزان را نسبت به روش توقف و انتظار تشریح نمایید.
۹. وظیفه زیر لایه کنترل دسترسی به محیط (MAC) را در شبکه های محلی بنویسید.
۱۰. انواع روش های کنترل دسترسی به محیط را نام برده و هریک را توضیح دهید.
۱۱. ویژگی های روش ALOHA را توصیف نمایید.
۱۲. تفاوت روش ALOHA خالص با روش ALOHA اسلات بندی شده توضیح دهید.
۱۳. نحوه عملکرد روش سرکشی را توصیف نمایید.
۱۴. تفاوت روش سرکشی چرخشی و سرکشی هاب را بنویسید.
۱۵. عملکرد پروتکل CSMA صد درصد متمرکز، درصد متمرکز و غیرمتمرکز را توضیح داده و بایکدیگرمقایسه نمایید.
۱۶. در پروتکل CSMA P، درصد متمرکز با افزایش مقدار P، نحوه تغییرات میزان تداخل و بهره وری از کانال را توضیح دهید.
۱۷. عملکرد پروتکل CSMA/CD و تفاوت آن را با CSMA توضیح دهید.
۱۸. سه وضعیت کاری پروتکل CSMA/CD را نام برده و توضیح دهید.
۱۹. استانداردهای IEEE برای شبکه های محلی را نام ببرید.
۲۰. عملکرد شبکه اترنت سخت و اجزای آن را توضیح دهید.
۲۱. عملکرد شبکه اترنت نرم و اجزای آن را توضیح دهید.
۲۲. نحوه تشخیص محل قطعی کابل را در اترنت توضیح دهید.
۲۳. عملکرد شبکه های 100BaseT را توضیح داده و برتری های آن را نسبت به اترنت معمولی تشریح نمایید.
۲۴. کاربرد کابل AUI در شبکه های اترنت سخت را توضیح داده و تعداد زوج سیم های آن و عملکرد هر زوج سیم را توصیف کنید.
۲۵. وظایف کارت شبکه (NIC) را در شبکه های اترنت توضیح دهید.
۲۶. نحوه گسترش شبکه های اترنت را با استفاده از تکرارکننده ها توضیح دهید.
۲۷. برتری شبکه اترنت ستاره ای را نسبت به شبکه اترنت نرم و سخت توصیف کنید.
۲۸. ساختار قاب های زیر لایه MAC اترنت را نوشته و عملکرد هر فیلد آن را توصیف نمایید.
۲۹. الگوریتم عقب گرد توانی دودوئی در اترنت را تشریح نمایید.
۳۰. برتری و جنبه های تمایز اترنت سریع را با اترنت پایه توصیف نمایید.
۳۱. وظایف زیر لایه های CS و PMD را در اترنت سریع بنویسید.
۳۲. انواع استانداردهای اترنت سریع را توصیف نمایید.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

۳۳. استانداردهای مختلف گیگا بیت اترنت را نوشته و بایکدیگر مقایسه نمایید.
۳۴. کاربردهای فن آوری ۱۰ گیگابیت اترنت را توصیف نمایید.
۳۵. برتری عمده شبکه گذرگاه نشانه نسبت به شبکه اترنت را توضیح دهید.
۳۶. نحوه تشکیل حلقه منطقی و ارسال داده را در شبکه های گذرگاه نشانه توصیف نمایید.
۳۷. کلاس های ترافیکی مختلف شبکه های گذرگاه نشانه و کاربرد هر کلاس ترافیکی را توصیف نمایید.
۳۸. کاربرد زمان سنجهای THT و HP-THT را در شبکه گذرگاه نشانه توصیف کنید.
۳۹. تفاوت اساسی که در ساختار قاب های MAC استاندارد اترنت و گذرگاه نشانه وجود دارد، را ذکر نمایید.
۴۰. عملکرد جعبه تقسیم و علت استفاده از آن را در شبکه های حلقه نشانه توصیف نمایید.
۴۱. عملکرد ایستگاه ناظر را در شبکه های حلقه نشانه توصیف نمایید.
۴۲. کاربرد فیلد وضعیت در ساختار قاب های MAC شبکه های حلقه نشانه را بنویسید.
۴۳. عملکرد ایستگاه های پایین جریان، بالا جریان و سر را در شبکه های DQDB توصیف نمایید.
۴۴. نحوه عملیات رزرو برش زمانی را در شبکه های DQDB توصیف کنید.
۴۵. عملکرد فیلد دسترسی را در ساختار قاب های DQDB تشریح نمایید.
۴۶. ساختار شبکه های SMDS را توصیف نمایید.
۴۷. رجیسترهای FDDI را نام برده و کاربرد هر رجیستر را تشریح نمایید.
۴۸. کاربرد زمان سنجهای FDDI را توصیف نمایید.
۴۹. وظایف زیرلایه های PHY و PMD را در شبکه های FDDI تشریح نمایید.
۵۰. عملکرد ایستگاه های DAC، DAS و SAS را در شبکه های FDDI تشریح نمایید.
۵۱. تفاوت پروتکل های کاراکترگرا و بیت گرا را بایکدیگر بنویسید.
۵۲. نحوه عملیات میان گذاری بایت را در پروتکل BSC توصیف نمایید.
۵۳. قاب های مختلف پروتکل BSC را نام برده و بایکدیگر مقایسه نمایید.
۵۴. ایستگاه های اولیه، ثانویه و ترکیبی را در HDLC توصیف نموده تفاوت آنها را با یکدیگر بنویسید.
۵۵. سه مد کاری پاسخ طبیعی (NRM)، پاسخ غیرهمزمان (ARM) و مد با لانس شده غیرهمزمان (ABM) را در HDLC با یکدیگر مقایسه نمایید.
۵۶. انواع قاب های HDLC را نام برده و عملکرد هریک را توصیف نمایید.
۵۷. نحوه عملیات درج صفر را در پروتکل HDLC توصیف کنید.

فصل چهارم

شبکه های بیسیم

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

فن آوری کامپیوتر در چند سال اخیر در زمینه های مختلفی نظیر حجم و قدرت پردازش اطلاعات، ابعاد فیزیکی قطعات کامپیوتر و کاهش قیمت محصولات کامپیوتر، پیشرفت سریعی داشته است. یکی از جنبه های پیشرفت سیستم های کامپیوتر، قابلیت حمل^۱ آنها می باشد. امروزه با استفاده از کامپیوترهای کیفی، کاربران می توانند در هر نقطه از دنیا به آخرین اطلاعات دسترسی داشته باشند.

یکی از دستاوردهای جدید در شبکه های کامپیوتری، پیدایش شبکه های محلی بیسیم است. شبکه محلی بیسیم، یک سیستم ارتباطی انعطاف پذیر می باشد که به عنوان یک جایگزین توسعه یافته برای شبکه های محلی با سیم در نظر گرفته می شود. با استفاده از فن آوری هایی نظیر امواج رادیویی، امواج مادون قرمز و امواج صوتی، شبکه های محلی بیسیم اقدام به ارسال و دریافت داده ها می نمایند که بدین ترتیب نیازی به اتصال های سیمی در این سیستم ها وجود ندارد.

امروزه شبکه های محلی بیسیم به عنوان یک سیستم همه منظوره که می توانند جایگزین مناسبی برای شبکه های سیمی باشند، شناخته می شوند. در شبکه های محلی با سیم، معمولاً ۴۰ درصد کل هزینه نصب شبکه، هزینه کابل کشی آن می باشد و چنانچه شبکه نیاز به تغییری داشته باشد، کابل کشی باید تغییر نموده که این امر باعث افزایش هزینه می گردد. طبیعی است در شبکه های محلی بیسیم، هزینه کابل کشی وجود ندارد و در صورت نیاز، ساختار شبکه به راحتی قابل تغییر می باشد. از این شبکه ها در محیط های مختلفی نظیر دفاتر کار، کارخانجات، آزمایشگاه های تحقیقاتی و دانشگاه ها می توان استفاده نمود. با استفاده از شبکه های محلی بیسیم، کاربران شبکه بدون این که به نقطه خاصی متصل شوند، قادر به استفاده از منابع مشترک شبکه می باشند. همچنین مدیران شبکه قادر به توسعه و تغییر شبکه خود بدون نیاز به سیم کشی می باشند.

فن آوری بیسیم رادیویی سریعترین روش برای راه اندازی یک شبکه بویژه هنگامی که توزیع مشترکین اولیه بصورت پراکنده است، می باشد. هر طیف فرکانسی به لحاظ تاریخی یک کالای بسیار گرانبها بوده است. برخلاف طرح های مدولاسیون دیجیتال امروزی، تکنیک های قدیمی مدولاسیون از عرض باند بطور مؤثر استفاده نمی کردند. در آمریکا، سازمان FCC^۲ مجوزهای طیف فرکانسی را تا سال ۱۹۹۳ بطور رایگان در اختیار اپراتورها قرار می داد. بنابراین انگیزه کافی برای توسعه فن آوری جدید مدولاسیون وجود نداشت. بعلاوه بخش مناسبی از طیف موجود، معمولاً برای کارهایی با اولویت بالا همانند آژانس های محلی مثل آتش نشانی و پلیس یا کاربردهای ملی همانند کنترل ترافیک هوایی، تله متری عمیق ماهواره ای و ارتباطات نظامی رزرو می شد. در نهایت طیف فرکانسی بسیار بالا (بالای ۲۰ گیگاهرتز) برای کاربردهای تجاری به سختی مورد پذیرش قرار گرفت.

با ظهور فن آوری دیجیتال، فرکانس های بالای ۲۰ گیگاهرتز از جنبه تجاری اهمیت یافتند. فرکانس های زیر ۲۰ گیگاهرتز نیز می توانند کاربران بیشتری را در سرعت های بالاتر (اصولاً بواسطه تکنیک های مدولاسیون دیجیتال و فشرده سازی) پشتیبانی نمایند. افزون بر این فن آوری های جدید، تغییر در خط مشی هایی که در صدور مجوز فرکانس صورت می گیرد نیز بطور وسیعی در ارزش طیف فرکانسی تأثیر گذاشته اند. چند سال پیش سازمان FCC در آمریکا عرض باند قابل دسترسی را قیمت گذاری نمود و بدینگونه انگیزه برای استفاده مؤثر از طیف فرکانسی ایجاد گردید. همه این عوامل دست به دست هم دادند و فن آوری بیسیم را بعنوان یک فن آوری منتخب برای استفاده در کاربردهای باند پهن، مناسب ساختند.

در چند سال اخیر، دولت آمریکا و برخی از دولتهای اروپایی، سرویس های بیسیم جدیدی را به بازار عرضه نمودند. در میان این فن آوری ها می توان از سرویس ماهواره ای پخش مستقیم (DBS^۳)، سرویس های ارتباط شخصی یا PCS (تلفن سلولی دیجیتال نسل دوم)، سرویس توزیع چند نقطه ای محلی (LMDS)، سرویس توزیع چند نقطه ای چند کاناله (MMDS)، طیف

^۱ Portability

^۲ Federal Communications Commission

^۳ Direct Broadcast Satellite

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

تلویزیونی دیجیتال، ماهواره های مدار کم LEO، باند ۲۴ گیگاهرتز، باند ۳۸ گیگاهرتز، فن آوری GSM، سرویس ارتباطات بیسیم (WCS) و نسل سوم تلفنهای همراه نام برد.

مجموع این سرویسها نشان می دهند که در چند سال گذشته، FCC استفاده از بیش از ۳ گیگاهرتز از طیف فرکانسی را برای سرویسهای تجاری، غیردفاعی و غیردولتی آزاد نموده است. این عرض باند وسیع را با ظرفیت ۱ گیگاهرتزی کابل کواکسیال یا ظرفیت ۱ مگاهرتزی زوج سیم های مسی به هم تابیده مقایسه نمایید. علاوه دارندگان طیف، اکنون محدودیتهای کمتری روی سرویسهایی که می توانند ارائه دهند، دارند. از آنجایی که سرویس صوتی نیاز به عرض باند خیلی کمی دارد، بخش زیادی از عرض باند برای سرویسهای دسترسی تصویری و اینترنت قابل استفاده خواهد بود. در نهایت بخش زیادی از طیف تلویزیون آنالوگ در محدوده های فرکانسی کمتر از ۵۴ مگاهرتز (هنگامی که شرکتهای پخش تلویزیونی به پخش دیجیتال روی آوردند) در اختیار سایر سرویسها قرار گرفت.

سرویسهای تلویزیون ماهواره، معمولاً گرانتر از سرویسهای کابلی بوده و قابلیت برنامه ریزی محلی را ندارند. همچنین تلفن های سلولی دارای کیفیت صوتی پایین، قیمتهای بالا و ارتباط پذیری کمی می باشند. سؤال اصلی در مورد شبکه های بیسیم آن است که آیا عملکرد آنها در سطح قابل قبولی از عملکرد، قابل پیاده سازی است یا خیر؟ البته مسئله هزینه پایین تر در مرحله دوم قرار می گیرد.

شبکه های بیسیم از فرکانسهای خیلی بالاتری نسبت به زیرساختارهای کابلی بهره می گیرند. بنابراین بحثهایی در مورد پایداری و کم هزینه بودن آنها برای سرویسهای پرسرعت هنوز ادامه دارد. سهولت استفاده از فن آوریهای بیسیم، جذابیت آن برای مشترکین، بالا بودن طیف قابل دسترس برای کاربران و ابداعات فنی که امکان استفاده مؤثرتر از طیف فرکانسی را می دهند همگی دست به دست هم داده اند تا فن آوری بیسیم بعنوان یک گزینه کلیدی برای دسترسی به خدمات باند پهن مطرح شود.

۴-۲- مشخصه های بیسیم

شبکه های بیسیم از طیف فرکانسی رادیویی که اصولاً بعنوان محدوده فرکانسی ۳۰۰ کیلوهرتز تا ۳۰۰ گیگاهرتز تعریف می گردند، استفاده می کنند. این محدوده فرکانسی بین صوت قابل شنیدن و نور مرئی قرار می گیرد. صوت قابل شنیدن متناسب با تغییرات در فشار هوا ارسال می گردد. جدول (۴-۱) کلاسهای باند پهن طیف فرکانسی را نشان می دهد.

جدول (۴-۱): باندهای فرکانسی عریض

تا	از	
20 KHz	3 KHz	صوت قابل شنیدن
300 GHz	300 KHz (RF)	امواج رادیویی
10^{14} Hz	300 GHz	امواج مادون قرمز
8×10^{14} Hz	8×10^{14} Hz	نور مرئی
10^{17} Hz	10^{15} Hz	امواج ماوراء بنفش
10^{22} Hz	10^{15} Hz	اشعه X

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

فرکانسهای پایین طیف امواج رادیویی به آسانی منتشر نمی شوند. فرکانسهای بالاتر بیشتر شبیه نور مرئی عمل می نمایند. فرکانسهای بالاتر همانند نور مادون قرمز یا نور مرئی را می توان با استفاده از آنتن هایی با اندازه معقول متمرکز نمود. بنابراین یک مزیت فرکانسهای بالا، امکان کانونی تر نمودن سیگنالهاست که خود امکان ارسال بخش بندی شده طیف رادیویی را می دهد و در نهایت سبب افزایش امکان استفاده مجدد از فرکانس می شود. همچنین فرکانسهای پایین تر می توانند از موانعی همچون دیوارهای ساختمانها عبور نمایند درحالی که فرکانسهای بالاتر رادیویی بوسیله اشیاء فیزیکی همانند قطرات باران در فرکانسهای خیلی بالا بلوکه می گردند. فرکانسهای معقول برای شبکه های دسترسی بیسیم در باند سلولی آنالوگ، تقریباً از ۸۰۰ مگاهرتز تا ۳۰ گیگاهرتز در دسترس می باشند. غیر از این موارد، فن آوری بیسیم در بسیاری از مشخصه های ارسال کابلی مثل تضعیف متناسب با فاصله که در نهایت محدوده و برد سیستم را تعیین می نماید، مشترک می باشند. برخی مشخصه های اصلی مفید برای مقایسه شبکه های دسترسی بیسیم به شرح زیر می باشند:

- **مکان:** مکان بخشی از طیف رادیویی می باشد که سرویس مورد نظر در آنجا قرار می گیرد. بدان معنا که مکان، موقعیت سرویس را در باند فرکانسی نشان می دهد.

- **مقدار عرض باند:** برخی شبکه های دسترسی از عرض باندی معادل ۱۰ مگاهرتز (برای مثال سرویس PCS) استفاده می کنند، در حالی که برخی شبکه های دسترسی همانند LMDs از عرض باندی معادل ۱/۱ گیگاهرتز بهره می برند. نوعاً فرکانس بالاتر به معنای باند بیشتر می باشد. مقدار عرض باند، نرخ ارسال داده ها را مشخص می نماید.

- **مدولاسیون:** همانند رسانه های کابلی، فرستنده های بیسیم نیز می توانند مشخصه هایی همچون فرکانس، دامنه و فاز سیگنال را تغییر دهند. فن آوری بیسیم، بعد دیگری را به پارامترهای مدولاسیون اضافه می کند. بدان معنا که امواج را می توان هم به طور افقی و هم بطور قائم پولاریزه نمود. این می تواند یک درجه آزادی به سایر پارامترهای مدولاسیون اضافه نماید. قسمت بندی^۱، یک درجه آزادی دیگر را به مدولاسیون اضافه می کند. این دو درجه آزادی امکان استفاده مجدد از فرکانس را می دهند.

- **شعاع مؤثر سرویس^۲:** برخی سرویسها همانند DBS، دارای یک شعاع مؤثر سرویس ملی، یا در اروپا یک شعاع مؤثر سرویس قاره ای هستند. شعاع مؤثر پخش DTV تا حدود ۵۰ کیلومتر در مکانهای نسبتاً باز می باشد. سایر خدمات همانند LMDs یا PCS دارای شعاع نسبتاً کوچک می باشند. این شعاع بواسطه توان ارسال محدود موجود در فرکانسهای بالا و تضعیف بیشتر، در حدود ۵ کیلومتر یا کمتر می باشد. مزیت داشتن یک شعاع مؤثر بزرگ بمعنای آن است که یک سرویس را می توان به مشترکین زیادی حتی به میلیونها مشترک با استفاده از یک فرستنده واحد عرضه نمود. برای مثال یک ماهواره می تواند اطلاعات را به همه ایالات متحده آمریکا یا اروپا ارسال نماید. این واقعیت سبب کاهش هزینه شده و همه مشترکین می توانند اطلاعات را بطور همزمان در یافت نمایند. عیب این روش در آن است که ارتباط محاوره ای و دوطرفه با افزایش شعاع مؤثر، کاهش می یابد. شعاع مؤثر بزرگ به معنای آن است که مشترکین بیشتری با فراهم آوردن خدمات شبکه بطور همزمان می توانند ارتباط برقرار کنند. استفاده از مسیر برگشتی با افزایش شعاع مؤثر روز به روز مشکلتر می شود.

جدول (۴-۲) نحوه تخصیص فرکانس ها را به سرویسهای بیسیم، نشان می دهد. سرویسهای باند باریک، عرض باند کافی را برای صوت ارائه می دهند. سرویسهای باند پهن دارای عرض باند بیشتری بوده و از کاربردهای تجاری پرسرعت تصویری پشتیبانی می نمایند. کلاسها یا رده های بیسیم باند پهن شامل سرویسهای ماهواره ای، موبایل و سرویسهای ثابت می باشد.

¹Sectorization

²Footprint

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

سرویسهای ماهواره ای را می توان در دو دسته مدارهای ژئوسنکرون یا مدارهای LEO طبقه بندی نمود . سرویسهای موبایل اساساً همان سرویسهای تلفن سلولی آشنا هستند . سرویسهای ثابت ، بین دونقطه انتهایی ثابت عمل می نمایند.

جدول (۴-۲) : فرکانسهای اختصاص یافته به سرویسهای باند پهن

از فرکانس (MHz)	تافرکانس (MHz)	کاربرد
54	806	کانالهای تلویزیونی
824	894	تلفن سلولی
902	928	باند ISM
890	960	تلفن GSM
850	19901	سرویس PCS باند پهن
2150	2162	MMDS
2305	2360	سرویس ارتباطات بیسیم (WCS)
2400	2483/5	باند ISM
2500	2596	سرویس ITFS که اکنون با MMDS ترکیب شده است .
2596	2644	MMDS
2644	2686	ITFS (ترکیب شده با MMDS)
5150	5825	باند U-NII
12200	12700	ماهواره پخش مستقیم (DBS)
27500	28350	LMDS
29100	31300	LMDS

۴-۳- ارتباطات نقطه به نقطه و نقطه به چند نقطه

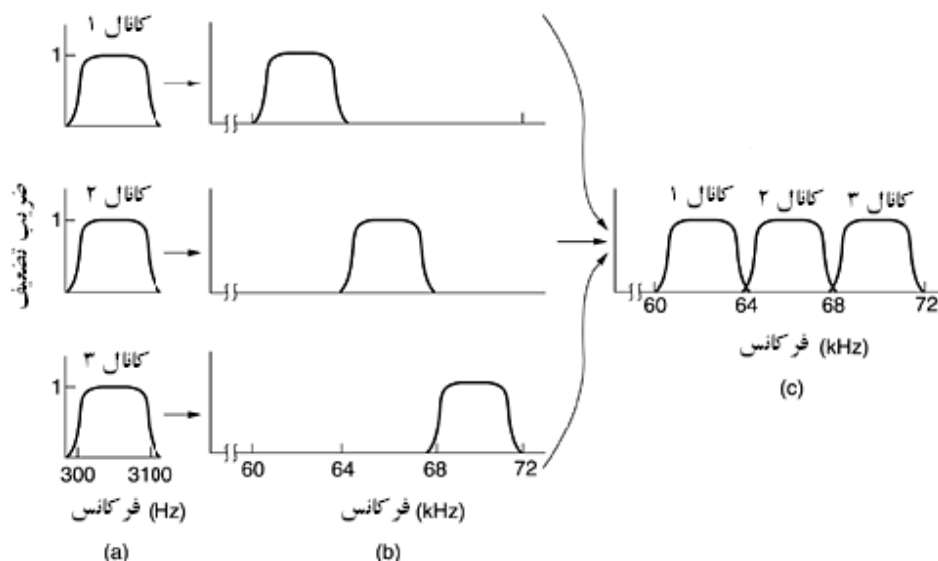
برخی ارتباطات بیسیم همانند رله مایکروویو از نوع ارتباطات نقطه به نقطه می باشد. یک فرستنده دقیقاً با یک گیرنده ارتباط برقرار می نماید. نوع دیگر ارتباط از نوع نقطه به چندنقطه می باشد. یک فرستنده با چندین گیرنده بطور همزمان (همانند ارتباط ماهواره ای و پخش تلویزیونی) ارتباط برقرار می کند.

از جمله مزایای ارتباطات نقطه به نقطه، اختفا و تضمین عرض باند می باشد. از طرف دیگر فن آوری نقطه به نقطه متکی بر یک دستگاه فرستنده و گیرنده برای هر جلسه ارتباطی است که این خود سبب افزایش هزینه می گردد. درمورد ارتباطات فرکانس بالا، توسعه فن آوری نقطه به چند نقطه بعنوان یک تکنیک کاهش هزینه مهم در نظر گرفته می شود زیرا یک فرستنده می تواند به تعداد زیادی از کاربران سرویس دهی نماید. در مورد مسیر برگشتی، به یک مکانیزم خاص نیاز داریم که نرم افزار این سرویس را پیچیده تر می سازد اما بسیاری از کارشناسان معتقدند که کاهش هزینه سخت افزاری ، امری با ارزش می باشد. ارتباطات نقطه به چند نقطه، سبب صرفه جویی در طیف و صرفه جویی در هزینه در سایت مرکزی می گردد. ایجاد قابلیت ارتباط دوطرفه در این فن آوری، چالش حقیقی فن آوری دسترسی بیسیم محسوب می شود.

دریک سیستم نقطه به چند نقطه ، یک فرستنده اطلاعات رادر مسیر جریان پایین به چندین گیرنده ارسال می نماید. هنوز برسر استفاده از تکنیک تسهیم سازی فرکانسی و تسهیم سازی زمانی بمنظور نائل شدن به یک عملکرد ارتباطی دوطرفه بحث وجود دارد.

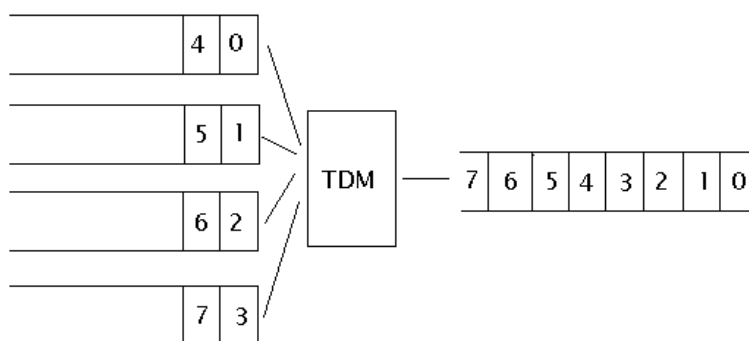
شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

همانطور که در شکل (۴-۱) نشان داده شده است، مدل قبلی، استفاده از فن آوری تسهیم سازی فرکانسی می باشد که طیف موجود را به دو کانال مجزا تقسیم می کند: یکی برای مسیر جریان بالا و دیگری برای مسیر جریان پایین.



شکل (۴-۱): تسهیم سازی فرکانسی (FDM) (a) پهنای باند اولیه (b) جابجایی پهنای باند بر اساس فرکانس حامل (c) کانالهای تسهیم سازی شده

یک روش جدیدتر که تسهیم ساز زمانی نام دارد امکان می دهد تا ترافیک در هر دو جهت روی یک کانال واحد، جریان یابد. اینکار دربرش های زمانی متفاوت به انجام می رسد. از تکنیک تسهیم ساز زمانی، گاهی اوقات بعنوان عملکرد ping-pong نام برده می شود. در شکل (۴-۲) نمونه ای از تسهیم سازی زمانی TDM نشان داده شده است.



شکل (۴-۲): تسهیم سازی زمانی TDM

از تکنیک تسهیم سازی فرکانسی در سالیان متمادی در تلفن سلولی استفاده گردیده است. هنگامی که از یک تلفن سلولی استفاده می کنید، از فرکانسهای ۸۲۴ مگاهرتز تا ۸۴۹ مگاهرتز استفاده می شود. اما هنگامی که به مکالمه روی تلفن سلولی گوش فرا می دهید از فرکانسهای ۸۶۹ مگاهرتز تا ۸۹۴ مگاهرتز بهره می گیرید.

با استفاده از تکنیک تسهیم ساز زمانی، تعدادی از اسلاتهای زمانی بطور پیوسته در هر دو جهت جریان می یابد. با اختصاص برش های زمانی در مسیر جریان بالا و جریان پایین متناسب با نیاز کاربر، صرفه جویی زیادی در عرض باند حاصل می گردد.

شبکه های کامپیوتری (دکتر محمد حسن یغمایی مقدم - دانشگاه فردوسی مشهد)

تعداد برش های زمانی در هر دو جهت ارتباط را می توان بطور تخمینی محاسبه نمود. این بدان معناست که تکنیک تسهیم ساز زمانی می تواند ارسال پی در پی اطلاعات را در هر جهت پشتیبانی نماید.

۴-۴- بررسی انواع شبکه های بیسیم

شبکه های بیسیم، ارتباط بین دستگاههای ارتباطی بیسیم با سرویس دهنده های اینترنت را برقرار می سازند. سازندگان تجهیزات کامپیوتری و مخابراتی، شبکه های بیسیمی ارائه داده اند که می توانند از دستگاهها و سرویسهای ارتباطی بیسیم پشتیبانی نمایند. شبکه های بیسیم به چهار خانواده اصلی تقسیم می شوند. این چهارگروه همراه با استانداردهایشان عبارتند از : IEEE 802.20 برای ارتباط شبکه های گسترده، IEEE 802.16 برای ارتباط شبکه های شهری، IEEE 802.11 برای ایجاد ارتباط شبکه های محلی در محدوده یک ساختمان و IEEE 802.15 برای دسترسی شخصی در محدوده یک اتاق. این شبکه ها، دستگاههای ارتباطی گوناگونی را برای استفاده در اینترنت عرضه می کنند. در ۵ سال گذشته، ارتباطات دستگاههای بیسیم صوتی تصویری از میزان ارتباطات دستگاههای کابلی فزونی یافته است. سرعت شبکه های کابلی امروزی در محدوده ۱/۵۴ مگابیت بر ثانیه (T1) می باشد، درحالیکه شبکه های گسترده سلولی در آمریکای شمالی از مرز ۲/۵۴ مگابیت بر ثانیه گذشته اند. درضمن یک شبکه محلی بیسیم مبتنی بر استاندارد 802.11a دارای سرعت ۵۴ مگابیت بر ثانیه می باشد و فن آوری بیسیم باند پهن قدرت ارسال ۱ گیگابیت بر ثانیه را نیز دارد.

۴-۴-۱- گستره ارتباطی شبکه های بیسیم

اصولاً کابل کشی و کابل برگردان شبکه ها امری وقت گیر و پرهزینه می باشد. شبکه های بی سیم دستگاههای ارتباطی را آزاد گذاشته و به کاربران امکان جابجایی می دهند و برای مبادله اطلاعات از دستگاههای رادیویی استفاده می کنند. در نهایت شبکه های بیسیم بر اساس نوع کاربرد و کلاس دستگاه بیسیم مطابق جدول (۴-۳) متمایز می گردند.

جدول (۴-۳): دستگاهها، شبکه ها و کاربردهای بیسیم

دستگاهها	شبکه ها	کاربرد ها
Web phone	WAN	ارسال و دریافت پیام
Handheld	LAN	مرورگر اینترنت
Pager	PAN	محواره
PORTAL	-	ارسال صدا
PC	-	وب
Appliance	-	ارتباطات

شبکه های بیسیم، ۶ کلاس دستگاه متفاوت را به یکدیگر متصل می نمایند که عبارتند از: تلفنهای وب ، دستگاههای ارتباطی قابل حمل دستی، پیجرها، پرتالهای صوتی، لوازم خانگی قابل استفاده به شبکه و Web PC. شبکه های بیسیم ۴ خانواده از کاربردهای بیسیم را نیز توسعه می دهند که عبارتند از: پیام دهی ، مرورگری وب ، ارتباط دوطرفه و کاربردهای صوتی. اصولاً انواع شبکه های بیسیم در مصرف توان، مقررات فرکانسی، خدمات و نرخ ارسال داده بایکدیگر تفاوت دارند. شبکه های ماهواره ای^۱ نیز جزو شبکه های بیسیم هستند اما ارتباطات دوطرفه ماهواره ای در حال حاضر بسیار گران است.

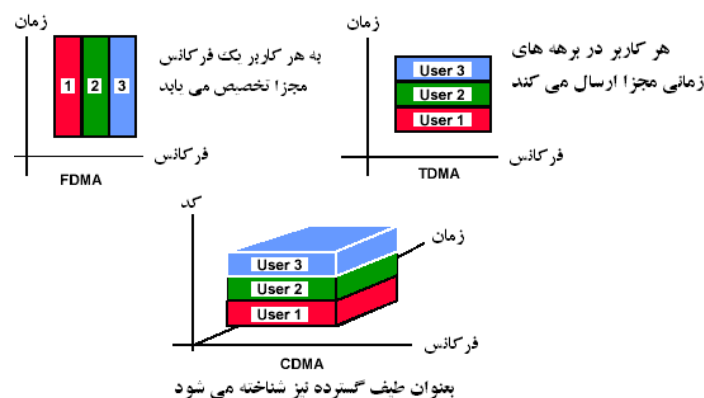
¹ Satellite Networking (SAN)

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

در شبکه های بیسیم مجموعه متنوعی از برجهای مخابراتی، دکل های سلولی، ایستگاههای پایه و نقاط دسترسی مورد استفاده قرار می گیرند. فرستنده گیرنده های مجهز به آنتن بمنظور مبادله داده ها یا صوت با دیگر دستگاههای بیسیم ارتباط برقرار می نمایند و سپس اطلاعات تقویت شده را به خطوط ارتباطی کابلی اینترنت ارسال می کنند. دستگاههای بیسیم جدید توانایی برقراری ارتباط با انواع شبکه ها را دارند. در این صورت کاربران امکان دسترسی به شبکه های گسترده، شبکه های محلی و شبکه های شخصی را با استفاده از اینترنت جهانی خواهند داشت.

شبکه های بیسیم در چگونگی عملکرد طیف، اختصاص طیف و استفاده از طیف فرکانسی در شرایط سلولی و موبایل بایکدیگر تفاوت دارند. هر شبکه از محدوده معینی از طیف الکترومغناطیسی بهره می گیرد. امواج رادیویی از فرکانسهایی که با افزایش انرژی همراه است شروع شده و در نهایت به امواج کوتاه می رسند. هنگامی که شما به رادیوی FM در فرکانس ۸۸/۵ مگاهرتز گوش می دهید، این ایستگاه اطلاعات خود را به رادیوی شما با فرکانس حامل ۸۸/۵ مگاهرتز ارسال می کند. شبکه های سلولی در یکی از دو باند ۸۰۰ مگاهرتز و ۱۹۰۰ مگاهرتز عمل می کنند. تفاوت بین پخش رادیویی معمول و شبکه سلولی در این است که برجهای پخش رادیویی فقط صحبت می کنند ولی برجهای سلولی علاوه بر صحبت، می شنوند. باندهای سلولی، بمنظور تضمین دسترسی مالک این باند، نیاز به مجوز دارند. یک اپراتور بایک مجوز بیسیم یک رابط هوایی^۱ همانند CDMA، FDMA و TDMA انتخاب می کند که این تکنیکها امکان استفاده از حداکثر تعداد مشترکین را فراهم می نمایند. در شکل (۳-۴) روش های دسترسی چند گانه در شبکه های بیسیم نشان داده شده است.

روشهای دسترسی چند گانه



شکل (۳-۴): مقایسه تکنیک های FDMA&TDMA&CDMA

رابط هوایی یک پروتکل ارسال رادیویی برای دستگاههای ارتباطی و ایستگاههای پایه می باشد. این طیف معمولاً گران بوده بطوریکه اروپایی ها بیش از صد میلیارد دلار در ۲۰ سال اخیر برای مجوزهای نسل سوم هزینه نمودند. از طرف دیگر بعضی از بخشهای این طیف همانند طیف ۲/۴ گیگاهرتز که به باند^۲ ISM معروف است و باند ۵/۷ گیگاهرتز که به نام U-NII^۳ معروف می باشد نیاز به مجوز ندارد. طیف بدون مجوز، بازار را برای دستگاههای فرستنده در محدوده شبکه های محلی و شخصی بیسیم باز نموده است.

سه اصل مهم در شبکه های سلولی می بایست به خوبی درک شوند. این سه اصل عبارتند از: تقسیم بندی سلولها، تکنیک handoff و استفاده مجدد از طیف فرکانسی. شبکه های سلولی دائماً هر محدوده معین جغرافیایی را به بخشهای

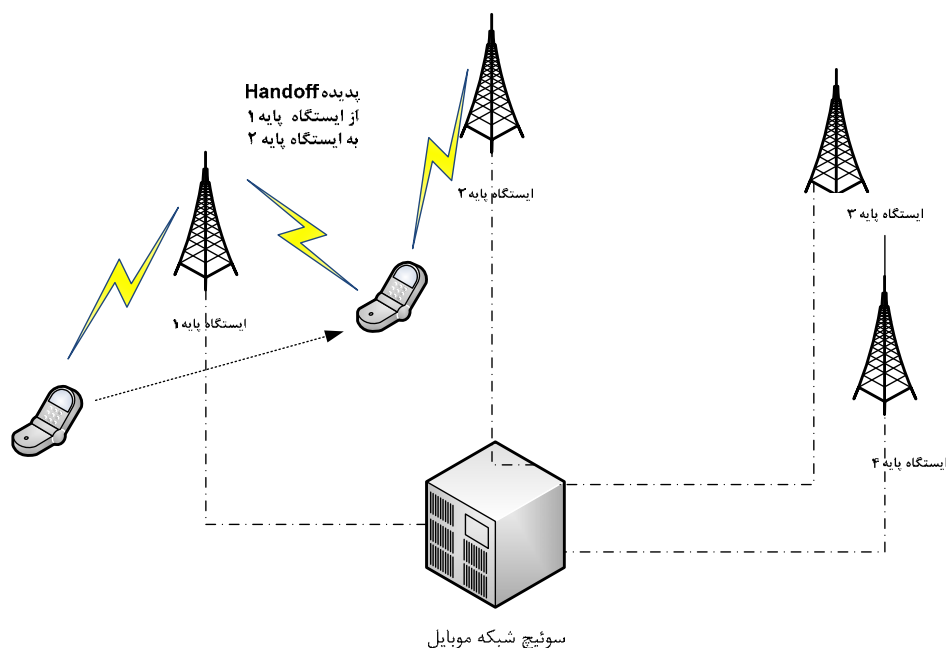
¹ Air interface

² Industrial, Scientific, and Medical

³ Unlicensed National Information Infrastructure

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

کوچکتر تقسیم می کنند و در هر بخش فرعی یک فرستنده گیرنده کم مصرفتر را به منظور استفاده مجدد از طیف فرکانسی اضافه می نمایند. این کار تعداد مشترکین را در یک محدوده معین جغرافیایی افزایش می دهد. مثلاً اتومبیلی که از برج سلولی A به برج سلولی B سفر می نماید، می باید از فرکانسی به فرکانس دیگر تغییر یابد. فضای مکالمه باقیمانده در محدوده سلولی A می تواند دوباره مورد استفاده قرار گیرد. به این فرایند handoff گویند. شخصی که در یک ساختمان اداری مبتنی بر شبکه های بیسیم 802.11 حرکت می کند، نیز به این سرویس نیاز دارد. در شکل (۴-۴) مثالی از این سرویس نشان داده شده است.



شکل (۴-۴) : سرویس handoff

کلیه شبکه های بیسیم از امواج رادیویی استفاده می نمایند، لذا برج های مخابراتی و دستگاه های ارتباطی هر دو دارای آنتن می باشند. فرستنده گیرنده های بیسیم به آنتن متصل گشته و سیگنال های اطلاعاتی را در محدوده محیط یک کره به برج ارسال و دریافت می نماید. شبکه های گسترده سلولی دارای یک کانال کنترلی همانند یک کانال پیجینگ می باشد. هنگامی که دستگاه های ارتباطی آماده برقراری ارتباط باشند، برج ارتباطی کانال کنترلی را به کانال های ارسال می فرستد. دوکانال عمده برای تلفن های شبکه گسترده، کانال های ارسال و دریافت هستند.

۴-۴-۲- شبکه های شخصی بیسیم

شبکه شخصی، یک شبکه کوتاه برد کم مصرف می باشد. برای مثال شبکه های مادون قرمز و Bluetooth را می توان نام برد. فرستنده های کم مصرف یا نقاط دسترسی، دارای اتصال کابلی به اینترنت هستند. اگرچه یک شبکه شخصی بیسیم می تواند بدون نیاز به نقطه دسترسی مستقیماً به یک دستگاه دیگر متصل گردد، اما طراحی این شبکه با برد کوتاه عقلانی به نظر نمی رسد. این فن آوری امکان می دهد ماشین های مجاور با یکدیگر ارتباط داده ای بر مبنای یک شبکه بیسیم برقرار نمایند. یک تلفن وب بیسیم بعنوان یک آنتن برای یک کامپیوتر laptop مجاور کار می کند، مجموعه ای از ماشین های سازگار با یکدیگر از طریق پروتکل discovery، نرم افزارهای خود را تعریف می نمایند. اغلب به این مجموعه فدراسیون دستگاه های ارتباطی می گویند. پروتکل discovery وظیفه مبادله اطلاعات مربوط به هویت دستگاه ها و قابلیت های سرویس دهی بین دستگاه ها را دارد. این پروتکل همچنین به معنای در دسترس بودن اطلاعات بطور بیسیم خواهد بود. ارسال مادون

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

قرمز (IrDA) یک روش محبوب برای ابزارهای دستی بمنظور مبادله داده ها یا چاپ نمودن اسناد بطور بیسیم در یک ارتباط نقطه به نقطه در فاصله حدودی ۴ متر می باشد. Bluetooth یک شبکه داده ای و صوتی بیسیم شخصی است که در محدوده ۱۰ متر عمل می کند.

۴-۳- شبکه های محلی بیسیم

شبکه خانگی و تجاری بیسیم قدرتمند دوطرفه، شبکه محلی نام دارد و از حروف اختصاری^۱ WLAN برای بیان آن استفاده می شود. یک شبکه محلی بیسیم می تواند منطقه ای به شعاع ۱۰۰ متر را تحت پوشش قرار داده و معمولاً بیش از ۲۰۰ دستگاه ارتباطی را به یکدیگر مرتبط نماید.

برخلاف شبکه های گسترده بیسیم که پرهزینه و نیاز به مجوز دارند، یک شبکه محلی بیسیم روی طیف بدون مجوز ارسال می شود. این شبکه بوسیله کامپیوترها، ابزارهای ارتباطی دستی و برخی تلفنهای سلولی جدید مورد استفاده قرار می گیرد. شرکتهای تجاری نیز از فرستنده های محلی در داخل ساختمان استفاده می کنند. از دیگر مزایای شبکه بیسیم محلی، عرض باند گسترده و تنوع تجهیزات می باشد. ازطرفی سرعت ارسال داده ها در شبکه های محلی مگابیت برثانیه بوده در حالیکه در تلفنهای سلولی برحسب کیلوبیت برثانیه می باشد.

محبوبترین استاندارد، اترنت بیسیم (IEEE802.11b) با محدوده تحت پوشش ۱۰۰ متر می باشد و سرعت ارسال آن ۱۱ مگابیت برثانیه است. این استاندارد روی طیف بدون مجوز ۲/۴ گیگاهرتز ارسال می شود. دستگاههای Bluetooth، تلفن های بیسیم و شبکه های رادیویی خانگی نیز در این فرکانس عمل می کنند و می توانند سبب بروز تداخل گردند. شبکه های محلی بیسیم دارای مزایای عمده زیر هستند.

- **قابلیت جابه جا پذیری^۲**: کاربران محلی شبکه های بیسیم در هر نقطه ای از شبکه، قادر به دسترسی به اطلاعات شبکه می باشند. طبیعی است این امکان در شبکه های با سیم دیده نمی شود.
- **نصب سریع و آسان^۳**: نصب شبکه های محلی بیسیم به سرعت و به آسانی امکان پذیر است و برخلاف شبکه های محلی سیم دار نیاز به صرف وقت و هزینه برای کابل کشی نمی باشد.
- **انعطاف پذیری در نصب^۴**: شبکه های محلی بیسیم به راحتی قابل گسترش می باشند و با انعطاف پذیری بالا می توان این نوع شبکه ها را پیاده سازی نمود.
- **کاهش هزینه ها^۵**: هر چند تجهیزات مورد نیاز شبکه های محلی بیسیم به مراتب بیشتر از شبکه های محلی سیم دار است ولی هزینه نصب، نگهداری و توسعه این شبکه ها کمتر از شبکه های محلی سیم دار می باشد، بنابراین در دراز مدت هزینه این شبکه ها کمتر از شبکه های با سیم خواهد بود.
- **مقیاس پذیری^۶**: شبکه های محلی بیسیم جهت ارضاء نمودن نیازهای موجود در شبکه، قادر به پیاده سازی با ساختار متنوعی می باشند. پیکربندی این شبکه ها به راحتی قابل تغییر است و همچنین توسعه و گسترش آنها آسان می باشد.

برخی از کاربردهای مهم شبکه های محلی بیسیم به شرح زیر است:

^۱ Wireless LAN

^۲ Mobility

^۳ Flexibility

^۴ Scalability

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

الف) در بیمارستانها، پزشکان و پرستارها با استفاده از یک کامپیوتر قابل حمل کیفی قادر به اتصال به شبکه های محلی بیسیم می باشند و بدین ترتیب در هر نقطه از بیمارستان و در هر لحظه می توانند از اطلاعات پزشکی موجود در شبکه استفاده نمایند.

ب) گروه های حسابداری و شرکت های مشاوره ای با استفاده از امکانات شبکه های محلی بیسیم با سرعت بالا قادر به انجام وظایف خود می باشند.

ج) دانشجویان دانشگاهها با استفاده از امکانات شبکه های محلی بیسیم در هر نقطه از دانشگاه قادر به ورود به شبکه اینترنت و همچنین استفاده از منابع کتابخانه می باشند.

د) مدیران شبکه های کامپیوتری در محیط های متغیر، با استفاده از شبکه های محلی بیسیم بالاسری مورد نیاز برای توسعه و تغییرات در شبکه های کامپیوتری را به شدت کاهش می دهند.

ه) سایت های آموزشی در سازمان های حرفه ای و همچنین دانشجویان دانشگاه ها با استفاده از شبکه های محلی بیسیم به راحتی قادر به دسترسی اطلاعات و مبادله اطلاعات و آموزش از راه دور می باشند.

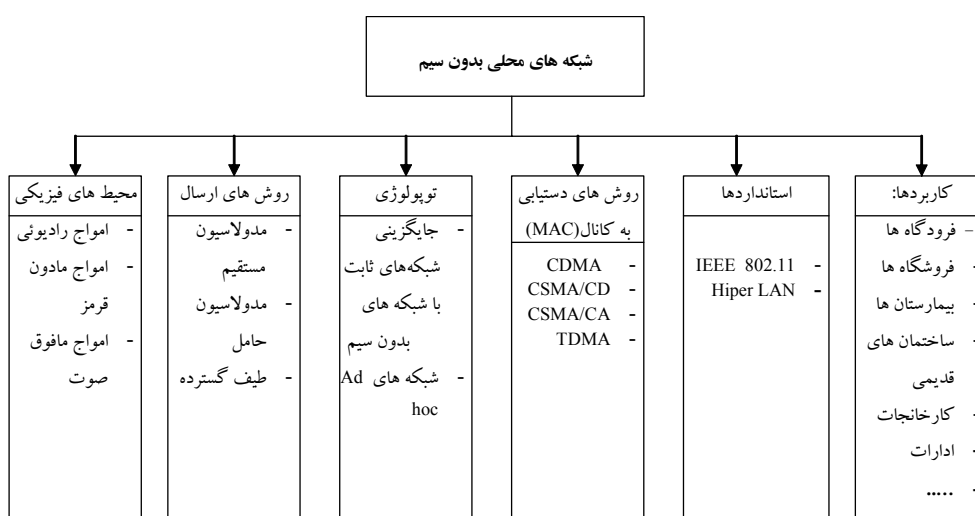
و) مدیران شبکه های کامپیوتری برای نصب شبکه های محلی کامپیوتری در ساختمان های قدیمی و مستهلک بدون نیاز به اعمال تغییرات در ساختمان، قادر به نصب شبکه های محلی بیسیم می باشند.

ز) کارمندان شعبات مختلف اداره ها با نصب و پیکربندی مناسب شبکه های محلی بیسیم، نیاز به سیستم اطلاعات مدیریت اطلاعاتی (MIS¹) محلی ندارند؛ بلکه به راحتی قادر به استفاده از سیستم مدیریت اطلاعات شعبه مرکزی خود می باشند.

ن) کارگران انبارها و کارخانجات با استفاده از امکانات شبکه های محلی بیسیم، قادر به مبادله اطلاعات با بانک اطلاعاتی مرکزی خود می باشند و بدین وسیله بهره وری بیشتری قابل دستیابی می باشد.

ی) مقامات و مدیران اجرایی با استفاده از شبکه های محلی بیسیم در جلسات خود قادر به تصمیم گیری های سریع و فوری از طریق دستیابی به اطلاعات موجود در شبکه می باشند.

فناوری ها و مسائل مختلف مربوط به شبکه های محلی بیسیم در شکل (۴-۵) نشان داده شده است.



شکل (۴-۵): فناوری ها و مسائل وابسته به شبکه های محلی بیسیم

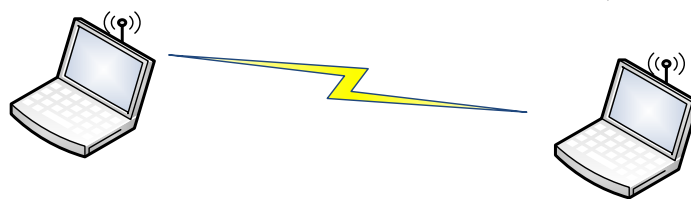
¹ Management Information System

۴-۳-۱- عملکرد شبکه های محلی بیسیم

امروزه استفاده از امواج رادیویی در پیاده سازی شبکه های محلی بیسیم بر سایر روش های موجود ترجیح داده می شود. در این شبکه ها داده های ارسالی کاربران به صورت حامل های رادیویی ارسال می شوند و گیرنده به خوبی قادر به دریافت و تشخیص آنها می باشد. در سمت فرستنده، داده های دیجیتالی ارسالی به وسیله عملیات مدولاسیون به امواج رادیویی مناسب تبدیل می شوند و ارسال می گردند. چنانچه حامل های بسامدی متفاوتی برای کاربر استفاده شود در این صورت هیچ گونه تداخلی بین امواج ارسالی دیده نخواهد شد. هر گیرنده برای دریافت اطلاعات خود از فیلتر خاصی استفاده می کند که با کمک این فیلتر، داده های هر کاربر دریافت می شوند و سایر بسامدهای ورودی فیلتر می گردند. هریک از ایستگاه های موجود در شبکه های محلی بیسیم مجهز به فرستنده/گیرنده رادیویی می باشد که در حقیقت نقطه دسترسی کاربر به شبکه است. هر یک از نقاط دسترسی فوق قادر به پشتیبانی از چندین کاربر می باشند. آنتن های متصل به نقاط دسترسی شبکه، معمولاً در ارتفاع بالایی نصب می شوند تا تمام کاربران قادر به دریافت و ارسال سیگنال های رادیویی باشند. کاربران انتهایی شبکه های محلی بیسیم از طریق آداپتورهای مخصوص که بر روی کامپیوترهای شخصی قابل حمل نصب شده اند، به شبکه متصل می گردند. آداپتورهای فوق از طریق آنتن های مخصوص ارتباط کاربران را از طریق فرستنده/گیرنده به شبکه برقرار می سازند.

۴-۳-۲- ساختار شبکه های محلی بیسیم

شبکه های محلی بیسیم به دو صورت ساده و پیچیده قابل پیاده سازی می باشند. در ساده ترین حالت چنانچه دو کامپیوتر مجهز به آداپتور رادیویی در فاصله معقولی از یکدیگر قرار داشته باشند، قادر به پیاده سازی شبکه بیسیم همتا به همتا می باشند. طبیعی است که چنین شبکه ای نیاز به مدیریت ندارد. هر کامپیوتر در حکم یک خدمات گیرنده شبکه است و قادر به استفاده از منابع خدمات گیرنده های دیگر می باشد، ولی امکان استفاده از منابع خدمات دهنده مرکزی را ندارد. در شکل (۴-۶)، نمونه ای از شبکه بیسیم همتا به همتا نشان داده شده است.

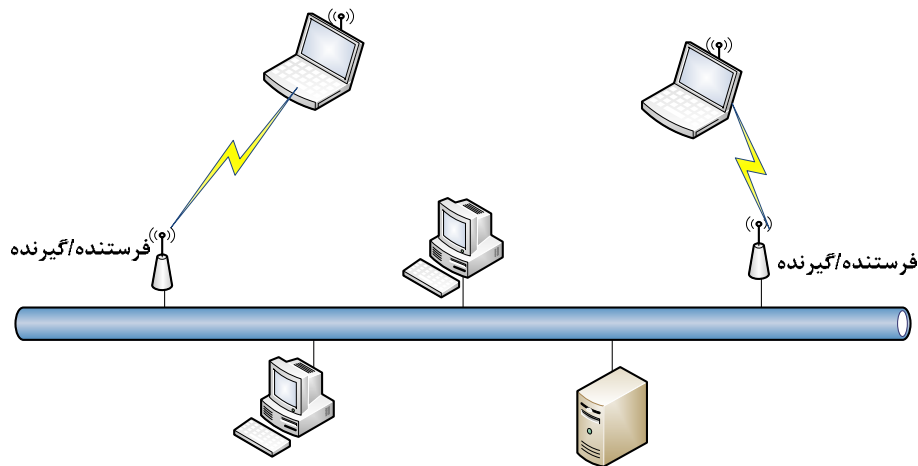


شکل (۴-۶): نمونه ای از یک شبکه بیسیم همتا به همتا

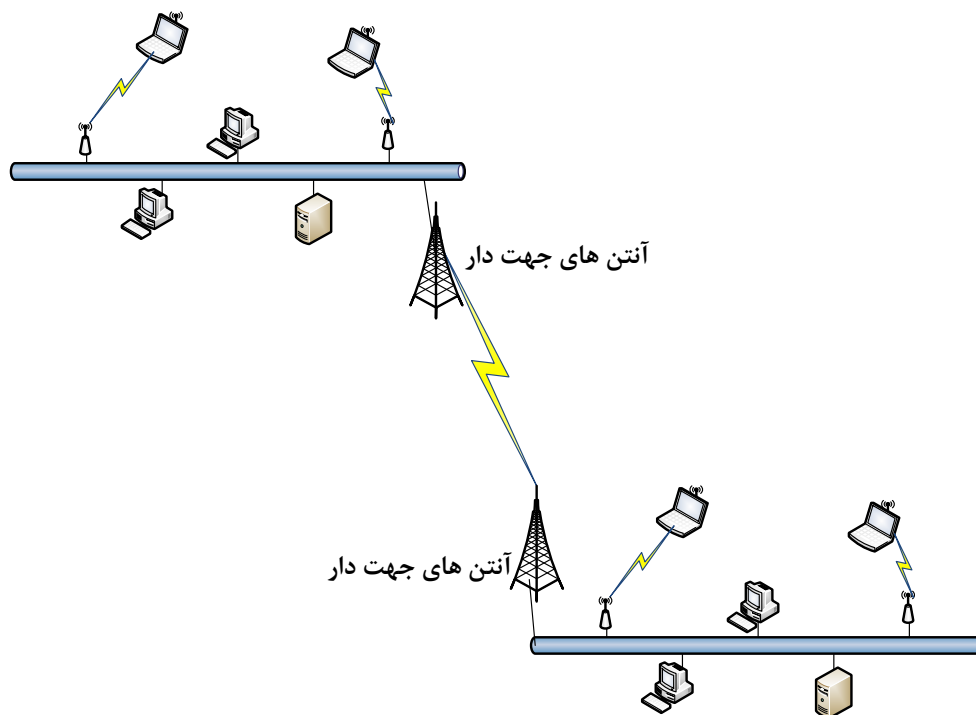
با نصب یک فرستنده/گیرنده، محدوده فاصله بین کامپیوترها افزایش می یابد. هر فرستنده/گیرنده از طریق یک شبکه سیم دار به خدمات دهنده مرکزی متصل است. بنابراین در این حالت هر خدمات گیرنده شبکه، ضمن این که می تواند از منابع خدمات گیرنده دیگر استفاده کند، قادر به استفاده از منابع خدمات دهنده شبکه نیز می باشد. هر فرستنده/گیرنده، قادر به خدمات دادن به ۱۵ الی ۵۰ خدمات گیرنده می باشد. فاصله هر خدمات گیرنده تا فرستنده/گیرنده حداکثر بین ۵۰۰ تا ۱۰۰۰ فوت می باشد. بنابراین در شبکه های وسیع تر نیاز به چندین فرستنده/گیرنده می باشد. در شکل (۴-۷) نمونه ای از یک شبکه محلی بیسیم با استفاده از چندین فرستنده/گیرنده نشان داده شده است.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

در طراحی شبکه های محلی بیسیم، باید امکان توسعه و افزودن فرستنده/گیرنده های بیشتر پیش بینی شده باشد. چنانچه بخواهیم دو شبکه محلی بیسیم را که در دو ساختمان مختلف و دور از هم قرار دارند را به یکدیگر متصل نماییم، از آنتن های جهت دار که به فرستنده/گیرنده شبکه متصل می شوند استفاده می گردد. در شکل (۴-۸) نمونه ای از اتصال دو شبکه محلی بیسیم با استفاده از آنتن های جهت دار آورده شده است.



شکل (۴-۷): یک شبکه بیسیم با چندین فرستنده/گیرنده



شکل (۴-۸): اتصال دو شبکه محلی بیسیم با استفاده از آنتن های جهت دار

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

برای پیاده سازی ارتباط بیسیم بین دونقطه، فن آوری های مختلفی ارائه شده است. هر یک از این فن آوری ها دارای مزایا و محدودیت های خاص خود می باشند. برخی از این فن آوری ها عبارتند از : استفاده از امواج رادیویی و مایکروویو ، استفاده از امواج مافوق صوت^۱ و استفاده از سیگنال های نوری. در زیر به بررسی مختصر هر یک از این روش ها می پردازیم.

امواج رادیویی

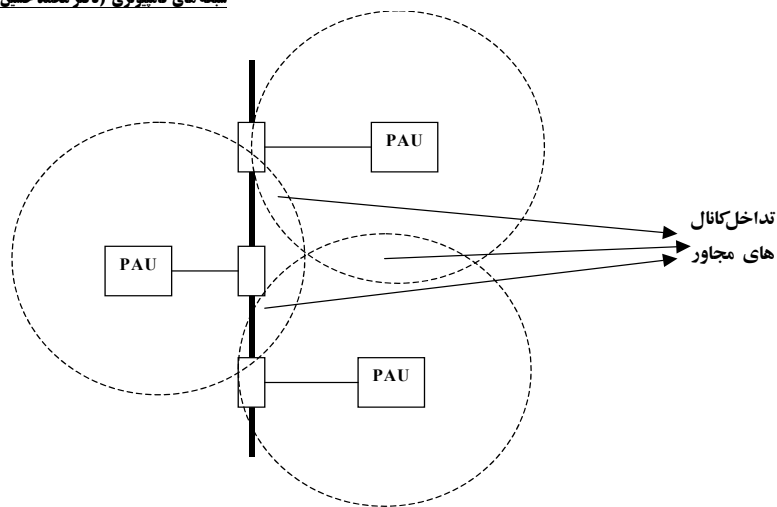
در فن آوری امواج رادیویی ازدو روش باند باریک و طیف گسترده^۲ استفاده می شود. در سیستم های رادیویی باند باریک، داده های کاربران بر روی باند بسامدی مشخصی ارسال و دریافت می گردند. از آنجایی که پهنای باند تخصیص یافته در این روش فقط به اندازه باند عبور اطلاعات می باشد، بنابراین به این روش باند باریک گفته می شود. با هماهنگی ساختن دقیق کاربران در بسامدهای مختلف، از وقوع تداخل بین کانال های مخابراتی جلوگیری می شود. در سیستم های رادیویی برای جلوگیری از وقوع تداخل، هر کاربر دارای یک فیلتر خاص می باشد که با کمک آن، اطلاعات ارسالی و دریافتی خود را از سایرین جدا می کند. از دید کاربران، یکی از معایب عمده این روش نیاز به اخذ مجوز بسامدی برای پیاده سازی شبکه های بی سیم می باشد.

یکی از مشکلات روش رادیویی، تداخل امواج می باشد. در این شبکه ها، پهنای باند موجود به تعدادی زیرباند تقسیم می شود. برای جلوگیری از تداخل، زیرباندهای مجاور از بسامدهای متفاوت استفاده می نمایند. در شکل (۴-۹) مثالی از تخصیص بسامد برای یک سیستم بیسیم آورده شده است. براساس این شکل، از سه بسامد f_1 ، f_2 و f_3 در شبکه استفاده شده است. تخصیص بسامد، طوری انجام می گیرد که سلول های مجاور یکدیگر از بسامدهای متفاوت استفاده کنند.

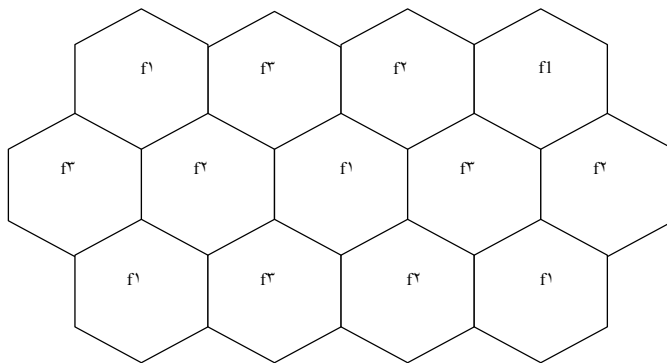
^۱ Ultrasonic

^۲ Spread spectrum

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۱



الف



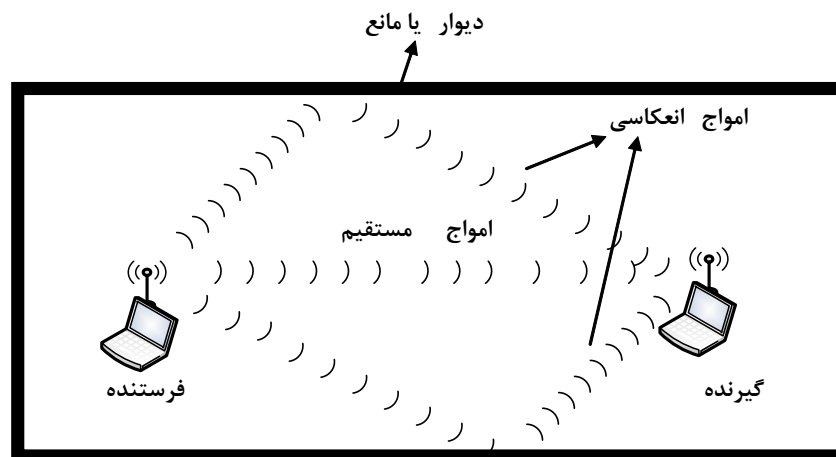
ب

شکل (۴-۹) مثالی از شبکه بیسیم با سه زیر باند الف) تداخل امواج ب) تخصیص کانال

یکی دیگر از مشکلات سیستم های رادیویی، مشکل چند مسیره^۱ است. در شبکه های بیسیم و در هر لحظه از زمان، گیرنده سیگنال های متعددی از جهت های مختلف که از یک فرستنده واحد به آن می رسد را دریافت می دارد. این پدیده باعث تداخل بین سمبل ها (ISI^۲) می شود. در شکل (۴-۱۰) مثالی از پدیده چند مسیره آورده شده است.

^۱ Multi path
^۲ Inter symbol Interference

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۴-۱۰): مثالی از پدیده چند مسیره

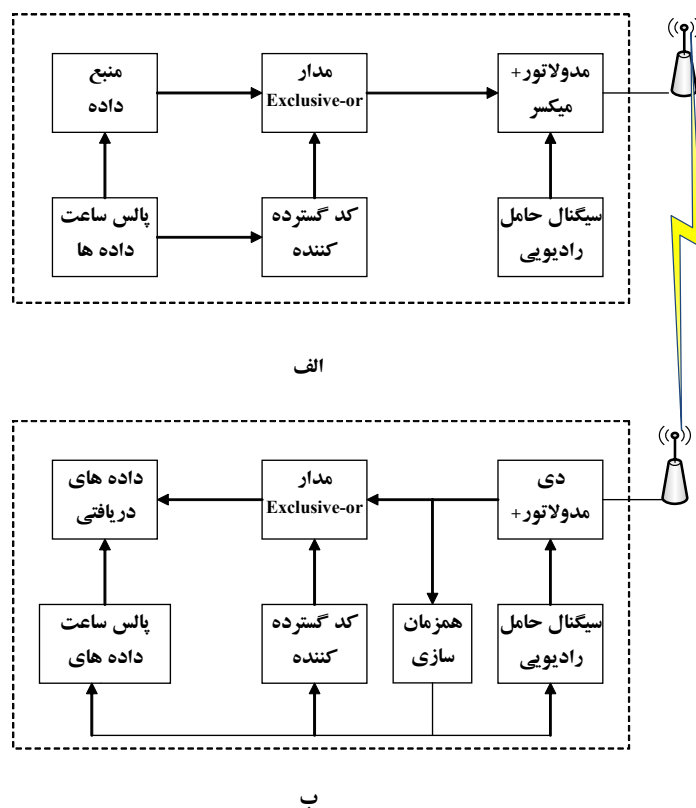
برای حل مشکل چند مسیره، درگیرنده ها از تکنیکی به نام یکنواخت سازی^۱ استفاده می شود. براساس این تکنیک، سیگنال های انعکاس یافته از سیگنال دریافتی مستقیم، کم شده و سیگنال حاصل به گیرنده وارد می شود. بیشتر سیستم های بی سیم امروزه از فن آوری طیف گسترده استفاده می کنند. این روش یک تکنیک بسامدهای رادیویی می باشد که اغلب در کاربردهای نظامی برای پیاده سازی یک سیستم ارتباطی مطمئن و امن استفاده می گردد. در این فن آوری بین استفاده بین از پناهی باند و قابلیت اطمینان بالا یک مصالحه انجام می گیرد. در این روش برای رسیدن به امنیت بالا سیگنال های ارسالی در تمام پناهی باند موجود پخش می شوند که این امر باعث نیاز به پناهی باند زیاد می گردد. چنانچه گیرنده مشخصه های فرستنده را داشته باشد، قادر به جمع آوری اطلاعات ارسالی از میان سیگنال های نویز خواهد بود. دو نوع روش مختلف برای پیاده سازی سیستم های طیف گسترده وجود دارند که عبارتند از: روش پرش بسامدی (FH) و روش رشته بیتی مستقیم (DS^۳). در روش DS برای هر رشته بیت ارسالی یک الگوی بیتی اضافی که در اصطلاح چپ نامیده می شود تولید می گردد. هر چه طول این چپ بیشتر باشد احتمال بازیابی داده های اصلی بیشتر خواهد بود. در شکل (۴-۱۱) بلوک دیاگرام فرستنده و گیرنده روش DS نشان داده شده است.

^۱ Equalization

^۲ Frequency hopping

^۳ Direct sequence

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

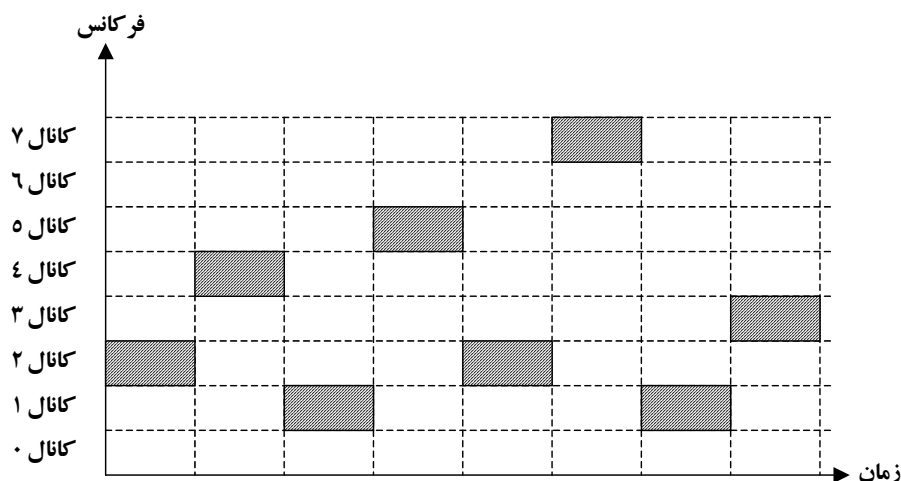


شکل (۴-۱۱): بلوک دیاگرام روش DS (الف) فرستنده (ب) گیرنده

مطابق با شکل فوق، در سمت فرستنده ابتدا داده های ارسالی به وسیله مدار Exclusive-or با یک رشته بیت تولید شده توسط کد گسترده کننده، به یک رشته بیت طولانی تصادفی تبدیل می شوند. خروجی مدار Exclusive-or به واحد مدولاتور و میکسر ارسال می شود. در این واحد رشته بیت تصادفی تولید شده که داده های اصلی در دل آنها وجود دارد، به صورت امواج رادیویی تبدیل می شوند و در تمام باند بسامدی موجود گسترده می شوند. بدین صورت گیرنده های غیرمجاز قادر به جداسازی داده های ارسالی نخواهند بود.

در سمت گیرنده، سیگنال های رادیویی دریافتی با کمک دی مدولاتور و میکسر به صورت رشته بیت درمی آیند. رشته بیت دریافتی وارد مدار Exclusive-or می گردد و در آنجا با کمک کد گسترده کننده، داده های اصلی فرستنده استخراج می شود. در روش FH با یک الگوی مشخص که هم فرستنده و هم گیرنده قادر به تشخیص آن می باشند، بسامد سیگنال ارسالی با گذشت زمان تغییر می نماید. به هریک از بسامدهای ارسالی، یک کانال گفته می شود. در شکل (۴-۱۲) عملکرد روش FH نشان داده شده است. در این مثال از هشت کانال بسامدی مختلف استفاده می شود. همان طور که در شکل نیز مشاهده می شود، بسامد کانال ارسالی فرستنده با گذشت زمان و براساس یک الگوی مشخص تغییر می نماید. تغییرات فوق نسبت به نرخ ارسال داده ها، می تواند خیلی سریع و یا خیلی کند صورت گیرد. چنانچه تغییرات بسامد سیستم FH نسبت به زمان کند باشد، همزمانی گیرنده با فرستنده به سادگی قابل دستیابی است.

شبهه های کامیوتري (دکتر محمد حسين یغمایی مقدم - دانشگاه فردوسی مشهد)

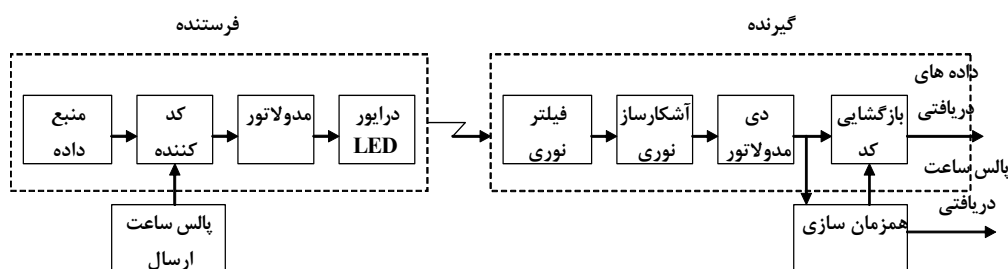


شکل (۴-۱۲): مثالی از روش FH با هشت کانال بسامدی

امواج مادون قرمز

قبل از این که فن آوری فیبرنوری به طور گسترده مورد استفاده قرار گیرد، نیمه هادی های نوری مانند دیودهای لیزری و دیودهای نوری در حوالی دهه ۷۰ گسترش فراوانی پیدا کردند. امروزه از تجهیزات الکترونیک نوری که در طول موج های ۸۴۰ تا ۹۵۰ نانومتر کار می کنند، در کاربردهایی نظیر کنترل از راه دور سیستم ها و هدفون های بیسیم استفاده می شود. همچنین می توان از این فن آوری در شبکه های محلی بیسیم نیز استفاده نمود. این فن آوری دارای مشکلاتی نظیر قدرت انتشار امواج نوری و تداخل امواج و همچنین نویزهای موجود در محیط می باشد. به خاطر سرعت و انتشار بر روی خط مستقیم از دیودهای لیزری برای ارتباط کامپیوتری بین دو ساختمان استفاده می شود. برای سیستم های داخل ساختمان معمولاً از دیودهای نوری که دارای قدرت و سرعت کمتری می باشند استفاده می گردد. از آن جایی که سیگنال های مادون قرمز قادر به عبور از موانعی نظیر دیوارها و دربها نمی باشند، بنابراین فرستنده و گیرنده نوری باید در دید یکدیگر قرار داشته باشند. در این فن آوری، مشکل محدودیت بسامدی و تداخل امواج که در روش امواج رادیویی وجود دارد دیده نمی شود و استفاده از آن در محیط هایی که تداخل امواج الکترومغناطیسی زیاد می باشد مناسب است. فن آوری امواج مادون قرمز نسبت به امواج رادیویی ارزان تر می باشد.

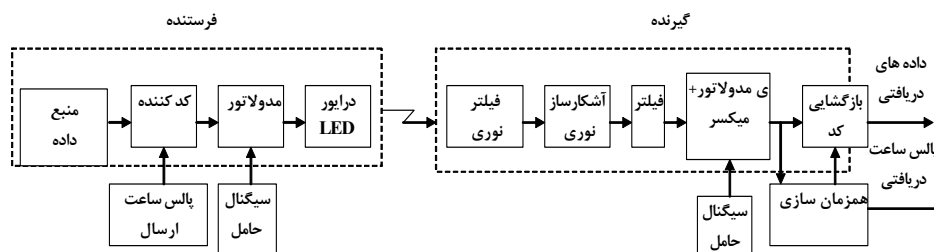
سیستم‌های مادون قرمز به دو صورت قابل پیاده سازی هستند که عبارتند از: روش مدولاسیون مستقیم و روش مدولاسیون سیگنال حامل. در روش مدولاسیون مستقیم، براساس یک یا صفر بودن بیت ارسالی، منبع نوری روشن یا خاموش می‌شود. برای نیل به همزمانی، رشته بیت ارسالی منبع، قبل از مدولاسیون، کد گذاری می‌شود. معمولاً از روش NRZ-I و یا روش منچستر برای کدگذاری داده های ارسالی استفاده می‌شود. در شکل (۴-۱۳) بلوک دیاگرام کلی فرستنده و گیرنده مادون قرمز نشان داده شده است.



شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

شکل (۴-۱۳): بلوک دیاگرام فرستنده و گیرنده مادون قرمز (روش مدولاسیون مستقیم)

در روش مدولاسیون سیگنال حامل که بلوک دیاگرام آن در شکل (۴-۱۴) نشان داده شده است، برای نیل به سرعت بالا مشابه سیستم های رادیویی از تکنیک های مدولاسیون سیگنال حامل نظیر FSK و PSK استفاده می گردد.



شکل (۴-۱۴): بلوک دیاگرام فرستنده و گیرنده مادون قرمز (روش مدولاسیون حامل) سیگنال

در هر دو فن آوری امواج رادیویی و امواج مادون قرمز، از محیط های پخشی استفاده می شود. در شبکه های محلی بیسیم از استانداردهای مختلف نظیر: ^۱CDMA، ^۲FDMA و ^۳TDMA، CSMA/CA، CSMA/CD، استفاده می گردد.

۴-۳-۲- شبکه های محلی بیسیم استاندارد 802.11

در سال ۱۹۹۷ اولین نسخه استاندارد شبکه محلی بیسیم با نام 802.11 منتشر شد و سپس در سال ۱۹۹۹، استاندارد 802.11b با سرعتی معادل ۵،۵ تا ۱۱ مگابیت بر ثانیه به بازار معرفی شد. این استاندارد برای پیاده سازی شبکه بیسیم در لایه های فیزیکی و دسترسی به شبکه طراحی شده است. موسسه WECA^۳ وظیفه معرفی و بررسی تجهیزاتی که با این استاندارد مطابقت دارند را برعهده دارد. اصطلاح WiFi^۴ که توسط این موسسه معرفی گردید، به معنی تجهیزاتی است که با این استاندارد مطابقت دارند. آزمایش های WECA بر اساس استاندارد 802.11 می باشد که لیست کامل این استاندارد ها در زیر آمده است:

802.11: استاندارد شبکه محلی بیسیم

802.11a: استاندارد شبکه بیسیم در محدوده 5 GHz

802.11b: استاندارد شبکه بیسیم در محدوده 2,4 GHz

802.11c: استاندارد عملیات های میانی در لایه انتقال داده 802.11

802.11d: بسط استاندارد 802.11 برای ناحیه های کاری مرتب

802.11e: استاندارد کیفیت سرویس در شبکه های محلی بیسیم

802.11f: استاندارد بررسی ارتباطات نقاط دسترسی در 802.11

802.11g: استاندارد ارتباط سریع تر در 802.11

^۱ Code-Division Multiple Access

^۲ Frequency Devision Multiple Access

^۳ Wireless Ethernet Compatibility Alliance

^۴ Wireless fidelity

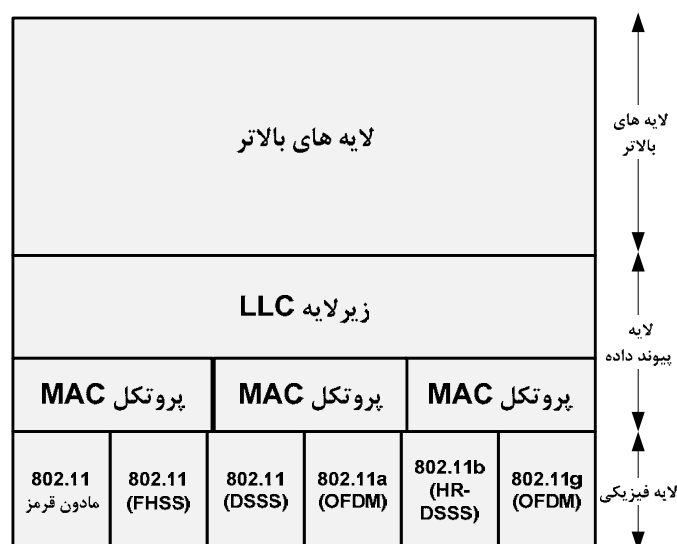
شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

802.11h: استاندارد مربوط به بالا بردن انتخاب کانال ها و توان کنترلی

802.11i: استاندارد بررسی امنیت و احراز هویت در 802.11

پشته پروتکل 802.11

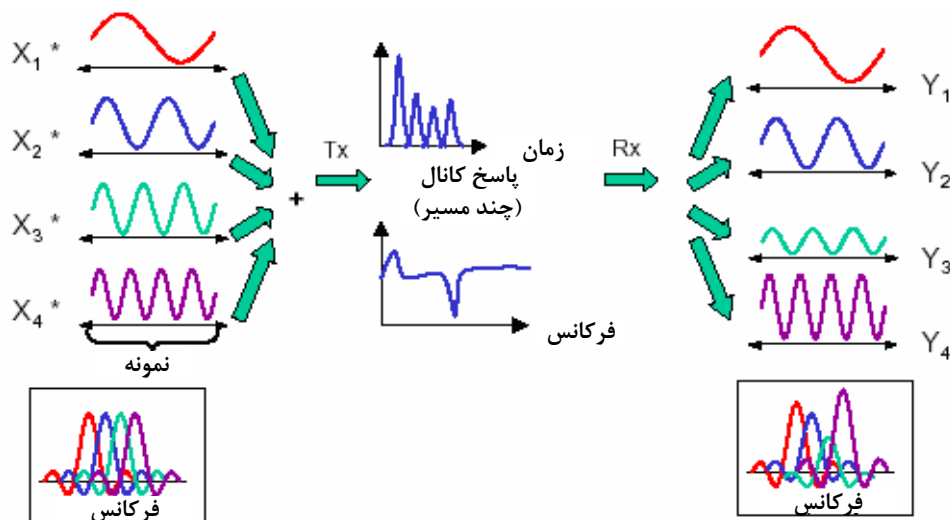
کلیه پروتکل های 802 ساختار تقریباً مشابهی دارند. لایه فیزیکی پشته پروتکل 802.11 متناظر با لایه فیزیکی OSI است، اما لایه پیوند داده ها در پروتکل های 802 به دو یا چند زیر لایه تقسیم می شود. در 802.11 زیر لایه MAC (کنترل دستیابی رسانه) چگونگی تخصیص کانال را مشخص می کند. در بالای آن زیر لایه LLC (کنترل پیوند منطقی) قرار دارد که وظیفه اش پنهان کردن انواع رسانه های 802 می باشد. در شکل (۴-۱۵) ساختار پشته استاندارد های 802.11 نشان داده شده است.



شکل (۴-۱۵): پشته پروتکل های 802.11

استاندارد 802.11 در سال ۱۹۹۷، سه تکنیک انتقال را در لایه فیزیکی مشخص کرد. روش مادون قرمز از تکنیکی مشابه کنترل راه دور تلویزیون استفاده می کند. دو روش دیگر از رادیوی برد کوتاه استفاده می کنند که تکنیک هایی به نام FHSS و DSSS در آن ها به کار می رود. در سال ۱۹۹۹ نیز روش های OFDM و HR-DSSS با سرعت های 54Mbps و 11Mbps معرفی شدند. در سال ۲۰۰۱ دومین تلفیق OFDM معرفی شد که باند فرکانس آن متفاوت از اولی بود. از نظر تکنیکی این ها به لایه فیزیکی تعلق دارند. در شکل (۴-۱۶) تلفیق فرکانسی OFDM نشان داده شده است.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۴-۱۶) : تلفیق فرکانسی OFDM

۴-۵- ملاحظات مشتریان شبکه های محلی بیسیم

- هر چند شبکه های محلی بیسیم از انعطاف پذیری بالا در نصب و پیکربندی برخوردار می باشند، اما مشتریان این شبکه ها باید فاکتورهای زیر را توجه داشته باشند:
- **محدوده پوشش:** در شبکه های محلی بیسیم، محدوده پوشش شبکه به عواملی مانند نوع تجهیزات استفاده شده، توان ارسالی و مسیر انتشار امواج بستگی دارد. برخورد امواج رادیویی با اشیایی نظیر ساختمانها، دیوارها، فلزات و حتی مردم باعث پراکندگی انرژی می شود که این مسأله محدوده پوشش سیستم را کاهش می دهد. اکثر سیستم های بیسیم از امواج رادیویی به خاطر قابلیت نفوذ ناپذیری آنها در دیوارها و سایر موانع استفاده می کنند. به طور نمونه شبکه های محلی بیسیم محدوده جغرافیایی بین ۱۰۰ تا ۳۰۰ فوت را پوشش می دهند.
 - **گذردهی^۱:** مشابه شبکه های محلی سیم دار، گذردهی شبکه های محلی بیسیم نیز بستگی به نوع محصول دارد. عواملی که گذردهی را محدود می نمایند عبارتند از: تعداد کاربران، فاکتورهای انتشار، نوع سیستم شبکه محلی بیسیم مورد استفاده و گلوگاه موجود در نقطه اتصال شبکه بیسیم به شبکه سیم دار محلی. اکثر شبکه های محلی بیسیم تجاری دارای سرعت ۱/۷ مگابیت بر ثانیه می باشند. کاربران شبکه های محلی اترنت و حلقه نشانه، هنگامی که از شبکه های محلی بیسیم استفاده می کنند، به طور محسوس کاهشی در کارایی شبکه حس نمی کنند. شبکه های محلی بیسیم، از گذردهی مناسب برای اغلب خدمات متداول شبکه های محلی سیم دار برخوردار می باشند.
 - **جامعیت و قابلیت اطمینان:** قابلیت اطمینان فن آوری شبکه های محلی بیسیم، بیش از ۵۰ سال است که در کاربردهای تجاری و نظامی به اثبات رسیده است. هر چند تداخل امواج رادیویی باعث کاهش گذردهی شبکه می شود، ولی با طراحی مناسب شبکه های محلی بیسیم می توان این مشکل را برطرف نمود.
 - **سازگاری با شبکه های موجود:** اکثر شبکه های محلی بیسیم قادر به اتصال به شبکه های سیم دار اترنت یا حلقه نشانه می باشند. از آنجایی که نودهای شبکه های محلی بیسیم همانند نودهای شبکه های محلی سیم دار مدیریت و پشتیبانی می شوند بنابراین امکان سازگاری و اتصال این شبکه ها با شبکه های موجود فعلی وجود دارد.

