شبکه های کامپیوتری

(Computer Networks)

تالیف :

دکتر محمد حسین یغمایی مقدم

دانشیار گروه مهندسی کامپیوتر

دانشگاه فردوسی مشهد

فصل اوّل

مفاهیم پایه شبکه های انتقال داده و شبکه های کامپیوتری

۱-۱- مقدمه‌ای بر شبکه‌های انتقال داده

در دنیای امروز، کامپیوترها دربسیاری از جنبه های زندگی انسان‌ها کاربرد پیدا کرده است. درمراکز تفریح از بازی‌های کامپیوتری که بسیار مورد علاقه جوانان است، استفاده می شود. در ادارات برای انجام امورتایپ و نامه نگاری، بایگانی پرونده‌ها و اطلاعات و ارائهٔ سرویس اطلاع رسانی به مراجعه کنندگان از سیستم‌های کامپیوتری استفاده می‌گردد. درآژانس‌های مسافرتی برای رزرو و فروش بلیط پروازهای داخلی و خارجی و همچنین فروش بلیط قطار واتوبوس از کامپیوترها استفاده می شود. دربیمارستان‌ها برای بایگانی و ضبط اطلاعات بیماران به‌طور وسیعی از سیستم‌های کامپیوتری استفاده می‌گردد. همچنین بسیاری از سیستم‌های پزشکی پیشرفته مثل دستگاه MRI[1]، دستگاه سونوگرافی و... از کامپیوتر استفاده می کنند. درمراکز صنعتی برای کنترل دستگاه‌های کارخانجات و افزایش بهره وری از کامپیوتر و ربات‌ها استفاده می‌گردد. دامنهٔ استفاده از کامپیوترها آنقدر گسترش یافته است که امروزه اکثر خانه‌ها مجهز به حداقل یک کامپیوتر می‌باشند. یکی ازموارد اصلی کاربرد کامپیوتر، دانشگاه‌ها و مراکز تحقیقاتی می‌باشد. درمراکز عملی پژوهشی، با استفاده از سیستم‌های کامپیوتری و نرم‌افزارها و سخت‌افزارهای مناسب، بسیاری از پروژه های تحقیقاتی انجام می‌شود.

برای استفادهٔ بهینه از اطلاعات موجود در کامپیوترها، لزوم تبادل داده ها بین آنها حس می‌گردد. یکی از ساده‌ترین روش‌های تبادل اطلاعات و جابجایی داده‌ها درکامپیوترها، استفاده از فلاپی دیسک ، دیسک فشرده (CD[2]) و حافظه های USB[3] می‌باشد. مسلماً استفاده از تجهیزات فوق درصورتی مناسب است، که اولاً حجم اطلاعات کم بوده و ثانیاً فاصلهٔ سیستم‌های کامپیوتری از یکدیگر زیاد نباشد. گسترش سیستم‌های کامپیوتری و افزایش حجم داده ها، متخصصین کامپیوتر را به فکر طراحی و پیاده سازی شبکه‌های انتقال داده انداخت. یکی از ساده‌ترین و اولین شبکه‌های انتقال داده ، شبکهٔ تلفن می‌باشد. با توجه به گستردگی و توسعهٔ زیاد شبکه‌های تلفن، استفاده از آن برای تبادل داده های کامپیوتری بسیار مناسب است، به‌طوری که امروزه نیز از شبکه‌های تلفن به عنوان یک شبکهٔ انتقال داده مناسب (برای سرعت‌های کم) استفاده می شود.

افزایش میزان کامپیوترها دردنیا وحجم زیاد اطلاعات، باعث شد تا سیستم‌های انتقال داده جدید طراحی و پیاده سازی شود. به‌طور 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

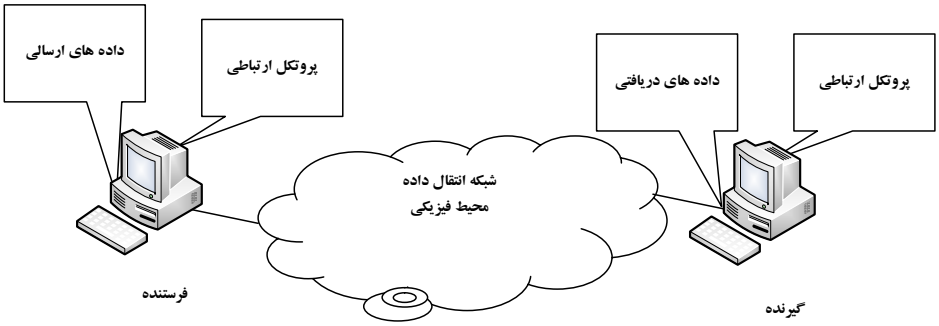
---

[1] Magnitude Radiation Imaging

[2] Compact Disk

[3] Universal Serial Bus

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



شکل (۱-۱): اجزای یک سیستم انتقال داده

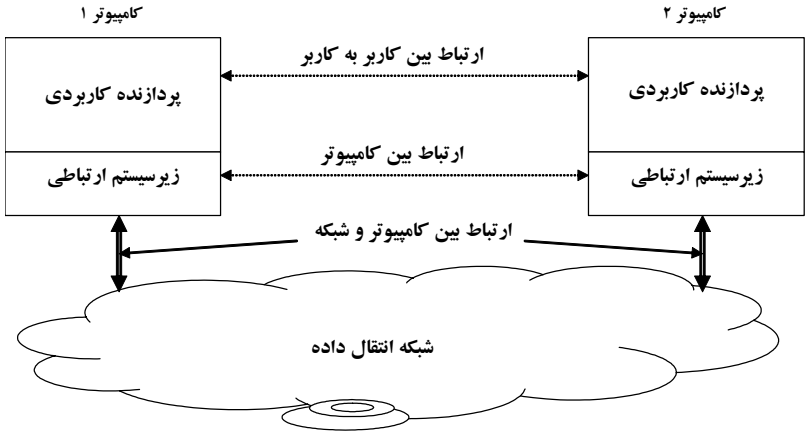
در یک شبکهٔ انتقال داده، فرستنده با استفاده از تجهیزات ارسال، اقدام به تبدیل داده‌های ۰و۱ خام به سیگنال‌های الکتریکی یا نوری قابل ارسال درمحیط فیزیکی می‌نماید. محیط‌های فیزیکی متعددی برای ارسال داده ها وجود دارند که درفصل دوم به بررسی آنها خواهیم پرداخت. در گیرنده نیز با استفاده از تجهیزات مناسب، سیگنال‌های دریافتی به صورت داده های اولیه تبدیل می‌شوند. برای مبادله صحیح داده ها بین فرستنده و گیرنده، هر دو باید از یک‌سری قوانین مشترک استفاده نمایند. این قوانین توسط پروتکل‌های ارتباطی مشخص می شود. هم فرستنده و هم گیرنده باید از پروتکل ارتباطی یکسانی برای ارسال و دریافت داده ها استفاده نمایند، درغیراین‌صورت تبادل داده ها میسر نمی‌باشد.

درشکل (۱-۲)، سه مورد از عملیات ارتباطی اصلی که باید درشبکه‌های انتقال داده درنظر گرفته شود، نشان داده شده است. هدف اصلی تمام شبکه‌های انتقال داده، فراهم سازی ارتباط لازم بین کاربران انتهایی شبکه می‌باشد. اما ازآنجایی‌که فن‌آوری‌های مختلفی برای پیاده سازی شبکه‌های انتقال داده وجود دارد، ممکن است که کاربران انتهایی از زیرسیستم‌های مختلفی برای برقراری ارتباط با شبکه استفاده نمایند.

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

- عملکرد[۱]
- قابلیت اطمینان[۲]
- امنیت[۳]

[۱] Performance
[۲] Reliability
[۳] Security



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

درشبکه‌های 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 می‌پردازیم. یکی از مهمترین عوامل تعیین‌کنندهٔ عملکرد یک شبکه انتقال داده، تعداد کاربران آن شبکه می‌باشد. از آنجایی‌که منابع موجود درشبکه محدود بوده و برای حجم مشخصی ازترافیک درنظرگرفته شده است، با افزایش تعداد کاربران شبکه، میزان ترافیک در شبکه نیز افزایش می یابد. افزایش ترافیک درشبکه باعث افزایش ازدحام وکاهش گذردهی شبکه می شود. یکی دیگر از عوامل عملکرد شبکه‌های انتقال داده، نوع محیط ارسال می‌باشد. درشبکه های انتقال داده محیط‌های ارسال متنوعی وجود دارد. مسلماً هرقدر محیط ارسال از سرعت بالا و کیفیت مطلوب‌تری برخوردار باشد، عملکرد شبکه افزایش می یابد. درفصل دوم، انواع محیط‌های ارسال درشبکه های انتقال داده بررسی خواهد شد. نوع سخت‌افزار و نرم‌افزار استفاده شده درکامپیوترهای شبکهٔ انتقال داده نیز درمیزان عملکرد شبکه دخالت دارد.

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

امنیت، یکی دیگر ازمعیارهای انتخاب شبکه های انتقال داده است. دسترسی های غیرمجاز افراد به اطلاعات محرمانه شبکه و میزان مقاومت شبکه درمقابل نفوذ ویروس از موارد ارزیابی امنیت شبکه‌های انتقال داده می‌باشد.

۱-۳- مراجع استانداردگذاری شبکه‌های کامپیوتری

در ابتدای مطرح‌شدن شبکه‌های انتقال داده و شبکه‌های کامپیوتری، هر شرکت خصوصی از پروتکل‌های خاص خود استفاده می‌نمود. طبیعی بود که به علت عدم رعایت یک استاندارد مشخص، ارتباط بین شبکه‌های فوق و اتصال کاربران به آن به دلیل عدم برابری پروتکل‌های دو شبکه غیرممکن بود. از این‌رو ایده‌های استفاده از استاندارد واحد در شبکه‌های کامپیوتری مطرح گردید. این کار نه تنها باعث امکان ارتباط و گسترش شبکه‌های کامپیوتری می‌شود، بلکه باعث رونق

محصولات مبتنی بر استاندارد در بازار کامپیوتر نیز می‌گردد. به‌طور کلی دو نوع استاندارد وجود دارد که عبارتند از استانداردهای اسمی[1] و استانداردهای رسمی[2]. استانداردهای اسمی، استانداردهایی هستند که توسط شرکت‌های بزرگ کامپیوتری و مخابراتی برای گسترش محصولات خود وضع شده‌اند. در مقابل استانداردهای رسمی توسط مراجع بین‌المللی مورد تأیید و تصویب قرارگرفته‌است.طبیعی است به علت طولانی‌بودن نسبی تصویب استانداردها در مراجع بین‌المللی، معمولاً اکثر استانداردهای شبکه ابتدا به صورت اسمی می‌باشند و توسط شرکت‌های بزرگ ارائه می‌شوند و به تدریج با گسترش و کاربردی‌شدن استانداردهای مربوطه، تبدیل به استانداردهای رسمی می‌شوند. درادامه به بررسی مهمترین مراجع استانداردگذاری در زمینه انتقال داده و شبکه‌های کامپیوتری می‌پردازیم.

۱-۳-۱ اتحادیه جهانی مخابرات (ITU[3])

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. درسال ۱۹۲۵ دو کمیته مشورتی به نام های CCIT و CCIF توسط اتحادیه جهانی مخابرات تعریف شدند. CCIF دررابطه با سرویس های تلفن و CCIT در زمینه سرویس های تلگراف فعال بودند. درسال ۱۹۵۶ این دوکمیته با یکدیگر ترکیب شده و کمیته مشورتی تلفن و تلگراف (CCITT[5]) ایجاد گردید. CCITT دارای اعضای مختلفی شامل: شرکت های تلگراف و تلفن کشورها، شرکت‌های خصوصی، سازمان‌های علمی و صنعتی، سایر سازمان‌های بین‌المللی دیگر و اعضایی که رشته اصلی آنها چیز دیگری می‌باشد؛ ولی علاقه‌مند به فعالیت‌های CCITT هستند، می باشد. در بین این پنج نوع عضو، فقط شرکت‌های پست و تلگراف و تلفن کشورها حق رأی دارند. CCITT موظف به ارائه توصیه‌نامه‌هایی در زمینهٔ شبکه تلفن و تجهیزات ارتباط داده می‌باشد. توصیه نامه‌های CCITT بعد از مدتی به صورت استانداردهای شناخته‌شده جهانی در می‌آیند. نمونه‌ای از استانداردهای CCITT می‌توان به V.35,X.25,X.21,... و V.24 اشاره نمود. اتحادیه جهانی مخابرات درشهر ژنو سوئیس مستقر می باشد.

۱-۳-۲- سازمان جهانی استاندارد (ISO[6])

این سازمان بین‌المللی در ۲۳ فوریه سال ۱۹۴۷ تأسیس گردید و اعضای آن سازمان‌های استاندارد ملی کشورهای مختلف می‌باشند. محل این سازمان درشهر ژنو سوئیس می باشد.این سازمان غیر دولتی بوده و۱۵۷ 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 رای می باشند، معمولا موسسات استاندارد هر کشور بوده که موظف به ارائه استاندارد درکشور می باشند. اعضای وابسته شامل کشورهایی هستند که دارای موسسات استاندارد کشوری نمی باشند. این اعضا فقط نسبت به استاندارهای ISO آگاهی پیدا کرده و درجریان تولید این استانداردها مشارکت ندارند. اعضای مشترک، مربوط به کشورهایی با اقتصاد کوچک می باشند که حق عضویت ناچیزی پرداخت کرده و فقط توسعه

---

[1] By fact
[2] By law
[۳] International Telecommunication Union
[4] Recommendation
[5] International Telegraph and Telephone Consultative Committee
[6] International Standard Organization
[7] Member bodies
[8] Correspondent members
[9] Subscriber members

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 زمینه‌های مختلفی استاندارد وضع شده است. این سازمان حدود ۲۰۰ کمیتهء فنی دارد که هریک موظف به یک زمینه خاصی می‌باشند. به‌عنوان مثال کمیتهٔ فنی شمارهء (۱) در زمینهٔ استانداردسازی گام دنده پیچ و مهره‌ها فعال است و کمیته فنی شماره (۹۷) در زمینه کامپیوتر و پردازش اطلاعات کار می‌نماید. البته با توجه به گستردگی موضوعات هر کمیته فنی، معمولاً در هر کمیته چندین گروه کاری فعال در غالب زیرکمیته‌ها وجود دارد که کارهای مختلف بین آنها تقسیم می‌شود.