^۱Throughput

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

- **سازگاری تجهیزات شبکه های محلی بیسیم با یکدیگر:** یکی از نکات مهمی که مشتریان باید به آن توجه داشته باشند، آن است که سیستم های شبکه های محلی بیسیم مربوط به فروشنده های مختلف، ممکن است سازگار با یکدیگر نباشند. سه دلیل مهم این امر عبارتند از:
 - الف) ممکن است هر فروشنده از فن آوری مختلفی استفاده نمایند که سازگار با فن آوری سایر تجهیزات فروشنده ها نباشد.
 - ب) ممکن است سیستم های مختلف از باندهای بسامدی مختلفی استفاده نمایند، که در این صورت قادر به ارتباط با یکدیگر نمی باشند.
 - ج) ممکن است تجهیزات شبکه های محلی بیسیم فروشندگان مختلف، با وجود استفاده از فن آوری و باند بسامدی یکسان، به دلیل تفاوت در پیاده سازی سیستم، سازگار با یکدیگر نباشند.
- **مجوز استفاده:** در ایالت متحده آمریکا اداره مدیریت بسامد، کلیه ارتباطات رادیویی و شبکه های محلی بیسیم را نظارت می نماید. سایر کشورها نیز اداره هایی برای این کار دارند. فروشندگان سیستم های شبکه های محلی بیسیم در هر کشور قبل از فروش محصول خود باید با اداره های مرتبط در آن کشور جهت دریافت مجوز بسامد وارد مذاکره شوند.
- **سادگی و استفاده آسان:** کاربران شبکه های محلی بیسیم برای استفاده از مزایای آن نیاز به اطلاعات زیادی ندارند. برنامه های کاربردی موجود در شبکه های محلی سیم دار، به راحتی قابل استفاده در شبکه های محلی بیسیم می باشند. نصب و راه اندازی شبکه های محلی بیسیم به دلیل عدم نیاز به کابل کشی آسان است. همچنین بعد از نصب تجهیزات شبکه های محلی بیسیم، امکان جابجایی آنها از یک محل به محل دیگر وجود دارد.
- **امنیت:** از آنجایی که ریشه اولیه فن آوری شبکه های محلی بیسیم از کاربردهای نظامی نشأت گرفته است، بنابراین امنیت این سیستم ها بسیار بالا می باشد. برای گیرنده های غیرمجاز دریافت اطلاعات ارسالی سایر کاربران مجاز، عملاً بسیار مشکل و پیچیده است. در سیستم های شبکه های محلی بیسیم، از تکنیکهای رمزنگاری پیچیده ای برای افزایش امنیت شبکه استفاده می شود.
- **هزینه:** پیاده سازی یک شبکه محلی بیسیم، دارای هزینه هایی جهت نصب نقاط دسترسی و همچنین آداپتورهای کاربران می باشد. تعداد نقاط دسترسی مورد نیاز در یک شبکه، به محدوده جغرافیایی پوشش شبکه و همچنین تعداد و نوع کاربران بستگی دارد. آداپتورهای شبکه های محلی بیسیم، معمولاً قیمت کمتری نسبت به تجهیزات نقاط دسترسی دارند. معمولاً هزینه نصب و نگهداری یک شبکه محلی بیسیم نصب شده، به دو دلیل عمده زیرنسبت به شبکه سیم دار معمولی کمتر است:
 - الف) در شبکه های محلی بیسیم هزینه های کابل کشی و نصب آن وجود ندارد.
 - ب) از آنجایی که شبکه های محلی بیسیم به سادگی قادر به حرکت، اضافه کردن، کاهش و یا تغییر کاربران می باشند، بنابراین هزینه های اضافی اجرایی کاهش می یابد.
- **مقیاس پذیری:** در شبکه های محلی بیسیم، امکان توسعه شبکه با اضافه کردن نقطه دسترسی به شبکه به آسانی فراهم می آید.
- **سلامتی:** توان خروجی از سیستم های شبکه های محلی بیسیم بسیار کم است. این توان خیلی کمتر از توان خروجی از تلفن های موبایل سلولی می باشد.

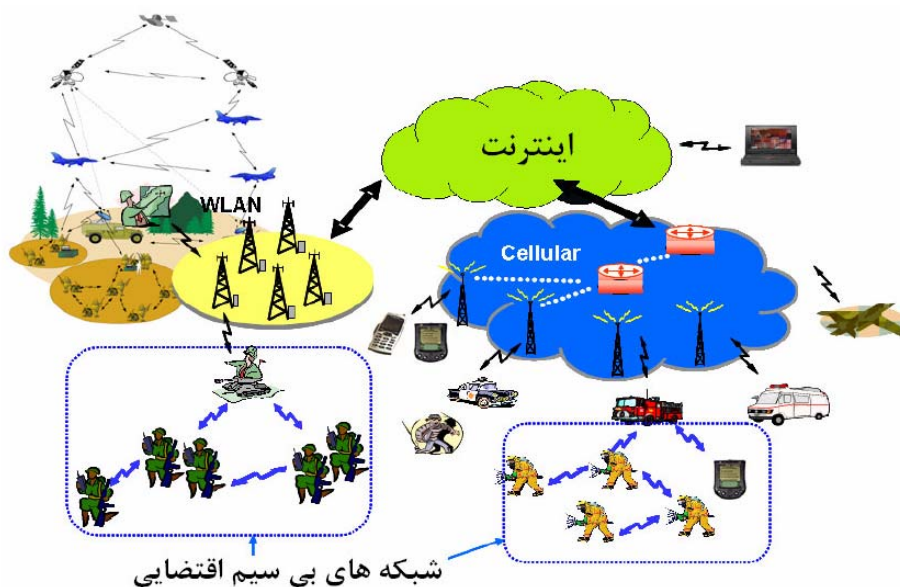
۴-۶- شبکه های بیسیم اقتضایی (MANET)¹

¹ Mobile Adhoc NETworks

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

شبکه های بیسیم اقتضایی، مجموعه ای از نودهای بیسیم است که می توانند به طور پویا در هر مکان و در هر زمان بدون استفاده از هرزیر ساخت شبکه ای تشکیل شده و بایکدیگر در ارتباط باشند. این شبکه ها یک سیستم خود مختار می باشند که نودهای سیار توسط کانال های بیسیم به هم متصل شده اند و می توانند آزادانه حرکت نموده و اغلب در آن واحد هم به عنوان نود و هم به عنوان مسیریاب عمل کنند.

شبکه های بیسیم اقتضایی، سیستمی مستقل از نود های سیار است که ممکن است مجزا بوده یا اینکه وجه مشترکی با شبکه ثابت داشته باشند، یعنی بوسیله یک یا چند نود به یک شبکه سیمی مانند اینترنت متصل باشند. نود های شبکه های بیسیم اقتضایی مجهز به آنتن های فرستنده و گیرنده بیسیم همه جهتی (پخش فراگیر)^۱ هستند. در هر لحظه، وابسته به مکان نود ها و الگوهای پوشش فرستنده و گیرنده آنها، یک ارتباط بیسیم چندگامی بین نود ها وجود دارد. این توپولوژی اقتضایی ممکن است با گذشت زمان به سبب جابجائی نود ها تغییر کند. در شکل (۴-۱۷) نمونه ای از کاربردهای مختلف شبکه های بیسیم اقتضایی نشان داده شده است.



شکل (۴-۱۷): نمونه ای از کاربردهای شبکه های بیسیم اقتضایی

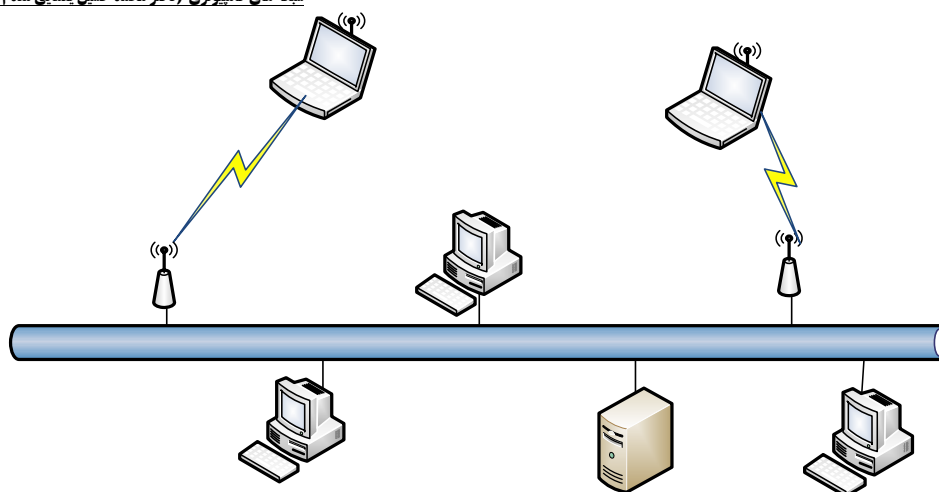
بطور کلی دو رویکرد مجزا برای ارتباط واحدهای سیار بیسیم با یکدیگر وجود دارد که عبارتند از:

- **ساختار یافته** : شبکه های بیسیم سلولی هستند که در آن دستگاه های سیار با استفاده از نقاط دسترسی مانند ایستگاه مرکزی که به یک ساختار شبکه ثابت متصل است، با هم ارتباط برقرار می کنند.

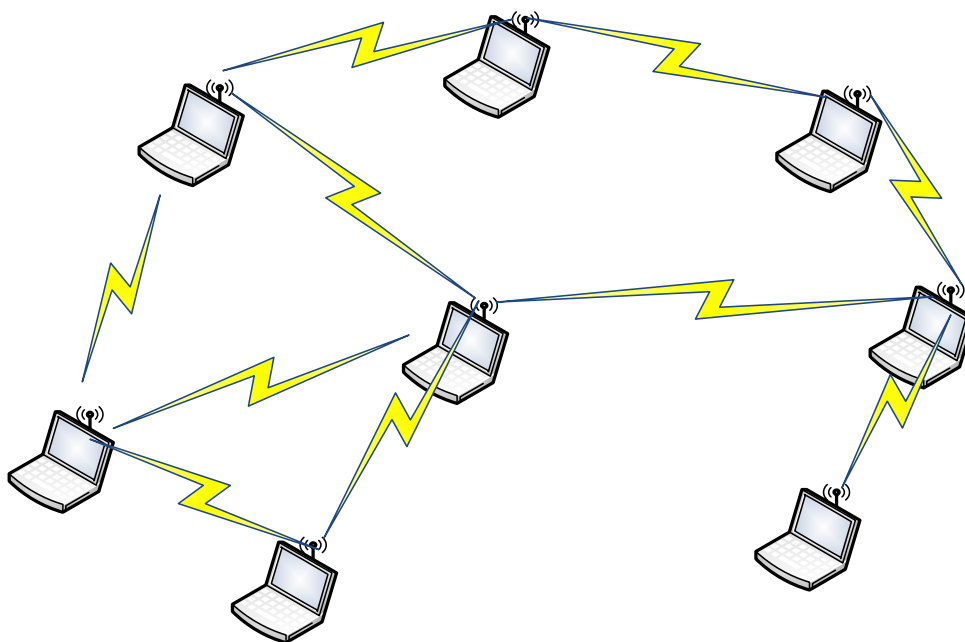
- **بی ساختار** : مثالی از رویکرد بدون ساختار، شبکه های بیسیم اقتضایی سیار می باشد. یک شبکه بیسیم اقتضایی مجموعه ای از نود های بیسیم است که می توانند بطور پویا یک شبکه تشکیل بدهند و بدون استفاده از هر گونه ساختار شبکه ثابت از پیش موجود، تبادل اطلاعات نمایند. شکل (۴-۱۸) مثالی از شبکه های بیسیم ساختار یافته و شبکه های بی ساختار را نشان می دهد .

^۱ Broadcast

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شبکه بیسیم ساختار یافته



شبکه بیسیم اقتضایی بی ساختار

شکل (۴-۱۸): انواع شبکه های بیسیم

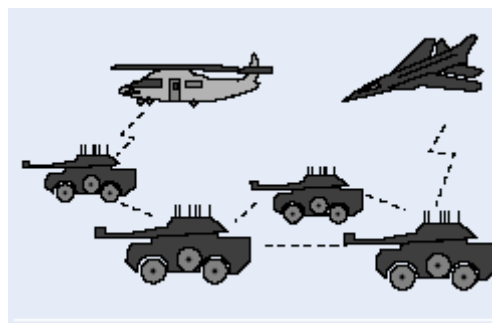
۴-۶-۱- کاربرد شبکه های اقتضایی بیسیم

شبکه های بیسیم اقتضایی هر جا که ساختار ارتباطی اندکی وجود داشته یا هیچ ساختار ارتباطی وجود ندارد و یا ایجاد ساختار از نظر اقتصادی مناسب نیست بکار گرفته می شوند. شبکه های بیسیم اقتضایی، دستگاه های کامپیوتری را قادر می سازند تا در حال حرکت نیز ارتباط خود با شبکه را حفظ کرده و همچنین به آسانی به شبکه وارد یا از آن خارج گردند. تنوع کاربردهای شبکه های بیسیم اقتضایی، از شبکه های سیار با پویایی بالا و با مقیاس بزرگ تا شبکه های ایستا و کوچک گسترده شده است. گذشته از کاربردهایی که از شبکه های ثابت و دارای ساختار معمولی به محیط بیسیم اقتضایی آمده اند،

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

سرویس ها و کاربردهای جدید بسیاری می توانند برای محیط اقتضایی ایجاد شوند. برخی از کاربردهای شبکه های بیسیم اقتضایی عبارتند از:

الف) محیط های نظامی (میدان جنگ) : شبکه های بیسیم اقتضایی ارتش را قادر می سازد تا بتوانند از تکنولوژی شبکه در منطقه نبرد استفاده نموده و یک شبکه اطلاعاتی بین سربازان، خودروها و مرکز فرماندهی اطلاعات ارتش فراهم سازند. بسیاری از تجهیزات نظامی کنونی مجهز به تکنولوژی ارتباط کامپیوتری است. شکل (۴-۱۹) مثالی از کاربرد نظامی شبکه های بیسیم اقتضایی بیسیم را نشان می دهد.



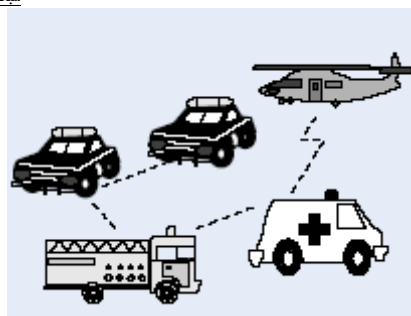
شکل (۴-۱۹): کاربرد نظامی شبکه های اقتضایی

ب) محیط های تجاری : شبکه های بیسیم اقتضایی می توانند بطور مستقل و سریع بین کامپیوترهای کیفی یا جیبی شبکه را تشکیل داده و ارتباط را برقرار نموده و اطلاعات را بین اعضا به اشتراک بگذارند. کاربرد دیگر ممکن است در شبکه های شخصی (PAN)^۱ باشد زمانی که می خواهیم برای تبادل اطلاعات، بین چند دستگاه کامپیوتری مستقیماً ارتباط برقرار کنیم، شبکه های شخصی یک زمینه کاربرد نویدبخش از شبکه های بیسیم اقتضایی در تکنولوژی آینده می باشند.

ج) عملیات نجات/ اضطراری : شبکه های بیسیم اقتضایی می توانند در عملیات های نجات/ اضطراری ، برای کمک به پرسنل در حال امداد رسانی در حوادثی مانند اطفاء حریق ، زلزله ، سیل و ... مورد استفاده قرار گیرند. عملیات نجات/ اضطراری همیشه در جاییکه ساختار ارتباطی شبکه سیمی وجود ندارد یا آسیب دیده، انجام می شود و نیاز به تشکیل سریع شبکه ارتباطی وجود دارد تا اطلاعات از یک عضو تیم نجات به عضو دیگر روی یک کامپیوتر جیبی انتقال یابد. شبکه های اقتضایی در عملیات های پلیسی نیز استفاده می گردند. شکل (۴-۲۰) مثالی از کاربرد در عملیات نجات/ اضطراری را نشان می دهد.

^۱ Personal Area Networks

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۴-۲۰): کاربرد شبکه های اقتضایی سیار در عملیات نجات/اضطراری

انواع ترافیک در شبکه های بیسیم اقتضایی کاملاً متفاوت از ترافیکهای موجود در شبکه های بیسیم معمولی که دارای زیر ساخت می باشند است. این ترافیک ها شامل موارد زیر می باشند:

- **ترافیک های همتا به همتا:** ارتباط بین دو نود که یک پرسش بین آنها قرار می گیرد. این نوع ترافیک شبکه معمولاً ثابت است.
- **ترافیک های انتها به انتها:** ارتباط بین دو نود فراتر از یک پرسش است اما یک مسیر پایدار بین آنها نگهداری می شود. دلیل این مسئله این است که چندین نود در یک منطقه در محدوده ارتباطی یکدیگر باقی می ماندند یا احتمالاً به صورت گروهی حرکت می کنند. این نوع ترافیک شبیه ترافیک استاندارد شبکه است.
- **ترافیک های پویا:** هنگامی اتفاق می افتد که نودها به طور پویا و تصادفی حرکت می کنند. مسیرها باید دوباره تشکیل شوند که پیامد آن اتصال نودها به صورت ضعیف^۱ می باشد.

۴-۶-۲- ویژگی های شبکه های اقتضایی بیسیم

شبکه های اقتضایی بیسیم دارای ویژگی ها و مشخصات مختص به خود می باشند. چندین ویژگی برجسته شبکه های اقتضایی عبارتند از :

الف) توپولوژی شبکه پویا: از آنجا که در شبکه های اقتضایی نود ها سیار هستند و می توانند آزادانه حرکت کنند، توپولوژی شبکه ممکن است سرعت و غیر قابل پیش بینی تغییر کند و در نتیجه ارتباطات بین ترمینال ها نیز با زمان تغییر کند. شبکه بیسیم اقتضایی باید با ترافیک و شرایط انتشار و همچنین الگوهای جابجایی نود های شبکه های سیار سازگار باشد. نود های سیار در شبکه همچنانکه حرکت می کنند مسیریابی بین خودشان را بطور پویا برقرار می کنند و شبکه را تشکیل می دهند. علاوه بر این یک کاربر در شبکه اقتضایی نه تنها درون شبکه اقتضایی فعالیت می کند بلکه ممکن است نیاز به دسترسی به شبکه ثابت عمومی (مانند اینترنت) نیز داشته باشند.

ب) نوسان ظرفیت اتصال : نرخ خطای بیت ارتباط بیسیم در شبکه های بیسیم اقتضایی از شبکه های سیمی بیشتر است، اما بر عکس پهنای باند آن کمتر است. یک مسیر انتها به انتها می تواند توسط چندین نشست به اشتراک گذاشته شود. در چنین شبکه هایی مسیر بین هر زوج کاربر ممکن است چندین ارتباط بیسیم را طی کند. درکل، توان مفید ارتباطات بیسیم، بعد از محاسبه تاثیر دسترسی های چندگانه، محوشدگی، نویز، تداخل و غیره، اغلب کمتر از بیشترین نرخ انتقال رادیویی است.

¹ loosed

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

ت) توان مصرفی : برخی یا همه نود های شبکه های بیسیم اقتضائی ، دستگاه های سیار با توانایی پردازش پایین ، حافظه و توان اندک بوده و به باتری های خود متکی هستند، به همین دلیل چنین دستگاه هایی نیاز به الگوریتم و مکانیزم های بهبود یافته ای برای بهینه سازی مصرف توان دارند و تمام لایه های پشته ی پروتکل باید به مصرف توان توجه نمایند.

ج) ترمینال مستقل : در شبکه های بیسیم اقتضائی، هر ترمینال سیار یک نود مستقل است که ممکن است هم به عنوان میزبان و هم مسیریاب عمل نماید. به عبارت دیگر، نود های سیار در کنار توانایی پردازش به عنوان یک میزبان ، می توانند توابع مسیریابی را به عنوان مسیریاب اجرا نمایند.

د) عملیات توزیع شده : از آنجا که کنترل مرکزی در فعالیت های شبکه وجود ندارد ، کنترل و مدیریت شبکه در بین ترمینال ها توزیع شده است . گرده هایی که در یک شبکه اقتضائی قرار دارند باید بین خود همکاری داشته باشند تا فعالیت های امنیتی و مسیریابی پیاده سازی گردد.

و) مسیریابی چندپرشه : انواع الگوریتم های مسیریابی اقتضائی مبتنی بر تفاوت ویژگی های لایه ی اتصال و پروتکل های مسیریابی می توانند تک پرشی یا چندپرشی باشند، شبکه اقتضائی یک پرشی از لحاظ ساختار و پیاده سازی ساده تر از چندپرشی می باشد. وقتی که مبدا و مقصد بیرون از دامنه ی انتقال بیسیم یکدیگر باشند بسته ها باید با استفاده از یک یا چند نود میانی هدایت شوند.

ی) امنیت محدود : معمولاً شبکه های بیسیم نسبت به شبکه های سیمی، بیشتر در معرض تهدیدهای امنیتی هستند زیرا امکان استراق سمع در این شبکه ها افزایش می یابد.

۴-۶-۳- چالش شبکه های اقتضائی بیسیم

بر خلاف شبکه های فیبر نوری و شبکه های سیمی ، ارتباطات بیسیم از هوا به عنوان رسانه انتقال استفاده می کنند و در نتیجه در معرض بسیاری از عوامل غیر قابل کنترل و موثر بر کارایی مانند شرایط جوی، موانع شهری (ساختمان ها) ، تداخل چندمسیری و جابجایی میزبان های بیسیم قرار دارند. صرفنظر از کاربردها، در شبکه های اقتضائی بیسیم چالش هایی مطرح می شود که باید به دقت مطالعه گردد ، این چالش ها شامل موارد ذیل هستند:

الف) مسیریابی : از آنجا که توپولوژی شبکه دائماً تغییر می کند و خطاهای ارتباطی موقتی و تغییرات مسیر بسیار رخ می دهد ، مفهوم مسیریابی بسته ها بین هر زوج نود یک امر چالش برانگیز خواهد بود . اغلب پروتکل ها باید به جای مسیریابی پیش گستر^۱ مبتنی بر مسیریابی واکنشی^۲ باشند . مسیریابی پخش فراگیر چالش دیگری است زیرا درخت پخش فراگیر به سبب جابجایی تصادفی نود ها درون شبکه خیلی ایستا نیست. مسیرهای بین نود ها ممکن است شامل چندین پرش باشند که نسبت به ارتباطات یک پرشی پیچیدگی بیشتری دارند.

ب) امنیت و قابلیت اطمینان : علاوه بر آسیب پذیری ارتباطات بیسیم، یک شبکه اقتضائی مشکلات امنیتی خاص مانند بسته های ارسالی توسط همسایه مهاجم را نیز دارد. خاصیت عملیات توزیع شده نیاز به الگوهای مختلف احراز اصالت و مدیریت کلید دارد. همچنین ویژگی های ارتباط بیسیم از قبیل دامنه محدود انتقال بیسیم، طبیعت پخش فراگیر رسانه بیسیم (مشکل ترمینال مخفی) گم شدن بسته ها ناشی از جابجایی و خطاهای انتقال داده ، مشکلات قابلیت اطمینان را بیشتر می کند.

پ) کیفیت سرویس (QoS)^۳ : ارائه سطوح مختلف کیفیت سرویس در یک محیط دائماً متغیر، چالش برانگیز خواهد بود زیرا ویژگی ذاتی کیفیت متغیر در شبکه های اقتضائی آنرا دشوارتر می سازد.

¹ Proactive

² Reactive

³ Quality of Service

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

ج) **ارتباطات بین شبکه ای**^۱: علاوه بر ارتباطات درون یک شبکه اقتضایی، در بسیاری از حالات نیاز به ارتباط بین شبکه ای بین شبکه بیسیم اقتضایی و شبکه ثابت داریم. پروتکل های مسیریابی در یک ترمینال سیار، چالشی برای مدیریت جابجایی نود ها به صورت هماهنگ می باشد.

د) **مصرف توان**: برای اغلب ترمینال های سیار، توابع مربوط به ارتباط باید برای مصرف توان بهینه سازی گردد، حفظ توان و مسیریابی با توجه به مصرف توان باید مورد توجه قرارگیرد. یک حقیقت که تمام شبکه های بیسیم دچار آن هستند نرخ خطای بیت بالا است، پروتکل TCP-Reno استاندارد در مواجهه با گم شدن بسته، اندازه پنجره ازدحام را به نصف کاهش می دهد. اگر این گم شدن بسته ناشی از ازدحام شبکه باشد، این رفتار ازدحام شبکه را برطرف می کند اما اگر علت گم شدن، خطای انتقال باشد کارایی کاهش خواهد یافت.

و) مسیریابی در شبکه های بیسیم اقتضایی: در شبکه های بیسیم اقتضایی، مسئله مسیریابی به علت وجود تحرک نودها و پویا بودن توپولوژی شبکه چالش بزرگی است. علاوه بر آن، نودهای شبکه های بیسیم اقتضایی معمولاً از لحاظ انرژی و قابلیت های محاسباتی و محدوده ارتباطی ضعیف هستند. سه روش عمومی برای مسیر یابی در شبکه های بیسیم اقتضایی وجود دارند. همه این سه نوع روش یک هدف دارند و آن اینست که زمانی که یک مبدأ می خواهد بسته ای را به مقصدی بفرستد، مسیر صحیحی وجود داشته باشد. به علت اختلاف در روشها، هر کدام مزایا و معایب خاص خود را دارند و خصوصیات مختلف شبکه به شیوه های متفاوتی بر آنها تاثیر می گذارد.

پرسش های فصل

۱. انواع باندهای فرکانسی را نوشته و کاربرد هریک را ذکر نمایید.
۲. منظور از شعاع موثر سرویس در شبکه های بیسیم را توضیح دهید.
۳. کاربرد تسهیم سازی فرکانسی را در شبکه های بیسیم توضیح دهید.
۴. شبکه های بیسیم به چند دسته تقسیم می شوند؟ مثالی از کاربرد هر دسته را بنویسید.
۵. مفهوم پدیده handoff را نوشته و با رسم شکل توضیح دهید.
۶. مزایای عمده شبکه های محلی بیسیم را تشریح نمایید.
۷. موارد کاربرد شبکه های محلی بیسیم را بنویسید.
۸. مشکلات عمده فن آوری امواج رادیویی و روش های حل آنها را در شبکه های محلی بیسیم توصیف نمایید.
۹. عملکرد روش DS را در شبکه های محلی بیسیم تشریح نمایید.
۱۰. عملکرد روش FH را در شبکه های محلی بیسیم تشریح نمایید.
۱۱. روش مدولاسیون سیگنال حامل و روش مدولاسیون مستقیم را در سیستم های بیسیم با فن آوری امواج مادون قرمز تشریح نمایید.
۱۲. ساختار شبکه های محلی بیسیم همتا به همتا را تشریح نمایید.
۱۳. فاکتورهای مهم انتخاب شبکه های محلی بیسیم را از دیدگاه مشتریان ذکر نمایید.
۱۴. پشته پروتکل 802.11 را رسم کرده و توضیح دهید.
۱۵. چند نمونه از کاربردهای اصلی شبکه های MANET را توضیح دهید.

¹ Internetworking

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

۱۶. تفاوت شبکه های MANET ساختار یافته و بی ساختار را توضیح دهید.

۱۷. ویژگی های اصلی شبکه های MANET را توضیح دهید.

۱۸. چالش های موجود در شبکه های MANET را ذکر کنید.

فصل پنجم

شبکه های حسگر بیسیم^۱

۵-۱- مقدمه

پیشرفتهای اخیر در کوچک سازی، طراحی مدارهای کم مصرف و تجهیزات ارتباطی بیسیم ساده و کم مصرف و نیز توسعه شرکت های تولید کننده منابع انرژی کوچک به همراه کاهش هزینه های تولید کارخانه ای موجب ایجاد دیدگاه فناوریک جدیدی با نام شبکه های حسگر بیسیم گردید. پیشرفت فناوری های MEMS، ارتباطات بیسیم و الکترونیک دیجیتال، امکان ساخت نود های حسگر کم هزینه، با مصرف کم، چند منظوره و در اندازه های کوچک را برای ارتباط در فواصل کوتاه فراهم ساخته است. این حسگرهای کوچک که شامل حسگر، واحد پردازش و واحد ارتباط می باشند، ایده شبکه های حسگر بیسیم را بر مبنای همکاری و هماهنگی تعداد زیادی از این نود ها ایجاد نموده اند. این شبکه ها، حداقل امکانات محاسباتی و برخی ابزارهای حسی را برای حس محیط پیرامونی خود در قالب نوع جدیدی از شبکه ها که بصورت گسترده در محیط قرار می گیرند بکار می برند. از حسگرها برای حس پارامترهایی نظیر دما، نور، لرزش، صدا، تابش، رطوبت و ... استفاده می شود. یک شبکه حسگر از تعداد زیادی نود های حسگر تشکیل شده که بصورت مترامی در اطراف پدیده فیزیکی مورد نظر پخش شده اند. نکته مهم در مورد شبکه های حسگر بیسیم این است که نیاز نیست مکان حسگرها کاملاً مهندسی شده باشد؛ این خاصیت در کاربردهایی که امکان چینش حسگرها وجود ندارد یا اینکه امکان تغییر محل آنها وجود دارد از اهمیت زیادی برخوردار است. نکته مهم دیگر در شبکه های حسگر بیسیم همکاری جمعی نود های حسگر می باشد. نود های حسگر شامل واحد پردازش می باشند، در نتیجه بجای ارسال داده خام به مقصد، از پردازنده خود استفاده کرده و بر روی داده ارسالی، محاسباتی در حد توان خود انجام می دهند و تنها قسمت های مورد نیاز داده مورد نظر را ارسال می نمایند. خصوصیتی که از شبکه های حسگر بیسیم ذکر گردید امکان پشتیبانی از کاربردهای زیادی را به وجود می آورد. بعنوان مثال می توان به کاربرد در موارد سلامت، صنایع نظامی، امنیت و ... اشاره کرد. در واقع می توان گفت شبکه های حسگر، کاربر نهایی را نسبت به محیط اطراف خود هوشمندتر و آگاه تر می سازد.

در شکل (۵-۱) نمونه ای از حسگرهای مختلف نشان داده شده است.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۵-۱): نمونه ای از حسگرهای مختلف

شناخت شبکه های حسگر بیسیم نیاز به شناخت تکنیک های شبکه های MANET دارد؛ با این وجود اکثر پروتکل ها و الگوریتم هایی که برای شبکه های MANET طراحی شده اند بطور کامل برای شبکه های حسگر بیسیم مناسب نمی باشند. تفاوت میان شبکه های حسگر بیسیم و شبکه های MANET عبارتند از:

- تعداد نودهای حسگر در شبکه های حسگر چندین برابر نودها در شبکه های MANET می باشد.
- حسگرها بسیار متراکم تر استفاده می شوند.
- حسگرها در مقابل مشکلات مقاومتر هستند.
- توپولوژی شبکه های حسگر بسیار پویاتر است.
- نود های حسگر از ارتباط همه پخشی استفاده می کنند در حالیکه شبکه های MANET از ارتباطات نقطه به نقطه استفاده می نمایند.
- نود های حسگر دارای محدودیت در توان مصرفی، تواناییهای محاسباتی و حافظه می باشند.
- نود های حسگر دارای شناسه عمومی نمی باشند و این به دلیل تعداد زیاد نود ها و حجم زیاد سر بار می باشد.

۵-۲- خصوصیات مهم شبکه های حسگر بیسیم

خصوصیات مهم شبکه های حسگر بیسیم به شرح زیر می باشد:

- **وابسته به کاربرد:** به دلیل ادغام فناوری های حسگر، پردازش و ارتباطات؛ محدوده وسیعی از کاربردها امکان پیاده سازی در شبکه های حسگر بیسیم را دارند. اما باید توجه نمود که نمی توان برای تمام کاربردها یک سناریو را اجرا نمود، بلکه هر کاربرد پیکربندی و پروتکل مخصوص به خود را نیاز دارد. به عنوان مثال شبکه های حسگر با تراکم پایین از حسگرها و نیز با تراکم بالایی از حسگرها کار می کنند در حالیکه پروتکل های ایندو حالت بسیار با یکدیگر متفاوت می باشند.
- **تعامل با محیط:** بدلیل تعامل شبکه های حسگر با محیط اطرافشان، خصوصیات ترافیکی آنها با دیگر شبکه های موجود متفاوت می باشد. بطور معمول شبکه های حسگر دارای ترافیکی با نرخ پایین می باشند، اما در مواقعی که پدیده مورد نظر روی می دهد دارای ترافیک انفجاری می گردند.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

- **مقیاس پذیری:** بصورت تئوری، شبکه های حسگر نسبت به شبکه های MANET دارای تعداد بسیار بیشتری نهاد می باشند که نیاز به راه حلهایی متفاوت و مقیاس پذیرتر دارند.
- **انرژی:** مشابه با بعضی انواع شبکه های MANET، منابع انرژی محدود بوده و مصرف انرژی مهمترین معیار برای پیکره بندی آنها می باشد. در بعضی موارد، باتری موجود در نود های حسگر قابل شارژ دوباره نمی باشد و به همین دلیل نیاز به طول عمر بیشتر حسگر می باشد.
- **خود پیکربندی:** مشابه با شبکه های MANET شبکه های حسگر نیاز به خود پیکربندی برای دارا بودن شبکه ای پیوسته دارند، اما بدلیل تفاوت در ترافیک و انرژی مصرفی روشهای متفاوتی مورد نیاز می باشد. به همین دلیل نود های حسگر نیاز به درک محل جغرافیایی خود دارند.
- **قابلیت اطمینان و کیفیت سرویس:** شبکه های حسگر بیسیم، مفاهیم متفاوتی از قابلیت اطمینان و کیفیت سرویس را ارائه می نمایند. در حال حاضر سرویسهایی که شبکه های حسگر ارائه می دهند کاملاً مشخص نمی باشد. در بعضی موارد ارسال عادی بسته کافی بوده و در بعضی موارد نیاز به اطمینان بسیار بالا در ارسال داریم. نرخ ارسال بسته معیار کاملی نمی باشد، مسئله مهم مقدار و کیفیت اطلاعات ارسالی به نود چاهک^۱ مورد نظر در مورد پدیده مشاهده شده می باشد.
- **داده محور:** در اکثر کاربردهای شبکه های حسگر، با استفاده افزونه از نود های حسگر می توان از منابع انرژی ضعیف تر و ارزانتر استفاده نمود. مورد مهمتر این است که این نود ها چه اطلاعاتی را مشاهده می نمایند. این تغییر در اولویتها ما را نیازمند تغییر در شبکه از نود محور به داده محور می نماید.
- **سادگی:** بدلیل کوچک بودن نود ها و محدود بودن انرژی، نرم افزار مورد استفاده در سطح شبکه و نود ها باید بسیار ساده تر از نرم افزارهای امروزی باشند. این سادگی نیاز به تغییر در لایه های استاندارد شبکه دارد. هنگامی که تعداد زیادی از نود های حسگر بصورت متراکم در کنار هم قرار گرفته باشند، نود های همسایه بسیار به یکدیگر نزدیک خواهند بود؛ در نتیجه ارتباط چند پرشه در شبکه های حسگر در مقایسه با ارتباطات مرسوم تک پرشه بسیار انرژی کمتری مصرف می نماید. بنابراین میزان انرژی که برای ارتباطات استفاده می گردد پایین می آید. یکی از مهمترین محدودیتهای موجود در نود های شبکه های حسگر، کمبود منابع انرژی می باشد. نود های حسگر معمولاً حاوی منابع انرژی محدود و غیر قابل تقویتی می باشند. بنابراین بر خلاف شبکه های قدیمی که دسترسی به کیفیت سرویس هدف اصلی می باشد، در پروتکل های شبکه های حسگر تکیه بر مصرف بهینه منابع می باشد. نود ها باید مکانیزمهای تعادلی که به کاربر نهایی امکان افزایش طول عمر شبکه را از طریق پهنای باند کمتر یا افزایش تاخیر ارسال می دهد را در خود ایجاد نمایند.

۵-۳- کاربردهای شبکه های حسگر

شبکه های حسگر شامل مدلهای مختلفی از حسگرها از قبیل دماسنج، تصویری، مادون قرمز، صوتی و رادار می باشند که توانایی مانیتور کردن انواع شرایط مختلف را دارند. شرایط ذکر شده عبارتند از: دما، رطوبت، حرکت، نور، فشار، ترکیبات تشکیل دهنده، سطح اختلالات، وجود یا عدم وجود بعضی اشیاء و خصوصیات جاری از قبیل سرعت، جهت، اندازه و ...

نود های حسگر در دریافت های پیوسته، دریافت پدیده ها، تشخیص پدیده ها، تعیین محل و کنترل محلی عامل ها مورد استفاده قرار می گیرند. مفهوم حسگرهای کوچک و ارتباطات بیسیم میان آنها زمینه های کاربردی جدیدی را پیش رو قرار داده است. کاربردهای این شبکه ها در دسته های نظامی، محیطی، بهداشتی و دیگر موارد تجاری تقسیم بندی می شود.

¹ Sink

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

دسته هایی از جمله اکتشاف فضایی، پردازش شیمیایی و پیش بینی بلایای طبیعی نیز با توجه کمتری قابل بررسی می باشند. در ادامه بعضی از کاربردهای شبکه های حسگر بصورت خلاصه ارائه می شوند.

• کاربردهای نظامی شامل:

- مانیتور کردن نیروهای خودی
- نظارت منطقه جنگی
- شناسایی نیروهای مقابل و منطقه مورد استفاده دشمن
- هدف گیری
- تخمین و بررسی خسارات نبرد
- شناسایی و کشف حملات شیمیایی، بیولوژیکی و هسته ای

• کاربردهای محیطی شامل:

- بررسی جابجایی حیوانات
- مانیتور کردن شرایط محیط
- شناسایی آتش جنگلها
- کشف و نگاشت پیچیدگیهای بیولوژیکی
- شناسایی زمین های مستعد

• کاربردهای بهداشتی شامل:

- مانیتور کردن وضعیت بیماران
- ردیابی و مانیتور کردن بیماران و پزشکان در محیط بیمارستان
- مدیریت دارو در بیمارستانها

• کاربردهای خانگی شامل:

- اتوماسیون خانه
- محیط هوشمند

• دیگر کاربردهای تجاری شامل:

- کنترل محیطی در ساختمانهای کاری (تهویه مطبوع و ...)
- موزه های تعاملی
- شناسایی و ردیابی دزدان ماشین
- کنترل و مدیریت کارخانجات
- شناسایی و ردیابی وسایل نقلیه

در طراحی شبکه های حسگر عوامل متعددی نظیر: توانایی تحمل خطا، مقیاس پذیری، هزینه تولید، محدودیتهای سخت افزاری، رسانه مورد استفاده در تبادلات، توپولوژی ، محیط ومصرف انرژی تاثیر مهمی دارند.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

۴-۵- گذشته، حال و آینده شبکه های حسگر

همانند بسیاری دیگر از فناوری ها، کار بر روی شبکه های حسگر از کارهای نظامی و دفاعی آغاز شد. در طول جنگ سرد، دولت آمریکا، حمایت از پروژه های به نام سیستم نظارت صوتی^۱ را بر عهده گرفت. در این پروژه با قرار دادن تعدادی حسگر در نقاط استراتژیک زیر اقیانوس، سعی در تشخیص نفوذ و ردیابی زیر دریایی های شوروی داشتند.

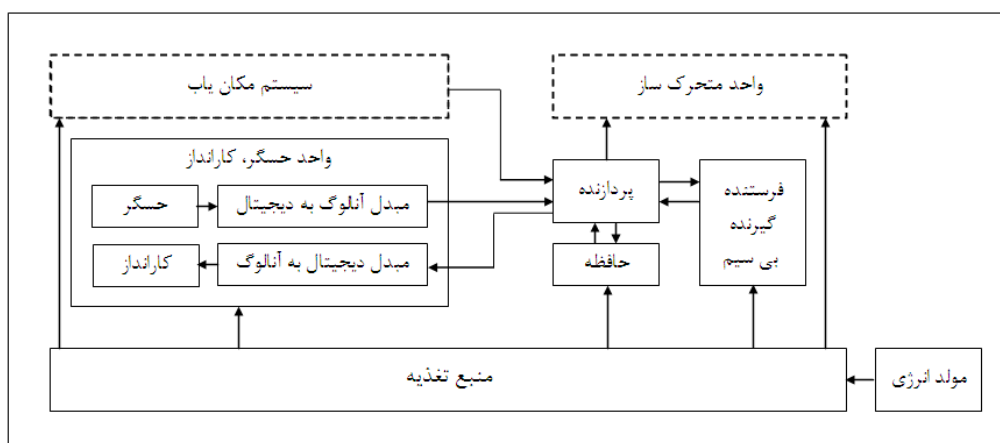
کار بر روی شبکه های حسگر بطور جدی از سال ۱۹۸۰ و با پروژه شبکه های حسگر توزیع شده در آژانس پروژه های تحقیقات دفاعی پیشرفته آمریکا آغاز شد. پروژه WINS در سال ۱۹۹۳ و با همکاری دانشگاه کالیفرنیا و مرکز علوم شرکت Rockwell شروع شد. این پروژه در سال ۱۹۹۸ به یک محصول تجاری تبدیل شد. در حدود سال ۱۹۹۹ دانشگاه برکلی دو پروژه تحقیقاتی بر روی شبکه های حسگر آغاز کرد. پروژه PicoRadio و پروژه Smart Dust یک پروژه کاملاً بلند پروازانه بود و هدف آن ساختن گره های حسگری با ابعاد یک میلیمتر مکعب بود که البته به موفقیت هایی هم رسید. برای داشتن تصور بهتر از ابعاد یک حسگر می توان گفت که این حسگرها چنان کوچک هستند که می توانند همانند گرد و غبار بوسیله جریان هوا جابجا شوند.

در سال های اخیر پروژه های بسیار دیگری مانند پروژه μ AMPS در دانشگاه MIT و پروژه SenseIT توسط آژانس پروژه های تحقیقات دفاع پیشرفته آمریکا در حال انجام است و تحقیقات در این زمینه با شتاب روز افزونی در مجامع علمی و تحقیقاتی در حال گسترش است.

شبکه های حسگر یکی از فن آوری های نوینی است که بسیاری از دانشمندان عقیده دارند، آینده بشر را تغییر خواهد داد. این فن آوری به خاطر مزایا و کاربردهای بسیاری که در زمینه های مختلف دارد، جزء فن آوری های استراتژیک بسیاری از کشورها محسوب می شود. در دسامبر ۱۹۹۹ مجله Business Week شبکه های حسگر جز یکی از مهم ترین فن آوری های قرن ۲۱ معرفی کرد که آینده بشر را تحت تاثیر قرار می دهد. در بررسی دیگری که توسط شرکت ON Work انجام شده پیش بینی می شود که تعداد گره های حسگر در سال ۲۰۱۰ به ۴۶۵ میلیون برسد و این در حالی است که در سال ۲۰۰۳ تعداد گره های حسگر موجود در جهان تنها ۳ میلیون عدد تخمین زده شده است.

۵-۵- معماری شبکه های حسگر بیسیم

یک نود حسگر از چهار جزء اصلی تشکیل شده است. شکل (۵-۲) این چهار جزء را نمایش می دهد که عبارتند: حسگر، واحد پردازش، واحد فرستنده/گیرنده و منبع تغذیه.



¹ Sound Surveillance System(SOSUS)

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

شکل (۵-۲): اجزاء یک نود حسگر

علاوه بر اجزاء ذکر شده، بسته به کاربرد مورد نظر اجزاء دیگری نیز در یک نود حسگر وجود دارند. این اجزاء عبارتند از سیستم تعیین کننده مکان، تولید کننده انرژی و موتور محرک مکان. واحد حسگر معمولاً از ۲ بخش تشکیل شده است: حسگر و مبدل آنالوگ به دیجیتال. موج آنالوگ توسط حسگرها بر مبنای پدیده مشاهده شده ایجاد می گردد و پس از آن توسط مبدل به سیگنال دیجیتال تبدیل شده و در نهایت در اختیار واحد پردازش قرار می گیرد. واحد پردازش که معمولاً دارای حافظه داخلی می باشد روالهایی که وظیفه نود را در همکاری با دیگر نود های شبکه اجرا می نمایند را مدیریت می کند. واحد فرستنده/گیرنده وظیفه ارتباط نود با شبکه را بر عهده دارد. از مهمترین واحدهای یک نود حسگر منبع تغذیه می باشد. منبع تغذیه امکان دارد توسط واحدی دیگر مانند سلول خورشیدی تقویت گردد. اکثر تکنیکهای مسیریابی و عملیات دریافت پدیده ها نیاز به اطلاع از محل نود با دقتی بالا دارند. در نتیجه نود های حسگر معمولاً دارای سیستم تعیین محل می باشند. محرک^۱ هم در برخی موارد برای اجرای وظایف نود مورد نیاز آن می باشد؛ وظیفه آن تغییر محل نود می باشد. با توجه به اجزاء ذکر شده، یک نود حسگر که تمام موارد فوق را در یک مجموعه در اختیار دارد دارای محدودیتهای زیر می باشد:

- باید انرژی مصرفی بسیار پایینی داشته باشد.
- باید بتواند در محیطهای با تراکم بالای حسگر عمل نماید.
- باید هزینه تولید آن پایین باشد.
- باید مستقل بوده و بدون مراقبت به عمل خود ادامه دهد.
- باید قابلیت انطباق با محیط را داشته باشد.

به این دلیل که اکثر نود های حسگر خارج از دسترس هستند طول عمر نود و شبکه وابسته به منابع انرژی نود می باشد. همچنین منبع تغذیه به واسطه اندازه محدودی که دارد از نظر قدرت و توان محدود می باشد. در دسته بندی دیگری برای یک نود حسگر ۴ جزء: ریزپردازنده، فرستنده/گیرنده، منبع تغذیه و سیستم عامل را در نظر می گیرند.

۵-۶- ساختار کلی شبکه های حسگر

قبل از ارائه ساختار کلی شبکه های حسگر، ابتدا برخی از تعاریف کلیدی به صورت زیر ارائه می گردند:

حسگر : وسیله ای که وجود شیء، رخداد یک وضعیت یا مقدار یک کمیت فیزیکی را تشخیص داده و به سیگنال الکتریکی تبدیل می کند. حسگر انواع مختلف دارد، مانند حسگرهای دما، فشار، رطوبت، نور، شتاب سنج، مغناطیس سنج و...
کارانداز : با تحریک الکتریکی، یک عمل خاص مانند باز و بسته کردن یک شیر یا قطع و وصل یک کلید را انجام می دهد.
نود حسگر: به نودی گفته می شود که فقط شامل یک یا چند حسگر باشد.
نود کارانداز: به نودی گفته می شود که فقط شامل یک یا چند کارانداز باشد.
نود حسگر کارانداز: به نودی گفته می شود که مجهز به حسگر و کارانداز باشد.

¹ Mobilizer

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

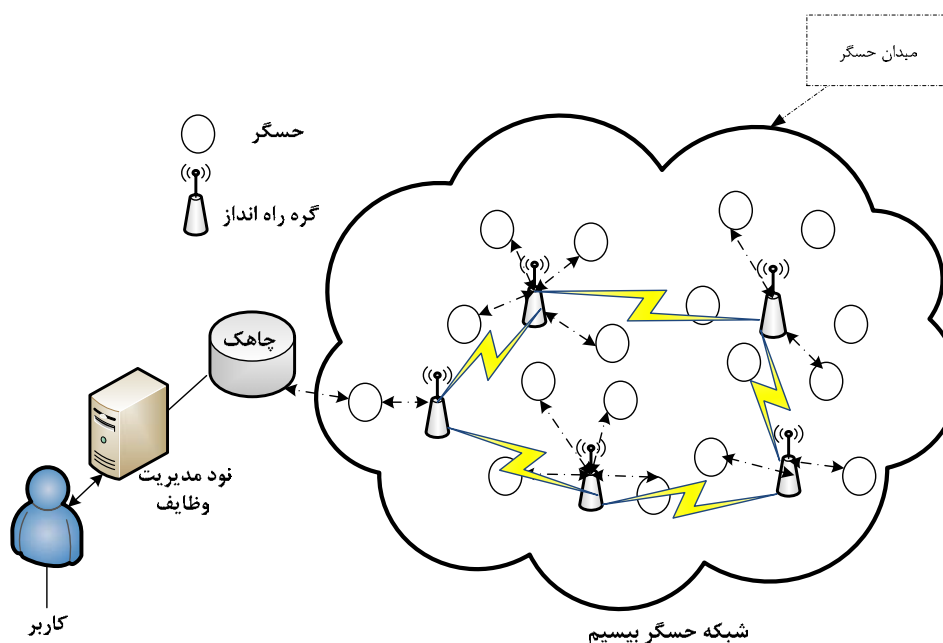
شبکه حسگر : شبکه ای که فقط شامل نود های حسگر باشد. این شبکه نوع خاصی از شبکه حسگر می باشد. در کاربردهایی که هدف جمع آوری اطلاعات و تحقیق در مورد یک پدیده می باشد ، استفاده می شود؛ مانند مطالعه بر روی گردبادها وسایر پدیده های محیطی.

میدان حسگر، کارانداز: ناحیه کاری که نود های شبکه حس و کار در آن توزیع میشوند.

چاهک: نودی که جمع آوری داده ها را به عهده داشته و ارتباط بین نود های حسگر و نود مدیر وظیفه^۱ را برقرار می کند.

نود مدیر وظیفه: نودی که شخصی بعنوان کاربر یا مدیر شبکه از طریق آن با شبکه ارتباط برقرار می کند. فرامین کنترلی و پرس و جو ها از طریق این نود به شبکه ارسال شده و داده های جمع آوری شده به آن بر می گردد.

شبکه حسگر، کار: شبکه ای متشکل از نود های حسگر و کار انداز است که حالت کلی شبکه های مورد بحث می باشد. به عبارت دیگر شبکه حسگر شبکه ای است با تعداد زیادی نود، که هر نود می تواند در حالت کلی دارای تعدادی حسگر و تعدادی کارانداز باشد. در حالت خاص یک نود ممکن است فقط حسگر یا فقط کارانداز باشد. نود ها در ناحیه ای که میدان حسگر نامیده می شود با چگالی زیاد پراکنده می شوند. یک چاهک مانیتورینگ کل شبکه را بر عهده دارد. اطلاعات بوسیله چاهک جمع آوری می شود و فرامین نیز از طریق آن منتشر می شوند. شکل (۳-۵) ساختار کلی شبکه های حسگر را نمایش می دهد. مدیریت وظایف می تواند متمرکز یا توزیع شده باشد. بسته به اینکه تصمیم گیری برای انجام واکنش در چه سطحی انجام شود، دو ساختار مختلف خودکار و نیمه خودکار وجود دارد. ترکیب این دو روش نیز قابل استفاده است.



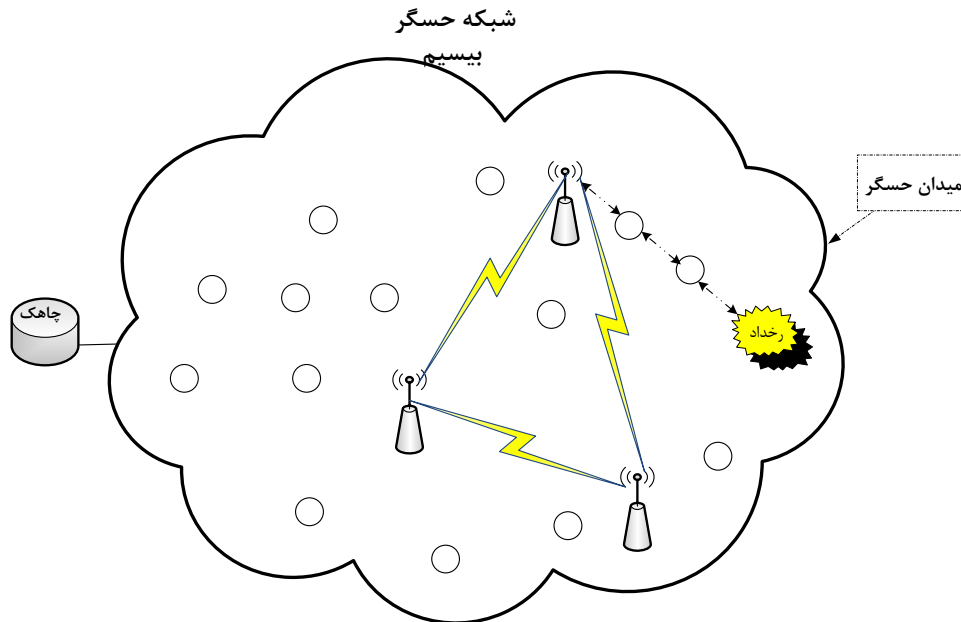
شکل (۳-۵): ساختار کلی یک شبکه حسگر

ساختار خودکار : حسگر هایی که یک رخداد یا پدیده را تشخیص می دهند، داده های دریافتی را به نود های کارانداز جهت پردازش و انجام واکنش مناسب ارسال می کنند. نود های کارانداز مجاور با هماهنگی یکدیگر تصمیم گیری کرده و عمل می نمایند. در واقع هیچ کنترل متمرکزی وجود ندارد و تصمیم گیری ها بصورت محلی انجام میشود. شکل (۴-۵) ساختار شبکه های حسگر خودکار را نمایش می دهد.

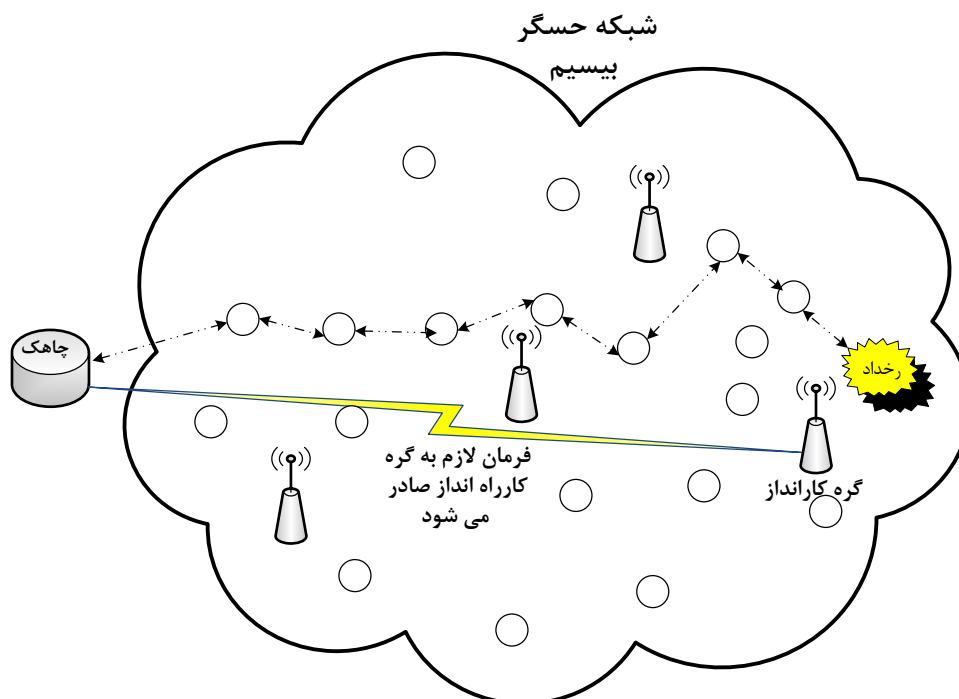
¹ Task manager node

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

ساختار نیمه خودکار: در این ساختار، داده ها توسط نود ها به سمت چاهک هدایت شده و فرمان از طریق چاهک به نود های کار انداز صادر می شود. شکل (۵-۵) ساختار نود های نیمه خودکار را نمایش می دهد.



شکل (۵-۴): ساختار خودکار



شکل (۵-۵): ساختار نیمه خودکار

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

از طرف دیگر در کاربردهای خاصی ممکن است از ساختار بخش بندی شده یا سلولی استفاده شود که در هر بخش یک سردهسته^۱ وجود دارد که داده های نود های دسته خود را به چاهک ارسال می کند. در واقع هر سردهسته مانند یک دروازه^۲ عمل میکند.

۵-۷- توپولوژی شبکه های حسگر

وجود نود های دست نیافتنی و غیر قابل نگهداری که مستعد بروز خطا هستند در شبکه های حسگر به مسئله پشتیبانی از توپولوژی اهمیت خاصی می دهد. صدها یا هزارها نود حسگر در منطقه مورد نظر با فاصله ای کم از یکدیگر قرار می گیرند. با توجه به تراکم نود ها و مستعد خطا بودن آنها، نیاز به دقت فراوان در نگهداری توپولوژی وجود دارد. نود های حسگر را می توان دسته جمعی یا تک تک در سر جایشان قرار داد. نود ها را می توان:

- توسط هواپیما در محیط مورد نظر پخش کرد.
- توسط موشک، توپ یا راکت پخش نمود.
- درون یک کارخانه قرارداد.
- توسط انسان یا ربات قرار داد.

با توجه به دسترس ناپذیر و غیر قابل نگهداری بودن نود ها، انتظار می رود در هنگام جایگذاری نود ها به شیوه ای مهندسی عمل نماییم. جایگذاری مورد نظر بایستی:

- هزینه جایگذاری را کاهش دهد.
- نیاز به پیش سازماندهی و برنامه ریزی قبلی نداشته باشد.
- در جایگذاری انعطاف وجود داشته باشد.
- خود سازماندهی و ظرفیت تحمل خطا را در نود ها افزایش دهد.

پس از بکارگیری شبکه، توپولوژی به دلالی نظیر: مکان، قابلیت دسترسی، انرژی موجود، بروز خطا در نود، و جزئیات کاری تغییر می کند.

۵-۸- معماری شبکه

معماری شبکه به عنوان یک کل از دیدگاه های زیر قابل بررسی می باشد:

- معماری پروتکل ها که از دیدگاه کاربردها و انرژی اهمیت دارد.
- کیفیت سرویس، قابلیت اطمینان، افزونگی، عدم دقت در عمل حسگرها را باید در نظر گرفت.
- ساختار آدرس دهی در شبکه های حسگر بیسیم کاملاً با شبکه های عادی متفاوت می باشد. مقیاس پذیری و نیازمندیهای انرژی نیاز به یک ساختار free-address دارد. اعطای آدرس توزیع شده می تواند یک تکنیک باشد، هرگاه آدرسها در همسایه های ۲ پرشی یکتا باشند. ساختار آدرس دهی داده محور و جغرافیایی نیز مورد نیاز می باشد.
- تعریف خصوصیات شبکه های حسگر بیسیم و ظرفیت پردازش اطلاعات در شبکه توسط نود ها اهمیت زیادی دارد. این موضوع مربوط به تجمع داده ها از چندین حسگر است. زمانیکه قصد همگرایی در یک یا چند چاهک ،

¹ Cluster head

² Gateway

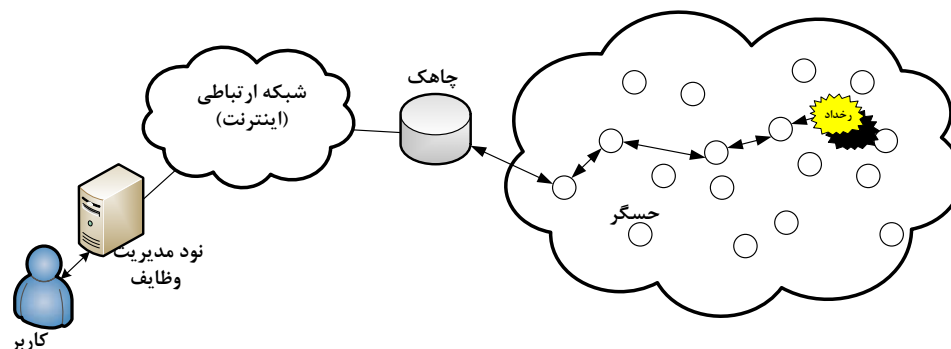
شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

- پردازش سیگنال توزیع شده یا بهره برداری از ساختار هماهنگ نود ها در احساس پدیده ها نیاز می باشد، از تکنیک های تجمیع داده ها استفاده می گردد. به علاوه تجمیع داده ها باعث کاهش تعداد بسته های ارسالی می گردد.
- بر پایه پردازش درون شبکه ای، سرویسهای که شبکه های حسگر بیسیم در سطح شبکه ارائه می کنند هنوز کاملاً مشخص نشده است. سرویس ها و عملیات، تنها انتقال بیت ها از یک نود به نود دیگر نمی باشد بلکه کار گسترده تر می باشد.
- زمانیکه سرویسهای شبکه بصورت جزئی یا کلی توسط نودهای خارج از شبکه حسگر درخواست گردند نیاز به مفهوم دروازه خواهیم داشت. اینکه چگونه شبکه های حسگر را بصورت لایه های عادی شبکه برای ارتباط با دیگر پروتکل های ارتباطی سازماندهی نماییم، هنوز موضوعی برای مطالعات بیشتر می باشد.
- در مدت زمان معین، امکان تغییر وظایف شبکه های حسگر بیسیم وجود دارد، یعنی تمام نود ها را با وظیفه جدید و نرم افزار عملیات مورد نظر آن پیکربندی کنیم.

۵-۹- معماری ارتباطات شبکه های حسگر

نود های حسگر معمولاً در منطقه هدف همانند آنچه که در شکل (۵-۶) نشان داده شده است، پخش می گردند.

شبکه حسگر بیسیم



شکل (۵-۶): نود های حسگر که در منطقه هدف پخش شده اند

هر کدام از نود های مورد نظر توانایی جمع آوری داده ها و مسیریابی آنها به نود چاهک و کاربر نهایی را دارند. داده ها از طریق معماری چند پرشی همانطور که در شکل (۵-۶) نمایش داده شده است، مسیریابی و ارسال می گردند. نود چاهک ممکن است از طریق ماهواره یا اینترنت با نود مدیریت وظایف ارتباط برقرار نماید.

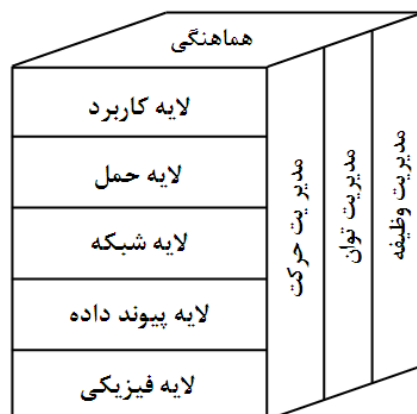
پروتکلی که توسط نود چاهک و دیگر نود ها استفاده می گردد در شکل (۵-۷) نمایش داده شده است. این پشته پروتکل بر مصرف انرژی و مسیریابی آگاه می باشد، داده ها را با پروتکل های شبکه یکپارچه می نماید، از طریق رسانه های بیسیم ارتباطی مناسب از لحاظ مصرف انرژی برقرار کرده و تلاشهای هماهنگ نود های شبکه را ارتقاء می بخشد. پروتکل مورد نظر شامل لایه کاربرد، لایه حمل، لایه شبکه، لایه پیوند داده و لایه فیزیکی می باشد. از دیدگاهی دیگر، پروتکل مذکور شامل سه صفحه مدیریت شامل: مدیریت مصرف انرژی، مدیریت تحرک و مدیریت وظایف می باشد.

انواع مختلفی از نرم افزارها وابسته به وظیفه شبکه حسگر در لایه کاربرد موجود می باشند. لایه حمل به پشتیبانی از جریان داده در صورتیکه شبکه حسگر بدان نیاز داشته باشد کمک می نماید. لایه شبکه به منظور حمایت از مسیریابی داده های ارسالی از لایه حمل مورد استفاده قرار می گیرد. هنگامیکه محیط دارای اختلالات زیادی باشد و نود ها امکان تحرک داشته باشند، پروتکل لایه MAC بایستی توجه خاصی بر روی مصرف انرژی داشته باشد و حداقل تداخلات را برای همه پخش

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

همسایه ها ایجاد نماید. لایه فیزیکی نیاز به تکنیک های مدولاسیون، ارسال و دریافتی ساده و قابل اطمینان دارد. به علاوه صفحات مدیریت مصرف انرژی، مدیریت تحرک و مدیریت وظایف، مصرف انرژی، تحرک و توزیع وظایف میان نود های حسگر را مانیتور می نمایند. این صفحات به نود های حسگر در اجرای وظایف خود به همراه مصرف انرژی کمتر در سطح شبکه کمک می کنند.

صفحه مدیریت انرژی چگونگی مصرف انرژی توسط نود را مدیریت می کند. بعنوان مثال، نود حسگر ممکن است پس از دریافت پیام از همسایه خود، گیرنده اش را خاموش نماید. این اقدام می تواند در جهت عدم دریافت مجدد پیام مورد نظر باشد؛ همچنین زمانیکه سطح انرژی نود حسگر پایین است می تواند به همسایه های خود اعلام کند که به علت کمبود انرژی نمی تواند در مسیریابی بسته ها مشارکت نماید، بلکه انرژی باقیمانده را برای احساس پدیده ها مورد استفاده قرار خواهد داد. صفحه مدیریت تحرک حرکت نود ها را شناسایی و ثبت می کند، در نتیجه مسیر بازگشتی به کاربر همواره حفظ شده و نود های حسگر همسایه های خود را همواره خواهند شناخت. نود های حسگر با شناخت همسایه هایشان می توانند میان اجرای وظایف و مصرف انرژی خود تعادل ایجاد نمایند؛ زیرا می دانیم که نیازی نیست تمام نود های حسگر مربوط به یک شبکه حسگر در یک لحظه فعال و در حال اجرای وظیفه خود باشند. در نتیجه بعضی نود ها بر پایه انرژی باقیمانده خود نسبت به دیگر نود ها کار بیشتری اجرا می کنند. با کمک صفحات مدیریت ذکر شده، نود های حسگر می توانند با یکدیگر در شرایطی کار کنند که انرژی کمتری مصرف گردد، داده ها مسیر یابی شود و منابع میان نود ها به اشتراک گذارده شود؛ بدون آنها هر نود حسگر بایستی بصورت انفرادی فعالیت نماید. از دیدگاه کلی، اگر نود های حسگر با یکدیگر همکاری داشته باشند می توانند در سطح شبکه انرژی کمتری استفاده کرده و طول عمر شبکه را افزایش دهند.



شکل (۵-۷): پشته پروتکل شبکه های حسگر

۵-۹-۱- لایه کاربرد

شبکه های حسگر جنبه های کاربردی متفاوتی دارند؛ دستیابی به این کاربردها از طریق اینترنت اهمیت تحقیقاتی زیادی دارد. طراحی پروتکل مدیریت لایه کاربرد مزایای فراوانی دارد. پروتکل های مدیریت لایه کاربرد، سخت افزار و نرم افزار را از دیدگاه کاربرد های شبکه های حسگر مخفی نگاه می دارند.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

مدیران سیستم ها از طریق پروتکل مدیریت لایه کاربرد با شبکه های حسگر ارتباط برقرار می کنند. بر خلاف دیگر شبکه ها، نود ها در شبکه های حسگر فاقد یک شناسه عمومی بوده و معمولاً فاقد ساختار مشخصی می باشند. بنابراین پروتکل مدیریت لایه کاربرد از طریق نام گذاری بر پایه خصوصیات و آدرس دهی بر پایه مکان به نود ها دسترسی می یابد.

- پروتکل مدیریت لایه کاربرد یک پروتکل مدیریتی است که عملیتهای نرم افزاری مورد نیاز برای وظایف مدیریتی زیر را فراهم می نماید:
- فراهم نمودن قوانین مربوط به تجمیع داده ها، آدرس دهی بر پایه خصوصیات و خوشه بندی برای نود های حسگر.
- تبادل داده های مربوط به الگوریتمهای شناسایی مکان.
- هماهنگ سازی زمانی نود های حسگر.
- تحرک نود های حسگر.
- فعال و غیر فعال کردن نود های حسگر.
- درخواست پیکربندی و وضعیت نود های شبکه های حسگر و پیکربندی دوباره شبکه حسگر.
- تصدیق هویت، پخش کلید و امنیت در تبادلات داده ای.

۵-۹-۲- لایه حمل

این لایه بصورت مخصوص هنگامیکه قصد ارتباط با شبکه حسگر از طریق دیگر شبکه ها از جمله اینترنت یا هر شبکه خارجی دیگر را داریم، مورد نیاز می باشد. تا کنون تلاش خاصی برای بیان جوانب مختلف درگیر با این لایه صورت نپذیرفته است. TCP با کمک مکانیزم پنجره ارسال خود با اکثر نیازمندیهای شبکه های حسگر هماهنگ می باشد. روشهایی مانند TCP Splitting برای تعامل شبکه های حسگر با شبکه هایی مانند اینترنت مورد نیاز می باشند. در این روش اتصال، TCP در نود های چاهک اتمام یافته و در ادامه پروتکلی مخصوص وظیفه ارتباطات میان نود چاهک و دیگر نود ها را بر عهده می گیرد. در نتیجه، ارتباط میان کاربر و نود چاهک توسط UDP یا TCP از طریق اینترنت یا ماهواره صورت می پذیرد و در سمت دیگر، ارتباط میان نود چاهک و دیگر نود ها بدلیل کمبود حافظه در نود های حسگر می تواند توسط پروتکلی شبیه به UDP انجام پذیرد.

بر خلاف پروتکل هایی مانند TCP، مدل ارتباطات انتها به انتها در شبکه های حسگر بر اساس آدرس دهی عمومی نمی باشد. این مدل ها بایستی بر پایه نامگذاری مبتنی بر خصوصیات برای تعیین مقصد بسته ها باشند. عواملی از جمله مصرف انرژی، مقیاس پذیری و خصوصیات مانده مسیریابی داده محور، نیاز به پروتکل های مختلف در لایه حمل دارد. در نتیجه این نیازمندیها احساس نیاز به پروتکل های لایه حمل جدید را افزایش می دهد.

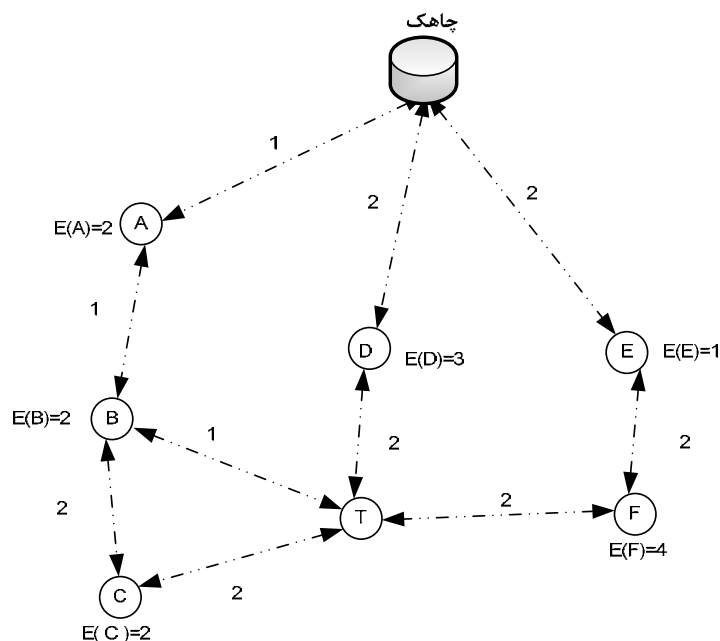
۵-۹-۳- لایه شبکه

نود های شبکه بصورت مترامی در نزدیکی محلهای مورد بررسی گسترده می گردند. نیاز به پروتکل های مسیریابی بیسیم چند پرشه میان نود چاهک و دیگر نود ها در این لایه به خوبی حس می شود. پروتکل های مورد استفاده در شبکه های MANET بصورت کامل برای شبکه های حسگر مناسب نمی باشند. لایه شبکه در شبکه های حسگر بر اساس اصول زیر طراحی می گردند:

- مصرف حداقل انرژی یکی از اصول مهم می باشد.
- شبکه های حسگر اکثراً داده محور می باشند.
- تجمیع داده ها تنها زمانی که مانعی برای تلاش جمعی نود های حسگر نباشد کارا می باشد.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

- شبکه حسگری که دارای آدرس دهی مبتنی بر خصوصیات و آگاه از مکان^۱ باشد شبکه ای ایده آل می باشد. یکی از روشهای موجود برای مسیریابی، انتخاب مسیری که از نظر مصرف انرژی مناسب است، می باشد. به عنوان مثال شبکه حسگر نشان داده شده در شکل (۵-۸) را در نظر بگیرید. در این شکل نود T نود مبدا حس کننده پدیده می باشد. اعداد نشان داده شده بر روی هر لینک رادیویی، نشان دهنده میزان انرژی لازم برای ارسال پیام از طریق آن لینک می باشد. مقدار تابع $E()$ نشان دهنده میزان انرژی باقیمانده در نود مورد نظر می باشد. به عنوان مثال $E(B)=2$ نشان دهنده این مطلب است که در نود حسگر B میزان ۲ واحد انرژی باقیمانده است. نود T می تواند از طریق ۴ مسیر زیر با نود چاهک ارتباط برقرار کند:



شکل (۵-۸): مسیرهای با مصرف انرژی مناسب

- مسیر ۱: T-B-A-Sink و $PA=4$ و $\alpha=3$
- مسیر ۲: T-C-B-A-Sink و $PA=6$ و $\alpha=6$
- مسیر ۳: T-D-Sink و $PA=3$ و $\alpha=4$
- مسیر ۴: T-F-E-Sink و $PA=5$ و $\alpha=6$

PA نشان دهنده انرژی موجود و α بیانگر انرژی مورد نیاز برای ارسال بسته از طریق مسیر مورد نظر می باشد. انتخاب مسیر مناسب از بین مسیرهای موجود، می تواند بر مبنای یکی از اصول زیر باشد:

- مسیری با حداکثر انرژی موجود: مسیری که حداکثر انرژی موجود را دارد را انتخاب می نماییم. PA نهایی مسیری با جمع انرژی باقیمانده در هر یک از نود های طول مسیر محاسبه می گردد. بر این اساس مسیر ۲ در شکل (۵-۸) انتخاب می گردد. مسیر ۲ شامل نود های مسیر ۱ علاوه یک نود اضافه می باشد. بنابراین با این وجود که این مسیر بالاترین PA را داراست، اما مسیر مناسب از نظر مصرف انرژی نمی باشد. با این شرایط مسیر ۴ را به عنوان مناسبترین مسیر از نظر میزان انرژی موجود انتخاب می نماییم.

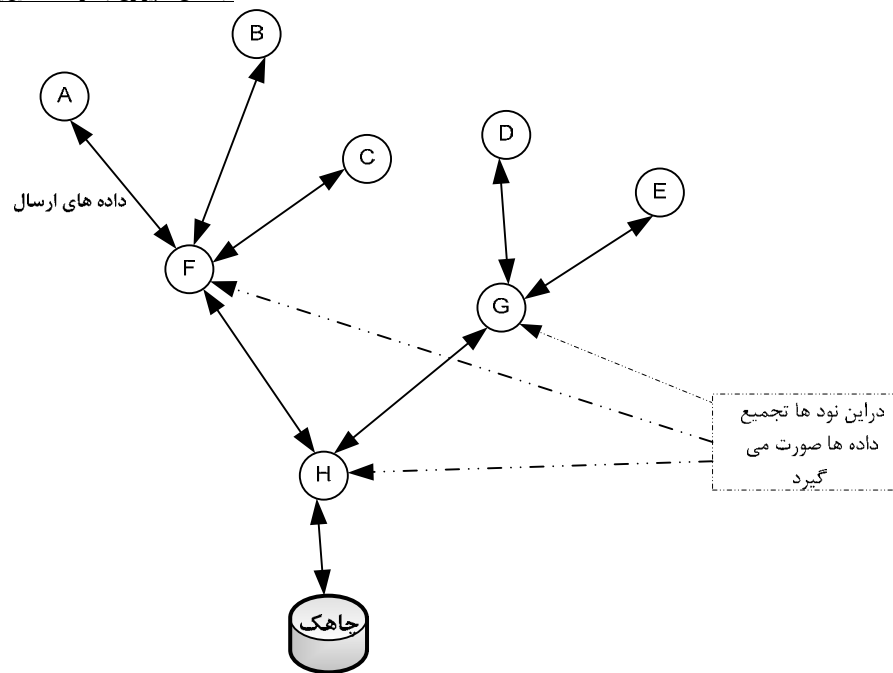
¹ - Location awareness

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

- کمترین انرژی مصرفی در طول مسیر: مسیری که کمترین انرژی را برای ارسال بسته از مبدا به نود چاهک مصرف می کند را انتخاب می نماییم. همانطور که در شکل (۵-۸) مشاهده می شود، مسیر ۱ از این نظر مناسبترین مسیر می باشد.
 - مسیر با کمترین پرش: مسیری که دارای کمترین پرش برای ارسال بسته به مقصد است را انتخاب می نماییم. مسیر ۳ در شکل (۵-۸) از این نظر بهترین گزینه می باشد. باید به این نکته توجه نمود که تعداد پرش، زمانی اهمیت می یابد که دارای چندین مسیر با α نهایی یکسان باشیم؛ در اینصورت مسیری با کمترین میزان پرش از میان آنها انتخاب می گردد.
 - مسیری که دارای بالاترین حداقل میزان انرژی یک نود باشد: مسیری که در طی آن نود دارای کمترین انرژی در مقایسه با نود مشابه در دیگر مسیرها دارای بالاترین انرژی باشد انتخاب می گردد. در شکل (۵-۸) مسیر ۳ و پس از آن مسیر ۱ از این نظر بهترین مسیرها می باشند.
- جنبه مهم دیگر در این مسیریابی، مسیریابی داده محور است. در مسیریابی داده محور، انتشار درخواست ها برای توزیع وظایف هر نود مورد استفاده قرار می گیرد. دو روش کلی برای این منظور وجود دارد:
- نود چاهک درخواست ها را توزیع نماید.
 - نود های شبکه داده های موجود خود را اعلام کرده و نود چاهک داده های مورد علاقه خود را درخواست نماید.
- مسیریابی داده محور نیاز به نامگذاری مبتنی بر خصوصیات دارد. در حالت نامگذاری مبتنی بر خصوصیات کاربران علاقه مند درخواست خصوصیات یک پدیده می باشند تا درخواست از یک نود خاص. بعنوان مثال، "منطقه ای که دمای آن بیش از ۳۵ درجه سانتیگراد می باشد" درخواست معمول تری نسبت به "دمای خوانده شده توسط یک نود خاص" است. نامگذاری مبتنی بر خصوصیات از خصوصیات پدیده ها برای اعلام درخواست ها استفاده می نماید.
- تجمیع داده^۱ تکنیکی برای حل مشکل تشابه و حجم زیاد داده در مسیریابی داده محور می باشد. در این تکنیک، شبکه حسگر حالت یک درخت وارونه را دارد. در شکل (۵-۹) نود چاهک شرایطی محدود از پدیده ای خاص را از نود ها درخواست نموده است.

¹ Data aggregation

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۵-۹): مثالی از تجمیع داده

داده ها از نود های مختلف در صورتیکه در مورد صفاتی مشابه از پدیده ای خاص بوده و در مسیری یکسان تا نود چاهک قرار گیرند، تجمیع می گردند. بعنوان مثال نود حسگر F داده های رسیده از نود های A, B, C را تجمیع می نماید. به عبارت دیگر تجمیع داده، داده های مختلف رسیده از نود های گوناگون را به مجموعه ای از اطلاعات معنی دار تبدیل می نماید. در این کاربرد تجمیع داده را آمیزش داده^۱ می نامند. البته در آمیزش داده بایستی توجه نمود که در اثر این عمل، اطلاعات مفقود نگردند.