۱-۳-۳- انجمن مهندسان برق و الکترونیک (IEEE[1])

انجمن مهندسان برق و الکترونیک یکی از بزرگترین سازمان‌های حرفه‌ای در سطح دنیا می‌باشد. این انجمن دارای حدود ۳۶۰ هزار عضو از ۱۷۵ کشور مختلف جهان می باشد. این انجمن درشهر نیویورک آمریکا ثبت شده است. این انجمن علاوه بر انتشارات بسیار زیادی که در زمینه‌های مختلف کامپیوتر و برق دارد. هر ساله چندین کنفرانس بین‌المللی در زمینه‌های مختلف مرتبط با فعالیت‌های خود برگزار می‌نماید. کنفرانس‌ها و مجلات انجمن مهندسان برق و الکترونیک از اعتبار و اهمیت بسیار زیادی در دنیا برخوردار می‌باشد. گروه کاری ۸۰۲ از انجمن مهندسان برق و الکترونیک در زمینه شبکه‌های محلی فعال می‌باشد.

۱-۴- شبکه های کامپیوتری

قرن حاضر، قرن ارتباطات نام دارد. با پیدایش کامپیوتر و فن‌آوری‌های ارتباطات، بسیاری از مشکلات زندگی انسان‌ها رفع شده‌است. شبکه‌های کامپیوتری که از اتصال چندین کامپیوتر در نقاط مختلف به‌وجود می‌آیند، نقش بسیار مهمی در انتقال اطلاعات و نزدیکی انسان‌ها به یکدیگر داشته‌اند. با استفاده از امکانات شبکه‌های کامپیوتری و اینترنت، امکان استفاده از سرویس زیادی نظیر: تبادل اطلاعات، ارسال نامه‌های الکترونیکی، انتقال فایل، کنفرانس های صوتی و تصویری، آموزش از راه دور، تبادل داده‌های تجاری وغیره فراهم شده‌است. شبکه‌های کامپیوتری جهت استفاده مشترک از منابع و برقراری ارتباط بین کاربران به‌وجود می‌آیند. در این بخش به ذکر مقدمات اولیه شبکه‌های کامپیوتری و معرفی مفاهیم اولیهٔ و پایه‌ای آن می‌پردازیم.

۱-۴-۱- اهداف و مزایای شبکه‌های کامپیوتری

در اتصال کامپیوترها و ایجاد شبکه‌های کامپیوتری، اهداف زیر مدنظر می‌باشد:

- ***به اشتراک‌گذاری منابع[2]:*** یکی از مزایای عمده شبکه‌های کامپیوتری تقسیم منابع می‌باشد. در یک شبکه کامپیوتری، کلیه کاربران شبکه در صورتی‌که مجاز به استفاده از شبکه باشند، می‌توانند به منابع موجود در شبکه نظیر برنامه‌های کاربردی، بانک‌های اطلاعاتی و تجهیزات سخت‌افزاری نظیر چاپگر، مودم و غیره دسترسی پیدا نمایند.
- ***قابلیت اطمینان بالا[3]:*** یکی از مشکلات استفاده انفرادی از کامپیوترها این است که چنانچه برروی یک کامپیوتر نرم‌افزار یا سخت‌افزار 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 می‌باشد. به عبارت دیگر قابلیت اطمینان یک کامپیوتر به تنهایی

---

[1] Institute of Electrical and Electronics Engineer
[2] Resource sharing
[3] High reliability

پایین است و این امر به خصوص در کاربردهای مهم نظیر کنترل و هدایت سیستم‌های نظامی پیشرفته نظیر هواپیما، موشک و غیره مشکل‌زا است. یکی از روش‌های افزایش قابلیت اطمینان، استفاده از شبکه‌های کامپیوتری و سیستم‌های توزیع شده می‌باشد. در این حالت منابع مهم برروی چندین ایستگاه شبکه نصب می‌شوند تا درصورت خرابی یکی ازسیستم‌ها، بتوان ازطریق سایر ایستگاه‌های شبکه به منابع دسترسی پیدا نمود.

- ***صرفه‌جویی مالی:*** استفاده از شبکه‌های کامپیوتری، باعث صرفه‌جویی مالی نیز می‌شود. هرچند نصب و راه‌اندازی شبکه‌های کامپیوتری خود نیاز به هزینه و امکانات نرم‌افزاری و سخت‌افزاری خاص خوددارد، ولی در کل می‌توان به این نتیجه رسید که شبکه‌های کامپیوتری باعث صرفه‌جویی درهزینه‌ها می‌گردند. به‌عنوان مثال چنانچه در یک اداره، چندین کارمند به یک نرم‌افزارخاص نیاز داشته باشند، می‌توان به جای آن‌که برای تک‌تک آنها نرم‌افزار مربوطه را خریداری و نصب و راه‌اندازی نمود، یک نسخه از آن را تهیه کرد و در شبکه نصب کرد (به شرط آن‌که نرم‌افزار قابلیت نصب در شبکه را داشته باشد). در این حالت چندین کاربر می‌توانند به‌طور همزمان به شبکه متصل شوندو از امکانات آن نرم‌افزار بهره ببرند. همچنین به‌عنوان مثال دیگر می‌توان در شبکه، یک چاپگر نصب و راه‌اندازی نمود. دراین حالت کاربران قادرند با استفاده از امکانات شبکه، از چاپگر به‌طور مشترک استفاده نمایند، که طبیعی است این امر باعث صرفه‌جویی در خرید چندین چاپگر برای کاربران شبکه می‌گردد.
- ***ایجاد ارتباط بین مردم:*** یکی دیگر از اهداف و مزایای عمده شبکه‌های کامپیوتری، ایجاد ارتباط بین مردم می‌باشد. این مسئله با گسترش سریع اینترنت و سرویس متنوع آن به خوبی مشاهده می‌شود. به‌عنوان مثال با کمک سرویس پست الکترونیکی[1] ،کاربران مختلف در سطح شبکه اینترنت که ممکن است در فواصل بسیار دوری از هم قرار داشته باشند، قادر به ارسال نامه‌های الکترونیکی به یکدیگرمی‌باشند. همچنین با استفاده از امکانات شبکه اینترنت، افراد مختلف می‌توانند در گروه‌های خبری و مباحثه‌ای گوناگون شرکت کرده و با استفاده از امکانات شبکه به مباحثه و تبادل نظر با یکدیگر بپردازند.

۱-۴-۲- انواع شبکه‌های کامپیوتری

از نظر وسعت، می‌توان شبکه‌های کامپیوتری را به سه نوع مختلف تقسیم‌بندی نمود که عبارتند از:

- ***شبکه‌های محلی*** **(LAN[2])** : این نوع شبکه‌ها دارای وسعت بسیار کمی می‌باشند و معمولاً در سطح یک ساختمان نظیر یک اداره کوچک و دانشکده‌های مختلف یک دانشگاه نصب و راه‌اندازی می‌شوند. شبکه‌های محلی جهت اشتراک منابع سخت افزاری (مثل چاپگر) و منابع نرم افزاری(مثل برنامه‌های کاربردی و بانک‌های اطلاعاتی)، بین کامپیوترهای شخصی و یا ایستگاه‌های کاری[3] استفاده می‌شوند. درشبکه‌های محلی یکی از کامپیوترهای شبکه که معمولاً از سرعت بالا و حجم حافظه زیادی برخوردار است؛ به عنوان سرویس دهنده[4] شبکه استفاده می‌شود. نرم‌افزارها و داده‌های لازم درسرویس دهنده شبکه ذخیره سازی می‌شود و سایر ایستگاه‌های شبکه که مشتری[5] نام دارند، قادر به استفاده از آنها می‌باشند. سرعت انتقال اطلاعات در شبکه‌های محلی بسیار بالا می‌باشد. نویزپذیری اطلاعات و احتمال

---

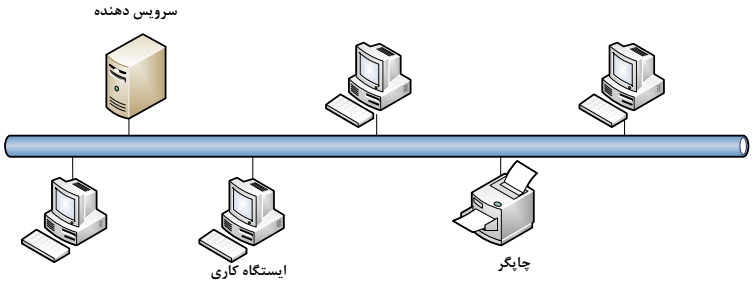
۱ Electronic mail (E-mail)
۲ Local Area Network
۳ Workstations
٤ Server
٥ Client

اتلاف داده‌ها در شبکه‌های محلی بسیار پایین است. شبکه‌های محلی معمولاً دارای تملک خصوصی می‌باشند. شبکه‌های اترنت، حلقه نشانه[۱] و گذرگاه نشانه[۲] مثال‌هایی از این نوع شبکه‌ها می‌باشند.

- ***شبکه‌های شهری*** **(MAN[3])** : همانطوری که از نام این شبکه‌ها معلوم می‌شود، شبکه‌های شهری از نظر گستردگی در سطح یک شهر می‌باشند. از شبکه‌های شهری می توان برای اتصال شبکه‌های کوچکتر محلی به یکدیگر استفاده نمود. همچنین شبکه‌های انفرادی مثل شبکه تلوزیون کابلی که در سطح شهر گستردگی دارد نیز ازاین نوع شبکه‌ها می‌باشد. چنانچه شرکتی دارای چندین شعبه در سطح شهر باشد، با استفاده از امکانات شبکه‌های شهری، قادر به اتصال شبکه‌های محلی خود به یکدیگر است. شبکه‌های شهری می‌توانند به هر دو صورت خصوصی و یا عمومی اداره و مدیریت شوند. به‌عنوان مثال شبکه‌های DQDB[4] و SMDS[5] از نوع شبکه‌های شهری می‌باشند.
- ***شبکه‌های گسترده*** **(WAN[6])*:*** این نوع شبکه‌ها دارای وسعت بسیار زیادی (درسطح یک کشور و یا حتی کل جهان) می‌باشند. به‌عنوان مثال شبکه‌های ملی هر کشور و یا شبکه جهانی اینترنت و شبکه تلفن، نمونه‌هایی از شبکه‌های گسترده هستند. برخلاف شبکه‌های محلی که به سخت افزار خاصی وابسته می‌باشند، در شبکه‌های گسترده امکان استفاده از تجهیزات متفاوتی که در فواصل طولانی به یکدیگر متصل شده اند، وجود دارد. شبکه‌های گسترده ای که توسط یک شرکت مدیریت و مورد استفاده قرار می گیرند، شبکه‌های enterprise نامیده می شوند. برخی از استانداردهای شبکه‌های گسترده عبارتند از: ATM, ISDN, MPLS[7] وX.25. در شکل (۱-۳)، انواع شبکه‌های کامپیوتری شامل شبکه‌های محلی، شبکه‌های شهری و شبکه‌های گسترده نشان داده شده است.

۱-۴-۳- ساختار شبکه‌های کامپیوتری

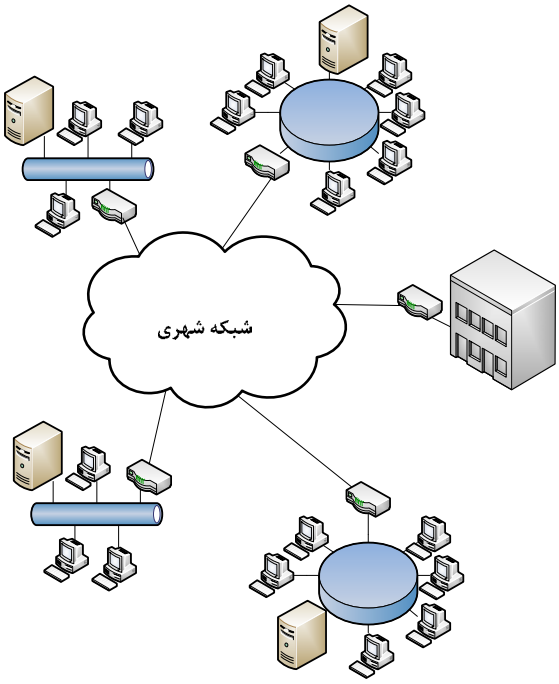
در شکل (۱-۴)، ساختار کلی شبکه‌های کامپیوتری نشان داده شده است. همانطور که در شکل دیده می‌شود، شبکه‌های کامپیوتری ازدو قسمت اصلی تشکیل شده‌اند که عبارتند از زیرشبکه[8] و کامپیوترهای میزبان[9].



(الف)

---

[۱] Token ring
[۲] Token bus
[۳] Metropolitan Area Network
[٤] Distributed Queue Dual Bus
[٥] Switched Multi-megabit Data Services
[٦] Wide Area Network
[۷] Multi-Protocol Label Switching
[۸] Subnet
[۹] Host

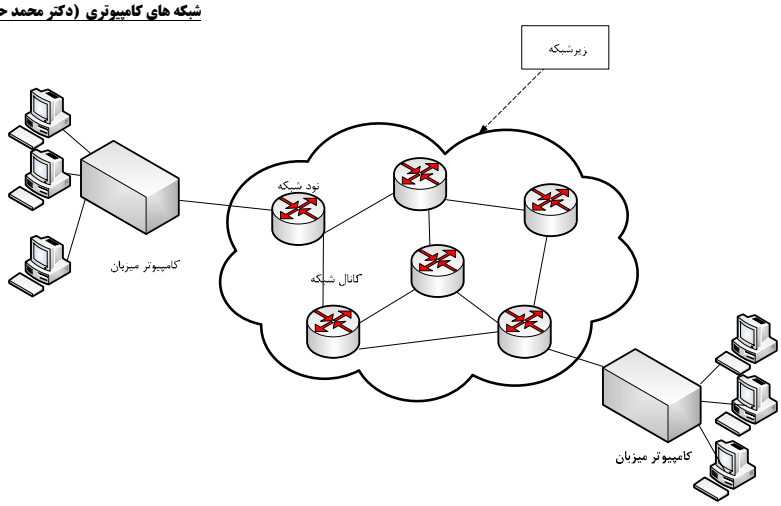


(ب)

(ج)

شکل (۱-۳): انواع شبکه‌های کامپیوتری الف) شبکهٔ محلی ب) شبکهٔ شهری ج) شبکهٔ گسترده

وظیفهٔ اصلی زیرشبکه، انتقال و هدایت پیام‌ها و اطلاعات کاربران از مبدأ به مقصد می‌باشد. کاربران شبکه از طریق کامپیوترهای میزبان اطلاعات ارسالی خود را به زیرشبکه می‌فرستند و زیرشبکه نیز اطلاعات دریافتی را به سمت مقصد هدایت و مسیریابی می‌نماید.



شکل (۱-۴) : ساختار شبکه‌های کامپیوتری

زیر شبکه خود نیز از دو قسمت تشکیل می‌شود که عبارتند از: خطوط انتقال[1] و نودهای شبکه. نودهای شبکه با نام‌های مرکز سوئیچ و IMP[2] نیز شناخته می‌شوند. هر بسته ارسالی کامپیوترهای میزبان، بعد از ورود به زیرشبکه تحویل نودهای شبکه می‌شود و در آن‌جا منتظر می‌ماند تا عملیات سوئیچینگ یا مسیریابی بر روی آن انجام شود و کانال خروجی مناسب آن پیدا گردد. سپس ازطریق کانال خروجی تحویل نود یا کامپیوتر میزبان بعدی می‌شود. به این دلیل در اصطلاح گفته می‌شود که شبکه‌های کامپیوتری به صورت " ذخیره و هدایت پیشرو" [3] عمل می‌کنند.

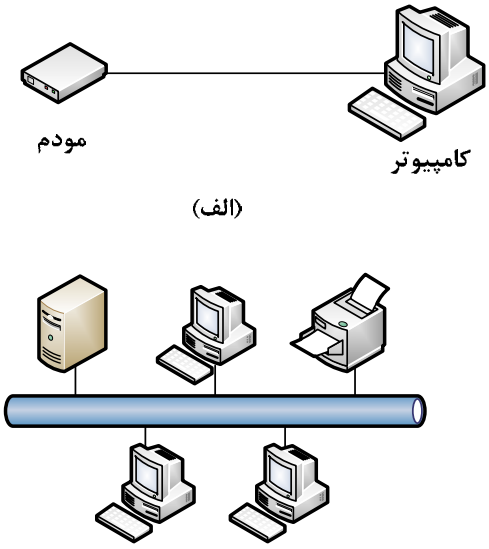
در شبکه‌های کامپیوتری دو نوع کانال شبکه موجود است که عبارتند از:

- کانال‌های نقطه به نقطه[4]
- کانال‌های پخشی[5]

در شکل (۱-۵) این دو نوع کانال نشان داده شده است. همان‌طور که از شکل مشهود است، در کانال‌های نقطه به نقطه یک مسیر اختصاصی بین دو نقطه انتهایی وجود دارد. از کانال‌های نقطه به نقطه، فقط دوایستگاهی که در انتهای کانال به آن متصل هستند، می‌توانند استفاده نمایند.

---

۱ Channel
۲ Interface Message Processor
۳ Store and forward
٤ Point to point
٥ Broadcast



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

در کانال‌های پخشی، تمام کامپیوترهای متصل به کانال از یک مسیر مشترک برای ارسال و دریافت اطلاعات استفاده می‌نمایند. ازآنجایی‌که در کانال‌های پخشی تمام ایستگاه‌ها از طریق یک کانال مشترک اقدام به ارسال و دریافت بسته‌ها می‌کنند، این احتمال وجود دارد که بسته‌های ارسالی ایستگاه‌های مختلف با یکدیگر تداخل نموده و از بین بروند. بنابراین یکی از مهمترین مشکلات کانال‌های پخشی، تصادم[۱] بسته‌ها می‌باشد.

در شبکه‌های کامپیوتری، نحوهٔ اتصال کامپیوترها به یکدیگر از طریق کانال‌های انتقال، توپولوژی شبکه نامیده می‌شود. به‌طور کلی هفت نوع توپولوژی شبکه وجود دارد که عبارتند از:

- ستاره‌ای[2]
- حلقه [3]
- درخت [4]
- کامل [5]
- حلقه‌های متقاطع [۶]
- نامنظم
- گذرگاه مشترک[7]

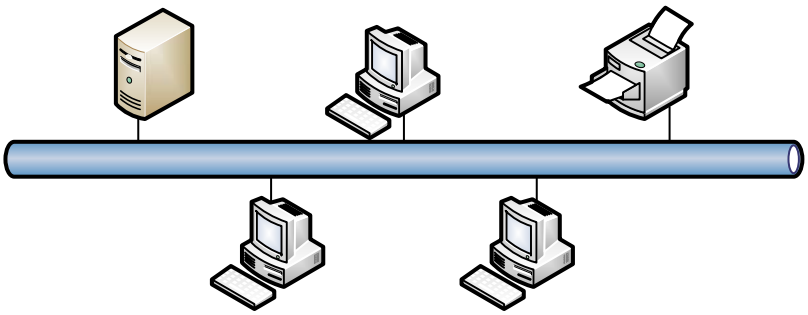
در شکل‌های (۱-۶) الی (۱-۱۱) توپولوژی‌های مختلف شبکه نشان داده شده است.

---

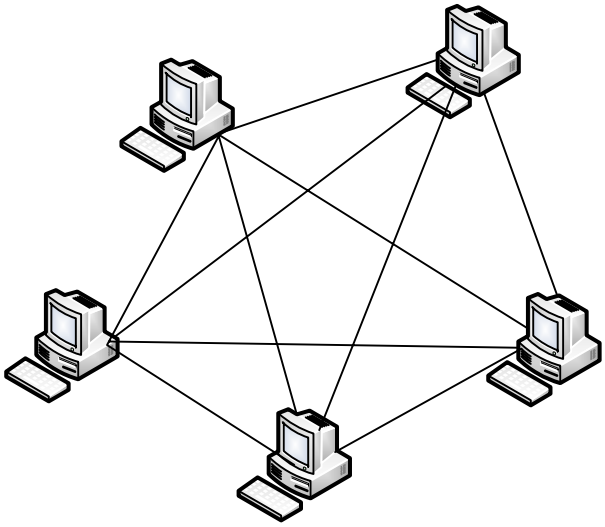
[۱] Collision
[۲] Star
[۳] Ring
[٤] Tree
[٥] Complete
[٦] Interesting ring
[۷] Bus

همان‌طور که اشاره شد، یکی از مهمترین مشکلات و مسائلی که در کانال‌های پخشی وجود دارد، امکان تداخل اطلاعات ارسالی توسط ایستگاه‌های مختلف شبکه با یکدیگر می‌باشد. ازآنجایی‌که در کانال‌های پخشی از یک محیط مشترک برای ارسال اطلاعات چندین کامپیوتر استفاده می‌شود (که این خود یک مزیت عمده کانال‌های پخشی است؛ زیرا تعداد کانال‌های مورد نیاز کاهش می‌یابد و باعث صرفه‌جویی مالی می‌شود). بنابراین باید کانال به‌طور مناسب در اختیار کاربران قرار داده شود. دو روش عمده تخصیص کانال به کاربران وجود دارد که عبارتند از: تخصیص کانال به صورت ایستا[1] و تخصیص کانال به صورت پویا[2].

در روش تخصیص کانال به صورت ایستا، از روش تقسیم زمانی استفاده می‌شود. به این ترتیب که زمان به برش‌های ثابتی تقسیم‌بندی می‌شود و هر ایستگاه اجازهٔ دسترسی به کانال را در یک برش زمانی خاص دارد. هر برش زمانی به یک ایستگاه اختصاص دارد و سایر ایستگاه‌ها اجازه ارسال اطلاعات را ندارند، که این امر باعث عدم وجود تداخل می‌شود. 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 می‌ماند و از ظرفیت آن به‌طور بهینه استفاده نمی‌شود. همچنین چنانچه تعداد ایستگاه‌ها زیاد باشد، زمان انتظار برای دستیابی به کانال برای هر ایستگاه نیز زیاد خواهد بود.

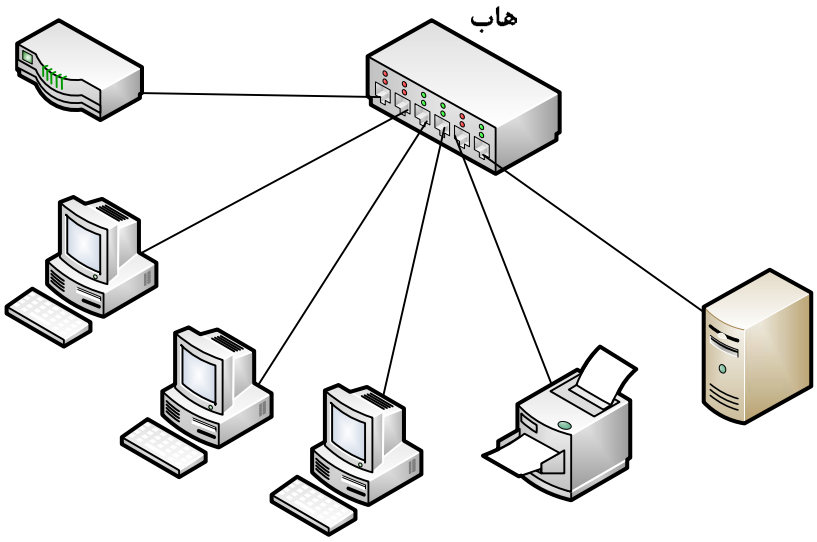


شکل (۱-۶): توپولوژی گذرگاه مشترک

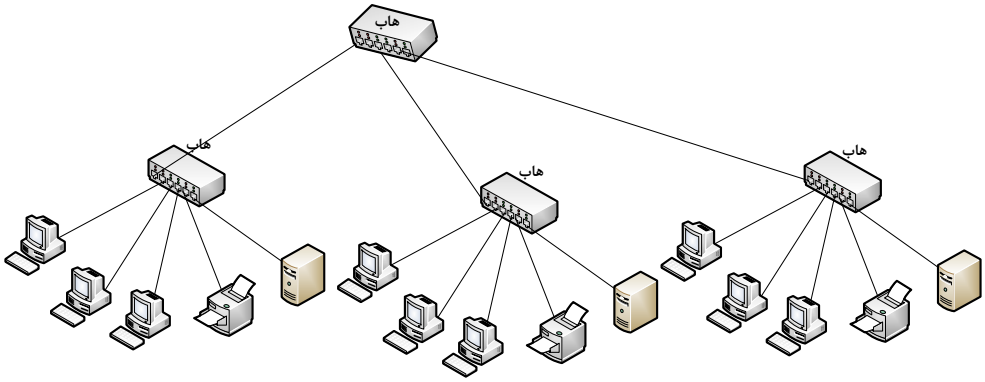


شکل(۱-۷): توپولوژی کامل

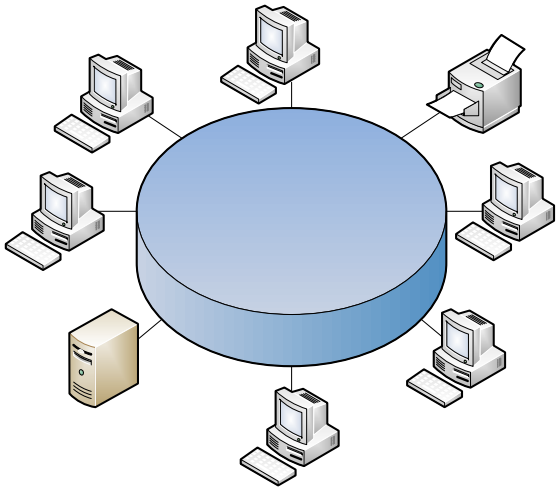
[1] Static channel allocation
[2] Dynamic channel allocation



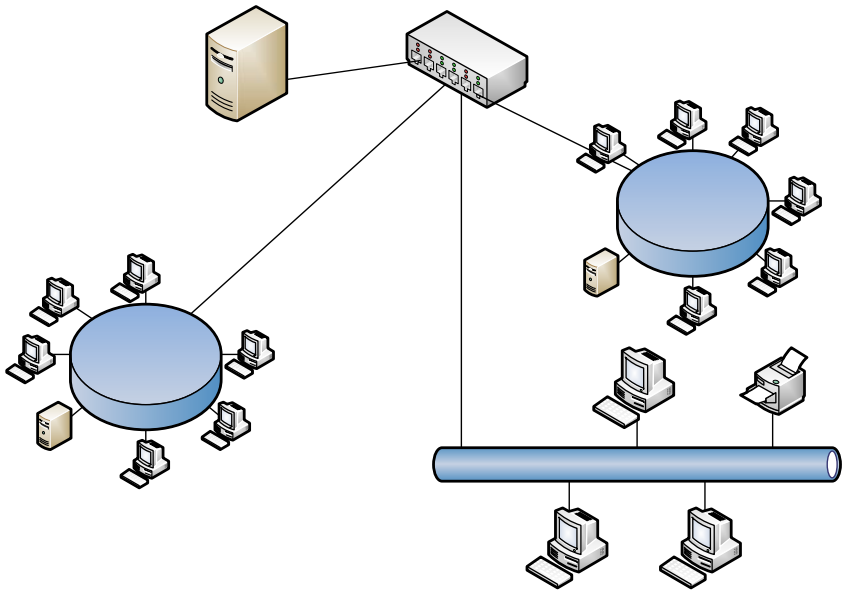
شکل (۱-۸): توپولوژی ستاره ای



شکل (۱-۹): توپولوژی درخت



شکل (۱-۱۰): توپولوژی حلقه

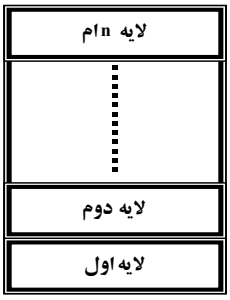


شکل (۱-۱۱): توپولوژی ترکیبی

روش تخصیص کانال به صورت پویا، خود به دو نوع تقسیم می‌شود 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 تصمیم‌گیری در مورد ارسال یا عدم ارسال سایر ایستگاه‌های شبکه می‌باشد. هر ایستگاه شبکه قبل از ارسال اطلاعات، ابتدا باید مجوز ارسال را از ایستگاه مرکزی دریافت دارد و بعد از آن‌که مجوز ارسال را دریافت نمود، قادر به ارسال اطلاعات می‌باشد. در روش غیرمرکزی، ایستگاه مرکزی در شبکه موجود نیست، بلکه خود ایستگاه‌ها در مورد ارسال یا عدم ارسال خود تصمیم‌گیری می‌نمایند. امروزه اکثر شبکه‌های محلی از کانال‌های پخشی و تخصیص کانال به صورت پویا استفاده می‌کنند.

۱-۴-۴- ساختار لایه‌ای و معماری شبکه[1]

در شبکه‌های کامپیوتری جهت برقراری ارتباط و تبادل اطلاعات بین دو کامپیوتر میزبان، یک‌سری عملیات باید انجام شود. جهت کاهش پیچیدگی شبکه و افزایش انعطاف‌پذیری آن در مقابل تغییرات احتمالی، عملیات یک شبکه به صورت لایه‌های مختلفی تقسیم‌بندی می‌گردد. به‌طوری که هر لایه برروی لایه دیگری قرار دارد و با آن در ارتباط است. هر لایه شبکه وظایف خاص خود را به عهده دارد و از لایه‌های دیگر مستقل می‌باشد. در مدل لایه‌ای شبکه، هر لایه ازسرویس لایه پایین‌تر خود استفاده می‌نماید که به لایه بالاتر خود سرویس می‌دهد. هر لایه شبکه برای انجام وظایف خود از یک‌سری قواعدو قراردادهای استاندارد استفاده می‌نماید که به آن پروتکل گفته می‌شود. یک شبکهٔ کامپیوتری ممکن است از چندین لایه برای انجام عملیات و وظایف خود استفاده نماید. به مرز بین دو لایه مجاور، واسط[2] گفته می‌شود. تبادل اطلاعات بین لایه‌های مجاور از طریق واسط‌های لایه‌ها انجام می‌گردد. در مدل لایه‌ای شبکه، کاربران شبکه از طریق بالاترین لایه شبکه، از سرویس و امکانات شبکه استفاده می‌نمایند. اطلاعات ایجاد شده در بالاترین لایه شبکه، برای ارسال به شبکه و تحویل به مقصد، باید از لایه‌های مختلف شبکه عبور نماید تا به پایین‌ترین لایه برسد و ازطریق محیط فیزیکی وارد زیرشبکه گردد. در شکل (۱-۱۲) مثالی از مدل لایه‌ای شبکه آورده شده است.