۵-۹-۴- لایه پیوند داده

لایه پیوند داده وظیفه تسهیم سازی جریانهای داده، تشخیص قاب داده، دستیابی به رسانه و کنترل خطا را بر عهده دارد. این لایه، اتصالات مطمئن نقطه به نقطه و نقطه به چند نقطه را در شبکه برقرار می نماید. پروتکل های لایه پیوند داده که به پروتکل های MAC معروف هستند، باید در شبکه های حسگر خود سازمان چند پرشه دو هدف زیر را بدست آورند. مورد اول، ساخت یک زیر ساخت برای شبکه می باشد. زمانیکه چند هزار نود در محدوده مورد نظر منتشر شده اند، لایه پیوند داده بایستی ارتباطات میان آنها را به منظور ارسال اطلاعات برقرار نماید. هدف دوم، اشتراک منابع ارتباطی شبکه به صورتی کارا میان نود های شبکه می باشد. تمام پروتکل های قدیمی لایه MAC بر اساس توانایی آنها در اشتراک منابع دسته بندی می گردند. بایستی به این نکته توجه نمود که هیچ کدام از پروتکل های قدیمی لایه پیوند داده، بصورت کامل برای شبکه های حسگر مناسب نمی باشند. در سیستم های سلولی، ایستگاه پایه بصورت سیمی در نظر گرفته می شود. نود های متحرک تنها با یک پرش به ایستگاه متصل می باشند. این نوع شبکه بصورت زیر ساخت در نظر گرفته می شود. مهمترین هدف برای لایه پیوند داده در این نوع شبکه ها فراهم نمودن کیفیت سرویس و پهنای بندی کارا می باشد. مصرف انرژی به جهت نامحدود بودن منابع انرژی در نود های این نوع شبکه، در مراحل بعدی اهمیت قرار دارد. همانند شیوه دستیابی برای این نوع شبکه

¹ Data fusion

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

ها که شبکه های غالب امروزی می باشند، نیاز به یک ایستگاه پایه داریم که این مورد در شبکه های حسگر ناممکن می باشد. در نتیجه، هماهنگ سازی در سطح شبکه بسیار مشکلتر می گردد. علاوه بر موارد ذکر شده مصرف انرژی بصورت مستقیم بر روی طول عمر شبکه های حسگر تاثیر می گذارد که متفاوت با دیگر شبکه ها است، در نتیجه مصرف انرژی پروتکل مورد استفاده به مهمترین پارامتر تبدیل می گردد. MANET و Bluetooth نزدیکترین شبکه ها به شبکه های حسگر بیسیم هستند، با این تفاوت که شبکه های حسگر دارای نود های بسیار بیشتر و محدوده رادیویی بسیار کمتری نسبت به دو شبکه دیگر هستند.

پروتکل های لایه پیوند داده در شبکه های حسگر بیسیم بایستی دارای استراتژی رویارویی با خطا، مدیریت تحرک و مصرف انرژی باشند. پروتکل های مختلفی برای لایه پیوند داده در شبکه های حسگر پیشنهاد شده اند. اما ارائه پروتکلی کارا برای لایه پیوند داده بعنوان موضوعی تازه مورد بررسی می باشد. شیوه های مبتنی بر تقاضا به جهت سربار بالای پیامهای مورد نیاز آن و تاخیر برقراری لینک های ارتباطی، برای شبکه های حسگر مناسب نمی باشند.

۵-۱۰-۱- فنآوریهای جاسازی شده^۱ شبکه

شبکه های حسگر بیسیم، فنآوریهای اطلاعاتی مختلف مانند سخت افزار، سیستمهای نرم افزاری، شبکه و متدهای برنامه سازی را گرد هم آورده است.

۵-۱۰-۱- ریزپردازنده، منبع انرژی و حافظه

یک نود در شبکه حسگر بیسیم از ریزپردازنده، حافظه، حسگرها، مبدل آنالوگ به دیجیتال، فرستنده و گیرنده، کنترل کننده و منبع انرژی تشکیل شده است. با پیشرفت فنآوری مدارهای نیمه هادی و کوچک شدن اندازه آنها، مصرف انرژی آنها نیز کاهش یافته و در ابزارهای کوچکتری قابل استفاده می باشند. در یک کنترل کننده کوچک، کوچک سازی، کارایی را با وجود افزایش قدرت عملیاتی افزایش داده است. اکثر مدارها می توانند به حالت خواب رفته و انرژی بسیار کمی را در این حالت مصرف نمایند. بطوریکه می توان ابزارها را در مواقع بیکاری در حالت خواب نگاه داشت تا مصرف انرژی کمی داشته باشند ولی کارایی آنها کاهش نیابد. این مصرف انرژی می تواند از طرق مختلف بدست آید. سلولهای خورشیدی می توانند انرژی معادل ۱۰ میلی وات بر سانتیمتر مربع در محیط باز و ۱۰ تا ۱۰۰ میکرو وات در محیطهای بسته تولید نمایند. منابع انرژی مکانیکی مانند لرزش پنجره ها و لوله های انتقال آب نیز برای تامین انرژی مورد استفاده قرار می گیرند.

یک منبع انرژی مکعبی عادی که اندازه های در حد سانتیمتر دارد قابلیت تولید انرژی در حدود ۱۰۰۰ میلی آمپر در ساعت را دارا می باشد و چنین منبع انرژی، در اکثر موارد به جهت اندازه کوچک آن قابل استفاده می باشد. با این وجود، ریزپردازنده های با مصرف انرژی پایین دارای حافظه RAM در حدود ۱۰ کیلو بایت و حافظه ROM در حدود ۱۰۰ کیلو بایت (یعنی تقریباً ۱۰۰۰۰ بار ضعیف تر از یک کامپیوتر عادی) می باشند. این فضای حافظه محدود اکثر فضای موجود تراشه ها و منابع انرژی را مصرف می نمایند. طراحان سعی در استفاده از حافظه های سریع با ظرفیت ۱ مگا بایت را در نود ها دارند.

۵-۱۰-۲- ریز حسگرها

¹ Embedded network technology

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

حسگرها بنوعی چشم و گوش نود های شبکه های حسگر می باشند. تغییر در مشخصات محیط اطراف حسگرها، موجب تغییر در خصوصیات الکتریکی آنها می گردد. حسگرها به شکلی طراحی می گردند که تغییرات محیط موجب تغییرات آنها در محدوده های معین گردد. برای مثال حسگر دما، یک مقاومت الکتریکی می باشد که با تغییر دما به آرامی تغییر می یابد. یک مبدل آنالوگ به دیجیتال، ولتاژ را به اعداد تبدیل کرده و ریزپردازنده می تواند آنها را پردازش و ذخیره نماید. سلولهای نوری نیز به شکلی مشابه عمل می نمایند؛ با این تفاوت که با تغییر شدت نور، از خود واکنش نشان می دهند. ساختارهای پیچیده دیگری نیز برای شناسایی دیگر پدیده ها طراحی شده اند. این ابزارها غالباً مصرف انرژی پایینی داشته و برای محیطهای مورد نظر ما مناسب می باشند. با طراحی مبدلهای آنالوگ به دیجیتال، حسگرها نیز به دلیل کارایی بالا، انرژی معادل ریز پردازنده ها مصرف می کنند. سیستمهای ریزالکترو مکانیکی^۱ می توانند پدیده های مختلف فیزیکی را بصورتی ارزان و کارا احساس نمایند. محققان، توانایی ساخت قطعات الکترونیکی در اندازه های میکروسکوپی را دارا می باشند. نکته مهم در اینباره قیمت مناسب این ابزارها می باشد. از این فناوری به شکل گسترده ای در حسگرها استفاده می گردد.

۵-۱۰-۳- ریز رادیوها

در حال حاضر اکثر کارخانجات، حسگرها را در ابعاد وسیع در ابزارهای مختلف مورد استفاده قرار می دهند. این توسعه بدلیل امکان ارتباط حسگرها با دیگر ابزارها و تبدیل رویدادهای فیزیکی به اطلاعات و استفاده از اطلاعات در سطح دیگر می باشد. امکانات رادیویی امروزی با کمک فناوری CMOS، امکان ساخت ابزارهای بیسیم مانند پیجرها، بیسیم ها، تلفن های بیسیم و شبکه های محلی بیسیم برای کامپیوتر های لپ تاپ، ایجاد نموده است. در شبکه های گسترده بیسیم، تلفن های بیسیم صدها میلی وات انرژی مصرف کرده و بر پایه زیر ساختی قدرتمند بنا شده اند. شبکه های حسگر بیسیم ها حدود ۲۰ میلی وات انرژی مصرف کرده و توانی در حدود ۱۰ متر را دارا می باشند. برای ابزارهای کوچکی که قصد کار در فواصل طولانی را دارند، شبکه بایستی مسیریابی را بصورت پرش به پرش از طریق نود ها همانطور که در اینترنت اجرا می گردد به اجرا در آورد. با این وجود، ارتباطات یکی از پرمصرف ترین موارد مصرف انرژی شبکه های حسگر بیسیم می باشد، بطوریکه مصرف انرژی ارسال یک بیت به اندازه مصرف انرژی لازم برای اجرای ۱۰۰۰ دستورالعمل می باشد. در نتیجه در شبکه های حسگر در هر جا که امکان پردازش اطلاعات وجود داشته باشد، این کار صورت می پذیرد.

۵-۱۰-۴- مشکلات سیستم

شبکه های حسگر، بایستی سخت افزار محدود موجود خود را به چندین فعالیت همزمان همانند بررسی محیط از طریق حسگرها، پردازش داده ها و ارسال جریانهای داده تخصیص دهند. ارتباطات بالقوه میان دستگاهها بایستی شناسایی شده و سپس اطلاعات میان مبدا و مقصد منتقل گردند. بدین منظور سیستم های عامل متعددی در شبکه های حسگر بیسیم ارائه شده اند. سیستم های عامل عادی مانند Unix بر روی پردازنده های ۳۲ بیتی با سرعت ۵۰ تا ۱۰۰ مگا هرتز با مقدار مناسبی حافظه RAM و حافظه جانبی چند گیگا بیتی به راحتی اجرا می گردند. امروزه، لپ تاپ ها با چنین امکاناتی تا چند ساعت امکان کار دارند. یک حالت عادی برای شبکه های حسگر، این است که بایستی با یک باتری قلمی کوچک برای یک سال به فعالیت خود ادامه دهند. مسئله دیگر اینست که نود های حسگر با محیط سروکار دارند در صورتیکه کامپیوترهای عادی با موجودی بنام انسان که بسیار پیچیده است کار می نمایند.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

یکی از مهمترین سیستم های عامل در شبکه های حسگر بیسیم، سیستم عامل TinyOS می باشد. TinyOS بستری را برای نصب سیستمهای وابسته به کاربرد به شکلی که بتوانند با کمبود منابع کار کنند، فراهم می نماید. اساس ترین کار این سیستم عامل اینست که سخت افزار، هنگامیکه نیازی به فعال بودن آن نیست سیکل های پردازنده را مصرف ننماید. هر برنامه کاربردی تنها اجزایی که بدانها نیاز دارد را به کار می گیرد.

۵-۱۰-۵- زیرساخت شبکه های حسگر

نود های حسگر ساخته شده دانشگاه برکلی به همراه سیستم عامل TinyOS بصورت گسترده ای در سیستمهای اکتشاف مورد استفاده قرار می گیرند. شرکت اینتل به تازگی محصولی با نام iMote طراحی نموده که از تراشه ای تجاری به همراه ریزپردازنده ARM قدرتمند، حافظه و یک فرستنده و گیرنده قوی در یک بسته استفاده می نماید. فرستنده و گیرنده مورد نظر از فناوری Bluetooth استاندارد که بصورت گسترده ای در لپ تاپ ها و تلفن های بیسیم مورد استفاده قرار گرفته اند، استفاده می نماید. رادیو در پهنای باند بالایی عمل کرده و از پروتکل نسبتاً پیچیده ای استفاده می کند. معمولاً پردازنده ARM مدیریت فرستنده و گیرنده Bluetooth را برای ارسال بسته ها از طریق پورت سریال بر عهده دارد. در TinyOS، iMote بصورت مستقیم بر روی پردازنده ARM اجرا شده و سیستمی مستقل را فراهم نموده که حسگرهای مختلف، مسیرهای مختلف، پردازش جریانهای اطلاعاتی سطح بالا و مدیریت مصرف انرژی را سرویس دهی می نماید.

اکثر اجزاء سطح پایین TinyOS مستقیماً بر روی سخت افزار پیاده سازی می گردند. این موضوع منجر به مصرف انرژی پایین و افزایش کارایی اجزاء می گردد. از طرف دیگر نود هایی با پردازنده های ۳۲ بیتی که سیستمهای عامل معمولی مانند لینوکس و ابزار ارتباطی قدرتمند مانند IEEE 802.11 یا مودم تلفن های بیسیم را استفاده می کنند نیز موجود می باشند. این کلاس از نود ها نقش کلیدی را در اکثر طراحی ها بازی می نمایند. در پایین ترین سطح توقع، این نود ها در شبکه بعنوان دروازه برای بازیابی اطلاعات از نود های حسگر و به جهت مانیتور، پیکربندی و تعیین وظایف سیستم مورد استفاده قرار می گیرند. در سیستمهای پیچیده تر غیر همگن بشکل گسترده تری در نقاط مختلف شبکه به جهت تجمع، ذخیره و ادغام داده ها و نیز میزبانی برای حسگرهای با اهمیت تر مورد استفاده قرار می گیرند. بدلیل شدت فعالیت این نود ها، به منابع انرژی قویتر و ابزارهای شارژ دوباره منابع نیاز داریم. البته این نود ها امکان تبادل انرژی با یکدیگر را دارا می باشند.

۵-۱۰-۶- شبکه های خود سازمان

ارتباطات بیسیم و سنجش از راه دور از گذشته در ابزارهایی مانند ماهواره ها و موشک ها مورد استفاده قرار گرفته اند. یک شبکه از مجموعه وسیعی از نود ها تشکیل شده است که هر کدام با چندین لینک به دیگر نود ها متصل شده اند. اطلاعات پرش به پرش از مبدا تا مقصد مسیریابی می گردند. در یک شبکه سیمی، هر مسیریاب به مجموعه مشخصی از دیگر مسیریاب ها متصل می باشد که بصورت کلی یک گراف مسیریابی را تشکیل می دهند. در شبکه های حسگر بیسیم هر نود دارای یک رادیو می باشد که امکان ارتباط با تمام نود های مجاور را به آن می دهد. با تبادل اطلاعات، نود ها می توانند همسایگان خود را تشخیص داده و از الگوریتمی توزیع شده برای مسیریابی داده تا مقصد طبق نیازهای برنامه کاربردی استفاده می نمایند. موقعیت فیزیکی نود ها درجه اول اهمیت را داراست، اما ملاکهای دیگری مانند تداخلات، تحرک و عوامل محیطی نیز در تصمیم گیری موثر می باشند.

۵-۱۰-۷- اتصال

تواناییهای شبکه ای شبکه های حسگر بیسیم، در لایه های مختلف پخش شده اند. پایین ترین سطح ابزار، کانال فیزیکی را کنترل می کند. رادیو خاصیت همه پخشی دارد، به این معنی که زمانیکه یک نود داده ای را ارسال نماید تمام نود های دیگرتوانایی دریافت آنها دارند. برای جلوگیری از تداخل، کنترل کننده لایه فیزیکی به کانال گوش کرده و تنها زمانیکه کانال خالی باشد اقدام به ارسال داده می کند. زمانیکه نود داده ای برای ارسال ندارد، در کانال ارتباطی به دنبال نشانه ای خاص در ابتدای بسته ها می گردد تا به نوعی خود را با فرستنده هماهنگ کند. لایه مدیریت بسته، بافر را مدیریت کرده، بسته ها را برای ارسال زمانبندی کرده، خطا ها را شناسایی و بررسی نموده، بسته های گم شده را اداره کرده و در نهایت بسته ها را در اختیار برنامه های کاربردی مورد نظر آنها قرار می دهد.

۵-۱۱- انتشار و جمع آوری داده

توسعه دهندگان شبکه های حسگر، از ظرفیت ارتباطی موجود برای پیاده سازی پروتکل هایی که امکان گردآوری داده و پردازش اطلاعات و هماهنگ سازی فعالیت ها را دارند، استفاده می نمایند. فعالیت پایه در این شبکه ها، انتشار اطلاعات از طریق نود های مختلف می باشد. می توان با کمک پروتکل flooding، نود مبدا داده مورد نظر خود را برای تمام نود های در دسترس پخش نماید. نود های گیرنده نیز عملیاتی مشابه با نود مبدا به جهت ارسال داده اجرا می نمایند. بنابراین این امکان وجود دارد که یک نود مدلهای مختلف یک بسته را از همسایگان مختلف خود دریافت نماید. البته مکانیزمی برای شناسایی بسته های تکراری وجود دارد. پروتکل مورد بحث از تکنیکهای خاص برای کاهش حجم ارتباطات اضافی، استفاده می نماید.

شبکه از انتشار برای ارسال فرمانها، اعلام هشدار، پیکربندی و تخصیص وظایف استفاده می کند. از انتشار برای برقراری مسیرها نیز استفاده می گردد. هر بسته، ارسال کننده و فاصله آن تا ریشه را مشخص می نماید. برای تشکیل درختی توزیع شده، نود ها نزدیکترین نود مجاور خود تا ریشه را تعیین می نمایند. هر شبکه می تواند از عکس این درخت برای جمع آوری داده از نود های مختلف شبکه استفاده نماید.

ریشه می تواند بعنوان دروازه ای به شبکه ای قدرتمندتر یا نقطه ای برای تجمیع شبکه حسگر همانطور که در برخی برنامه های کاربردی مورد نیاز می باشد، عمل نماید. شبکه بطور پیوسته در حال گسترش اطلاعات خود در مورد توپولوژی می باشد و به این شکل مسیرهای مناسب تر را پیدا می کند. الگوهای ارتباطی که در شبکه های حسگر بیسیم مورد استفاده قرار می گیرند، با آنچه که در اینترنت وجود دارد، کاملاً متفاوت است.

۵-۱۲- مصرف انرژی و پهنای باند

ارتباطات، مهمترین عامل مصرف انرژی در نود های شبکه های حسگر می باشد. از طرف دیگر مسئله پهنای باند محدود نیز اهمیت دارد. شبکه های حسگر بیسیم سعی در کم نمودن مصرف انرژی از طریق محدود کردن ارسال پیام و خاموش نمودن فرستنده و گیرنده هنگام بیکاری آنها دارد. روشهای مختلفی برای این منظور وجود دارند. برای مثال، نود ها می توانند داده ها را بصورت محلی پردازش نموده و تنها زمانیکه واقعاً نیاز به ارتباط با دیگر نود ها دارند اقدام به ارسال داده نمایند. از این روش در سیستم هشدار هوشمند یا در سیستمهای مانیتورینگ محیط که بر روی جمع آوری اطلاعات در زمان مناسب و محل معلوم تاکید دارند به کار می رود.

تجمیع داده در طول شبکه، ارتباطات شبکه ای را کاهش می دهد. برای مثال یک برنامه کاربردی به تعیین متوسط دمای تعدادی از نود ها که در منطقه جغرافیایی خاصی قرار دارند نیاز دارد. انتخاب زیر مجموعه ای از خواندن ها می تواند در

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

سطح برگ های درخت صورت پذیرد، سپس هر نود داده رسیده را با داده های خود پردازش کرده و تنها یک بسته از داده را ارسال می نماید. به عبارت دیگر هر نود خلاصه ای آماری از زیر درخت خود در اختیار دارد. به این شکل حجم داده انتقالی کاهش می یابد.

فشرده سازی و زمانبندی می توانند در تنظیم مصرف انرژی در لایه پایینی نقش موثری داشته باشند. بعضی پروتکل ها به واسطه نگهداری ساختار ارتباطی خود، مدیریت تداخلات و افزایش اطمینان، مجبور به تحمل سرباری اضافه می باشند. شبکه های حسگر با اضافه کردن داده های مدیریتی به بسته های داده عادی، از ارسال پیامهای مدیریتی صریح اجتناب می کنند. آنها با پیش زمانبندی، تداخلات را کاهش داده و زمان فعال رادیو را کم می کنند. این موارد با رفتار برنامه های کاربردی سطح بالا هماهنگ می گردد. بعنوان مثال، نمونه گیری داده با نرخ پایین بصورت دوره ای را می توان ذکر نمود. در حالتی دیگر شبکه با پیاده سازی روالهای حفظ انرژی در لایه های پایینی می تواند نقش خود را ایفا نماید. بعنوان مثال می توان دستیابی تقسیم زمانی را نام برد.

۵-۱۳- پارامترهای ارزیابی سیستم

در بخش های قبلی کاربردهای مختلف شبکه های حسگر بیسیم مورد بررسی قرار گرفت. اکنون به بررسی پارامترهایی می پردازیم که با کمک آنها می توان شبکه های حسگر بیسیم را ارزیابی نمود. برای انجام این امر، بایستی اهداف اصلی بکارگیری این نوع شبکه ها و مزایای اصلی این شبکه ها نسبت به دیگر شبکه ها را شناسایی نماییم. پارامترهای ارزیابی کلیدی برای شبکه های حسگر عبارتند از: طول عمر، محدوده پوشش، هزینه، سادگی بکارگیری، زمان پاسخگویی، دقت، امنیت و نرخ نمونه گیری کارا. بصورت کلی به بررسی موارد ذکر شده خواهیم پرداخت. بایستی توجه نمود بعضی از این پارامترها به یکدیگر وابسته می باشند. در برخی موارد نیاز است برای افزایش کارایی، پارامتری مانند طول عمر شبکه، کارایی یک پارامتر دیگر مانند نرخ نمونه گیری را کم کنیم.

۵-۱۳-۱- طول عمر

طول عمر هر شبکه حسگر بیسیم پارامتری حیاتی برای آن می باشد. از اهداف کاربردهای مانیتورینگ محیطی و امنیتی اینست که نود ها در محیط خارجی بدون هیچ مراقبت و پشتیبانی قرار داده شوند. اصلی ترین عامل محدودیت در طول عمر شبکه های حسگر بیسیم، منابع انرژی می باشند. هر نود بایستی به شکلی منبع انرژی خود را برنامه ریزی نماید که بتواند طول عمر کل شبکه را افزایش دهد. در بعضی کاربردها میانگین طول عمر شبکه مهمترین عامل نبوده بلکه کمترین میزان انرژی در نود ها اهمیت اول را دارد. در مورد سیستمهای امنیت بیسیم، هر نود بایستی چندین سال عمر نماید.

در بعضی موارد می توان از منابع انرژی خارجی برای نود ها استفاده نمود، اما بایستی یادآور شد که یکی از خصوصیات مهم شبکه های حسگر بیسیم، سادگی نصب آنها می باشد. نیاز به استفاده نود ها از منبع انرژی خارجی این مزیت را از بین می برد. در اینحالت می توان تنها چند نود محدود را به منبع انرژی خارجی متصل نمود.

عامل مهم در تعیین طول عمر یک نود، میزان ارتباطات رادیویی آن می باشد. در یک نود حسگر بیسیم ارتباطات رادیویی مهمترین عامل مصرف انرژی می باشد. این مصرف می تواند با کاهش مصرف انرژی تبادلات یا کاهش حجم تبادلات، کاهش یابد.

۵-۱۳-۲- محدوده پوشش

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

پس از طول عمر، محدوده پوشش مهمترین پارامتر برای شبکه های حسگر بیسیم می باشد. تحت پوشش قرار دادن منطقه وسیع جغرافیایی، همواره از مزیت های یک سیستم می باشد. این موضوع توانایی و ارزش سیستم را برای کاربر به شکل قابل توجهی افزایش می دهد. بایستی توجه نمود که محدوده تحت پوشش با محدوده لینک های ارتباطی مورد استفاده توسط شبکه تفاوت دارد. تکنیک ارتباطات چند پرشه، منطقه تحت پوشش شبکه را ماوراء توانایی فنآوری رادیویی افزایش می دهد. با این وجود، برای محدوده ارسالی مورد نظر، ارتباطات چند پرشه مصرف انرژی نود ها را افزایش می دهد.

مقیاس پذیری، مولفه ای کلیدی در شبکه های حسگر بیسیم می باشد. کاربر در ابتدا می تواند شبکه ای محدود را برقرار کرده و به مرور زمان آنرا گسترش دهد. کاربر بایستی به فنآوری مورد استفاده خود برای مقیاس پذیری آتی اطمینان داشته باشد. افزایش در تعداد نود های یک شبکه، طول عمر یا نرخ نمونه گیری موثر را تحت تاثیر قرار می دهد. تعداد نقاط حس بیشتر موجب افزایش داده های تولید شده توسط شبکه شده و در نهایت باعث افزایش مصرف انرژی در شبکه می گردد. این موضوع با نرخ نمونه گیری کمتر جبران می گردد.

۵-۱۳-۳- هزینه و سادگی در استفاده

یک مزیت اساسی در شبکه های حسگر بیسیم، سادگی در راه اندازی آنها می باشد. افرادی که با فنآوری کامپیوتری آشنایی ندارند، نمی توانند با زیر ساختهای ارتباطی شبکه ها کار نمایند. برای راه اندازی موثر، شبکه های حسگر بیسیم بایستی بتوانند خود را پیکربندی نمایند. بصورت ایده آل، سیستم بایستی قادر باشد خود را با هر تغییر فیزیکی هماهنگ نماید. اما در واقعیت، سیستم بایستی بر روی محل فیزیکی نود ها محدودیت هایی اعمال نماید. به عبارت دیگر، هر نود بایستی توانایی اکتشاف لینک های ارتباطی خود و تعیین کیفیت آنها داشته باشد.

علاوه بر فاز پیکربندی ابتدایی، سیستم بایستی بتواند خود را با تغییرات فیزیکی محیط تطبیق دهد. در طول دوره زندگی شبکه، امکان تغییر محل قرارگیری نود ها و یا تداخل ارتباطات آنها به هر دلیل دیگری وجود دارد؛ در این شرایط، شبکه بایستی توانایی پیکربندی دوباره خود را دارا باشد. برقراری و پیکربندی ابتدایی، اولین قدم های چرخه زندگی یک شبکه می باشد. در دراز مدت، امکان دارد هزینه پشتیبانی سیستم از هزینه ابتدایی ایجاد آن بیشتر شود. کاربردهای امنیتی نیاز دارند که سیستمها کاملاً مطمئن باشند. بعلاوه تست های سخت افزاری و نرم افزاری قبل از برقراری شبکه برای آن مورد نیاز می باشد. در دنیای واقعی، بخشی از سرمایه انرژی شبکه بایستی به پشتیبانی شبکه و رسیدگی به آن اختصاص یابد. تولید ترافیک مربوط به تشخیص و پیکربندی دوباره شبکه، عمر آنها کوتاه تر نموده و نیز نرخ نمونه گیری موثر را کاهش می دهد.

۵-۱۳-۴- زمان پاسخگویی

در سیستمهایی مانند سیستم هشدار دهنده، زمان پاسخگویی پارامتری حیاتی می باشد. یک سیگنال هشدار، زمانیکه حمله ای صورت می گیرد بایستی بلافاصله ارسال گردد. با وجود مصرف انرژی کم، نود ها بایستی توانایی ایجاد پیامهای بلادرنگ و با فوریت بالا را که بتواند شبکه را بسرعت طی نمایند، داشته باشند. بایستی توجه نمود که اتفاقاتی مورد نظر بی هیچ ترتیبی و در هر زمانی می توانند به وقوع بپیوندند. در برخی کاربردها، شبکه های حسگر بیسیم تنها اگر زمان پاسخگویی مورد نظر را تامین نمایند، می توانند عملیاتی باشند.

توانایی در ایجاد زمان پاسخگویی مناسب با برخی از تکنیک هایی که تاکنون برای افزایش طول عمر شبکه پیشنهاد شده، تناقض دارد. بعنوان مثال در یکی از روشها برای افزایش طول عمر شبکه، رادیوی نود ها در بازه های زمانی معین فعال می باشند و در مابقی اوقات خاموش می گردد، در اینحالت اگر بعنوان مثال نودی رادیو خود را در هر دقیقه یک بار فعال نماید

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

امکان اینکه بتوان زمان پاسخگویی مناسبی ایجاد نماییم، غیر ممکن خواهد بود. برای بهبود زمان پاسخگویی می توان از تعدادی نود در شبکه استفاده نمود که همواره فعال بوده و وظیفه ارسال داده به مقصد را دارا می باشند، البته این مورد سادگی برقراری شبکه را کاهش می دهد.

۵-۱۳-۵- دقت

در کاربردهای محیطی و پی جویی، بایستی توسط نود های مختلف نمونه گیری از محیط اجرا شود تا ماهیت پدیده حس شده تعیین گردد. دقت این عملیات وابسته به نرخ انتشار پدیده مورد نظر در محیط تحت نظارت شبکه می باشد. بعنوان مثال در تعیین متوسط دمای یک محدوده، نمونه ها بایستی بلافاصله از یکدیگر برداشت شوند درحالیکه برای تعیین فعالیتهای لرزشی یک ساختمان، بایستی نمونه ها با فاصله چند میلی ثانیه ای برداشت گردند. برای دستیابی به دقت مورد نظر در شبکه بایستی از یک ساعت عمومی برای تعیین موقعیت رویدادها نسبت به یکدیگر استفاده نماییم. در یک سیستم توزیع شده، بایستی برای این ساعت عمومی انرژی صرف نمود؛ اطلاعات مربوط به ساعت میان نودهای مختلف در بازه های زمانی معین مبادله می گردد. اندازه بازه های زمانی مذکور به دقت مورد نظر بستگی دارد.

۵-۱۳-۶- امنیت

با وجود اینکه طبیعت داده هایی مانند دمای محیط و دیگر داده های مربوط به پدیده های محیطی بی ضرر هستند، اما امن نگاه داشتن این داده ها اهمیت زیادی دارد. به عنوان مثال از روی میزان دما و نور مورد استفاده در یک ساختمان می توان به راحتی به الگوی کاری آن ساختمان پی برد؛ حال با استفاده از الگوی مذکور می توان شرایط حمله به محل مورد نظر را طرح ریزی نمود. شبکه های حسگر بیسیم بایستی بتوانند اطلاعات جمع آوری کرده را از استراق سمع مصون بدارند. در کاربردهایی که مبتنی بر امنیت هستند، امنیت داده اهمیت بیشتری می یابد. سیستم علاوه بر اینکه بایستی پوشش داده ها از استراق سمع را حفظ کند، بایستی ارتباطات را اعتبار سنجی نماید. برای ایجاد امنیت کافی است دو اصل اجتناب از استراق سمع و اعتبار سنجی را در شبکه اعمال نماییم. نکته دیگر در مسئله امنیت اینست که امکان خلل در عملیات عادی با تداخلات زائد وجود نداشته باشد. استفاده از رمزنگاری و اعتبار سنجی، هزینه های پهنای باند و انرژی را به همراه دارد. پردازشهای بیشتری برای اجرای رمزنگاری و رمزگشایی داده ها و بیتهایی اضافی برای اعتبار سنجی مورد نیاز می باشد. این موضوع مستقیماً بر روی کارایی شبکه موثر می باشد.

۵-۱۳-۷- نرخ نمونه گیری موثر^۱

در شبکه جمع آوری داده، نرخ نمونه گیری داده اولین پارامتر کارایی می باشد. نرخ نمونه گیری موثر را میزان نمونه گیری در هر نود و ارتباط با نقطه جمع آوری کننده در شبکه تعریف می گردد. خوشبختانه کاربردهای جمع آوری داده محیطی، تنها نیاز به جمع آوری داده با نرخ ۱ یا ۲ نمونه گیری در دقیقه را دارند. با این وجود علاوه بر نرخ نمونه گیری یک نود، بایستی تاثیر شبکه چند پرشی را بر توانایی ارسال داده توسط هر نود در نظر گرفت. در درخت جمع آوری داده، یک نود بایستی داده مربوط به تمام نود های زیرین خود را منتقل کند. اگر هر نود تنها یک واحد داده ارسال کرده و هر نود ۶۰ نود زیرین داشته باشد، در اینصورت نود بایستی ۶۰ برابر داده ارسال نماید. علاوه بر آن، نود مورد نظر بایستی ۶۰ داده را در ابتدا در یک دوره

^۱ Effective sample rate

شبکه های کامپیوتری (دکتر محمد حسن یغمایی مقدم - دانشگاه فردوسی مشهد)

نمونه گیری دریافت نماید. این افزایش غیر خطی در ارتباطات داده ای بر روی شبکه تاثیر قابل توجهی می گذارد. با توجه به مسائل مطرح شده، نرخ انتقال داده و حداکثر اندازه شبکه بر روی نرخ نمونه گیری موثر مستقیماً تاثیر می گذارند. یک روش برای افزایش نرخ نمونه گیری موثر، استفاده از پردازش درون شبکه ای می باشد. انواع مختلفی از فشرده سازی برای استفاده کارا تر از پهنای باند در حالی که نرخ نمونه گیری ثابت می ماند، می تواند مورد استفاده قرار گیرد. در زمانیکه نرخ نمونه گیری ثابت نیست، می توان از حافظه اضافی در نود ها برای ذخیره داده ها بصورت موقت استفاده نمود. از پردازش درون شبکه ای می توان برای تعیین زمان وقوع پدیده مورد نظر و فراهم کردن شرایط شبکه به ویژه حافظه موجود در نود برای حس آن استفاده نمود.

۵-۱۴- پارامترهای ارزیابی نود ها

در بخش قبل، مجموعه ای از پارامتر ها که برای ارزیابی کارایی شبکه های حسگر بیسیم بصورت کلی برقرار شده اند، بررسی گردیدند. می توان پارامترهای کارایی سیستم را به پارامترهای کارایی شخصی نود ها که پشتیبانی کننده آنها هستند وابسته نمود. هدف نهایی اینست که درک نماییم چگونه معماری سطح پایین سیستم بر روی کارایی برنامه های کاربردی تاثیر می گذارند. بدلیل اینکه پارامترهای برنامه های کاربردی به یکدیگر وابسته هستند، همانطور که در ادامه مشاهده خواهد شد، بهبود در یکی از آنها به قیمت کاهش دیگر پارامترها صورت می پذیرد.

۵-۱۴-۱- انرژی

برای اینکه برنامه کاربردی بتواند برای چندین سال فعال باشد، بایستی مصرف انرژی نود ها بسیار پایین باشد. بر خلاف تلفن بیسیم که صدها میلی آمپر انرژی مصرف کرده و طول عمری چند روزه دارد، متوسط مصرف انرژی نود های حسگر بایستی در حد چند میکرو آمپر باشد. این مصرف انرژی کم در صورتیکه از سخت افزار کم مصرف و عملیات با مصرف انرژی پایین استفاده نماییم امکان پذیر می باشد.

در طول فعالیت عملیات، ارتباطات رادیویی بخش اصلی مصرف انرژی را در اختیار دارد. بایستی از الگوریتم ها و پروتکل هایی استفاده نماییم که ارتباطات رادیویی را تا جایی که ممکن است کاهش دهند. با استفاده از پردازش محلی، می توان به هدف ذکر شده دست یافت. برای مثال، رویدادهایی که در نود های مختلف اتفاق داده است را در یک نود ادغام کرده، سپس اطلاعات بدست آمده را ارسال می نماییم.

بصورت معمول، یک نود بایستی بطور متوسط مصرفی در حدود ۲۰۰ میکرو آمپر داشته باشد تا بتواند برای یکسال با کمک دو باتری AA فعال بماند. در صورتیکه مصرف انرژی یک تلفن بیسیم ۴۰۰۰ میکرو آمپر می باشد.

۵-۱۴-۲- قابلیت انعطاف

با توجه به محدوده برنامه های کاربردی که در یک شبکه حسگر بیسیم اجرا می گردند، به سادگی به پارامتر قابلیت انعطاف نود ها پی می بریم. به عبارت دیگر، معماری نود بایستی منعطف باشد. هر برنامه کاربردی به ترکیبی متفاوت از طول عمر، نرخ نمونه گیری، زمان پاسخگویی و پردازش درون شبکه ای نیاز دارد. یک معماری از شبکه حسگر بیسیم بایستی به اندازه کافی منعطف باشد تا بتواند با محدوده مناسبی از کاربردها هماهنگ گردد. به علاوه، با توجه به محدودیتهای مالی، هر نود تنها به سخت افزار و نرم افزاری که برنامه کاربردی استفاده کننده از آن نیاز دارد، تجهیز می گردد. یک معماری بایستی مجموعه مناسب و کافی از سخت افزار و نرم افزار را فراهم نماید. در نتیجه این نود ها به سخت افزار و نرم افزار متفاوتی برای دستیابی به کارایی قابل قبول برای هر برنامه کاربردی نیاز دارند.

۵-۱۴-۳- قابلیت اطمینان

با توجه به توقعاتی که از یک نود شبکه حسگر برای طول عمر آن می رود، بایستی از قابلیت اطمینان قابل قبولی برخوردار باشد. در یک کاربرد ساده، صدها نود بایستی در یک توپولوژی خاص برای سالهای متوالی عمل نمایند. برای دستیابی به این هدف، سیستم بایستی به نحوی ایجاد گردد که نسبت به خرابی نود ها تا حد مناسبی قابلیت تطبیق داشته باشد. به علاوه، هر نود بایستی تا جاییکه امکان دارد مطمئن ایجاد گردد.

طراحی کردن سیستمها بصورت تابعی، ابزاری قدرتمند برای پیاده سازی آنها می باشد. می توان وظایف سیستم را به زیر مجموعه های مجزا تقسیم نمود، بطوریکه در نهایت با تست کردن هر کدام و تجمیع آنها به سیستم نهایی رسید. به منظور ساده سازی این روال، زیرمجموعه های ذکر شده بایستی تا جاییکه ممکن است مستقل از یکدیگر طراحی گردند. همانطور که یک سیستم بایستی در قبال خرابی نود ها مطمئن باشد، بایستی واسطی مطمئن برای ارتباط با دیگر نود ها نیز داشته باشد؛ به این دلیل که این شبکه ها اغلب با دیگر شبکه های بیسیم در تعامل هستند. اطمینان لینک های ارتباطی میان شبکه های بیسیم مختلف در صورتیکه از لینک های چند کاناله و رادیوی طیف گسترده استفاده شود، افزایش می یابد. در حال حاضر اکثر نود های حسگر از یک یا بیشتر فرکانس برای عملیات خود استفاده می نمایند. توانایی در جلوگیری از تداخلات، اهمیت قابل توجهی در کاربرد موفق شبکه های حسگر دارد.

۵-۱۴-۴- امنیت

به منظور اینکه بتوانیم نیازمندیهای امنیتی برنامه های کاربردی را برطرف نماییم، بایستی هر نود شبکه توانایی اجرای الگوریتمهای پیچیده رمزنگاری و تصدیق هویت را دارا باشد. انتقال داده بیسیم از نظر خرابی بسیار آسیب پذیر می باشد. تنها راه حفظ امنیت داده ها در این ارتباطات، رمز نگاری تمام ارتباطات می باشد. واحد پردازش مرکزی نود، وظیفه رمزنگاری را بر عهده دارد. در بعضی موارد از یک ابزار تخصصی کمکی نیز به همراه واحد پردازش استفاده می شود. به منظور امن کردن تمام ارتباطات داده ای، تمام نود ها بایستی داده هایی که در اختیار دارند را نیز بصورت امن حفظ نمایند. در صورتیکه نود ها داده های حساس مربوط به برنامه های کاربردی را نداشته باشند، حداقل کلید رمز مربوط به ارتباطات درون شبکه را خواهند داشت. اگر این کلیدها آشکار شود، امنیت شبکه کاملاً از بین خواهد رفت. به منظور حفظ امنیت، کلید بایستی به نحوی در نود ها ذخیره شود که بازایی آن تقریباً غیر ممکن باشد.

۵-۱۴-۵- ارتباطات

پارامترهای کلیدی برای هر شبکه حسگر بیسیم نرخ ارتباطات، مصرف انرژی و محدوده آن می باشند. محدوده ارتباطی هر نود، کاملاً بر روی حداقل تراکم نود های شبکه موثر می باشد. اگر فاصله میان دو نود از حد معینی بیشتر گردد، دیگر امکان برقراری ارتباط میان آنها با اطمینان مورد نظر شبکه وجود نخواهد داشت. اکثر برنامه های کاربردی، تراکم مورد نیاز نود ها را از تراکمی که برای حس کردن نیاز دارند تعیین می نمایند. اگر محدوده ارتباط رادیویی نیاز به تراکم بیشتری داشته باشد، بایستی از نود های بیشتری برای رسیدن به تراکمی مطمئن، استفاده نماییم.

نرخ ارتباطات، تاثیر مستقیمی بر کارایی نود دارد. نرخ ارتباطات بیشتر، به معنی دریافت نرخ نمونه گیری بیشتر و کاهش مصرف انرژی می باشد. زمانیکه نرخ ارسال بیتی افزایش یابد، ارتباطات به زمان کمتری نیاز داشته و مصرف انرژی کاهش می یابد. اما در برخی موارد افزایش نرخ ارسال داده با افزایش مصرف انرژی همراه می باشد. به صورت کلی، نرخ ارتباطات بالاتر

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

موجب افزایش کارایی شبکه می گردد؛ اما بایستی بدانیم که افزایش در نرخ ارتباطات تاثیر قابل توجهی بر روی مصرف انرژی و نیازمندیهای محاسباتی می گذارد. بصورت کلی، مزایای افزایش نرخ ارسال داده تحت تاثیر دیگر فاکتورها قرار می گیرد.

۵-۱۴-۶- محاسبات

پردازش داده درون شبکه ای و مدیریت پروتکل های ارتباط بیسیم سطح پایین، مهمترین عملیات محاسباتی برای یک نود حسگر می باشند. همانطور که در بخشهای قبلی ذکر شد، نیازمندیهای بلادرنج مشخصی برای ارتباطات و حس وجود دارد. زمانیکه داده وارد شبکه می گردد، واحد پردازش مرکزی بایستی بطور همزمان رادیو و ذخیره/رمزگشایی داده را کنترل و اجرا نماید؛ در نتیجه نرخ ارتباط بیشتر نیاز به توان محاسباتی بالاتر دارد.

۵-۱۴-۷- همزمانی

به منظور پشتیبانی از هماهنگی در داده های خوانده شده، نود ها می بایست از یک ساعت هماهنگ با دیگر نود ها استفاده نمایند. نود ها بصورت دوره ای بدلیل فعال و غیر فعال شدن با یکدیگر همکاری می نمایند. خطا در مکانیزم زمانی آنها موجب کاهش کارایی می گردد که نتیجه آن افزایش چرخه کار سیستم را به همراه دارد. در سیستمهای توزیع شده، ساعت ها بدلیل تفاوت در سرعت حرکتشان به مرور زمان دچار اختلاف می شوند. بسته به دما، ولتاژ و رطوبت، اسیلاتورهای ساعت در فرکانسهای مختلفی عمل می نمایند. در نتیجه این اختلافات، نیاز به مکانیزمهای هماهنگی زمان داریم تا دقت را افزایش دهیم.

۵-۱۴-۸- اندازه و هزینه

اندازه فیزیکی و هزینه هر نود حسگر تاثیر مستقیمی بر روی سادگی و هزینه برقراری سیستم دارد. هزینه کلی مالکیت و هزینه ابتدایی برقراری سیستم دو پارامتر کلیدی در تطبیق و به کارگیری فناوری شبکه های حسگر بیسیم می باشند کاهش در هزینه هر نود به معنی خرید تعداد نود بیشتر، افزایش تراکم شبکه و جمع آوری داده بیشتر می باشد. اندازه فیزیکی نیز بر برقراری ساده شبکه تاثیری مستقیم دارد. نود های کوچک تر در مکانهای متنوع تری قابل استفاده بوده و در نتیجه می توانند در کاربردهای بیشتری مورد استفاده قرار بگیرند. در کاربردهای پی جویی، نود های کوچک تر و کم هزینه تر به معنی توانایی در پی جویی اهداف بیشتر می باشد.

۵-۱۵- بررسی برخی از تجارب عملی موجود در شبکه های حسگر بی سیم

در این بخش به بررسی برخی از حسگرهای موجود که توسط شرکت های معتبر فعال در این زمینه ارائه شده است می پردازیم.

۵-۱۵-۱- گرہ حسگر MICAZ

یکی از اولین و معروفترین شرکت هایی که برای کار در زمینه شبکه های حسگر بوجود آمد شرکت Crossbow است. این شرکت نودهای گوناگونی را برای کاربردهای مختلف شبکه های حسگر تولید می کند. یکی از انواع نودهای حسگر تولید این شرکت MICAZ است که در این قسمت به بررسی آن خواهیم پرداخت.

بر اساس مستندات شرکت Crossbow این نوع از نودهای حسگر دارای مشخصات زیر است:

○ یک پردازنده ۸ بیتی Atmel ATmega

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

- ۱۲۸ کیلو بایت حافظه Flash
- ۴ کیلو بایت حافظه EEPROM برای پیکربندی
- تبدیل کننده آنالوگ به دیجیتال ۱۰ بیتی
- گیرنده/فرستنده در باند فرکانسی ۲۴۰۰ تا ۲۴۸۳/۵ مگاهرتز
- سرعت انتقال داده برابر با ۲۵۰ کیلوبیت برثانیه
- محدوده آنتن گیرنده/فرستنده در محیط داخل ساختمان ۲۰ تا ۳۰ متر و در خارج آن ۷۵ تا ۱۰۰ متر
- گیرنده/فرستنده منطبق بر استاندارد Zigbee
- منبع تغذیه ۲ عدد باتری AA
- سیستم عامل TinyOS

در شکل (۵-۱۰) نمونه ای از گره های حسگر MICAz نشان داده شده است.



شکل (۵-۱۰): نمونه ای از گره حسگر MICAz و MICAz OEM

۵-۱۵-۲ Zebranet

Zebranet شبکه‌ای است که برای نظارت بر زندگی حیوانات وحشی طراحی شده است. بررسی این شبکه از این جهت اهمیت دارد که چالش‌های جدیدی را در رابطه با شبکه‌های حسگر مطرح کرده است. در این شبکه نودهای حسگر بر روی گردن حیوانات (گورخر) نصب می‌شوند. نودهای بکار رفته در این شبکه مجهز به سیستم موقعیت یاب جهانی هستند تا بتوانند محل دقیق حیوانات مورد بررسی و مهاجرت آنها را ثبت کنند. علاوه بر این، نودها مجهز به حسگرهای دما و رطوبت هوا و حسگرهای برای تحت نظر گرفتن علائم حیاتی حیوانات تحت نظر است.

در این شبکه مرکز ثابتی برای جمع آوری داده‌ها وجود ندارد و محققان بطور دوره‌ای به میان حیوانات می‌روند تا اطلاعات ثبت شده را جمع آوری کنند. به همین خاطر در این شبکه علاوه بر تحرک نودها، چاهک نیز متحرک است. همچنین چاهک ممکن است برای مدت زمان طولانی (چندین روز) در دسترس نباشد (به عبارتی دیگر برای جمع آوری داده‌ها وارد منطقه نشود).

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

در این شبکه اطمینان از رسیدن اطلاعات جمع آوری شده به مرکز اهمیت زیادی دارد ولی تاخیر در رسیدن اطلاعات چندان مهم نیست. از طرفی نودهای طراحی شده باید دارای وزن باشند که این مسئله خود باعث محدودیت شدید در طراحی نودها و انرژی در دسترس آنها می شود.

از سوی دیگر شبکه طراحی شده باید ناحیه ای به مساحت صدها تا هزاران کیلومتر مربع را پوشش دهد. با وجود تعداد کم نودهای حسگر موجود در این ناحیه، در بسیاری از مواقع برقراری ارتباط بین نودها امکان پذیر نیست.

برای مسیریابی بسته ها در ZebraNet دو پروتکل مختلف پیشنهاد شده است، پروتکل اول یک پروتکل flooding ساده است و پروتکل دوم پروتکلی بر مبنای تاریخچه^۱ است.

ارسال flooding یک الگوریتم ساده برای مسیریابی در شبکه های حسگر بیسیم است. در این پروتکل هر نود بسته های خود را برای تمام همسایه ها ارسال می کند. به این ترتیب می توان با احتمال بالایی از رسیدن بسته ها به مرکز مطمئن بود. گرچه ارسال سیل آسا مطمئن ترین راه برای رسیدن بسته به مرکز است ولی از نظر مصرف منابع موجود (پهنای باند، حافظه، انرژی و ...) راه حل مناسبی نیست.

در پروتکل مسیریابی بر مبنای تاریخچه، به هر یک از نودها عددی نسبت داده می شود که مشخص کننده میزان موفقیت آن نود در ارتباط با چاهک و ارسال داده ها به آن است. در ابتدا مقدار این عدد صفر است. نودها بطور متناوب همسایه های خود را مورد بررسی قرار می دهند. هنگامی که نودی در همسایگی چاهک قرار می گیرد یک واحد به مقدار عدد فوق افزوده می شود. هنگامی که نودی به تعداد دفعات مشخصی نتواند در همسایگی خود چاهک را پیدا کند، یک واحد از مقدار این عدد کسر می شود. برای فرستادن یک بسته به مرکز به این صورت عمل می شود که اگر چاهک به عنوان یکی از همسایه ها پیدا شود، بسته مستقیماً به چاهک فرستاده می شود ولی اگر این طور نباشد بسته به نودی فرستاده می شود که بزرگترین عدد (بیشترین احتمال همسایگی با چاهک در گذشته نزدیک) را دارد. به این ترتیب سعی می شود بسته با کمترین تعداد نود میانی به مرکز منتقل شود. آنچه مسلم است این است که میزان موفقیت این الگوریتم بستگی به میزان تحرک نودها و چاهک دارد.

۵-۱۵-۳ Smart Dust

پروژه Smart Dust در دانشگاه برکلی تلاشی برای پی بردن به این مطلب است که آیا می توان نودهای حسگر به اندازه یک میلیمتر مکعب ساخت؟ اندازه این نودها آنقدر کوچک است که مانند ذرات گرد غبار می توانند در هوا معلق باشند و محیط اطراف خود را برای چند ساعت تا چند روز تحت نظارت قرار دهند. معماری که برای ساخت چنین نودهایی پیشنهاد شده، معماری بدیع و خلاقانه است و چالش ها و فرصت های بسیاری را در دنیای شبکه های حسگر پیش رو قرار می دهد.

قسمت عمده حجم پیشنهاد شده برای این نودها را منبع تغذیه آن تشکیل می دهد. در حال حاضر در هر میلیمتر مکعب از باتری های موجود، حداکثر حدود ۱ ژول انرژی می توان ذخیره کرد. به همین خاطر در اینجا با محدودیت بسیار شدید انرژی روبرو هستیم. در طرح پیشنهاد شده، همچنین قسمت های دیگر یک نود حسگر همانند پردازنده، گیرنده/فرستنده و انواع حسگرها نیز وجود دارد. علاوه بر این یک باتری خورشیدی نیز برای جمع آوری انرژی از محیط اطراف پیش بینی شده است. این باتری خورشیدی در هر روز حدود ۱ ژول انرژی در نور خورشید و حدود یک هزارم ژول در فضای بسته را تولید می کند.

¹ History based

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

در حال حاضر و با توجه به تکنولوژی های موجود، ساخت حسگرها و پردازنده های با حجم بسیار کوچک و مصرف انرژی بسیار پایین مقدور است. مشکل اصلی ساخت نودهایی با حجم چند میلیمتر مکعب سیستم ارتباطی آن است. دو گزینه موجود برای ساخت سیستم ارتباطی امواج رادیویی و امواج نورانی هستند. به دلایل مختلف استفاده از امواج رادیویی (که متداول ترین گزینه در دیگر شبکه های حسگر هستند) در این پروژه مقدور نیست. اول اینکه برای فرستادن و دریافت اطلاعات با استفاده از امواج رادیویی به آنتنی با اندازه چند سانتی متر نیاز است. در صورتی که در این پروژه گره ساخته شده قرار است حجمی برابر چند میلی متر مکعب داشته باشد. دوم اینکه میزان مصرف انرژی در انتقال با استفاده از امواج رادیویی بیش از حد قابل قبول است. به همین خاطر محققان پروژه Smart Dust امواج نورانی برای انتقال داده ها انتخاب کرده اند.

۵-۱۵-۴ - دانشگاه های فعال در زمینه شبکه های حسگر

در حال حاضر تحقیقات در زمینه شبکه های حسگر در بسیاری از دانشگاه ها و مراکز تحقیقاتی جهان انجام می شود. از میان این دانشگاه ها، دانشگاه برکلی با انجام تحقیقاتی که منجر به تولید گره های حسگر سری mica و سیستم عامل TinyOS شده است را می توان پیش گام تحقیقات در این زمینه دانست. همچنین در تعداد کمی از دانشگاه های جهان، درسی با عنوان شبکه های حسگر ارائه می شود. از آن جمله می توان به دانشگاه های MIT, Stanford, Berkeley, Harward اشاره کرد.

پرسش های فصل:

۱. تفاوت اصلی بین شبکه های حسگر بیسیم و شبکه های MANET را بنویسید.
۲. خصوصیات اصلی شبکه های حسگر بیسیم را نام برده و مختصراً توضیح دهید.
۳. برخی از کاربردهای شبکه های حسگر بیسیم را نام ببرید.
۴. به غیر از کاربردهای ذکر شده در این فصل، طرحی پیشنهاد کنید که در آن بتوان از شبکه های حسگر بیسیم استفاده نمود.
۵. معماری داخلی هر نود حسگر را رسم کرده و اجزای آن را توضیح دهید.
۶. خصوصیات اصلی که یک نود در شبکه های حسگر بیسیم باید داشته باشد را توضیح دهید.
۷. با رسم شکل، ساختار شبکه ای حسگر را کشیده و انواع نودهای موجود در آن را تشریح کنید.
۸. نحوه توزیع و قراردادن نودها را در شبکه های حسگر بیسیم توصیف کنید.
۹. پشته پروتکل شبکه های حسگر بیسیم را رسم کرده و عملکرد هر لایه را به اختصار بنویسید.
۱۰. با رسم یک شکل، مسیریابی آگاه از انرژی در شبکه های حسگر بیسیم را توضیح دهید.
۱۱. منظور از تجمع و آمیزش داده ها در شبکه های حسگر بیسیم را توضیح دهید.
۱۲. پارامترهای ارزیابی سیستمی شبکه های حسگر بیسیم را توضیح دهید.
۱۳. پارامترهای ارزیابی نودهای حسگر را بنویسید.
۱۴. به غیر از نمونه های ذکر شده در این فصل، چند نمونه از نودهای حسگر بیسیم موجود را تشریح نمایید.
۱۵. چند نمونه عملی از پروژه های پیاده سازی شده شبکه های حسگر بیسیم را بنویسید.

فصل ششم

لایه شبکه

۶-۱- مقدمه

در این فصل به بررسی لایه شبکه و وظایف آن می پردازیم. همان طور که در فصل اول به آن اشاره شد، لایه شبکه که سومین لایه در مدل مرجع OSI می باشد، موظف به هدایت بسته ها از مبدأ به سمت مقصد است. بدین منظور لایه شبکه باید از توپولوژی شبکه در لایه های پایین تر مطلع باشد تا بتواند بهترین مسیر ممکن را به سمت مقصد پیدا نماید. به طور خلاصه وظایف اصلی لایه شبکه عبارتند از:

- ارائه سرویس به لایه بالاتر از خود (لایه حمل)
 - مسیریابی بسته ها از مبدأ به مقصد
 - کنترل ازدحام
 - ارتباط بین شبکه ای
- در زیر به بررسی هر یک از وظایف فوق می پردازیم.

۶-۲- سرویس لایه شبکه به لایه حمل

همان طور که می دانیم در مدل لایه ای، هر لایه موظف به ارائه سرویس مناسب به لایه بالاتر از خود می باشد. لایه شبکه، نیز موظف به فراهم آوردن سرویس لازم برای لایه حمل می باشد. در طراحی سرویس لایه شبکه باید سرویس مستقل از فن آوری شبکه طراحی شود. همان طور که قبلاً اشاره شد در هر لایه شبکه در مدل OSI دو نوع سرویس می تواند موجود باشند که عبارتند از: سرویس اتصال گرا و سرویس بی اتصال. لایه شبکه نیز قادر به ارائه هر دو نوع سرویس ذکر شده به لایه حمل می باشد.

در سرویس اتصال گرا ابتدا کاربر با ارسال پیام خاصی به شبکه، از آن درخواست برقراری اتصال به یک مقصد خاص می کند. چنانچه شبکه منابع کافی در اختیار داشته باشد، با درخواست کاربر موافقت می کند و یک مسیر مشخص از مبدأ به مقصد برای کاربر فراهم می آورد. به این مسیر به وجود آمده در اصطلاح مدار مجازی گفته می شود. بسته های ارسالی فرستنده

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

به ترتیب از این مسیر ارسال می شوند تا این که ارسال اطلاعات به اتمام برسد. بعد از اتمام ارسال اطلاعات، مسیر مجازی به وجود آمده از بین می رود. به خاطر به وجود آمدن یک مسیر اولیه بین مبدأ و مقصد، تمامی بسته ها به ترتیب از این مسیر عبور می کنند و به مقصد تحویل داده می شوند. بنابراین ترتیب بسته ها در سرویس اتصال گرا، حفظ می شود. همچنین لایه شبکه در سرویس اتصال گرا موظف به کنترل سرعت و کنترل جریان داده ها از مبدأ به مقصد می باشد. در شبکه های اتصال گرا این احتمال وجود دارد که در شبکه چندین مسیر مجازی موجود باشد، در این صورت برای مشخص نمودن این که بسته ورودی به کدام مدار مجازی موجود در شبکه اختصاص دارد، از یک فیلد به نام شناسه اتصال استفاده می شود.

در سرویس بدون اتصال، فرستنده بدون هیچ گونه عملیات اولیه ای، اقدام به ارسال قاب های خود می کند. در این صورت قاب های ارسالی به طور مستقل پردازش می شوند و این احتمال وجود دارد که از مسیرهای متفاوتی به مقصد ارسال گردند. بنابراین ممکن است که ترتیب بسته ها در مقصد از بین برود. با مقایسه سرویس اتصال گرا با سرویس بی اتصال می توان به این نتیجه رسید که سرویس اتصال گرا پیچیدگی بیشتری نسبت به سرویس بی اتصال دارند. چنانچه یک شبکه در سطح لایه سوم از سرویس اتصال گرا استفاده نماید، به آن شبکه مدار مجازی گفته می شود. همچنین شبکه هایی که از سرویس بی اتصال استفاده می نمایند، شبکه های داده گرام نامیده می شوند. در زیر به مقایسه این دو نوع شبکه از جنبه های مختلف می پردازیم:

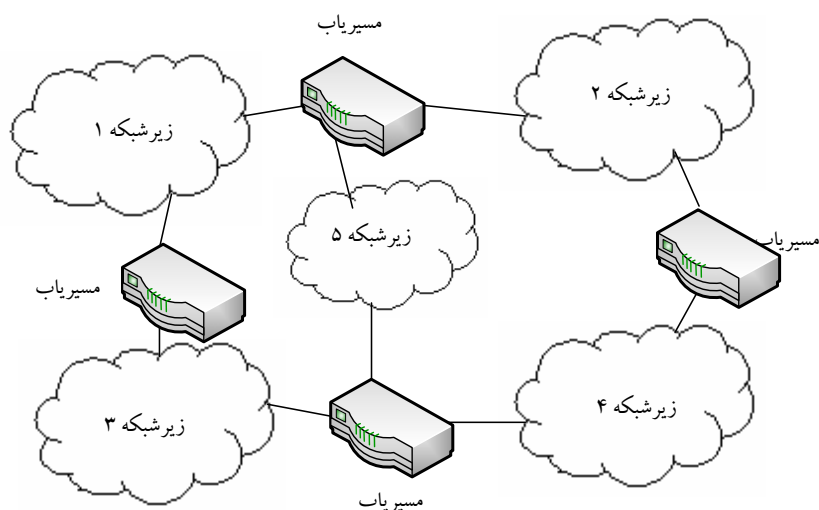
- **آدرس دهی:** با توجه به این که در شبکه های مدار مجازی ابتدا قبل از ارسال داده ها، یک مسیر مشخص بین مبدأ و مقصد به وجود می آید و سپس داده های ارسالی از این مسیر راهی مقصد می شوند، بنابراین در شبکه های مدار مجازی به آدرس مبدأ و مقصد فقط در فاز برقراری اتصال اولیه نیاز می باشد و بعد از آن از یک مشخص کننده اتصال برای تعیین مدار مجازی هر بسته استفاده می شود. بسته های ارسالی در شبکه های داده گرام به طور مستقل پردازش می گردند و مسیریابی می شوند بنابراین در تمامی بسته های ارسالی فوق به آدرس مبدأ و مقصد نیاز می باشد.
- **اطلاعات وضعیت شبکه:** همان طور که گفته شد در شبکه های مدار مجازی این احتمال که چندین مدار مجازی مختلف در شبکه فعال باشند زیاد است. برای تمایز بسته های ورودی و تعیین مدار مجازی هر بسته، از یک مشخص کننده اتصال در هر بسته استفاده می شود. همچنین نودهای میانی شبکه دارای جداولی می باشند که در آنها اطلاعات تمام مدارهای مجازی قرار دارد. بنابراین در شبکه های مدار مجازی اطلاعات وضعیت شبکه ذخیره می شود؛ در حالی که در شبکه های داده گرام این اطلاعات ثبت نمی گردد.
- **مسیریابی:** در شبکه های مدار مجازی هنگام برقراری اتصال اولیه مسیریاب های شبکه با توجه به آدرس فرستنده و گیرنده اقدام به مسیریابی و انتخاب بهترین مدار مجازی ممکن بین مبدأ و مقصد می نمایند. بعد از آن که مدار مجازی به وجود آمد همه بسته های ارسالی متعلق به یک مدار مجازی خاص، از طریق فیلد مشخص کننده اتصال از مدار مجازی مشخص شده عبور می کنند تا به مقصد برسند. در شبکه های داده گرام با توجه به این که هر بسته مستقل از بسته های دیگر پردازش می شود، هر بسته ورودی به طور جداگانه مسیریابی می شود.
- **خراب شدن یک نود:** در شبکه های مدار مجازی چنانچه یکی از نودهای میانی شبکه از کار بیافتد، در این صورت تمامی مدارهای مجازی عبوری از آن از بین می روند، در حالی که در شبکه های داده گرام با خراب شدن یک نود، سایر نودهای شبکه بسته های ورودی را از طریق نودهای دیگر به سمت مقصد هدایت می کنند.
- **کنترل ازدحام:** در شبکه های مدار مجازی چنانچه بافر کافی برای نودهای میانی شبکه در نظر گرفته شود، کنترل ازدحام به سادگی انجام می گردد؛ در حالی که کنترل ازدحام در شبکه های داده گرام مشکل تر از شبکه های مدار مجازی می باشد.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

- پیچیدگی: شبکه های مدار مجازی بیشترین پیچیدگی را در سطح لایه شبکه دارند در حالی که در شبکه های داده گرام بیشترین پیچیدگی در سطح لایه حمل می باشد.

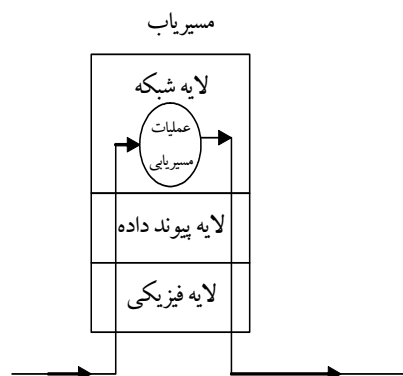
۳-۶- مسیریابی

در طی چند سال اخیر میزان تقاضا برای شبکه های ارتباطی به شدت افزایش یافته است. با گسترش سرویس اینترنت نظیر پست الکترونیکی، جستجو در بانکهای اطلاعاتی، تبادل فایل و سایر سرویس متداول نیاز به تبادل بین شبکه ای حس می گردد. با استفاده از مسیریاب های شبکه امکان دسترسی به شبکه جهانی اینترنت و سرویس آن فراهم می آید. در شکل (۱-۶) نمونه ای از اتصال زیر شبکه های مختلف از طریق مسیریاب های شبکه نشان داده شده است. درون زیر شبکه ها از پروتکل های مختلفی نظیر Ip ، Ipx ، X.25 ، XNS ، ... استفاده می شود. هر مسیریاب برای انجام عملیات مسیریابی از پروتکل های مسیریابی مانند : IS-IS , RIP , OSPF و ... استفاده می کند.



شکل (۱-۶): اتصال شبکه های مختلف با کمک مسیریاب به یکدیگر

مسیریاب های شبکه در سطح لایه سوم مدل مرجع OSI عمل می نمایند. لایه شبکه داده های لایه حمل را دریافت نموده و با افزودن سرآیندهای مناسبی نظیر آدرس منطقی مبدأ و مقصد، آن را به لایه پایین تر تحویل می دهد. در شکل (۲-۶) مدل لایه ای مسیریاب نشان داده شده است.



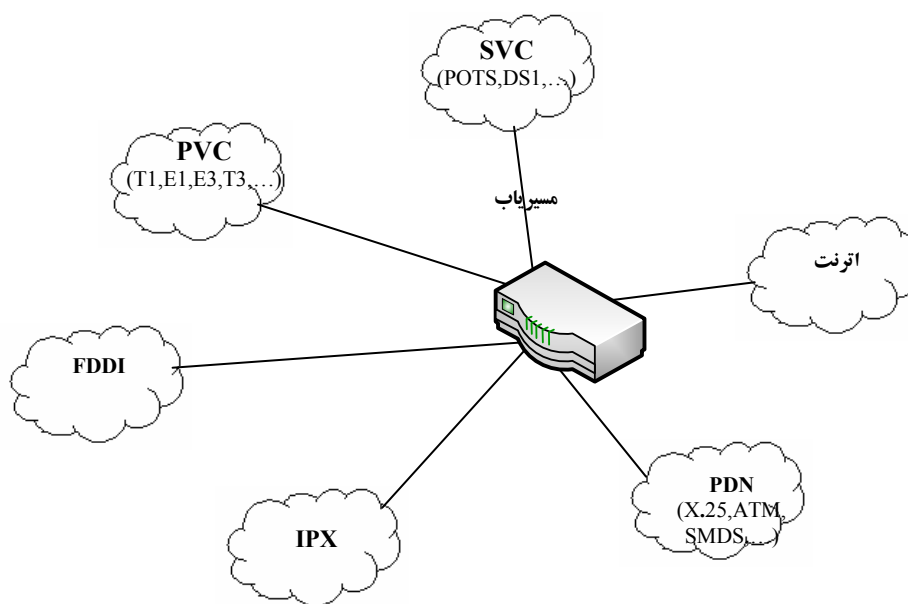
شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

شکل (۶-۲): مدل لایه ای یک مسیریاب شبکه

مسیریاب های شبکه، عملیات فیلترینگ و هدایت به جلو بسته های ورودی را انجام می دهند. از مسیریاب ها می توان به عنوان یک تکرارکننده و یا پل نیز استفاده نمود. به غیر از هدایت بسته ها از مبدأ به مقصد، هر مسیریاب قادر به ارائه سرویس ارزش افزوده دیگری نیز می باشد که برخی از مهمترین آنها عبارتند از: مرتب سازی ترافیک^۱، فیلترینگ امنیتی^۲، مدیریت شبکه و نگهداری منابع شبکه.

مطابق با شکل (۶-۳) هر مسیریاب قادر به پشتیبانی از چندین فن آوری مختلف شبکه می باشد. هر مسیریاب شبکه، برای هدایت بسته ها به مقصد از الگوریتم های مسیریابی استفاده می کند. هر چند اجزای هر الگوریتم مسیریابی با یکدیگر متفاوت می باشد اما تمام آنها دارای اهداف مشخص زیر می باشند:

- **بهینه بودن:** هر الگوریتم مسیریابی باید براساس ضوابط انتخاب مسیر، بهترین مسیر را انتخاب کند.
- **همگرایی سریع:** الگوریتم مسیریابی خوب باید در برابر تغییرات توپولوژی شبکه به سرعت همگرا گردد.
- **قدرت:** چنانچه توپولوژی شبکه تغییر نماید، الگوریتم مسیریابی باید دوباره بهترین مسیر را به دست آورد.
- **سادگی پیاده سازی:** الگوریتم مسیریابی باید حتی الامکان پهنای باند شبکه را اشغال ننماید و بالاسری پردازش کمی داشته باشد.



شکل (۶-۳): فن آوری های مختلف مسیریاب

۶-۳-۱- الگوریتم های مسیریابی

^۱Traffic sequencing

^۲Security filtering

^۳Robustness

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

مهمترین وظیفه لایه شبکه، مسیریابی و راهبری بسته های اطلاعاتی از ماشین مبدأ به ماشین مقصد است. در بیشتر زیرشبکه ها، بسته های اطلاعاتی جهت رسیدن به مقصد از چندین نود میانی می گذرند و بنابراین باید بهترین مسیر برای رسیدن به مقصد شناسایی و انتخاب شود، تا بسته ها به آن مسیر هدایت شوند. الگوریتم مسیریابی، بخشی از نرم افزار لایه شبکه است؛ که موظف به تصمیم گیری درباره کانال خروجی یک بسته ورودی و هدایت آن در کانال فوق می باشد. در شبکه های داده گرام برای هر بسته ورودی باید این تصمیم گیری صورت گیرد؛ چرا که در این شبکه ها ممکن است بهترین مسیر به طور دایم تغییر کند. در شبکه های مدار مجازی، یافتن مسیر فقط در فاز برقراری ارتباط انجام می شود. در هر صورت، آنچه که در مسیریابی مهم است: صحت، سادگی، پایداری، قدرت، شفافیت و بهینه بودن مسیریابی می باشد.

شاید بتوان گفت پایداری، مهمترین هدف برای الگوریتم مسیریابی است. البته لازم به ذکر است که ممکن است در مواردی در اهداف فوق تداخل پیش بیاید و این اهداف با یکدیگر متضاد باشند اما در هر صورت می توان به سطحی رسید که تمام اهداف تا حدودی برآورده شوند.

الگوریتم های مسیریابی را می توان به دو گروه عمده تقسیم کرد: الگوریتم های غیرواقعی و الگوریتم های واقعی. الگوریتم های غیرواقعی، تصمیم های مسیریابی خود را بر اساس ترافیک و توپولوژی جاری شبکه انجام نمی دهند، بلکه انتخاب مسیر از هر نود به نود دیگر، زمانی که شبکه را اندازه می شود صورت می گیرد. به اینگونه مسیریابی، مسیریابی ایستا نیز گفته می شود.

الگوریتم های واقعی، تصمیمات مسیریابی خود را با تغییر توپولوژی و غالباً ترافیک، تغییر می دهند. این الگوریتم ها، اطلاعات مسیریابی را به نحوی متفاوت با الگوریتم های ایستا به دست می آورند و نیز مسیر خود را زمانی که بار ترافیکی و یا توپولوژی شبکه تغییر می کند، تغییر می دهند. به این الگوریتم ها، الگوریتم های پویا نیز گفته می شود.

۶-۳-۱-۱- الگوریتم های ایستا

برای تشریح الگوریتم های مسیریابی، زیر شبکه به صورت یک گراف در نظر گرفته می شود که هر نود آن یک مسیریاب است و هر یال، معرف یک کانال ارتباطی است. برخی از مهمترین الگوریتم های مسیریابی ایستا در شبکه های کامپیوتری به شرح زیر می باشند:

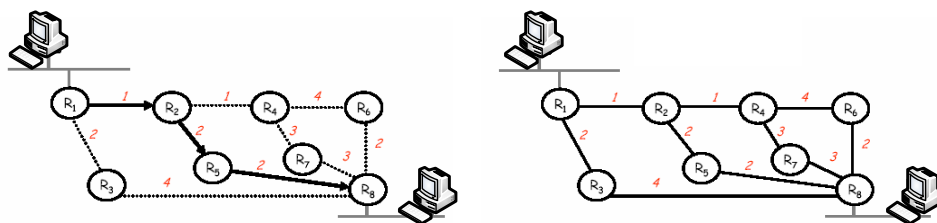
- **الگوریتم کوتاهترین مسیر^۱**: در این الگوریتم، هدف یافتن کوتاهترین مسیر موجود بین مبدأ و مقصد می باشد که این کوتاهترین مسیر تعابیر متفاوتی می تواند داشته باشد و این تعابیر بر اساس معیارهای مختلف صورت می گیرد. مثلاً میتوان از معیار تعداد پرش هایی که باید در طی مسیر از آنها گذشت استفاده نمود. براساس این معیارها به هر یال گراف شبکه، یک برچسب نسبت داده می شود که از این برچسبها برای محاسبه کوتاهترین مسیر استفاده می گردد. برچسب های موجود بر روی هر یال شبکه معرف مشخصه های گوناگونی نظیر فاصله، پهنای باند، متوسط ترافیک، هزینه ارتباطی، متوسط طول صف و تاخیر اندازه گیری شده می باشند. با اجرا شدن الگوریتم کوتاهترین مسیر بر روی مسیریاب های شبکه، فاصله همه نودهای دیگر با مسیریاب جاری مشخص می شود. یکی از مهمترین الگوریتم های مسیریابی کوتاهترین فاصله، الگوریتم Dijkstra می باشد. در شکل (۶-۴) مثالی از الگوریتم فوق آورده شده است. در این شکل کوتاهترین مسیر بین کامپیوتر میزبان A و کامپیوتر میزبان B از طریق مسیریاب های R1-R2-R5-R6 می باشد.
- **الگوریتم سیل^۲**: الگوریتم ایستای دیگری که در این جا معرفی می شود، الگوریتم سیل است. در این الگوریتم هر نود شبکه هر بسته اطلاعاتی دریافتی خود را به کلیه درگاه های خروجی خود، به جز درگاهی که بسته از آن وارد شده است، می فرستد. طبیعی است که در این حالت تعداد زیادی بسته اطلاعاتی یکسان وجود خواهد داشت. در هر بسته

^۱ Shortest path

^۲ Flooding

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

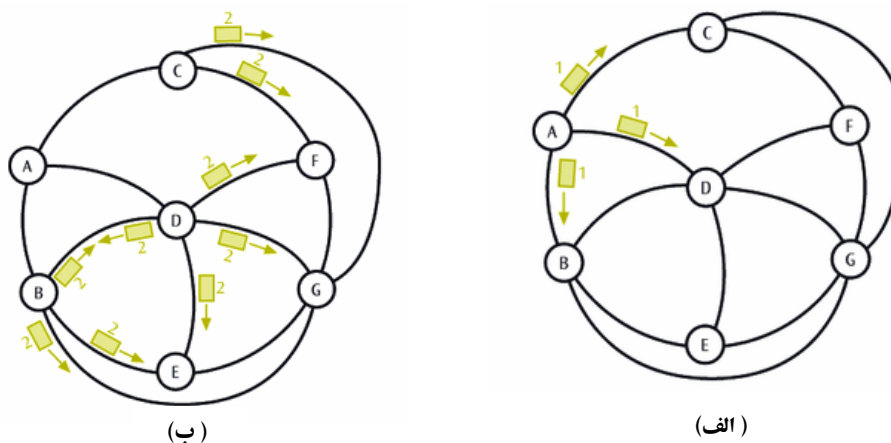
اطلاعاتی، یک فیلد در قسمت سرآیند وجود دارد که حاوی یک شمارنده می باشد. هر بار که بسته ای به یک نود می رسد و نود می خواهد آن را منتشر کند، یکی از مقدار این فیلد کم می شود. زمانی که مقدار فیلد فوق به صفر رسید، نود دریافت کننده بسته از انتشار آن جلوگیری می کند. در حالت ایده آل مقدار اولیه این شمارنده باید برابر با تعداد پرش های موجود در مسیر باشد. اگر فرستنده از تعداد پرش های موجود بین خود و مقصد مطلع نباشد، در بدترین حالت از قطر شبکه (یعنی طولانی ترین مسیر ممکن بین مبدأ و مقصد در آن زیر شبکه) استفاده می کند. یک روش دیگر برای جلوگیری از انتشار بی خودی بسته ها این است که هر بسته دارای یک شماره سریال خاص خود باشد. هر نود شبکه که یک بسته ورودی را منتشر می سازد، شماره سریال آن را در حافظه خود ذخیره می کند. با ورود بسته جدید ابتدا شماره سریال آن با شماره سریال بسته های موجود در حافظه مقایسه می شود و در صورت عدم تطابق، بسته ورودی منتشر می گردد. البته باید از مکانیسم های کنترلی برای جلوگیری از رشد بیش از حد لیست شماره سریال های بسته ها در حافظه های نودهای میانی شبکه استفاده نمود. در شکل (۶-۵) مثالی از مسیریابی سیل آورده شده است.



(ب)

(الف)

شکل (۶-۴): مثالی از مسیریابی کوتاهترین فاصله



(ب)

(الف)

شکل (۶-۵): مثالی از مسیریابی سیل

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

در بیشتر شبکه های کامپیوتری امروزی، از الگوریتم های مسیریابی پویا به جای الگوریتم های ایستا استفاده می شود. دو الگوریتم مسیریابی پویای بردار فاصله^۱ و وضعیت لینک^۲ از اهمیت زیادی در شبکه های کامپیوتری برخوردار می باشند که به بررسی آنها می پردازیم.

الگوریتم مسیریابی بردار فاصله

در این الگوریتم هر مسیریاب یک جدول (یک بردار)، که نشان دهنده بهترین مسیر شناخته شده تا هر مقصد و نحوه رسیدن به آن مقصد است را ذخیره می کند. این جداول با تبادل اطلاعات بین همسایه ها به روزآوری می شوند. این الگوریتم با نامهای دیگری نظیر الگوریتم مسیریابی توزیع شده بل من - فورد و الگوریتم فورد-فوجستون نیز شناخته می شود. الگوریتم فوق اولین الگوریتم مسیریابی استفاده شده در شبکه آرپانت می باشد. الگوریتم مسیریابی^۳ RIP که امروزه در شبکه جهانی اینترنت استفاده می شود، از روش مسیریابی بردار فاصله استفاده می کند. بسیاری از شرکت های تولید کننده مسیریاب، نظیر شرکت Cisco و Apple Talk نیز از فرم پیشرفته این الگوریتم در مسیریاب های خود استفاده می کنند. الگوریتم مسیریابی بردار فاصله یک الگوریتم وفقی می باشد که در آن هر مسیریاب شبکه به طور متناوب در فواصل زمانی معین جدول مسیریابی خود را برای دیگر مسیریاب های شبکه ارسال می کند. هر مسیریاب با دریافت جداول مسیریابی از مسیریاب های مجاور خود، اقدام به روزآوری جدول مسیریابی خود می کند. طبیعی است که بعد از مدتی، جدول مسیریابی کلیه مسیریاب های شبکه به روزآوری می شود و بدین ترتیب هر مسیریاب، کل شبکه را شناسایی می کند.

به عنوان مثال برای درک بیشتر این الگوریتم شبکه نشان داده شده در شکل (۶-۶) را در نظر بگیرید. در این شکل هفت شبکه مختلف از طریق مسیریاب های A,B,C,D,E و F به یکدیگر متصل شده اند. در شروع کار شبکه، هر مسیریاب فقط شبکه هایی را که به آنها اتصال مستقیم دارد می شناسد. در مثال فوق، ارزش عددی هر لینک^۱ می باشد. به عبارت دیگر مسیریاب های شبکه در انتخاب مسیر، مسیری را که دارای کمترین پرش می باشد، در نظر می گیرند.

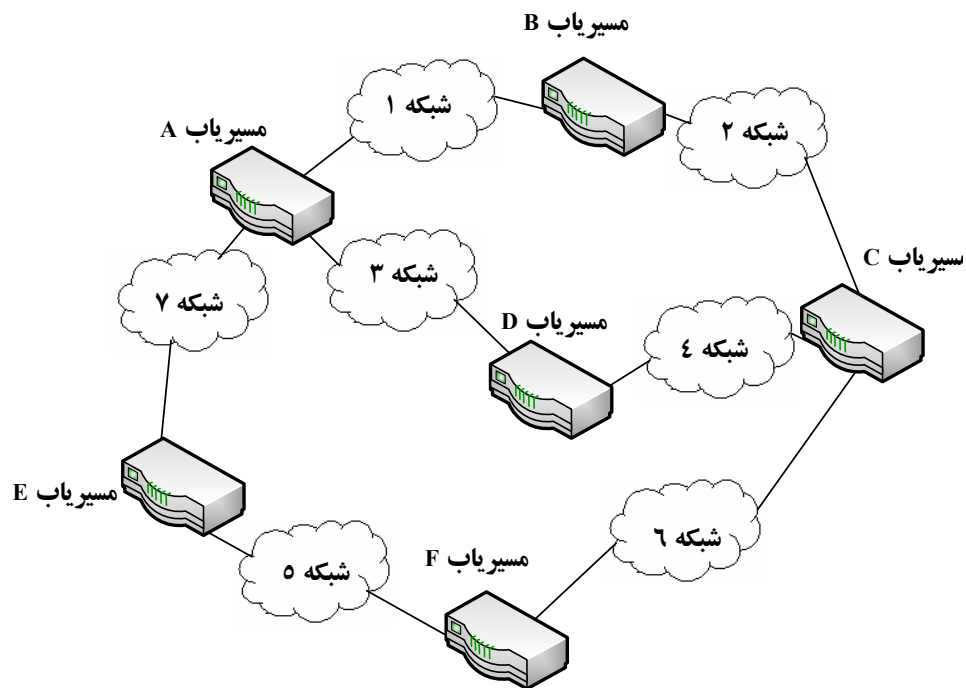
در شکل (۶-۷) نحوه به روزآوری جداول مسیریابی مسیریاب های شبکه نشان داده شده است. دیده می شود که بعد از گذشت مدتی، تمامی مسیریاب های شبکه از وضعیت شبکه مطلع شده و جدول مسیریابی خود را کامل می نمایند. البته بعد از این که جداول مسیریابی شبکه کامل شد، مسیریاب های شبکه همچنان به طور متناوب هر چند وقت یک بار اقدام به ارسال جداول مسیریابی خود به یکدیگر می نمایند. بدین ترتیب اگر تغییری در شبکه رخ دهد، نزدیکترین مسیریاب متوجه تغییر می شود و بعد از مدتی تمام مسیریاب های شبکه از بروز تغییر فوق آگاه می شوند.