شکل (۱-۱۲): مثالی از مدل لایه‌ای شبکه

مجموع لایه‌ها و پروتکل‌های یک شبکه را معماری شبکه می‌گویند. با استفاده از مشخصات و اطلاعات موجود از معماری یک شبکه می‌توان نرم‌افزارها و سخت‌افزارهای هر لایه را طراحی و تولید نمود.برای درک بهتر مدل لایه‌ای شبکه به یک مثال توجه نمایید. فرض کنید که مدیران عامل دو شرکت بین‌المللی می‌خواهند با یکدیگر ارتباط برقرار نمایند. چنانچه این دو مدیرعامل به زبان‌های یکدیگر آشنا نباشند، هر یک باید یک مترجم استخدام نماید. مترجمان نیز از طریق امکانات مخابراتی پیام وسخنان خود را به اطلاع یکدیگر می‌رسانند. در این حالت یک مدیرعامل متن پیام خود را به مترجم خود تحویل می‌دهد. مترجم نیز با استفاده از امکانات مخابراتی پیام را برای مترجم مقابل خود ارسال می‌دارد. در آن‌جا، مترجم متن پیام را به زبان اصلی برمی گرداند و تحویل مدیرعامل می‌دهد. طبیعی است در مثال اخیر دو مدیرعامل (بالاترین لایه) نمی‌توانند به‌طور مستقیم اطلاعات و پیام خود را ارسال دارند، بلکه باید از طریق مترجم و امکانات مخابراتی (لایه‌های پایین‌تر) این کار را انجام دهند. در ساختار لایه‌ای با مسائل و مشکلات مختلفی روبرو هستیم که در زیر به ذکر هر یک از این مسائل و روش حل آنها می‌پردازیم:

---

[1] Network architecture
[2] Interface

۱. ***نیاز به مکانیسمی برای برقراری و قطع ارتباط:*** ازآنجایی‌که در یک شبکهٔ کامپیوتری تعداد زیادی کامپیوتر موجود می‌باشد که هر یک نیز می‌تواند شامل چندین فرآیند مختلف در حال اجرا باشد، بنابراین هر لایه شبکه برای برقراری و قطع ارتباط با لایهٔ متناظر خود درطرف مقابل باید مجهز به مکانیسم‌های خاصی باشد. برای این کار نیاز به نوعی آدرس‌دهی برای تعیین فرآیند طرف مقابل می‌باشد.

۲. ***عدم تطابق سرعت لایه‌های فرستنده و گیرنده:*** در یک مدل لایه‌ای شبکه این امکان وجود دارد که دو لایه متناظر با سرعت یکسان اطلاعات را برای یکدیگر ارسال ننمایند. 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 بافرمیانی و فیدبک ارسالی بین مبدأ و مقصد تا حدی مشکل فوق را حل می کند.

۳. ***محدودیت اندازه بسته‌ها:*** یکی دیگر از مشکلات موجود در مدل لایه‌ای این است که بسته‌های ارسالی هرلایه دارای حداکثر طول معینی می‌باشند. بنابراین هنگام ارسال بسته‌های یک لایه به لایه پایین‌تر، چنانچه حداکثر طول بسته‌های لایه پایین‌تر از طول بسته‌های دریافتی لایهٔ بالا کمتر باشد، در این صورت امکان ارسال چنین بسته‌هایی وجود ندارد. یکی از روش‌های حل این مشکل، تکه‌سازی[1] بسته‌ها به بسته‌های کوچکتر است. در گیرنده نیز بسته‌های تکه‌تکه شده بازسازی می‌گردند و بستهٔ اولیه استخراج می‌شود.

۴. ***وقوع خطا در بسته‌های دریافتی:*** ازآنجایی‌که بسته‌های ارسالی یک لایه درنهایت وارد زیرشبکه شده و از طریق کانال‌های مخابراتی به سمت مقصد ارسال می‌شوند، این امکان وجود دارد که ضمن ارسال بسته‌ها، خطاهایی در آنها اتفاق بیفتد. برای تشخیص و درصورت امکان تصحیح این خطاها باید چاره‌ای اندیشیده شود. یکی از روش‌های متداول، استفاده از مکانیسم‌های کنترل خطا می‌باشد. در این مکانیسم‌ها لایه فرستنده به اطلاعات ارسالی یک‌سری اطلاعات اضافه الحاق می‌نماید. لایه گیرنده با پردازش بر روی اطلاعات دریافتی، متوجه وقوع خطای احتمالی در اطلاعات می‌شود.

۵. ***عدم رعایت ترتیب بسته‌ها:*** چنانچه بین کامپیوتر میزبان مبدأ و مقصد چندین مسیر مختلف موجود باشد، در این صورت این امکان وجود دارد که بسته‌های ارسالی از مسیرهای مختلف به مقصد فرستاده شوند. ازآنجایی‌که مسیرهای ارسالی بسته‌ها، الزاماً با یکدیگر یکسان نمی‌باشند، بنابراین ممکن است که بسته‌های ارسالی در مقصد به ترتیب دریافت نشوند. برای رفع این مشکل از شمارهٔ بسته[2] استفاده می گردد. هر بستهٔ ارسالی دارای یک شمارهٔ منحصربه‌فرد می‌باشد که به ترتیب ارسال بسته‌ها این شماره نیز یک واحد افزایش می‌یابد. درسمت گیرنده با بررسی شمارهٔ بسته، رعایت یا عدم رعایت ترتیب بسته‌ها مشخص می شود. در مدل لایه‌ای برای تعیین تعداد لایه‌ها باید نکات زیر را در نظر داشت :

- یک لایه هنگامی ایجاد می‌شود که نیاز به سطح جدیدی از جداسازی عملیات داشته باشیم.
- هر لایه، عملیات مشخص و تعریف شده‌ای را انجام می‌دهد.
- عملیات هر لایه توسط پروتکل‌های استاندارد بین‌المللی مشخص می‌شود.
- مرز بین لایه‌ها باید طوری انتخاب شودکه جریان عبوراطلاعات ازنقاط واسط حداقل گردد.
- تعداد لایه‌ها باید به اندازهء کافی بزرگ باشد که بتوان بین عملیات لایه‌ها تفاوت گذاشت. از طرف دیگر تعداد لایه‌ها نباید بیش از حد زیاد باشد که باعث پیچیدگی ساختار و معماری شبکه گردد.

۱-۴-۵- مدل مرجع OSI

---

[1] Fragmentation
[2] Sequence number

در سال ۱۹۸۳ از سوی سازمان جهانی استاندارد مدل مرجع OSI ارائه گردید. این مدل برای اتصال سیستم‌های باز به یکدیگر ارائه شده‌است. یک سیستم باز در حقیقت مجموعه‌ای از پروتکل‌هایی می‌باشد که امکان اتصال دو سیستم مختلف به یکدیگر را صرفنظراز معماری لایه‌های پایینی آنها فراهم می آورد. با استفاده از مدل مرجع OSI امکان اتصال سیستم‌های مختلف و برقراری ارتباط بین آنها بدون نیاز به اعمال تغییرات در منطق سخت‌افزار و نرم‌افزار پایینی آنها وجود دارد. مدل مرجع OSI به تنهایی یک پروتکل نمی‌باشد، بلکه یک مدل مرجع برای فهم بهترو طراحی یک معماری انعطاف پذیر برای شبکه‌های کامپیوتری است. این مدل دارای ۷ لایه می‌باشد که در شکل(۱-۱۳) نشان داده شده است.مطابق با شکل فوق در مدل لایه‌ای OSI لایه‌های زیر موجود می‌باشند:

۱-۴-۵-۱- لایهٔ فیزیکی

وظیفهٔ اصلی این لایه، ارسال بیت‌های خام ۰ و ۱ بر روی کانال ارتباطی شبکه می‌باشد. تعیین سطوح ولتاژ برای بیت‌های ۰و۱ ، 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.

شکل (۱-۱۳): مدل لایه‌ای OSI

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

- ***ساختار کانال‌های اتصالی:*** همان‌طور که قبلاً نیز به آن اشاره گردید، کانال‌های ارتباطی در شبکه دارای دونوع نقطه به نقطه و پخشی می‌باشند.
- ***ارسال داده‌ها در کانال:*** برای ارسال داده‌ها بین دو سیستم کامپیوتری، سه روش ارسال وجود دارد که عبارتند از:
  - ارسال کاملاً یک طرفه[1]: در این نوع ارسال، یک طرف ارتباط همواره فرستنده و طرف دیگر همواره گیرنده می باشد.

[1] Simplex

- ارسال یک طرفه[1]: در این نوع ارسال، در هر لحظه فقط یکی از دو سیستم کامپیوتری قادر به ارسال می‌باشند. به عبارت دیگردرهرلحظه از زمان، یک طرف ارتباط فرستنده و طرف مقابل گیرنده می باشد. البته برخلاف روش کاملاً یک طرفه، هردوطرف ارتباط قادر به ارسال ودریافت اطلاعات می‌باشند(ولی در زمان‌های متفاوت).
- ارسال دوطرفه[2]: در این نوع ارسال، هر دو طرف ارتباط در هر لحظه توأم با هم قادر به ارسال و دریافت اطلاعات می‌باشند.

- ***توپولوژی:*** همان‌طور که قبلاً اشاره گردید، نحوه اتصال ایستگاه‌های شبکه به یکدیگر، توپولوژی شبکه نامیده می‌شود.
- ***نوع سیگنال:*** در لایهٔ فیزیکی برای ارسال داده‌های منطقی ۰ و ۱ ، از دو نوع سیگنال آنالوگ و دیجیتال استفاده می شود. همچنین نحوهء کدگذاری و تبدیل داده‌های ۰و ۱ منطقی به سیگنال‌های مناسب، دراین لایه مشخص می شود.
- ***واسط ارتباطی***: در لایه فیزیکی نوع واسط ارتباطی که برای اتصال ایستگاه‌های شبکه به محیط ارسال استفاده می‌شود، مشخص می‌گردد.
- ***محیط ارسال:*** برای ارسال داده‌های ۰و ۱ منطقی، به‌صورت سیگنال‌های مناسب در شبکه، محیط‌های 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- لایهٔ پیوند داده[3]

در این لایه، اطلاعات ارسالی در قالب قاب‌هایی با طول مشخص ارسال می‌شوند. این قاب‌ها به ترتیب پشت سر یکدیگر ارسال می‌گردند. معمولاً گیرنده نیز با دریافت هر قاب، یک پیام گواهی مثبت یا منفی که نشان‌دهنده دریافت صحیح و یا دریافت نادرست قاب می‌باشد، به فرستنده ارسال می‌دارد. چنانچه پیام‌های گواهی مثبت یامنفی دربین 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 می‌باشد.
- چنانچه فرستنده با سرعت بیشتر از آنچه گیرنده قادر به دریافت است، ارسال نماید در این صورت بافر گیرنده به‌سرعت پر می‌شود و اطلاعات از بین می‌رود. لایه پیوند داده با استفاده از عملیات کنترل جریان قادر به تنظیم سرعت ارسال فرستنده با سرعت دریافت گیرنده می‌باشد. بایدتوجه داشت که عملیات کنترل خطا و کنترل جریان در لایهٔ دوم، کانال به کانال انجام می‌شوند.
- در کانال‌های پخشی که چندین ایستگاه به طور مشترک ازکانال استفاده می‌نمایند، برای جلوگیری از تداخل بسته‌ها با یکدیگر باید از مکانیسم‌های مناسبی در لایه پیوند داده استفاده نمود.

---

[1] Half-duplex
[2] Full-duplex
[3] Data link layer

- در لایه پیوند داده هر ایستگاه، دارای یک آدرس منحصربه‌فرد می‌باشد که به آدرس فیزیکی مشهور است. ازآنجائی‌که ایستگاه‌های مختلف در شبکه دارای آدرس فیزیکی متفاوت از یکدیگر می‌باشند، امکان ارسال و دریافت قاب‌ها بین آنها وجود دارد.
- در لایه پیوند داده، اطلاعات ارسالی به صورت قاب‌های 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 درسرآیند[۱] ودنباله[۲] هرقاب استفاده می‌گردد.

پروتکل‌هایی نظیر HDLC[3] و SDLC[۴] مثال‌هایی از استانداردهای لایهٔ دوم می‌باشند.

۱-۴-۵-۳- لایهٔ شبکه[۵]

لایهٔ شبکه موظف به کنترل زیر شبکه می باشد. هنگامی‌که یک بسته اطلاعاتی از کامپیوتر میزبان مبدأ به کامپیوتر میزبان مقصد ارسال می‌شود، لایهٔ شبکه موظف به مسیریابی[۶] و هدایت صحیح بسته درون زیر شبکه می‌باشد. چنانچه به‌طور ناگهانی تمام کاربران شبکه اقدام به ارسال بسته به درون زیر شبکه نمایند در این صورت شبکه با ازدحام[۷] روبرو می‌شود. ایجاد ازدحام در شبکه باعث کاهش کارآیی و کیفیت سرویس می‌شود که امری نامطلوب است. کنترل ازدحام و رفع آن از وظایف اصلی لایهٔ شبکه است. ارتباط بین شبکه‌ای[۸] یکی دیگر از وظایف لایهٔ شبکه می‌باشد. هنگامی‌که بسته‌های ارسالی کاربران در راه رسیدن به مقصد ازشبکه‌های میانی دیگری عبور نمایند، مشکلات ومسائل زیادی در ورود بسته به شبکه جدید به‌وجود می‌آید. برخی ازاین مشکلات عبارتنداز: عدم تطابق نحوهٔ آدرس‌دهی دوشبکه، عدم یکسان‌بودن اندازه بسته‌های دو شبکه و یا عدم تطابق پروتکل‌های دو شبکه. رفع مشکلات فوق و فراهم‌آوردن سرویس لازم برای اتصال شبکه‌ها به یکدیگر، از وظایف لایهٔ شبکه است.

آدرس دهی منطقی، تبدیل آدرس‌های منطقی به آدرس‌های فیزیکی و تسهیم‌سازی کانال که به کمک آن امکان استفاده مشترک همزمان چندین وسیله ازکانال فراهم می آید، از دیگر وظایف لایه سوم می‌باشد.

۱-۴-۵-۴- لایهٔ حمل[۹]

این لایه، بسته‌های لایهٔ بالاتر را دریافت می‌دارد و آنها را در صورت لزوم به قطعات کوچکتری تقسیم می‌نماید و به لایهٔ شبکه ارسال می‌کند. لایه حمل برای سرویس‌دهی به لایه جلسه، موظف به برقراری اتصال‌های مختلف با مقصد می‌باشد. عملکرد این لایه به صورت انتها به انتها است. این مطلب به این معنی می‌باشد که اتصال‌های 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

فقط بین کامپیوترهای میزبان انتهایی ایجاد می‌شوند. برخلاف لایهٔ شبکه که موظف به تحویل تک‌تک بسته‌های ارسالی به مقصد می‌باشد، لایه حمل موظف به تحویل سالم و بدون خطای کل پیام ارسالی به لایهٔ همتای خود در مقصد است.

ازآنجائی‌که اکثر کامپیوترهای شبکه قادر به اجرای همزمان چندین نرم افزار مختلف می‌باشند، تحویل صحیح بسته‌ها از مبدأ به مقصد تنها به معنی سالم رساندن بسته ها به کامپیوتر مقصد نمی باشد، بلکه بسته هر نرم‌افزار اجرایی در سمت مبدأ باید به همان نرم‌افزار متناظر خود در سمت مقصد برسد. برای انجام این کار، لایه حمل در شبکه‌های کامپیوتری از آدرس خاصی به نام آدرس درگاه[۱] استفاده می نماید. لایه شبکه با استفاده از آدرس منطقی بسته‌ها، آنها را به کامپیوتر مقصد می‌رساند. در سمت مقصد، لایه حمل با استفاده از آدرس سوکت، هربسته را به نرم‌افزار مربوط به آن تحویل می‌دهد.

لایهٔ 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 لایهٔ حمل در طی سه مرحله انجام می‌شود که عبارتند از: برقراری اتصال، ارسال داده و قطع اتصال. با استفاده از مسیر منطقی ایجاد شده توسط هر اتصال، لایهٔ حمل قادر به انجام عملیات مرتب‌سازی بسته‌ها، کنترل جریان و تشخیص و تصحیح خطا می‌باشد.

۱-۴-۵-۵- لایهٔ جلسه[۲]

با کمک امکانات این لایه، کاربران مختلف شبکه که بر روی کامپیوترهای میزبان متفاوتی قرار دارند، قادر به برقراری جلسه بین یکدیگر می‌باشند. ورود به یک کامپیوتر از راه دور و انتقال فایل بین دو ماشین شبکه، مثال‌هایی از جلسات این لایه می‌باشند. مدیریت نشانه[۳] از سایر وظایف این لایه به شمار می‌آید. چنانچه در برخی از پروتکل‌ها نخواهیم که دو طرف جلسه همزمان اقدام به شروع به کار نمایند، در این صورت برای مدیریت این کار، لایهٔ جلسه نشانه‌هایی بین دو کامپیوتر مبدأ و مقصد مبادله می‌نماید. کامپیوتری که این نشانه را در اختیار دارد قادر به انجام عملیات حساس مشخص شده می‌باشد.

یکی دیگر از وظایف این لایه، همزمانی است. برای درک بحث همزمانی، به ذکریک مثال می پردازیم. فرض کنید که در حال ارسال یک فایل بسیار پرحجم از یک کامپیوتر به کامپیوتر دیگری می‌باشیم. چنانچه در حین ارسال ارتباط قطع شود، باید انتقال اطلاعات دوباره ازسرگرفته شود. برای رفع این مشکل، لایه جلسه با کمک امکانات همزمانی قادر می‌باشد که در صورت قطع ارتباط فقط از همان نقطهٔ قطع قبلی، دوباره اطلاعات را ارسال کند.

۱-۴-۵-۶- لایهٔ ارائه[۴]

یکی از وظایف لایه ارائه، تبدیل کدها به یکدیگر می‌باشد. چنانچه دو کامپیوتر که از کدهای متفاوتی برای ثبت و نمایش اطلاعات استفاده می‌نمایند (مانند کدهای ASCII[5] و یا EBCDIC[6]) بخواهند با یکدیگر ارتباط برقرار کنند، با استفاده از امکانات لایه ارائه تبدیل کدها به یکدیگر انجام می‌شود. سایر وظایف این لایه عبارتست از:

---

[۱] Port address

[۲] Session layer

[۳] Token management

[۴] Presentation layer

[۵] American Standard Code for Information Interchange

[۶] Extended BCD Information Code

- ***رمزنگاری***[1]*:* دراین لایه برای افزایش امنیت در ارسال داده‌ها (به‌خصوص در کاربردهایی نظیر تجارت الکترونیکی) از روش‌های رمزنگاری استفاده می شود.
- ***فشرده سازی:*** برای کاهش زمان ارسال داده‌ها، و استفاده کارآمدتر از شبکه، از روش‌های فشرده‌سازی در این لایه استفاده می‌شود.
- ***امنیت:*** یکی دیگر از وظایف این لایه، تأمین امنیت ارتباط از طریق ایجاد شناسه کاربر و کلمهٔ رمز عبور می‌باشد.

۱-۴-۵-۷- لایهٔ کاربرد[2]

کاربران شبکه از طریق امکانات و پروتکل‌های این لایه قادر به استفاده ازسرویس شبکه می‌باشند. در لایه کاربرد، نرم‌افزارهای کاربردی متنوع نظیر پست الکترونیکی، انتقال فایل، اتصال از راه دور به یک ماشین وغیره در اختیار کاربران قرار می‌گیرد. یکی دیگر از وظایف لایه کاربرد، ایجاد ترمینال مجازی[3] 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 لایه‌ای شبکه، اطلاعات ارسالی کاربر در بالاترین لایه ایجاد می‌شود و به ترتیب از لایه‌های شبکه عبور می کند تا وارد لایه فیزیکی گردد و از آنجا وارد شبکه می‌شود. در مدل لایه ای، هر لایه شبکه دارای وظایف خاصی می‌باشد که برای انجام وظایف خود به بسته‌های دریافتی از لایه بالاتر یک‌سری اطلاعات سرآیند اضافه می‌نماید و بسته ایجادشده را تحویل لایه پایین‌تر از خود می‌دهد. لایه پایین‌تر نیز این عمل را تکرارمی نماید و به بسته دریافتی از لایه بالاتر خود، سرآیند اضافه می کند و آن را تحویل لایه پایین‌تر می‌دهد. البته در بعضی از لایه‌ها به خصوص در لایه دوم، علاوه بر سرآیند ممکن است که یک‌سری اطلاعات دنباله نیز به آخر بسته ها اضافه شود.

بنابراین با عبور بسته‌ها از لایه‌های مختلف شبکه، هر لایه برای انجام وظایف خود، یک‌سری اطلاعات به بسته‌ها اضافه می‌نماید که باعث افزایش طول بسته می شود. در پایین‌ترین لایه یعنی لایه فیزیکی، بسته‌های دریافتی بیت به بیت ارسال می‌شوند تا اینکه با عبور از شبکه و مسیریابی تحویل مقصد شوند. درسمت مقصد، بسته دریافتی از پایین‌ترین لایه تحویل لایه‌های بالاتر می‌شود. هر لایه موظف به پردازش برروی سرآیند ایجادشده توسط لایه متناظر در مبدأ می‌باشد. هر لایه در مقصد سرآیند یا دنباله ایجاد شده توسط مبدأ را حذف نموده و سپس بسته را تحویل لایه بالاتر خود می‌دهد. 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 برمی‌دارد و آن را حذف می‌نماید تا این‌که داده‌های خالص تحویل بالاترین لایه شوندو کاربرقادر به استفاده از آنها می‌شود.

در شکل (۱-۱۴) مراحل ارسال و دریافت بسته‌ها در یک شبکه مبتنی بر مدل لایه‌ای OSI نشان داده شده است. در مدل OSI به سه لایه پایینی(فیزیکی، پیوند داده وشبکه) لایه‌های شبکه گفته می‌شود. همچنین چهار لایه بالایی (حمل،جلسه،ارائه وکاربرد)، لایه‌های کاربر نامیده می شوند. نودهای میانی شبکه تنها حداکثر تا لایه سوم را دارا می‌باشند،

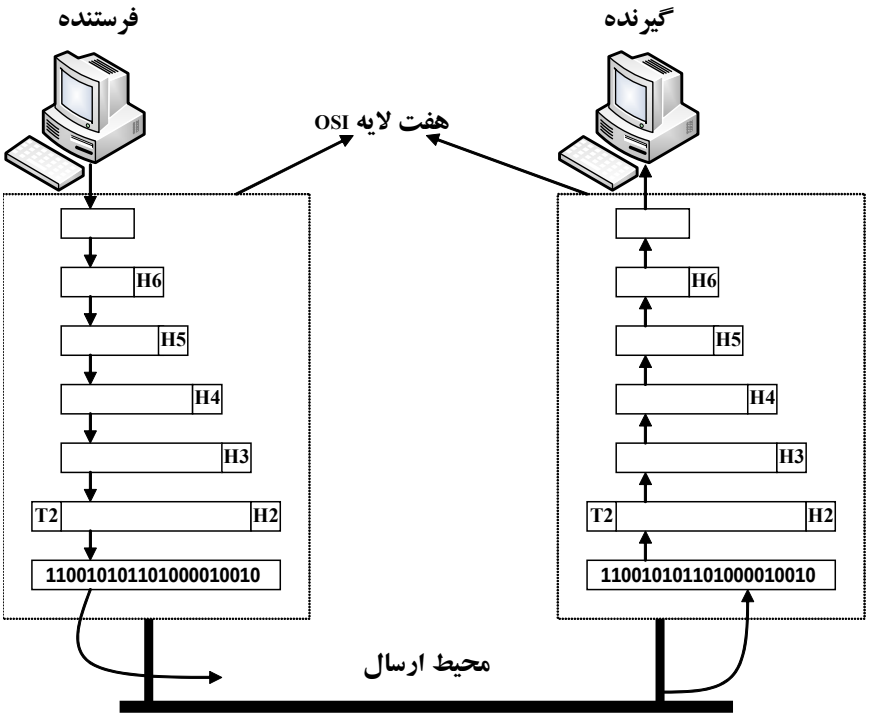
---

[1] Encryption

[2] Application layer

[3] Virtual terminal

ولی کامپیوترهای میزبان تمام هفت لایه را شامل می‌شوند. بسته‌های ارسالی هر لایه که شامل داده‌های لایه بالاتر و اطلاعات سرآیند همان لایه می‌باشند، دراصطلاح واحد داده‌ای پروتکل(PDU[1]) نام دارند.



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

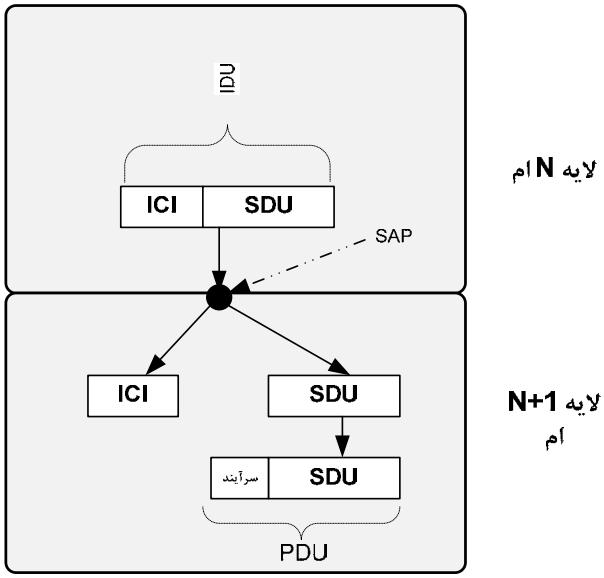
همان‌طور که قبلاً اشاره شد، در مدل OSI هر لایه شبکه باید به لایه بالاتر از خود سرویس بدهد. هر لایه برای ارائه سرویس خود به لایه بالاتر، از عناصر فعال خود که موجودیت[2] نام دارند استفاده می‌نماید. یک موجودیت در یک لایه شبکه می‌تواند یک فرآیند نرم‌افزاری و یا یک واحد سخت‌افزاری باشد. درهردوسمت فرستنده وگیرنده و درهرلایه، موجودیت‌های متناظر وجود دارند که دراصطلاح به آنها موجودیت‌های همتا[3] گفته می‌شود. سرویسی را که لایه Nام به لایه بالاتر از خود (لایه N+1ام) ارائه می‌دهد بوسیله موجودیت‌های آن لایه انجام می‌شود.

سرویس ارائه شده لایه از طریق نقاط دسترسی به سرویس (SAP[4]) در اختیار لایه بالاتر قرار می‌گیرد. هر نقطه دسترسی به سرویس در مدل لایه‌ای دارای آدرس مشخص و معینی می‌باشد. به‌عنوان 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 می‌شود. شماره تلفن نیز آدرس نقطه دسترسی به سرویس تلفن می‌باشد. در سیستم عامل یونیکس، نقاط دسترسی به سرویس، سوکت می‌باشند و آدرس نقاط دسترسی به سرویس همان شماره سوکت‌ها هستند.

---

[1] Protocol Data Unit
[2] Entity
[3] Peer entity
[4] Service Access Point

قبل از ارسال اطلاعات بین دو لایه، آن‌دو باید به یک‌سری توافقات اولیه در مورد قواعد و ویژگی‌های هر لایه برسند. مطابق با شکل (۱-۱۵)، لایه N+1 ام شبکه از طریق یک نقطه دسترسی به سرویس، یک واحد داده‌ای به نام واحد داده‌ای واسط (IDU[1]) را به موجودیت فعال لایه N ام ارسال می‌دارد. هر واحد داده ای واسط از دو قسمت تشکیل شده است که عبارتند از: واحد داده‌ای سرویس (SDU[2]) و اطلاعات کنترلی واسط (ICI[3]) . از اطلاعات کنترلی واسط برای انجام امور کنترلی خاص استفاده می‌شود و جزو داده‌های ارسالی نمی‌باشد. هر لایه از اطلاعات کنترلی واسط لایه بالاتر خود استفاده می‌نماید و بعد از استفاده، آنها را از بین می‌برد. لایهN 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 هرتکه سرآیند مناسب اضافه می شود و کل بسته درقالب یک واحد داده ای پروتکل(PDU[4]) ارسال می گردد.