^۱ Distance vector routing

^۲ Link state routing

^۳ Routing Information Protocol

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۶-۶): یک شبکه نمونه برای توصیف مسیریابی بردار فاصله

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)**مسیریاب A**

مسیریاب بعدی	فاصله	نکته
-	۱	۱
-	۱	۷
-	۱	۳

مسیریاب B

مسیریاب بعدی	فاصله	نکته
-	۱	۱
-	۱	۲

مسیریاب C

مسیریاب بعدی	فاصله	نکته
-	۱	۲
-	۱	۴
-	۱	۶

مسیریاب D

مسیریاب بعدی	فاصله	نکته
-	۱	۳
-	۱	۴

مسیریاب E

مسیریاب بعدی	فاصله	نکته
-	۱	۵
-	۱	۷

مسیریاب F

مسیریاب بعدی	فاصله	نکته
-	۱	۵
-	۱	۶

زمان ۰

مسیریاب بعدی	فاصله	نکته
-	۱	۱
-	۱	۷
-	۱	۳
B	۲	۲
D	۲	۴
E	۲	۵

مسیریاب بعدی	فاصله	نکته
-	۱	۱
-	۱	۲
A	۲	۳
A	۲	۷
C	۲	۴
C	۲	۶

مسیریاب بعدی	فاصله	نکته
-	۱	۲
-	۱	۴
-	۱	۶
B	۲	۱
D	۲	۳
F	۲	۵

زمان T

مسیریاب بعدی	فاصله	نکته
-	۱	۳
-	۱	۴
A	۲	۱
A	۲	۷
C	۲	۲
C	۲	۶

مسیریاب بعدی	فاصله	نکته
-	۱	۵
-	۱	۷
A	۲	۱
A	۲	۳
F	۲	۶

مسیریاب بعدی	فاصله	نکته
-	۱	۵
-	۱	۶
E	۲	۷
C	۲	۲
C	۲	۴

مسیریاب بعدی	فاصله	نکته
-	۱	۱
-	۱	۷
-	۱	۳
B	۲	۲
B	۳	۶
E	۲	۵
D	۲	۴

مسیریاب بعدی	فاصله	نکته
-	۱	۱
-	۱	۲
A	۲	۳
A	۲	۷
C	۲	۴
C	۳	۵
C	۲	۶

مسیریاب بعدی	فاصله	نکته
-	۱	۲
-	۱	۴
-	۱	۶
B	۲	۱
D	۲	۳
F	۳	۷
F	۲	۵

زمان 2T

مسیریاب بعدی	فاصله	نکته
-	۱	۳
-	۱	۴
A	۲	۱
A	۲	۷
C	۲	۲
C	۳	۵
C	۲	۶

مسیریاب بعدی	فاصله	نکته
-	۱	۵
-	۱	۷
A	۲	۱
A	۲	۳
A	۳	۲
A	۳	۴
F	۲	۶

مسیریاب بعدی	فاصله	نکته
-	۱	۵
-	۱	۶
E	۲	۷
C	۲	۲
E	۳	۱
E	۳	۳
C	۲	۴

شکل (۶-۷): مراحل تکمیل جدول مسیریابی شبکه نشان داده در شکل (۶-۶)

مسیریابی وضعیت لینک

مسیریابی وضعیت لینک، یک جایگزین مناسب با قابلیت انعطاف پذیری بالاتر و قدرت بیشتر از مسیریابی بردار فاصله است که منشأ پیدایش آن شبکه آرپانت می باشد. استفاده از این الگوریتم در چند سال اخیر گستردگی زیادی یافته است، به طوری که امروزه در اینترنت هم از این نوع مسیریابی استفاده وسیعی می شود. دو مشکل عمده روش مسیریابی بردار فاصله، باعث گردید که امروزه از مسیریابی وضعیت لینک در شبکه جهانی اینترنت استفاده وسیعی شود. نخست این که در مسیریابی بردار فاصله، معیار محاسبه تاخیر طول صف می باشد و الگوریتم هیچ توجهی به پهنای باند خطوط برای ارزیابی تاخیر ندارد. مساله دوم این که همگرا شدن الگوریتم بردار فاصله وقتی که مکانیسمهای شناسایی حلقه های مسیریابی نیز استفاده می شوند طولانی می باشد. به علت وجود دو مشکل فوق در مسیریابی بردار فاصله، مسیریابی وضعیت لینک جایگزین آن گردید. امروزه شکل های متنوعی از این نوع مسیریابی به طور گسترده در شبکه های کامپیوتری استفاده می شود.

در مسیریابی وضعیت لینک هر مسیریاب باید مراحل زیر را اجرا نماید:

۱- همسایگانش را شناسایی نماید و آدرس شبکه آنها را یاد بگیرد.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

۲- تاخیر و هزینه رسیدن به هر یک از همسایگانش را اندازه گیری کند.

۳- آنچه را که یاد گرفته است در قالب یک بسته اطلاعاتی در آورد و این بسته اطلاعاتی را به کلیه مسیرهای دیگر ارسال کند.

۴- کوتاهترین مسیر تا هر یک از مسیرهای دیگر را حساب کند.

طبق آنچه که در شماره ۳ گفته شده است، هر مسیرهای موظف به ساختن یک بسته اطلاعاتی است، که این بسته اخبار وضعیت لینک (LSA^1) نامیده می شود. پس از آن که ساخت LSA در مسیرهای کامل گردید، نوبت به ارسال آن به دیگر مسیرهای است که این کار به عهده یک پردازنده به نام سیل می باشد. در واقع ایده اصلی عملکرد این پردازنده از همان روش مسیریابی سیل که در بخش الگوریتم های ایستا گفته شد، گرفته شده است. پردازنده سیل باید سریع و قابل اعتماد باشد. بعد از گذشت چند دوره زمانی، پایگاه های داده وضعیت لینک در مسیرهای همگرا و یکسان خواهند شد. هر چه الگوریتم بهتر باشد این زمان همگرایی کوتاهتر خواهد بود. زمان همگرایی در الگوریتم فوق به میزان تأخیر انتشار در شبکه نیز بستگی دارد. بعد از همگرایی پایگاه های داده به کمک آن بهترین مسیر برای رسیدن به سایر نودها محاسبه می شود که در اصطلاح به این مرحله محاسبه مسیر گفته میشود. در مرحله محاسبه مسیر غالباً از الگوریتم های کوتاهترین فاصله نظیر $Dijkstra$ استفاده می شود. به همین جهت گاهی به پروتکل های وضعیت لینک، پروتکل های مبتنی بر کوتاهترین مسیر نیز گفته میشود. البته به غیر از الگوریتم کوتاهترین فاصله، می توان از الگوریتم های دیگری نیز استفاده نمود.

یکی از مسائل مهم در الگوریتم وضعیت لینک، بروز آوری LSA ها است. هر مسیرهای شبکه، زمانی که در محیط محلی اش تغییری رخ میدهد، LSA های خود را به روز درمی آورد. مدت زمانی که طول می کشد تا مسیرهای متوجه بروز تغییرات در محیط محلی اش شود، تأثیر زیادی در واکنش یک پروتکل وضعیت لینک به تغییرات شبکه دارد. ممکن است توسط دیگر پروتکل های در حال اجرا در مسیرهای شبکه، تغییرات در محیط عملیاتی محلی هر مسیرهای تشخیص داده شود. در بسیاری از پروتکل های وضعیت لینک، به طور متناوب هر مسیرهای نشانه "سلام" را به دیگر همسایگان شان می فرستد تا بدین وسیله متوجه غیبت احتمالی یک مسیرهای همسایه گردد. برای کسب اطمینان بیشتر، اکثر پروتکل های وضعیت لینک به طور متناوب LSA های خود را حتی وقتی که در شبکه تغییری رخ نداده باشد هم به روز درمی آورند.

در محاسبه مسیر می توان از روش های مسیریابی متنوعی نظیر مسیریابی پرش به پرش^۲ و مسیریابی مبدأ^۳ استفاده نمود. هر دو پروتکل فوق در الگوریتم مسیریابی وضعیت لینک حمایت می شوند. در مسیریابی پرش به پرش، بسته های ارسالی با استفاده از آدرس گیرنده بسته به سمت مقصد هدایت می شوند. در این روش بسته ورودی به هر مسیرهای (پرش) که می رسد، آن مسیرهای به طور مستقل از سایر مسیرهای و با توجه به جدول مسیریابی خود و آدرس مقصد بسته، اقدام به مسیریابی بسته می کند. در روش مسیریابی پرش به پرش احتمال وقوع حلقه های مسیریابی زیاد می باشد.

برای درک بهتر پروتکل مسیریابی وضعیت لینک، به ذکر یک مثال می پردازیم. به عنوان مثال شبکه نشان داده شده در شکل (۶-۸) (الف) را در نظر بگیرید. فرض کنید که هدف محاسبه بهترین مسیر بین نود A و نود E می باشد. همانطور که از شکل مشاهده می شود، بین دو نود فوق ۶ مسیر مختلف شامل: $ABE, ACE, ABDE, ACDE, ABDCE, ACDCE$ وجود دارد. بدیهی است که بهترین مسیر موجود مسیر $ABDE$ می باشد که دارای هزینه کمتر از سایر مسیرها است. مراحل الگوریتم وضعیت لینک به شرح زیر است:

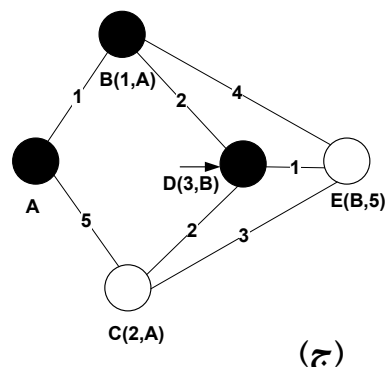
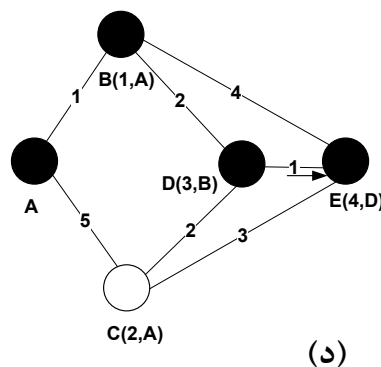
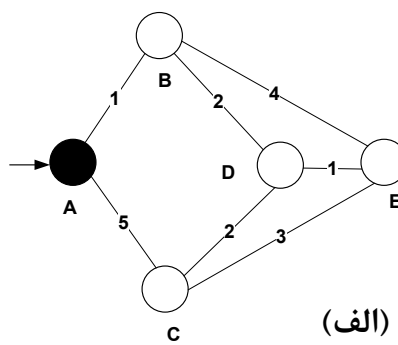
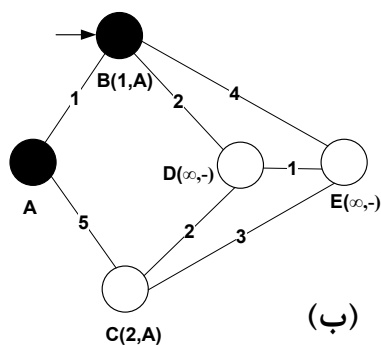
^۱ Link State Advertisement

^۲ Hop by hop routing

^۳ Source routing

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

۱. ابتدا نود مبدا A به عنوان نود شروع انتخاب شده و وضعیت آن دائمی می شود. نودهای دائمی در شکل به صورت دایره پررنگ نشان داده می شوند. نودهایی که دائمی نشده اند با دایره خالی نشان داده شده اند.
۲. با توجه به شکل، از بین نودهای B و C که ارتباط مستقیم به نود شروع A دارند، نود B به عنوان نود بعدی در مسیر انتخاب می شود. این نود در مقایسه با نود C دارای فاصله کمتری تا نود مبدا A است. وضعیت نود B به صورت دائمی درآمده و پررنگ می شوند.
۳. نود B به عنوان نود بعدی انتخاب شده و نودهای همسایه آن که ارتباط مستقیم با آن دارند بدست می آیند. با توجه به شکل فوق نودهای D و E به نود B متصل بوده ولی نود D دارای فاصله کمتری تا B بوده و بنابراین این نود به عنوان نود بعدی انتخاب می شود و وضعیت آن دائمی می شود.
۴. همسایه بعدی نود D که کمترین هزینه را دارا می باشد، نود E است. بنابراین نود فوق به عنوان نود بعدی انتخاب می شود.
۵. با توجه به اینکه نود E نود مقصد می باشد، بنابراین الگوریتم خاتمه یافته و مسیر ABDE با فاصله برابر با ۵ بدست می آید.



شکل (۶-۸): مثالی از مسیریابی وضعیت لینک

۴-۶- کنترل ازدحام

یکی دیگر از وظایف مهم لایه شبکه کنترل ازدحام می باشد. هنگامی که تعداد بسته های ارسالی کاربران به شبکه بیش از حد زیاد باشد، در این صورت بافر اکثر نودهای شبکه پرمی شود و پس از آن نودهای شبکه قادر به ارائه سرویس مطلوب به کاربران خود نمی باشند. در یک شبکه کامپیوتری، تعداد بسته های تحویل داده شده به مقصد، متناسب با تعداد بسته های

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

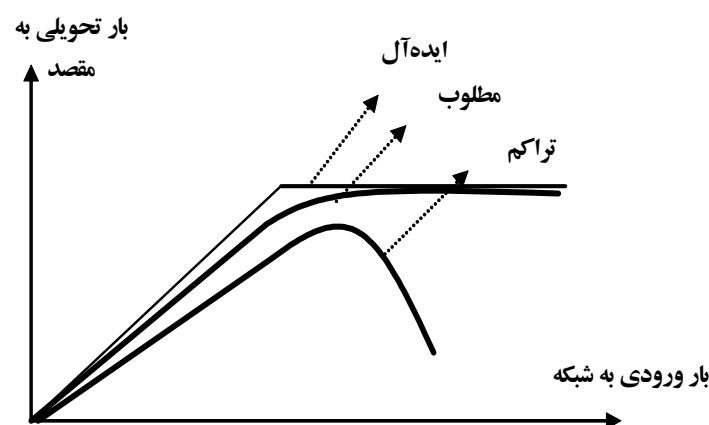
ارسالی می باشد. چنانچه بسته های ارسالی بیش از ظرفیت شبکه باشند، در این صورت نودهای شبکه قادر به تحمل انبوه بسته های ورودی نمی باشند و بدین ترتیب بسته های ورودی از بین می روند که این امر مشکل ازدحام و ازدحام را بدتر و بدتر می کند. چنانچه ترافیک ورودی به شبکه بیش از حد زیاد باشد، در این صورت کارایی شبکه به شدت افت می کند و تقریباً هیچ بسته ای به مقصد نمی رسد.

عوامل مختلفی باعث ایجاد ازدحام در شبکه های کامپیوتری می شوند. اولین عامل موثر در ایجاد ازدحام در نودهای شبکه، سرعت پردازش پایین نودهای شبکه می باشد. چنانچه نودهای میانی شبکه سرعت پردازش کمی داشته باشند، در این صورت تمامی بافرهای میانی شبکه لبریز می شوند.

دومین دلیل ایجاد ازدحام در شبکه های کامپیوتری، کند بودن سرعت لینک های خروجی هر نود می باشد. به عبارت دیگر چنانچه نرخ ورود ترافیک به نودهای شبکه، بیشتر از ظرفیت خطوط خروجی باشد، احتمال وقوع ازدحام زیاد می باشد. چنانچه در شبکه، ازدحام به وجود آید، بافرهای میانی شبکه لبریز می شوند و باگذشت زمان در صورتی که اقدام مناسب انجام نشود، وضعیت ازدحام بدتر می گردد. اگر بسته ارسالی فرستنده در بافرهای میانی شبکه از بین برود، فرستنده بعد از مدتی دوباره اقدام به ارسال بسته فوق می کند؛ که این امر باعث افزایش شدت ازدحام می شود. با توجه به این که فرستنده با ارسال هر بسته، آن را در حافظه خود ذخیره می سازد تا در صورت نیاز دوباره آن را ارسال نماید، چنانچه ازدحامی در شبکه به وقوع پیوندد، بسته های ارسالی فرستنده از بین رفته و بدین ترتیب فرستنده هیچگاه نمی تواند بافر خود را خالی نماید.

باید توجه نمود که کنترل ازدحام با کنترل جریان متفاوت می باشد. کنترل ازدحام به روال های لازم جهت کنترل تمام نودهای شبکه و بافرهای میانی آنها برای جلوگیری از کاهش کارایی شبکه دلالت دارد؛ در حالی که کنترل جریان فقط بین دو نقطه انجام می شود و هنگامی که یک فرستنده سریع به یک گیرنده کند، داده هایی را ارسال می دارد از کنترل جریان برای تعدیل سرعت ارسال فرستنده و تنظیم آن با سرعت دریافت گیرنده استفاده می شود.

در شکل (۶-۹) نمودار تعداد بسته های تحویل داده شده در مقصد بر حسب تعداد بسته های ارسالی به شبکه رسم شده است. همان طور که در این شکل دیده می شود، با افزایش تعداد بسته های ارسالی به شبکه، تعداد بسته های تحویل داده شده در مقصد نیز افزایش می یابد. چنانچه بسته های ارسالی از حدی بیشتر شوند، شبکه با ازدحام مواجه می گردد و قادر به ارائه کارایی مطلوب خود نمی باشد.



شکل (۶-۹): تاثیر ازدحام بر کارایی شبکه

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

یکی دیگر از وظایف مهم لایه شبکه ، ارتباط بین شبکه های می باشد. همان طور که در فصل اول به آن اشاره شد، شبکه های کامپیوتری دارای مزایای متعددی می باشند. شبکه سازی و اتصال شبکه های کامپیوتری به یکدیگر نیز دارای مزایای زیادی است. در راستای ایجاد یک شبکه وسیع جهانی، اتصال شبکه ها به یکدیگر و ایجاد یک شبکه بزرگتر دارای مزایا و اهداف متعددی می باشد.

اتصال یک یا چند شبکه و ایجاد یک شبکه بزرگتر و اتصال آنها به یکدیگر را ارتباط بین شبکه ای گویند. چنانچه فرستنده و گیرنده یک بسته در دو شبکه متفاوت با پروتکل های غیریکسان قرارداد داشته باشند، در این صورت لزوم تبدیل بسته ها از یک پروتکل به پروتکل دیگر و استفاده از تجهیزات خاص ارتباط بین شبکه ای حس می شود. به شبکه هایی که از اتصال چند شبکه به یکدیگر به وجود می آید، در اصطلاح **internet** گفته می شود. البته باید توجه نمود که شبکه جهانی **Internet** نمونه کاملی از یک **internet** است که در آن میلیون ها کامپیوتر به یکدیگر متصل شده اند.

اتصال شبکه ها به یکدیگر و ایجاد یک شبکه وسیعتر در رده های مختلفی قابل انجام می باشد که عبارتند از:

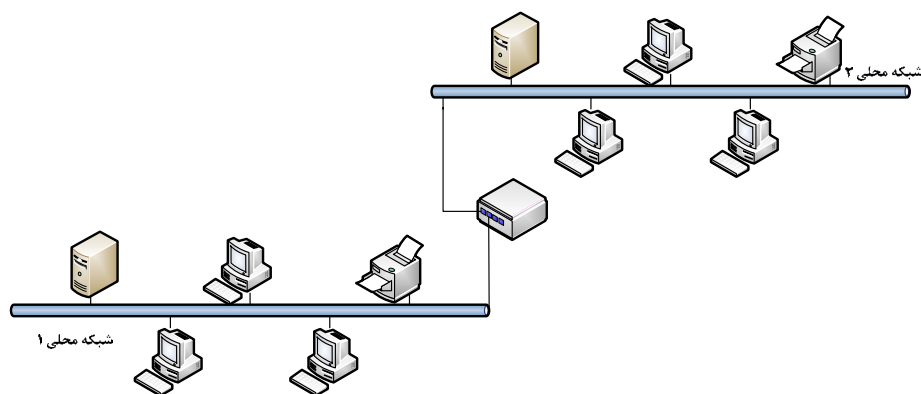
- **اتصال LAN به LAN**: در این حالت دو شبکه محلی مستقیماً با کمک تجهیزات ارتباط بین شبکه ای به یکدیگر متصل می شوند. به عنوان مثال اتصال دو شبکه محلی در یک ساختمان به یکدیگر نمونه ای از اتصال **LAN** به **LAN** می باشد.

- **اتصال LAN به WAN**: در این حالت یک شبکه محلی به یک شبکه گسترده اتصال می یابد. برقراری اتصال فوق به تجهیزات ارتباط بین شبکه ای نیاز دارد. به عنوان مثال اتصال شبکه محلی یک دانشگاه به اینترنت نمونه ای از اتصال **LAN** به **WAN** است.

- **اتصال WAN به WAN**: در این حالت دو شبکه گسترده از طریق تجهیزات مناسب به یکدیگر متصل شده و قادر به تبادل اطلاعات با یکدیگر می باشند. اتصال شبکه دیتای یک کشور به شبکه جهانی اینترنت، نمونه ای از این نوع اتصال می باشد.

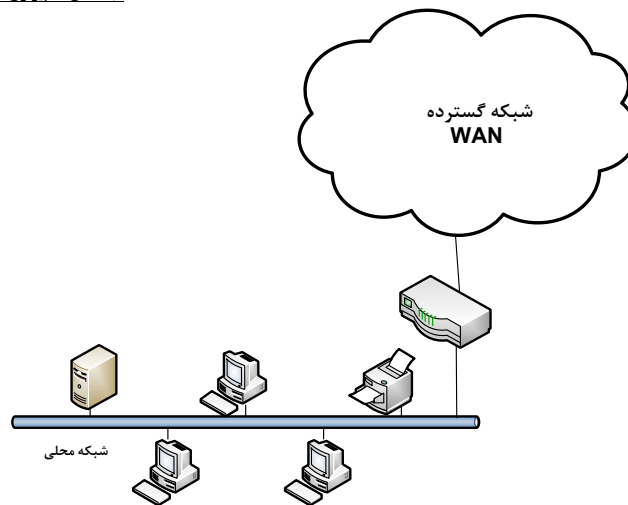
- **اتصال دو LAN از طریق یک یا چند WAN**: در این حالت دو شبکه محلی که در فاصله دور از یکدیگر قرار گرفته اند، از طریق امکانات ارتباط بین شبکه ای با کمک یک شبکه گسترده به یکدیگر متصل می شوند. اتصال دو شبکه محلی یک سازمان از طریق شبکه مخابرات نمونه ای از این نوع اتصال است.

در شکل (۶-۱۰) مثالی از انواع اتصال فوق آورده شده است. جهت اتصال دو شبکه به یکدیگر از تجهیزات ارتباط بین شبکه ای استفاده می شود. براساس این که دو شبکه ای که به یکدیگر متصل می شوند، در چه لایه هایی با یکدیگر مشترک و در چه لایه هایی با یکدیگر متفاوت هستند، از تجهیزات متفاوتی برای اتصال آنها به یکدیگر استفاده می شود. در زیر به بررسی مهمترین تجهیزات ارتباط بین شبکه ای می پردازیم.

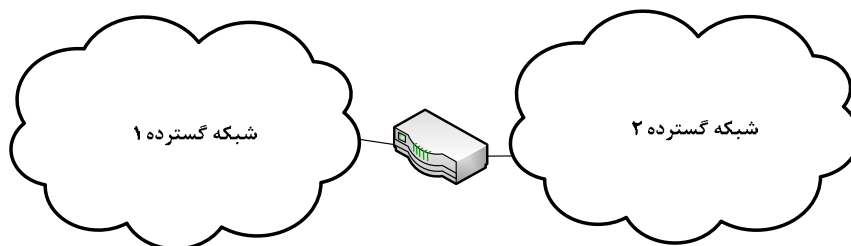


(الف)

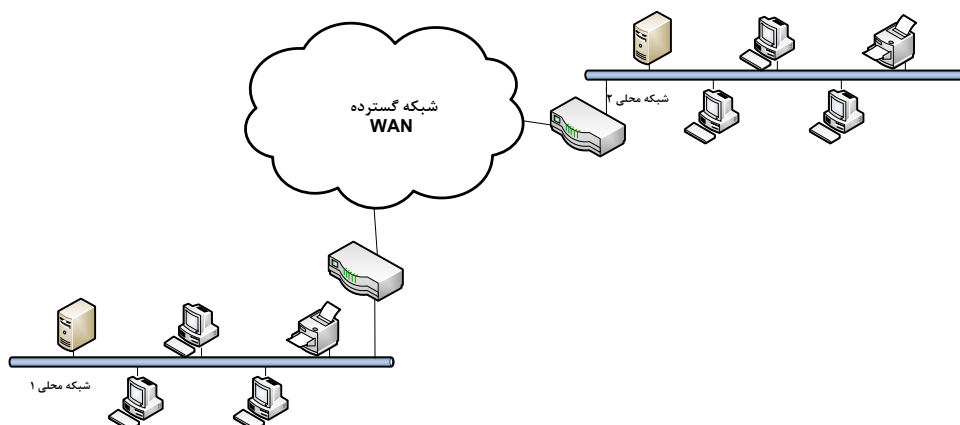
شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



(ب)



(ج)



(د)

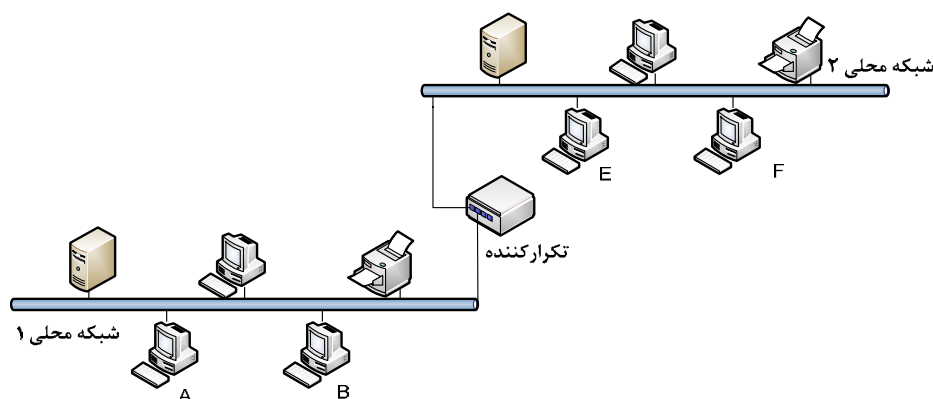
شکل (۶-۱۰) اتصال شبکه ها به یکدیگر

الف (اتصال LAN به LAN ب) اتصال LAN به WAN

ج) اتصال WAN به WAN د) اتصال LAN به LAN از طریق WAN

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

یک تکرارکننده در سطح لایه فیزیکی عمل می کند و جهت گسترش شبکه های محلی استفاده می شود. همان طور که در فصل قبل نیز اشاره شد، چنانچه کابل شبکه بیش از حد طولانی باشد، در این صورت سیگنال ارسالی در کابل تضعیف می شود و دیگر قابل دریافت در گیرنده نمی باشد. برای رفع این مشکل از تکرارکننده استفاده می گردد. در شکل (۶-۱۱) مثالی از نحوه استفاده از تکرارکننده برای اتصال دو شبکه محلی آورده شده است. باید توجه نمود که دو قسمت مختلف شبکه که توسط یک تکرارکننده به هم متصل می شوند، در حقیقت جزئی از یک شبکه واحد می باشند. مطابق با شکل فوق چنانچه به عنوان مثال ایستگاه A قابی را برای ارسال به ایستگاه B، وارد شبکه نماید، تمامی ایستگاه های شبکه از جمله E و F نیز این قاب را دریافت می دارند. به عبارت دیگر تکرارکننده هیچ گونه هوشمندی در فیلتر نمودن ترافیک از خود نشان نمی دهد و کلیه ترافیک های ورودی به خود را عبور می دهد و به طرف مقابل ارسال می دارد.



شکل (۶-۱۱) : اتصال دو قسمت مختلف شبکه توسط یک تکرارکننده

۶-۵-۲- پل

یک پل در هر دو سطح لایه فیزیکی و پیوند داده از مدل لایه ای OSI عمل می کند. توسط یک پل امکان تقسیم بندی یک شبکه بزرگ به قطعات کوچکتر فراهم می آید. برخلاف تکرارکننده، پل ها قابلیت فیلتر نمودن ترافیک های ورودی را به خود دارند. پل آدرس مقصد قاب ورودی را بررسی می کند و در صورتی که آدرس گیرنده قاب در طرف دیگر پل قرار داشته باشد، اجازه عبور بسته را می دهد ولی در غیر این صورت از عبور بسته جلوگیری می کند.

با توجه به نحوه عملکرد پل، می توان نتیجه گرفت که یکی از مزایای عمده آن قابلیت فیلتر نمودن ترافیک و جلوگیری از ارسال ترافیک های ناخواسته به سایر قسمت های یک شبکه می باشد. در شکل (۶-۱۲) مثالی از دو شبکه که با استفاده از پل به یکدیگر متصل شده اند آورده شده است. به عنوان مثال در این شکل، چنانچه ایستگاه A قابی را به مقصد ایستگاه D ارسال دارد، با توجه به این که فرستنده و گیرنده قاب در یک شبکه قرار دارند، پل متوجه شده و اجازه عبور قاب را از خود نمی دهد؛ ولی چنانچه مقصد قاب ارسالی A، ایستگاه G باشد، قاب از پل عبور می کند.

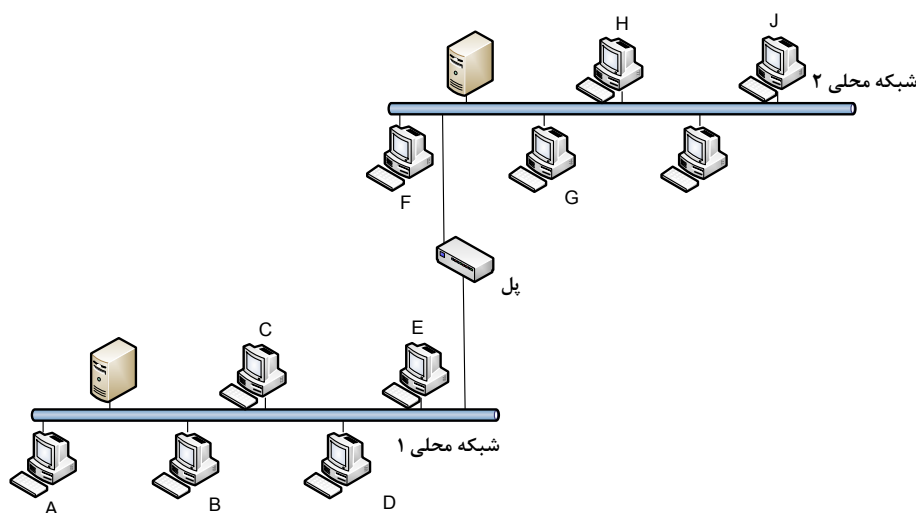
هر پل برای انجام صحیح عملیات فیلتر نمودن بسته ها، باید حاوی یک جدول آدرس باشد که تمامی آدرس های فیزیکی ایستگاه های موجود در شبکه را دارا می باشد. با توجه به این که جدول مسیریابی آدرس فوق به چه صورت ایجاد و مدیریت شود، سه نوع مختلف از پل وجود دارند که در زیر به بررسی آنها می پردازیم:

- **پل ساده** : این نوع پل، ساده ترین و ارزانترین نوع پل می باشد. در این نوع پل، جدول آدرس ایستگاه ها باید به صورت دستی توسط یک اپراتور وارد گردد. طبیعی است که جدول فوق ثابت می باشد و در صورتی که یک ایستگاه

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۱

جدید به شبکه اضافه شود، جدول آدرس باید به روزآوری شود. همچنین در صورت حذف یک ایستگاه از شبکه، آدرس آن ایستگاه در جدول آدرس پل باید از بین برود.

- **پل آموزش گیرنده:** این نوع پل به صورت خودکار اقدام به تولید جدول آدرس می کند. روش ایجاد جدول آدرس به این صورت است که پل با شروع به کار شبکه و ارسال قاب بین ایستگاه های شبکه، اقدام به آموزش و فراگیری آدرس های فیزیکی هر یک از ایستگاه های شبکه می کند. در ابتدای راه اندازی شبکه، جدول آدرس های پل آموزش گیرنده خالی می باشد، ولی با گذشت زمان این جدول تکمیل می شود. با توجه به قدرت بالای این نوع پل و توانایی ایجاد جداول آدرس به صورت خودکار، قیمت پل های آموزش گیرنده به مراتب بیشتر از پل های ساده می باشد.
- **پل چندین درگاه!** سومین نوع پل، پل چندین درگاه می باشد. این نوع پل که خود می تواند از نوع ساده و یا آموزش گیرنده باشد، دارای چندین درگاه می باشد و می توان به وسیله آن چندین شبکه مختلف را به یکدیگر متصل نمود.



شکل (۶-۱۲): اتصال دو شبکه مختلف به یکدیگر به وسیله پل

۶-۵-۳- مسیر یاب

یکی دیگر از مهمترین تجهیزات ارتباط بین شبکه ای، مسیر یاب های شبکه می باشد. مسیر یاب ها به آدرس های شبکه دسترسی دارند و با کمک نرم افزار مسیر یابی خود، قادر به محاسبه و انتخاب بهترین مسیر بین مبدأ و مقصد می باشند. هر مسیر یاب شبکه در سطح لایه سوم مدل مرجع OSI عمل می کند و با دریافت یک بسته از یکی از درگاه های ورودی خود و با پردازش بر روی سرآیند بسته های لایه سوم، آدرس گیرنده بسته را تعیین می کند و سپس با کمک جدول مسیر یابی خود، مسیر مناسب برای ارسال بسته به مقصد را به دست می آورد. در شکل (۶-۱۳) مثالی از نحوه اتصال چندین شبکه به وسیله مسیر یاب های شبکه آورده شده است.

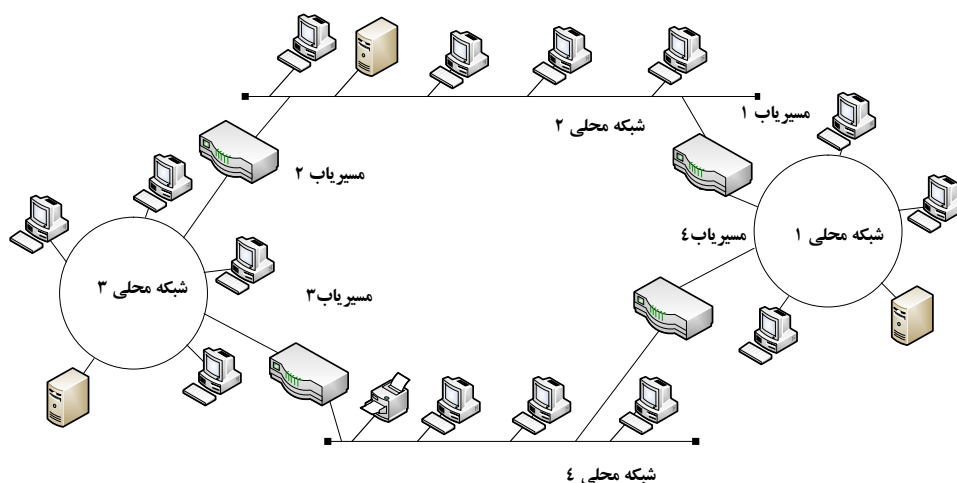
۶-۵-۴- دروازه^۲

^۱ Multiport bridge

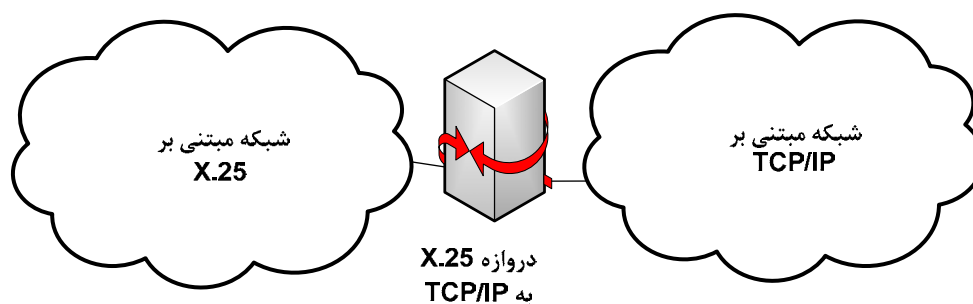
^۲ Gateway

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

مطابق با شکل (۶-۱۴) یک دروازه در سطح تمام ۷ لایه OSI عمل می کند. یک دروازه در حقیقت به صورت یک مبدل پروتکل عمل می کند. هنگامی که بخواهیم دو شبکه کاملاً متفاوت را که دارای معماری های مختلف هستند به یکدیگر متصل نماییم، از دروازه استفاده می شود. به عنوان مثال چنانچه بخواهیم یک شبکه TCP/IP را به یک شبکه X.25 متصل نماییم، با توجه به این که این دو شبکه دارای معماری های مختلف هستند و پروتکل های مختلفی در این دو شبکه وجود دارد، برای اتصال این دو شبکه نیاز به یک دروازه داریم.



شکل (۶-۱۳): اتصال چندین شبکه مختلف به یکدیگر با استفاده از مسیر یاب



شکل (۶-۱۴): اتصال دو شبکه مختلف به یکدیگر با استفاده از دروازه

۶-۶- شبکه سرویس مجتمع دیجیتال (ISDN)

ISDN که یک نوع شبکه سوئیچینگ مداری است، تحولی در شبکه های مخابراتی به حساب می آید. شبکه ISDN قادر به برقراری اتصال های انتها به انتها بر روی خطوط دیجیتال می باشد. بسیاری از شرکت های مخابرات کشورها اقدام به جایگزینی شبکه آنالوگ موجود خود با شبکه کاملاً دیجیتال ISDN کرده اند. بدین ترتیب در این شبکه ها امکان برقراری ارتباطات محلی و بین المللی با سرعت بالا و کیفیت خوب فراهم می آید.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

در شبکه های ISDN، کاربران قادر به ارسال اطلاعات داده، صوت، تصویر و فاکس بر روی یک شبکه دیجیتال واحد می باشند. هدف اصلی ISDN فراهم سازی سرویس دیجیتال یک پارچه برای کاربران می باشد. این سرویس به ۳ دسته کلی سرویس حامل^۱، تله سرویس و سرویس تکمیلی^۲ تقسیم بندی می شوند.

سرویس حامل، محیطی فراهم می آورند که در آن کاربران قادر به ارسال اطلاعات صوت و تصویر و داده بدون آن که شبکه، محتوای اطلاعات را تغییر دهد می باشند. در این گونه سرویس، شبکه اطلاعات موجود در بسته ها را پردازش نمی کند، بنابراین هیچ گونه تغییری در محتوای آنها ایجاد نمی شود. این سرویس متعلق به ۳ لایه اول مدل مرجع OSI می باشند. برای پیاده سازی سرویس حامل می توان از شبکه های سوئیچینگ مداری، سوئیچینگ بسته ای، Frame Relay یا Cell Relay استفاده نمود.

در سرویس تله سرویس، شبکه ممکن است محتویات بسته های دریافتی را پردازش و یا تغییر دهد. این سرویس مطابق با لایه ۴ الی ۷ مدل مرجع OSI می باشند. سرویس فوق متکی بر امکانات سرویس حامل هستند و برای برآورده کردن نیازهای کاربران، بدون آن که آنها از جزئیات پردازش در شبکه آگاه باشند طراحی شده اند. برخی از مهمترین سرویس تله سرویس عبارتند از: تلفن، تله تکس، تله فاکس، تلکس و کنفرانس راه دور. سرویس تکمیلی، قابلیت های اضافی به سرویس حامل و تله سرویس اضافه می نمایند. نمونه ای از این سرویس عبارتند از: سرویس شارژینگ معکوس، انتظار مکالمه و تبادل پیام که تماماً در شرکت های تلفنی امروزی استفاده می شوند.

۶-۶-۱- تاریخچه ISDN

شبکه های مخابراتی اولیه تماماً به صورت آنالوگ عمل می کردند و از آنها برای ارسال اطلاعات آنالوگ نظیر صوت استفاده می شده است. با پیدایش پردازشهای دیجیتال، مشتریان علاوه بر صوت، محتاج به مبادله داده گردیدند. در این زمینه مودم برای مبادله پیام های دیجیتال بر روی خطوط آنالوگ موجود طراحی و ساخته شد.

به منظور کاهش هزینه ها و بهبود کارایی شبکه، شرکت های تلفنی با حفظ سرویس آنالوگ خود به تدریج شروع به افزودن فن آوری دیجیتال به شبکه های خود کردند. در این مقطع زمانی مشتریان به سه نوع تقسیم بندی می شدند که عبارت بودند از: مشتریان سنتی سرویس آنالوگ، مشتریانی که از امکانات شبکه آنالوگ برای ارسال اطلاعات دیجیتال از طریق مودم استفاده می نمودند و مشتریانی که از سرویس دیجیتال برای مبادله اطلاعات دیجیتال استفاده می کردند.

با توجه به این که در آن مقطع زمانی، مشتریان گروه اول برجسته ترین و بیشترین مشتریان شرکت های تلفنی را تشکیل می دادند، بنابراین بیشتر سرویس پیشنهادی شرکت های تلفنی همچنان آنالوگ باقی ماند. با گذشت زمان و پیدایش شبکه های دیجیتال، مشتریان علاقمند به استفاده از انواع شبکه های داده گردیدند.

به منظور برآورده کردن این نیازها شرکت های تلفن اقدام به ایجاد شبکه های مجتمع دیجیتال نمودند. یک شبکه مجتمع دیجیتال مجموعه ای از شبکه ها می باشد که برای برآورده کردن نیازهای مختلف کاربران طراحی شده است. برای دسترسی به شبکه های مجتمع دیجیتال از کانال های سرعت بالای دیجیتال که به صورت زمانی بین کاربران تقسیم می شوند، استفاده می گردد.

هر چند امروزه خطوط دیجیتالی نظیر DDS، DSS و غیره موجود می باشد، ولی همچنان برخی مشترکین از خطوط آنالوگ استفاده می نمایند.

^۱Bearer services

^۲Supplementary services

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۱

شبکه های ISDN سرویس مشترکین را با شبکه های مجتمع دیجیتال ترکیب می نمایند. سرویس دیجیتال به مراتب کارآمدتر و انعطاف پذیرتر از سرویس آنالوگ می باشد. به منظور دستیابی به مزایای شبکه های مجتمع دیجیتال، خطوط آنالوگ موجود با خطوط دیجیتال جایگزین می شوند. در این حالت صوت آنالوگ در مبدأ تبدیل به دیجیتال می شود و نیازی به حامل های آنالوگ ندارد. بنابراین امکان ارسال داده، صوت، تصویر و فاکس بر روی شبکه های دیجیتال فراهم می شود. در شبکه های ISDN تمام سرویس مشتریان از آنالوگ به دیجیتال تبدیل می شوند. به خاطر انعطاف پذیری بالای این شبکه ها، امکان دسترسی کاربران به سرویس درخواستی وجود دارد. هر کاربر از طریق یک خط دیجیتال به اداره مرکزی ISDN متصل می شود. سرعت خطوط دیجیتال متناسب با نیازهای کاربران، متفاوت می باشد.

برای دسترسی به انعطاف پذیری بیشتر، خطوط دیجیتال بین مشتریان و شبکه ISDN به کانال هایی با اندازه های متفاوت تقسیم بندی می شود. در ISDN، سه نوع کانال وجود دارد که هر یک دارای نرخ ارسال متفاوتی هستند. این ۳ کانال عبارتند از: کانال B (با سرعت ۶۴ کیلوبیت بر ثانیه)، کانال D (با سرعت ۱۶ و ۶۴ کیلو بیت بر ثانیه) و کانال H (با سرعت ۳۸۴، ۱۵۳۶ و ۱۹۲۰ کیلوبیت بر ثانیه).

کانال B، کانال پایه کاربر می باشد که با کمک آن کاربران قادر به ارسال هر گونه اطلاعات دیجیتال به صورت دو طرفه با حداکثر نرخ ارسال ۶۴ کیلو بیت بر ثانیه می باشند. به عنوان مثال از کانال B می توان برای مبادله داده های دیجیتال، صوت دیجیتال و یا سایر اطلاعات کم سرعت استفاده کرد. با استفاده از تسهیم سازها می توان داده های چندین منبع مختلف را به صورت یک جا بر روی خطوط ارسال کرد.

کانال های D، با توجه به نیاز کاربران می توانند دارای سرعت ۱۶ یا ۶۴ کیلوبیت بر ثانیه باشند. قبل از پیدایش ISDN اطلاعات کنترلی (نظیر برقراری ارتباط، سیگنال زنگ، وقفه در ارتباط و یا اطلاعات همزمانی) در همان کانالی که داده ها ارسال می شدند، مبادله می گردیدند. در شبکه های ISDN سیگنال های کنترلی از کانال مخصوص خود (کانال D) استفاده می کنند. به این حالت، سیگنالینگ کانال مشترک گفته می شود، زیرا کانال D اطلاعات سیگنالینگ تمام مشتریان موجود در یک مسیر را حمل می کند.

کانال های H برای دسترسی به سرعت های بالاتر نظیر ۳۸۴ کیلوبیت بر ثانیه (H_0)، ۱۵۳۶ کیلو بیت بر ثانیه (H_{11}) و ۱۹۲۰ کیلو بیت بر ثانیه (H_{12}) استفاده می شوند. با استفاده از این نرخ های ارسال می توان برنامه های کاربردی سرعت بالا نظیر تصاویر زنده ویدیویی و کنفرانس های صوتی و تصویری راه دور را پیاده سازی نمود.

واسط های کاربران به شبکه های دیجیتال در حال حاضر به دو نوع واسط نرخ پایه (BRI^1) و واسط نرخ اولیه (PRI^2) تقسیم بندی می شوند. متناسب با سرعت مورد نیاز کاربران می توان از هر یک از این دو نوع واسط استفاده کرد. واسط نرخ پایه از دو کانال B و یک کانال ۱۶ کیلو بیتی D تشکیل شده است. بنابراین مجموع نرخ کانال پایه ۱۴۴ کیلو بیت ثانیه می باشد. برای عملکرد مناسب این کانال نیاز به ۴۸ کیلوبیت بر ثانیه بالاسری اضافی می باشد، بنابراین نرخ کلی این کانال ۱۹۲ کیلوبیت بر ثانیه است. از این نوع کانالها در کاربردهای سرعت پایین استفاده می شود.

واسط PRI شامل ۳۲ کانال B و یک کانال ۶۴ کیلو بیت بر ثانیه D است. علاوه بر آن از ۸ کیلو بیت بر ثانیه بالاسری برای نگهداری این کانال استفاده می شود؛ بنابراین نرخ کلی این کانال ۱/۵۴۴ مگابیت بر ثانیه است. با توجه به سرعت بالای این واسط ها، از آنها در کاربردهای سرعت بالا نظیر اتصال شبکه های محلی به یکدیگر استفاده می گردد. واسط های PRI سازگار با خطوط T_1 می باشند. البته در اروپا واسط های فوق شامل ۳۰ کانال B و ۲ کانال D است. بنابراین نرخ

^۱ Basic Rate Interface

^۲ Primary Rate Interface

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

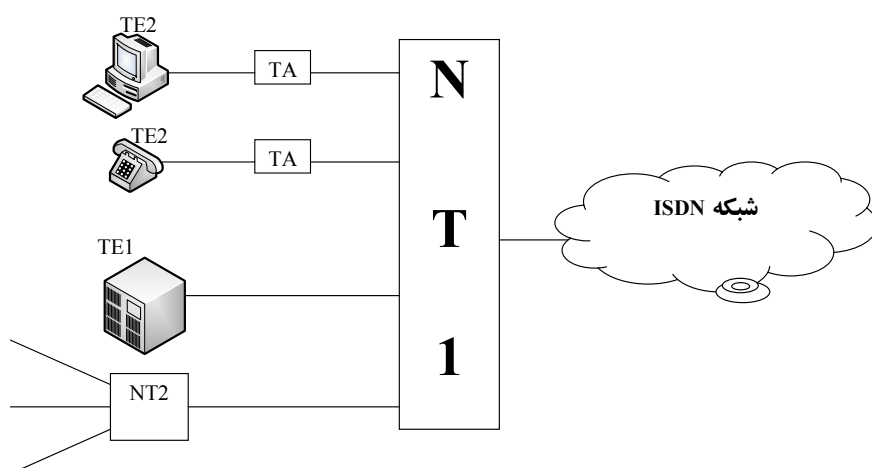
کلی آن ۲/۰۴۸ مگابیت بر ثانیه می باشد که سازگار با خطوط E_1 است. برای نیازهای تخصصی تر سایر ترکیب های مختلف نظیر $4H_0+D$ ، $3H_0+D$ و $H_{12}+D$ استفاده می گردد.

در شبکه های ISDN تجهیزاتی که برای اتصال کاربران به شبکه در نرخ ارسال پایه و یا نرخ ارسال اولیه استفاده می شوند، براساس وظایفی که برعهده آنها است به گروه های عملیاتی متفاوتی تقسیم می شوند. از میان این گروه ها، مشتریان تجهیزات ویژه ای را که به بهترین شکل، مناسب نیازهای آنها می باشد انتخاب می کنند.

در شبکه های ISDN با استفاده از وسایل و تجهیزات انتخاب شده کاربر، گروه های عملیاتی قابل پیاده سازی می باشند. این گروه های عملیاتی عبارتند از پایان دهنده های شبکه (نوع ۱ و ۲)، تجهیزات پایانه (نوع ۱ و ۲) و آداپتورهای پایانه. یک پایان دهنده شبکه نوع ۱ ($NT1^1$) به عنوان پایان دهنده الکتریکی و فیزیکی شبکه ISDN به تجهیزات کاربر عمل می کند. در $NT1$ رشته داده های ارسالی کاربران به صورت قاب های مشخصی تبدیل می شود و سپس بر روی خطوط دیجیتال ارسال می گردد. عملیات $NT1$ مشابه عملیات لایه فیزیکی در مدل مرجع OSI می باشد. پایان دهنده شبکه نوع ۲ ($NT2^2$) عملیات لایه های فیزیکی، پیوند داده و شبکه را در مدل مرجع OSI انجام می دهد. توسط $NT2$ عملیات مختلفی نظیر تسهیم سازی (لایه ۱) کنترل جریان (لایه ۲) و بسته بندی (لایه ۳) انجام می شود. در حقیقت $NT2$ عملیات پردازش سیگنالها را بین تجهیزات تولید کننده داده و $NT1$ انجام می دهد.

بین $NT1$ و $NT2$ یک کانال فیزیکی نقطه به نقطه وجود دارد. عملیات $NT1$ و $NT2$ در انواع تجهیزات مختلف نظیر مرکز تلفن خصوصی و یا حتی یک شبکه محلی قابل پیاده سازی است.

تجهیزات پایانه نوع ۱ ($TE1^3$) مشابه DTE در شبکه X.25 عمل می کند. به هر وسیله ای که استاندارد ISDN را حمایت نماید، نظیر تلفن دیجیتال، پایانه های داده، تجهیزات صوت مجتمع و فاکس دیجیتال، $TE1$ اطلاق می شود. تجهیزات پایانه نوع ۲ ($TE2^4$)، شامل وسایل غیر ISDN نظیر: پایانه ها، ایستگاه های کاری و کامپیوتر میزبان می باشد. تجهیزات $TE2$ مستقیماً سازگار با ISDN نیست، بلکه برای اتصال آنها به شبکه ISDN نیاز به تجهیزات خاصی به نام آداپتورهای پایانه (TA^5) می باشد. در شکل (۶-۱۵) مثالی از گروه بندی عملیاتی $TE1$ ، $TE2$ ، TA ، $NT1$ و $NT2$ آورده شده است.

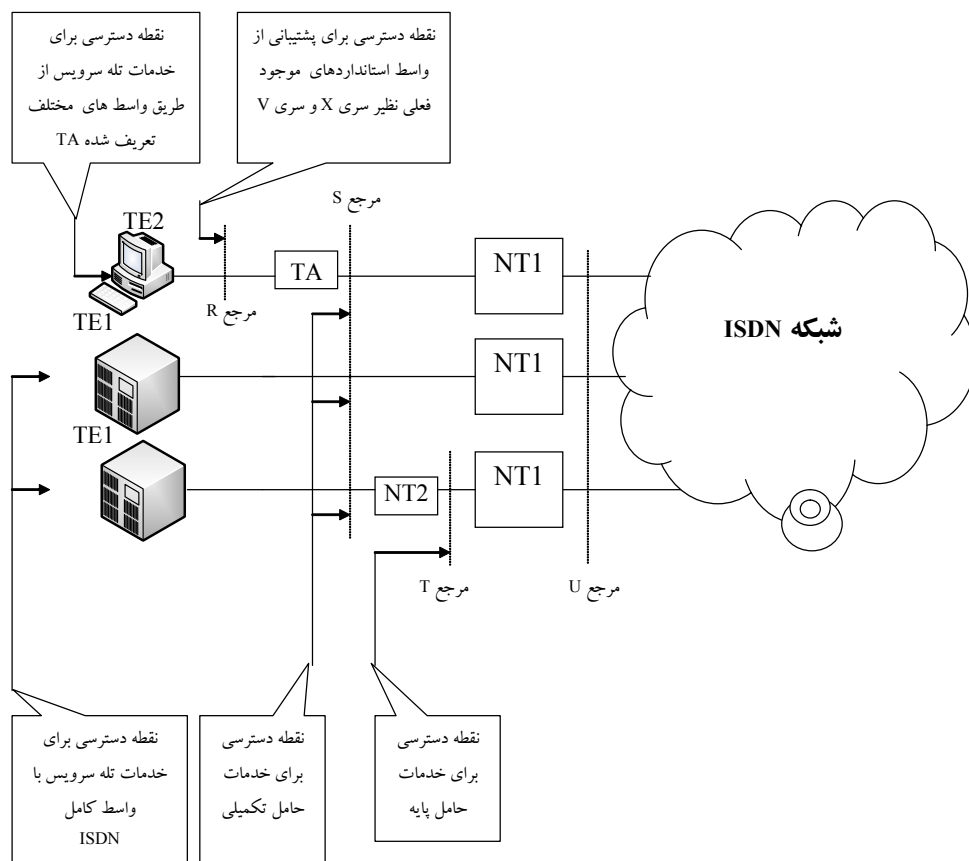


- ¹ Network Terminator 1
- ² Network Terminator 2
- ³ Terminal Equipment 1
- ⁴ Terminal Equipment 2
- ⁵ Terminal Adapter

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

شکل (۶-۱۵): گروه های عملیاتی ISDN

در شبکه های ISDN واسط بین دو گروه عملیاتی ISDN که قبلاً توضیح داده شد، توسط نقاط مرجع خاصی با نام نقاط مرجع R، S، T و U شناخته می شود. در شکل (۶-۱۶) جایگاه نقاط مرجع فوق آورده شده است. مطابق با این شکل نقطه مرجع R، واسط بین TA و TE2، نقطه مرجع S، واسط بین TA و NT1 و همچنین TE1 و NT1، نقطه مرجع T، واسط بین NT1 و NT2 و نقطه مرجع U واسط بین NT1 و شبکه ISDN را مشخص می کند.



شکل (۶-۱۶): نقاط مرجع ISDN

۶-۶-۲- لایه های ISDN

سازمان ITU-T از مدل توسعه یافته ای به عنوان مدل مرجع ISDN استفاده نموده است. در ISDN به جای استفاده از یک معماری ۷ لایه مشابه OSI، سه صفحه جدا از هم شامل: صفحه کاربر، صفحه کنترل و صفحه مدیریت تعریف شده است. صفحه کاربر عملیات کانال B و H را تعریف می کند (اتصال کاربر به کاربر). صفحه کنترل، عملیات کانال سیگنالینگ D و صفحه مدیریت، عملیات مدیریت دو صفحه دیگر را انجام می دهد. تمام این سه صفحه به ۷ لایه مطابق با مدل مرجع OSI تقسیم می شوند. در شکل (۶-۱۷) مدل لایه ای ISDN نشان داده شده است. همچنین در شکل (۶-۱۸) مدل لایه ای صفحه کاربر (کانال B) و صفحه کنترل (کانال D) نشان داده شده است.

صفحه مد پیریت	
صفحه کاربر	صفحه کنترل
لایه کاربرد	لایه کاربرد
لایه ارائه	لایه ارائه
لایه جلسه	لایه جلسه
لایه حمل	لایه حمل
لایه شبکه	لایه شبکه
لایه پیونداده	لایه پیونداده
لایه فیز یکی	لایه فیز یکی

صفحه مد پیریت

مطابق با شکل (۶-۱۸) در سطح لایه فیزیکی هر دو صفحه مشابه یکدیگر هستند. در این لایه از نرخ ارسال پایه و اولیه استفاده می‌شود. در سطح لایه پیوند داده، صفحه کاربر از پروتکل LAP-B و صفحه کنترل از پروتکل LAP-D استفاده می‌کند. در سطح لایه شبکه، صفحه کاربر از شبکه‌های سوئیچینگ مداری، سوئیچینگ بسته ای (X.25)، شبکه‌های Framc relay و یا شبکه‌های دیگری نظیر ATM استفاده می‌کند. در این لایه در صفحه کنترل از پروتکل کنترل مکالمه Q.931 استفاده می‌شود. از سوی ISDN برای لایه‌های بالاتر (لایه‌های ۴ الی ۷) در صفحه کاربر پروتکل خاصی تعریف نشده است، بلکه پروتکل‌ها براساس انتخاب کاربر تعیین می‌شود. همچنین در لایه‌های بالاتر در صفحه کنترل از پروتکل‌های سیگنالینگ انتها به انتها استفاده می‌گردد.

استاندارد فیزیکی ISDN توسط دو استاندارد ITU-T، I.430 و I.431 تعریف شده است. در این دو استاندارد، تمام جنبه های واسطه های BRI و PRI توصیف شده اند. مهمترین جنبه های توصیف شده در این استاندارد عبارتند از: مشخصات فیزیکی و الکتریکی واسطه های R، S، T و U، روش کد گذاری، نحوه تسهیم سازی کانال و منبع تغذیه.

واسطه R توسط ISDN تعریف نشده است و کاربر می تواند از همه استانداردهای EIA نظیر: EIA-232، EIA-499، EIA-530 و یا از استانداردهای سری X و یا V (نظیر X.21) سازمان ITU-T استفاده نماید. در نقطه مرجع S از سوی ITU-T استاندارد ISO8887 تعیین شده است. در این استاندارد از اتصال دهنده های ۴، ۶ و یا ۸ سیمه استفاده می شود. سیم های موجود در واسطه S مطابق با جدول (۶-۲) استفاده می گردند.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

کانال B	کانال D
لایه های ۶، ۵، ۴ و ۷ انتخاب کاربر	سیگنالینگ انتها به انتهای کاربر
لایه شبکه X.25 و ...	لایه شبکه کنترل مکالمه (Q.931)
لایه پیوند داده LAPB و ...	لایه پیوند داده LAPD
لایه فیزیکی PRI و BRI	لایه فیزیکی PRI و BRI

شکل (۶-۱۸): لایه های ISDN برای کانال های B و D

جدول (۶-۲): سیم های موجود در واسط S

نام	TE	NT
A	منبع تغذیه ۳	دریافت کننده تغذیه ۳
B	منبع تغذیه ۳	دریافت کننده تغذیه ۳
C	ارسال	دریافت
D	دریافت	ارسال
E	دریافت	ارسال
F	ارسال	دریافت
G	دریافت کننده تغذیه ۲	منبع تغذیه ۲
H	دریافت کننده تغذیه ۲	منبع تغذیه ۲

در ISDN از روش کدگذاری AMI استفاده می گردد. در واسط U و در هر جهت یک کابل زوج سیم به هم تابیده شده استفاده می شود. در این واسط مکانیسم 2B1Q که بر خلاف AMI به جای استفاده از دو سطح سیگنال، از ۴ سطح سیگنال استفاده می کند، تعیین شده است.

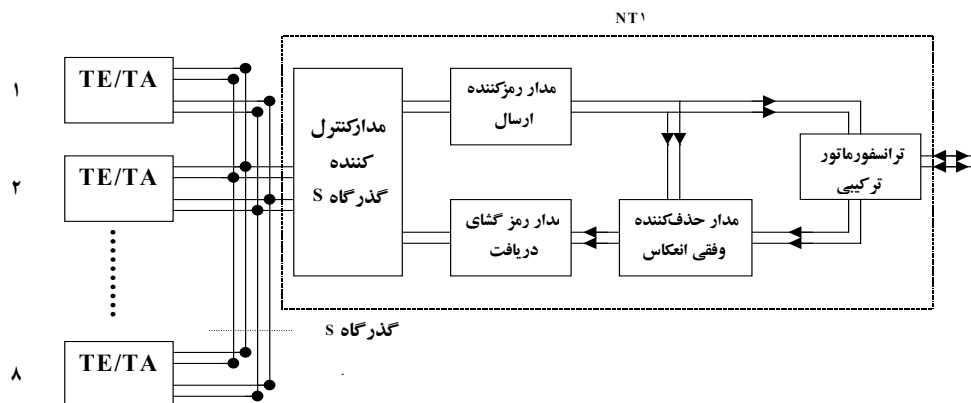
بر اساس فاصله بین وسیله ارسال داده تا NT1 از توپولوژی ستاره یا گذرگاه مشترک در BRI استفاده می شود. در اتصال های نقطه به نقطه تجهیزات کاربران می توانند تا فاصله هزار متری از NT1 قرار داشته باشند. در اتصال های چند نقطه حداکثر فاصله کانال می تواند ۲۰۰ متر باشد. چنانچه در کانال های چند نقطه، ایستگاه ها در انتهای کانال متمرکز گردند؛ در این حالت تاخیر انتشار برای همه آنها یکسان خواهد بود و می توان طول کانال را به ۵۰۰ متر افزایش داد. حداکثر امکان اتصال ۸ ایستگاه به NT1 وجود دارد. در هر لحظه فقط دو ایستگاه قادر به دسترسی به کانال B می باشند.

در شکل (۶-۱۹) ساختار واسط کاربر به شبکه در لایه فیزیکی ISDN نشان داده شده است. مطابق با این شکل بین تجهیزات کاربر و شبکه از یک زوج سیم به هم تابیده شده استفاده می گردد. با توجه به این که ارسال به صورت کاملاً دوطرفه

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۲

می باشد، بنابراین نیاز به یک ترانسفورماتور ترکیبی^۱ می باشد. توسط ترانسفورماتور ترکیبی، سیگنال دریافتی از خط از سیگنال ارسالی جدا شده و به مدار گیرنده تحویل داده می شود. از آن جا که عملیات جداسازی فوق به صورت ایده آل انجام نمی گردد، این احتمال وجود دارد که مقداری از سیگنال ارسالی به درون گیرنده فیدبک شود. برای حذف سیگنال فیدبکی فوق نیاز به مدار حذف کننده انعکاس^۲ می باشد. برای آن که مدار حذف کننده انعکاس فوق به صورت ایده آل عمل کند، نباید بین سیگنال ارسالی با سیگنال دریافتی هیچ گونه همبستگی^۳ موجود باشد. برای جلوگیری از ایجاد همبستگی در سیگنال ارسالی و دریافتی، از مدار رمز کننده^۴ در سمت ارسال و رمز گشا^۵ در سمت دریافت استفاده می شود. این مدار اقدام به درهم ریختن رشته بیت ارسالی می کند و بدین ترتیب رشته بیت ارسالی به صورت کاملاً تصادفی تبدیل می شود.

همان طور که در شکل (۶-۱۹) مشاهده می شود، تجهیزات TE و TA از طریق دو زوج سیم (یک زوج برای ارسال و یک زوج برای دریافت) به NT1 اتصال می یابند. در ISDN، این امکان وجود دارد که حداکثر ۸ تا تجهیزات TE/TA به یک NT1 اتصال یابند.



شکل (۶-۱۹): واسط کاربر به شبکه در ISDN

از روش CSMA برای دسترسی به کانال D استفاده می شود. هنگامی که ایستگاهی به کانال D دسترسی یافت، قادر به درخواست کانال B می باشد و چنانچه کانال B آزاد موجود باشد اتصال برقرار خواهد شد.

در واسط های PRI از ۲۳ کانال B و یک کانال D استفاده می شود. در این واسط ها نیز نقاط مرجع U, T, S, R تعریف می گردند. نقاط مرجع S, R در این حالت مشابه نقاط متناظر در واسط BRI می باشند. نقطه مرجع T مشابه نقطه مرجع S می باشد، که در آن از روش کدگذاری B8ZS استفاده می شود. واسط U نیز در PRI مشابه BRI می باشد، با این تفاوت که از نرخ ارسال ۱/۵۴۴ مگابیت بر ثانیه استفاده می گردد.

^۱ Hybrid transformer

^۲ Echo canceler

^۳ Correlation

^۴ Scrambler

^۵ Descrambler

۶-۶-۲-۲- لایه پیوند داده

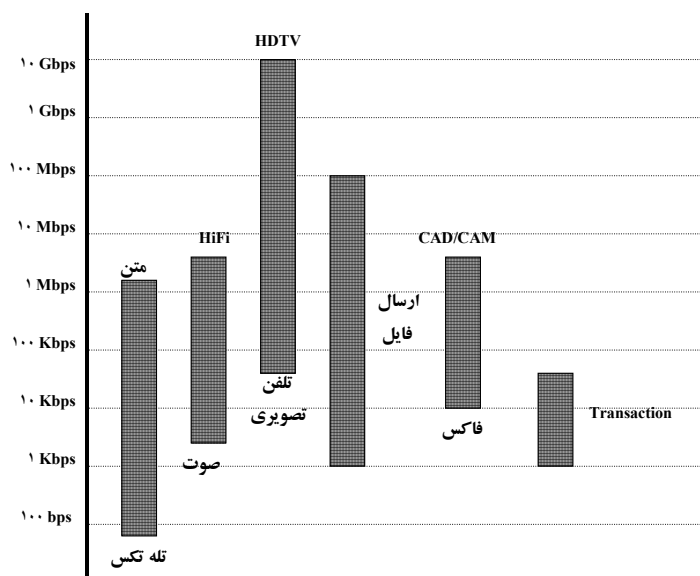
کانال های D_B (صفحه کاربر و صفحه کنترل) از پروتکل های پیوند داده متفاوتی استفاده می نمایند. همان طور که قبلاً گفته شد کانال B از پروتکل LAPB و کانال D از پروتکل LAPD استفاده می کند. LAPD مشابه پروتکل HDLC می باشد با این تفاوت که در آن تغییرات خاصی انجام گرفته است.

۶-۶-۲-۳- لایه شبکه

هنگامی که با استفاده از کانال D اتصال اولیه به وجود آمد، صفحه کاربر با استفاده از پروتکل هایی مانند سوئیچینگ مداری، X.25 و یا سایر پروتکل ها اقدام به ارسال اطلاعات بین کاربران می کند.

ISDN-۳-۶-۶ باند یهن (BISDN¹)

هنگامی که برای اولین بار ISDN مطرح شد، سرعت‌های ۶۴ کیلو بیت بر ثانیه تا ۱/۵۴۴ مگابیت بر ثانیه برای برآورد کردن نیازهای ارسال آن زمان کافی بود. با توسعه شبکه‌های کامپیوتری و ارائه سرویس جدیدتر، سرعت‌های فوق کافی نمی‌باشد. از این رو استاندارد ISDN باند پهن ارائه گردید. در این استاندارد، اتصال بین کاربر و شبکه تا سرعت ۶۰۰ مگا بیت بر ثانیه می‌تواند افزایش یابد. در شکل (۶-۲۰) نرخ ارسال بیت برای سرویس مختلف BISDN نشان داده شده است.



شکل (۶-۲۰): نرخ ارسال بیت برای سرویس مختلف BISDN

همان‌طور که اشاره شد، پیدایش ISDN تحول عظیمی در سیستم‌های آنالوگ تلفن ایجاد نمود. پیدایش B-ISDN در حقیقت انقلاب بزرگی در فن‌آوری مخابرات به حساب می‌آید. در B-ISDN به جای استفاده از کابل‌های فلزی، از محیط‌های ارسال جدیدی نظیر فیبر نوری استفاده می‌شود.

¹ Broadband ISDN

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۱

BISDN قادر به ارائه دونوع سرویس به کاربران خود می باشد که عبارتند از: سرویس تاثیر متقابل^۱ و سرویس توزیعی^۲.

در سرویس تاثیر متقابل یک یا دو مشتری با یک سرویس دهنده در ارتباط متقابل می باشند. این نوع سرویس خود به سه دسته زیر تقسیم می شوند:

- **سرویس محاوره ای^۳**: این نوع سرویس ، مبادله دوطرفه به صورت زمان حقیقی را پشتیبانی می کند. از این سرویس زمان حقیقی در تلفن، تلفن های تصویری، کنفرانس های ویدئویی، ارسال داده و نظیر اینها استفاده می شود.

- **سرویس پیامی^۴**: در این نوع سرویس اطلاعات به صورت ذخیره و هدایت به جلو مبادله می شوند. این نوع سرویس به صورت دوطرفه هستند، که در آن یک مشتری از مشتری مقابل درخواست اطلاعات می کند. ممکن است اطلاعات درخواستی در همان لحظه حاضر نباشد و درخواست کننده مدتی منتظر پاسخ بماند. پست صوتی^۵، پست داده^۶ و پست ویدئویی^۷ نمونه ای از این نوع سرویس می باشد.

- **سرویس بازیافتی^۸**: از این نوع سرویس برای بازیافت اطلاعات از یک منبع مرکزی به نام مرکز اطلاعات استفاده می شود. این سرویس مشابه کتابخانه ها باید اجازه دسترسی عمومی به کاربران را فراهم آورند. در این سرویس، اطلاعات توزیع نمی شوند مگر آن که درخواستی برای آن از جانب مشتریان دریافت شود.

سرویس توزیعی به صورت یک طرفه از طرف سرویس دهنده به سمت مشتریان می باشند و برخلاف سرویس تاثیر متقابل، مشتریان قادر به ارسال درخواست برای دستیابی به سرویس مورد نظر خود نمی باشند. این نوع سرویس به دو صورت : تحت کنترل کاربر، و بدون کنترل کاربر قابل پیاده سازی می باشند. در سرویس توزیعی بدون کنترل کاربر، بدون آن که کاربر درخواستی برای سرویس و زمان پخش آنها داشته باشد، سرویس از سوی سرویس دهنده بین کاربران توزیع می شود. برنامه های تلوزیونی، نمونه ای از این سرویس می باشند. سرویس توزیع تحت کنترل کاربر، به صورت چرخشی به کاربر ارسال می شود. این نوع سرویس به صورت متناوب تکرار می شوند تا این که کاربر قادر به دریافت آنها در زمانهای دلخواه خود باشد. پخش برنامه های آموزشی^۹ و تلوزیون پولی، نمونه ای از این نوع سرویس می باشد. به عنوان مثال در تلوزیون پولی، یک برنامه خاص در زمان های معینی پخش می شود، کاربر برای مشاهده این برنامه باید تلوزیون خود را در زمان های خاصی که این برنامه پخش می شود، روشن کند. برای پیاده سازی سرویس BISDN از فن آوری ATM که در بخش های بعدی توضیح داده می شود استفاده می گردد.

^۱ Interactive services

^۲ Distributive services

^۳ Conversational services

^۴ Messaging services

^۵ Voice mail

^۶ Data mail

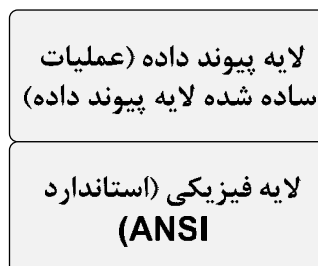
^۷ Video mail

^۸ Retrieval services

^۹ Educational broadcasting

۶-۷- شبکه Frame Relay

در شبکه های frame relay، جهت افزایش سرعت عملیات پردازش و هدایت قاب های لایه دوم، کلیه عملیات لایه شبکه و بخشی از عملیات لایه پیوند داده حذف شده است. بنابراین در مقایسه با شبکه های X.25 که دارای ۳ لایه می باشند، شبکه های frame relay تنها ۱/۵ لایه دارند که در شکل (۶-۲۱) نشان داده شده است.



شکل (۶-۲۱): لایه های frame relay

۶-۷-۱- ساختار قاب ها در frame relay

در شبکه های frame relay، در سطح لایه پیوند داده از نسخه ساده شده پروتکل HDLC استفاده می شود. جهت سادگی و افزایش سرعت، عملیات کنترل جریان و کنترل خطای پیشرفته که در HDLC استاندارد وجود دارد، در شبکه های frame relay استفاده نمی شود.

در شکل (۶-۲۲) ساختار قاب های لایه دوم در frame relay نشان داده شده است. همان طور که در این شکل نیز دیده می شود، ساختار این قاب ها مشابه ساختار قاب های HDLC می باشد. فیلدهای پرچم، FCS و اطلاعات در قاب های frame relay مشابه فیلدهای فوق در HDLC می باشند، اما فیلد های آدرس و کنترل در قاب های frame relay با یکدیگر ترکیب شده و فیلد آدرس را تشکیل می دهند. در فیلد آدرس زیر فیلدی به نام "مشخص کننده اتصال لایه پیوند داده" ($DLCI^1$) وجود دارد، که از آن برای هدایت قاب های frame relay استفاده می شود. با توجه به ساختار قاب های frame relay، در فیلد آدرس، زیر فیلدهای زیر موجود می باشد:

- **فیلد $DLCI$:** این فیلد که به دو تکه ۶ و ۴ بیتی تقسیم شده است (مجموعاً ۱۰ بیت)، برای مشخص کردن اتصال لایه پیوند استفاده می شود.
- **فیلد دستور/پاسخ (C/R^2):** از این فیلد برای تعیین این که قاب ارسالی از نوع دستور یا پاسخ است استفاده می شود.
- **فیلد آدرس توسعه یافته (EA^3):** این بیت مشخص می کند که بایت جاری آخرین بایت آدرس است یا خیر؟ اگر این بیت صفر باشد، نشان دهنده این است که یک بایت آدرس دیگر وجود دارد و چنانچه این بیت ۱ باشد، به معنی آن است که بایت آدرس دیگری وجود ندارد. چنانچه طول آدرس ۲ بایت باشد، اولین فیلد EA برابر صفر و فیلد دوم برابر با ۱ می باشد. چنانچه برنامه کاربردی به آدرس بیشتر از دو بایت نیاز داشته باشد، در این صورت هر دو فیلد EA برابر صفر می باشند و یک بایت سوم آدرس اضافه می شود که در آن ۷ بیت نشان دهنده آدرس و بیت هشتم که همان فیلد EA است، برابر با ۱ می باشد.

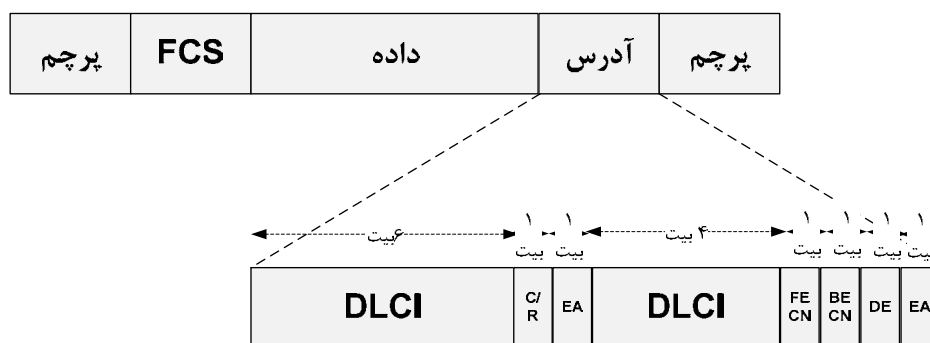
^۱ Data Link Connection Identifier

^۲ Command/Response

^۳ Extended Address

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۱

- **فیلد اعلام صریح ازدحام در مسیر پیشرو (FECN^۱):** چنانچه در نودهای میانی شبکه ازدحام رخ دهد، در این صورت این فیلد ۱ می شود، که نشان دهنده این است که در مسیر عبور قاب ها از مبدأ به مقصد ازدحام رخ داده است. گیرنده با مشاهده فعال بودن این بیت متوجه می شود که در داخل شبکه، ازدحام رخ داده است و متوجه می شود که این احتمال وجود دارد که به خاطر ازدحام قاب های بعدی با تأخیر دریافت شوند.
- **فیلد اعلام صریح ازدحام در مسیر پسرو (BECN^۲):** برای اعلام وقوع ازدحام در مسیر مخالف مسیری که قاب ها از آن عبور می کنند، این بیت فعال می شود. گیرنده با فعال کردن این فیلد به فرستنده در خصوص وقوع ازدحام هشدار می دهد.
- **فیلد شایستگی حذف (DE^۳):** از این بیت برای تعیین اولویت قاب استفاده می شود. در شرایط بحرانی که ازدحام در شبکه رخ داده است، با استفاده از این فیلد قاب های ارسالی اولویت بندی شده و آنهایی که اولویت کمتری دارند در معرض حذف قرار می گیرند. قاب هایی که فیلد DE آنها ۱ است اولویت بیشتری نسبت به قاب های با فیلد DE برابر با صفر دارند.



شکل (۶-۲۲): ساختار قاب های frame relay

۶-۸-۲- عملکرد frame relay

شبکه های Frame relay از اتصال های مدارمجازی دایمی (PVC^۴) استفاده می کنند. برای مشخص کردن مدارمجازی دایمی از فیلد DLCI استفاده می شود. با توجه به این که طول ناحیه DLCI برابر با ۱۰ بیت می باشد، حداکثر می توان ۱۰۲۴ مدارمجازی دایمی مختلف ایجاد نمود. چنانچه بایت سوم آدرس نیز در سرآیند قاب های frame relay قرار گیرد، در این صورت می توان حداکثر تعداد مدارهای مجازی دایمی شبکه را افزایش داد. در شکل (۶-۲۳) مثالی از کاربرد فیلد DLCI نشان داده شده است.

هریک از سوئیچ های شبکه های frame relay دو وظیفه عمده به عهده دارند که عبارتند از: کنترل خطا (با استفاده از فیلد FCS موجود در هرقاب) و سوئیچینگ و هدایت قاب ها با استفاده از فیلد DLCI موجود در سرآیند قاب ها. هریک از سوئیچ های میانی شبکه، برای هدایت قاب ها از مبدأ به مقصد، دارای یک جدول DLCI می باشند. با بررسی فیلد DLCI هر قاب و مراجعه به جدول فوق، شماره درگاه خروجی که قاب باید از طریق آن به سوئیچ بعدی ارسال شود، مشخص می گردد.

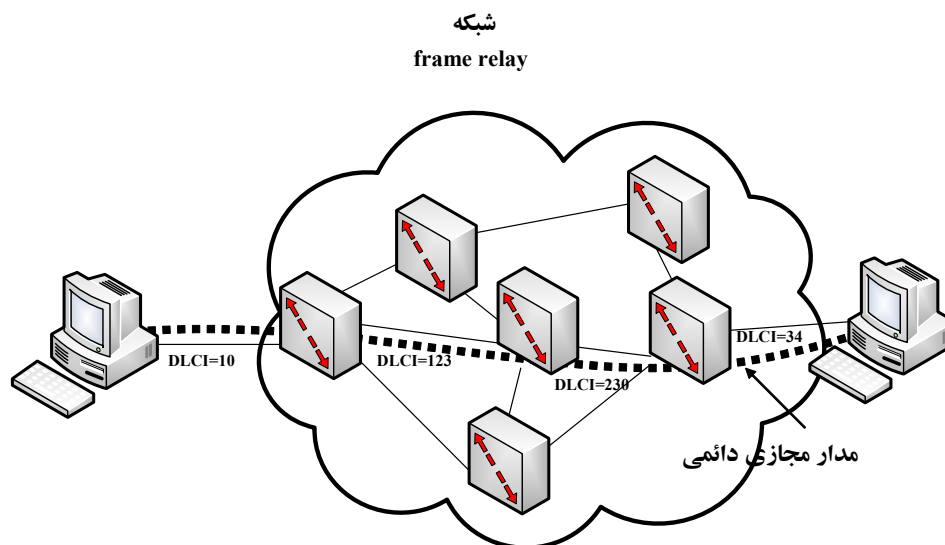
^۱ Forward Explicit Congestion Notification

^۲ Backward Explicit Congestion Notification

^۳ Discard Eligibility

^۴ Permanent Virtual Circuit

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۶-۲۳): مثالی از ایجاد مدارهای مجازی دائمی با استفاده از فیلد DLCI

یکی دیگر از عملیات هرسوئیچ در شبکه های frame relay، کنترل ازدحام می باشد. همان طور که قبلاً اشاره گردید، در سرآیند قاب های frame relay، دو بیت به نام های بیت FECN و بیت BECN وجود دارند، که از آنها برای کنترل ازدحام در شبکه استفاده می شود. هنگامی که یکی از سوئیچ های شبکه متوجه وقوع ازدحام در خود شود، با ۱ کردن بیت FECN به سوئیچ بعدی در مسیر پیشرو از وقوع ازدحام اطلاع می دهد. گیرنده نیز با دریافت قاب هایی که بیت FECN آنها ۱ است، قاب هایی با بیت BECN برابر با ۱ به فرستنده اولیه ارسال می دارد و به آن درمورد وقوع ازدحام در شبکه خبر می دهد.

۸-۶- شبکه ATM

فن آوری ATM، از سوی انجمن ATM به عنوان یک فن آوری جدید برای پیاده سازی سرویس BISDN ارائه گردید و توسط سازمان ITU_T مورد تصویب قرار گرفت. در فن آوری ATM اهداف زیر مورد توجه می باشد:

- استفاده از محیط های ارسال بسیار سریع به ویژه فیبر نوری
- ایجاد یک شبکه انعطاف پذیر که قادر به اتصال به سایر شبکه ها باشد
- استفاده از ATM به عنوان یک شبکه شالوده با قیمت ارزان برای اتصال شبکه های مختلف به یکدیگر
- توانایی برقراری ارتباط با سایر شبکه های موجود در دنیا
- پیاده سازی ATM به صورت اتصال گرا برای دستیابی به مزایای شبکه های اتصال گرا
- پیاده سازی قسمت های مختلف آن به صورت سخت افزاری و نرم افزاری برای افزایش سرعت

هرچند بسیاری از اهداف فوق هنوز به طور کامل به تحقق نرسیده است، ولی تلاش های زیادی در راستای رسیدن به اهداف فوق در دست انجام است. در شبکه های سوئیچینگ بسته ای، اطلاعات کاربران در قالب بسته هایی به طول متغیر

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد^۱)

ارسال می شود، درحالی که در شبکه های ATM، اطلاعات ارسالی کاربران در قالب بسته هایی به طول ثابت ۵۳ بایت ارسال می گردد. به علت کوچک بودن بسته های ارسال در ATM، به آنها سلول^۱ گفته می شود.

در ATM با توجه به طول کم هر سلول، پردازش هر سلول در نودهای میانی در زمان بسیار کمی صورت می گیرد و همچنین تأخیر ارسال در شبکه های ATM، بسیار ناچیز است.

ATM یک نوع شبکه اتصال گرا است که در آن قبل از ارسال داده ها، یک مدار مجازی بین مبدأ و مقصد به وجود می آید و سپس سلول های متعلق به هر پیام، به طور کامل از طریق یک مدار مجازی به مقصد ارسال می شود و در گیرنده نیز به ترتیب دریافت می شود. در شبکه های ATM، از سوئیچینگ لایه دوم برای هدایت و مسیریابی سلول ها استفاده می شود. در ATM ارسال اطلاعات کاربران به صورت غیرهمزمان انجام می شود. مفهوم غیرهمزمان بودن ATM آن است که داده های تولیدی کاربران به طور مستقل تولید می شوند و لزومی در رعایت یک زمان بندی خاص نمی باشد. با توجه به این که در ATM از کانال های سریع و مطمئن استفاده می شود، احتمال خرابی سلول ها بسیار کم می باشد. در ATM، توانایی تصحیح یک بیت خطا در سلول های ارسالی وجود دارد و نیازی به ارسال دوباره سلول نمی باشد. همچنین از روال های پیچیده کنترل ازدحام و کنترل جریان استفاده نمی شود. شکل (۶-۲۴) نشان دهنده مدل لایه ای ATM است.

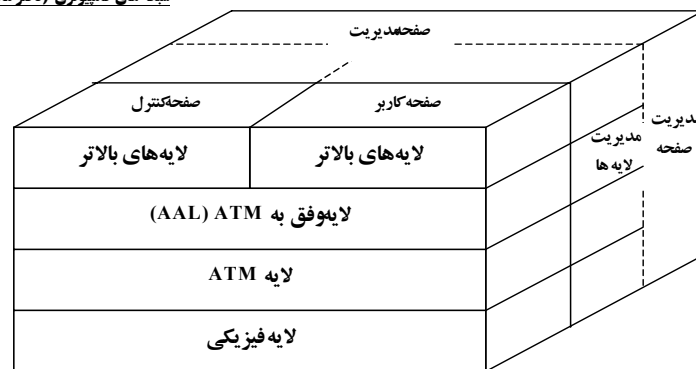
فن آوری ATM دارای ویژگیهای زیر می باشد:

- **عدم نیاز به کنترل خطا و کنترل جریان به صورت لینک به لینک:** در شبکه ATM چنانچه در کانال ارتباطی خطایی به وجود آید، عملیات کنترل خطا به صورت لینک به لینک انجام نمی شود. با توجه به این که معمولاً از کانال های فیبر نوری که از کیفیت بالایی برخوردار هستند در شبکه ATM استفاده می شود، احتمال خرابی کانال در ATM بسیار کم است. بنابراین کنترل خطا در ATM بصورت انتها به انتها انجام می گردد.
- **فن آوری ATM اتصال گرا است:** در این شبکه ابتدا بین فرستنده و گیرنده یک مدار مجازی به وجود می آید، سپس داده های ارسالی به طور کامل از این مدار عبور می کند و بعد از اتمام داده ها مدار مجازی از بین می رود.
- **کاهش سرآیند:** در ATM عملیات پردازش بر روی سرآیند کاهش یافته است، بنابراین سرعت پردازش سرآیندهای ATM بسیار زیاد است.
- **طول کم:** طول بسته های ATM بسیار کوچک است (۵۳ بایت) بنابراین بافرهای میانی شبکه ATM کاهش می یابد و تأخیر صف در شبکه کم می گردد.
- **حمایت از انواع ترافیک ها:** شبکه ATM قادر به ارائه انواع سرویس صوت، ویدئو و داده می باشد.

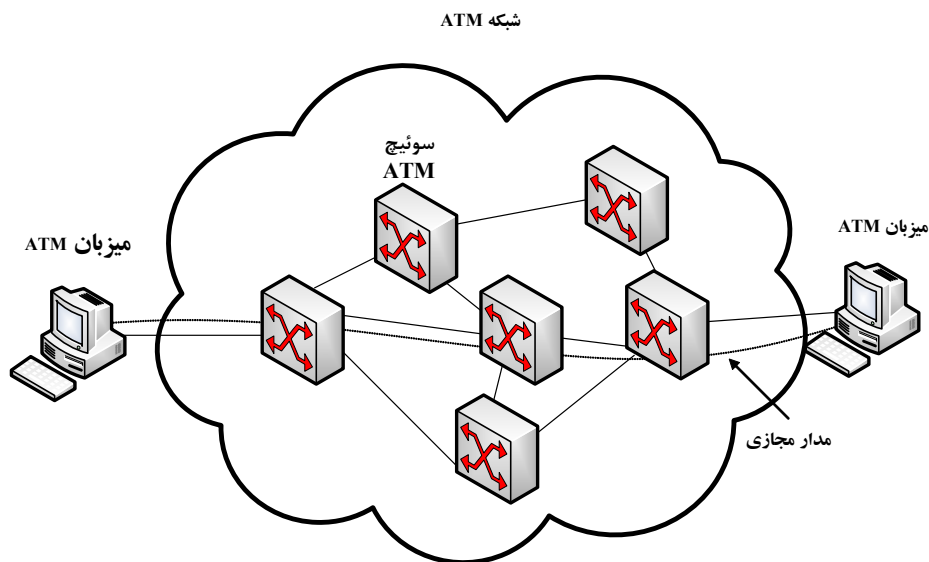
همان طور که در شکل (۶-۲۵) دیده می شود، در شبکه های ATM برای هر کاربر انتها به انتها یک مسیر مجازی به وجود می آید و با کمک تسهیم سازهای ATM ترافیک ارسالی کاربران با یکدیگر ترکیب می شوند و وارد شبکه ATM می شوند. هر شبکه ATM از دو جزء اصلی تشکیل شده است که عبارتند از: کامپیوترهای میزبان و سوئیچ های شبکه. کامپیوترهای میزبان به وسیله آداپتورهای ATM و با کمک کانال فیزیکی که ارتباط آن را به سوئیچ های شبکه برقرار می سازد، به شبکه ATM متصل می باشند. در شبکه های ATM برای برقراری ارتباط بین دو کامپیوتر میزبان از اتصال های مجازی استفاده می شود. نقطه انتهایی اتصال های مجازی فوق کامپیوترهای میزبان ATM می باشند.

^۱ Cell

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد) ۲۴



شکل (۶-۲۴): مدل لایه های ATM



شکل (۶-۲۵): یک اتصال انتها به انتها در ATM

سوئیچ ATM که در داخل شبکه نصب می شود، دارای چندین درگاه ورودی و خروجی می باشد، که ارتباط آن را به کامپیوترهای میزبان ATM و سایر سوئیچ های ATM برقرار می سازد. سلول های ورودی به سوئیچ های ATM بر اساس فیلد مشخص کننده اتصال، که در سرآیندهای سلول های ATM قرار دارند به درگاه خروجی مناسب ارسال می شوند. در ATM دو نوع اتصال وجود دارد که عبارتند از: اتصالات دایمی (PVC) و اتصالات سوئیچینگ (SVC). در اتصالات PVC یک مدار مجازی دایمی بین فرستنده و گیرنده موجود است. برای برقراری این نوع اتصالات نیاز به روال های سیگنالینگ نمی باشد. این نوع اتصالات مشابه خطوط استیجاری در شبکه تلفن هستند. در اتصالات SVC برای ایجاد مدار مجازی بین مبدأ و مقصد از روال های سیگنالینگ استفاده می شود. در ATM چهار نوع پیام سیگنالینگ وجود دارد که عبارتند از:

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)^۲

برقراری ارتباط: از این پیام ها برای پایه گذاری و برقراری ارتباط مدارهای مجازی SVC بین فرستنده و گیرنده استفاده می شود. در ATM پنج پیام اصلی برای برقراری ارتباط وجود دارد که عبارتند از: برقراری ارتباط، پیشرفت ارتباط^۱، اتصال، گوش به زنگ^۲ و گواهی اتصال^۳. در شکل (۶-۲۶) مثالی از مراحل برقراری ارتباط در ATM با استفاده از پیام های فوق آورده شده است.

بررسی وضعیت ارتباط: در شبکه های ATM برای بررسی وضعیت ارتباط های موجود از پیام های: اعلام وضعیت^۴، بررسی وضعیت^۵ و آگاهی دادن^۶ استفاده می شود. توسط کاربر یا شبکه برای دریافت وضعیت ارتباط های موجود از پیام بررسی وضعیت استفاده می گردد. در پاسخ به پیام فوق، پیام اعلام وضعیت ارسال می شود. برای نمایش اطلاعات وضعیت ارتباط از پیام آگاهی دادن استفاده می گردد.

قطع ارتباط: در شبکه های ATM بعد از برقراری ارتباط و ارسال اطلاعات، مدار مجازی به وجود آمده باید قطع گردد. بدین منظور از پیام های زیر استفاده می شود:

پیام رها سازی: این پیام توسط کاربر برای درخواست قطع ارتباط و یا توسط شبکه برای اعلام قطع مدار مجازی ارسال می گردد.

پیام تکمیل رهاسازی: در پاسخ به درخواست قطع ارتباط، کاربر یا شبکه پیام فوق را ارسال می کند و به دنبال آن مدار مجازی قطع می شود و مرجع ارتباط آزاد می شود.

پیام آغاز دوباره: این پیام توسط کاربر یا شبکه ارسال می شود و نشان دهنده درخواست آغاز دوباره یک VCC مشخص و یا تمامی VCC های موجود می باشد.

پیام های مربوط به ارتباط های نقطه به چند نقطه^۷: به طور کلی در شبکه های ATM دو نوع اتصال وجود دارد که عبارتند از: اتصال های نقطه به نقطه و اتصال های نقطه به چند نقطه. در اتصال های نقطه به چند نقطه مطابق با شکل (۶-۲۷) یک کاربر به نام کاربر ریشه، با چندین کاربر دیگر به نام کاربران برگ در ارتباط می باشد. کاربر ریشه با کمک روال های استاندارد سیگنالینگ با اولین کاربر برگ ارتباط برقرار می سازد. بعد از برقراری ارتباط کاربر ریشه با اولین کاربر برگ، از پیام های زیر برای برقراری ارتباط با سایر کاربران برگ استفاده می شود:

پیام افزودن کاربر جدید^۸: از این پیام برای اضافه کردن یک کاربر جدید به اتصال موجود استفاده می شود.

پیام گواهی افزودن کاربر جدید^۹: در پاسخ به پیام افزودن کاربر جدید، این پیام که نشان دهنده پاسخ مثبت به عملیات افزودن کاربر جدید به اتصال موجود است، ارسال می گردد.

پیام رد افزودن کاربر جدید^{۱۰}: در پاسخ به پیام افزودن کاربر جدید، این پیام که نشاندهنده پاسخ منفی به عملیات افزودن کاربر جدید به اتصال موجود است، ارسال می گردد.

^۱ Call proceeding

^۲ Alerting

^۳ Connect acknowledge

^۴ Status

^۵ Status enquiry

^۶ Notify

^۷ Point to multi-point

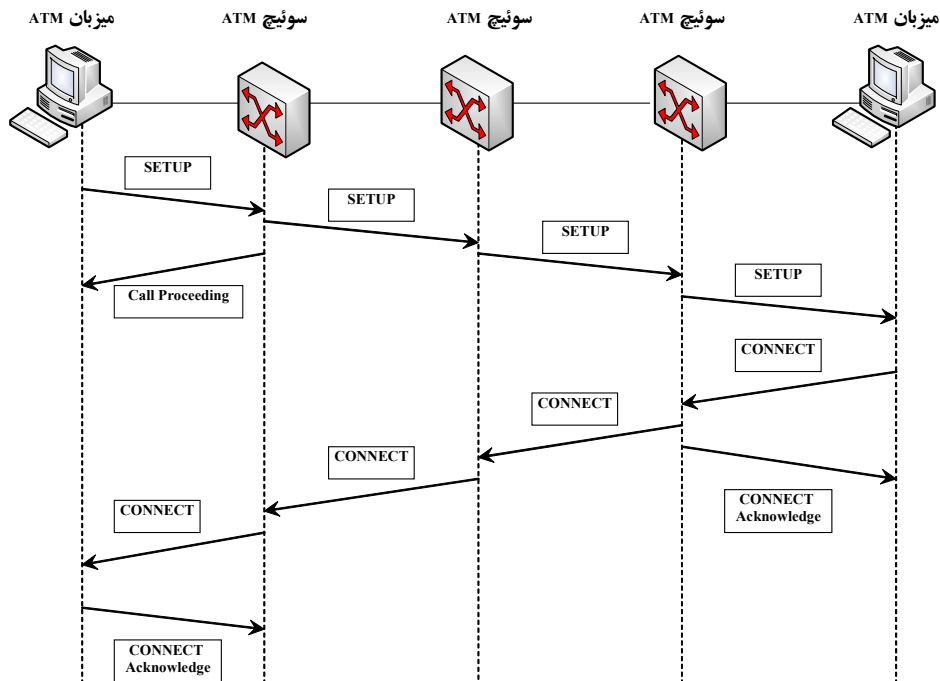
^۸ Add party

^۹ Add party acknowledge

^{۱۰} Add party reject

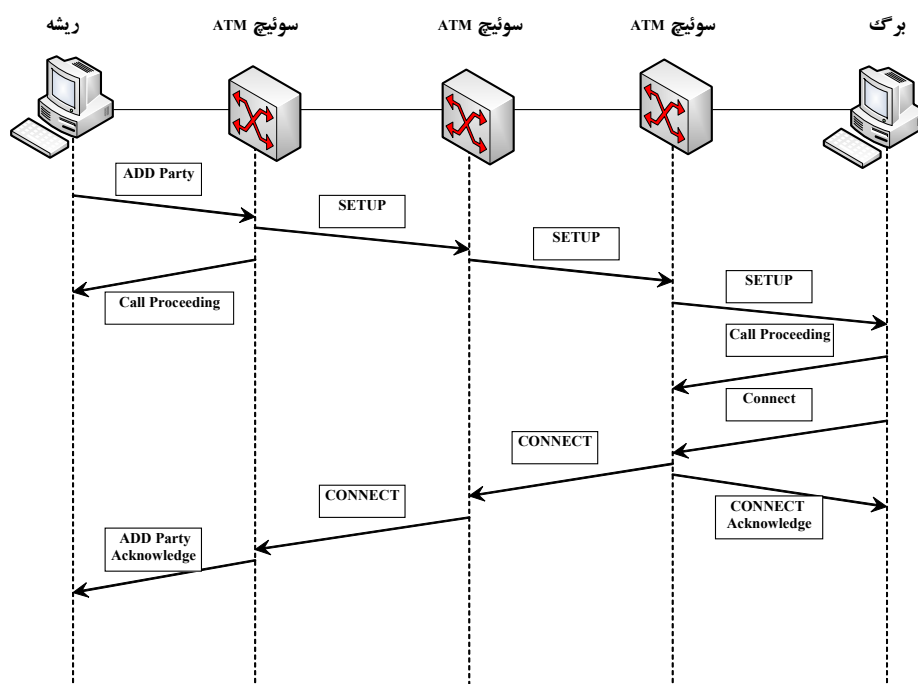
شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۱

- **پیام حذف کاربر^۱:** جهت حذف یک کاربر در اتصال موجود از این پیام استفاده می شود.
- **پیام گواهی حذف کاربر^۲:** در پاسخ به پیام حذف کاربر، این پیام ارسال می گردد که نشان دهنده عملیات موفق حذف یک کاربر از اتصال موجود است.



شکل (۶-۲۶): مثالی از برقراری ارتباط در ATM

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۶-۲۷): برقراری اتصال های نقطه به چند نقطه در ATM

۶-۹-۱- لایه فیزیکی در ATM

مطابق با استاندارد ITU-T I.321، لایه فیزیکی در ATM شامل دو زیر لایه می باشد که عبارتند از: زیر لایه همگرایی ارسال (TC^1) و زیر لایه وابسته به محیط فیزیکی. در توصیه نامه های G.703 و G.957 سازمان ITU-T این زیر لایه ها توصیف شده است. زیر لایه TC در ATM موظف به عملیاتی نظیر تنظیم نرخ ارسال سلول و تولید و اطمینان از سالم بودن فیلد HEC در سرآیند سلول های ATM می باشد. علاوه بر عملیات فوق این زیر لایه وظیفه تبادل سلول های مدیریتی (OAM^2) با لایه مدیریت را بر عهده دارد.

در لایه فیزیکی ATM، محیط ارسال و نحوه کدگذاری بیت های ارسالی مشخص می شود. استانداردهای SONET و SDH از مهمترین استانداردهای لایه فیزیکی در ATM می باشند. در ATM از کانال های فیزیکی مطمئن و سریع استفاده می شود که برخی از مهمترین این کانال ها عبارتند از:

- کانال DS-1 (با سرعت 1.544 Mb/s)
- کانال DS-3 (با سرعت 44.736 Mb/s)
- کانال J2 (با سرعت 6.312 Mb/s)
- کانال E1 (با سرعت 2.048 Mb/s)
- کانال E3 (با سرعت 34.368 Mb/s)
- کانال E4 (با سرعت 139.264 Mb/s)

^۱ Transmission Convergence

^۲ Operation And Maintenance

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

- کانال SONET OC-3 (با سرعت 155.52Mb/s)
- کانال STS-3c/STM-1 (با سرعت 622.08 Mb/s)
- کانال SONET OC-12 (با سرعت 2488.32 Mb/s)

در جدول (۳-۶) برخی از استانداردهای واسط های الکتریکی و نوری مورد استفاده در شبکه های ATM آورده شده است.

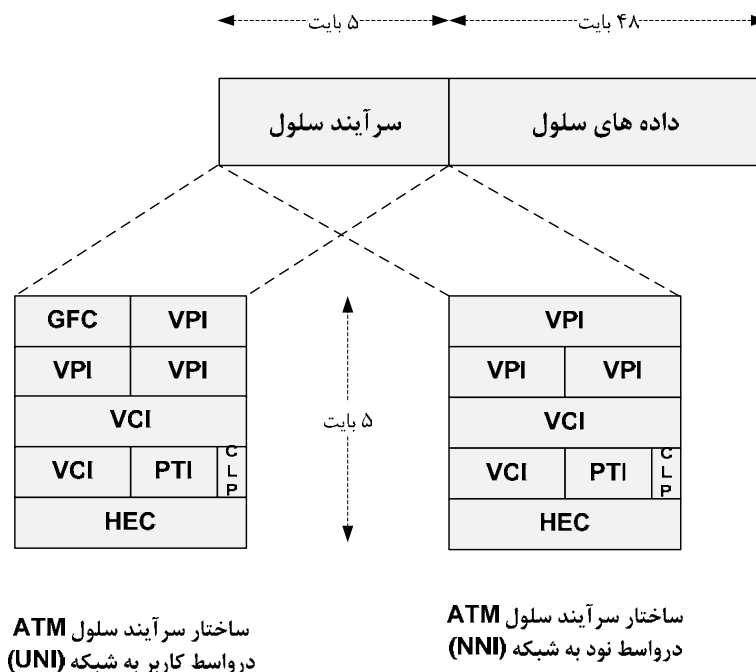
جدول (۳-۶): استانداردهای واسط های الکتریکی و نوری مورد استفاده در ATM

واسط های الکتریکی	واسط نوری	سرعت ارسال (بر حسب مگابیت بر ثانیه)
STS-1	OC-1	51.840
STS-2	OC-2	103.680
STS-3	OC-3	155.520
...	...	...
STS-6	OC-6	311.040
...	...	...
STS- <i>n</i>	OC- <i>n</i>	<i>n</i> *51.840
...	...	...
STS-256	OC-256	13271.040

۶-۹-۲- لایه ATM

در شبکه های ATM، لایه ATM که دومین لایه می باشد، عهده دار وظایفی نظیر مسیریابی و سوئیچینگ ، مدیریت ترافیک و تسهیم سازی کانال می باشد. لایه ATM، بسته های به طول ۴۸ بایت را از لایه بالاتر خود دریافت می کند و با اضافه کردن ۵ بایت سرآیند، سلول هایی به طول ۵۳ بایت تولید می کند و آنها را ارسال می کند. در شکل (۶-۲۸) ساختار سلول های ATM و فیلدهای موجود در آن نشان داده شده است.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد^۲)



شکل (۶-۲۸): ساختار سلول های ATM

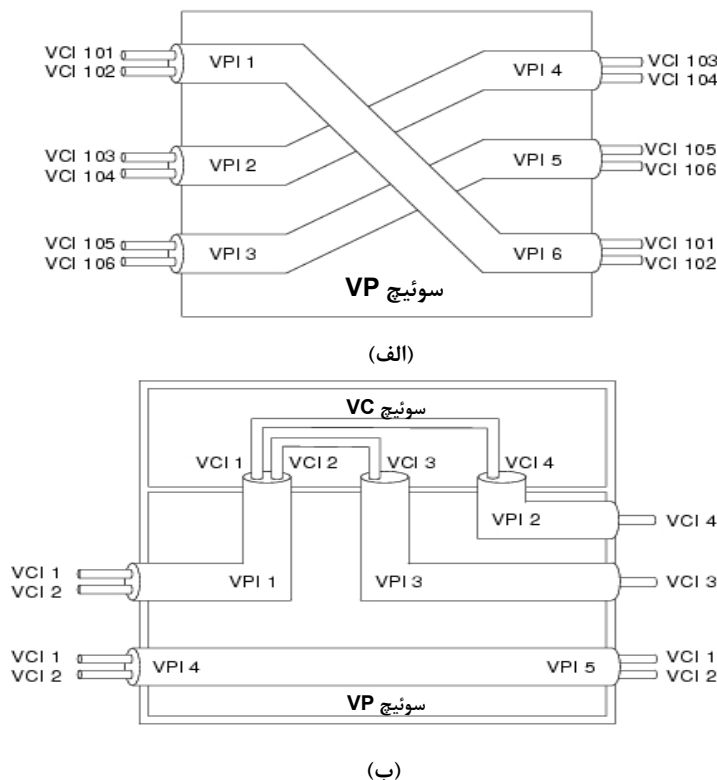
در سرآیند سلول های ATM فیلدهای زیر موجود است:

- **فیلد^۱ GFC**: از این فیلد برای کنترل جریان در واسط کاربر به شبکه (UNI^۲) استفاده می شود.
- **فیلد VPI و VCI**: از این فیلدها برای مشخص نمودن مدار مجازی استفاده می شود. در شکل (۶-۲۹) نمونه ای از کاربرد فیلدهای فوق نشان داده شده است. ارزش مقادیر موجود در این فیلدها محلی بوده و از هر سوئیچ به سوئیچ دیگر تغییر می کند. سوئیچ های ATM براساس نوع برخورد آنها با فیلد VPI/VCI به دودسته سوئیچ های VP و سوئیچ های VP/VC تقسیم بندی می شوند. سوئیچ های VP فقط مقدار فیلد VPI سلول های ATM را تغییر داده و مقدار VCI آنها را تغییر نمی دهند در حالیکه سوئیچ های VP/VC هر دو فیلد VPI/VCI را تغییر می دهند. در شکل (۶-۲۹) نمونه ای از این دونوع سوئیچ نشان داده شده است.

^۱ Generic Flow Control

^۲ User Network Interface

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۲



شکل (۶-۲۹): نمونه ای از سوئیچ های ATM (الف) سوئیچ VP (ب) سوئیچ V/VC

- **فیلد PT**: توسط این فیلد سه بیتی نوع داده های موجود در سلول های ATM مشخص می شود. سلول های ATM می توانند از نوع داده های کاربر، مدیریتی و یا کنترل شبکه باشند.
- **فیلد CLP^۱**: از این بیت برای کنترل ازدحام در ATM و تعیین نوع اولویت بسته ها استفاده می شود. بسته های با اولویت بالا دارای CLP=0 و بسته های کم اهمیت دارای CLP=1 می باشند. هنگامی که در سوئیچ های میانی شبکه، ازدحامی رخ دهد و بافرهای سوئیچ ها در آستانه پر شدن قرار گیرند، بسته های کم اولویت (CLP=1) از بین می روند و بسته های مهم (CLP=0) قبول می شوند.
- **فیلد HEC^۲**: از این فیلد برای تشخیص و تصحیح تک بیت خطا که ممکن است در سرآیند سلول های ATM رخ دهد استفاده می شود.

پس از برقراری اتصال و ایجاد مدارمجازی، انتقال اطلاعات صورت می گیرد. فرستنده مقدار VPI/VCI تخصیص یافته خود را در داخل فیلد مربوطه موجود در سرآیند سلول های ATM قرار داده و به سمت سوئیچ شبکه ارسال می دارد. سوئیچ شبکه با استفاده از جدول اتصال که در فاز برقراری اتصال ایجاد شده است، اقدام به مسیریابی سلول ها و ارسال آنها به سمت مقصد می نماید. هریک از اتصال های شبکه دارای مقدار خاصی از VPI/VCI می باشد و بدینوسیله از تداخل و اشتباه در مسیریابی سلول ها جلوگیری می شود. به عنوان مثال عملکرد سوئیچ ATM نشان داده شده در شکل (۶-۳۰) را در نظر بگیرید. در این شکل ترافیک های ویدئو در درگاه شماره ۱ دارای مقدار VPI/VCI برابر با 0/37 می باشند و طبق جدول

^۱ Cell Loss Priority

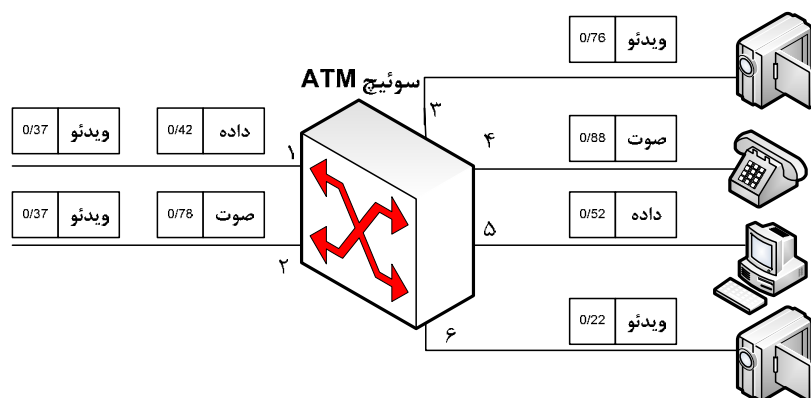
^۲ Header Error Correction

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

اتصال این سلول ها با مقدار جدید VPI/VCI مساوی با 0/76 به درگاه شماره ۳ ارسال می شوند. همچنین سلول های صوتی ارسالی به درگاه شماره ۲ با مقدار VPI/VCI برابر با 0/78 به درگاه شماره ۴ ارسال شده و مقدار VPI/VCI آنها برابر با 0/88 می شود. جدول اتصال این سوئیچ به صورت نشان داده شده در جدول (۴-۶) می باشد.

جدول (۴-۶): جدول اتصال سوئیچ ATM نشان داده شده در شکل (۶-۳)

شماره درگاه ورودی	مقدار VPI/VCI	شماره درگاه خروجی	مقدار VPI/VCI
ورودی	خروجی		
۱	0/37	۳	0/76
۱	0/72	۵	0/52
۲	0/37	۶	0/22
۳	0/78	۴	0/88



شکل (۶-۳): مثالی از عملکرد یک سوئیچ ATM

۶-۹-۳- لایه AAL^۱

لایه AAL در ATM به دو زیر لایه SAR^۲ و CPCS^۳ تجزیه می شود. در زیر لایه SAR بسته های دریافتی از لایه بالاتر به پیام های ۴۸ بیتی تجزیه می گردند. زیر لایه CPCS که به لایه بالاتر از AAL بستگی دارد، عملیات اضافه نمودن سرآیند را انجام می دهد. لایه AAL فقط در سمت کاربر انتهایی قرار دارد و سوئیچ های شبکه فاقد لایه فوق می باشند. شبکه ATM، ۴ کلاس مختلف سرویس را پشتیبانی می کند که این سرویس توسط مشخصه های اصلی زیر مشخص می گردند:

(۱) **ارتباط زمانی**^۱: برخی از سرویس شبکه ATM از نوع زمان حقیقی می باشند و نیاز به حفظ ارتباط زمانی بین مبدأ و مقصد دارند. به عنوان مثال سرویس صوت ۶۴ کیلوبیت بر ثانیه PCM از این نوع می باشند. در مقابل برخی از سرویس شبکه نظیر انتقال فایل بین کامپیوترها نیازی به حفظ ارتباط زمانی ندارند.

^۱ ATM Adaptation Layer

^۲ Segmentation AND Reassembly

^۳ Common Part Convergence Sublayer

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۱

۲) **نرخ ارسال:** برخی از سرویس شبکه دارای نرخ ارسال ثابت می باشند و برخی از سرویس دیگر دارای نرخ ارسال متغیر هستند.

۳) **نحوه اتصال:** سرویس شبکه های ATM به دو دسته اتصال گرا و بدون اتصال تقسیم بندی می شوند. در جدول (۴-۶) انواع کلاس های AAL و وابستگی آنها به مشخصه های فوق نشان داده شده است.

جدول (۴-۶) : انواع کلاسهای AAL در شبکه های ATM

نوع کلاس AAL	ارتباط زمانی	نرخ ارسال	نحوه اتصال	مثال
AAL1	نیاز دارد	ثابت	اتصال گرا	ویدئو غیر فشرده شده
AAL2	نیاز دارد	متغیر	اتصال گرا	تصاویر ویدیویی
AAL3/4	نیاز ندارد	متغیر	اتصال گرا	کاربردهای SMDS
AAL5	نیاز ندارد	متغیر	بدون اتصال	سرویس های با نرخ ارسال متغیر

۶-۹-۳-۱- انواع لایه های AAL

لایه AAL در ATM به ۴ نوع تقسیم بندی می شوند که عبارتند از: AAL1، AAL2، AAL3/4 و AAL5. AAL1 مخصوص ارسال اطلاعات با نرخ ثابت می باشد. در AAL1 ارتباط زمانی بین مبدأ و مقصد حفظ می شود و از آن برای کاربردهایی که به تأخیر حساس هستند، نظیر ارسال صوت و ویدئو استفاده می شود. در AAL1 عملیات خطایابی در مقصد انجام می گردد. AAL2 کلاسهای B ترافیک های ATM را پشتیبانی می کند. به خاطر سادگی و بالاسری کم AAL5 و همچنین عدم شناخت کامل رفتار ترافیک های متغیر با زمان هنوز به طور کامل استاندارد نشده است. AAL3/4 برای ترافیک های کلاس های C و D مناسب می باشد. در AAL3/4 سرعت ارسال اطلاعات متغیر است و اطلاعات زمانی بین مبدأ و مقصد ارسال نمی گردند. دو نوع مد کاری برای AAL3/4 وجود دارد که عبارتند از: مد مطمئن و مد نامطمئن. در حالت کاری مطمئن، کنترل خطا و کنترل جریان بین مبدأ و مقصد انجام می شود و بنابراین بسته ها به طور سالم به مقصد تحویل داده می شوند. در حالت کاری نامطمئن امکان معیوب رسیدن بسته ها به مقصد وجود دارد. AAL5 مشابه با AAL3/4 می باشد و مشابه با آن دارای دو مد مطمئن و نامطمئن است. در AAL5 هیچ گونه سرآیندی توسط زیرلایه SAR به بسته اضافه نمی شود، بنابراین زمان پردازش سرآیند کم شده است. AAL5 توسط انجمن ATM استاندارد گردیده است. به غیر از انواع AAL که در بالا به آن اشاره گردید، یک نوع لایه AAL دیگر به نام SAAL² نیز وجود دارد که از آن برای ایجاد یک محیط مطمئن جهت تبادل اطلاعات سیگنالینگ بین کاربران استفاده می شود.

۶-۱۰- شبکه های خصوصی مجازی (VPN³)

در چند ساله اخیر، شرکت های چندملیتی به مزایای استفاده اشتراکی از داده ها از طریق شبکه های کامپیوتری گسترده پی برده اند. امروزه با استفاده از فن آوری VPN ها امکان استفاده از مزایای استفاده اشتراکی داده ها برای کلیه

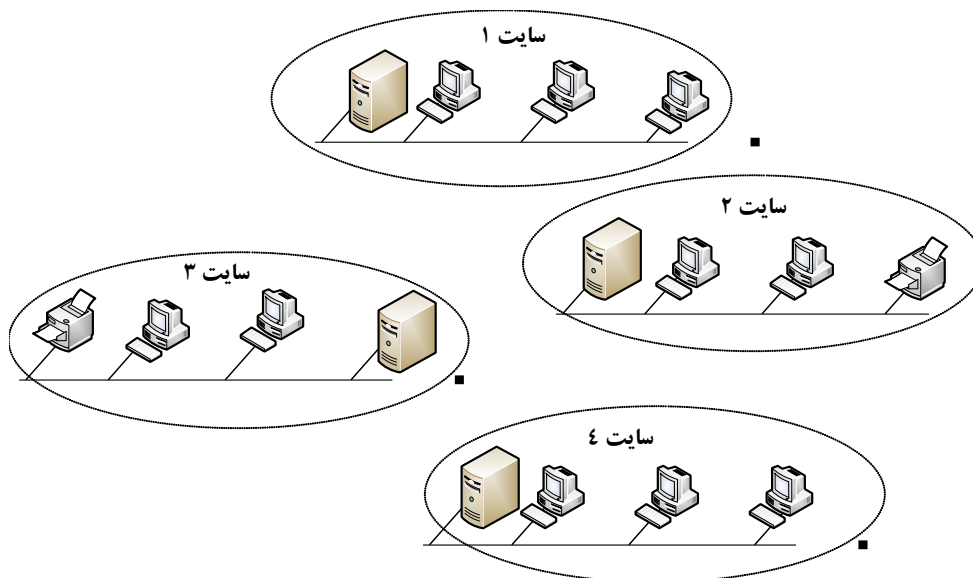
^۱ Time relation

^۲ Signaling AAL

^۳ Virtual Private Network

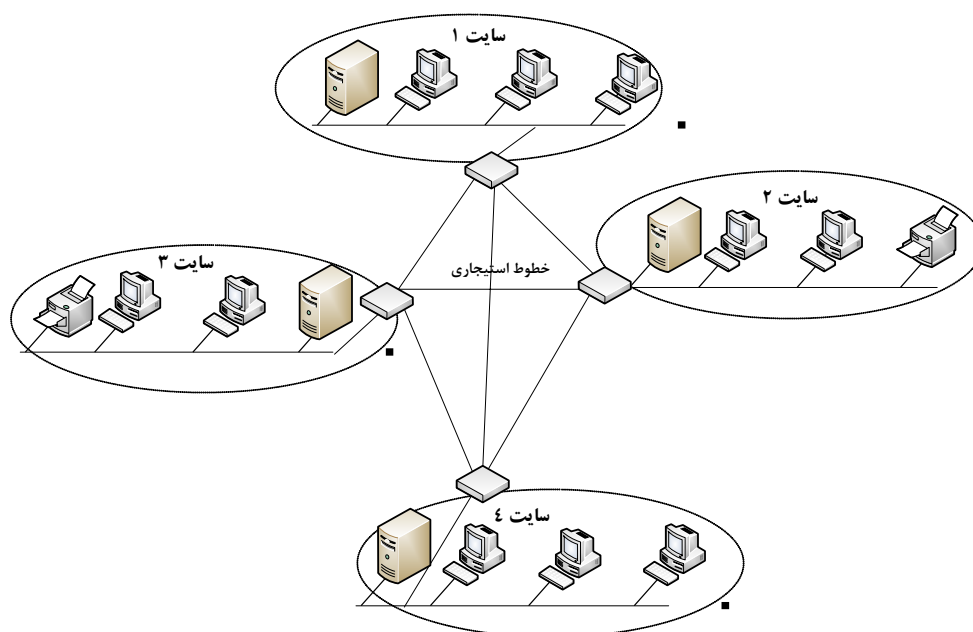
شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

شرکت ها، حتی شرکت های کوچک فراهم شده است. در حالت عادی، چنانچه شرکتی دارای سایت های کامپیوتری متعدد در نقاط مختلفی از دنیا باشد، امکان استفاده اشتراکی از داده ها بین شعبات مختلف شرکت وجود ندارد. به عنوان مثال در شکل (۳۱-۶) چهار سایت کامپیوتری مختلف یک شرکت که در نقاط گوناگون قرار دارند، نشان داده شده است.



شکل (۳۱-۶): سایت های کامپیوتری مجزا از یکدیگر

به خاطر عدم وجود اتصال های لازم بین سایت های کامپیوتری فوق، امکان استفاده اشتراکی از داده ها برای سایت های کامپیوتری وجود ندارد. با استفاده از خطوط استیجاری، مبادله مستقیم داده ها بین کامپیوترهای مختلف سایت های کامپیوتری فراهم می آید. این مسئله در شکل (۳۲-۶) نشان داده شده است.



شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

شکل (۶-۳۲): اتصال سایت های کامپیوتری مجزا از یکدیگر به وسیله خطوط استیجاری

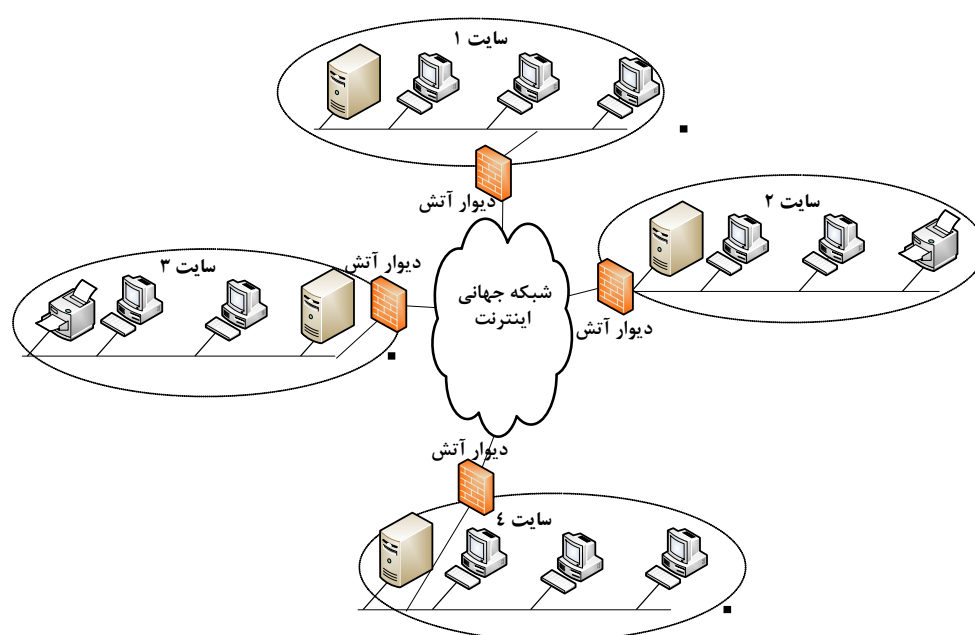
حتی بعد از گسترش اینترنت و امکان استفاده از آن به خاطر قیمت پایین تر نسبت به خطوط استیجاری، به خاطر مشکلات امنیتی موجود در اتصال های اینترنتی، شرکت ها همچنان مایل به استفاده از خطوط گران قیمت استیجاری برای مبادلات داده های خود بودند. اخیراً با استفاده از فن آوری VPN، امکان مبادلات تجاری امن بین کامپیوترهای شبکه با استفاده از بستر اینترنت فراهم شده است.

VPN ها قادر به برقراری اتصالات خصوصی تونل بین سایت های کامپیوتری مختلف شرکت ها در بستر اینترنت می باشند. تونل های فوق درست مشابه خطوط استیجاری می باشند با این تفاوت که هزینه تونل های خصوصی VPN به مراتب کمتر از خطوط استیجاری است. طبق آمار موجود VPN ها باعث صرفه جویی ۳۰ تا ۷۰ درصدی هزینه نسبت به خطوط استیجاری می شوند.

برخلاف خطوط استیجاری گران قیمت، با استفاده از رمزنگاری های قوی داده های کامپیوترها به طور امن از طریق VPN ها مبادله می شود، طوری که نه تنها نفوذگران اینترنت بلکه خود ISP ها نیز قادر به استراق سمع داده ها نخواهند بود.

امروزه سازمان های مختلف با استفاده از دیواره های آتشین از دسترسی غیرمجاز افراد خارج از شبکه به منابع کامپیوتری سازمان خود جلوگیری می کنند. البته دیواره های آتشین قادر به تشخیص و جدا سازی افراد خارجی مجاز و همچنین کارمندان و همکاران تجاری شرکت ها از افراد خارجی غیرمجاز نمی باشند.

مطابق با شکل (۶-۳۳) دیواره های آتشین مدرن، بدون آن که امنیت داده های سایت های کامپیوتری به خطر بیافتد قادر به برقراری ارتباط های VPN بین سایت های مختلف می باشند. فن آوری های مدرن VPN با استفاده از روش های رمزنگاری جدید قادر به اتصال سایت های کوچک و بزرگ به یکدیگر از طریق اینترنت می باشد طوری که کاربران راه دور به همان کیفیت کاربران محلی قادر به استفاده از منابع شبکه می باشند. به عنوان مثال کاربران راه دور مشابه کاربران محلی قادر به استفاده از داده های موجود در سرویس دهنده های وب هستند.



شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۱

شکل (۳۳-۶): اتصال سایت های کامپیوتری مجزا از یکدیگر به وسیله VPN

با استفاده از رمزنگاری، امکان مخفی سازی اطلاعات محرمانه نظیر رمز عبور و داده های داخل پست های الکترونیکی وجود دارد. رمزنگاری VPN شامل دو قسمت است که عبارتند از:

- الگوریتم رمز نگاری
- کلید رمزنگاری

معمولاً الگوریتم رمزنگاری دانش عمومی بوده و همه از روش آن آشنا هستند، ولی کلید رمزنگاری همواره مخفی می باشد. الگوریتم های رمزنگاری نوین مثل DES^1 ، از کلید رمز ۱۱۲ بیتی یا بیشتر استفاده می کنند. امنیت داده های رمز شده به امنیت کلید رمز بستگی دارد. هنگامی که دو سایت در مورد پیاده سازی VPN به توافق رسیدند، کلیدهای رمز خود را بین یکدیگر مبادله می کنند. علاوه بر کاهش هزینه های VPN نسبت به خطوط استیجاری، در VPN ها با استفاده از ارتباط های مطمئن امکان تبادل داده های تجاری و محرمانه وجود دارد. VPN های مدرن امروزه نیازی به فن آوری های محرمانه ندارند، بلکه با استفاده از سخت افزارها و نرم افزارهایی که به راحتی قابل نصب می باشند، امکان استفاده از VPN وجود دارد. همچنین نصب VPN نیازی به تغییر در پیکره بندی سرویس دهنده های شبکه ندارد. سر بار اضافی عملیات رمزنگاری VPN در شبکه به دیوارهای آتش و مسیریاب های شبکه منتقل می شود و به سرویس دهنده شبکه بار اضافی تحمیل نمی شود.

۱-۱۰-۶ پروتکل امنیتی اینترنت ($Ipsec^2$)

امروزه در اکثر محصولات VPN، از پروتکل امنیتی Ipsec برای افزایش اطمینان شبکه استفاده می شود. Ipsec از فن آوری امنیتی کامل و جامعی استفاده می کند. Ipsec برای برنامه های کاربردی موجود امکانات محافظتی شفافیتی فراهم می آورد، طوری که بدون نیاز به اعمال تغییرات نرم افزاری در برنامه های کاربردی موجود، امکان محافظت پیام های آنها وجود دارد. در شکل (۳۴-۶) جایگاه پروتکل Ipsec در معماری TCP/IP نشان داده شده است.

لایه کاربرد
TCP/IP
پروتکل IPsec
درایور کارت شبکه
کارت شبکه

شکل (۳۴-۶): جایگاه پروتکل Ipsec

Ipsec برای تمام پیام های ارسالی، سه قابلیت حافظتی زیر را فراهم می سازد:

^۱ Data Encryption Standard

^۲ Internet Protocol Security

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۲

- رمزنگاری
- تصدیق هویت^۱
- حفظ تمامیت و درستی داده ها^۲

همان طور که قبلاً اشاره شد، رمزنگاری باعث پنهان ساختن محتویات پیام می گردد. تصدیق هویت باعث می شود که هویت فرستنده پیام مورد تایید و تصدیق گیرنده قرار گیرد. حفظ تمامیت و درستی داده ها، مانع دست کاری کردن تمام یا بخشی از پیام توسط افراد غیرمجاز می شود. این سه قابلیت حافظتی Ipsec مانع از دزدی و سرقت داده ها می شود. براساس میزان گستردگی شبکه، نحوه استفاده از محصولات Ipsec متفاوت می باشد. سایت های بزرگ از پروتکل Ipsec که در داخل دیواره آتشین قرار دارد، برای محافظت اتصال های اینترنتی خود استفاده می کنند. سایت های کوچکتر می توانند از پروتکل Ipsec که داخل مسیریاب شبکه مخفی شده است، استفاده نمایند. کاربران انفرادی در ادارات کوچک و یا منازل می توانند از نسخه های رومیزی^۳، پروتکل Ipsec بر روی کامپیوترهای خود استفاده کنند. تنها در صورتی که ترافیک ورودی به شبکه از یک کاربر و یا سایت مورد تأیید تولید شده باشد، Ipsec اجازه ورود آن را به شبکه سازمان می دهد.

سیر تکاملی Ipsec

امروزه Ipsec، به یکی از مهمترین پروتکل های امنیتی رایج مورد استفاده در صنعت تبدیل شده است. در سال ۱۹۸۰ آژانس امنیتی ملی آمریکا^۴، به منظور توسعه و ایجاد پروتکل های همه منظوره امنیتی شبکه، شروع به اجرای پروژه ای به نام SDNS^۵ نمود.

در اوایل سال ۱۹۹۰، چندین شریک اولیه SDNS با همکاری یکدیگر اقدام به توسعه و طراحی پروتکل امنیتی جدیدی برای Ipv6 نمودند. به خاطر رواج بیشتر Ipv4 نسبت به Ipv6، پروتکل امنیتی طراحی شده برای استفاده در Ipv4^۶ فوق داده شد. در سال ۱۹۹۰، پروتکل Ipsec ارائه گردید.

بعد از آن تحقیقات و مطالعات زیادی برای تجدید نظر و توسعه و تکامل بیشتر پروتکل Ipsec انجام شد. پروتکل IKE^۶ برای مدیریت اتوماتیک کلیدهای رمزنگاری در Ipsec مورد تأیید قرار گرفت. تمام بازنگری های اعمال شده بر روی پروتکل Ipsec از طریق کمیته های استاندارد گزاری کنترل و نظارت می شود.

Ipsec قادر به استفاده در دیواره های آتشین و مسیریاب های متعدد می باشد. برای بررسی سازگاری محصولات، اکثر تولیدکنندگان دیواره آتشین و مسیریاب های شبکه اقدام به برگزاری آزمایش های تست سازگاری محصولات خود می نمایند. امروزه از Ipsec در سیستم عامل های ویندوز ۲۰۰۰ استفاده می شود.

پیاده سازی Ipsec VPN

شکلهای مختلف پیاده سازی Ipsec VPN به صورت زیر می باشد:

- سایت به سایت
- سرویس گیرنده / سرویس دهنده

^۱ Authentication

^۲ Integrity protection

^۳ desktop

^۴ National security agency

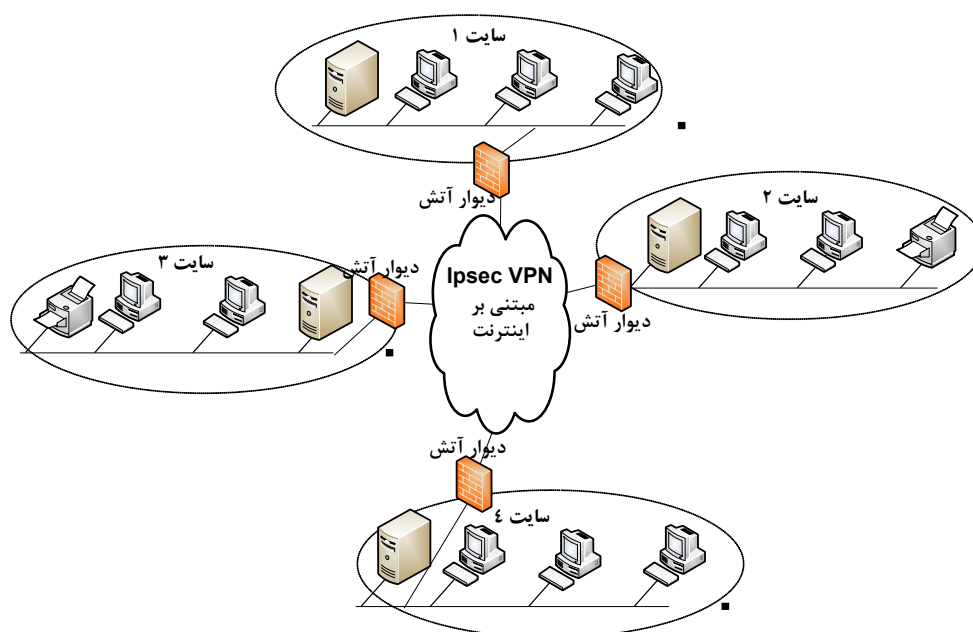
^۵ Secure Data Network System

^۶ Internet Key Exchange

شبکه های کامپیوتری (دکتر محمد حسن یغمایی مقدم - دانشگاه فردوسی مشهد)

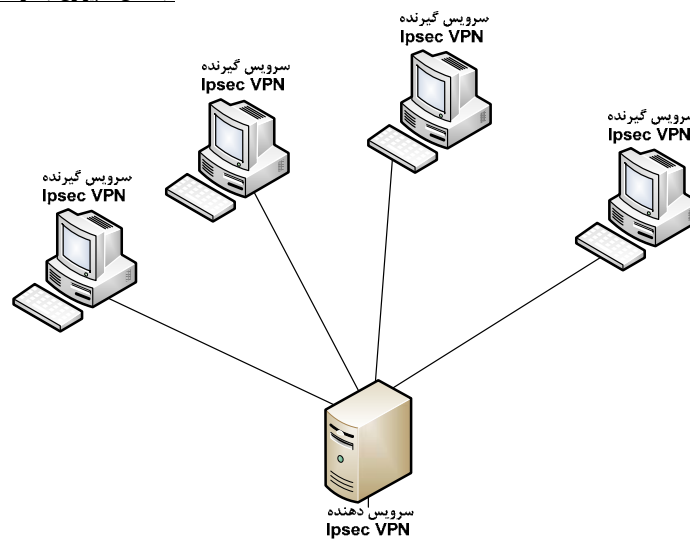
- ترکیب هردو روش

VPN های سایت به سایت از دو یا چند سایت جدا از هم که با استفاده از VPN به یکدیگر متصل شده و از داده های یکدیگر به صورت اشتراکی استفاده می کنند، تشکیل شده است. VPN های مبتنی بر مدل سرویس گیرنده/ سرویس دهنده از تعدادی کاربر راه دور که از طریق اینترنت به سایت مرکزی (سرویس دهنده) متصل هستند، تشکیل می شوند. مطابق با شکل (۳۵-۶) در VPN های سایت به سایت، هر سایت از طریق یک دیوار آتشین به اینترنت اتصال یافته است. از دیوار آتشین به همراه Isec برای محافظت داده های مبادله شده بین سایت ها استفاده می شود. برای برقراری VPN های سایت به سایت، هر سایت نیاز به اتصال اینترنت به همراه دیوارهای آتشین با قابلیت Isec دارد. برای برقراری اتصال های رمز شده مطمئن بین سایت ها، براساس پروتکل IKE، سایت ها باید اعتبارنامه های رمزنگاری خود را بین یکدیگر مبادله نمایند. در شکل (۳۶-۶) ساختار VPN های مبتنی بر مدل سرویس گیرنده/سرویس دهنده نشان داده شده است. در این ساختار یک سایت VPN با استفاده از پروتکل Isec اقدام به برقراری ارتباط های مطمئن با یک یا چند سرویس گیرنده انفرادی می کند. هردو طرف سرویس دهنده و سرویس گیرنده باید مجهز به نرم افزار Isec باشند.



شکل (۳۵-۶): اتصال سایت های کامپیوتری مجزا از یکدیگر به وسیله Isec VPN مبتنی بر اینترنت

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)^۱



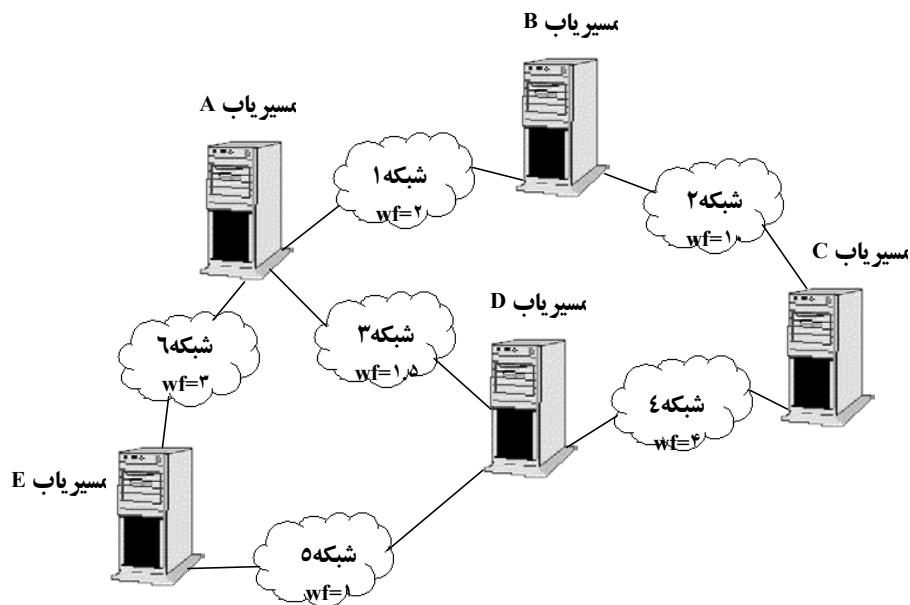
شکل (۶-۳۶): VPN از نوع سرویس گیرنده/سرویس دهنده

پرسش های فصل

۱. چهار وظیفه اصلی لایه شبکه را نام ببرید.
۲. شبکه های داده گرام و شبکه های مدار مجازی را از جنبه های مختلف با یکدیگر مقایسه نموده و برتری هریک را بردیگری توضیح دهید.
۳. ویژگی های اصلی الگوریتم های مسیریابی را نام برده و توضیح دهید.
۴. الگوریتم های مسیریابی ایستا را نام برده و نحوه عملکرد هریک را به اختصار توضیح دهید.
۵. برتری الگوریتم های مسیریابی پویا را بر الگوریتم های مسیریابی ایستا تشریح کنید.
۶. نحوه عملکرد الگوریتم مسیریابی بردار فاصله را توضیح دهید.
۷. در شبکه زیر مراحل ایجاد و تکمیل جداول مسیریابی هر مسیریاب را با استفاده از الگوریتم مسیریابی بردار فاصله توصیف کنید. (ارزش عددی هر لینک با WT^1 نشان داده شده است)

^۱Weight factor

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



۸. نحوه عملکرد الگوریتم مسیریابی وضعیت لینک را توضیح دهید.
۹. نقاط ضعف و قوت دو الگوریتم مسیریابی بردار فاصله و وضعیت لینک را با یکدیگر مقایسه کنید.
۱۰. مفهوم ازدحام در شبکه های کامپیوتری را نوشته و دلایل ایجاد آن را توصیف کنید.
۱۱. مفهوم ارتباط بین شبکه ای را توضیح دهید.
۱۲. رده های مختلف اتصال شبکه ها به یکدیگر را نوشته و از هر یک مثالی ذکر کنید.
۱۳. عملکرد تکرار کننده را در اتصال شبکه ها به یکدیگر توضیح دهید.
۱۴. عملکرد پل را در اتصال شبکه ها به یکدیگر توضیح دهید.
۱۵. برتری پل را نسبت به تکرار کننده توضیح دهید.
۱۶. انواع پل را نوشته و عملکرد هر یک را توضیح دهید.
۱۷. عملکرد مسیریاب را در اتصال شبکه ها به یکدیگر توضیح دهید.
۱۸. عملکرد دروازه را در اتصال شبکه ها به یکدیگر توضیح دهید.
۱۹. سه دسته کلی سرویس را در شبکه های ISDN نام برده و هر یک را توضیح دهید.
۲۰. انواع کانال های ISDN و سرعت هر یک را بنویسید.
۲۱. عملکرد TE1, TE2, NT1, NT2 و TA را در ISDN توضیح دهید.
۲۲. با رسم شکل جایگاه نقاط مرجع R, S, T و U را در ISDN بنویسید.
۲۳. مدل لایه های ISDN را نوشته و پروتکل هایی را که در هر لایه استفاده می شود را توضیح دهید.
۲۴. ساختار واسط کاربر به شبکه در لایه فیزیکی ISDN را با رسم شکل توصیف کنید.
۲۵. برتری B-ISDN را بر ISDN نوشته و موارد کاربرد آن را توضیح دهید.
۲۶. انواع سرویس ارائه شده توسط B-ISDN را توضیح دهید.
۲۷. ساختار قاب ها را در frame relay نوشته و عملکرد هر فیلد آن را توضیح دهید.
۲۸. با ذکر یک مثال نحوه ایجاد اتصال بین دو کامپیوتر را در شبکه های frame relay توضیح دهید.
۲۹. اهدافی را که در طراحی فن آوری ATM مد نظر بوده است، نام ببرید.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)^۲

۳۰. ویژگی ها و مزایای عمده ATM را بنویسید.
۳۱. انواع اتصال ها را در ATM نوشته و نحوه ایجاد مدار مجازی در آن را توضیح دهید.
۳۲. مفهوم آسنکرون بودن ATM را توصیف کنید.
۳۳. کاربرد سیگنالینگ در ATM را نوشته و انواع پیام های آن را توضیح دهید.
۳۴. برای برقراری اتصال های نقطه به چند نقطه در ATM از چه پیام هایی استفاده می شود؟
۳۵. ویژگی های لایه فیزیکی در ATM را نوشته و انواع کانال های فیزیکی را که در ATM استفاده می شود نام ببرید.
۳۶. ساختار سلول های ATM را رسم نموده و عملکرد هریک از فیلدهای موجود در سرآیند سلول های ATM را توضیح دهید.
۳۷. انواع کلاس های سرویس پشتیبانی شده لایه AAL در ATM را نوشته و مشخصه های مشخص سازی این سرویس را توضیح دهید.
۳۸. عملکرد شبکه های خصوصی مجازی را توضیح دهید.
۳۹. پروتکل امنیتی Ipsec را در اینترنت توصیف کنید.
۴۰. قابلیت های محافظتی Ipsec را توضیح دهید.
۴۱. روش های مختلف پیاده سازی Ipsec VPN را توصیف کنید.

فصل هفتم

معماری TCP/IP

۷-۱- تاریخچه TCP/IP

برای اولین بار در سال ۱۹۶۲ فردی به نام J.C.R. Licklider از دانشگاه MIT آمریکا، ایده ایجاد یک شبکه جهانی از کامپیوتر ها را مطرح نمود و آنرا برای توسعه بیشتر به آژانس پروژه تحقیقاتی پیشرفته دفاعی آمریکا (DARPA^۱)، منتقل کرد. به دنبال آن، دانشمند دیگری به نام Leonard Kleinrock از دانشگاه MIT آمریکا وبا همکاری با دانشگاه UCLA تئوری سوئیچینگ بسته ای را که پایه و اساس عملکرد شبکه جهانی اینترنت شد، ارائه نمود. در سال ۱۹۶۵ آقای Lawrence Roberts از دانشگاه MIT اقدام به اتصال کامپیوتری در Massachusetts آمریکا به کامپیوتر دیگری در ایالت کالیفرنیا این کشور و از طریق خطوط تلفنی نمود. در سال ۱۹۶۶ این شخص تجربه عملی فوق را به DARPA منتقل نمود. در سال ۱۹۶۸ DARPA قرارداد همکاری با شرکت BBN برای پیاده سازی نرم افزار شبکه

^۱Deffence Advance Research Project Agency

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

آرپانت که از قدیمترین شبکه های سوئیچینگ بسته ای می باشد، منعقد ساخت. بسیاری از مراکز تحقیقاتی و دانشگاه ها و پایگاه های نظامی از شبکه آرپانت برای پیاده سازی و آزمایش پروژه های تحقیقاتی خود استفاده کردند.

در سال ۱۹۶۹ با استفاده از شبکه فوق، چهار دانشگاه اصلی آمریکا به نام های دانشگاه UCLA، انیستیتوی تحقیقاتی Stanford، دانشگاه UCSB و دانشگاه Utah به یکدیگر متصل شدند. در سال ۱۹۷۰ مراکز دیگری شامل دانشگاه MIT، دانشگاه Harvard، شرکت های BBN و SDC به شبکه فوق اضافه شدند. به دنبال آن در سال ۱۹۷۱، آزمایشگاه های Lincoln دانشگاه MIT و دانشگاه های Carnegie-Mellon و Case-Western Reserve به شبکه فوق اتصال یافتند. در سال ۱۹۷۵ کنترل شبکه آرپانت از DARPA گرفته شد و به آژانس ارتباطات دفاعی آمریکا (DCA) منتقل گردید. این آژانس نظامی، از آرپانت به عنوان بخشی از شبکه دفاعی ملی (DNN) استفاده کرد.

در دهه ۷۰، معماری TCP/IP توسط فردی به نام Bob Kahn در شرکت BBN ارائه گردید و بعدها توسط Vint Cerf در دانشگاه Stanford و دیگران توسعه یافت. در سال ۱۹۸۰ وزارت دفاع آمریکا معماری فوق را جایگزین پروتکل قدیمی^۱ NCP در شبکه خود نمود. این معماری در سال ۱۹۸۳ به صورت جهانی مورد پذیرش قرار گرفت.

در سال ۱۹۸۳، شبکه آرپانت به دو شبکه تجزیه گردید. حاصل تجزیه این شبکه، دو شبکه مستقل دیگر به نام های میلنت و آرپانت شد. شبکه آرپانت به عنوان یک شبکه تحقیقاتی و آزمایشگاهی باقی ماند و میلنت برای کاربردهای نظامی و انتقال داده های محرمانه استفاده گردید. هر دو شبکه از بستر سخت افزاری یکسانی برای تبادل اطلاعات استفاده می کردند و امکان تبادل اطلاعات بین این دو شبکه وجود داشت. از شبکه آرپانت به عنوان یک شبکه پایه و اساسی برای پیاده سازی شبکه جهانی اینترنت استفاده شد. شبکه آرپانت دارای ۵۰ مینی رایانه مدل C30 و C300 ساخت شرکت BBN بود که از آن به عنوان سوئیچ های شبکه استفاده می شد. شبکه آرپانت دارای وسعت زیادی بود و تقریباً سراسر آمریکا و اروپای غربی را گسترش می داد. در ابتدای راه اندازی شبکه آرپانت اغلب از کانال های خطوط اجاره ای با سرعت ۵۶ کیلوبیت بر ثانیه استفاده می گردید، ولی امروزه از کانال های با سرعت بالاتر برای اتصال نودهای شبکه اینترنت استفاده می شود. با گسترش اینترنت، شبکه آرپانت از میان برداشته شد و جای خود را به شبکه گسترده و جهانی اینترنت داد. البته شبکه نظامی میلنت همچنان به کار خود ادامه می دهد. در سال ۱۹۸۶ شبکه NSFNET^۲ با استفاده از کانال های ۵۶ کیلوبیت بر ثانیه در ایالت متحده آمریکا توسعه یافت.

در شکل (۷-۱) مدل لایه ای و معماری TCP/IP که از آن به عنوان معماری شبکه جهانی اینترنت استفاده می شود، نشان داده شده است. یکی از قابلیت های عمده TCP/IP، امکان استفاده از آن در اتصال شبکه ها به یکدیگر جهت ایجاد یک شبکه وسیع تر می باشد. با استفاده از معماری TCP/IP امکان اتصال چندین شبکه محلی و ایجاد یک شبکه وسیع تر فراهم می آید. معماری TCP/IP قبل از مدل لایه ای مرجع OSI به وجود آمد و بنابراین لایه های TCP/IP به طور کامل با لایه های OSI مطابقت ندارند.

همان طور که در شکل (۷-۱) نیز مشاهده می شود، در معماری TCP/IP از پنج لایه فیزیکی، پیوند داده، شبکه، حمل و لایه کاربرد استفاده می شود. می توان گفت که لایه کاربرد در TCP/IP معادل سه لایه جلسه، ارائه و کاربرد در مدل OSI می باشد. در سطح لایه حمل در مدل TCP/IP از دو پروتکل^۳ TCP و^۴ UDP و در سطح لایه شبکه از پروتکل اینترنت^۵ (IP) استفاده می شود. یکی از مزایای بسیار عمده معماری TCP/IP که باعث گسترش و محبوبیت آن شده است، این

^۱ Network Control Protocol

^۲ National Science Foundation Network

^۳ Transmission Control Protocol

^۴ User Datagram Protocol

^۵ Internet Protocol

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۱

است که در این معماری هیچ استاندارد و پروتکل خاصی برای لایه های اول و دوم وضع نشده است. این امر باعث می شود که به راحتی بتوان از TCP/IP بر روی فن آوری های مختلف لایه فیزیکی استفاده کرد. در سطح لایه کاربرد، از پروتکل های کاربردی مانند FTP^۱، DNS^۲، TELNET^۳ و SMTP^۳ استفاده می شود.

ping	telnet & rlogin	FTP	SMTP	SNMP	Trace Route	لایه کاربرد	
DNS	TFTP	BOOTP	RIP	OSPF			
TCP		UDP		ICMP		لایه حمل	
IP						لایه شبکه	
		LLC		HDLC	PPP	لایه پیوند داده	
اترنت	802.3	X.25	حلقه نشانه	frame relay	ATM SMD\$...		
فیبرنوری		UTP	کابل هم محور		مایکروویو	ماهواره	لایه فیزیکی

شکل (۷-۱): معماری TCP/IP

۷-۲- نیاز به آدرس های IP

در شبکه های کامپیوتری، با اتصال چند شبکه به یکدیگر، شبکه اینترنت ایجاد می شود. باید توجه نمود که شبکه جهانی اینترنت که در آن میلیون ها کامپیوتر از طریق هزاران شبکه مختلف به یکدیگر متصل شده اند، نوع خاصی از شبکه اینترنت است. یکی از کارهای اصلی در ساختن یک شبکه TCP/IP، اختصاص دادن آدرسهای اینترنت به نود های شبکه می باشد. آدرسهای اینترنت در شبکه های TCP/IP آدرسهای IP نامیده می شوند. هنگام تخصیص آدرسهای IP، لازم است که چند عامل را در نظر بگیریم. اولین عامل که باید در نظر گرفته شود این است که هر آدرس شبکه IP یکتا باشد. آدرسهای IP دارای یک ساختار معین هستند. نمی توان فقط یک نود را به شبکه IP متصل کرد و به آن یک آدرس IP واحد اختصاص داد بلکه علاوه بر آن باید مراقب بود که آدرس IP با آدرسهای IP نود های دیگر آن بخش شبکه سازگار باشد. هنگام پیاده سازی معماری TCP/IP بر روی یک شبکه، یکی از کارهایی که باید انجام شود انتخاب و پیکره بندی درست آدرسهای IP است. دو نسخه فعلی از پروتکل IP موجود است که عبارتند از: IP نسخه ۴ (IPV4) و IP نسخه ۶ (IPV6). IP نسخه ۴ که هنوز پروتکل مهم اینترنت است از آدرسهای ۳۲ بیتی استفاده می کند. پروتکل IP نسخه ۶ که پروتکل نسل بعدی است، برای جایگزینی IP نسخه ۴ طراحی شده است. پروتکل IP نسخه ۶ از آدرسهای ۱۲۸ بیتی استفاده می نماید. برای اتصال نود ها به اینترنتی که شامل بیش از یک شبکه می باشد، باید از یک مدل آدرس دهی منطقی سازگار در شبکه استفاده شود. آدرسهای منطقی مشخص کننده های یکتایی می باشند. می توان برای تعیین این آدرسها از مقادیر عددی یا اسمی استفاده نمود. آدرسهای شبکه مشخص کننده های نقطه دسترسی به سرویس^۴ در لایه شبکه مدل مرجع هستند. این آدرسها، آدرسهای SAP شبکه^۵ (NSAP) نام دارند و می بایست برای همه پروتکل هایی که در لایه شبکه مدل مرجع ارتباط برقرار می کنند، یکتا باشند.

^۱Simple Network Management Protocol

^۲Domain Name System

^۳Simple Mail Transfer Protocol

^۴Service Access Point (SAP)

^۵Network SAP

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

در سطح لایه شبکه مدل مرجع TCP/IP، معمولاً از یک مقدار عددی به جای مقدار اسمی برای آدرسهای NSAP استفاده می شود. این انتخاب به خاطر آن است که برای پروتکل های لایه های پایین مدل مرجع، کار با مقادیر عددی به جای اسم های نمادین مفیدتر است. آدرس IP باید ساختاری داشته باشد تا مسیریابی را به طور کارآمد محاسبه کند. محاسبات مسیریابی با اعداد دودویی به جای اسمی نمادین کارآمدتر است و این دلیل دیگری است که چرا مقادیر عددی برای آدرسهای شبکه مناسبتر از اسمی نمادین هستند. به طور کلی لایه های بالاتر مدل مرجع TCP/IP مایل به استفاده از آدرسهای اسمی می باشند، درحالیکه لایه های پایین تر از آدرسهای عددی استفاده می کنند.

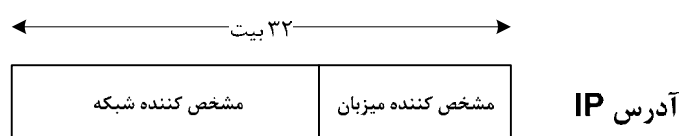
آدرسهای NSAP برای هر اتصال به شبکه فیزیکی مورد نیاز است. اگر N اتصال شبکه از یک میزبان موجود باشد، بایستی N آدرس NSAP به آنها نسبت داد. سخت افزار شبکه مانند یک بورد شبکه برای ایجاد اتصال به شبکه استفاده می شود و آدرسهای سخت افزاری شبکه مقادیر عددی هستند. طراحان اینترنت از یک مدل آدرس دهی منطقی شبکه برای آدرسهای IP استفاده نموده اند که از هر آدرس لایه فیزیکی مستقل می باشد.

معماری TCP/IP روی انواع مختلف سخت افزار شبکه قابل اجرا می باشد. برای مثال اترنت، شبکه حلقوی و FDDI از آدرسهای فیزیکی ۴۸ بیتی استفاده می کنند. بقیه انواع سخت افزار شبکه ممکن است از آدرس های ۸ بیتی، ۱۶ بیتی و یا ۳۲ بیتی استفاده کنند. با استفاده از آدرس های منطقی به جای آدرس های فیزیکی، پروتکل اینترنت مجبور نیست به صفات سخت افزاری شبکه زیرین ربط داده شود. از آنجا که آدرس های IP به آدرس های سخت افزاری وابسته نیستند، می توان سخت افزار زیرین را با سخت افزار جدیدتر بدون نیاز به تغییر آدرس منطقی جایگزین کرد. به بیان دیگر می توان شبکه را با تکنولوژیهای سریع تر و کارآمدتر ارتقاء داد بدون اینکه نیازی به تغییر آدرس های منطقی باشد.

۷-۳- ساختار آدرس های IP

برای مسیریابی بسته های IP، مسیریابها باید قادر به تمایز بین شبکه های منطقی مختلف باشند. طراحان شبکه تصمیم گرفتند تا آدرس IP را طوری ساختار دهی کنند که قادر باشند فرق بین شبکه های منطقی مختلف را تشخیص دهند. با اندازه ۳۲ بیتی آدرس NSAP، حداکثر تعداد اتصالاتی که در یک زمان می توان در شبکه داشت 2^{32} است که برابر با ۴,۲۹۴,۹۶۷,۲۹۶ یا در حدود ۴ میلیارد می باشد. بعضی از آدرسهای IP برای اهداف خاصی رزرو شده اند و نمی توانند به اتصالات شخصی شبکه اختصاص داده شوند. شکل (۷-۲) تقسیم آدرس IP را نشان می دهد. همانطور که در شکل (۷-۲) دیده می شود، آدرس IP دارای طول کلی چهار بایت می باشد که از دو قسمت عمده تشکیل شده است و عبارتند از:

- بخش مشخص کننده شبکه ($netid^1$)
- بخش مشخص کننده میزبان ($hostid^2$)



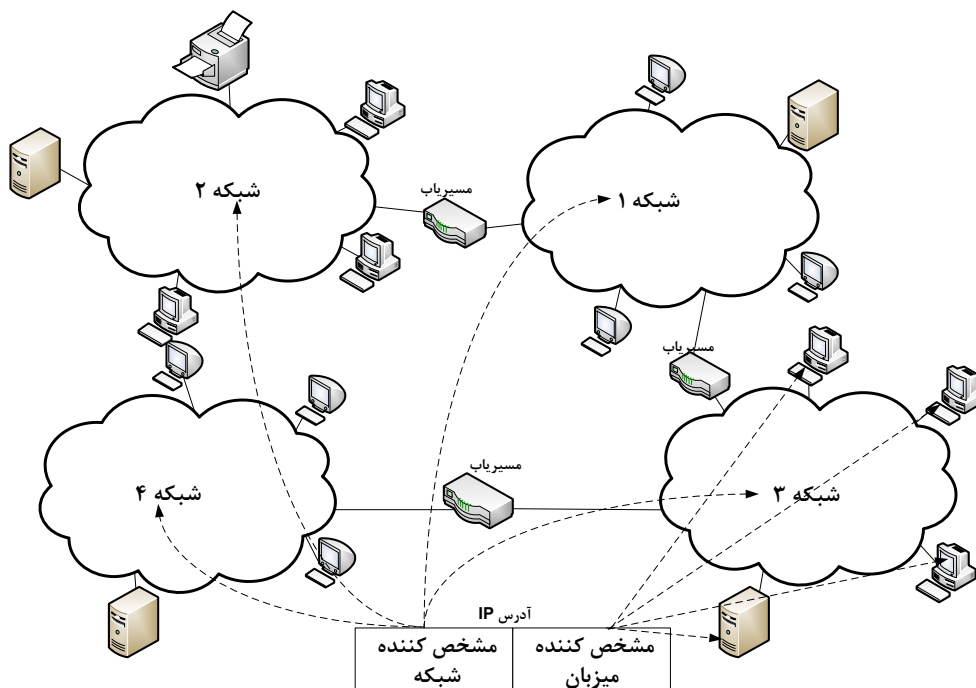
شکل (۷-۲): استفاده از آدرس IP برای شناسایی شبکه و میزبان

¹Network identifier

²Host identifier

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد) ۲

آدرس IP را بطور منطقی می توان به وسیله زوج (مشخص کننده میزبان، مشخص کننده شبکه) توصیف کرد. قسمت مشخص کننده شبکه، آدرس شبکه متصل را توصیف کرده و مشخص کننده میزبان کاربر را درون شبکه نشان می دهد. شکل (۷-۳) نشان دهنده این است که چگونه می توان از مشخص کننده های شبکه یکتا برای تشخیص شبکه های متصل استفاده کرد.



شکل (۷-۳): مثالی از شبکه نشان دهنده مقادیر مشخص کننده شبکه برای تشخیص شبکه

تقسیم آدرس IP به یک مشخص کننده شبکه و یک مشخص کننده میزبان، یک مدل آدرس دهی "سلسله مراتبی" است. آدرس دهی سلسله مراتبی برای مسیریابی کارآمدتر طراحی شده است. نگرانی اصلی مسیریابها رساندن بسته IP به شبکه مقصد است. برای این منظور مسیریابها باید اطلاعاتی درباره مشخص کننده های شبکه و نه مشخص کننده های میزبان ذخیره کنند. مشخص کننده های شبکه از مشخص کننده های میزبان کوتاهتر بوده و باعث می شود مقدار اطلاعاتی که مسیریابها باید بدانند مدیریت پذیرتر باشند. اگر تفاوتی بین شماره شبکه و شماره میزبان وجود نداشت و یک مدل آدرس دهی متوالی بجای یک مدل آدرس دهی سلسله مراتبی استفاده می شد، مسیریابها می بایست توانایی ذخیره همه ۴ میلیارد آدرس های IP را داشته باشند.

همه میزبانهای متصل به یک شبکه دارای یک مشخص کننده شبکه یکسان بوده و مشخص کننده میزبان آنها متفاوت است. برای اینکه مسیریابی به طور صحیح انجام شود، شبکه های متصل باید مشخص کننده شبکه یکتا داشته باشند. شبکه هایی که مشخص کننده شبکه یکسان دارند، دارای یک پیشوند عمومی می باشند که آدرس های IP میزبان های درون شبکه را نشان می دهد.

با تقسیم مشخص کننده شبکه و مشخص کننده میزبان، ۳ کلاس آدرس اولیه ایجاد گردید. در کنار ۳ کلاس A و B و C دو کلاس آدرس دیگر D و E نیز تعریف شده اند که در شکل (۷-۴) نشان داده شده است. کلاس D برای عملیات چندپخش (Multicast) و کلاس E برای انتقال پیامها به یک گروه انتخابی از نودها (Multicast) استفاده می شود.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

استفاده می شود. کلاس E برای استفاده های آینده رزرو شده است. جدول (۷-۱) تعداد شبکه ها و تعداد میزبانهایی که در هر کلاس آدرس IP قابل دسترسی هستند را نشان می دهد.



شکل (۷-۴): کلاسهای تعریف شده آدرس IP

کلاس A برای شبکه های خیلی بزرگ مناسب است اما چون فیلد مشخص کننده شبکه آن فقط ۷ بیت است، تنها ۱۲۷ تا از چنین شبکه هایی قابل ایجاد می باشد. آرپانت اصلی مثالی از یک شبکه کلاس A است. شبکه های کلاس B شبکه هایی با اندازه متوسط هستند که برای سازمانهای متوسط و بزرگ مناسبند. شبکه های کلاس C برای سازمان های کوچک مناسبند. در شبکه های کلاس C، هر شبکه نمی تواند بیشتر از ۲۵۴ میزبان داشته باشد.

جدول (۷-۱): تعداد شبکه ها و میزبان ها در هر کلاس آدرس

نوع کلاس	محدوده تغییرات مشخص کننده شبکه	تعداد شبکه	تعداد میزبان
کلاس A	۰ تا ۱۲۷	۱۲۷	۱۶۷۷۷۲۱۴
کلاس B	۱۲۸ تا ۱۹۱	۱۶۳۸۳	۶۵۵۳۴
کلاس C	۱۹۲ تا ۲۲۳	۲۰۹۷۱۵۱	۲۵۴
کلاس D	۲۲۴ تا ۲۳۹	-	-
کلاس E	۲۴۰ تا ۲۴۷	-	-

برای راحتی بیشتر، آدرس های IP ۳۲ بیتی با ۴ عدد دهمی نمایش داده می شوند. اعداد دهمی بوسیله نقطه از هم جدا می شوند. این نوع نمایش آدرس، نشانه گذاری دهمی نقطه دار نامیده می شود. در زیر یک آدرس IP در شکل دودویی و نشانه گذاری دهمی نقطه دار آن نشان داده شده است.