شکل(۱-۱۵): مرز مشترک دو لایه

۱-۴-۷- سرویس اتصال‌گرا و بی‌اتصال

هر لایه شبکه قادر به ارائه دو نوع سرویس مختلف به لایه بالاتر از خود می‌باشد. این دو نوع سرویس عبارتند از : سرویس اتصال‌گرا[5] و سرویس بی‌اتصال[6] . یکی از کاربردهای بارز سرویس اتصال‌گرا، 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 شماره‌گیری می‌نماید. در این مرحله شبکه تلفن درخواست کاربر را برای برقراری ارتباط دریافت می‌نماید و ارتباط کاربر را با مخاطب برقرار می‌سازد. بعد از آن‌که مخاطب گوشی تلفن خود را برداشت عملاً ارتباط برقرارمی‌شود و دو طرف، قادر به صحبت با یکدیگر می‌باشند. در نهایت پس از اتمام مکالمه با گذاشتن گوشی، ارتباط قطع می شود.

---

[1] Interface Data Unit
[2] Service Data Unit
[3] Interface Control Information
[4] Protocol Data Unit
[5] Connection oriented
[6] Connectionless

در شبکه‌های کامپیوتری اتصال گرا نیز مشابه شبکه تلفن، کاربر ابتدا از شبکه می‌خواهد که یک مسیر اولیه بین کامپیوترمبداء و مقصد برقرار نماید. پس ازآن‌که این مسیر توسط شبکه بین کاربران مبدأ و مقصد بوجود آمد، کاربران قادر به ارسال اطلاعات خود می‌باشند. پس از اتمام ارسال اطلاعات، مسیر بوجودآمده از بین می‌رود.

در سرویس بی‌اتصال، بدون آن‌که کاربرآمادگی گیرنده را بررسی نماید، اقدام به ارسال اطلاعات به شبکه می کند. طبیعی است که بسته‌های ارسالی کاربران در این نوع سرویس، به‌طور مستقل پردازش می شوند و از مسیرهای مختلف به مقصد می‌رسند. در این نوع سرویس، این احتمال وجود دارد که بسته‌ها به ترتیب به مقصد نرسند، زیرا ممکن است که بسته اول از یک مسیر طولانی‌تر نسبت به بسته دوم به مقصد برسد که این امر باعث دیرتر رسیدن بسته اول نسبت به بسته دوم در مقصد می‌شود. سیستم پست نمونه ای از سرویس بی اتصال است.

برای افزایش کیفیت و اطمینان از دریافت صحیح بسته‌ها 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 درسیستم می‌شود، ولی ازطرف دیگر باعث افزایش اطمینان و کیفیت سرویس می‌گردد. به‌عنوان مثال پروتکل انتقال فایل (FTP[1]) نوعی سرویس اتصال‌گرا همراه با پیام تصدیق می‌باشد. در سرویس پست الکترونیکی نیازی به ارسال پیام تصدیق ازطرف گیرنده نمی‌باشد و این نوع سرویس از نوع بی‌اتصال بدون پیام تصدیق است. به سرویس بی‌اتصال به دلیل شباهت آن با سیستم تلگرام، سرویس داده‌گرام[2] نیز می‌گویند.

سرویس اتصال‌گرا همراه با پیام تصدیق خود به دو نوع تقسیم‌بندی می‌شوند. در نوع اول که جریان پیام‌ها[3] نام دارد، حد و مرز پیام‌های ارسالی در گیرنده قابل تشخیص می‌باشد. به‌عنوان مثال اگر فرستنده، ۱۰ پیام یک کیلو بایتی ارسال دارد، در گیرنده نیز می‌توان این ۱۰ پیام یک کیلو بایتی را از یکدیگر تشخیص داد. ولی در نوع دوم که رشته بایت‌ها[4] نام دارد، گیرنده قادر به تشخیص و تفکیک پیام‌ها از یکدیگر نمی‌باشد. در این حالت اگر فرستنده به‌طور مثال، ۱۰ پیام یک کیلو بایتی ارسال کند، گیرنده فقط یک پیام ۱۰ کیلو بایتی دریافت می‌نمایدو نمی‌تواند تشخیص دهد که این ۱۰ کیلوبایت اطلاعات ورودی در اصل ۱۰ پیام یک کیلوبایتی متفاوت بوده است.

در بعضی از کاربردهای شبکه، که از سرویس بی‌اتصال استفاده می‌شود، ارسال پیام گواهی و تصدیق دریافت ازطرف گیرنده ضروری ولازم به نظر می‌رسد. این نوع سرویس را در اصطلاح سرویس داده‌گرام همراه با پیام تصدیق می‌نامند. به‌عنوان مثال ارسال نامه‌های سفارشی درسیستم پستی که فرستنده می‌خواهد از دریافت نامه در گیرنده مطمئن شود، نمونه‌ای از این نوع سرویس می‌باشد. نوعی دیگر از سرویس موجود در شبکه‌های کامپیوتری، سرویس درخواست- پاسخ[5] است. در این نوع سرویس، فرستنده با ارسال یک داده‌گرام، درخواست خود را برای گیرنده ارسال می‌دارد. گیرنده نیزدر پاسخ به درخواست فرستنده یک داده‌گرام که حاوی پاسخ به درخواست فرستنده است ارسال می‌کند. به‌عنوان مثال جستجو در بانک‌های اطلاعاتی نوعی سرویس درخواست ـ پاسخ است.

در هر لایه شبکه، برای ارائه سرویس اتصال‌گرا یا بی‌اتصال از یک مجموعه عملیات پایه‌ای[6] استفاده می‌شود. عملیات پایه‌ای به چهار نوع تقسیم‌بندی می‌شوند که عبارتند از:

---

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

۱- عملیات پایه‌ای درخواست[۱]: این عملیات برای اعلام درخواست انجام یک کار خاص مانند درخواست برقراری اتصال و یا درخواست ارسال داده‌ها در شبکه به کار می‌رود.

۲- عملیات پایه‌ای اعلام[۲]: هنگامی‌که در موجودیت همتا در سمت گیرنده عملیات پایه‌ای‌درخواست دریافت گردید، برای اطلاع دادن به لایه بالایی، عملیات پایه‌ای اعلام ارسال می‌شود که کاربر را از ورود یک درخواست از سمت مقابل مطلع می‌سازد.

۳- عملیات پایه‌ای پاسخ[3]: هنگامی‌که 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 پایه‌ای پاسخ استفاده می‌کند.

۴- عملیات پایه‌ای تأیید[۴]: هنگامی‌که پاسخ موجودیت همتا به درخواست فرستنده ارسال شد، در سمت فرستنده اولیه این پاسخ به صورت عملیات پایه‌ای تأیید به اطلاع آن رسیده می‌شود. به این ترتیب فرستنده متوجه می‌گردد که آیا درخواستش مورد قبول واقع شده است یا خیر؟

عملیات پایه‌ای‌می‌تواند شامل مشخصه‌هایی باشد که به کمک این مشخصه ها می توان مشخصاتی نظیر: آدرس فرستنده درخواست‌کننده، نوع سرویس درخواستی و حداکثر طول بسته‌های ارسالی را به اطلاع طرف مقابل رساند.

از نظر نحوه ارسال عملیات پایه‌ای بین دو موجودیت همتا، سرویس شبکه را می‌توان به دو نوع تقسیم‌بندی نمود که عبارتند از: سرویس تأییدشده[5] و سرویس بدون تأیید[6] . درسرویس تأییدشده، از هر چهار نوع عملیات پایه‌ای درخواست، اعلام، پاسخ و تأیید استفاده می‌شود، اما درسرویس بدون تأیید، فقط از عملیات پایه‌ای درخواست و اعلام استفاده می‌گردد.

برای درک بهتر مفاهیم عملیات پایه‌ای به یک مثال توجه می‌نماییم. فرض کنید در یک لایه برای ارائه سرویس اتصال‌گرا، هشت عملیات پایه‌ای زیر مورد استفاده قرار می‌گیرند:

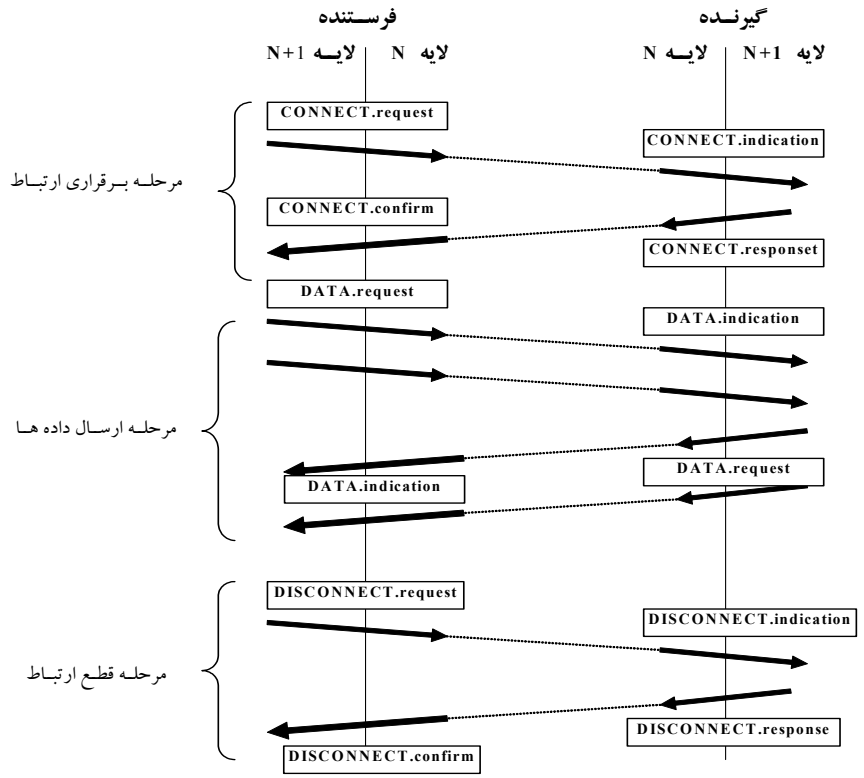
- **CONNECT.request:** از این عملیات پایه‌ای برای ارسال درخواست برقراری اتصال فرستنده استفاده می‌شود(با مقایسه با یک ارتباط تلفنی برداشتن گوشی و گرفتن شماره تلفن مخاطب می‌باشد).
- **CONNECT.indication:** در سمت گیرنده، این عملیات پایه‌ای برای آگاه‌سازی لایه بالایی از ورود یک درخواست برقراری اتصال استفاده می‌شود(در ارتباط تلفنی زنگ زدن تلفن مخاطب می‌باشد).
- **CONNECT.response:** گیرنده، برای اعلام قبول یا رد درخواست ورودی و پاسخ‌دهی به آن از این عملیات پایه‌ای استفاده می‌نماید(در ارتباط تلفنی برداشتن گوشی توسط مخاطب می‌باشد).
- **CONNECT.confirm:** این عملیات پایه‌ای برای اطلاع دادن در مورد قبول یا رد درخواست به فرستنده که درخواست‌کننده اولیه بوده است، استفاده می‌شود(در ارتباط تلفنی قطع‌شدن صدای زنگ تلفن در سمت تماس گیرنده می‌باشد).
- **DATA.request:** ازاین عملیات پایه‌ای برای ارسال داده استفاده می‌شود(در ارتباط تلفنی صحبت‌های ارسالی بین تماس گیرنده و مخاطب می‌باشد).
- **DATA.indication:** برای مطلع ساختن گیرنده نسبت به ورود داده استفاده می‌شود (درارتباط تلفنی شنیدن صحبت‌های یک طرف توسط طرف مقابل می‌باشد).

---

[۱] Request primitive
[۲] Indication primitive
[۳] Response primitive
[٤] Confirm primitive
[٥] Confirm services
[٦] Unconfirmed services

- **DISCONNECT.request**: این عملیات پایه‌ای نشان‌دهنده درخواست قطع اتصال می‌باشد(در ارتباط تلفنی، قطع ارتباط و قرار دادن گوشی برروی تلفن می‌باشد).
- **DISCONNECT.indication**: از این عملیات برای مطلع ساختن موجودیت همتا در گیرنده از درخواست قطع اتصال، استفاده می‌شود (در ارتباط تلفنی شنیدن اتمام مکالمه و گذاشتن گوشی تلفن از جانب طرف مقابل می‌باشد).

ازآنجایی‌که در مثال فوق برای برقراری اتصال از هرچهار نوع عملیات پایه‌ای استفاده می‌گردد، ولی برای قطع اتصال فقط از دو عملیات پایه‌ای استفاده می‌شود، بنابراین می‌توان نتیجه گرفت که برقراری اتصال، یک نوع سرویس تأییدشده و قطع اتصال، یک نوع سرویس بدون تأیید می‌باشد. در شکل (۱-۱۶) دیاگرام زمانی و مراحل ارسال عملیات پایه‌ای فوق بین فرستنده و گیرنده نشان داده شده است. البته در این شکل برای مرحله قطع ارتباط از ۴ عملیات پایه‌ای استفاده شده است.



شکل(۱ –۱۶): دیاگرام زمانی و مراحل ارسال عملیات پایه‌ای بین دو لایه همتای شبکه

۱-۴-۸ - سوئیچینگ

به‌طور کلی در شبکه‌های کامپیوتری دو نوع مختلف سوئیچینگ وجود دارد که عبارتند از: سوئیچینگ مداری[1] و سوئیچینگ بسته‌ای[2].

در سوئیچینگ مداری، یک مسیر فیزیکی با یک ظرفیت ثابت بین فرستنده و گیرنده ایجاد می شود. شبکه‌های سوئیچینگ مداری در حقیقت برای انتقال صوت طراحی شده‌اند. در شبکه‌های تلفن بعد از برقراری یک اتصال صوتی بین دو نقطه، این اتصال تا پایان ارتباط برقرار می‌باشد. شبکه‌های سوئیچینگ مداری برای ارسال داده‌ها مناسب نیست. یکی از مهمترین دلایل آن این است که بیشتر داده‌های کامپیوتری به صورت انفجاری[3] می‌باشند. بدین معنی که در یک لحظه از زمان حجم زیادی از داده‌ها برای ارسال وجود دارد و در یک لحظه دیگر، ممکن است هیچ داده‌ای برای ارسال موجود نباشد. بنابراین چنانچه بخواهیم از سوئیچینگ مداری برای ارسال داده‌ها استفاده نماییم، در زمان عدم ارسال داده و عدم استفاده از پهنای باند ظرفیت شبکه بدون استفاده می‌ماند و از بین می‌رود.

یکی دیگر از دلایل نامناسب بودن شبکه‌های سوئیچینگ مداری برای ارسال داده‌های کامپیوتری آن است که در شبکه‌های داده نرخ ارسال متغیر می‌باشد. در شبکه‌های داده در لحظاتی که داده‌هایی 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 می‌باشد. ازآنجایی‌که در شبکه‌های سوئیچینگ مداری ظرفیت اتصال ثابت است، بنابراین نمی‌توان از آن برای ارسال داده‌های کامپیوتری با نرخ ارسال متغیر استفاده نمود. عدم انعطاف‌پذیری شبکه‌های سوئیچینگ مداری نسبت به تغییرات، از دیگر دلایل نامناسب بودن شبکه‌های سوئیچینگ مداری برای تبادل داده‌های کامپیوتری می‌باشد. از دیگر معایب سوئیچینگ مداری، می‌توان به عدم قابلیت اولویت گذاری داده‌ها در آن اشاره نمود. برای ارسال داده‌های کامپیوتری باید مکانیسم‌هایی برای اولویت گذاری بسته‌ها وجود داشته باشد تا بتوان بین داده‌های مختلف فرق گذاشت.