آدرس IP = ۱۰۰۱۰۰۰۰ ۰۰۰۱۰۰۱۱ ۰۱۰۰۱۰۱۰ ۱۱۰۰۱۰۰۱

آدرس IP = 144.19.74.201

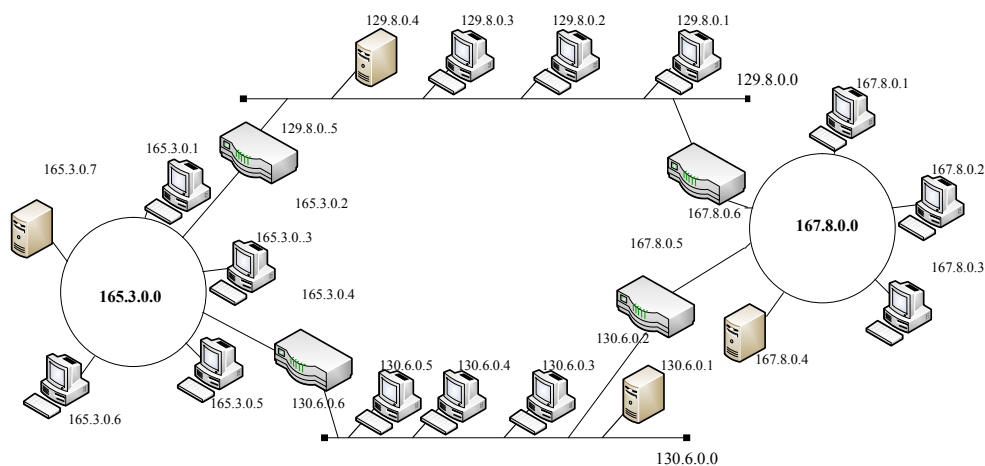
شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

جدول (۷-۲)، بازه مقادیر اولین عدد دهمی یک آدرس IP را در نشانه گذاری دهمی نقطه دار نشان می دهد. با استفاده از این جدول کلاس آدرس IP را به آسانی با بررسی اولین عدد دهمی آدرس IP می توان مشخص کرد.

جدول (۷-۲): تشخیص کلاس آدرس IP از اولین عدد دهمی

کلاس آدرس	حداقل مقدار اولین بایت آدرس	حداکثر مقدار اولین بایت آدرس
A	۰	۱۲۶
B	۱۲۷	۱۹۱
C	۱۹۲	۲۲۳
D	۲۲۴	۲۳۹
E	۲۴۰	۲۴۷

در شکل (۷-۵) مثالی از تخصیص آدرس های IP در یک شبکه اینترنت نشان داده شده است.



شکل (۷-۵): مثالی از آدرس های IP در یک شبکه اینترنت

۷-۴- آدرسهای خاص IP

برخی از آدرسهای IP دارای مفهوم خاصی بوده و برای کاربردهای خاصی رزرو شده اند. این آدرسهای خاص به شرح زیر می باشند:

۷-۴-۱- آدرس 0.0.0.0

در این آدرس، فیلد شماره شبکه صفر است که به معنی "این شبکه" می باشد. فیلد شماره میزبان نیز صفر است، که به معنی "این نود" در شبکه است. این آدرس معمولاً زمانی استفاده می شود که یک نود شبکه سعی می کند تا آدرس خود را مشخص کند. به عنوان مثال، نود های شبکه برای انتساب یک آدرس IP از یک سرویس دهنده مرکزی BOOTP استفاده می کنند. هنگامی که نود IP یک تقاضای ابتدایی را به سرویس دهنده BOOTP می فرستد، نود IP فرستنده که فاقد آدرس IP است از مقدار 0.0.0.0 در فیلد آدرس IP مبدا استفاده می کند تا نشان دهد که "این نود" (شماره میزبان صفر) در "این شبکه" (شماره شبکه صفر) است. هنگامی که نود، آدرس IP خود را از پاسخ BOOTP بدست آورد دیگر از آدرس 0.0.0.0 استفاده نمی کند. آدرس 0.0.0.0 در جداول مسیریابی نیز استفاده می شود تا ورودیهای شبکه را برای آدرس IP مسیریاب پیش فرض نشان دهد. باید توجه نمود که آدرس IP 0.0.0.0 را فقط می توان به عنوان آدرس IP مبدا استفاده کرد و هرگز به عنوان آدرس IP مقصد استفاده نمی شود.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۱

۷-۴-۲- آدرس 0.hostid

این آدرس به معنی شماره میزبان در "این شبکه" است. اگر یک نود در شبکه ای بسته ای را دریافت کند که شماره شبکه در آدرس IP مقصد صفر باشد اما شماره میزبان موجود در آدرس مقصد با آن نود مطابقت داشته باشد، نود بسته را خواهد پذیرفت. گیرنده مقدار صفر را در شماره شبکه به معنی این شبکه تفسیر می کند.

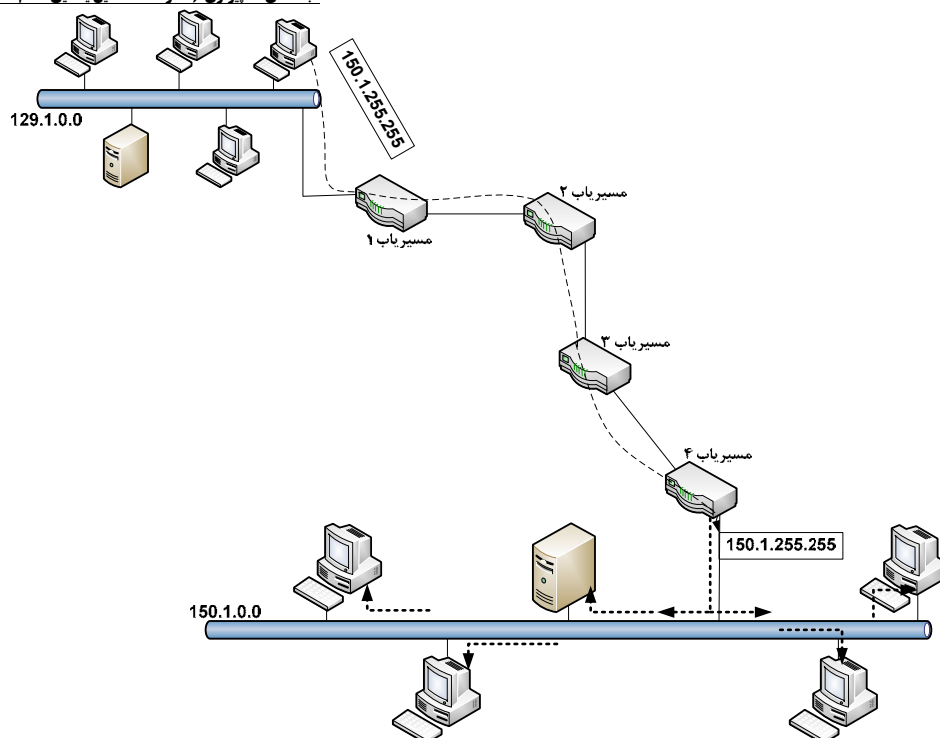
۷-۴-۳- آدرس netid.255

این آدرس همه پخش مستقیم^۱ بوده و به معنی ارسال بسته به همه نود ها در یک شبکه خاص است. این آدرس می تواند بعنوان آدرس IP مقصد یک بسته IP استفاده شده و هرگز نمی تواند به عنوان آدرس مبدأ باشد. یک آدرس همه پخش مستقیم توسط همه نود های شبکه دیده می شود. بنابراین به عنوان مثال برای شماره شبکه 137.53، آدرس همه پخش 137.53.255.255 خواهد بود.

پیام های همه پخش مستقیم به یک شبکه خاص فرستاده می شوند که شماره آن شبکه در فیلد شماره شبکه آدرس IP مقصد مشخص می شود. مسیریابهای شبکه، قادر به پیش بردن بسته های همه پخش مستقیم می باشند و بسته IP را به مسیریاب نهایی که به شبکه مقصد متصل است، می فرستند. مسیریاب شبکه مقصد مجبور خواهد بود که بسته IP را به همه نود های شبکه بفرستد. همانطور که در شکل (۷-۶) دیده می شود، آدرس های همه پخش مستقیم از مسیریاب های میانی شبکه عبور کرده و در شبکه مقصد به همه میزبان ها به صورت همه پخش ارسال می شوند. در این مثال، ایستگاهی در شبکه بالا به آدرس شبکه 129.1.0.0 بسته همه پخش مستقیم به آدرس 150.1.255.255 ارسال می دارد. این بسته از تمام مسیریاب های میانی عبور کرده تا به مسیریاب متصل به شبکه مقصد برسد (مسیریاب ۴). این مسیریاب متوجه می شود که آدرس مقصد به صورت همه پخش مستقیم است. بنابراین با استفاده از قابلیت همه پخش لایه ۲، بسته دریافتی را به همه میزبان های شبکه ارسال می دارد.

¹ Directed broadcast

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۶-۷): مثالی از یک همه پخشی مستقیم

البته می توان با پیکره بندی مناسب مسیریاب های شبکه، از پیش بردن بسته های همه پخشی مستقیم توسط مسیریاب های شبکه جلوگیری نمود.

۷-۴-۴- آدرس 255.255.255.255

این آدرس خاص، نشان دهنده یک آدرس همه پخشی محدود است که از جانب مبدا به همه نود های آن شبکه ارسال می شود. همه پخشی محدود در شبکه های محلی قابل استفاده است و هرگز از مرز یک مسیریاب عبور نمی کند. در یک همه پخشی مستقیم، فرستنده باید مقدار شماره شبکه را در بخش خاص آدرس مقصد قرار دهد. اگر همه پخشی در یک شبکه محلی مورد نظر باشد، می توان از همه پخشی محدود استفاده کرد که نیازی به داشتن شماره شبکه ندارد. یک آدرس همه پخشی محدود هرگز به عنوان یک آدرس IP مبدا استفاده نمی شود، بلکه فقط می تواند به عنوان یک آدرس IP مقصد استفاده گردد.

۷-۴-۵- آدرس netid.0

این آدرس که همه بیت های مشخص کننده میزبان در آن صفر است، هرگز به یک میزبان خاص انتساب داده نمی شود و نشان دهنده خود شبکه است. به عنوان مثال، آدرس IP 137.53.0.0 را در نظر بگیرید. این یک آدرس شبکه کلاس B است که به شبکه کلاس B 137.53 اشاره می کند.

۷-۴-۶- آدرس 127.x.x.x

با بررسی جدول (۷-۲)، می توان متوجه شد که عدد ۱۲۷ که باید در بازه مقادیر کلاس A باشد، در مجموعه آدرس های کلاس A استفاده نمی شود. این عدد برای قابلیت برگشت حلقه رزرو شده است. آدرس برگشت حلقه یک آدرس مخصوص است. در خیلی از کاربردهای شبکه، تمایل به بررسی و تست نرم افزار وسیستم عامل شبکه می باشد. نتایج موجود در هر بسته ای که توسط یک برنامه کاربردی به آدرس 127.X.X.X ارسال شود، بدون دستیابی به واسطه شبکه به برنامه کاربردی برمی گردد. بسته از بافر انتقال به بافر دریافت در همان کامپیوتر کپی می شود. به این دلیل است که آدرس 127.X.X.X آدرس برگشت حلقه نامیده می گردد. آدرس برگشت حلقه نرم افزاری را می توان برای تشخیص پیکره بندی صحیح TCP/IP استفاده کرد. برای مثال می توان از این خاصیت همراه با ابزار Ping استفاده نمود تا از کار کردن نرم افزار لایه IP اطمینان حاصل کرد. ابزار Ping یک بسته ICMP را به یک آدرس IP مقصد می فرستد و لایه IP در آن آدرس به آن پاسخ می دهد. در فصل بعد، با عملکرد پروتکل ICMP آشنا خواهیم شد.

۷-۴-۷- آدرس های تک پخشی، همه پخشی و چند پخشی

هنگامیکه یک بسته IP به یک آدرس IP انفرادی فرستاده می شود، یک بسته IP تک پخش نامیده می شود و فرآیند ارسال بسته، تک پخشی نام دارد. از تک پخشی برای برقراری ارتباط بین دو نود IP استفاده می شود. هنگامیکه یک بسته IP به همه نود های یک شبکه خاص فرستاده می شود، همه پخشی نام دارد. در چند پخشی یک آدرس کلاس D به عنوان آدرس مقصد استفاده می گردد. بسته IP به گروهی از نودها تحویل داده می شود که توسط یک آدرس کلاس D مشخص می شوند. سیستم هایی که آدرس چندپخشی یکسان دارند به یک گروه چندپخشی متعلق هستند. به اعضای یک گروه چندپخشی همانطور که یک آدرس کلاس D انتساب داده می شود، می بایست یک آدرس IP از گروه آدرس کلاس C,B,A نیز انتساب گردد. گروه چندپخشی به دو طریق می تواند یک بسته IP را دریافت کند:

- بسته های IP مستقیماً به آدرس IP خصوصیشان فرستاده شود (کلاس C,B,A)

- بسته های IP به آدرس چندپخشی آنها ارسال شود (کلاس D)

آدرسهای کلاس D با عددی در بازه ۲۲۴ تا ۲۳۹ شروع می شوند. برای انجام چندپخشی، یک میزبان باید توانایی پیوستن به یک گروه چندپخشی یا بیرون رفتن از گروه چند پخشی را داشته باشد. این توانایی معمولاً با یک خط دستور و سیستم عامل خاص پیاده سازی می شود. نرم افزار لایه IP باید توانایی شناسایی آدرسهای چند پخشی بسته های IP ورودی و خروجی را داشته باشد. پیاده سازیهای قدیمی IP، قادر به شناسایی آدرسهای چندپخشی نبودند. هر میزبان در شبکه IP توانایی پیوستن به یک گروه چندپخشی را دارد. لازم نیست میزبانها در یک شبکه محلی منفرد باشند بلکه این امکان وجود دارد که هر میزبان در یک شبکه مختلف و دور از یکدیگر وجود داشته باشند. این شبکه ها بوسیله مسیریابها از هم جدا می شوند. در نتیجه مسیریابها باید بدانند که چگونه بسته های چند پخشی را در شبکه پیش ببرند. برای انجام اینکار بطور کارآمدتر مسیریابها باید بدانند که آیا میزبانهای موجود در یک شبکه متصل محلی بخشی از یک گروه چند پخشی هستند یا خیر؟ بدین منظور مسیریابها اطلاعاتی را بین یکدیگر مبادله می کنند و کشف می کنند که آیا اعضای گروه در شبکه های دور وجود دارند یا خیر؟ میزبانهایی که به یک گروه چندپخشی می پیوندند یا آن را ترک می کنند از پروتکل مدیریت گروه اینترنت^۱ (IGMP) برای گزارش عضویشان در گروه به مسیریابهای همسایه استفاده می کنند. مسیریابهای همسایه این گزارش را دریافت نموده و جداول داخلی خود را درباره میزبانهایی که اعضای یک گروه چند پخشی هستند را به روز می رسانند. مسیریابها توانایی سرشماری میزبانها را بوسیله پرس وجو درباره عضویت جایشان در فواصل معین نیز دارند. این

¹ Internet Group Management Protocol(IGMP)

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

سرشماریها با استفاده از آدرس چندپخشی مخصوص 224.0.0.1 به همه سیستمها در این زیر شبکه فرستاده می شود. هنگامی که یک چند پخشی به یک شبکه محلی فرستاده می شود، از توانایی سخت افزاری چند پخشی شبکه های محلی استفاده می شود.

۷-۵- زیر شبکه سازی

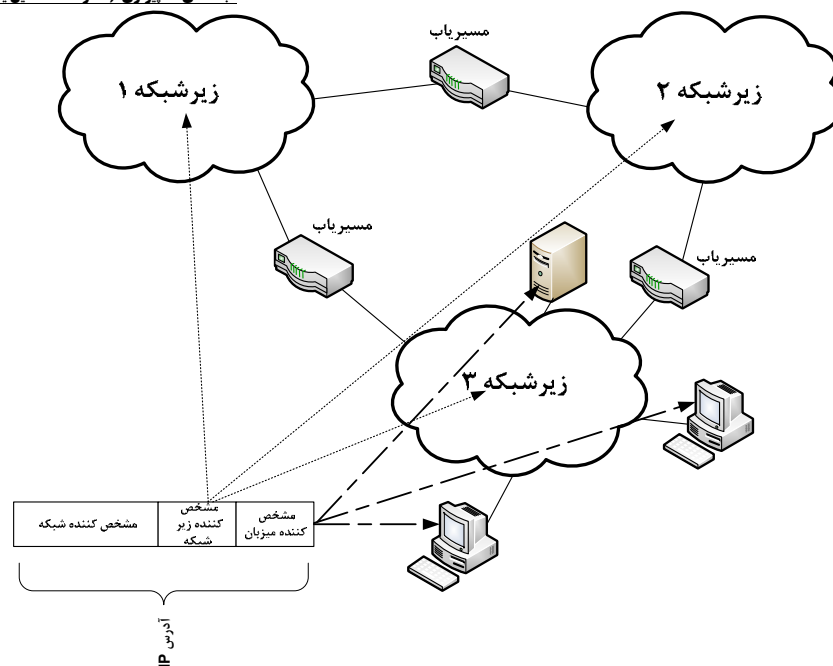
آدرس های IPv4 برای تخصیص به شبکه های مختلف با ابعاد متفاوت طراحی شده اند. این قالب های آدرس در مراحل آغازین اینترنت به خوبی کار می کردند، اما با رشد و گسترش اینترنت و افزایش تعداد میزبان های شبکه، به تدریج ضعف قالب های آدرس IP نمایان گردید. این ضعف، عدم استفاده بهینه از فضای آدرس های IP و وجود اتلاف در آنها بود. برای حل مشکل اتلاف فضای آدرس IP، مفهوم زیر شبکه سازی در سال ۱۹۸۵ مطرح گردید.

زیر شبکه ها با استفاده از یک شماره شبکه، امکان اتصال چندین شبکه را به یکدیگر ممکن می سازند. همانطور که قبلاً ذکر شد، آدرس شبکه برای همه میزبان های داخل یک شبکه یکسان است. معمولاً طراحان شبکه، یک آدرس شبکه یکتا را به یک شبکه داده شده انتساب می دهند و سپس به میزبانها، مقادیر قسمت میزبان آدرس IP انتساب داده می شود. این تنظیم منتج به این امر می شود که همه میزبانهای داخل یک شبکه یک پیشوند آدرس شبکه یکسان داشته باشند. تعداد بیتهای استفاده شده در پیشوند آدرس شبکه به قالب آدرس IP بستگی دارد. برای قالب آدرس کلاس A، ۸ بیت برای آدرس شبکه و ۲۴ بیت برای آدرس میزبان استفاده می شود. برای آدرس کلاس B، ۱۶ بیت برای آدرس شبکه و ۱۶ بیت برای آدرس میزبان استفاده می شود. برای قالب آدرس کلاس C، ۲۴ بیت برای آدرس شبکه و ۸ بیت برای آدرس میزبان استفاده می گردد. مزیت استفاده از مدل دو بخشی آدرس شبکه و آدرس میزبان برای آدرس های IP، کمینه کردن تعداد ورودی ها در جدول مسیر یابی است. به جای اینکه برای هر میزبان در یک شبکه یک رکورد در جدول مسیریابی داشته باشیم، میتوان با استفاده از یک رکورد مجرد جدول مسیریابی همه میزبان های در یک شبکه را خلاصه کرد. این رکورد جدول مسیریابی فقط شامل قسمت آدرس شبکه است که پیشوند مشترک برای همه میزبان های شبکه می باشد. مسیریابها، پیشوند مشترک شبکه های مقصد را در جدول مسیریابی خود با پیشوند آدرس IP مقصد موجود در بسته انطباق می دهند. یک انطباق منجر به انتخاب مسیر خاص برای مسیریابی بسته می شود. هنگامی که یک مسیر یاب یک بسته را به یک شبکه می فرستد، مسیر یاب تنها قسمت شبکه آدرس IP مقصد بسته را بررسی میکند و قسمت میزبان آدرس IP مقصد را بررسی نمی نماید.

به عنوان مثال یک شبکه IP را با شماره شبکه 149.108.0.0 در نظر بگیرید که ۱۶ بیت قابل انتساب دارد. این ۱۶ بیت کلاً ۲^{۱۶} ترکیب شماره میزبان را که برابر با ۶۵۵۳۶ است ممکن می سازد. از ۶۵۵۳۶ ترکیب نمی توان الگوی متشکل از بیتهای ۱ (همه بیتها ۱) را استفاده کرد. چون این الگو برای آدرس همه پخشی رزرو شده است. همچنین نمیتوان الگوی متشکل از بیت های صفر (همه بیتها صفر) را برای انتساب شماره میزبان استفاده کرد، زیرا این الگو برای خود شبکه رزرو شده است. بنابراین از کل ۶۵۵۳۶ شماره میزبان ممکن، تنها از دو شماره میزبان نمی توان استفاده کرد. بنابراین در کل ۶۵۳۵۴ میزبان باقی می ماند.

استفاده از قابلیت زیر شبکه سازی، شبکه را قادر می سازد تا بدون اینکه بقیه شبکه متصل شده از تغییرات در شبکه داخلی مطلع شوند، به طور داخلی ساختاردهی گردند. شکل (۷-۷) ارتباط بین فیلدهای یک آدرس IP و زیر شبکه را نشان می دهد.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد) ۲۵۲



شکل (۷-۷): زیر شبکه و شماره های زیر شبکه

مسیریاب های موجود بین زیر شبکه ها، باید از تعداد بیت تخصیص داده شده به زیر شبکه سازی، مطلع باشند. مزایای زیر شبکه سازی شامل موارد زیر است:

- کاهش ترافیک شبکه
- افزایش کارایی شبکه
- ساده سازی مدیریت
- ساختار دهی مجدد یک شبکه داخلی بدون اثر گذاشتن شبکه های خارجی
- بهبود بخشیدن امنیت

۷-۵-۱- پوشش زیر شبکه^۱

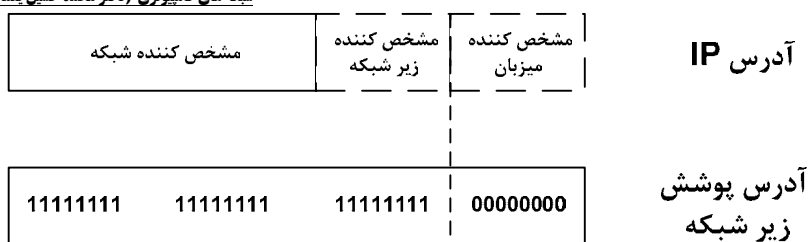
پوشش زیر شبکه بوسیله مسیریابها و میزبانهای زیر شبکه به منظور تشخیص و جداسازی فضای کامپیوتر میزبان از فضای زیر شبکه استفاده می شود. پوشش زیر شبکه فیلد مشخص کننده میزبان را به شماره زیر شبکه و شماره میزبان تقسیم می کند. پوشش زیر شبکه یک عدد ۳۲ بیتی است که مقدار آن با استفاده از قوانین زیر شکل می گیرد:

- ۱ها در پوشش زیر شبکه متعلق به قسمت مشخص کننده شبکه و شماره زیر شبکه در آدرس IP است.
- صفر ها در پوشش زیر شبکه متعلق به قسمت شماره میزبان در آدرس IP است.

شکل (۷-۸) مثالی از نحوه کاربرد این قوانین را نشان می دهد. این شکل یک شماره شبکه کلاس B را نشان می دهد که برابر 255.255.255.0 می باشد.

¹ Subnet mask

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۷-۸): نمایش پوشش زیر شبکه

از آنجاییکه در قالب بسته های IP کلاس B فضای مشخص کننده میزبان برابر با ۱۶ بیت می باشد، بنابراین در حالت عادی و بدون استفاده از زیر شبکه سازی، مقدار آدرس پوشش برای کلاس B برابر با 255.255.0.0 است. اگر مقدار پوشش زیر شبکه 255.255.255.0 برای یک شبکه کلاس B استفاده شود، این مقدار نشان میدهد که از زیر شبکه سازی استفاده شده است. با توجه به تعداد ۱های موجود در آدرس پوشش زیر شبکه فوق، می توان دریافت که فضای مشخص کننده میزبان در آدرس کلاس B فوق برابر با ۸ بیت می باشد.

۷-۵-۲- انتساب کارآمد شماره های زیر شبکه

در زیر شبکه سازی، قسمت میزبان آدرس IP به دو فیلد تقسیم می شود که عبارتند از شماره زیر شبکه و شماره میزبان. با این تقسیم بندی، آدرس IP دارای سلسله مراتب سه سطحی می شود. این عمل منجر به صرفه جویی در مسیریابی و استفاده مجدد از یک پیشوند شماره شبکه مشترک برای زیر شبکه ها می شود.

۷-۶- آدرسهای شبکه های خصوصی (اینترنت ها)

در سال ۱۹۹۴، برای کاهش نیاز به آدرس های IP جدید، RFC1597 راجع به اختصاص آدرس به شبکه های خصوصی ارائه شد. نویسندگان این RFC، مدلی را برای انتساب آدرس های IP در شبکه های خصوصی پیشنهاد کردند. شبکه های خصوصی اتصال محدودی به اینترنت دارند. میزبان های موجود در این شبکه ها را می توان به گروه های زیر کلاس بندی کرد:

- میزبانهایی که نیاز به دستیابی به میزبانهای در سازمانهای تجاری دیگر یا اینترنت ندارند.
- میزبانهایی که نیاز به دستیابی به سرویسهای خارجی محدودی مانند FTP، e-mail، remote login، Netnews و غیره دارند که می توان با استفاده از دروازه لایه کاربرد این دستیابی را فراهم نمود.
- میزبانهایی که نیاز به دستیابی در سطح لایه شبکه به شبکه خارج از سازمان تجاری دارند. این نیازمندی از طریق اختصاص اتصال های IP با آدرس های معتبر، رفع می شود.

برای تخصیص آدرس به میزبان های نوع اول، می توان از آدرس های IP غیر معتبر استفاده نمود. این آدرسها فقط در همان شبکه خصوصی اعتبار داشته و از دنیای خارج قابل دسترسی نمی باشند. چون با این میزبان ها هیچ مبادله بسته خارج از شبکه خصوصی رخ نمی دهد، مشکل آدرس IP تکراری هرگز دیده نخواهد شد. میزبان های دسته دوم که به وسیله دروازه سطح کاربرد از اینترنت خارجی ایزوله شده اند، نیازی به آدرس های IP یکتا در اینترنت ندارند. به این دلیل که دروازه سطح کاربرد، آدرس های IP این میزبانها را از شبکه خارجی مخفی می سازند. بنا به دلایل امنیتی، خیلی از سازمانهای

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)^۲

تجاری برای اتصال به شبکه داخلی خود به اینترنت از دروازه های لایه کاربرد (مانند دیوار آتش^۱) استفاده می کنند. شبکه داخلی معمولاً بطور مستقیم به اینترنت دسترسی ندارند و فقط یک یا چند میزبان دیوار آتش از اینترنت قابل رویت هستند. در این حالت، شبکه داخلی می تواند از شماره های IP غیر یکتا استفاده کند.

توسط نهاد IANA^۲ آدرس های IP تخصیص داده می شود. نهاد IANA توسط ICANN^۳ اداره می شود. ICANN یک شرکت غیرانتفاعی کالیفرنیا ای آمریکا می باشد که در سال ۱۹۹۸ تاسیس گردید و وظیفه عمده آن مدیریت تخصیص نام ها و آدرس های IP می باشد.

IANA سه بلوک از فضای آدرس IP را برای شبکه های خصوصی رزرو کرده است تا به میزبان های گروه یک و دو انتساب داده شود. این سه بلوک آدرس عبارتند از:

- ۱ شبکه کلاس A از آدرس 10.0.0.0 تا 10.255.255.255
- ۱۶ شبکه کلاس B از آدرس 172.16.0.0 تا 172.31.255.255
- ۲۵۶ شبکه کلاس C از آدرس 192.168.0.0 تا 192.168.255.255

چنانچه یک سازمان تجاری تصمیم بگیرد تا از آدرس های IP خارج از فضای آدرس فهرست شده فوق استفاده کند، این کار را می تواند بدون هیچ هماهنگی با IANA انجام دهد. این فضای آدرس می تواند توسط خیلی از سازمانهای تجاری استفاده شود و نیاز به انتساب شماره شبکه های جدید نمی باشد. آدرسهای فوق در فضای آدرس خصوصی سازمان تجاری، یکتا هستند اما در شبکه یکتا نمی باشند. اگر یک سازمان تجاری برای کاربردها و وسایل متصل به شبکه خود نیاز به فضای آدرس یکتای سرتاسری داشته باشند، چنین آدرسهایی را از سرویس دهنده اینترنت بدست خواهند آورد. از آنجاییکه آدرس های خصوصی معنی سرتاسری ندارند، اطلاعات مسیریابی درباره شبکه های خصوصی نباید خارج از سازمان تجاری منتشر شوند.

۷-۶-۱- سیستم ترجمه آدرس های شبکه (NAT^۴)

سیستم NAT آدرس های IP شبکه محلی را به آدرسهای یکتا برای استفاده بر روی اینترنت تبدیل می کند. هرچند این روش برای ایجاد آدرس های بیشتر برای استفاده در شبکه داخلی ابداع شده است، ولی می توان از آن برای مخفی کردن اطلاعات مربوط به سیستمهای داخلی نیز استفاده کرد. NAT می تواند تمام اطلاعات مربوط به پروتکلهای TCP/IP شبکه داخلی را مخفی کرده طوری که از دید کاربران خارجی چنین به نظر برسد که تمام ترافیک از یک آدرس خاص منتشر می شود. سیستم NAT همچنین این امکان را فراهم می کند که هر محدوده آدرسی را بتوان برای سیستمهای داخلی استفاده کرد، بدون اینکه کوچکترین مشکلی برای شبکه پیش بیاید.

عملکرد NAT به این صورت است که یک دستگاه (مثل کامپیوتر یا مسیریاب) به عنوان دروازه ورود به اینترنت عمل می کند و با این کار آدرس های ایستگاه های کاری را به آدرس دستگاهی که NAT روی آن فعال است ترجمه می کند. به بیان دیگر NAT روی دستگاهی که به اینترنت وصل شده فعال می شود و ایستگاه های کاری و به طور کلی شبکه داخلی را از دید اینترنت پنهان می دارد. از سوی دیگر اینترنت، کل شبکه را به صورت یک دستگاه ساده می بیند که به اینترنت متصل می باشد.

^۱ Firewall

^۲ Internet Assigned Numbers Authority

^۳ Internet Corporation for Assigned Names and Numbers

^۴ Network Address Translation

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد ۹۵)

NAT روی شبکه تغییری ایجاد نمی کند و نیازی به تنظیمات دوباره روی ایستگاه های کاری نیست. فقط ایستگاه های کاری می بایست آدرس دروازه خروجی از شبکه را که همان آدرس دستگاهی است که NAT روی آن فعال شده را بدانند. چهار عملکرد اصلی NAT به ترتیب میزان استفاده در زیر آمده است:

- ترجمه ایستا : حالتی است که یک سیستم خاص (مثلا یک سرور دهنده) همیشه دارای ترجمه آدرس ثابتی است که امکان برقراری ارتباط از طرف سیستمهای خارجی با آن را فراهم می کند.
 - ترجمه پویا (اتوماتیک): حالتی است که یک عده از سیستمهای داخلی از یک یا چند آدرس برای ارتباط با شبکه خارجی استفاده می کنند. این روش برای مخفی کردن مشخصات سیستمهای داخلی یا گسترش محدوده آدرسهای مورد استفاده در شبکه داخلی استفاده می شود.
 - توزیع بار : در این حالت یک آدرس ثابت به یک سری آدرس دیگر ترجمه می شود که همه سرور دهنده هایی هستند که به یک درخواست خاص پاسخ می دهند. این روش برای توزیع بار یک سرور دهنده پرتراфик بر روی یک سری سرور دهنده استفاده می شود.
 - افزونگی : در حالتی که یک شبکه از چند روش برای اتصال به اینترنت استفاده می کند، از این روش استفاده می شود تا در صورت قطع شدن هر کدام از مسیرها از مسیر دیگر استفاده شود.
- NAT دارای برخی مشکلات نیز می باشد. بعضی پروتکلها از طریق NAT قابل استفاده نمی باشند، از جمله این پروتکل ها عبارتند از:

- پروتکلهایی که نیاز به برقراری ارتباط مجدد با سرویسگیر دارند : هیچ مسیر مشخصی به سمت سرویسگیر وجود ندارد پروتکلهای H.323 ، RSH و IRC از این دسته اند.
- پروتکلهایی که آدرسهای TCP/IP را داخل اطلاعات بسته قرار می دهند.
- پروتکلهایی که اطلاعات سرآیند TCP/IP را رمز می کنند. پروتکل PPTP از این دسته پروتکل هاست.
- پروتکلهایی که از آدرس فرستنده برای چک کردن مسائل امنیتی استفاده می کنند.
- علاوه بر موارد فوق، پروتکل ICMP نیز با NAT مشکل دارد. نرم افزار ICMP بعضی وقتها قسمت اول بسته اصلی را که شامل آدرسهای ترجمه نشده می باشد، داخل پیام ICMP قرار می دهد. البته از لحاظ امنیتی هیچ لزومی ندارد که بسته های ICMP بتوانند از دیواره آتش عبور کنند.

استفاده از NAT یک سری مشکلات امنیتی نیز دارد که به مواردی از آنها در اینجا اشاره می شود:

- ترجمه ایستا = عدم امنیت: استفاده از ترجمه ایستا سیستمهای داخلی را محافظت نمی کند. استفاده از ترجمه ایستا، فقط آدرس و شماره درگاه سرویسگیر را بصورت یک به یک عوض می کند و هیچ مکانیزم امنیتی روی ارتباط ایجاد شده برقرار نمی کند. برای محافظت از یک سرور داخل شبکه باید از پراکسی استفاده کرد.
- یک ارتباط همیشه دوطرفه است: وقتی یک سرویسگیر با یک سرور دهنده ارتباط برقرار می کند، یک ارتباط از سرور دهنده به سمت سرویسگیر نیز ایجاد می شود. برقراری ارتباط با بعضی سرور دهندهها، مثلاً یک وب سایت ، ممکن است منجر به بروز مشکلات امنیتی در شبکه شود. از آنجا که روی تمام ارتباطات ایجاد شده از طرف شبکه داخلی نمی توان کنترل داشت بهتر است برای هر سرور از پراکسی استفاده کرد تا محتویات بسته هایی که وارد شبکه می شوند کنترل شود.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۲

تکنیک زیر شبکه سازی در سال ۱۹۸۵ برای استفاده کار آمد تر از اختصاص آدرسهای IP برای شبکه های بزرگ مطرح شد. زیر شبکه سازی برای شبکه هایی با فضای آدرس بزرگ مانند کلاس A و کلاس B کاملاً خوب کار می کند، اما این قالب های آدرس شبکه خیلی عمومی بوده و به سرعت در حال پرشدن می باشند. همچنین می توان از زیر شبکه سازی برای آدرس های کلاس C استفاده کرد. اما یک آدرس کلاس C فقط ۲۵۴ میزبان را پشتیبانی می کند. در بسیاری از شبکه ها ممکن است تقسیم شبکه کلاس C عملی نباشد. مخصوصاً هنگامیکه لازم است تعداد میزبانهای پشتیبانی شده در هر زیر شبکه بیشتر از ۱۲۶ تا باشد.

آدرس های کلاس A و کلاس B به سرعت در حال استفاده و روبه اتمام می باشند. این پدیده که نشان دهنده اتمام فضای آدرس می باشد، پدیده^۱ ROADS خوانده می شود. با وجود اینکه آدرسهای کلاس A و کلاس B روبه اتمام می باشند، ولی هنوز تعداد کافی از آدرسهای کلاس C موجود می باشد. سازمانهای بزرگ که نیاز به پشتیبانی بیشتر از ۲۵۴ میزبان دارند مجبورند از چندین آدرسهای شبکه کلاس C استفاده کنند.

فرض کنید که یک سازمان برای پشتیبانی ۶۵۵۳۴ میزبان نیاز به یک آدرس کلاس B دارد. اگر این سازمان نتواند یک آدرس کلاس B به شبکه خود اختصاص دهد، می تواند این کار را با استفاده از چندین آدرس کلاس C انجام دهد. سوال این است که چند آدرس کلاس C برای پشتیبانی ۶۵۵۳۴ لازم است؟ جواب در حدود ۲۵۶ است. این ۲۵۶ آدرس کلاس C را می توان به عنوان یک بلوک اختصاص داد. به عنوان مثال مجموعه آدرس های کلاس C زیرقادر به تامین یک آدرس کلاس B می باشند:

202.100.0.0 تا 202.100.255.255

این تکنیک، ابر شبکه سازی نام دارد. در حقیقت ابر شبکه سازی این قابلیت را به مدیران شبکه می دهد که با استفاده از چند بلوک آدرس کلاس C، بتوان یک آدرس کلاس B بدست آورد.

مزیت این تنظیم بهره وری بهتر از فضای آدرس است. برای مثال اگر یک سازمان نیاز به شبکه ای با ۸۰۰۰ میزبان دارد بهتر است بجای انتساب یک آدرس کلاس B مجرد از یک بلوک ۳۲ تایی آدرس کلاس C استفاده کنند. یک شبکه کلاس B تا ۶۵۵۳۴ میزبان را پشتیبانی می کند اما در این مثال ۵۷۵۳۵ = ۶۵۵۳۴ - ۸۰۰۰ آدرس بکار نخواهد رفت. بنابراین با تخصیص بهینه تعداد آدرس های مورد نیاز با استفاده از روش ابر شبکه سازی، امکان استفاده بهینه از فضای آدرس های IP فراهم شده و از هر گونه اتلاف در فضای آدرس های IP جلوگیری می شود.

تکنیک ابر شبکه سازی برای استفاده ارائه دهندگان سرویس اینترنت (ISP^۲) برای تداوم اتصال اینترنت طراحی شده است. معمولاً فقط ISP ها اجازه دارند تا بلوک های بزرگ آدرس از آدرس ها کلاس C را فراهم کنند. ISP ها می توانند بلوک های کوچکتر این آدرس های کلاس C را به سازمانهای دیگر که می خواهند تعداد زیادی از کامپیوتر های خود را به اینترنت متصل کند اختصاص بدهند. بعلاوه بسیاری از سازمانهای تجاری که به آنها بلوک های آدرس کلاس C انتساب داده شده است از ابر شبکه سازی استفاده می کنند. ابر شبکه سازی اندازه جداول مسیریابی را نیز کاهش می دهد.

۷-۷-۱- مسیر یابی درون ناحیه ای بدون کلاس اینترنت (CIDR^۳)

اختصاص بلوک های آدرس کلاس C از اتمام از اتمام سریع آدرس های کلاس B جلوگیری می کند. اما از طرف دیگر، این اختصاص کلاس C به ذخیره شدن ورودی های اضافی در جدول مسیریابی مسیریابها نیاز دارد. همانطور که اشاره شد، برای تامین یک آدرس کلاس B نیاز به یک بلوک ۲۵۶ تایی از آدرس های کلاس C می باشد. بنابراین مسیریاب های شبکه،

^۱ Running Out of Address Space

^۲ Internet Service Provider

^۳ Classless Inter Domain Routing

شبکه های کامپیوتری (دکتر محمد حسن یغمایی مقدم - دانشگاه فردوسی مشهد)

در جدول مسیریابی خود به جای استفاده از یک رکورد، از ۲۵۶ رکورد استفاده می نمایند. این امر افزایشی را در تعداد ورودی های جدول مسیریابی با با ظرفیت ۲۵۶ نشان می دهد. به عنوان مثال اگر یک مسیر یاب که از آدرسهای کلاس B استفاده می کند ۲ مگابایت حافظه برای جدول مسیریابی خود نیاز داشته باشد، با عوض کردن این آدرسها با آدرسهای کلاس C به حافظه ای برابر با $2 \times 256 = 512$ مگابایت نیاز دارد.

برای رفع مشکل فوق، از تکنیک مسیریابی درون ناحیه ای بدون کلاس اینترنت (CIDR) استفاده می شود. تکنیک CIDR برای خلاصه کردن یک بلوک از آدرس های کلاس C به یک ورودی جدول مسیریابی مجرد استفاده می شود. این ترکیب منجر به کاهش تعداد ورودی های جداگانه جدول مسیریابی می شود. بلوک آدرس های کلاس C بوسیله یک ورودی جدول مسیریابی که به صورت زیر است ترکیب می شوند:

(پوشش ابر شبکه ، پایین ترین آدرس در بلوک)

پایین ترین آدرس در بلوک، آغاز بلوک آدرس است و پوشش ابر شبکه، تعداد آدرس های کلاس C در بلوک را مشخص می کند. پوشش ابر شبکه، برای پیشوند یکسان همه آدرس های کلاس C شامل ۱ است و برای قسمتهایی از آدرس های کلاس C که مقادیر متفاوت دارند صفر می باشد. به عنوان مثال، ورودی جدول مسیریابی CIDR زیر را در نظر بگیرید :

(200.1.160.0, 255.255.224.0)

نمایش بیتی 200.1.260.0 و 255.255.224.0 که پوشش CIDR است به صورت زیر است:

110010000 00000001 10100000 00000000

111111111 11111111 11100000 00000000

با بررسی CIDR ، قسمت مشترک در فضای آدرس های کلاس C به صورت زیر می باشد:

11001000 00000001 101

صفر ها در پوشش CIDR به قسمت متغیر بلوک آدرسهای بلوک آدرسهای کلاس C تعلق دارند. بنابراین بازه آدرسهای C بین آدرسهای کلاس C پایین و بالای زیر است:

11001000 00000001 10111111 11111111=200.1.191.255

نشانه گذاری دیگری که می توان برای بلوک های CIDR استفاده به شرح زیر است:

تعداد بیت های پیشوند مشترک / پایین ترین آدرس در بلوک

تعداد بیت های پیشوند مشترک، بیانگر تعداد ۱ های پوشش ابر شبکه است. بنابراین مثال های زیر نمایشهای هم ارز بلوک CIDR هستند:

(200.1.160.0 , 255.255.224.0)=200.1.160.0/19

۷-۸- آدرسهای IP نسخه ۶

همانطور که قبلا در این فصل اشاره شد، با بزرگ شدن اینترنت، فضای آدرس ۳۲ بیتی برای آدرس های IP نسخه ۴، رو به اتمام می باشد. هر اتصال شبکه IP در اینترنت نیاز به یک آدرس IP یکتا دارد. بعضی از تجهیزات شبکه، بیشتر از یک اتصال شبکه دارند که نتیجه آن مصرف سریع آدرسهای IP قابل انتساب است. تخمین زده شده است که آدرسهای IP ۳۲ بیتی، می توانند بیشتر از ۲/۱۰۰/۰۰ شبکه و چیزی حدود ۳۷۲۰ میلیون میزبان را مهیا سازد. با این وجود ، مدل اختصاصی فضای آدرس IP نسخه ۴ زیاد کارآمد نیست. حتی با وجود تکنیک های زیرشبکه سازی و ابرشبکه سازی که امکان استفاده بهینه از فضای آدرس های IP را فراهم می کند، همچنان مشکل کمبود آدرس های IP نسخه ۴ حس می گردد.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۱

برای رفع مشکل فوق، موسسه استانداردگذاری اینترنت (IETF¹) تصمیم به طراحی پروتکل اینترنت نسل بعدی گرفت که به عنوان IPng یا IP نسخه ۶ (IPv6) شناخته می شود. یکی از اهداف طراحی IPv6 استفاده از آدرسهای ۱۲۸ بیتی می باشد که چهار برابر اندازه بیتی آدرسهای IPv4 است. IPv6 نیز از مفهوم شماره های شبکه و شماره های میزبان استفاده می کند، اما این مفهوم را به چند سطح توسعه داده است. آدرس دهی سلسله مراتبی در IPv6 مسیریابی کارآمدتری را پشتیبانی می کند. آدرس IPv6 با استفاده ۳۲ بیت آدرسهای IPv4 در بیهیهای پائین مرتبه فضای آدرس و اضافه کردن یک پیشوند ثابت ۹۶ بیتی می تواند شامل یک آدرس IPv4 باشد. پیشوند ۹۶ بیتی شامل ۸ بیت صفر است که با ۱۶ بیت صفر یا ۱۶ بیت ۱ دنبال می شود. IPv6 با هدف امکان تعامل و ارتباط با سیستمهای IPv4 طراحی شده است که یک دوره همزیستی را برای دو سیستم IP سبب می شود. هدف این است که سیستمهای IPv4 جاری را عاقبت با سیستمهای IPv6 جایگزین کرد.

پروتکل IPv6 سیستمهای قابل حمل متحرک را پشتیبانی می کند. این خاصیت به کاربران کامپیوترهای قابل حمل و وسایل دیگر اجازه می دهد تا بدون انجام پیکره بندی دستی از هر جایی به شبکه متصل شوند. همچنین IPv6 قابلیت رمزنگاری را در لایه اینترنت پشتیبانی می کند و پشتیبانی بهتری را برای ترافیک بلادرنگ مهیا می سازد. ترافیک داده های بلادرنگ تضمینی را برای حداکثر تاخیر بسته های ارسالی در شبکه نیاز دارد.

چون آدرس های IPv6 ۱۲۸ بیت طول دارند، استفاده از نشانه گذاری دهدهی نقطه دار یک نشانه گذاری مناسب برای نوشتن آدرس های IPv6 نیست. اگر برای نوشتن آدرسهای IPv6 از نشانه گذاری دهدهی نقطه دار استفاده شود، می بایست یک رشته را شامل ۱۶ عدد دهدهی که با نقطه از هم جدا شده اند نوشت. طراحان IPv6 استفاده از نشانه گذاری شانزده شانزدهی دو نقطه دار را برای نوشتن الگوی بیتی انتخاب کردند. هریک از مقادیر شانزده شانزدهی به عنوان ۱۶ بیت نوشته شده اند که بوسیله کاراکتر دو نقطه (:) از هم جدا شده اند. به عنوان مثال یک آدرس IPv6 می تواند به صورت زیر نوشته شود:

5800:00C3:E3C3:F1AA:48E3:D923:D495:AAFE

با استفاده از نشانه گذاری شانزده شانزدهی دو نقطه دار ارقام و کاراکتر های جدا سازی کمتری مورد نیاز است. دوتکنیک مختلف برای کاهش نمایش آدرس های IPv6 ارائه شده است. تکنیک اول این است که می توان صفرهای موجود در آدرس را حذف نمود. به عنوان مثال، آدرس IPv6 زیر را در نظر بگیرید:

48A6:0000:0000:0000:0000:0DA3:003F:0001

با پرش از صفر های اضافی این آدرس را می توانید به صورت آدرس ساده شده زیر بنویسید:

48A6:0:0:0:0:DA3:3F:1

تکنیک دوم از فشرده سازی صفر استفاده می کند. به این صورت که یک رشته از صفرهای تکراری در آدرس های IPv6 را می توان حذف نمود و به جای آن "::" جایگزین کرد. بنابراین آدرس IPv6 پیش را می توان به صورت زیر نوشت:

48A6::DA3:3F:1

نمایش IPv6 آدرس 170.1.1.1 IPv4 به صورت زیر می باشد:

0:0:0:0:0:AA01:101

همچنین می توان این آدرس را به صورت زیر نیز نمایش داد:

::AA01:101

¹ Internet Engineering Task Force

پرسش های فصل

۱. دو مزیت اصلی معماری TCP/IP را شرح دهید.
۲. رابطه بین تعداد اتصال های یک میزبان به شبکه با تعداد آدرسهای IP مورد نیاز آن میزبان را توضیح دهید.
۳. مستقل بودن آدرس IP از آدرس فیزیکی چه مزایا و چه معایبی به دنبال خواهد داشت.
۴. مزیت استفاده از یک مقدار آدرس منطقی برای آدرسهای IP چیست؟
۵. کاربرد هریک از کلاس های آدرس IP را توصیف نمایید.
۶. مفهوم آدرس دهی تک پخشی، چند پخشی و همه پخشی را توضیح دهید.
۷. برای عملیات تک پخشی، چند پخشی و همه پخشی در مدل آدرس دهی IP چه تمهیداتی دیده شده است؟
۸. مزایا و عیب های تقسیم آدرس IP به یک netid و یک hostid چیست ؟
۹. تفاوت بین یک آدرس همه پخشی مستقیم و یک آدرس همه پخشی محدود را با ذکر مثال مناسب توضیح دهید.
۱۰. یک آدرس برگشت حلقه نرم افزاری چیست ؟ قالب آن را توصیف کنید . چند نمایش آدرس برگشت حلقه وجود دارد ؟
۱۱. کاربردهای آدرس IP 0.0.0.0 و 255.255.255.255 را بنویسید.
۱۲. یک شبکه کلاس C با آدرس 194.34.56.0 داده شده است چند میزبان برای این شبکه امکان دارد ؟ برای آدرس کلاس B 166.23.0.0 چه طور؟
۱۳. مفهوم و کاربرد آدرس های خصوصی را نوشته و توضیح دهید که تحت چه شرایطی یک سازمان خواستار استفاده از آدرس های خصوصی است ؟
۱۴. در یک شبکه اینترنت ، به چه نوع میزبان هایی می توان یک آدرس IP خصوصی انتساب داد ؟ آیا می توان یک آدرس IP خصوصی به یک میزبان یا مسیریابی که برای دنیای خارج قابل رویت است، اختصاص داد؟
۱۵. نوع کلاس IP آدرس های زیر را بدست آورید:

23.1.3.5	198.34.54.23	233.12.3.4
45.2.3.67	178.11.23.5	254.12.34.5
۱۶. مفهوم و کاربرد زیر شبکه سازی را با ذکر یک مثال مناسب توصیف نمایید.
۱۷. مزایای زیر شبکه سازی را بنویسید.
۱۸. عملکرد پروتکل NAT را با ذکر یک مثال توضیح دهید.
۱۹. مفهوم و کاربرد ابر شبکه سازی را با ذکر یک مثال مناسب توصیف نمایید.
۲۰. پدیده ROADS را توضیح دهید.

فصل هشتم

پروتکل های لایه شبکه در اینترنت

لایه شبکه در معماری TCP/IP شامل چند پروتکل مهم می باشد. در این فصل به بررسی پروتکل های این لایه شامل : پروتکل ARP¹، پروتکل RARP² و پروتکل IP می پردازیم.

۸-۱- پروتکل ARP

آدرس های IP به صورت منطقی تعریف شده و از آن برای ایجاد شبکه های مجازی استفاده می شود. همانطور که در فصل قبل گفته شد، این آدرس ها دارای طول ۳۲ بیت می باشند. باید توجه داشت که انتقال بسته های IP مستلزم استفاده از لایه دوم می باشد. به عبارت دیگر از آنجاییکه پروتکل IP در لایه سوم قرار دارد، طبق روال ارسال داده در معماری لایه ای شبکه، انتقال بسته های لایه سوم مستلزم استفاده از امکانات لایه دوم می باشد. بنابراین از آنجاییکه بسته های IP در دل قابهای لایه دوم مثل اترنت و یا شبکه حلقه نشانه قرار می گیرند، برای ارسال آنها به مقصد نیاز به دانستن آدرس سخت افزاری کامپیوتر مقصد می باشد. به عبارت دیگر از آنجاییکه در کامپیوتر مقصد، ابتدا لایه دوم قاب را از شبکه برداشته و بعد به لایه سوم که پروتکل IP است تحویل می دهد، لذا دانستن تنها آدرس IP مقصد کفایت نکرده و باید آدرس سخت افزاری مربوط به لایه دوم کامپیوتر مقصد نیز داشته باشیم. بدین منظور از پروتکل خاصی به نام پروتکل ARP استفاده می شود. در معماری TCP/IP از پروتکل DNS^۳ برای نگاشت بین آدرس های اسمی که در برنامه های کاربردی استفاده می شوند و آدرس های IP که در سطح لایه سوم استفاده می شود، بهره گرفته می شود. برخلاف پروتکل فوق، از پروتکل ARP برای استخراج آدرس لایه سخت افزاری (که به آن آدرس MAC^۴ نیز گفته می شود) از آدرس IP استفاده می شود. سوالی که اینجا مطرح می شود این است که چگونه می توان با داشتن آدرس IP مقصد، آدرس سخت افزاری مربوط به لایه دوم آن را بدست آورد؟

یکی از ساده ترین راه حل ها این است که هر کامپیوتر شبکه، دارای جدولی باشد که در آن جدول آدرس IP و آدرس MAC همه کامپیوتر های شبکه نوشته شده است. هرگاه کامپیوتری نیاز به آدرس MAC کامپیوتر دیگری داشته باشد، با فرض آنکه آدرس IP آن را می داند، به این جدول مراجعه کرده و آدرس MAC آن را بدست می آورد. این راه حل گرچه ساده به نظر می رسد، ولی مشکل اصلی آن این است که در صورت تغییر آدرس MAC یک ایستگاه (به عنوان مثال در هنگامی که کارت شبکه یک کامپیوتر عوض شود) باید رکورد مربوط به آن کامپیوتر جداول مربوط به سایر کامپیوتر ها نیز عوض شود که این کار نیاز به صرف هزینه و وقت زیاد است.

¹ Address Resolution Protocol

² Reverse Address Resolution Protocol

³ Domain Name System

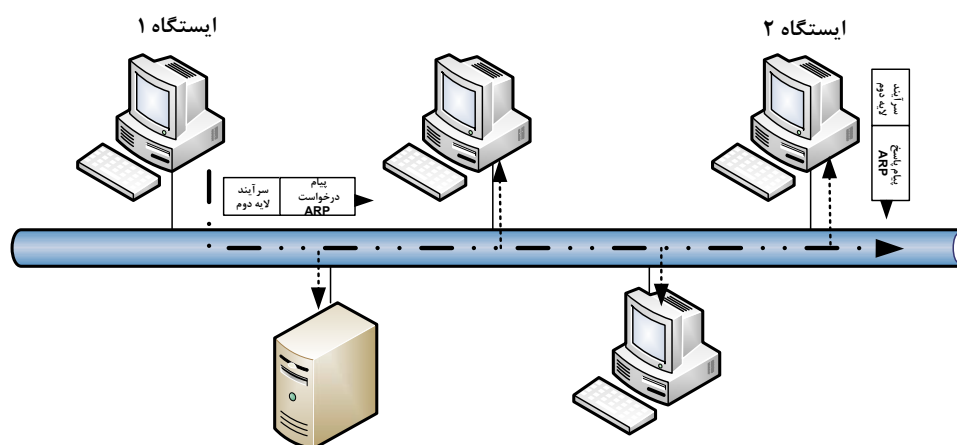
⁴ Medium Access Control

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

این روش پیکره بندی دستی TCP/IP برای تعریف انطباق بین آدرس های IP و آدرس های MAC در گذشته استفاده می گردید. در سیستم های امروزه مدل انعطاف پذیر تری برای مشخص سازی پویای آدرس MAC با دانستن آدرس IP میزبان مورد نیاز است. این مکانیزم پویا به عنوان یک پروتکل جدا تحت عنوان پروتکل ARP پیاده سازی شده است.

۸-۱-۱- نحوه عملکرد پروتکل ARP

شکل (۸-۱) یک نمای ساده از چگونگی عملکرد پروتکل ARP را نشان می دهد. در این شکل فرض می شود که ایستگاه ۱ می خواهد داده ای را برای ایستگاه ۲ ارسال دارد. بدین منظور باید ابتدا آدرس MAC ایستگاه ۲ را بدست آورد.



شکل (۸-۱): عملکرد ARP

ایستگاه ۱ یک قاب همه پخشی MAC را که پیام درخواست ARP نامیده می شود، به شبکه می فرستد. پیام درخواست ARP شامل آدرس IP و آدرس MAC میزبان فرستنده یعنی ایستگاه ۱ و آدرس IP و آدرس MAC مقصد یعنی ایستگاه ۲ است. پیام درخواست ARP شامل یک فیلد خالی برای آدرس سخت افزاری مقصد یعنی ایستگاه ۱ است. همه نود ها در شبکه فیزیکی پیام درخواست همه پخشی ARP را دریافت می کنند. سایر نود های شبکه قاب همه پخشی را دریافت می کنند، آدرس IP خود را با آدرس IP موجود در قاب درخواست ARP مقایسه می نمایند. تنها میزبانی که همان آدرس IP خواسته شده در پیام درخواست ARP را دارد، به درخواست فوق پاسخ می دهد. اگر ایستگاه ۲ در شبکه موجود باشد، آدرس سخت افزاری خود را در فیلد خاصی در پیام فوق قرار داده و به آن پاسخ می دهد. به پیام ارسالی، پیام پاسخ ARP می گویند. بعد از آنکه ایستگاه ۱ پاسخ ARP را دریافت کرد، در یک جدول خاص به نام جدول حافظه پنهان ARP که در حافظه اصلی خود نگهداری می کند، زوج آدرس IP و سخت افزاری ایستگاه ۲ را قرار می دهد. در صورتیکه در آینده نیاز به ارسال مجدد به ایستگاه ۲ باشد، ابتدا ایستگاه ۱ محتوای این جدول را جستجو کرده و در صورت نیافتن آدرس سخت افزاری ایستگاه ۲ روال درخواست ARP را انجام می دهد. محتویات جدول فوق، یک زمان زندگی خاصی دارند که در اکثر پیاده سازی های TCP/IP مقدار آن برابر با ۱۵ دقیقه می باشد.

بعد از اینکه مهلت زمانی فوق برای یک میزبان خاص تمام شد، قاب درخواست ARP مجدداً برای کشف آدرس سخت افزاری میزبان فرستاده می شود.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

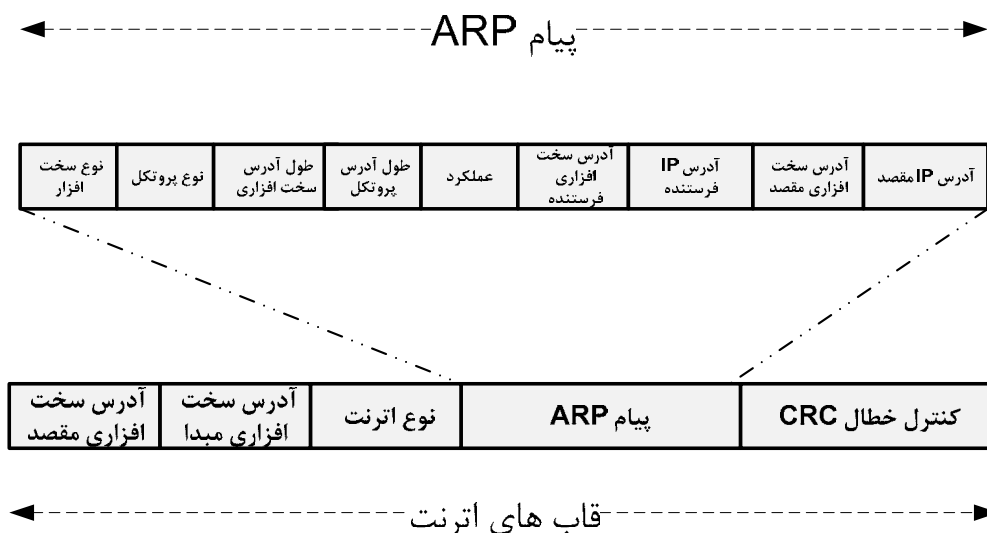
در هنگام ارسال پیام درخواست ARP از آنجاییکه آدرس سخت افزاری مقصد هنوز معلوم نیست، بنابراین درخواست فوق در لایه دوم به صورت همه پخش ارسال شده طوری که همه میزبان های شبکه بتوانند آنرا دریافت نمایند. پاسخ ARP که توسط نود مقصد فرستاده می شود یک قاب همه پخش نیست، زیرا نود گیرنده درخواست ARP، آدرس سخت افزاری فرستنده پیام فوق را در فیلد خاصی در پیام فوق بدست آورده و در هنگام پاسخ دهی به درخواست فوق، قاب پاسخ را به صورت تک پخش ارسال می دارد. فرض عملکرد پروتکل ARP این است که شبکه فیزیکی زیرین توانایی همه پخش را پشتیبانی می کند که در مورد شبکه های محلی مانند اترنت، شبکه حلقوی، FDDI، ARCnet، و غیره صدق می کند.

۸-۱-۲- ساختار بسته های ARP

شکل (۸-۲) قالب بسته های درخواست ARP و پاسخ ARP را نشان می دهد. پروتکل ARP در آغاز برای اترنت DIX طراحی شده بود. بعداً برای شبکه های محلی دیگر مانند شبکه های محلی IEEE802 توسعه داده شد. پیام های ARP در قالب قاب های لایه پیوند داده بسته بندی می شود. شکل (۸-۳) مثالی از یک بسته ARP را نشان میدهد که در یک قاب اترنت جاسازی شده است.



شکل (۸-۲): قالب بسته ARP



شکل (۸-۳): بسته ARP بسته بندی شده در یک قاب اترنت

بانگاهی به شکل (۸-۲) درمی یابیم که فیلد نوع سخت افزار، اولین فیلد در بسته ARP است. این فیلد که دوبایت طول دارد (بایت ۸ بیتی) نشان دهنده نوع سخت افزار شبکه است. مقدار ۱ در فیلد نوع سخت افزار نشان دهنده یک شبکه اترنت

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

است. جدول (۸-۱) کدهای انتساب داده شده را برای مقادیر نوع سخت افزار در بسته ARP برای شبکه های مختلف نشان می دهد.

جدول (۸-۱): مقادیر نوع سخت افزار ARP

فیلد نوع سخت افزار توصیف	ARP
اترنت ۱۰ مگابیت بر ثانیه	۰
اترنت آزمایشی ۳ مگابیت بر ثانیه	۲
حلقه نشانه	۴
Chaos Net	۵
شبکه های IEEE 802	۶
ARCNET	۷
SMDS	۱۴
Frame Relay	۱۵
ATM	۲۱ و ۱۹ و ۱۶
HDLC	۱۷
Fiber Channel	۱۸

فیلد نوع پروتکل، نشان دهنده نوع پروتکل لایه بالاتر است. این فیلد ۲ بایت طول دارد. در مورد شبکه های TCP/IP آدرس پروتکل، آدرس IP است که برای این آدرس سخت افزاری مورد نیاز است. مقدار نوع پروتکل، نوع پروتکل لایه سوم را مشخص می کند. برای پروتکل IP مقدار عدد مبنای شانزده ۸۰۰ برای فیلد نوع پروتکل استفاده می شود. فیلد طول آدرس سخت افزاری بر حسب بایت است. این فیلد ۱ بایت طول دارد. مقدار فیلد فوق بوسیله مقدار فیلد نوع سخت افزار کنترل می شود. اگر نوع سخت افزار ۱ باشد، یک شبکه اترنت را نشان می دهد که آدرس سخت افزاری آن ۸ بایت است. بنا بر این مقدار فیلد طول آدرس سخت افزاری برای شبکه های اترنت ۸ است.

فیلد طول آدرس پروتکل، طول آدرس پروتکل مورد استفاده در لایه سوم را بر حسب بایت است. این فیلد ۱ بایت طول دارد. فیلد فوق بوسیله مقدار فیلد نوع پروتکل کنترل می شود. اگر نوع پروتکل ۸۰۰ (در مبنای شانزده) باشد، پروتکل IP را مشخص می کند که آدرس IP آن ۴ بایت است. بنابراین مقدار فیلد طول آدرس پروتکل برای شبکه های IP ۴ است. فیلد عملکرد ۲ بایت طول دارد و نشان دهنده این است که آیا بسته فعلی یک بسته درخواست ARP و یا یک بسته پاسخ ARP است. البته به غیر از این دوبرسته، این فیلد می تواند به عملکردهای دیگری اشاره داشته باشد. جدول (۸-۲) مقادیر ممکن در فیلد عملکرد را نشان می دهد، بعضی از مقادیر جدول (۸-۲) برای پروتکل های آزمایشی پیشنهادی هستند و ممکن است هرگز آنها را در شبکه های موجود نبینید.

جدول (۸-۲): مقادیر عملکرد برای بسته ARP

فیلد نوع عملکرد	توصیف
۱	پیام درخواست ARP
۲	پیام پاسخ ARP
۳	پیام درخواست RARP
۴	پیام پاسخ RARP
۵	پیام درخواست DRARP

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

پیام پاسخ DRARP	۶
پیام خطای DRARP	۷
پیام درخواست InARP	۸
پیام پاسخ InARP	۹
پیام ARP NAK	۱۰

فیلد آدرس سخت افزاری فرستنده، نشان دهنده آدرس سخت افزاری نود فرستنده درخواست ARP است. فرستنده، آدرس سخت افزاری خود را با خواندن آن از کارت شبکه بدست آورده و این فیلد را پر می کند. آدرس IP فرستنده نشان دهنده آدرس IP نود فرستنده درخواست ARP است. فرستنده، آدرس IP خود را با خواندن از یک فایل پیکره بندی یا خواندن حافظه پنهان خود که شامل اطلاعات پیکره بندی شبکه است بدست می آورد و در فیلد متناظر قرار می دهد.

فیلد آدرس سخت افزاری مقصد، آدرس سخت افزاری نود مقصد را نشان می دهد. این مقدار برای فرستنده پیام درخواست ARP شناخته شده نیست. این مقدار، مقداری است که فرستنده درخواست ARP سعی به مشخص کردن آن می کند. این فیلد معمولاً بیت‌های ۱ یا بیت‌های صفر دارد. آدرس سخت افزاری مقصد می تواند آدرس همه پخش سخت افزار باشد که آن را برای بعضی از جنبه های پیاده سازی مناسب می سازد.

فیلد آدرس IP مقصد در بسته درخواست ARP دربرگیرنده آدرس IP نودی است که قرار است آدرس سخت افزاری آن مشخص شود. این مقدار به وسیله فرستنده درخواست ARP فراهم می شود. ساختار بسته پاسخ ARP همانند قالب بسته درخواست ARP می باشد اما مقدار فیلد عملکرد آن ۲ است که نشان دهنده یک پاسخ ARP است.

استفاده از قالب یکسان برای درخواست ها و پاسخ های ARP، باعث می شود که از بافر بسته درخواست ARP دوباره برای پاسخ ARP استفاده شود. پاسخ ARP همان طول پیام درخواست ARP را دارد و چندین فیلد یکسان هستند. هنگامی که یک نود IP یک پاسخ ARP می فرستد، آدرس سخت افزاری خود را در فیلد آدرس سخت افزاری فرستنده قرار می دهد.

فیلد های بسته پاسخ ARP به شرح زیر می باشند :

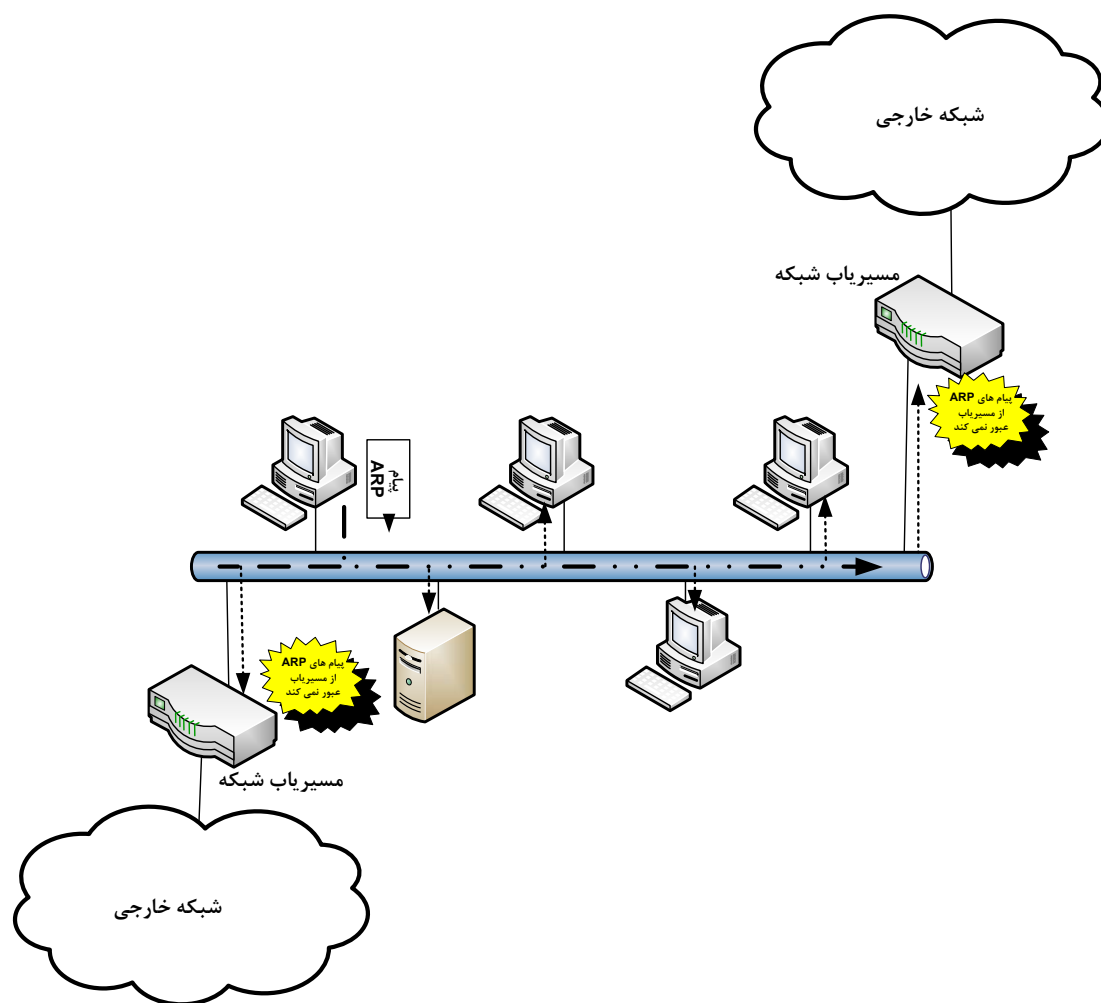
- آدرس سخت افزاری فرستنده: شامل آدرس سخت افزاری نود مقصد (دلیل اصلی عملکرد ARP)
- آدرس IP فرستنده : شامل آدرس IP نود مقصد.
- آدرس سخت افزاری مقصد : شامل آدرس سخت افزاری فرستنده درخواست ARP است. نود مقصد آن را با بررسی فیلد آدرس سخت افزاری فرستنده در پیام درخواست ARP بدست می آورد.
- آدرس IP مقصد : شامل آدرس IP فرستنده در پیام درخواست ARP است. نود مقصد آن را با بررسی فیلد آدرس IP فرستنده در درخواست ARP بدست می آورد.

هنگامی که کامپیوتر مقصد در یک شبکه راه دور قرار داشته باشد، عملکرد پروتکل متفاوت می باشد. اگر مقصد در یک شبکه دور باشد (یک شبکه دیگر به جای شبکه محلی) ، فرستنده باید آدرس سخت افزاری درگاه مسیریابی را که بسته IP باید به آن ارسال شود را پیدا کند.

در مورد شبکه های همه پخش از پروتکل ARP برای یافتن آدرس سخت افزاری نود مقصد استفاده می شود. پروتکل ARP به عنوان بخشی از ماژول IP در شبکه هایی که نیاز به تجزیه آدرس دارند، مانند شبکه های محلی همه پخش (اترنت ، شبکه حلقوی و غیره) پیاده سازی می شود. مطابق شکل (۸-۴)، پروتکل ARP توسط پروتکل IP بسته بندی نمی شود

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

بلکه مستقیماً توسط پروتکل لایه پیوند داده بسته بندی می گردد. این بدان معنی است که پیام های پروتکل ARP را نمی توان مسیریابی کرد، یعنی نمی تواند از مرز یک مسیر یاب عبور کند. قبل از ارسال پیام درخواست ARP، پروتکل ARP سعی می کند تا آدرس مقصد را در حافظه پنهان محلی خود پیدا کند. جدول حافظه پنهان ARP که ساختار آن در شکل (۸-۵) نشان داده شده است، جفت ورودی های آدرس های IP و آدرس سخت افزاری متناظر را نگه می دارد. اگر آدرس IP مقصد در جدول حافظه پنهان ARP پیدا شود، آدرس سخت افزاری متناظر با آدرس IP مقصد را جستجو نموده و آن را به ماژول ARP برمی گرداند.



شکل (۸-۴): محدودیت ARP در بخش شبکه محلی

در صورتیکه آدرس سخت افزاری کامپیوتر مقصد در جدول مربوطه پیدا نشود، ماژول ARP یک قاب لایه پیوند داده تولید می کند که شامل درخواست ARP برای کشف آدرس سخت افزاری نود مقصد است. درخواست ARP در لایه پیوند داده به همه نود ها در شبکه محلی پخش می شود. همانطور که قبلاً ذکر شد، پاسخ ها و درخواست های ARP به بخش شبکه محلی محدود شده و از مرز مسیریاب عبور نمی کنند.

نوع پروتکل (IP)	آدرس پروتکل (آدرس	آدرس سخت افزاری	شماره واسط	برچسب زمانی
های IP)				

شکل (۸-۵): جدول حافظه پنهان ARP

هنگامی که یک درخواست ARP دریافت می شود، لایه پیوند داده در نود مقصد بسته را به ماژول مربوط به ARP می دهد. قاب درخواست ARP در سطح لایه پیوند داده همه پخش می شود، بنابراین همه نود ها در شبکه محلی آن را دریافت می کنند با این وجود فقط نودی که آدرس IP آن مطابق با آدرس IP مقصد است با یک پاسخ ARP جواب می دهد. مراحل انجام شده توسط ماژول ARP در نود گیرنده به شرح زیر می باشد.

۱. آیا نوع سخت افزار را در فیلد نوع سخت افزار بسته درخواست ARP می شناسم ؟
۲. اگر جواب مرحله ۱ بلی است ، به طور اختیاری طول آدرس های سخت افزاری را در بسته درخواست ARP بررسی کن.
۳. آیا چگونگی پردازش پروتکل را در فیلد نوع پروتکل در بسته درخواست ARP می دانم؟
۴. اگر جواب مرحله ۳ بلی است، به طور اختیاری طول آدرس پروتکل را در بسته درخواست ARP بررسی کن .
۵. پرچم ادغام را برای کنترل پردازش ARP در مراحل بعدی به False مقدار دهی کن.
۶. اگر جفت "<نوع پروتکل ، آدرس پروتکل فرستنده >" هم اکنون در جدول ترجمه نود موجود است، فیلد آدرس سخت افزاری فرستنده را با ورودی اطلاعات جدید در بسته به روز برسان و پرچم ادغام را true کن.
۷. آیا آدرس پروتکلی مقصد هستم ؟ (به این معنی که آدرس IP من همان است که در فیلد آدرس IP مقصد آمده است؟)
۸. اگر جواب مرحله ۷ بلی است سپس با تعیین کردن این که آیا پرچم ادغام false است ادامه بده . اگر پرچم ادغام false است، ۳ تایی (نوع پروتکل ، آدرس پروتکل فرستنده ، آدرس سخت افزاری فرستنده) را به جدول ترجمه اضافه کن .
۹. آیا مقدار فیلد عملکرد، نشان دهنده یک درخواست است ؟
۱۰. اگر جواب مرحله ۹ بلی است، با عوض کردن فیلد های پروتکل و سخت افزار، قرار دادن آدرس های پروتکل و سخت افزار محلی در فیلد های فرستنده ادامه بده. فیلد عملکرد را به پاسخ ARP مقدار دهی کن. بسته را به آدرس سخت افزار مقصد (جدید) در همان سخت افزار که درخواست دریافت شده بفرست.

در الگوریتم فوق، قبل از این که فیلد عملکرد در مرحله ۶ بررسی شود ۳ تایی "> نوع پروتکل ، پروتکل فرستنده آدرس سخت افزاری فرستنده >" به جدول حافظه پنهان ARP ادغام می شود. این مرحله فقط زمانی رخ می دهد که یک نود یک ورودی برای آدرس IP فرستنده در جدول حافظه پنهان ARP دارد.

۸-۱-۳- نظارت بر شبکه با کمک پروتکل ARP

از پروتکل ARP می توان به عنوان یک وسیله نظارتی برای بدست آوردن اطلاعات لازم درباره فعالیت پروتکل های سطح بالا استفاده کرد. به عنوان مثال با بررسی فیلد نوع پروتکل موجود در قاب های ARP می توان اطلاعات مفیدی درمورد پروتکل های لایه سوم موجود در شبکه بدست آورد. هنگامی که سیستم نظارتی شبکه، یک پیام ARP را دریافت می نماید، با بررسی آن می تواند به اطلاعات مفیدی نظیر: نوع پروتکل، آدرس IP فرستنده و گیرنده و آدرسهای سخت افزاری آنها دستیابی داشته باشد.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

علاوه بر آن می تواند طول آدرس سخت افزاری و آدرس پروتکل را از فیلد های مربوطه موجود در بسته ARP مشخص کند. باید توجه نمود که در خواست های ARP در سطح پیوند داده همه پخشی می شوند و یک سیستم ناظر همه در خواست های ARP را دریافت می کند. اگر فیلد عملکرد یک بسته ARP نشان دهنده درخواست ARP باشد و آدرس پروتکل مقصد با آدرس پروتکل ایستگاه ناظر مطابقت کند، ایستگاه ناظر نیز یک پاسخ ARP را مانند هر نود مقصد دیگر می فرستد.

۸-۱-۴- مهلت های زمانی^۱ در جدول حافظه پنهان ARP

محتویات جداول حافظه پنهان ARP اغلب دارای یک مکانیزم مهلت زمانی می باشند. ورودی های جدول حافظه پنهان ARP ممکن است همراه با خود مقادیر برچسب زمانی داشته باشند. اگر یک نود در شبکه جابجا شود، معمولا قبل از نقل مکان خاموش می شود. خاموش کردن یک نود، جدول حافظه پنهان ARP آن را پاک می کند. بنابراین ورودی های قدیمی باعث اشتباه نمی شوند، سایر نود های شبکه عموما آگاه نیستند که یک نود خاص نقل مکان کرده یا خاموش شده است.

اگر نود به مکانی در همان بخش شبکه نقل مکان کرده باشد، اطلاعات حافظه پنهان ARP درباره نود نقل مکان کرده هنوز معتبر هستند، زیرا در این حالت آدرس IP و آدرس سخت افزاری نود نقل مکان کرده تغییر نمی کند. اگر نود خاموش شود سایر نود ها توانایی دسترسی به این نود را ندارند. سایر نود ها اطلاعات حافظه پنهان ARP خود را برای دستیابی به این نود استفاده می کنند اما قادر به ایجاد اتصال نیستند. اگر نود به مکانی در بخش متفاوتی از شبکه نقل مکان کرده باشد، در این صورت پشت یک مرز مسیریاب است. در این حالت آدرس IP نود نقل مکان کرده حتی اگر آدرس سخت افزاری همان باقی بماند، باید تغییر کند. از آنجاییکه انتقال پیام های ARP از مرز یک مسیریاب امکان پذیر نمی باشد، بنابراین فرض می شود که نود جدید خاموش شده یا غیر قابل دسترسی است.

همچنین برچسب های زمانی هنگامی که درخواست های ARP از نودی که ورودی آن در جدول حافظه پنهان ARP موجود است، دریافت می شود، به روز رسانی می شوند. چنانچه هیچ بسته ای از یک نود در یک مدت زمان معین دریافت نشود، در این صورت ورودی مربوط به آن رکورد در جدول ARP پنهان حذف می شود. مدت زمان معین فوق برابر با مقدار مهلت زمانی ARP می باشد.

خیلی از پیاده سازی ها اجازه قراردادن ورودی های دستی را در جدول حافظه پنهان ARP می دهند. از آنجاییکه عملیات پویای ARP، آدرس IP و سخت افزاری مرتبط را مشخص می کند، معمولا نیازی به قرار دادن ورودی های دستی در جدول ARP نیست. ورودی های دستی ARP مهلت زمانی ندارند و می توانند برای رفع مشکلات با ورودی های نادرست در جدول ARP به خاطر مشکلات آدرس IP تکراری یا عملکرد بد نرم افزار استفاده شوند.

۸-۱-۵- ARP در شبکه های پل بندی شده

اگر در یک شبکه TCP/IP مشکل فیزیکی ایجاد شود، ترمیم در لایه های پائین انجام می گردد. مازول ARP سعی می کند در لایه های پائین تر به وسیله همه پخشی یک درخواست ARP اتصال را ترمیم کند. با این وجود هنگامی که چندین نود شروع به ارسال همه پخشی در خواست ARP کنند، ازدحام به وجود می آید. این امر هنگامی که میزبان مرکزی به خاطر نقص اتصال از کار افتاده است و اتصال فیزیکی آن به شبکه محلی قطع شده است، می تواند اتفاق بیفتد. به عنوان مثال، اگر ۱۵۰۰ ایستگاه به یک میزبان مرکزی در شبکه متصل باشند و اتصال شبکه به میزبان فوق از بین برود، همه

¹ Timeout

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

۱۵۰۰ ایستگاه فوق به طور همزمان شروع به ارسال قاب های همه پخشی ARP می کنند. در بعضی از سیستم ها، درخواست ARP در هر ثانیه فرستاده می شود. با ۵۰۰ ایستگاه فرستنده همه پخشی ARP، در هر ثانیه ۵۰۰ بسته همه پخشی فرستاده می شود. این ترافیک همه پخشی مقدار مهمی از ترافیک شبکه ایجاد می کند که به قابلیت دسترسی به سایر نود های شبکه اثر منفی می گذارد. ترافیک همه پخشی حتی نود هایی را که در حال حاضر به شبکه دستیابی ندارند، کند می کند. به این دلیل که کارت شبکه و نرم افزار مربوطه باید هر بسته همه پخشی را بررسی و پردازش نمایند. ماژول ARP نیز برای هر درخواست همه پخشی اجرا می شود. پردازش حتی ۵۰ درخواست ARP در هر ثانیه مقدار زیادی از بار پردازشی را متحمل نود نموده و باعث کند کردن آن نود می شود. در نتیجه همه نود های شبکه به نظر کند میشوند. همه پخشی های تکراری ARP، در شبکه هایی که بوسیله پل از یکدیگر جدا شده اند، وضعیت را بدتر نیز می نماید. در این حالت، درخواست ها و جواب های ARP باید از طریق این پل ها ارسال شوند. تکثیر ترافیک همه پخشی از وسط پل ها می تواند یک اثر افزایشی داشته باشد و ترافیک شبکه را بیشتر افزایش دهد.

۸-۱-۶- آدرس های تکراری و ARP

در یک شبکه باید آدرس های IP یکتا باشند. چون عنصر بشری در انتساب آدرس های IP وارد می شود، سهوا امکان انتساب نود های شبکه به آدرس های IP یکسان وجود دارد که باعث وقوع اشتباه و بی ثباتی در شبکه می شود. برای درک بهتر مشکل آدرس های IP تکراری، دو سناریوی مختلف زیر بررسی می شوند:

- آدرس های IP تکراری در سرویس گیرنده های TCP/IP
- آدرس های IP تکراری در سرویس دهنده های TCP/IP

ابتدا به بررسی مشکل آدرس های IP تکراری در سرویس گیرنده های TCP/IP می پردازیم. بدین منظور به ذکر یک مثال می پردازیم. به عنوان مثال شبکه ای را در نظر بگیرید که دو سرویس گیرنده TCP/IP به نامهای ایستگاه ۱ و ایستگاه ۲ در آن به یک سرویس دهنده مرکزی TCP/IP به آدرس IP 144.19.74.102 دسترسی دارند. آدرس سخت افزاری سرویس دهنده A است. فرض کنید که ایستگاههای ۱ و ۲ آدرس IP یکسان 144.19.74.1 را استفاده می کنند. آدرس های سخت افزاری آنها به ترتیب B و C است. ایستگاه ۱، یک جلسه FTP را با سرویس دهنده TCP/IP برقرار می کند. قبل از آغاز جلسه FTP، ایستگاه ۱ باید برای بدست آوردن آدرس سخت افزاری سرویس دهنده، یک درخواست همه پخشی ARP برای آدرس سخت افزاری سرویس دهنده TCP/IP در شبکه منتشر کند. با دریافت درخواست ARP، سرویس دهنده TCP/IP یک ورودی را برای فرستنده درخواست ARP (ایستگاه ۱) در جدول حافظه پنهان ARP خود اضافه می کند و یک پاسخ ARP را به فرستنده ارسال می نماید. با دریافت پاسخ ARP، ایستگاه ۱ یک ورودی را برای سرویس دهنده TCP/IP در جدول حافظه پنهان محلی خود اضافه می کند. در این لحظه جدول حافظه پنهان ARP برای سرویس دهنده TCP/IP به شرح زیر است:

آدرس سخت افزاری	آدرس IP
B	144.19.74.1

همچنین جدول حافظه پنهان ARP برای ایستگاه ۱ به شرح زیر است :

آدرس سخت افزاری	آدرس IP

A

144.19.74.102

حال فرض کنید که ایستگاه ۲ تلاش به برقراری یک جلسه TCP/IP با همان سرویس دهنده TCP/IP می کند. قبل از ایجاد اتصال، ایستگاه ۲ باید آدرس سخت افزاری سرویس دهنده TCP/IP را بدست آورد. بدینمنظور ایستگاه ۲ با ارسال یک درخواست ARP این امر را انجام دهد. با دریافت درخواست ARP، سرویس دهنده TCP/IP می خواهد یک ورودی برای فرستنده درخواست ARP (ایستگاه ۲) در جدول حافظه پنهان ARP خود اضافه کند و یک پاسخ ARP را به فرستنده ارسال کند. سرویس دهنده TCP/IP در می یابد که از قبل یک ورودی برای 144.19.74.1 در جدول حافظه پنهان ARP خود دارد. با توجه به توصیه نامه RFC826 درباره پروتکل ARP، سرویس دهنده TCP/IP باید ورودی موجود را با ورودی جدید جایگزین کند.

بیشتر پیاده سازی های TCP/IP این جایگزینی را بی صدا و بدون ارسال پیام اخطار درباره امکان ایجاد مشکل آدرس IP تکراری، انجام می دهند. بعضی از پیاده سازی های TCP/IP یک پیام اخطار درباره امکان مشکل آدرس IP تکراری ارسال می دارند. سرویس دهنده TCP/IP به درخواست ARP از ایستگاه ۲ جواب می دهد. با دریافت پاسخ ARP، ایستگاه ۲ یک ورودی را برای سرویس دهنده TCP/IP در جدول حافظه پنهان ARP محلی خود اضافه می کند. در این لحظه جدول حافظه پنهان ARP برای سرویس دهنده TCP/IP به شرح زیر است :

آدرس سخت افزاری

آدرس IP

C

144.19.74.1

جدول حافظه پنهان ARP برای ایستگاه ۲ به شرح زیر است :

آدرس سخت افزاری

آدرس IP

A

144.19.74.102

هنگامی که سرویس دهنده TCP/IP به ایستگاه ۱ داده ارسال می کند، آدرس سخت افزاری ایستگاه ۱ را که آدرس IP 144.19.74.1 است، در جدول حافظه پنهان ARP محلی خود جستجو می کند و داده را به این آدرس سخت افزاری می فرستد. متأسفانه این آدرس سخت افزاری ایستگاه ۲ است و داده به ایستگاه ۲ فرستاده میشود. ایستگاه ۱ در انتظار برای یک پاسخ می ماند. در نهایت مهلت زمانی اتمام یافته و یا ممکن است ایستگاه برای ترمیم خطا دوباره راه اندازی شود. در هر صورت برنامه کاربردی فوق که تا مدتی پیش خوب کار می کرده است، ممکن است به طور ناگهانی از کار بیافتد. البته ممکن است که ایستگاه ۲ با دریافت داده غیرمنتظره که در اصل برای ایستگاه ۱ در نظر گرفته شده بوده است، آن را رد کند و به طور اختیاری یک پیام خطا تولید کرده و جلسه خود را با سرویس دهنده TCP/IP ادامه دهد. همچنین ایستگاه ۲ نیز با داده های غیر منتظره گیج شده و آن نیز متوقف می شود.

حال با ذکر یک مثال به بررسی مشکل آدرس های IP تکراری در سرویس دهنده های TCP/IP می پردازیم. به عنوان مثال، یک شبکه محلی با دو سرویس دهنده به نام سرویس دهنده ۱ و سرویس دهنده ۲ رادرنظر بگیرید. فرض کنید که به طور اشتباه به هر دو ایستگاه آدرس IP تکراری 144.19.74.102 تخصیص داده شده است. آدرس های سخت افزاری سرویس دهنده ها به ترتیب A و B می باشند. فرض کنید یک ایستگاه با آدرس IP 144.19.74.1 سعی می کند تا به سرویس دهنده TCP/IP با آدرس IP 144.19.74.102 متصل شود. آدرس سخت افزاری ایستگاه C است. ایستگاه سعی می کند تا به سرویس دهنده ۲ متصل شود. قبل از ایجاد اتصال TCP/IP، ایستگاه فوق یک درخواست همه پختی

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

ARP را برای کشف آدرس سخت افزاری سرویس دهنده TCP/IP منتشر می کند. دو سرویس دهنده TCP/IP با همان آدرس IP مقصد 144.19.74.102 وجود دارند. با دریافت درخواست ARP فوق، هر دو سرویس دهنده ۱ و سرویس دهنده ۲ یک ورودی را برای فرستنده درخواست ARP در جدول حافظه پنهان محلی ARP خود اضافه می کنند و یک پاسخ ARP را به فرستنده ارسال می نمایند. ایستگاه پاسخ ARP اول را می پذیرد و بی صدا پاسخ دوم را نادیده می گیرد. اگر پاسخ ARP سرویس دهنده ۲ زودتر به ایستگاه برسد، ایستگاه یک ورودی برای سرویس دهنده ۲ در جدول حافظه پنهان ARP محلی خود اضافه می کند. در این لحظه جداول حافظه پنهان ARP برای سرویس دهنده ها و ایستگاه به شرح زیر است:

جدول حافظه پنهان ARP سرویس دهنده ۱:

آدرس سخت افزاری	آدرس IP
C	144.19.74.1

جدول حافظه پنهان ARP سرویس دهنده ۲:

آدرس سخت افزاری	آدرس IP
C	144.19.74.1

جدول حافظه پنهان ARP ایستگاه:

آدرس سخت افزاری	آدرس IP
B	144.19.74.102

سپس ایستگاه محاوره را با سرویس دهنده ۲ به جای سرویس دهنده ۱ که در اصل قصد دارد، ادامه می دهد. اگر سرویس دهنده ۲ سرویس مورد نظر را نداشته باشد، اتصال قطع شده و کاربر یک پیام خطا راجع به پشتیبانی نشدن سرویس در سرویس دهنده دریافت می کند. اگر سرویس دهنده ۲ سرویس مورد انتظار ایستگاه را داشته باشد، کاربر سعی به برقراری ارتباط با آن سرویس می کند. اگر سرویس مورد نظر Telnet یا FTP باشد، نیاز به شناسه کاربر و رمز عبور می باشد. اگر کاربر یک حساب اتصال با همان شناسه و رمز عبور که در سرویس دهنده ۱ داشته است، در سرویس دهنده ۲ نداشته باشد، اتصال پذیرفته نمی شود. در صورتیکه شناسه کاربر و کلمه رمز عبور در هر دو سرویس دهنده یکسان باشد، کاربر به سرویس دهنده اشتباه متصل می شود. در این حالت این امکان وجود دارد که کاربر به دلیل آنکه به سرویس دهنده اشتباه متصل شده است، فایلها یا داده هایی را که انتظار آنها را داشته است، دریافت نکند.

۸-۱-۸- بررسی تکراری بودن آدرس های IP با کمک پروتکل ARP

در بسیاری از نسخه های معماری TCP/IP، هر کامپیوتر در هنگام راه اندازی یک درخواست ARP را در شبکه منتشر می نماید. در این پیام، آدرس IP مقصد موجود در پیام درخواست ARP مساوی با آدرس IP نود ارسال کننده پیام می باشد. هدف از ارسال پیام درخواست ARP فوق، کشف این مطلب است که آیا نودی با آدرس IP تکراری وجود دارد یا خیر؟ در صورتیکه نود ارسال کننده پیام، در پاسخ به درخواست فوق، پیام پاسخ ARP دریافت نماید، بدین معنی است که نود دیگری با آدرس IP نود فرستنده وجود دارد و این نشان دهنده وجود آدرس های IP تکراری در شبکه می باشد. در صورت وقوع این حالت، نودی که متوجه وجود آدرس تکراری در شبکه شده است، باید به نحوه مناسب تکراری بودن آدرس فوق را به اطلاع برساند.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

با توجه به اینکه قاب های ARP از مسیر یاب های موجود درمرزهای شبکه قابل عبور نمی باشند، بنابراین روال فوق وجود یا عدم وجود آدرس های IP تکراری درهمان شبکه محلی مقصد را بررسی نموده و نمی تواند مشکلات آدرس IP تکراری را که در بخش های دیگر شبکه که با مسیر یاب به هم متصل شده اند را تشخیص دهد.

یکی دیگر از کاربردهای انتشار پیام درخواست ARP درابتدای راه اندازه همه نودهای شبکه این است که چنانچه کارت شبکه نود فرستنده پیام تعویض شده و آدرس سخت افزاری آن تغییر کرده باشد، دراین صورت با ارسال پیام فوق، تمام نودهای دیگر شبکه، آدرس جدید نود فرستنده را درجدول ARP پنهان خود قرار داده و آن را به روز رسانی می نمایند.

۸-۲- پروتکل RARP

هنگام توصیف عملکرد پروتکل ARP فرض براین بود که هر نود، آدرس IP خود را می داند. سوالی که مطرح می شود این است که چگونه یک نود آدرس IP خود را بدست می آورد؟ می توان آدرس IP نود رادرانباره محلی آن که معمولاً یک فایل است، ذخیره نمود. اسم و محل آن فایل به پیاده سازی TCP/IP و سیستم عامل بستگی دارد. با این وجود بعضی از کامپیوترها انباره محلی ندارند. این کامپیوترها همه اطلاعات سیستم را در یک سرویس دهنده دور نگه می دارند. این کامپیوترها، ایستگاه های بدون دیسک خوانده می شوند. البته ممکن است که ایستگاه های بدون دیسک امروزی، دارای یک دیسک محلی باشند، اما این دیسک برای افزایش سرعت سیستم عامل استفاده می شود نه برای ذخیره سازی پارامتر های مربوط به معماری TCP/IP.

معمولاً ایستگاه های بدون دیسک، یک کپی از تصویر سیستم عامل را در سرویس دهنده های دور نگهداری می کنند. هنگام راه اندازی، ایستگاه بدون دیسک یک کپی از تصویر سیستم عامل را از سرویس دهنده دور به حافظه خود بارگذاری می کند. قبل ازانجام این کار، نیاز به یک آدرس IP دارد. این آدرس IP نمی تواند یک مقدار تصادفی باشد، بلکه باید یکتا و دارای همان پیشوند آدرس های IP سایر نود های بخش شبکه باشد. معمولاً ایستگاه بدون دیسک، آدرس IP خود را با ارسال یک درخواست به سرویس دهنده های آن بخش شبکه بدست می آورد. چون ایستگاه فوق، اطلاعات آدرس سرویس دهنده دور را نمی داند، این درخواست به صورت یک قاب همه پخشی لایه پیوند داده ارسال می شود. بدین منظور از پروتکل RARP استفاده می شود. اطلاعاتی که توسط پروتکل RARP جستجو می شود، برخلاف اطلاعات جستجو شده توسط پروتکل ARP است. سرویس گیرنده RARP، آدرس سخت افزاری خود را می داند اما آدرس IP خود را ندارد، درصورتیکه سرویس گیرنده ARP، آدرس سخت افزاری و آدرس IP خود را می داند اما آدرس سخت افزاری ایستگاه مقصد را نمی داند.

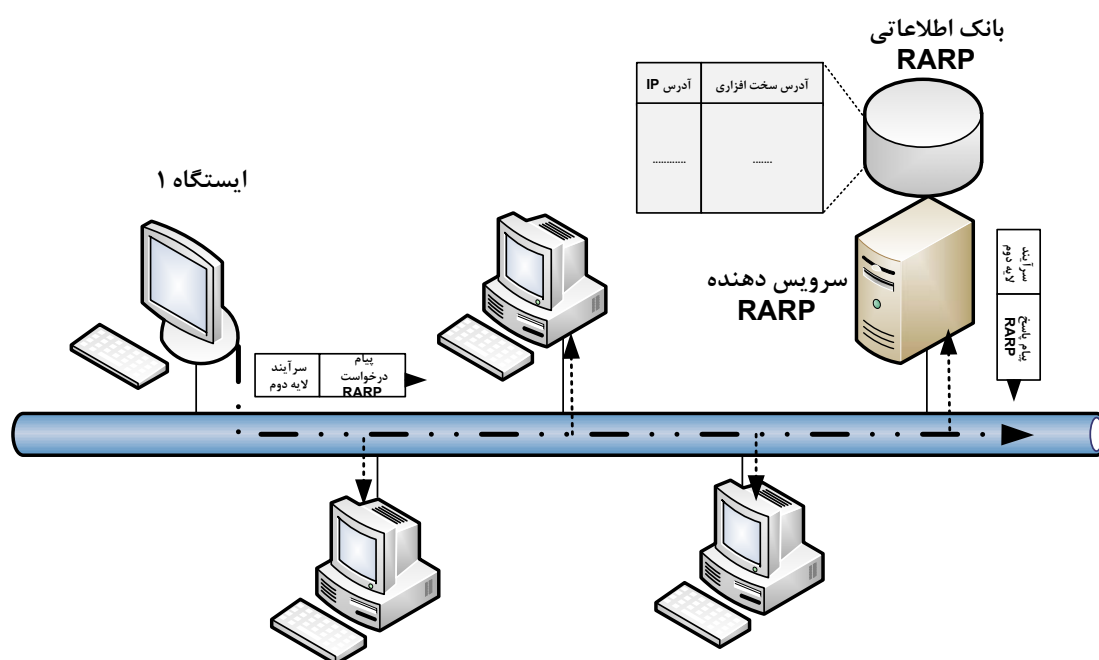
از ایستگاه های بدون دیسک برای کاهش هزینه های سخت افزاری، ساده سازی پیکره بندی، امکان به روز رسانی توسط نگه داشتن اطلاعات بحرانی در یک جایگاه مرکزی و درامان ماندن از ویروس های نرم افزاری، استفاده می شوند.

۸-۲-۱- عملکرد پروتکل RARP

در پروتکل RARP، نودی که می خواهد آدرس IP خود را کشف کند (سرویس گیرنده RARP)، یک پیام درخواست را به نام پیام درخواست RARP در شبکه محلی همه پخشی می کند. چون سرویس گیرنده RARP، آدرس سخت افزاری یا آدرس IP سرویس دهنده دور را نمی داند، بنابراین پیام درخواست RARP فوق در لایه پیوند داده همه پخشی می شود. همه نود های موجود در شبکه محلی، پیام درخواست RARP را دریافت می کنند اما تنها نود هایی که به عنوان سرویس دهنده های RARP عمل می کنند، به درخواست فوق پاسخ می دهند. چنانچه بیشتر از یک سرویس دهنده RARP وجود داشته باشد، همه سرویس دهنده های RARP تلاش می کنند تا درخواست RARP را پردازش نمایند. معمولاً

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

سرویس گیرنده RARP، اولین پاسخ دریافتی را پذیرفته و بقیه را نادیده می گیرد. سرویس دهنده RARP جدولی از آدرس های IP نود های شبکه را نگه داری می کند. این جدول توسط یک شناسه یکتا که برای هر ماشین خاص است، شاخص دار شده است. این شناسه یکتا به درخواست RARP فرستاده می شود. برای ایستگاه های بدون دیسک این شناسه یکتا، یک پارامتر سخت افزاری خاص می باشد که به آسانی قابل خواندن است. به دلیل یکتا بودن آدرس های سخت افزاری، طراحان RARP از آدرس های سخت افزاری به عنوان شناسه های یکتای فوق استفاده می کنند. هنگامی که یک سرویس دهنده RARP یک درخواست RARP را دریافت می نماید، جدول خود را بررسی می کند. اگر یک ورودی در جدول RARP پیدا کرد که با آدرس سخت افزاری موجود در پیام درخواست RARP مطابقت دارد، آدرس IP متعلق به آن را در پیام پاسخ RARP بر می گرداند. از آنجاییکه سرویس دهنده RARP آدرس سخت افزاری سرویس گیرنده RARP را از پیام درخواست RARP بدست می آورد، بنابراین نیازی به ارسال پیام پاسخ RARP به صورت همه پخشی نمی باشد. قالب بسته های دریافت و پاسخ RARP با قالب بسته های ARP یکسان می باشد. شکل (۸-۶) مثالی از عملکرد پروتکل RARP را نشان می دهد. در این مثال فرض بر این است که ایستگاه شماره ۱، آدرس IP ندارد. بدین منظور پیام درخواست RARP به صورت همه پخشی در لایه ۲ ارسال می دارد. این پیام به سرویس دهنده RARP می رسد. سرویس دهنده با جستجو در بانک اطلاعاتی خود، آدرس IP متناظر با آدرس سخت افزاری ایستگاه فرستنده را پیدانموده و برای آن از طریق پیام پاسخ RARP ارسال می دارد.



شکل (۸-۶): مثالی از عملکرد RARP

توصیف فیلدهای موجود در پیام های درخواست و پاسخ RARP به شرح زیر می باشد:

پیام درخواست RARP

آدرس سخت افزاری مقصد در لایه دوم = همه پخشی

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

آدرس سخت افزاری مبدا در لایه دوم = آدرس سخت افزاری سرویس گیرنده RARP (ارسال کننده پیام)
 فیلد Ether Type موجود در قالب های پروتکل پیوند داده لایه دوم = 8035 hex
 فیلد عملکرد موجود در بسته درخواست RARP = ۳ (نشان دهنده پیام درخواست RARP)
 آدرس سخت افزاری فرستنده موجود در بسته درخواست RARP = آدرس سخت افزاری سرویس گیرنده RARP
 (ارسال کننده پیام)
 آدرس IP فرستنده موجود در بسته درخواست RARP = نامشخص است. معمولاً از 0.0.0.0 استفاده می شود.
 آدرس سخت افزاری مقصد موجود در بسته درخواست RARP = آدرس سخت افزاری سرویس گیرنده RARP
 آدرس IP مقصد موجود در بسته درخواست RARP = نامشخص

پیام پاسخ RARP

آدرس سخت افزاری مقصد در لایه دوم = آدرس سخت افزاری سرویس گیرنده RARP
 آدرس سخت افزاری مبدا در لایه دوم = آدرس سخت افزاری سرویس دهنده RARP
 فیلد Ether Type موجود در قالب های پروتکل پیوند داده لایه دوم = 8035 hex
 فیلد عملکرد موجود در بسته های RARP = ۴ (پاسخ RARP)
 آدرس سخت افزاری فرستنده موجود در بسته پاسخ RARP = آدرس سخت افزاری سرویس دهنده RARP .
 آدرس IP فرستنده موجود در بسته پاسخ RARP = آدرس IP سرویس دهنده RARP .
 آدرس سخت افزاری مقصد موجود در بسته پاسخ RARP = آدرس سخت افزاری سرویس گیرنده RARP .
 آدرس IP مقصد موجود در بسته پاسخ RARP = آدرس IP سرویس گیرنده RARP (این جواب است)

در خیلی از پیاده سازیهای TCP/IP، پروتکل RARP به طور اتوماتیک توسط ماژول ARP یا ماژول IP فراهم نشده بلکه باید به عنوان یک فرایند جداگانه در کامپیوتری که به عنوان سرویس دهنده RARP عمل می کند، اجرا گردد.

۸-۲-۲- مشکلات RARP

در صورتیکه بخاطر یک نقص اتصال سخت افزاری یا بخاطر از کار افتادن، سرویس دهنده RARP در دسترس نباشد، سرویس های گیرنده های RARP قادر به راه اندازی نیستند. در این حالت سرویس گیرنده های RARP، به منظور بدست آوردن آدرس IP خود، به طور پیوسته درخواست های همه پخشی RARP را می فرستند. اگر سرویس گیرنده های RARP زیادی به طور هم زمان درخواست RARP را منتشر کنند، این امر بار ترافیکی سنگینی را در شبکه ایجاد می کند. بنابراین مشکلات ایجاد شده به خاطر دریافت نکردن یک پاسخ RARP، به مراتب جدی تر از دریافت نکردن یک پاسخ ARP است. اگر پاسخ ARP دریافت نشود، به این معنی است که یک میزبان خاص و سرویس های آن در دسترس نبوده و سرویس گیرنده ARP هنوز می تواند برای دستیابی به سایر نود های شبکه تلاش کند. اما اگر پاسخ RARP دریافت نشود، سرویس گیرنده RARP نمی تواند راه اندازی شود. در این حالت سرویس گیرنده های RARP زیادی به ارسال درخواست های همه پخشی RARP به طور نامحدود ادامه می دهند به امید اینکه سرویس دهنده RARP در نهایت به درخواست آنها پاسخ دهد. بنابراین این مسئله می تواند ترافیک زیادی را در شبکه ایجاد کند.

۸-۲-۳- سرویس دهنده های اصلی و پشتیبان RARP

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد^۱)

رای دستیابی مطمئن تر به سرویس های RARP، از چندین سرویس دهنده RARP به طور همزمان استفاده می شود. با کمک سرویس دهنده های RARP چند گانه، همه سرویس دهنده ها به طور همزمان برای جواب دادن به درخواست همه پخشی RARP تلاش می کنند. فقط یکی از جواب های RARP توسط سرویس گیرنده RARP مورد استفاده قرار گرفته و سایر پاسخ های RARP دیگر حذف می شوند. برای جلوگیری از پاسخ های RARP چندتایی، یکی از سرویس دهنده ها به عنوان سرویس دهنده اصلی و سایر سرویس دهنده ها RARP به عنوان سرویس دهنده ثانویه در نظر گرفته می شوند. با دریافت یک پیام درخواست RARP، سرویس دهنده اصلی RARP به درخواست پاسخ می دهد و سرویس دهنده های ثانویه پاسخی نمی دهند فقط زمان ورود درخواست RARP را یادداشت می کنند. اگر سرویس دهنده اصلی در بازه زمانی معینی پاسخ نداد، سرویس دهنده ثانویه RARP فرض می کند که سرویس دهنده اصلی از کار افتاده و به درخواست RARP پاسخ می دهد.

۸-۳- پروتکل اینترنت (IP)

با استفاده از پروتکل اینترنت (IP) می توان که پروتکل های لایه حمل مانند پروتکل های TCP و UDP، را فقط به عنوان یک شبکه IP دانست درحالیکه در واقعیت ممکن است که فقط یک شبکه IP نباشد و پروتکل های دیگری را در کنار TCP/IP پشتیبانی کنند. پروتکل IP سرویس های بدون اتصال را برای لایه بالاتر مهیا می سازد. این سرویس بدون اتصال با بسته هایی که شامل آدرس های IP مقصد و مبدا و سایر پارامتر های دیگر مورد نیاز برای عملکرد IP هستند، پیاده سازی می شوند.

لایه IP برای ارسال بسته های خود به سخت افزار زیرین شبکه تکیه دارد. به این معنی که بسته IP توسط قاب شبکه زیرین مانند اترنت، شبکه حلقوی و یا شبکه های سوئیچینگ بسته ای، بسته بندی می شود. پروتکل های لایه بالا مانند TCP و UDP نیازی به آگاهی از بسته بندی سخت افزار شبکه ندارند. پروتکل های لایه بالا، کیفیت مطمئن سرویس مانند تاخیر کم و گذردهی مناسب را انتظار دارند. این عوامل پارامترهای کیفیت سرویس نامیده میشوند. لایه های بالاتر پارامترهای کیفیت سرویس را همراه با داده های خود به لایه IP پاس می دهند. لایه IP سعی براین دارد تا پارامتر های کیفیت سرویس را به سرویس های تهیه شده توسط سخت افزار زیرین شبکه نگاشت دهد. ممکن است که سخت افزار زیرین شبکه، قادر به فراهم سازی این سرویسها باشند.

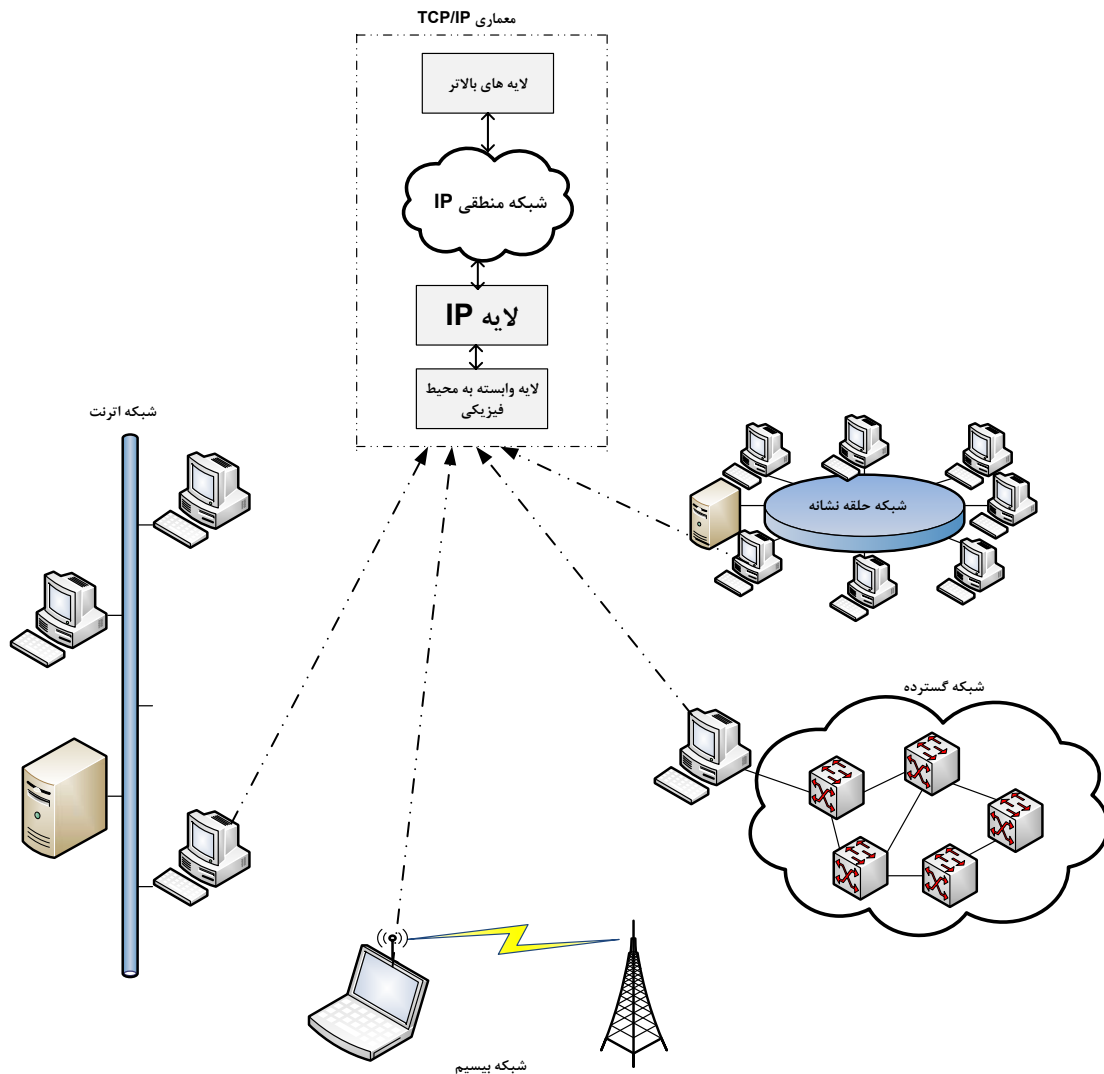
شکل (۸-۷)، شبکه های ناهمگون مختلفی شامل: اترنت، شبکه حلقه نشانه، شبکه بیسیم و شبکه گسترده را نشان می دهد. در تمامی این شبکه ها میزبان هایی وجود دارند که از معماری TCP/IP استفاده می نمایند. در این شبکه ها، پروتکل IP در تمام شبکه ها اجرا می شود. میزبان های شبکه با کمک اتصال های IP به شبکه متصل می شوند. این اتصالات شبکه توسط یک شناسه ۳۲ بیتی یکتا به نام آدرس IP مشخص می شوند. لایه IP یک انتزاع را برای هر یک از سه شبکه به لایه های بالاتر معرفی می کند. این انتزاع به صفات فیزیکی شبکه ها مانند اندازه آدرس، حداکثر واحد ارسال در لایه پیوند داده، پهنای باند شبکه، حداکثر سرعت ارسال داده و غیره بستگی دارد.

طبق تعریف، به حداکثر میزان نرخ قابل ارسال در یک شبکه فیزیکی، حداکثر واحد ارسال (MTU^1) گفته می شود. به عنوان مثال در شبکه نشان داده شده در شکل (۸-۷) اندازه MTU شبکه اترنت ۱۵۰۰ بایت است. اندازه MTU برای شبکه حلقه نشانه IEEE802.5 از نوع ۴ مگابیت بر ثانیه، ۴۴۴۰ بایت است. این اندازه برای شبکه حلقوی IEEE802.5

¹ Maximum Transfer Unit

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

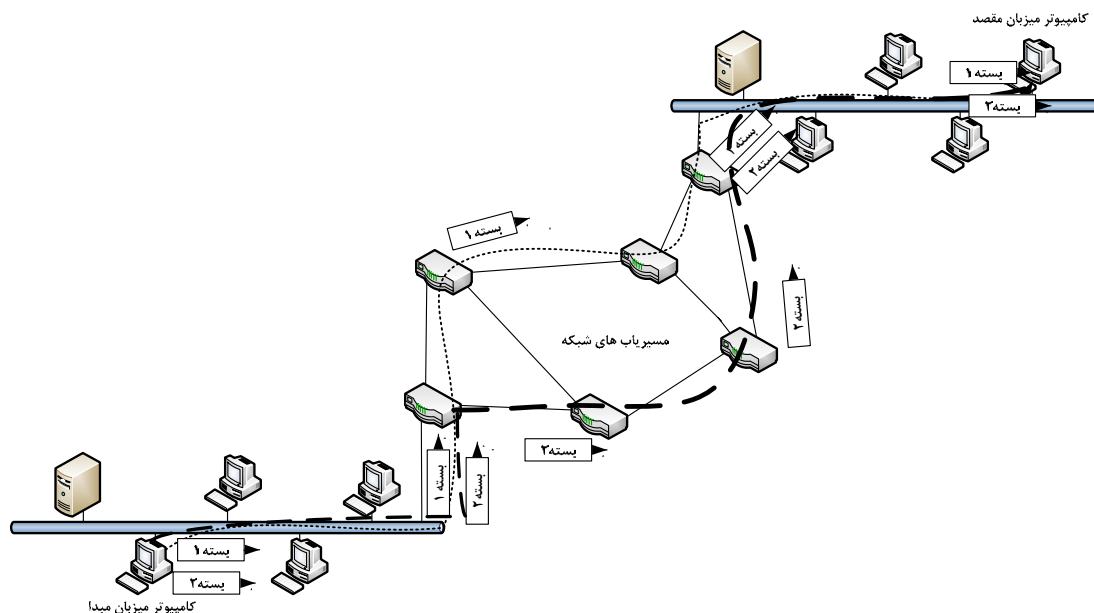
۱۶ مگابیت بر ثانیه، ۱۷۹۴۰ بیت می باشد. در شبکه های X.25 اندازه MTU اختیاری بوده و در بازه ۶۴ بیت تا ۴ کیلو بیت قابل تغییر است. باید توجه داشت که حداقل طول یک بسته IP نمی تواند از ۵۷۶ بیت کمتر باشد. پروتکل IP بدون اتصال بوده که هر بسته در آن به طور مستقل مسیریابی می شود. بنابراین ممکن است بسته های متوالی در مسیر های متفاوت انتقال داده شوند.



شکل (۸-۷): نمونه ای از استفاده از IP بر روی شبکه های فیزیکی مختلف

در شکل (۸-۸) مثالی از مسیریابی بسته ها در یک شبکه IP نشان داده شده است.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۸-۸): مسیریابی مستقل بسته های IP

به خاطر اختلاف تاخیرهای زمینی در بین مسیر ها، این امکان وجود دارد که بسته ها با ترتیبی متفاوت با آن ترتیبی که فرستاده شده اند به مقصد برسند. لایه IP هیچ تلاشی برای تحویل مرتب بسته ها به لایه های بالاتر نمی کند. همچنین این پروتکل هیچ تلاشی برای تحویل مطمئن بسته ها به مقصد نمی نماید. مشکل ترتیب بسته ها و تحویل مطمئن داده ها توسط یک پروتکل لایه بالا مانند TCP حل می شود.

چون IP تلاشی بر ای حل ترتیب دهی و تحویل مطمئن داده ها نمی کند، به آسانی به هر نوع سخت افزار شبکه قابل نگاشت می باشد. پروتکل های لایه بالا، سطوح اطمینان اضافی را چنانکه مورد نیاز برنامه های کاربردی است فراهم می کنند. بنابراین شبکه IP بدون تضمین بوده و به صورت بهترین تلاش عمل می کند. این بدان معنی است که پروتکل IP سعی می کند که بهترین کار ممکن را برای تحویل بسته های IP انجام دهد ولی تحویل سالم و به ترتیب بسته ها را ضمانت نمی کند. در پروتکل IP هر بسته مستقل از بقیه بسته ها مسیر یابی می شود. هر بسته شامل آدرس IP مقصد و آدرس IP فرستنده می باشد.

مسیریاب های میانی شبکه با استفاده از آدرس IP مقصد، بسته های IP را به مقصد درست پیش می برند. مستقل بودن پروتکل IP از پروتکل های زیرین شبکه باعث می شود که بسته های IP بدون توجه به اندازه MTU لایه های پایین تر، ارسال شوند. نود های میانی شبکه IP در صورت نیاز می توانند یک بسته بزرگ را تکه سازی نمایند.

پروتکل IP برای تطبیق دادن با انواع مختلف سخت افزار شبکه طراحی شده است. همانطور که قبلا اشاره شد، شبکه های مختلف محدودیت های متفاوتی برای حداکثر اندازه داده قابل ارسال توسط قاب لایه پیوند داده دارند. جدول (۸-۳) اندازه MTU انواع سخت افزار های مختلف شبکه را فهرست کرده است.

جدول (۸-۳): اندازه های MTU شبکه های مختلف

نوع شبکه	اندازه MTU
اترنت	۱۵۰۰ بایت
IEEE 802.3	۱۴۹۲ بایت

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

۴۴۴۰ بایت تا ۱۷۹۴۰ بایت (بستگی به سرعت ارسال در شبکه

دارد)

۴۳۵۲ بایت

۸۱۶۶ بایت

۹۱۸۰ بایت

شبکه حلقوی IEEE 802.5

FDDI

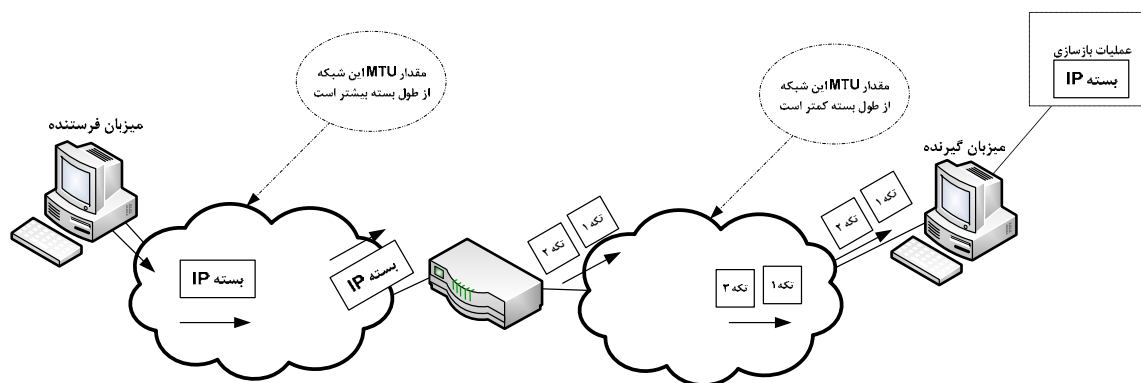
IEEE 802.4

SMDS

حداکثر طول یک بسته IP ۶۵۵۳۶ بایت است. مقدار MTU اغلب شبکه ها از مقدار حداکثر طول قابل ارسال بسته های IP به مراتب کمتر می باشد. هیچ مکانیزم کارآمدی برای تعیین MTU شبکه های میانی توسط پروتکل IP وجود ندارد. اگر این امر انجام شود، فرستنده می تواند بسته های IP را به اندازه ای تنظیم کند که از اندازه MTU شبکه های میانی تجاوز ننماید. ولی درعمل شبکه های IP با استفاده از مکانیزم تکه سازی قادر به تحویل بسته هایی با اندازه دلخواه به هر شبکه می باشند.

۸-۳-۱- تکه سازی IP

اگر یک بسته IP از اندازه MTU شبکه ای که باید از آن عبور کند، بیشتر باشد دراین صورت نمی تواند در یک تکه کامل فرستاده شود. دراین حالت باید بسته IP به تکه های کوچکتری که از اندازه MTU شبکه تجاوز نمی کند، شکسته شود. این فرایند، عملیات تکه سازی نامیده می شود. هر تکه از بسته اصلی به عنوان یک بسته IP مستقل فرستاده می شود. در سرآیند IP اطلاعات کافی برای مشخص کردن تکه، حمل می شود. میزبان مقصد با استفاده از اطلاعات تکه سازی موجود در سرآیند بسته های IP قادر به سر هم کردن تکه ها می باشد. شکل (۸-۹) فرایند ارسال یک بسته IP را در شبکه هایی با اندازه های مختلف MTU نشان می دهد. در این مثال، اندازه MTU شبکه B کوچکتر از اندازه بسته ارسالی است. مسیریاب R1 این حقیقت را تشخیص داده و بسته های IP را به اندازه های کوچکتری تکه سازی می کند تا از اندازه MTU شبکه B تجاوز نکند. بسته های تکه شده به طور مستقل مسیریابی می شوند و به میزبان C می رسند. اگر چه اندازه MTU شبکه C از اندازه تکه های بسته IP بزرگتر بوده و حتی می تواند با بسته اصلی مطابقت کند، ولی مسیر یاب R2 موجود درمرز بین شبکه های B و C هیچ تلاشی برای دوباره سرهم کردن تکه ها برای تشکیل بسته اصلی نمی کند. عملیات بازسازی تکه های بسته IP توسط ماژول IP موجود در کامپیوتر میزبان درمقصد انجام می شود. هرگز مسیر یابهای میانی شبکه عملیات فوق را انجام نمی دهند.



شکل (۸-۹): تکه سازی بسته IP

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

هنگامی که میزبان B نیاز به پاسخ به میزبان A داشته باشد در این صورت اندازه بسته را طوری تنظیم می کند تا از اندازه MTU شبکه B تجاوز نکند. بسته های ارسالی از میزبان C به میزبان A می تواند بدون هیچ تکه سازی تحویل داده شود. با این وجود، مسیر یاب های میانی شبکه سعی نمی کنند که برای افزایش کارایی انتقال، بسته های کوچکتر را با یکدیگر ترکیب نموده و یک بسته بزرگتر ایجاد نمایند. باید به این نکته توجه نمود که در شبکه های IP بسته های تکه شده فقط در مقصد سر هم می شوند.

۸-۳-۲- قالب بسته IP

همانطور که در شکل (۸-۱۰) نشان داده شده است، بسته های IP از دو قسمت تشکیل شده اند که عبارتند از: سرآیند IP و داده های IP. سرآیند IP برای مطابقت با خواص لایه IP طراحی شده است. سرآیند IP باید حداقل شامل اطلاعات زیر باشد:

- آدرس IP مبدا و مقصد: این اطلاعات لازم است چون IP یک پروتکل بدون اتصال است و اطلاعات کامل آدرس مقصد و مبدا باید در هر بسته موجود باشد.
- کیفیت سرویس: این فیلد برای مشخص کردن نوع سرویس مورد انتظار از شبکه زیرین لازم است.
- اطلاعات تکه سازی: چون بسته IP ممکن است که در داخل شبکه تکه سازی شود، باید فیلدهایی برای کمک به تشخیص تکه ها، درون بسته اصلی باشد.
- اندازه بسته: از آنجاییکه اندازه بسته های IP می تواند متغیر باشد، بنابراین باید فیلدی برای مشخص کردن طول کلی بسته IP وجود داشته باشد.
- اندازه سرآیند IP: بسته های IP می تواند شامل فیلدهای اختیاری برای مشخص کردن امکانات IP استفاده شده برای امنیت، مسیر یابی مبدا و غیره باشد. این عامل اندازه طول سرآیند IP را متغیر می سازد. بنابراین اندازه واقعی بسته IP باید در سرآیند IP نشان داده شود.



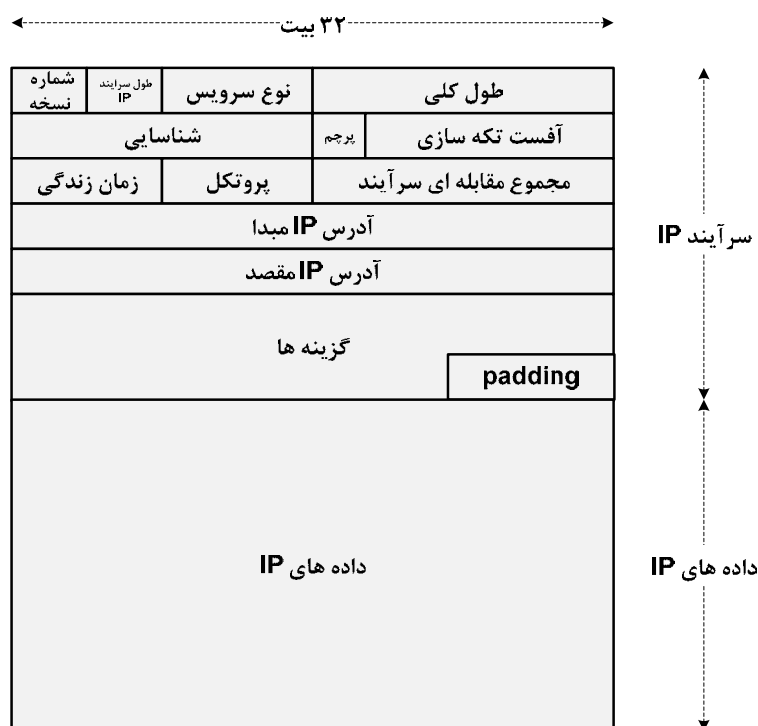
شکل (۸-۱۰): نحوه بسته سازی داده ها در معماری TCP/IP

کمترین طول سرآیند IP ۲۰ بایت است. چون در سرآیند IP، فیلدی برای امکانات اضافی در نظر گرفته شده است، بنابراین طول سرآیند ممکن است بیشتر از ۲۰ بایت باشد. شکل (۸-۱۱)، فیلدها و ساختار سرآیند IP را نشان می دهد. قالب سرآیند IP با جزئیات کامل در RFC 791 و RFC 1122 بحث شده است. همچنین RFC 1349 استفاده فیلد نوع سرویس را با جزئیات کامل در سرآیند IP توصیف می کند.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

۸-۳-۱- فیلد شماره نسخه

مطابق با شکل (۸-۱۱)، فیلد شماره نسخه در سرآیند بسته های IP دارای ۴ بیت طول می باشد و نشان دهنده شماره نسخه پروتکل IP است. این امر توانایی معرفی ساختارهای آینده بسته IP را فراهم می سازد. شماره نسخه فعلی IP ۴ است و به این علت پروتکل فعلی اینترنت، پروتکل IPV4 نامیده می شود. نسل آتی پروتکل IP دارای مقدار فیلد شماره نسخه برابر با ۶ است. به این علت، پروتکل آتی IP، با عنوان IPV6 شناخته می شود. جدول (۸-۴) مقادیر مختلف فیلد شماره نسخه نشان داده شده است. باید توجه نمود که مقادیر شماره نسخه ۷، ۸ و ۹ پروتکل های IP پیشنهادی و تجربی برای حل مشکل محدودیت آدرس های ۳۲ بیتی انتساب داده شده اند که این پروتکل ها با آمدن پروتکل IPV6 کنار گذاشته شده اند.



شکل (۸-۱۱): ساختار بسته های IP

فیلد شماره نسخه توسط فرستنده، گیرنده و مسیریاب های میانی برای مشخص کردن قالب سرآیند IP استفاده می شود. برای بررسی فیلد نسخه، نیاز به نرم افزار IP می باشد تا بدین وسیله اطمینان حاصل شود که قالب سرآیند همان قالب مورد انتظار است. بدین ترتیب اگر نرم افزار IP فقط بتواند بسته های نسخه ۴ را پردازش کند، بسته هایی را که مقدار شماره نسخه آنها غیر از ۴ می باشند، رد می گردند.

جدول (۸-۴): مقادیر مختلف شماره نسخه IP

توصیف	شماره نسخه
رزرو	۰ و ۱۵
انتصاب داده نشده است	۱-۳ و ۱۰-۱۴
پروتکل فعلی اینترنت (IPV4)	۴

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

پروتکل آزمایشی Stream IP	۵
پروتکل آتی اینترنت (IPv6)	۶
پروتکل اینترنت TP/IX	۷
پروتکل اینترنت P	۸
پروتکل TUBA	۹

پروتکل Stream IP، یک پروتکل آزمایشی است که برای تضمین سرویس انتها به انتها در اینترنت استفاده می شود. این پروتکل در RFC 1819 توصیف شده است. پروتکل TP/IX، پروتکل "P" و TUBA همه زمانی مدعی جدی جایگزینی IPv4 بودند، اما با آمدن پروتکل IPv6 این سه پروتکل اهمیت خود را از دست داده اند. پروتکل اینترنت "P"، یک پروتکل جدید با خواص پیشرفته و آدرس هایی با طول متغیر است. این پروتکل، بعد از مدتی که از پیدایش آن می گذشت با پروتکل اینترنت ساده (SIP) ادغام گردید. پروتکل SIP از آدرس دهی ۶۴ بیتی استفاده می کند و نحوه گذر بین IPv4 و آدرس دهی طولانی تر را توصیف می کند. پروتکل SIP در RFC 1710 توصیف شده است. پروتکل TP/IX، یک پروتکل قدیمی بوده که پایه معماری مشترک برای اینترنت گردید. پروتکل TUBA در RFC 1347، RFC 1526، RFC 1561 توصیف شده است

۸-۳-۲-۲- فیلد طول سرآیند اینترنت (IHL)

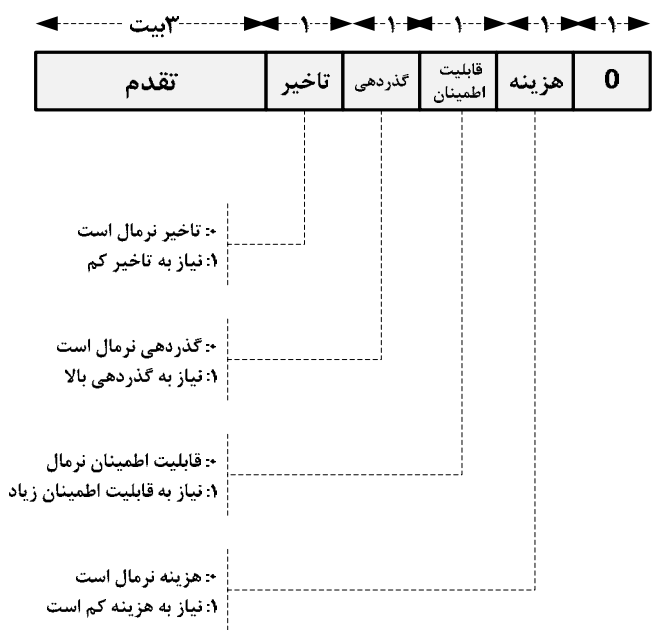
فیلد طول سرآیند اینترنت، طول سرآیند بسته های IP را برحسب کلمات ۳۲ بیتی نشان می دهد. این فیلد ۴ بیت طول دارد. از آنجاییکه سرآیند IP شامل فیلد امکانات با طول متغیر است، فیلد طول سرآیند اینترنت مورد نیاز می باشد. مقدار معمول این فیلد، ۵ کلمه ۳۲ بیتی است. در این حالت امکانات اضافی در بسته IP وجود ندارد. حداکثر طول سرآیند بسته های IP با در نظر گرفتن فیلد امکانات، برابر با ۶۰ بایت است. در این حالت مقدار IHL، ۱۵ کلمه ۳۲ بیتی خواهد بود.

۸-۳-۲-۳- فیلد نوع سرویس^۱ (TOS)

فیلد نوع سرویس، نوع سرویس درخواستی را از نظر پارامترهایی نظیر: میزان تقدم، تاخیر، گذردهی و اطمینان را مشخص می کند. اجزای این فیلد ۸ بیتی در شکل (۸-۱۲) نشان داده شده است.

^۱ Type of Service

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد) ۲



شکل (۸-۱۲): ساختار فیلد نوع سرویس برای بسته های IP

۳ بیت اول، مقدار ترتیب تقدم همراه با بسته IP را نشان می دهد. فیلد ترتیب تقدم ۳ بیت طول دارد و کدینگ آن در جدول (۵-۸) نشان داده شده است.

جدول (۵-۸): مقادیر زیر فیلد ترتیب تقدم در فیلد نوع سرویس

توصیف	مقدار تقدم
تقدم عادی	۰۰۰
تقدم دارای اولویت	۰۰۱
تقدم فوری	۰۱۰
تقدم آنی	۰۱۱
تقدم برتر از آنی	۱۰۰
تقدم بحرانی	۱۰۱
تقدم کنترل بین شبکه ای	۱۱۰
تقدم کنترل شبکه	۱۱۱

از ۴ بیت بعدی که به دنبال فیلد ترتیب تقدم در ساختار فیلد نوع سرویس می آیند، برای نشان دادن نوع سرویس درخواستی استفاده می شود. این کدها همان طور که در جدول (۶-۸) نشان داده شده اند به صورت زیر تفسیر شده اند.

جدول (۶-۸): کدهای نوع سرویس

توصیف	کد
نیاز به تاخیر کم	۱۰۰۰
نیاز به حداکثر گذردهی	۰۱۰۰
نیاز به حداکثر قابلیت اطمینان	۰۰۱۰

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

نیاز به کمترین هزینه
سرویس معمولی

۰۰۰۱
۰۰۰۰

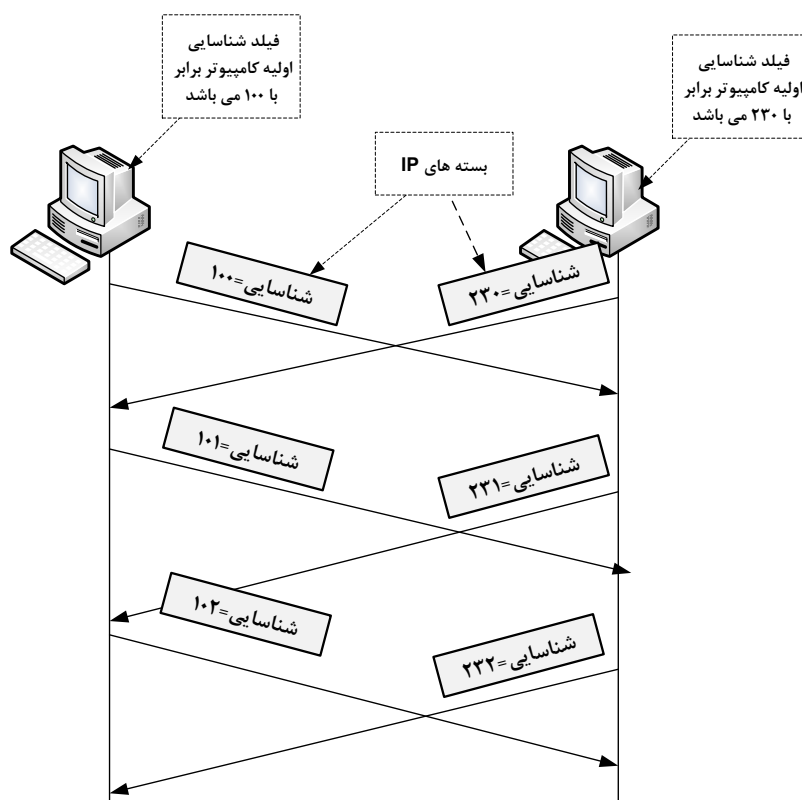
آخرین بیت فیلد نوع سرویس همواره برابر با ۰ می باشد و برای استفاده در آینده رزرو شده است.

۸-۳-۲-۴- فیلد طول کلی

فیلد طول کلی نشان دهنده طول بسته IP شامل سرآیند IP و داده بر حسب بایت می باشد. این فیلد ۱۶ بیت طول دارد و بسته را به حداکثر اندازه ۶۵۵۳۵ بایت محدود می کند. از آنجائیکه معمولاً اندازه MTU اغلب شبکه ها خیلی کمتر از ۶۵۵۳۵ بایت است، بنابراین بسته هایی که ۶۵۵۳۵ بایت طول دارند برای اغلب میزبانها و شبکه ها غیر قابل عبور می باشند. همچنین چنانچه بسته های IP به بزرگی ۶۵۵۳۵ بایت باشند در این صورت طراحی با فرهای ارسال در فرستنده و همچنین بافرهای مسیر یاب های میانی کارآمد نیست. معمولاً اندازه بسته برای اغلب شبکه ها و میزبانها بندرت از ۱۶ KB تجاوز میکند. همه نود های IP باید توانایی دریافت بسته هایی را با طول حداقل ۵۷۶ بایت داشته باشند. همانطور که قبلاً اشاره شد، بسته هایی که دارای طول بیشتر از اندازه MTU شبکه زیرین باشند، باید تکه سازی شوند.

۸-۳-۲-۵- فیلد شناسایی

فیلد شناسایی برای هر بسته به طور یکتا مقدار دهی می شود و نشان دهنده شماره بسته است. هر طرف ارسال، در ابتدای اتصال از یک مقدار اولیه به عنوان شماره بسته استفاده می کنند. همانطور که در شکل (۸-۱۳) نشان داده شده است، با ارسال هر بسته جدید، یکی به مقدار این فیلد اضافه می شود. اغلب پیاده سازیهای IP از یک شمارنده حافظه عمومی استفاده می کنند که با ارسال هر بسته IP، یک واحد افزایش می یابد.



شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

شکل (۸-۱۳): مثالی از کاربرد فیلد شناسایی

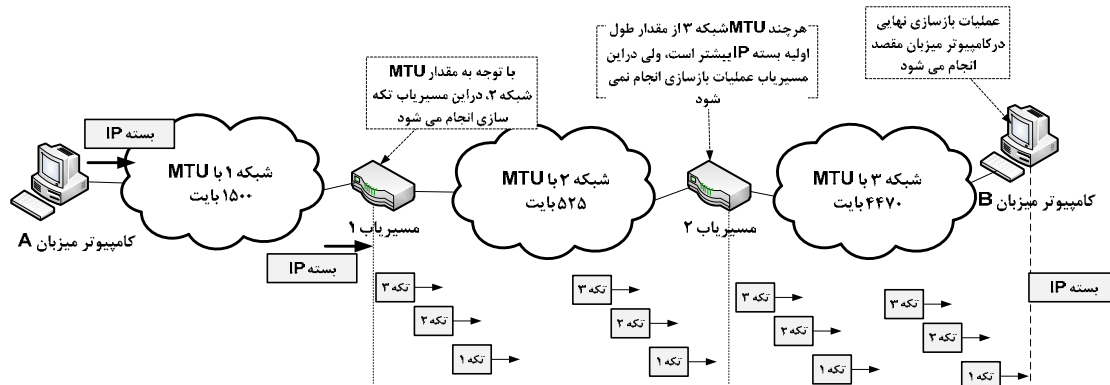
فیلد شناسایی ۱۶ بیت طول دارد که این امر اجازه می دهد تا بسته ها از ۰ تا ۶۵۵۳۵ شماره گذاری شوند. فیلد شناسایی دراصل برای شناسایی تکه های بسته IP که متعلق به یک بسته اصلی خاص هستند، استفاده می شود. باید توجه نمود که درهنگام تکه سازی یک بسته IP به تکه های کوچکتر، مقدار این فیلد درتمام تکه های IP تغییرنکرده و یکسان می باشد.

۸-۳-۲-۶- فیلد های پرچم و افست تکه سازی

فیلد پرچم سه بیت طول دارد. اولین بیت این فیلد همواره صفر است. بیت های دوم و سوم به ترتیب بیت های DF^1 و MF^2 می باشند. اگر مقدار پرچم DF برابر با ۱ باشد، به این معنی است که نباید بسته تکه سازی شود. چنانچه فرستنده بداند که گیرنده توانایی کافی برای بازسازی تکه های بسته اصلی را ندارد، آنگاه مقدار فیلد DF را برابر با ۱ قرار می دهد تا از تکه سازی احتمالی بسته IP درنودهای میانی جلوگیری شود. به عنوان مثال برنامه boot strap که در Rom کامپیوتر اجرا می شود، داده ها را از یک ماشین سرویس دهنده بار گذاری می نماید. اگر کل داده برای جا شدن در یک بسته طراحی شده باشد، فرستنده می تواند پرچم DF را ۱ قرار دهد.

چنانچه پرچم MF برابر با ۱ باشد، گیرنده متوجه خواهد شد که تمام تکه های بسته اصلی هنوز نیامده اند و تکه های بیشتری درراه می باشند. مقدار ۰ درفیلد پرچم فوق، نشان دهنده این است که این تکه، آخرین تکه می باشد. برای بسته های IP کامل، پرچم MF همیشه ۰ خواهد بود که نشان می دهد تکه های بیشتری از این بسته وجود ندارد.

درادامه با ذکر یک مثال نحوه تکه سازی در پروتکل IP را توضیح می دهیم. شبکه نشان داده شده در شکل (۸-۱۴) را در نظر بگیرید که در آن یک میزبان A در شبکه ۱ بسته های IP را به میزبان B در شبکه ۳ می فرستد. مقدار MTU در شبکه های ۱ و ۲ به ترتیب ۱۵۰۰، ۵۲۵، ۴۴۷۰ بایت است. مسیر یاب ۱ شبکه های ۱ و ۲ را به هم پیوند می دهد و مسیر یاب ۲ شبکه های ۲ و ۳ را به هم متصل می کند. فرض کنید بسته ای با مقدار شناسایی ۵ به اندازه ۱۵۰۰ بایت به وسیله میزبان A فرستاده می شود. هنگامی که مسیر یاب ۱ با این بسته مواجه می شود، قبل از این که بسته را به شبکه ۲ ارسال نماید، باید آن را تکه سازی کند. دلیل این امر آن است که اندازه MTU شبکه ۲ کوچکتر از اندازه بسته می باشد. انتخاب می شوند که بسته های تکه شده داخل MTU شبکه ۲ که ۵۲۵ بایت است جا شوند.



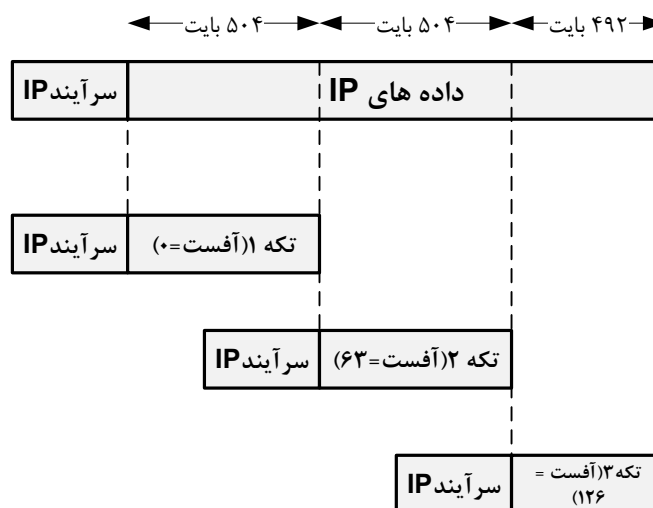
¹ Don't Fragment

² More Fragment

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

شکل (۸-۱۴): مثالی از نحوه تکه سازی IP

فیلد افست تکه سازی، مکان داده مربوط به آغاز بسته اصلی را نشان می دهد. این فیلد ۱۳ بیت طول دارد. با بررسی قالب سرآیند IP، به این نتیجه می توان رسید که تنها ۱۳ بیت فضا برای این فیلد در نظر گرفته شده است. از آنجاییکه حداکثر طول یک بسته IP می تواند تا ۶۵۵۳۵ بایت باشد، طول این فیلد برای توصیف مقادیر بزرگتر از ۸۱۹۲ بایت به اندازه کافی نیست. به این دلیل فیلد افست تکه سازی با ضمیمه کردن ۳ بیت صفر توسعه می یابد. در نتیجه مقدار افست تکه سازی همیشه ضربی از ۸ بایت است و همواره تکه ها را در واحد های ۸ بایتی توصیف می کند. به عبارت دیگر، مقدار افست تکه سازی باید در ۸ ضرب شود تا افست حقیقی تکه بدست بیاید. بنابراین طول همه تکه ها غیر از آخرین تکه، باید مضرب ۸ باشند. به علاوه تکه ها باید داخل اندازه MTU شبکه جا شوند. با توجه به اندازه MTU ۵۲۵ بایت با تفریق اندازه معمول سرآیند IP که ۲۰ بایت است، ۵۰۵ بایت برای اندازه تکه حاصل می شود. از آنجاییکه این عدد مضرب ۸ نمی باشد، کوچکترین اندازه بعدی تکه که قابل تقسیم بر ۸ است ۵۰۴ است. بنا براین می توان اندازه تکه های بسته IP را ۵۰۴ بایت انتخاب نمود. شکل (۸-۱۵) شکستن بسته IP اصلی را به تکه های کوچکتر نشان می دهد. طول تکه های اول و دوم برابر با ۵۰۴ بایت می باشد و آخرین تکه دارای طول ۴۹۲ بایت است.



شکل (۸-۱۵): مثالی از تکه سازی بسته اصلی IP

هر تکه باید سرآیند IP خودش را داشته باشد. مقدار فیلد شناسایی در بسته های IP تکه شده، برابر با مقدار متعلق به بسته اصلی است. این امر مشخص می کند که تکه IP به یک بسته اصلی خاص تعلق دارد. مقادیر تنظیمات پرچم و افست تکه سازی بسته های IP تکه سازی شده در جدول (۸-۶) نشان داده شده است:

شماره تکه	طول کلی	شناسایی	پرچم DF	پرچم MF	آفست تکه سازی
تکه اول	۵۰۴ بایت	۵	۰	۱	۰
تکه دوم	۵۰۴ بایت	۵	۰	۱	۶۳
تکه سوم	۴۹۲	۵	۰	۰	۱۲۶

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

برای این که گیرنده قادر به بازسازی تکه های بسته IP باشد، باید همه آنها را دریافت نماید. به منظور انجام عملیات بازسازی، گیرنده ازفیلدهای : اندازه هر تکه (فیلد طول کلی سرآیند بسته IP)، مقدار افست تکه سازی و پرچم MF استفاده می کند. با استفاده از فیلدهای فوق، گیرنده قادر خواهد بود تا مشخص کند که آیا همه تکه ها را دریافت کرده است یا خیر؟ باید توجه نمود که مقدار پرچم MF تکه آخر صفر می باشد. همچنین تکه اول با مقدار پرچم MF برابر ۱ و افست تکه سازی برابر با صفر شناسایی می شود. همچنین برای تکه های میانی، مقدار پرچم MF برابر با ۱ و مقدار افست تکه سازی غیر صفر است. بعد از تکه سازی بسته های IP، هر تکه در مسیر های جداگانه احتمالی به سمت مقصد حرکت می کند. تکه های IP در گیرنده مجدداً بازسازی می شوند. باید توجه داشت که هیچ گاه در یک مسیر یاب میانی عملیات بازسازی انجام نمی شود. علیرغم این که ممکن است شبکه های میانی دارای اندازه MTU بزرگتر از اندازه تکه باشند، تکه ها در بسته هایی با اندازه کوچک حمل می شوند که در نتیجه باعث کاهش بازدهی پروتکل می شود. همچنین باید توجه داشت که تکه سازی زیاد منجر به ترافیک زیاد شبکه می شود.

اگر یک تکه گم شود، امکان بازسازی بسته اصلی نبوده و علیرغم انتقال موفق تکه های باقیمانده، بسته اصلی باید حذف شود. در صورت از بین رفتن یک بسته، پروتکل های لایه بالا مانند TCP متوجه شده و درخواست ارسال مجدد بسته گم شده از مقصد را می نمایند. گیرنده بسته های IP بعد از دریافت اولین تکه، یک زمان سنج خاصی را که زمان سنج باز سازی نام دارد، راه اندازی می نماید. اگر این زمان سنج قبل از رسیدن سائرتکه ها تمام شود، گیرنده تکه های باقیمانده را حتی اگر به درستی دریافت شده اند، از بین می برد. با افزایش تعداد تکه ها، احتمال از دست دادن یک بسته IP نیز افزایش می یابد. هنگامی که زمان سنج باز سازی به اتمام می رسد، یک پیام ICMP خاص به فرستنده ارسال می شود تا بدینوسیله به گیرنده اعلام شود که زمان سنج بازسازی تمام شده است.

انجام عملیات بازسازی بسته های IP درگیرنده، با وجود مشکلاتی که در قبل توضیح داده شد، این مزیت عمده را در پی دارد که باعث ساده سازی مسیریابهای میانی شبکه می شود. مسیریابهای IP هیچگونه نگرانی درمورد انجام عملیات باز سازی و ذخیره کردن مجدد تکه های IP ندارند. اگر چندین شبکه با اندازه MTU کوچک وجود داشته باشند، از آنجاییکه بسته IP باز سازی شده قبل از عبور از یک شبکه با اندازه MTU کوچک باید مجدداً تکه سازی شود، بنابراین بازسازی مجدد تکه های IP در مسیریابهای میانی شبکه کاری بیهوده است.

۸-۳-۲-۷- فیلد زمان زندگی (TTL¹)

فیلد زمان زندگی که برحسب ثانیه اندازه گیری می شود، نشان دهنده حداکثر زمانی است که یک بسته IP می تواند در شبکه زنده بماند. در هر مسیریاب میانی، مقدار زمان لازم برای پردازش یک بسته از مقدار فیلد فوق کم می شود. هنگامی که فیلد فوق برابر با صفر می شود، زمان زندگی بسته به اتمام رسیده و بسته باید از بین برود. فیلد TTL دو وظیفه عمده زیر را انجام می دهد:

- زمان زندگی سگمنت های TCP را محدود می کند.
- به حلقه های مسیریابی داخل شبکه خاتمه می دهد.

هنگامی که مقدار فیلد TTL در یک بسته IP صفر می شود، یک پیام ICMP برای آگاهی از این حقیقت به مبدا فرستاده می شود. اگر چه TTL برحسب ثانیه اندازه گیری می شود، تخمین زدن دقیق زمان لازم برای عبور بسته های IP از یک مسیریاب شبکه کار مشکلی است. بدینمنظور، مسیریاب های شبکه باید زمانی را که بسته IP داخل مسیریاب شده یاد داشت نموده و از زمان خروج بسته از مسیریاب، کم نمایند. حاصل تفریق فوق برابر با زمان لازم برای پردازش بسته

¹ Time to Live

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۱

در مسیر یاب IP می باشد. چون پردازش فوق زمان بر می باشد، بنابراین بسیاری از مسیر یاب ها برای سادگی مقدار TTL را از ۱ کم می کنند. به خاطر این امر فیلد TTL نشان دهنده حداکثر تعداد پرش های مجاز یک بسته در شبکه می باشد. بعضی از پیاده سازی های قبلی پروتکل IP اشتباها مقدار TTL را ۱۶ می گرفتند. دلیل استفاده از عدد ۱۶ این است که عدد فوق برای پروتکل مسیریابی RIP نشان دهنده فاصله بی نهایت می باشد. سایر نکات مهم برای فیلد TTL به صورت زیر است:

- یک میزبان نباید یک بسته IP را با مقدار فیلد TTL برابر با ۰ بفرستد. همچنین یک میزبان نباید یک بسته را فقط به خاطر این که با TTL کمتر از ۲ دریافت شده حذف کند.
- پروتکل های لایه بالا می توانند از TTL برای پیاده سازی یک حوزه وسیع جستجو برای یک منبع اینترنت استفاده کنند.
- مقدار TTL باید حداقل برابر با قطر شبکه باشد. منظور از قطر شبکه، طولانی ترین مسیر ممکن از مبدا به مقصد است. البته در اکثر موارد مقدار منطقی TTL برابر با دو برابر قطر فوق تنظیم می شود.
- لایه IP باید ابزاری را برای لایه حمل فراهم کند تا بتوان فیلد TTL هر بسته ارسالی را تنظیم نمود. هنگامی که از یک مقدار TTL ثابت استفاده می شود، مقدار فوق باید قابل پیکره بندی باشد. متأسفانه خیلی از پیاده سازی ها، قادر به تعیین مقدار اولیه TTL نبوده و از مقدار پیش فرض ۳۲ یا ۶۴ استفاده می نمایند.

۸-۳-۲-۸- فیلد پروتکل

فیلد پروتکل برای مشخص کردن پروتکل لایه بالایی که باید داده های موجود در بسته IP را دریافت کند، استفاده می شود. به عبارت دیگر از این فیلد برای تسهیم سازی و غیر تسهیم سازی داده به پروتکل های لایه بالا استفاده می شود. به عنوان مثال مقدار فیلد پروتکل برای پروتکل TCP برابر با ۶ است. این مقدار برای UDP برابر با ۱۷ و برای ICMP برابر با ۱ است. هنگامیکه پروتکل IP در سمت گیرنده متوجه شد که مقدار فیلد فوق در بسته دریافتی برابر با ۶ است، می فهمد که داده های موجود در بسته IP متعلق به پروتکل TCP بوده و باید به ماژول TCP تحویل داده شود. به طور مشابه هنگامیکه IP می بیند مقدار فیلد پروتکل ۱ است، می فهمد که این بسته باید به ماژول ICMP تحویل داده شود.

۸-۳-۲-۹- فیلد مجموع مقابله ای سرآیند^۱

این فیلد فقط برای بررسی خطای احتمالی در سرآیند IP استفاده می شود. مکمل ۱ تمام مقادیر ۱۶ بیتی موجود در سرآیند IP با هم جمع می شود (بجز خود فیلد مجموع مقابله ای سرآیند)، سپس مکمل ۱ مجموع حساب می شود. مقدار حاصل جمع فوق، برابر با مقدار مجموع مقابله ای سرآیند بوده و در فیلد مناسب قرار می گیرد. از آنجاییکه فیلد TTL در هر مسیر یاب کاهش می یابد و باعث تغییرات در سرآیند IP می شود، بنابراین مقدار سرآیند در هر مسیر یاب تغییر کرده و این باعث می شود که مقدار مجموع مقابله ای در هر مسیر یاب دوباره حساب شود. شواهد نشان می دهد که این مکانیزم در تشخیص خطاهای انتقال بسته مناسب است.

۸-۳-۲-۱۰- آدرس های IP مبدا و مقصد

^۱ Cheak sum

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۲

آدرس IP مبدا و آدرس IP مقصد، آدرس های IP ۳۲ بیتی نودهای مبدا و مقصد هستند. از آنجاییکه شبکه های IP از نوع بدون اتصال می باشند، هر بسته به صورت مستقل پردازش و مسیریابی شده و بنابراین نیاز است که در هر بسته IP مقادیر آدرس های IP مبدا و مقصد موجود باشند. مسیریاب ها از مقدار آدرس IP مقصد برای انجام مسیریابی هر بسته IP استفاده می کنند.

۸-۳-۳-۱۱- فیلد های گزینه و padding

از فیلد گزینه برای فراهم سازی برخی امکانات اضافی در پروتکل IP استفاده می شود. فیلد گزینه دارای طول متغیر می باشد. با توجه به اینکه طول سرآیند بسته های IP حتما باید مضربی از ۳۲ بیت باشد، فیلد padding در انتهای گزینه قرار دارد. چنانچه طول فیلد گزینه مضربی از ۴ بایت نبود، به مقدار کافی در ناحیه padding بیت صفر اضافه می شود تا فیلد گزینه مضربی از ۳۲ بیت باشد. در صورتیکه فیلد گزینه مضربی از ۳۲ بیت باشد، نیازی به فیلد padding وجود ندارد. در ادامه به بررسی گزینه های مهم IP می پردازیم.

۸-۳-۳-۳- گزینه های IP^۱

پروتکل IP دارای یکسری امکانات اضافی برای انجام برخی عملیات اختیاری می باشد. از آنجاییکه این امکانات اختیاری بوده و الزامی در استفاده آنها نمی باشد، با عنوان گزینه های IP شناخته می شوند. گزینه های IP به شرح زیر است :

- امنیت
- ثبت مسیر
- مسیریابی مبدا دقیق^۲
- مسیریابی مبدا ضعیف^۳
- برچسب زمانی اینترنت

همه نودهای شبکه IP باید قادر به پردازش و حمایت از گزینه های IP باشند. این گزینه هادرانتهای سرآیند IP ظاهر می شوند. برای مثال در محیط هایی که به امنیت بالا نیاز دارند، ممکن است گزینه امنیت در همه بسته های IP لازم باشد. طول فیلد گزینه متغیر است و باید مضربی از کلمات ۳۲ بیتی باشند. در صورت لزوم، می توان از مقادیر پرکننده صفر برای رساندن طول گزینه به ضرب ۳۲ بیت استفاده نمود. دو قالب برای مقادیر گزینه IP وجود دارند. قالب اول فقط شامل یک بایت منفرد از گزینه می باشد. قالب دوم گزینه، شامل یک بایت نوع گزینه، یک بایت طول گزینه و بایت های داده گزینه، می باشد. بایت طول گزینه دربرگیرنده اندازه همه اجزای گزینه شامل فیلد های نوع گزینه ، طول گزینه و داده گزینه می باشد.

بایت نوع گزینه ، اولین بایت موجود در گزینه است که از آن برای تعیین نوع گزینه استفاده می شود. فیلد نوع گزینه شامل سه فیلد زیر می شود:

- پرچم کپی شده (۱ بیت)
- کلاس گزینه (۲ بیت)
- شماره گزینه (۵ بیت)

^۱ IP Options

^۲ Strict Source Routing

^۳ Loose Source Routing

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

پرچم کپی شده، نحوه پردازش فیلد گزینه درهنگام عملیات تکه سازی درمسیریاب ها را کنترل می کند. چنانچه این پرچم ۱ باشد، بدان معنی است که گزینه ها باید در همه تکه های بسته IP کپی شود. هنگامی که پرچم فوق صفر باشد، بیانگر آن است که گزینه ها باید دراولین تکه IP و نه در همه تکه های بسته IP کپی شوند. فیلد کلاس گزینه دو بیت طول دارد و می تواند مقداری از صفر تا سه داشته باشد. کد ۰ به منظور کنترل شبکه و کد ۲ برای اشکال زدایی واندازه گیری به کار می رود. کد ۱ و ۳ برای استفاده های آتی رزرو شده است. فیلد کلاس برای مشخص کردن نوع کلاس گزینه استفاده می شود. گزینه های مختلفی برای عملیات کنترل شبکه و اشکال زدایی استفاده می شوند. فیلد شماره گزینه ۵ بیت طول دارد و به وسیله آن می توان حداکثر ۳۲ گزینه را برای کلاس گزینه داده شده تعیین نمود. جدول (۸-۷) گزینه های مختلف تعریف شده را فهرست کرده است.

جدول (۸-۷): گزینه های مختلف IP

طول گزینه	شماره گزینه	کلاس گزینه	پرچم کپی شده	مقدار	نام اختصاری گزینه	توصیف گزینه
—	۰	۰	۰	۰	EOOL	انتهای لیست گزینه: این گزینه فقط ۱ بیت را اشغال نموده و بایت طول ندارد. هنگامی که گزینه ها در انتهای سرآیند اتمام نیابند، از این گزینه استفاده می شود.
—	۱	۰	۰	۱	NOP	بدون عملکرد: این گزینه فقط ۱ بیت اشغال نموده و بایت طول ندارد. برای همتراز کردن بایتها در یک لیست گزینه ها استفاده می شود.
۱۱	۲	۰	۱	۱۳۰	SEC	امنیت اصلی: برای حمل اطلاعات مربوط به امنیت شبکه استفاده می شود.
متغیر	۳	۰	۱	۱۳۱	LSR	مسیریابی مبدا ضعیف: برای مسیریابی بسته IP براساس مسیرهیه شده به وسیله مبدا استفاده می شود.
متغیر	۵	۰	۱	۱۳۳	E-SEC	امنیت توسعه یافته: برای مشخص کردن امنیت اضافی استفاده می شود
متغیر	۷	۰	۰	۷	RR	ثبت مسیر: برای ردیابی مسیری که بسته IP طی می کند، استفاده می شود
۴	۸	۰	۱	۱۳۶	SID	در پروتکل Stream IP استفاده شده و هم اکنون غیر مستعمل است.
متغیر	۹	۰	۱	۱۳۷	SSR	مسیر یابی مبدادقیق: برای مسیریابی بسته IP به کمک مسیرهتعیین شده توسط مبدا استفاده می شود.
متغیر	۴	۲	۰	۶۸	TS	برچسب زمانی اینترنت: برای ثبت برچسب های زمانی در طی مسیر ارسال بسته استفاده می شود. این گزینه در کلاس اندازه گیری و اشکال زدایی تعریف شده است

بخش های بعدی انواع مختلف گزینه IP را با جزئیات بیشتر توضیح می دهد :

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

۸-۳-۳-۱- انتهای لیست گزینه و گزینه های بدون عملکرد

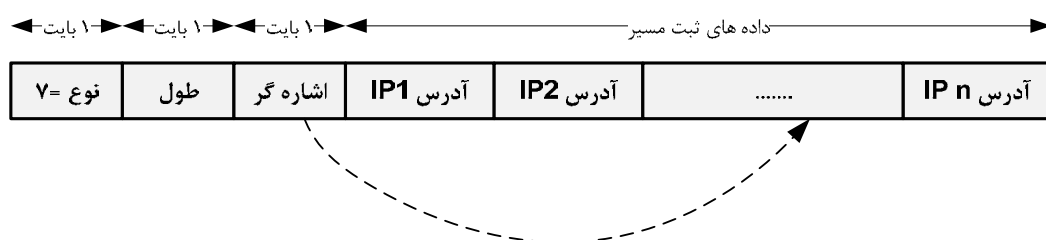
تنها گزینه های تک بایتی، گزینه های انتهای لیست گزینه و گزینه بدون عملکرد می باشند. انتهای لیست گزینه، یک گزینه تک بایتی حاوی بیت های صفر است. این گزینه، انتهای لیست گزینه را نشان می دهد. این گزینه در انتهای لیست همه گزینه ها و نه در انتهای هر گزینه استفاده می شود. گزینه فوق، در صورتی که انتهای گزینه ها از جهات دیگر در مرز ۳۲ بیت نباشد، مورد نیاز است. گزینه بدون عملکرد بین گزینه ها استفاده شده و ابتدای یک گزینه بعدی را در یک مرز ۳۲ بیتی همتراز می کند.