در شبکه‌های سوئیچینگ بسته‌ای، داده‌های ارسالی به صورت بسته‌هایی به طول مشخص ارسال می‌شوند. شبکه‌های سوئیچینگ بسته‌ای دو نوع می‌باشند که عبارتند از:

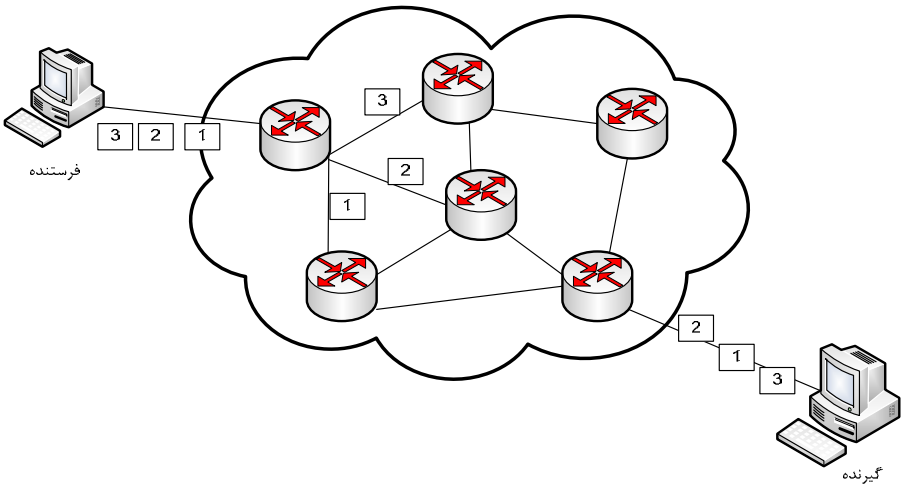
- شبکه‌های داده‌گرام
- شبکه‌های مدار مجازی[4]

شبکه‌های داده‌گرام از نوع بی‌اتصال می‌باشد. مطابق با آنچه که در شکل (۱-۱۷) نشان داده شده است، در شبکه‌های داده‌گرام بسته‌های ارسالی به‌طور مستقل از یکدیگر وارد نودهای شبکه می شود و مسیریابی می‌گردند. ازآنجایی‌که هر بسته، مستقل از سایر بسته‌ها پردازش می‌شود، این احتمال وجود دارد که بسته‌های ارسالی از مسیرهای مختلفی عبور نمایند و به ترتیب نادرست به مقصد برسد. بنابراین یکی از مهمترین مشکلات شبکه‌های داده‌گرام عدم رعایت ترتیب بسته‌ها می‌باشد.

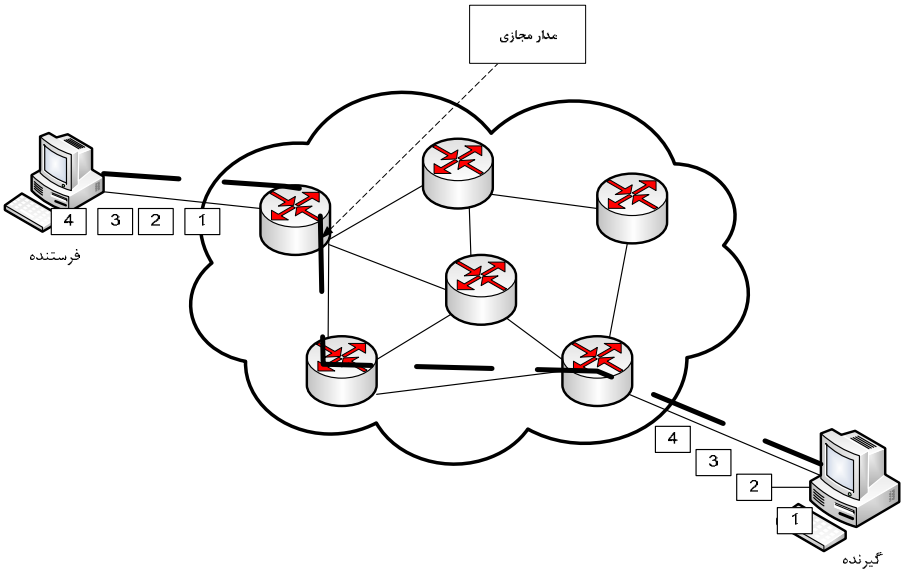
شبکه‌های سوئیچینگ بسته‌ای از نوع مدار مجازی، از روش اتصال‌گرا برای برقراری ارتباط بین مبدأ و مقصد استفاده می‌نماید. در این نوع شبکه‌ها قبل از ارسال داده‌ها، یک مدار مجازی بین فرستنده و گیرنده برقرار می‌شود و بسته‌های ارسالی بین مبدأو مقصداز مسیر مجازی به‌وجود آمده عبورمی‌نمایندو بنابراین تمامی بسته‌ها به ترتیب به مقصد می‌رسند. بعد از اتمام ارسال داده‌ها، مسیر مجازی به‌وجودآمده از بین می‌رود. در شکل(۱-۱۸) مثالی از یک شبکه مدار مجازی آورده شده است.

---

[1] Circuit switching
[2] Packet switching
[3] Bursty
[4] Virtual circuit



شکل (۱-۱۷): شبکه‌های داده‌گرام



شکل (۱-۱۸): شبکه‌های مدار مجازی

در شبکه‌های مدار مجازی، دو نوع مدار مجازی وجود دارند که عبارتند از مدار مجازی سوئیچ شده (SVC[1]) و مدار مجازی دایمی (PVC[2]). مدارهای مجازی دایمی به‌طور دائم دراختیارفرستنده وگیرنده قرار دارند و نیازی به انجام عملیات برقراری و قطع ارتباط نمی‌باشد. در مدارهای مجازی سوئیچ شده، برای برقراری مدار مجازی بین فرستنده و گیرنده، باید روال‌های خاصی انجام شود. بعد از ارسال داده‌ها، مدار مجازی سوئیچ شده آزادمی شود تا بتوان از ظرفیت آن برای سایر اتصال‌های موجود در شبکه استفاده نمود. شبکه‌های X.25 و ATM مثال‌هایی از سوئیچینگ بسته‌ای مدار مجازی هستند درحالی‌که پروتکل اینترنت ازنوع داده‌گرام است.

پرسش‌های فصل

۱. حداقل ۱۰ مورد از کاربرد کامپیوتر درجامعه را نام ببرید.

---

[1] Switched Virtual Circuit
[2] Permanent Virtual Circuit

۲. سه مشخصه اصلی سیستم‌های 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 درطراحی شبکه های انتقال داده را نام برده و عوامل مؤثر درهریک راتوضیح دهید.
۶. استانداردهای اسمی و نامی را توضیح داده و تفاوت آنها را بایکدیگر بنویسید.
۷. سه مرکز اصلی استانداردگذاری درشبکه‌های انتقال داده را نام برده و توضیح دهید.
۸. مفهوم مدل لایه ای را درشبکه‌های کامپیوتری توضیح دهید.
۹. مسائل و مشکلاتی را که درساختار لایه ای با آن روبرو هستیم را عنوان نموده و راه حل هریک را توضیح دهید.
۱۰. علت انجام عملیات تکه سازی و بازسازی در شبکه‌های کامپیوتری را توضیح دهید.
۱۱. نکاتی را که درمدل لایها ی درموردانتخاب تعداد لایه‌ها و عملیات هرلایه با آن روبرو هستیم را تشریح نمایید.
۱۲. مدل مرجع OSI را توضیح دهید.
۱۳. وظایف لایه فیزیکی را درمدل OSI توضیح دهید.
۱۴. مسائل مختلفی که درلایه فیزیکی مدل OSI باآنها روبرو هستیم را توصیف نمایید.
۱۵. وظایف لایه پیونددادہ را درمدل OSI توضیح دهید.
۱۶. وظایف لایه شبکه را در مدل OSI توضیح دهید.
۱۷. مفهوم ازدحام را در شبکه‌های کامپیوتری توضیح داده و روش مقابله باآن را تشریح نمایید.
۱۸. وظایف لایه حمل را درمدل OSI توضیح دهید.
۱۹. وظایف لایه جلسه را درمدل OSI توضیح دهید.
۲۰. وظایف لایه ارائه را درمدل OSI توضیح دهید.
۲۱. وظایف لایه کاربرد را درمدل 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 وعملیات انجام شده توسط آنها را بنویسد.
۲۵. سرویس اتصال گرا را توضیح داده و برای آن مثالی ذکر کنید.
۲۶. سرویس بی اتصال را توضیح داده و برای آن مثالی ذکرنمایید.
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 با یکدیگر را بنویسید.
۲۹. عملکرد سوئیچینگ مداری و سوئیچینگ بسته ای را توصیف نموده و با یکدیگر مقایسه نمایید.

فصل دوم

لایهٔ فیزیکی

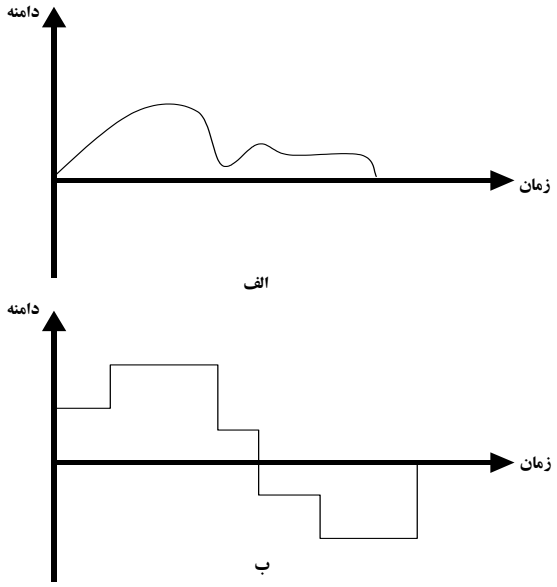
۲-۱- مقدمه

همان‌طور که درفصل 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 می‌شود. در این لایه اطلاعات از شکل منطقی خود خارج شده و به صورت سیگنال‌های الکتریکی وارد رسانه های فیزیکی مناسب شده و به سمت مقصد ارسال می‌گردد. در سمت مقصد لایهٔ فیزیکی سیگنال‌های دریافتی را دوباره به صورت رشته بیت‌های منطقی در آورده و تحویل لایه های بالاتر می‌دهد.در این فصل به معرفی وظایف لایه فیزیکی در شبکه‌های کامپیوتری و استانداردهای مربوط به آن می‌پردازیم.

۲-۲- سیگنال‌های الکتریکی

یکی از مهم‌ترین وظایف لایهٔ فیزیکی انتقال اطلاعات به صورت سیگنال‌های الکتریکی از طریق رسانه های ارسال می‌باشد. اطلاعات ارسالی فوق شامل صوت دیجیتال شده ،تصویر، داده‌های عددی و کاراکترهای کامپیوتری می‌باشند.از آنجایی‌که اطلاعات ارسالی به صورت دیجیتال می‌باشد و شامل ۰و۱ منطقی است، برای ارسال در رسانه انتقال باید به سیگنال‌های الکتریکی تبدیل شوند .

سیگنال‌های الکتریکی به دو دسته کلی تقسیم بندی‌می‌شوندکه عبارتند: ازسیگنال‌های آنالوگ وسیگنال‌های دیجیتال. سیگنال‌های دیجیتال مقادیر مشخص و محدودی را اختیار می‌نمایند، در حالی‌که سیگنال‌های آنالوگ هر مقداری در محدودهٔ تغییرات خود می‌توانند داشته باشند. در شکل (۲-۱) نمونه‌ای از سیگنال‌های آنالوگ و دیجیتال نشان داده شده است .



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

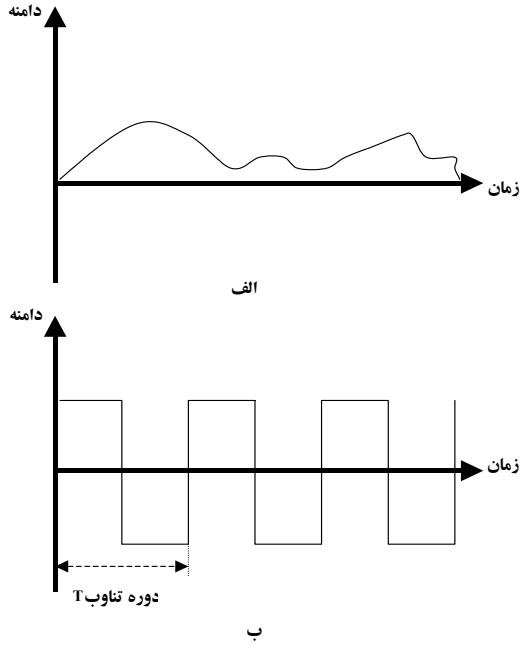
سیگنال‌های الکتریکی آنالوگ و دیجیتال به دو صورت متناوب و نامتناوب تقسیم‌بندی می‌شود. سیگنال‌های متناوب در فاصله‌های زمانی مشخص که دورهٔ تناوب آن نامیده می‌شود، تکرار می‌گردد. طبق تعریف تعداد تکرارهای یک موج متناوب در واحد زمان فرکانس نامیده می‌شود. چنانچه دوره تناوب سیگنال را با T نمایش دهیم، در این صورت فرکانس سیگنال (f) به صورت $f=1/T$ محاسبه می‌شود.

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

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

دوره تناوب	فرکانس
ثانیه	هرتز
میلی ثانیه	کیلوهرتز
میکروثانیه	مگاهرتز
نانوثانیه	گیگاهرتز
پیکوثانیه	تراهرتز

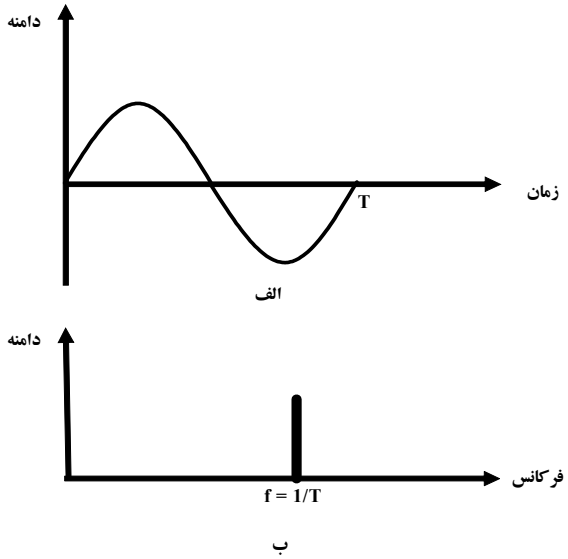
سیگنال‌های نامتناوب فاقد هرگونه تکرار منظم در فواصل زمانی معین می‌باشند. در شکل (۲-۲) نمونه‌ای از سیگنال‌های متناوب و نامتناوب نشان داده شده است .