۸-۳-۳-۲- گزینه امنیت

گزینه امنیت راهی را برای فراهم سازی امنیت برای میزبان ها مهیا می سازد. دو نوع گزینه امنیت وجود دارد که عبارتند از: امنیت پایه و امنیت توسعه داده شده. امنیت پایه برای مشخص کردن سطح امنیت، سمت های محرمانه، غیر دسته بندی شده سری و غیره استفاده می شود. امنیت توسعه داده شده برای معین کردن امنیت اضافی در یک سازمان نظامی استفاده می گردد.

۸-۳-۳-۳- گزینه ثبت مسیر

گزینه ثبت مسیر توسط فرستنده استفاده می شود و برای ثبت آدرس IP مسیر یاب هایی که بسته IP را به مقصد پیش می برند، استفاده می شود. در این گزینه، لیست مسیر یاب هایی که بسته از آنها عبور کرده است، ثبت می شود. مطابق با شکل (۸-۱۶)، گزینه ثبت مسیر با مقدار کد نوع گزینه ۱۳۱ شروع می شود. بایت دوم، طول گزینه است. سومین بایت موجود در گزینه فوق، بایت اشاره گر می باشد. این فیلد اشاره کننده به محلی است که باید نود دریافت کننده این گزینه، آدرس IP خود را در آن محل قرار دهد. کوچکترین مقدار اشاره گر ۴ است. اگر مقدار اشاره گر بزرگتر از فیلد طول گزینه باشد، محل خالی در فیلد ثبت داده وجود ندارد. به عبارت دیگر فیلد ثبت داده پر شده است. اگر لیست ثبت داده پر باشد، مسیر یاب بدون این که آدرس IP خودش را در لیست درج کند بسته را پیش می برد.



شکل (۸-۱۶): ساختار گزینه ثبت مسیر

اگر اشاره گر بزرگتر از طول گزینه نباشد، لیست ثبت داده پر نیست و محل های خالی در دسترس می باشد. مسیر یاب، آدرس IP خود را در مکانی که توسط فیلد اشاره گر مشخص می شود، درج نموده و مقدار فیلد اشاره گر را ۴ واحد که اندازه آدرس IP است افزایش می دهد. آدرس ثبت شده، آدرس IP واسط شبکه مسیر یابی است که از طریق آن باید این بسته پیش برده شود. هم فرستنده و هم گیرنده باید با استفاده و پردازش اطلاعات ثبت مسیر موافق باشند. فرستنده، گزینه ثبت مسیر و فضای کافی برای ثبت آدرس های IP مسیر یاب های میانی را به بسته IP اضافه می کند. گیرنده با پردازش لیست آدرس

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

های IP ثبت شده در فیلد ثبت داده، اطلاعات مفیدی از مسیر یاب های موجود در شبکه بدست می آورد. اگر گیرنده با پردازش داده های ثبت مسیر موافق نباشد، این اطلاعات توسط گیرنده نادیده گرفته می شود.

در شبکه های IP دوتنوع متفاوت از مسیریابی وجود دارد. مسیریابی پرش به پرش و مسیریابی مبدا. در مسیریابی پرش به پرش، در هر نود عملیات مسیریابی انجام شده و بهترین پرش بعدی برای تحویل بسته به مقصد تعیین می شود. سپس بسته برای رسیدن به مقصد نهایی، تحویل پرش بعدی می شود. این عملیات در همه پرش های بعدی انجام می شود تا نهایتا بسته به مقصد برسد. در مسیریابی مبدا، فرستنده کل مسیر یا بخشی از مسیری که باید بسته آن را طی نموده تا به مقصد برسد را تعیین می کند. به عبارت دیگر در مسیریابی مبدا، فرستنده مسیری را که بسته باید در رسیدن به مقصد دنبال کند دیکته می کند.

برای آزمایش یک مسیر خاص هنگامی که میدانیم مسیریاب ها معمولا آن مسیر را انتخاب نمی کنند، استفاده از گزینه مسیریابی مبدا بسیار مفید می باشد. همچنین این گزینه این انعطاف پذیری را ارائه می کند که بسته ها را از طریق شبکه هایی با اطمینان بالا مسیریابی نماییم. توپولوژی و مسیر واقعی که یک بسته IP در یک شبکه پیچیده باید دنبال کند، ممکن است به سادگی مشخص نشود و این مسئله یکی از نقاط ضعف این روش می باشد. دو نوع مسیریابی مبدا وجود دارد که عبارتند از مسیریابی مبدا دقیق و مسیریابی مبدا ضعیف.

در گزینه مسیریابی مبدا دقیق که در شکل (۸-۱۷) نشان داده شده است، فرستنده رشته ای از آدرس های IP نودهایی را که باید دقیقا در پیش بردن بسته از آنها استفاده شود، را همراه بسته ارسال می نماید. مسیر بین دو آدرس IP متوالی موجود در لیست مسیریابی مبدا، فقط می تواند شامل یک شبکه فیزیکی خاص باشد و امکان وجود نودهای میانی بین آنها وجود ندارد. اگر مسیر یاب های میانی نتوانند مسیر تعیین شده توسط این گزینه را دقیقا دنبال کنند، بسته حذف می شود.



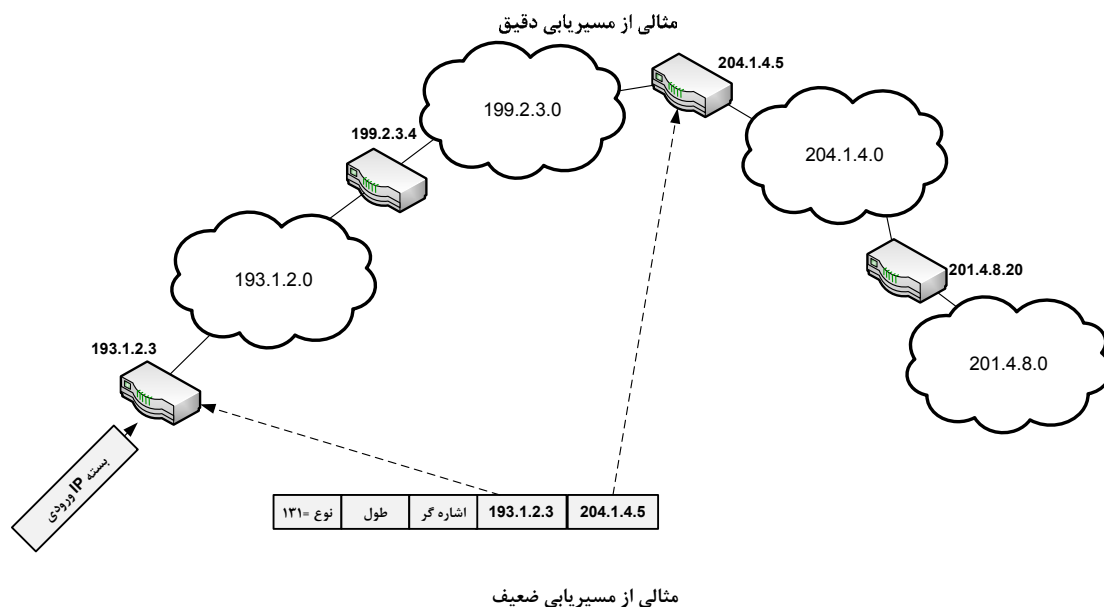
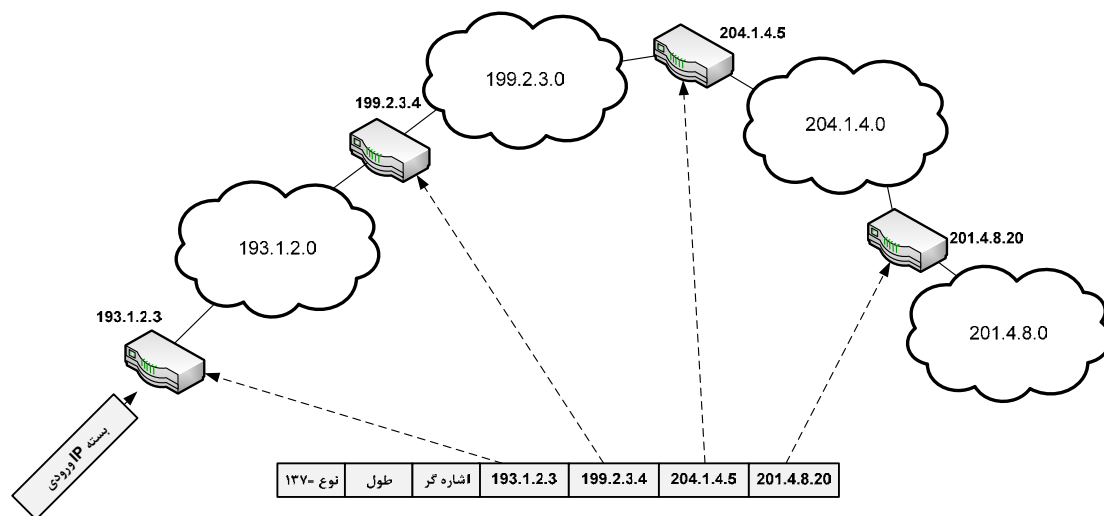
شکل (۸-۱۷): ساختار مسیریابی مبدا دقیق

مطابق با شکل (۸-۱۸)، در مسیریابی مبدا ضعیف، فرستنده رشته ای از آدرس های IP نودهایی را که باید در پیش بردن یک بسته دنبال شوند، در پیام ارسالی اضافه می نماید. برخلاف مسیریابی مبدا دقیق، در مسیریابی مبدا ضعیف، ممکن است مسیر بین دو آدرس IP متوالی شامل هر تعداد مسیریاب باشد. شکل (۸-۱۹) مقایسه بین مسیریابی مبدا دقیق و ضعیف را نشان می دهد.



شکل (۸-۱۸): ساختار مسیریابی مبدا ضعیف

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

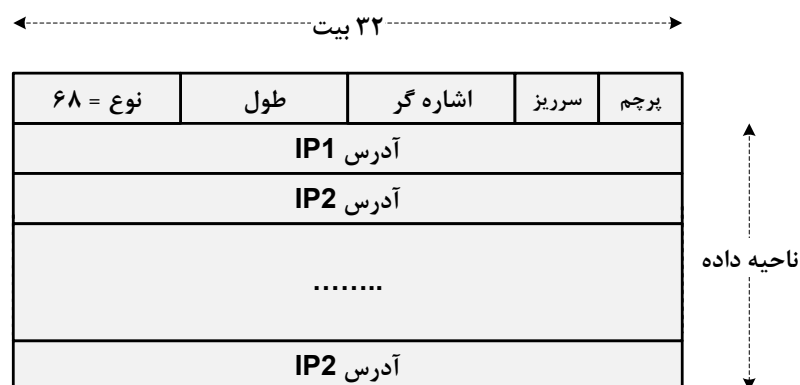


شکل (۸-۱۹): مقایسه مسیریابی مبدا دقیق و مسیریابی مبدا ضعیف

۸-۳-۴- برچسب زمانی اینترنت

از این گزینه برای ثبت زمان دریافت هر بسته IP در مسیریاب های درون شبکه استفاده می شود. چنانچه بخواهیم که زمان دریافت هر بسته و همچنین آدرس مسیریاب هایی که بسته IP را دریافت می کنند را داشته باشیم، از این گزینه استفاده می کنیم. برچسب های زمانی برحسب تعداد میلی ثانیه های گذشته از نیمه شب طبق ساعت UTC اندازه گیری می شود. UTC سابقاً GMT نامیده می شد و زمان صفر درجه طولی است. شکل (۸-۲۰) قالب گزینه برچسب زمانی اینترنت را نشان میدهد.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۸-۲۰): ساختار گزینه بر چسب زمانی اینترنت

در گزینه برچسب زمانی اینترنت، فیلد نوع گزینه ۶۸ است. فیلد طول گزینه، تعداد کل بایت های موجود در گزینه را نشان می دهد. هر ورودی در فیلد داده گزینه، شامل دو مقدار ۳۲ بیتی آدرس IP مسیریاب و برچسب زمانی، می باشد. بایت طول، مقدار فضای رزرو شده برای آدرس های IP و برچسب های زمانی را در فیلد داده مشخص می کند. فیلد اشاره گر، محل خالی بعدی برای قراردادن مقدار آدرس IP و برچسب زمانی نود فعلی می باشد. کمترین مقدار فیلد اشاره گر ۵ است. هنگامی که مقدار اشاره گر بزرگتر از مقدار فیلد طول است، ناحیه برچسب زمانی پر شده است. فیلد سرریز ۴ بیت طول دارد و نشان دهنده تعداد مسیریاب هایی است که به دلیل کوچکی زیاد فیلد داده، نمی توانند برچسب زمانی را در ناحیه مربوطه قرار دهند. حداکثر مقدار فیلد سرریز ۱۵ است. اگر فضای کافی برای درج یک برچسب زمانی کامل در ناحیه داده وجود نداشته باشد و یا شماره سرریز از ۱۵ تجاوز کند، بسته IP اشتباه در نظر گرفته شده و حذف می شود. در این صورت یک پیام ICMP از نوع خطا در پارامتر، به فرستنده ارسال می شود. فیلد پرچم، قالب اطلاعات در فیلد داده را کنترل می کند.

۸-۴- پروتکل ICMP^۱

همانطور که در قبل اشاره شد، پروتکل اینترنت از نوع بدون اتصال و بدون گارانتی می باشد. بنابراین پروتکل IP سعی نمی کند تا تحویل مطمئن بسته ها را ضمانت کند بلکه این کار را به پروتکل های لایه بالا مانند پروتکل TCP واگذار می نماید. با این وجود، IP امکاناتی را برای ارسال پیام های هشدار و تشخیص عیب از طریق پروتکل ICMP فراهم می سازد. مدیر شبکه می تواند از این پیام ها در تشخیص مشکلات احتمالی شبکه استفاده کند. پروتکل ICMP توسط چندین RFC اینترنت توصیف شده است. این RFC ها عبارتند از: RFC 1122 و RFC 1191, RFC 1256, RFC792, RFC950, RFC 1812, RFC 1122.

به دلیل بدون اتصال و بدون تضمین بودن پروتکل IP، احتمال اینکه بسته های IP با خطا مواجه شوند زیاد است. در شبکه های IP، فرستنده بسته های IP را ارسال نموده و آنها را به زیرلایه های شبکه زیرین تحویل می دهد. فرستنده راهی برای دانستن مشکلات احتمالی که ممکن است در ارسال بسته رخ بدهد ندارد. معمولاً خطاها و مشکلات احتمالی موجود در بسته های IP در مسیریاب های میانی کشف و گزارش می شود. برخی از مشکلاتی که ممکن است در هنگام ارسال بسته های IP با آنها مواجه شویم عبارتند از:

- اتمام پارامتر زمان زندگی (TTL) در بسته به خاطر وجود حلقه مسیریابی در شبکه.

^۱ Internet Control Message Protocol

شبکه های کامپیوتری (دکتر محمد حسن یغمایی مقدم – دانشگاه فردوسی مشهد)

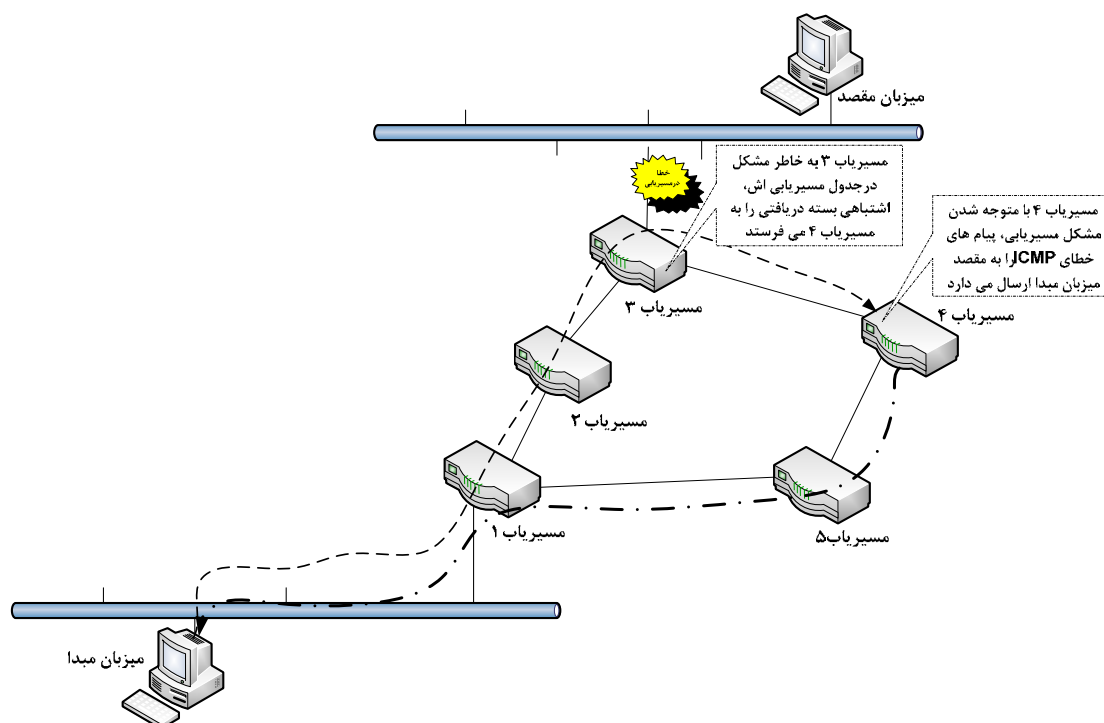
- عدم تحویل بسته به خاطر فقدان یک تکه از بسته .
 - در دسترس نبودن یک پروتکل ، سرویس یا میزبان خاص درمقصد.
 - عدم توانایی پیش بردن یک بسته به خاطر عدم اجازه تکه سازی.
 - وقوع ازدحام در یک مسیر یا شبکه.
- در هر یک از این موارد، از پروتکل ICMP برای هشدار دادن به فرستنده درباره مشکلات بوجود آمده فوق استفاده می شود. خود پروتکل IP هیچ مکانیزمی برای هشدار دادن به شبکه درباره این مشکلات ندارد، بلکه این پروتکل کمکی ICMP است که این کار را انجام می دهد. همه پیاده سازی های IP نیازمند به پشتیبانی ICMP هستند. بعضی از پیاده سازی های ICMP هنگام مواجهه با یک مشکل خاص پیامی ارسال نکرده درحالیکه برخی دیگر این کار را انجام می دهند. بنابراین در سطوح مختلفی از پیاده سازی پروتکل ICMP درنودهای شبکه وجود دارد.
- هم مسیر یا ب های میانی شبکه و هم میزبان های IP قادر به تولید و ارسال پیام های ICMP می باشند. مسیر یا ب های شبکه در هنگام مواجهه با مشکلاتی که باعث عدم توانایی آنها در پیش بردن بسته های دریافتی شود، اقدام به ارسال پیام های ICMP می نمایند. درحالیکه میزبان های شبکه، چنانچه با مشکلاتی نظیر عدم امکان تحویل بسته به پروتکل های لایه بالاتر مواجه شوند، بسته های ICMP ارسال می دارند. الزاما تمام بسته های ICMP برای گزارش مشکلات احتمالی در شبکه و یا میزبان های مقصد استفاده نمی شوند. برخی از پیام های ICMP برای عملیات خاص نظیر تست و جمع آوری اطلاعات از شبکه به کار می روند. بعضی از جنبه های مهم ICMP که باید از آن آگاه باشیم به شرح زیر است:
- همه پیاده سازی های IP نیز باید ICMP را پیاده سازی کنند.
 - ICMP در بالای IP اجرا می شود، یعنی ICMP یک سرویس گیرنده IP است حتی با این که ICMP در ماژول IP پیاده سازی می شود.
 - ICMP در هنگام تشخیص خطا به کار رفته و این بدین معنی نیست که قابلیت اطمینان پروتکل IP را افزایش داده است.
 - ICMP فقط در مورد اولین تکه بسته IP گزارش خطا را صادر می نماید. این تکه، تکه ای از بسته IP است که آفست تکه سازی آن ۰ است. مقصود از این کار پرهیز از ارسال پیام های ICMP برای هر یک از تکه های باقیمانده بسته است.
 - ICMP یک مکانیزم گزارش خطا برای بسته های IP است. ICMP پیام های خطا در مورد مشکلات بسته های خودش تولید نمی کند. به عبارت دیگر پیام های ICMP برای اعلام وقوع خطا برای خودشان استفاده نمی شوند.
- علاوه بر موارد فوق، پروتکل ICMP نباید در مورد مشکلات ایجاد شده ذیل پیامی ارسال دارد:
- مسیریابی یا تحویل پیام های ICMP: اگر پیام های خطای ICMP در مورد پروتکل ICMP تولید شوند، پیام ها به شدت زیاد شده و به ترافیک شبکه اضافه می شود.
 - همه پخشی یا چند پخشی بسته های IP: اگر پیام های خطای ICMP برای بسته های همه پخشی یا چند پخشی IP تولید شوند، هر نود دریافت کننده بسته همه پخشی / چند پخشی یک پیام ICMP را تولید می کند که این مسئله باعث افزایش ناگهانی ترافیک شبکه می شود.
 - همه پخشی یا چند پخشی لایه پیوند داده: اگر پیام های خطای ICMP برای بسته های همه پخشی یا چند پخشی لایه پیوند داده تولید شوند، هر نود دریافت کننده پیام های همه پخشی / چند پخشی یک پیام ICMP را تولید می کند و به ترافیک شبکه اضافه می شود.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

- بسته هایی با آدرس مبدهائی که یک نود IP یکتا را مشخص نمی کنند: برای بسته هایی که آدرس مبدا آنها آدرس های برگشت حلقه 127.x.x.x یا 0.0.0.0 یا آدرسی با پیشوند شبکه ۰ باشد، بسته های ICMP تولید نمی شود.

۸-۴-۱- تشخیص خطای ICMP

همان طور که در بخش پیش اشاره شد، ICMP یک مکانیزم گزارش خطا برای بسته های IP فراهم می آورد. پیام های خطای ICMP به مقصد فرستنده بسته IP ارسال می شوند. گیرنده بسته ICMP باید اقدام به عمل مقتضی برای رفع مشکل بوجود آمده نماید. به عنوان مثال شرایط شکل (۸-۲۱) را در نظر بگیرید که بسته ای از میزبان مبدا به میزبان مقصد فرستاده شده است و مسیری شامل مسیریاب های ۱، ۲ و ۳ را طی می کند.



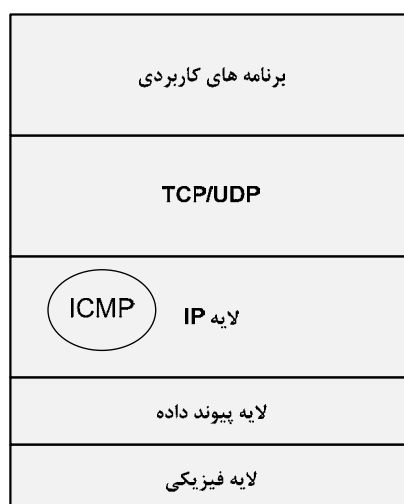
شکل (۸-۲۱): مثالی از کاربرد پیام ICMP

فرض کنید مسیریاب ۳ اطلاعات نادرستی درباره مقصد در جدول مسیریابی خود دارد و اشتباها به جای میزبان مقصد، بسته را به مسیریاب ۴ ارسال می کند. مسیریاب ۴ که متوجه وقوع خطا در شبکه شده است، یک پیام ICMP درباره مسیریابی نادرست به فرستنده پیام می فرستد. با توجه به اینکه پیام های ICMP فقط به مبدا تولید کننده بسته IP ارسال می شوند، بنابراین مسیریاب ۴ نمی تواند پیامی را به مسیریاب ۳ درباره دلیل مشکل فوق ارسال دارد. در این مثال، میزبان مبدا هیچ نقشی در خطای بوجود آمده نداشته است و بنابراین کاری برای رفع مشکل فوق نمی تواند انجام دهد. بنابراین سوالی که مطرح می شود این است که چرا ICMP محدود به ارسال پیام ها به مبدا اصلی است؟ جواب این است که سرآیند بسته های IP فقط دو فیلد آدرس شامل آدرس IP مبدا اصلی و آدرس IP مقصد نهایی را دارد. از آنجاییکه آدرس های IP مسیر یاب های میانی در فیلد سرآیند IP ثبت نمی شوند (مگر این که امکان ثبت مسیر IP توسط مبدا اصلی فعال شده باشد) بنابراین بسته های ICMP فقط باید برای مبدا اصلی ارسال می گردند. بنابراین در مثال فوق هنگامی که

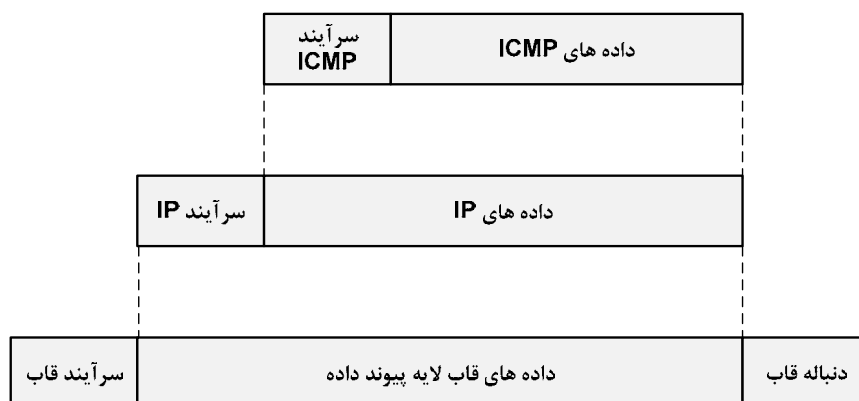
شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

مسیریاب ۴ می خواهد پیام ICMP را ارسال کند، فقط از آدرس های IP مبدا آغازین و مقصد نهایی آگاهی دارد و از مسیریاب های میانی که بسته را پردازش نموده اند اطلاعی ندارد. بنابراین نمی تواند پیام ICMP را به آنها بفرستد. با توجه به شرایط پیش آمده در این مثال، منطقی نیست که مسیریاب R4 بسته ICMP را به مقصد اصلی بفرستد چون به احتمال زیاد بسته اصلی مشکلی درون شبکه برای رسیدن به مقصد داشته است. همچنین مقصد اصلی در ایجاد مشکل فوق نقشی نداشته است و دلیل مشکل اخیر نیست بلکه دلیل مشکل مبدأ یا یکی از مسیریاب های میانی است. بنابراین ارسال پیام ICMP به مبدا تنها انتخاب منطقی است. به هر حال ارسال پیام ICMP به مبدا از اصلا نفرستادن هیچ پیامی بهتر است.

از آنجاییکه پیام های ICMP باید در اینترنت توسط مسیریاب ها حمل شوند، باید این پیام ها را توسط پروتکل IP بسته بندی نمود. به این معنی که پیام ICMP در بخش داده بسته IP گنجانده می شود. ماژول IP دریافت کننده داده، بسته IP را براساس مقدار فیلد پروتکل غیرتسهیم سازی نموده و آن را به ماژول ICMP می فرستد. شکل (۸-۲۲) لایه بندی پروتکل ICMP و IP را نشان می دهد. همچنین نشان می دهد که ماژول ICMP به عنوان قسمتی از ماژول IP پیاده سازی شده است. شکل (۸-۲۳) بسته بندی ICMP را داخل یک سرآیند IP نشان می دهد.



شکل (۸-۲۲): ارتباط ICMP و IP



شکل (۸-۲۳): بسته بندی ICMP

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)^۲

باتوجه به شکل (۸-۲۲) می توان فهمید که حتی با اینکه پیام ICMP توسط IP بسته بندی شده است، ICMP به عنوان یک پروتکل لایه بالا در نظر گرفته نمی شود بلکه یک بخش مورد نیاز پروتکل IP است. از پروتکل ICMP می توان برای ساخت کاربردهایی با مقصود خاص و ابزارهای تشخیصی استفاده نمود. این کاربرد های خاص را می توان به عنوان بخشی از لایه کاربرد در نظر گرفت. امکان PING، مثال خوبی از ابزارهای تشخیصی که از پروتکل ICMP استفاده می کنند، می باشد. این قابلیت در بسیاری از سیستم های TCP/IP در دسترس می باشد. امکان PING برای ارسال یک پیام درخواست echo به یک مقصد خاص استفاده می شود. اگر پیام درخواست echo به یک ماژول IP برسد، آن ماژول مجبور به ارسال یک پیام پاسخ echo است. با دریافت پیام پاسخ echo، فرستنده پیام متوجه می شود که نود IP مورد دسترس است.

سرآیند IP هیچ اولویت خاصی را برای تحویل پیام های ICMP مشخص نکرده است، بنابراین نود های IP با بسته های IP که دربرگیرنده پیام های ICMP هستند، با یک حالت عادی مانند هر بسته دیگری رفتار می کنند. چون IP تحویل پیام ها را ضمانت نمی کند، ممکن است پیام های ICMP گم شده و یا به خاطر ازدحام درمسیریاب های میانی حذف شوند. اگر درپردازش بسته های IP که شامل پیام های ICMP هستند با خطا مواجه شویم، هیچ پیام ICMP تولید نمی شود.

۸-۴-۲- سرویس های ICMP

پروتکل ICMP سرویس های متنوع زیر را تامین می نماید:

- echo: به عنوان یک تشخیص برای تعیین کردن دسترس پذیری به یک نود IP بکار می رود.
- غیرقابل دسترس بودن مقصد: برای اعلام غیر قابل دسترس بودن نود IP مقصد به کار می رود.
- فرو نشاندن مبدا^۱: برای نشان دادن مشکل ازدحام در شبکه و درخواست از مبدا برای کاهش سرعت ارسال به کار می رود.
- تغییرمسیر^۲: بوسیله مسیر یاب های میانی شبکه برای آگاهی دادن از وجود یک مسیر جایگزین استفاده می شود.
- تخطی زمانی^۳: برای اعلام صفرشدن مقدار فیلد TTL سرآیند IP به کار می رود.
- مشکل پارامتر^۴: برای نشان دادن یک مشکل در یکی از پارامترهای بسته IP به کار می رود.
- برچسب زمانی^۵: برای اندازه گیری زمان در اینترنت استفاده میشود.
- پوشش آدرس^۶: برای به دست آوردن اطلاعات پوشش زیر شبکه استفاده می شود.

۸-۴-۳- ساختار پیام های ICMP

ساختار پیام های ICMP در شکل (۸-۲۴) نشان داده شده اند. اولین بایت در سرآیند ICMP فیلد نوع می باشد که نشان دهنده نوع سرویس ICMP است. بایت بعدی فیلد کد است که بیشتر طبیعت نوع پیام را توصیف می کند. هم مقدار فیلد نوع و هم مقدار فیلد کد باید برای تعیین نوع پیام ICMP ارسالی در نظر گرفته می شوند.

¹ source quench

² redirect

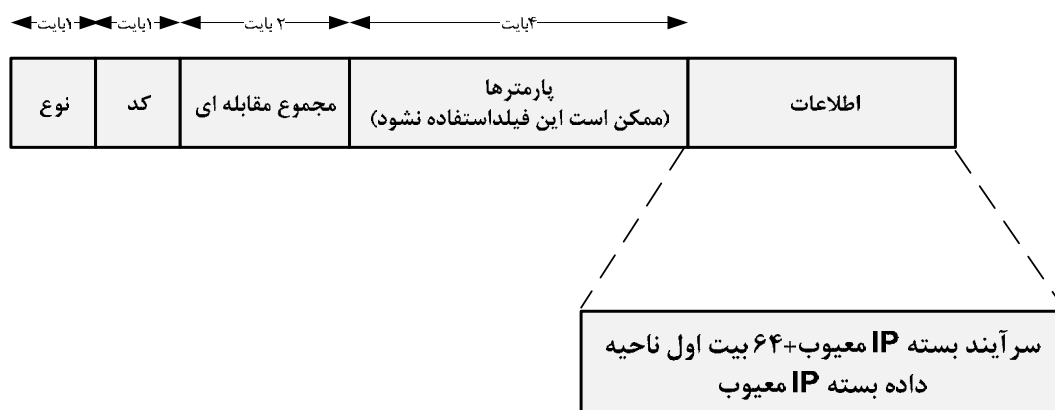
³ time exceeded

⁴ parameter problem

⁵ time stamp

⁶ address mask

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد) ۲۳



شکل (۸-۲۴): ساختار کلی پیام ICMP

جدول (۸-۸) مقادیر مختلف فیلد نوع ICMP را نشان می دهد. همچنین جدول (۸-۱۰) مقدار کد انتساب داده شده متعلق به نوع را نشان می دهد. بعضی از مقادیر نوع به پروتکل های آزمایشی انتساب داده شده اند و مقدار کد آنها لیست نشده است.

جدول (۸-۸): مقادیر نوع ICMP

مقدار فیلد نوع	توصیف
۰	پاسخ Echo
۱، ۲، ۳، ۴، ۵، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۲، ۱۳، ۱۴، ۱۵، ۱۶، ۱۷، ۱۸، ۱۹، ۲۰، ۲۱، ۲۲، ۲۳، ۲۴، ۲۵، ۲۶، ۲۷، ۲۸، ۲۹، ۳۰، ۳۱، ۳۲، ۳۳	انتساب داده نشده است
۲	انتساب داده نشده
۳	مقصد غیر قابل دسترس است
۴	فرو نشانیدن مبدا
۵	تغییر مسیر
۶	آدرس میزبان جایگزین
۸	درخواست Echo
۹	اعلان مسیریاب
۱۰	انتخاب مسیریاب
۱۱	تخطی از زمان
۱۲	مشکل پارامتر
۱۳	درخواست برچسب زمانی
۱۴	پاسخ برچسب زمانی
۱۵	درخواست اطلاعات
۱۶	پاسخ اطلاعات
۱۷	درخواست پوشش آدرس
۱۸	پاسخ پوشش آدرس
۱۹	رزرو شده برای کاربردهای امنیتی
۲۰-۲۹	رزرو شده برای کاربردهای آزمایشی
۳۰	ردیابی مسیر
۳۱	خطای ازدحام بسته
۳۲	تغییر مسیر میزبان قابل حمل
۳۳	IPv6 Where- Are- You

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

۳۴	IPV6 I- Am – Here
۳۵	درخواست ثبت قابل حمل
۳۶	پاسخ ثبت قابل حمل

جدول (۸-۱۰): فیلدهای کد ICMP

نوع	کدها	توصیف
۰ (پاسخ echo)	-	کد ندارد
۲۵۵-۱۰۲۰۷۰۳۷	-	انتساب داده نشده است
۳ (غیر قابل دسترس بودن مقصد)	۰	شبکه غیر قابل دسترس است
	۱	میزبان غیر قابل دسترس است
	۲	پروتکل غیر قابل دسترس است
	۳	درگاه غیر قابل دسترس است
	۴	تکه سازی مورد نیاز است ولی پرچم DF ۱ است
	۵	مسیریابی مبدا ناموفق
	۶	شبکه مقصد ناشناخته است
	۷	میزبان مقصد ناشناخته است
	۸	میزبان مبدا جدا شده است
	۹	ارتباط با شبکه مقصد از جانب مدیریت ممنوع شده است
۴ (فرو نشانندن مبدا)	۱۰	ارتباط با میزبان مقصد از جانب مدیریت ممنوع شده است
	۱۱	شبکه مقصد برای نوع سرویس درخواستی غیر قابل دسترس است
	۱۲	میزبان مقصد برای نوع سرویس درخواستی غیر قابل دسترس است
	-	کد ندارد
۵ (تغییر مسیر)	۰	تغییر مسیر بسته به خاطر شبکه (یا زیر شبکه)
	۱	تغییر مسیر بسته به خاطر میزبان
	۲	تغییر مسیر بسته به خاطر نوع سرویس و شبکه
	۳	تغییر مسیر بسته به خاطر نوع سرویس و میزبان
۶ (آدرس جایگزین میزبان)	۰	آدرس جایگزین برای میزبان
۸ (پاسخ Echo)	-	کد ندارد
۹ (اعلان مسیریابی)	-	کد ندارد
۱۰ (انتخاب مسیریاب)	-	کد ندارد
۱۱ (تخطی از زمان)	۰	زمان زندگی بسته برای عبور از شبکه اتمام یافته است
	۱	زمان بازسازی تکه های بسته IP درمقصد اتمام یافته است
۱۲ (مشکل پارامتر)	۰	اشاره گر خطا را نشان می دهد
	۱	گم شدن یک امکان مورد نیاز
	۲	طول بد
۱۳ (برچسب زمانی)	-	کد ندارد
۱۴ (پاسخ برچسب زمانی)	-	کد ندارد
۱۵ (درخواست اطلاعات)	-	کد ندارد
۱۶ (پاسخ اطلاعات)	-	کد ندارد
۱۷ (درخواست پوشش آدرس)	-	کد ندارد
۱۸ (پاسخ پوشش آدرس)	-	کد ندارد

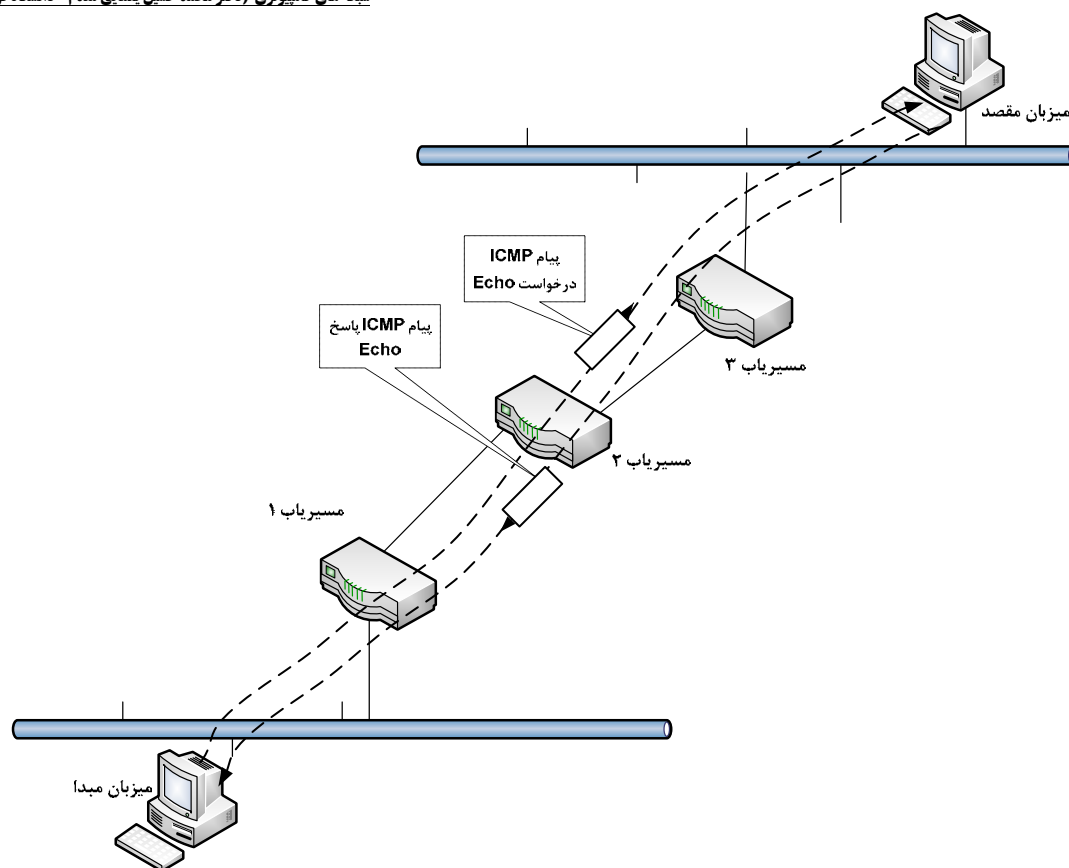
شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

دو بایت بعدی فیلد مجموع مقابله است که برای بررسی خطا در بسته ICMP به کار می رود. فیلد بررسی خطای فوق فقط شامل پیام ICMP بوده و سرآیند بسته IP را دربرنمی گیرد. الگوریتم بررسی خطا همان الگوریتم بررسی خطای است که برای پروتکل IP استفاده می شود. ۴ بایت بعدی شامل پارامترهای اختیاری است. پارامترهای واقعی مورد استفاده به پیام ICMP بستگی دارد. این فیلد اختیاری است و ممکن است بعضی از انواع پیام های ICMP آن را در بر نداشته باشند. فیلد اطلاعات، شامل سرآیند IP بسته معیوب به علاوه ۶۴ بیت از داده پروتکل لایه بالا موجود در بخش داده بسته IP معیوب می باشد. اطلاعات فوق برای مبدا ارسال کننده پیام بسیار مفید است و به کمک آن می تواند دلیل و نوع مشکل بوجود آمده را بفهمد. دلیل گنجاندن سرآیند بسته IP معیوب در پیام های ICMP این است که بتوان آدرس IP مقصد و مبدا فرستنده بسته را تعیین کرد. این آدرس ها بیان می کنند که بسته را کی و به کجا فرستاده است؟ ۶۴ بیت داده لایه بالا شامل قسمتی از سرآیند TCP یا همه سرآیند UDP می باشد. ۸ بایت اول سرآیند TCP شامل شماره درگاه های مقصد و مبدا و فیلد شماره ترتیب هستند. همانطور که در فصل های بعدی اشاره خواهد شد، شماره های درگاه نوع برنامه های کاربردی لایه بالا را مشخص می نمایند. از طرف دیگر اگر UDP به عنوان پروتکل لایه انتقال استفاده شود چون اندازه سرآیند UDP فقط ۸ بایت است، همه سرآیند UDP گزارش می شود. در ادامه به توصیف برخی از مهمترین پیام های ICMP می پردازیم.

۸-۴-۳-۱- پیام ICMP Echo

یکی از پر استفاده ترین پیام های ICMP، پیام فوق echo می باشد. ابزار PING که در اغلب سیستم های TCP/IP در دسترس است برای مقاصد تشخیصی خود از پیام فوق استفاده می کند. با استفاده از امکان PING قابل دسترس بودن یک نود IP خاص بررسی می شود؟ با کمک امکان PING یک پیام درخواست ICMP Echo با مقدار فیلد نوع برابر با ۸ به یک نود IP خاص ارسال می شود. نود IP با دریافت این پیام، یک پیام پاسخ ICMP Echo با فیلد نوع برابر با ۰ را به فرستنده ارسال می دارد. در پیام پاسخ Echo، یک کپی از داده های فرستاده شده در پیام درخواست Echo موجود می باشد. با دریافت موفق پیام پاسخ Echo مشخص می شود که لایه IP ولایه های پائین تر آن در سیستم انتقال بین مبدا و مقصد درست کار می کنند. اگر بین مبدا و مقصد هر تعداد مسیر یاب میانی وجود داشته باشد، با دریافت پیام پاسخ Echo مشخص می شود که مسیر یاب های فوق قادر به مسیر یابی بین مبدا و مقصد هستند. نود IP ای با کمک امکان PING در دسترس بودن آن بررسی می شود، یک میزبان یا یک مسیر یاب می باشد. شکل (۸-۲۵) مثالی از چگونگی عملکرد PING را نشان می دهد.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۸-۲۵): استفاده از پیام های درخواست / پاسخ ICMP Echo

۸-۴-۳-۲- ICMP در دسترس نبودن مقصد

همانطور که قبلاً گفته شد، شبکه IP یک سرویس بهترین تلاش را فراهم می کند. این امکان وجود دارد که پروتکل IP قادر به تحویل بسته IP به مقصد نباشد. عدم تحویل بسته ها، معمولاً به وسیله مسیریاب های شبکه شناسایی می شود. هنگامی که یک مسیریاب قادر به تحویل بسته به مقصد نباشد، یک پیام ICMP در دسترس نبودن مقصد را به فرستنده ارسال می دارد. پیام ICMP ارسالی فوق، فرستنده را از دلیل تحویل ناموفق آگاه کند. در این پیام، مقدار فیلد نوع ۳ است که نشان می دهد این یک پیام ICMP از نوع در دسترس نبودن مقصد است. فیلد کد، اطلاعات بیشتری را در مورد این که چرا مقصد در دسترس نیست می دهد. مقادیر فیلد کد در جدول (۸-۱۰) لیست شده بودند. در ادامه به بررسی مفهوم هریک از مقادیر فیلد کد آورده شده در جدول فوق می پردازیم.

هنگامی که شبکه مشخص شده در آدرس مقصد IP قابل دسترس نباشد، مقدار کد ۰ (شبکه در دسترس نیست) استفاده می شود. این پیام خطا فقط توسط مسیریاب ها تولید می شود. دلیل وقوع خطای فوق، ناشی از یک اشتباه در مشخص کردن آدرس IP مقصد و یا یک اشتباه در جدول مسیریابی مسیریاب تولید کننده پیام ICMP می باشد. آدرس مبدا موجود در سرآیند IP حمل کننده این پیام ICMP، مسیریابی را که این خطا را تولید کرده است مشخص می کند.

مقدار کد ۱ (میزبان در دسترس نیست) به وسیله مسیریابی تولید می شود که مستقیماً به شبکه مقصد متصل است. این کد نشان دهنده این است که بسته با موفقیت توسط مسیریاب ها تحویل داده شده است اما مسیریاب آخر قادر به ارتباط با میزبان مشخص شده نمی باشد. این امر به این دلیل می تواند باشد که تلاش پروتکل ARP انجام شده توسط مسیریاب برای پیدا کردن آدرس سخت افزاری مقصد موفقیت آمیز نبوده است. همچنین این احتمال وجود دارد که میزبان مقصد به

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

دلیل از کار افتادگی، پیکره بندی اشتباه یا تعیین آدرس IP نادرست در دسترس نباشد. باید توجه نمود که پیام خطای ICMP در دسترس نبودن مقصد بر نقص تحویل دلالت می کند حال آن که پیام خطای ICMP در دسترس نبودن شبکه نشان دهنده نقص مسیریابی است.

مقدار کد ۲ (در دسترس نبودن پروتکل) به وسیله میزبان مقصد تولید می شود. این پیام دلالت براین دارد که بسته به میزبان مقصد رسیده است اما پروتکل بالایی نظیر TCP، UDP و OSPF که IP باید محتویات بسته خود را به آن تحویل دهد، در دسترس نیست.

مقدار کد ۳ (در دسترس نبودن درگاه) هنگامی تولید می شود که پروتکل لایه حمل (UDP یا TCP) قادر به غیرتسهیم سازی بسته و تشخیص برنامه کاربردی لایه بالاتر نباشد. درموردی ممکن است پروتکل لایه حمل به خاطر عدم حضور یک سرویس کاربردی خاص در میزبان مقصد قادر به غیرتسهیم سازی بسته نباشد. سرویس های کاربردی به وسیله شماره های درگاه UDP و TCP مشخص می شوند.

مقدار کد ۴ (تکه سازی نیاز است ولی پرچم DF ۱ است) توسط مسیریاب های میانی شبکه تولید می شود. هنگامی که به خاطر اندازه MTU شبکه، نیاز به تکه سازی بسته IP باشد ولی پرچم DF موجود درسرآیند بسته IP مقدار ۱ داشته باشد، مسیریاب نمی تواند بسته را تکه سازی کند واز طرفی نمی تواند بسته را پیش ببرد و بنابراین باید آن را حذف نموده و یک پیام ICMP ارسال دارد.

مقدار کد ۵ (مسیریابی مبدا ناموفق) توسط یک مسیریاب تولید می شود. این پیام برای بسته های IP که از امکان مسیریابی مبدا IP استفاده می کنند، تولید میشود. با کمک امکان مسیریابی مبدا IP، می توان مسیر کامل و آدرس های مسیریاب هایی را که باید برای پیش بردن بسته استفاده شوند، مشخص نمود. اگر یک مسیریاب، نتواند بسته را براساس مسیر تعیین شده پیش ببرد، باید بسته را حذف کند. دراین حالت مسیریاب یک پیام نوع ۳ ICMP با کد ۵ به فرستنده می فرستد و بدین وسیله ناموفق بودن مسیریابی را به مبدا اطلاع می دهد.

هنگامی که یکی از مسیریاب های میانی شبکه از طریق جدول مسیریابی خود تشخیص دهد که شبکه مقصد ناشناخته می باشد، بسته ICMP با مقدار کد ۶ (شبکه مقصد ناشناخته است) به مبدا ارسال می دارد. این پیام در شبکه های فعال حقیقی تولید نمیشود، چون مسیریاب دراین حالت از یک پیام ICMP با نوع ۳ و با کد ۰ (در دسترس نبودن شبکه) استفاده می نماید.

در صورتیکه مسیریاب میانی شبکه با کمک لایه پیوند خود متوجه عدم وجود میزبان مقصد شود، از پیام ICMP با مقدار کد ۷ (میزبان مقصد ناشناخته است) استفاده می نماید. به عنوان مثال چنانچه لایه پیوند مسیریاب از طریق یک اتصال نقطه به نقطه به میزبان مقصد وصل باشد، دراین صورت قادر به تشخیص عدم وجود یک میزبان خاص می باشد.

هنگامی که مسیریاب شبکه تشخیص دهد که یک میزبان خاص از بقیه شبکه جدا شده است، از پیام های ICMP با مقدار کد ۸ (میزبان مبدا جدا شده است) استفاده می نماید. البته RFC ۱۸۱۲ توصیه می کند که مسیریاب های شبکه از کد خطای فوق استفاده ننمایند و در عوض از یکی از پیام های در دسترس نبودن شبکه (کد صفر) یا در دسترس نبودن میزبان (کد ۱) استفاده نمایند. بنابراین پیام های ICMP با کد ۸ فقط جنبه تاریخی داشته و استفاده ای نمی شود.

مدیر شبکه می تواند به دلایل مختلف از ارسال بسته ها توسط مسیریاب های شبکه و از طریق یک مسیر خاص جلوگیری نماید. حتی ممکن است که مسیریاب های شبکه مسیری به سمت مقصد یا شبکه تعیین شده داشته باشند و از نظر فنی مشکلی برای مسیریابی موجود نباشد ولی به عنوان بخشی از سیاست شبکه یک سازمان وبه خاطر عوامل مختلفی مانند دلایل مدیریتی، هزینه شبکه و امنیت، مدیر شبکه نخواهد بسته ها توسط مسیریاب از طریق مسیر خاصی پردازش شود. دراین حالت از بسته های ICMP نوع ۳ و کد ۹ و ۱۰ (ارتباط با شبکه/ میزبان مقصد از طرف مدیریت ممنوع شده است)،

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

استفاده می گردد. مقدار فیلد کد ۹ نشان می دهد که ارتباط با شبکه مقصد از طرف مدیریت ممنوع شده است، در صورتی که مقدار کد ۱۰ نشان دهنده این است که ارتباط با میزبان مقصد از طرف مدیریت ممنوع شده است.

چنانچه مسیر یاب های میانی شبکه قادر به تامین نوع سرویس درخواست شده در فیلد نوع سرویس موجود در سرآیند IP بسته ها باشد، نمی تواند بسته را به شبکه یا میزبان مقصد پیش ببرد. در این حالت یک بسته ICMP با نوع ۳ و کد های ۱۱، ۱۲ (شبکه/ میزبان مقصد برای نوع سرویس در دسترس نیست) ارسال می شود. کد ۱۱ نشان دهنده این است که شبکه مقصد برای مقدار کیفیت سرویس درخواستی در دسترس نیست در حالیکه کد ۱۲ نشان می دهد که میزبان مقصد برای کیفیت سرویس درخواستی در دسترس نمی باشد.

بسیاری از مسیر یاب های امروزه دارای نرم افزار فیلتر کردن بسته هستند که با کمک آن می توانند قوانین فیلتر کردن را اعمال نموده و از ارسال بسته ها به آدرس های IP خاص، نوع های پروتکل خاص و شماره های درگاه خاص جلوگیری کنند. این کار به خاطر دلایل امنیتی انجام شده و اولین خط دفاع در برابر کاربران متخاصم است. در این حالت از پیام های ICMP نوع ۳ و کد ۱۳ (ارتباط به خاطر دیواره های آتش از جانب مدیریت ممنوع شده است) استفاده می شود.

پیام های ICMP با کد ۱۴ (تخلف تقدم ميزبان)، توسط مسيرياب اولين پُرش به ميزبان فرستنده ارسال می شوند. مسيرياب اولين پُرش، اولين مسيريابی است که بسته برای رسيدن به مقصد خود بايد از آن عبور کند. اين پیام ICMP نشان دهنده اين است که تقدم خواسته شده برای آدرس مبدا / مقصد و شماره های درگاه مبدا/ مقصد، مجاز نمی باشند.

پیام ICMP با کد ۱۵ (تقدم در اثر عمل نمی کند) توسط مسیر یاب های میانی شبکه تولید میشود. مدیر شبکه این امکان را دارد که در جدول مسیریابی نودهای میانی شبکه، حداقل تقدم مورد نیاز برای عبور بسته ها از یک مسیر خاص را تعیین کند. اگر بسته ارسالی با مقدار تقدم پائین تر از آنچه در جدول مسیریابی مشخص شده است، ارسال گردد در این صورت بسته ها قادر به عبور از این مسیر نبوده و ناگزیر باید حذف شوند. در این حالت یک پیام ICMP با کد ۱۵ (تقدم در اثر عمل نمی کند) به سمت مبدأ ارسال می شود.

۸-۴-۳-۳-پیام ICMP فرونشاندن مبدا

از آنجاییکه شبکه های IP بدون اتصال می باشند، دهننگام مسیریابی و پیش بردن بسته ها به سمت مقصد، اطلاعات مربوط به آنها را درحافظه های خود ذخیره نمی نمایند. بنابراین ممکن است که مسیریاب های میانی شبکه به طور موقت دچار ازدحام شوند. درشرایطی که حافظه یا ظرفیت بافر بیشتری در مسیریاب های میانی شبکه برای ذخیره بسته های ورودی وجود ندارد، ازدحام بوجود می آید. بسته های ارسالی، قبل از پردازش و هدایت به سمت مقصد در بافر مسیریاب های میانی ذخیره می شوند. معمولا مسیریاب ها تلاش دارند که اتصالاتی را که تحت تاثیر ازدحام شبکه قرار گرفته اند، آهسته نمایند. هنگامی که یک مسیریاب متوجه وقوع ازدحام در بافرهای خود گردید، باید بسته های ورودی اضافی را حذف کند. یکی از بهترین روش های کاهش ازدحام شبکه، درخواست از میزبان های مبدا برای کاهش سرعت ارسال می باشد. بدینمنظور مسیر یاب از پیام ICMP فرونشاندن مبدا استفاده می کندو بدین ترتیب از فرستنده ها درخواست می کند که سرعت ارسال خود را کاهش دهند.

اگر قرار باشد برای هر بسته ای که مسیر یاب به خاطر پر بودن بافر های حافظه خود آن را حذف می کند یک پیام فرو نشاندن مبدا ارسال شود، در این صورت، پیام های ICMP فرونشاندن مبدا ارسالی، ازدحام را در شبکه افزایش می دهند و به سایر مسیر یاب ها اثر منفی می گذارند. برای رفع این مشکل، در پیاده سازی های پیشرفته پروتکل ICMP، پیام های فرو نشاندن مبدا، فقط به مبدا های ارسال می شود که بیشترین بسته ها را تولید می کنند. همچنین در برخی از پیاده سازی ها، مسیر یاب ها به جای این که صبر کنند تا بعد از پر شدن بافر، پیام ICMP فرونشاندن مبدا ICMP ارسال نمایند، هنگامی

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

که بافر در حال پر شدن است، ارسال پیام های فوق را شروع کرده تا بدینوسیله از سرریز شدن بافر های خود جلوگیری نمایند. سوالی که اینجا مطرح می شود این است که چگونه یک مبدا می فهمد که مشکل ازدحام رفع شده است؟ و چه هنگامی می تواند سرعت ارسال خود را افزایش دهد؟ متأسفانه هیچ پیام ICMP برای لغو یا معکوس کردن پیام فرو نشانیدن مبدا و نشان دادن این که مشکل ازدحام بر طرف شده است، وجود ندارد. بنابراین در سطح IP فرستنده نسبت به اینکه چه زمانی نرخ ارسال را افزایش دهد آگاه نمی باشد. برخلاف IP، پروتکل TCP نسبت به زمانی که باید نرخ ارسال را افزایش دهد، آگاهی دارد. این قابلیت در بخش کنترل جریان TCP پیاده سازی شده است که در فصل های بعدی آن را توصیف خواهیم نمود.

در ساختار پیام های فرو نشانیدن مبدا، مقدار فیلد نوع برابر با ۴ است. فیلد کد برابر با صفر بوده و از فیلد ۴ بایتی پارامتر استفاده نشده و همواره صفر است.

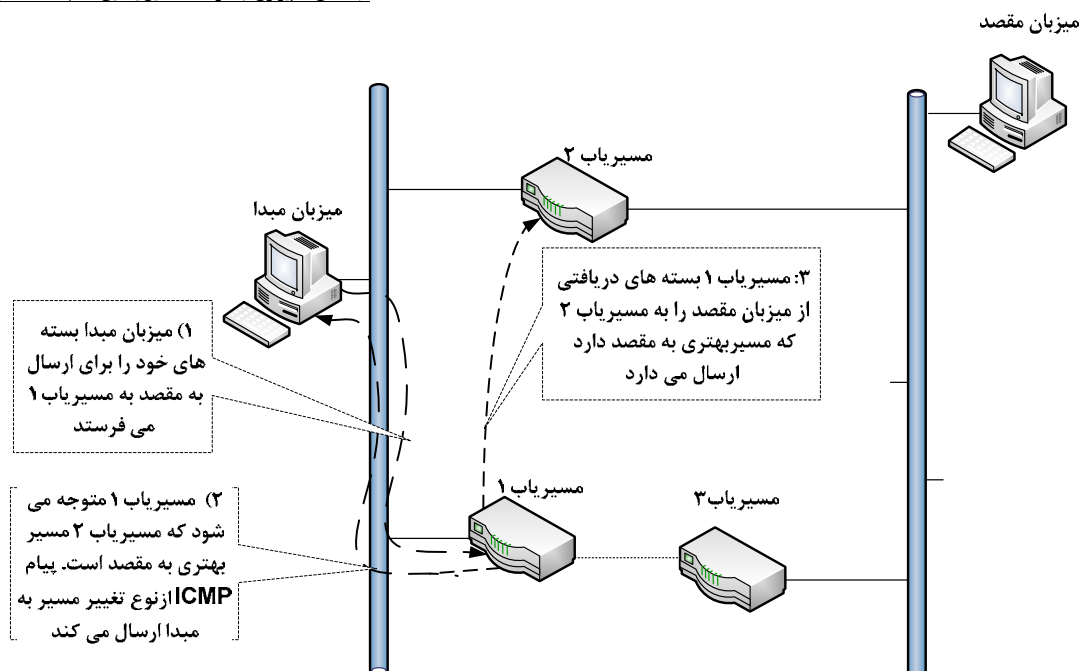
۸-۴-۳-۴- پیام ICMP تغییر مسیر

هنگامی که یک مسیر یاب شبکه بسته ای را برای ارسال دریافت نماید ولی تشخیص دهد که مسیر یاب دیگری مسیر بهینه تری برای ارسال بسته به سمت مقصد دارد، اقدام به ارسال پیام ICMP تغییر مسیر می نماید. مسیر یاب ها اطلاعات مسیر یابی را در شبکه با استفاده از پروتکل های مسیر یابی با یکدیگر رد و بدل می کنند. بنابراین مسیر یاب های شبکه، همواره اطلاعات بهینه یا اطلاعات نزدیک به بهینه را درباره مسیر های شبکه دارند. از طرف دیگر اطلاعات مسیر یابی میزبان ها بسیار کم بوده و قابل مقایسه با مسیر یاب ها نمی باشد. معمولاً یک میزبان شبکه آگاهی کمی نسبت به شبکه داشته و فقط مسیر یاب های پرش بعدی خود را می شناسد. مسیر یاب های پرش بعدی، مسیر یاب هایی هستند که یک پرش از میزبان مبدا فاصله دارند. بنابراین میزبان مبدا و مسیر یاب های پرش بعد مستقیماً به یک شبکه متصل شده اند.

میزبان های شبکه معمولاً دارای مسیر یاب پیش فرض می باشند که از آن برای پیش بردن بسته های ارسالی به مقصد هایی که صریحاً در جدول مسیر یابی میزبان لیست نشده است، استفاده می شود. جدول مسیر یابی، در ناحیه داده پیکره بندی مانند یک فایل در میزبان نگه داشته می شود. با توجه به اینکه مسیر یاب های شبکه مجهز به پروتکل های مسیر یابی می باشند، در صورت وقوع تغییر در توپولوژی شبکه، قادر به شناسایی مسیر های جدید هستند. معمولاً میزبان های شبکه در مبادلات پروتکل مسیر یابی به طور مستقیم شرکت نمی کنند. در نتیجه میزبان ها از تغییرات توپولوژی آگاه نبوده و ممکن است جداول مسیر یابی آنها شامل اطلاعات بهینه برای دستیابی به یک مقصد نباشد.

به عنوان مثال، شبکه نشان داده شده در شکل (۸-۲۶) را در نظر بگیرید. در این شکل، مسیر یاب جدید R2 به شبکه اضافه شده است. این مسیر یاب جدید دارای یک مسیر بهینه تری برای دستیابی به میزبان مقصد B است. از آنجایی که میزبان A هنوز متوجه اضافه شدن مسیر یاب جدید R2 به شبکه نشده است، بنابراین برای پیش بردن بسته هایش به مقصد B همچنان از مسیر یاب R1 استفاده می نماید. اگر مسیر یاب R1 تشخیص دهد که مسیر یاب R2 مسیر بهینه تری به مقصد دارد، یک پیام ICMP تغییر مسیر به فرستنده ارسال می کند. همچنین بسته را به مسیر یاب بهینه تر یعنی R2 ارسال می دارد.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)



شکل (۸-۲۶): مثالی از کاربرد پیام های ICMP تغییر مسیر

میزبان های شبکه با دریافت یک پیام ICMP تغییرمسیر، جدول مسیریابی خود را با اطلاعاتی درباره مسیریاب جدید برای دستیابی به مقصد به روزرسانی می نمایند. بنابراین بسته های بعدی که به همان مقصد فرستاده می شوند باید از مسیر بهینه تر که از پیام ICMP تغییرمسیر بدست می آید، استفاده نمایند. برخی از پیاده سازی های TCP/IP فاقد قابلیت فوق بوده و بسته های ICMP تغییر مسیر را نادیده می گیرند. از آنجاییکه با هر بسته ای که به مسیریاب غیر بهینه فرستاده می شود، یک پیام ICMP تغییر مسیر به مبدا ارسال می شود، این امر منتج به تولید ترافیک اضافی در شبکه می شود. درساختار پیام های ICMP تغییر مسیر، مقدار فیلد نوع برابر با ۵ است. همچنین مقادیر فیلد کد در این پیام ها، قبلا در جدول (۸-۱۰) نشان داده شده بود. در بسته های ICMP تغییر مسیر، فیلدی برای نمایش آدرس IP مسیریاب بهینه در نظر گرفته شده است.

۸-۴-۳-۵- پیام های ICMP اعلان و انتخاب مسیریاب

از این پیام ها برای پیاده سازی مکانیزم کشف مسیریاب استفاده می شود. با کمک این مکانیزم، میزبان ها قادر خواهند بود تا به طور پویا همه مسیریاب های موجود که مستقیم به شبکه آنها متصل شده اند را کشف نمایند. با استفاده از قابلیت کشف مسیریاب ICMP، میزبان های شبکه مجبور به وابستگی به پیکره بندی ایستا یا دستی جداول مسیریابی خود نخواهند بود، بلکه می توانند همه مسیر یاب هایی را که برای آنها در دسترس است به روشی که مستقل از پروتکل مسیریابی استفاده شده توسط مسیریاب ها است پیدا کنند.

قابلیت کشف مسیریاب ICMP، برای کشف مسیریاب های محلی که در شبکه به طور مستقیم به هم متصل هستند، استفاده می شود و پروتکل عمومی مسیریابی نمی باشد. پیام های ICMP اعلان مسیریاب، در بازه های متناوب ۷ تا ۱۰ دقیقه توسط مسیریاب ها فرستاده می شوند. همچنین از این پیام ها می توان در پاسخ به پیام ICMP انتخاب مسیریاب استفاده نمود.

۸-۴-۳-۶- پیام ICMP تخطی زمانی

پیام ICMP تخطی زمانی در شرایط زیر تولید می شود :

- هرگاه مقدار فیلد TTL موجود در بسته های IP به صفر رسید، مسیر یاب های شبکه یک پیام ICMP تخطی زمانی به سمت مبدا ارسال نموده و به آنها درمورد اتفاق فوق اطلاع رسانی می نمایند. مقدار کد برای این پیام صفر می باشد. اگر بسته ای در یک حلقه مسیریابی قرار گرفت، هر بار که مسیر یاب بسته را دریافت می نماید حداقل ۱ واحد فیلد TTL را کاهش می دهد. در نهایت فیلد TTL به صفر می رسد که در این زمان بسته باید دور انداخته شود و یک پیام ICMP تخطی زمانی تولید می گردد.
- هرگاه یک تکه از بسته های IP تکه شده به میزبان مقصد نرسد، میزبان مقصد یک پیام ICMP تخطی زمانی با مقدار کد برابر با ۱ ارسال می دارد. میزبان های شبکه معمولاً مجهز به یک زمان سنج بازسازی می باشند که با دریافت اولین تکه بسته شروع به کار می کند. چنانچه تا زمانیکه این زمان سنج فعال است، همه تکه های مربوط به یک بسته IP به میزبان مقصد نرسد، تکه های دریافتی حذف شده و یک پیام ICMP تخطی زمانی به مبدا ارسال می گردد.

مقدار فیلد نوع در ساختار پیام های ICMP تخطی زمانی، برابر با ۱۱ می باشد. همچنین مقدار کد این پیام ها ۰ یا ۱ است. کد ۰ بیانگر این مطلب است که پیام توسط مسیر یاب های میانی شبکه تولید شده است در حالیکه کد ۱ نشان دهنده اتمام زمان سنج بازسازی بسته ها در میزبان مقصد می باشد. پیام های ICMP تخطی زمانی توسط میزبان های شبکه تولید می شوند.

۸-۴-۳-۷- پیام ICMP مشکل پارامتر

چنانچه مسیر یاب و یا میزبان شبکه متوجه مشکلی در پارامترهای سرآیند IP بسته های دریافتی شوند، از پردازش بسته جلوگیری کرده و یک پیام ICMP مشکل پارامتر، با مقدار فیلد نوع برابر با ۱۲ ارسال می دارند. با کمک فیلد اشاره گرموجود در این پیام، محل و نوع پارامتری که دارای مشکل است، در سرآیند IP مشخص می شود. مقدار فیلد کد برابر با ۰، ۱ و ۲ می باشد. کد ۰ بیانگر این است که اشاره گر موجود در پیام ICMP مشکل پارامتر محل خطا را نشان می دهد. کد ۱ نشان دهنده نادرست بودن یکی از امکانات موجود در سرآیند IP است و نهایتاً کد ۲ نشان دهنده این است که طول بسته IP نادرست است. بنابراین در صورتیکه پیام فوق با کد ۱ ارسال شود، از فیلد اشاره گراستفاده ای نمی شود.

۸-۴-۳-۸- پیام ICMP درخواست برچسب زمانی/پاسخ برچسب زمانی

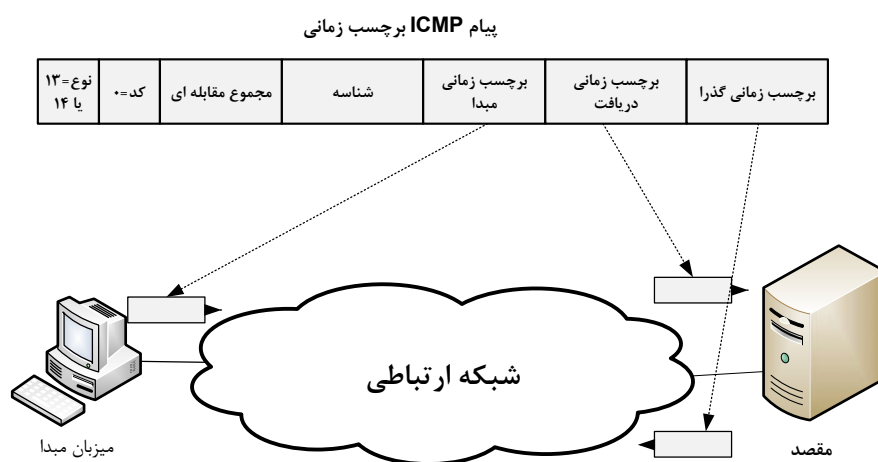
هر نود شبکه های IP دارای یک ساعت داخلی می باشد. برای همزمان سازی ساعت های نودهای شبکه، از پیام های ICMP درخواست برچسب زمانی/پاسخ برچسب زمانی استفاده می شود. البته می توان از پروتکل NTP¹ نیز برای همزمان سازی ساعت نودهای شبکه نیز استفاده نمود، اما استفاده از پیام های ICMP درخواست برچسب زمانی/پاسخ برچسب زمانی به مراتب ساده تر است.

در ساختار پیام های فوق، مقدار فیلد نوع برای پیام های درخواست برابر با ۱۳ و برای پیام های پاسخ برابر با ۱۴ می باشد. همچنین مقدار فیلد کد برابر با ۰ است. مقدار برچسب زمانی، برحسب تعداد میلی ثانیه های گذشته از نیمه شب طبق

¹ Network Time Protocol

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

ساعت جهانی اندازه گیری می شود. در ساختار پیام های فوق، سه فیلد برای درج برچسب زمانی در نظر گرفته شده است که عبارتند از: برچسب زمانی مبدا، برچسب زمانی دریافت و برچسب زمانی گذرا. برچسب زمانی مبدا، توسط مبدا فرستنده پیام مقداردهی می شود. گیرنده، به محض دریافت پیام فوق مقدار زمان جاری خود را در فیلد برچسب زمانی دریافت قرار می دهد. بعد از پردازش بسته دریافتی، در پاسخ به آن، پیام پاسخ ارسال می شود. در این حالت، گیرنده مقدار برچسب زمانی جاری را در فیلد برچسب زمانی گذرا قرار داده و ارسال می دارد. شکل (۸-۲۷) مثالی از نحوه مقدار دهی برچسب زمانی در این پیام ها نشان داده شده است.



شکل (۸-۲۷): مثالی از نحوه پر نمودن فیلدهای برچسب زمانی

۸-۳-۹- پیام های ICMP درخواست اطلاعات/پاسخ اطلاعات

از این پیام ها برای بدست آوردن آدرس IP میزبان هایی که آدرس IP خود را نمی دانند استفاده می شود. البته با وجود پروتکل هایی مثل RARP، BOOTP و DHCP که مکانیزم های عالی تری را برای کشف آدرس IP فراهم می کنند، استفاده از پیام های فوق مرسوم نبوده و به هیچ وجه توصیه نمی شود. برای پیام ICMP درخواست اطلاعات مقدار فیلد نوع برابر با ۱۵ بوده و برای پیام پاسخ آن این فیلد برابر با ۱۶ است. فیلد کد همواره ۰ است.

۸-۳-۱۰- پیام های ICMP درخواست پوشش آدرس/پاسخ پوشش آدرس

در فصل قبلی، مفهوم زیر شبکه سازی و آدرس های پوشش زیر شبکه توصیف شدند. میزبان های شبکه برای بدست آوردن پوشش زیر شبکه، از پیام ICMP درخواست پوشش آدرس استفاده می کنند. در این پیام ها مقدار فیلد نوع برابر با ۱۷ می باشد. همچنین در پاسخ به پیام درخواست فوق، پیام ICMP پوشش آدرس با مقدار فیلد نوع برابر با ۱۸ ارسال می شود. میزبان درخواست کننده آدرس پوشش زیر شبکه، درخواست خود را مستقیماً به آدرس مسیریاب شبکه ارسال می دارد. در حالتیکه میزبان فوق، آدرس مسیریاب را نداند، درخواست را به صورت همه پخش در شبکه پخش می کند. فقط مسیریاب های شبکه مجاز به پاسخ دهی به پیام های درخواستی فوق می باشند.

پرسش های فصل

۱. کاربرد و دلیل عمده استفاده از پروتکل ARP را توضیح دهید.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

۲. ساختار بسته های ARP را رسم نموده و کاربرد هر فیلد آن را بنویسید.
۳. محدودیت های پروتکل ARP را ذکر کنید.
۴. به چه علت پیام درخواست ARP به صورت همه پخش ارسال می شود؟
۵. آیا پیام پاسخ ARP نیز به صورت همه پخش ارسال می شود یا خیر؟ توضیح دهید.
۶. با ذکر یک مثال و رسم شکل، حداقل دو کاربرد اصلی پروتکل ARP را توضیح دهید.
۷. اگر یک میزبان شبکه به طور ایستا با اطلاعاتی درباره آدرس های MAC و آدرس های IP مطابق پیکره بندی شود، با چه مشکلاتی مواجه می شود؟
۸. چگونه آزمون آدرس IP تکراری ARP انجام می شود؟
۹. مشکلات ناشی از پروتکل ARP/RARP را در شبکه های پل بندی شده توضیح دهید.
۱۰. فرض کنید که در یک شبکه دو ایستگاه کاری وجود دارند که هر دو آدرس 197.12.35.67 دارند. آدرس های MAC دو ایستگاه فوق به ترتیب A و B می باشد. این دو ایستگاه همزمان اقدام به برقراری همزمان یک جلسه Telnet با یک سرور به آدرس IP 197.12.35.99 و آدرس سخت افزاری C می نمایند. به طور کامل توضیح دهید که در این حالت چه اتفاقی می افتد و مشکل ایجاد شده به چه صورت قابل رفع می باشد؟
۱۱. کاربرد پروتکل RARP را توضیح داده و ساختار بسته های آن را رسم کنید.
۱۲. نقش سرور دهنده های اصلی و ثانویه RARP چیست؟ توصیف کنید چگونه یک سرور دهنده ثانویه می تواند به یک درخواست RARP پاسخ دهد؟
۱۳. ویژگی های اصلی شبکه های IP را توضیح دهید.
۱۴. با توجه عدم اطمینان پروتکل IP، توضیح دهید که مشکل ناشی از گم شدن بسته ها در معماری TCP/IP به چه صورت قابل رفع می باشد؟
۱۵. ساختار بسته های IPv4 را رسم کرده و به طور خلاصه کاربرد هر فیلد را توضیح دهید.
۱۶. کمترین و بیشترین طول بسته های IP چقدر می باشد؟
۱۷. فرض کنید که نرم افزار IP موجود در یک مسیر یاب فقط بتواند بسته های نسخه ۴ را پردازش کند. اگر بسته هایی را با مقدار فیلد نسخه متفاوت دریافت کند چه اتفاقی می افتد؟
۱۸. کاربرد فیلد نوع سرور و اجزای آن را بنویسید.
۱۹. مفهوم MTU را نوشته و مقدار آن را برای شبکه های مختلف بنویسید.
۲۰. مفهوم تکه سازی و بازسازی بسته های IP را نوشته و فیلدهایی را که به این منظور به کار می روند، ذکر کنید.
۲۱. کاربرد فیلد TTL را در بسته های IP بنویسید؟
۲۲. مزایا و معایب بازسازی بسته های در مسیر یاب های میانی شبکه را توضیح دهید.
۲۳. یک بسته IP با اندازه ۱۵۰۰ بایت با پرچم DF برابر با ۱ در یک شبکه با اندازه MTU ۱۵۰۰ بایت فرستاده شده است مسیر به نود مقصد از شبکه هایی با اندازه MTU ۲۰۰۰ و ۴۴۷۰ بایت میگذرد آیا تکه سازی اتفاق می افتد؟ آیا IP قادر به تحویل بسته به مقصد می باشد؟
۲۴. یک بسته IP با اندازه ۱۵۰۰ بایت و مقدار فیلد شناسایی ۱۰۰ با پرچم DF برابر با صفر در یک شبکه با اندازه MTU ۵۰۰ بایت می گذرد. اندازه MTU شبکه مقصد ۱۵۰۰ بایت است آیا تکه سازی اتفاق می افتد؟ اگر چنین است تکه ها را با مقادیر فیلد های شناسایی MF و DF و افسست تکه سازی مشخص کنید.

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم - دانشگاه فردوسی مشهد)

۲۵. یک بسته IP با اندازه ۱۵۰۰ بایت و مقدار فیلد شناسایی ۱۰۰ با پرچم DF برابر با صفر در شبکه با اندازه MTU ۱۵۰۰ بایت فرستاده شده است. مسیر به نود مقصد از شبکه با اندازه MTU ۶۲۵ می گذرد. اندازه MTU شبکه مقصد ۵۲۵ بایت است آیا تکه سازی اتفاق می افتد؟ اگر چنین است تکه ها را در مسیر یاب بین شبکه ها مشخص کنید. برای هر تکه مقادیر فیلد های شناسایی، MF و DF و افست تکه سازی را نشان دهید.
۲۶. کاربرد گزینه های IP را نوشته و انواع آن را ذکر کنید.
۲۷. با ذکر یک مثال کاربرد امکان مسیریابی مبداء دقیق را ذکر کنید.
۲۸. با ذکر یک مثال تفاوت مسیریابی مبداء ضعیف با مسیریابی مبداء دقیق را بنویسید.
۲۹. گزینه برچسب زمانی اینترنت در چه موردی استفاده می شود؟
۳۰. حداقل ۵ مشکل را نام ببرید که از ICMP می توان برای گزارش دادن آنها استفاده کرد؟
۳۱. چه نوع وسایلی در یک شبکه می توانند پیام های ICMP را تولید کنند؟
۳۲. آیا استفاده از ICMP، IP را مطمئن تر می سازد؟ دلایل جواب خود را بیان کنید.
۳۳. اگر یک بسته IP تکه سازی شود آیا پیام های ICMP برای هر تکه تولید می شود؟ جواب خود را توجیه کنید.
۳۴. آیا ICMP در مورد بسته هایی که شامل پیام ICMP هستند استفاده می شود یا خیر؟ جواب خود را توجیه کنید.
۳۵. در چه حالت هایی از پیام های ICMP استفاده نمی شود؟
۳۶. چرا پیام های ICMP به تولید کننده اصلی بسته که گزارش شده فرستاده می شود؟ اگر یک خطا در جدول مسیریابی مسیریاب مسئول تولید پیام ICMP باشد، چرا نمی توان پیام ICMP را به خود مسیریاب فرستاد؟
۳۷. آیا ضمانتی وجود دارد که پیام های ICMP تحویل داده شده اند؟ جواب خود را توضیح دهید.
۳۸. ساختار بسته های ICMP را رسم کرده و عملکرد هر فیلد را توضیح دهید.
۳۹. مقصود از فیلد های نوع و کد در یک پیام ICMP چیست؟
۴۰. فیلد اطلاعات یک پیام ICMP شامل چه نوع اطلاعاتی می شود؟
۴۱. کاربرد امکان PING را با رسم یک شکل توضیح دهید.
۴۲. چه هنگامی پیام های ICMP نوع ۳، باید فرستاده شود؟
۴۳. توضیح دهید چگونه پیام ICMP نوع ۳ می توان برای تخمین کمترین اندازه MTU مسیر به مقصد استفاده کرد؟
۴۴. چه هنگامی پیام فرو نشانندن مبدا فرستاده می شود؟ چرا این پیام نباید توسط مسیریاب ها فرستاده شود؟ چه لایه ای از OSI مناسب ترین لایه برای اداره کردن مشکلی است که توسط پیام فرو نشانندن مبدا مشخص شده است؟
۴۵. دلایل ایجاد ازدحام در یک مسیریاب شبکه را توضیح دهید.
۴۶. با ذکر یک مثال کاربرد پیام تغییر مسیر ICMP را توضیح دهید.
۴۷. تحت کدام شرایط مسیریاب ها باید پیام های ICMP را تولید کنند؟
۴۸. در مورد پیام های ICMP که برای کشف مسیریاب استفاده می شود بحث کنید. مزایای این روش بر سایر تکنیک ها چیست؟
۴۹. در چه حالت هایی پیام ICMP تخطی از زمان فرستاده می شود؟
۵۰. چه هنگامی پیام ICMP مشکل پارامتر ارسال می شود؟

شبکه های کامپیوتری (دکتر محمد حسین یغمایی مقدم – دانشگاه فردوسی مشهد)

۵۱. کاربرد پیام های ICMP درخواست / پاسخ پوشش آدرس چیست ؟ سایر پروتکل های دیگر که می توانند برای این مقصود استفاده شوند چیست ؟