شکل (۲-۲): انواع سیگنال‌ها: الف) نامتناوب ب) متناوب

با استفاده از تبدیل فوریه، هر سیگنال نامتناوب را می‌توان به تعداد نامحدودی سیگنال متناوب تبدیل نمود. یکی از متداول‌ترین سیگنال‌های متناوب آنالوگ، سیگنال سینوسی می‌باشد. هر سیگنال سینوسی دارای ۳ مشخصهٔ اصلی است که عبارتند از: دامنه، فاز اولیه و فرکانس زاویه‌ای. برای نمایش یک سیگنال از دو حوزه به نام‌های حوزه زمان و حوزه فرکانس استفاده می‌شود. هرسیگنال فرکانس پایین در حوزه زمان دارای دوره تناوب بالایی می‌باشد و بالعکس دوره تناوب هر

سیگنال فرکانس بالا، کم است. همان‌طور که در شکل (۲-۳) نشان داده شده‌است، یک موج سینوسی خالص در حوزهٔ فرکانس فقط دارای یک مؤلفه است. چنانچه موج سینوسی دارای مولفهٔ DC باشد، در این صورت در فرکانس صفر یک مؤلفه درحوزهٔ فرکانس وجود دارد.



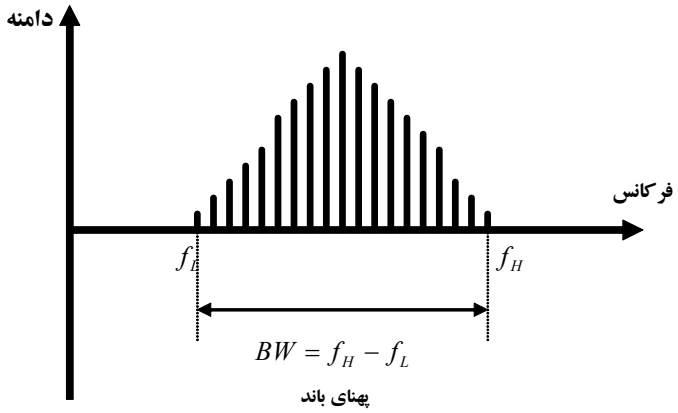
شکل (۲-۳): نمایش سیگنال سینوسی: الف) درحوزهٔ زمان ب) درحوزهٔ فرکانس

طبق تعریف، طیف فرکانسی[1] هر سیگنال مجموعه‌ای از مؤلفه‌های فرکانسی سیگنال درحوزه فرکانس می‌باشد. فاصله بین کمترین و بالاترین مؤلفه فرکانسی درطیف فرکانسی سیگنال، پهنای باند[2] نامیده می‌شود. در شکل (۲-۴) نمونه‌ای ازطیف فرکانسی سیگنال و پهنای باند آن نشان داده شده است .

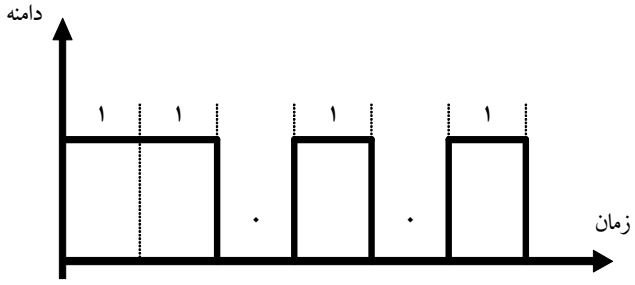
در شبکه‌های کامپیوتری برای تبادل داده ها ازسیگنال‌های دیجیتال استفاده می‌شود. در شکل (۲-۵) نمونه‌ای از یک سیگنال دیجیتال نشان داده شده است. اغلب سیگنال‌های دیجیتال به صورت نامتناوب می‌باشند. طبق تبدیل فوریه، هرسیگنال دیجیتال قابل تجزیه به تعداد نامحدودی موج سینوسی با فرکانس و دامنه‌های متفاوت می‌باشد. بنابراین طیف فرکانسی یک سیگنال دیجیتال در تمام فرکانسها دارای مؤلفه می‌باشد و پهنای باند آن بی‌نهایت است. هنگام ارسال سیگنال‌های دیجیتال دررسانه انتقال، برخی از مؤلفه‌های فرکانسی آن حذف می‌شوندکه این امرباعث وقوع اعوجاج درسیگنال خروجی می‌گردد. طبق تعریف، حداکثرنرخ بیت قابل ارسال در رسانه انتقال، ظرفیت کانال نامیده می‌شود. ظرفیت کانال به مشخصه‌هایی نظیر نسبت دامنهٔ سیگنال به نویز و همچنین نوع کدینگ مورد استفاده بستگی دارد.

---

[1] Spectrum
[2] Bandwidth



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



شکل(۲-۵): نمونه‌ای از یک سیگنال دیجیتال

اغلب سیگنال‌های دیجیتال به صورت نامتناوب می‌باشند. طبق تعریف طول زمانی ارسال یک بیت ، فاصله بیت[1] نامیده می‌شود. همچنین تعداد بیت‌های ارسالی در واحد زمان ، نرخ ارسال بیت[2] نامیده می‌شود .براساس تبدیل فوریه، هر سیگنال دیجیتال قابل تجزیه به تعداد نامحدودی موج سینوسی با فرکانس و دامنه های متفاوت است.

۲-۳- روش‌های کدینگ

در سیستم‌های انتقال ، قبل از ارسال داده‌های کامپیوتری باید آنها را به صورت کدهای مناسبی تبدیل کرد. نحوهٔ کد کردن اطلاعات به عواملی نظیر ساختار اصلی آنها و همچنین ساختار قابل ارسال در محیط بستگی دارد .

همان‌طور که قبلاً اشاره گردید سیگنال‌های الکتریکی به دودستهٔ آنالوگ و دیجیتال تقسیم مـی‌شـوند. چهـار روش مختلف کدینگ وجود دارد که عبارتند از :

- تبدیل سیگنال‌های دیجیتال به دیجیتال
- تبدیل سیگنال‌های دیجیتال به آنالوگ
- تبدیل سیگنال‌های آنالوگ به دیجیتال
- تبدیل سیگنال‌های آنالوگ به آنالوگ

---

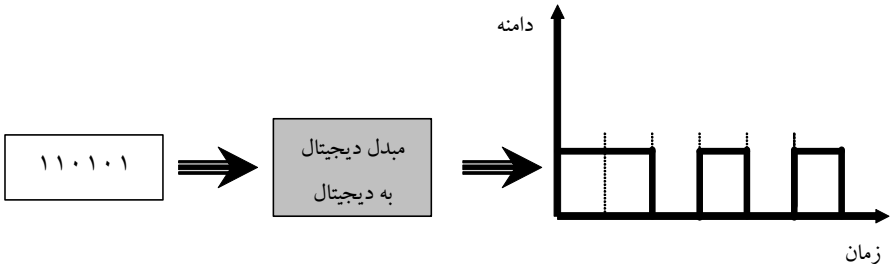
[1] Bit interval
[2] Bit rate

۲-۳-۱- تبدیل اطلاعات دیجیتال به دیجیتال

از این نوع کدینگ در ارسال اطلاعات دیجیتال بوسیلهٔ سیگنـال‌های دیجیتال استفاده می‌شود. به‌عنوان مثال کامپیوتربرای مبادله داده‌های دیجیتال خود به چاپگر، آنها را به شکـل سیگنال‌های دیجیتال تبدیل می‌نماید و ارسال می‌دارد. در شکل (۲-۶) ساختار کلی این نوع کدینگ نشان داده شده است. روش‌های مختلفی برای تبدیل اطلاعات دیجیتـال به سیگنال‌های دیجیتال وجود دارند، که مهم‌ترین این روش‌ها که درشبکه های کامپیوتری و انتقال داده‌هـا استـفاده می‌شوند عبارتند از :

- روش تک قطبی[۱]
- روش قطبی [2]
- روش دو قطبی [3]

در زیر به بررسی هر یک از این روش‌ها می‌پردازیم .



شکل (۲-۶): تبدیل دیجیتال به دیجیتال

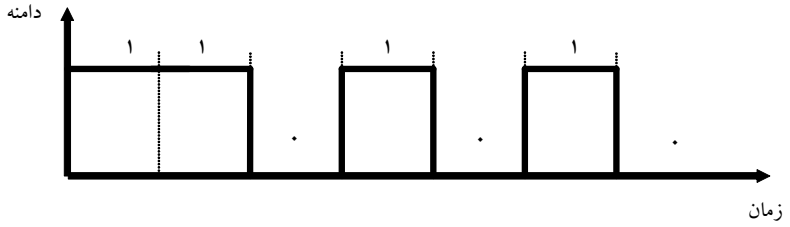
۲-۳-۱-۱- روش تک قطبی

در این روش، بیت ۰ با سیگنال الکتریکی با دامنهٔ صفر ولت و بیت ۱ با سیگنال الکتریکی با سطح غیر صفر ارسال می‌شود. از آنجایی‌که در این روش فقط از یک سطح ولتاژ استفاده می‌شود، به آن روش تک قطبی گفته می‌شود .در شکل (۲-۷) مثالی از روش‌کدینگ تک قطبی آورده شده است.

روش تک قطبی دارای دو مشکل عمده می‌باشد که عبارتند از: وجود DC و حفظ همزمانی فرستنده وگیرنده. از آنجایی‌که متوسط ولتاژ سیگنال ارسالی در این روش غیر صفر است، در این صورت در سیگنال ارسالی قسمت DC مشاهده می‌شود. برخی از رسانه های ارســال مانند ترانسفورماتورها و سیستم‌های مایکروویو قادر به انتقال سیگنال‌هایی که دارای متوسط غیر صفر هستند نمی‌باشند. یکی دیگر از مشکلات اصلی این روش عدم امکان همزمانی دقیق فرستنده و گیرنده است. چنانچه سیگنال دریافتی گیرنده تغییرات کمی داشته باشد، گیرنده قادربه تشخیص دقیق شروع و پایان هر بیت ارسالی نمی‌باشد.

---

[۱] Bit rate
[۲] Polar
[۳] Bipolar



شکل (۲-۷): مثالی از کدینگ تک قطبی

چنانچه رشته بیت ارسالی در روش تک قطبی به طور ممتد حاوی ۰ و یا۱ باشد در این صورت درسیگنال دیجیتال ارسالی تغییراتی وجود ندارد که این مسأله باعث عدم همزمانی دقیق گیرنده و فرستنده خواهد شد.

۲-۳-۱-۲- روش قطبی

روش کدینگ قطبی از دو سطح ولتاژ مثبت و منفی برای ارسال اطلاعات دیجیتال استفاده می‌نماید. 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 روش‌های متعددی می‌باشد که مهم‌ترین آنها عبارتند از :

- روش غیربازگشت به صفر(NRZ[1])
- روش بازگشت به صفر (RZ[2])
- روش دوفاز[3]

روش NRZ خود به دو روش دیگر تقسیم بندی می‌شود که عبارت است از: روش NRZ-L و روش NRZ–I . همچنین روش دو فاز به دو روش به نام‌های منچستر و روش منچستر تفاضلی تقسیم می‌گردد. از روش منچستر در شبکه محلی اترنت و از روش منچستر تفاضلی در شبکه‌های محلی حلقه نشانه استفاده می‌شود.

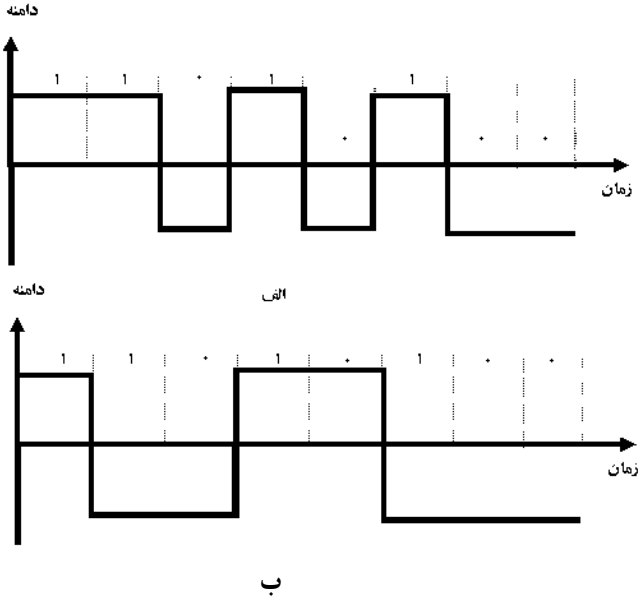
در روشNRZ سطح سیگنال ارسالی همواره مثبت و یا منفی می‌باشد. به عبارت دیگر در سیگنال ارسالی سطح صفر وجود ندارد. در روشNRZ-L برای بیت ۱، سطح سیگنال مثبت است و چنانچه بیت ارسالی ۰ باشد، سطح سیگنال ارسالی منفی خواهد بود . در روش NRZ-Iچنانچه بیت ارسالی ۱ باشد، سطح سیگنال ارسالی معکوس می‌شود و چنانچه بیت ارسالی صفر باشد، سطح ارسالی بدون تغییرمی ماند. در شکل (۲-۸) مثالی از روش‌های کدینگ NRZ-L و NRZ-Iآورده شده است.

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

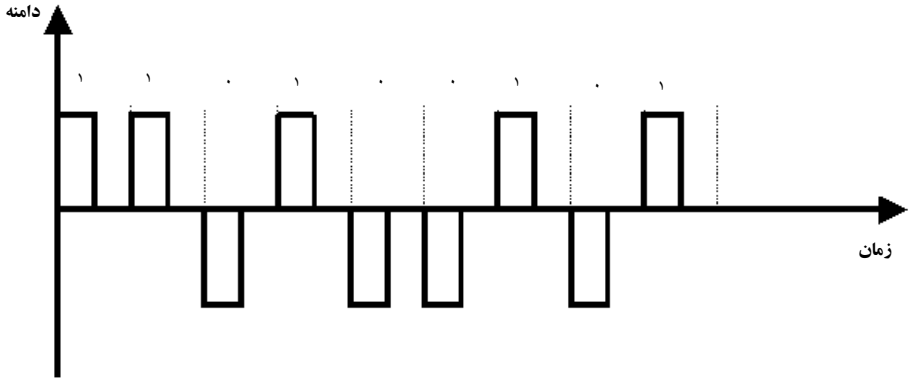
---

[1] Non Return Zero
[2] Return Zero
[3] Biphase

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

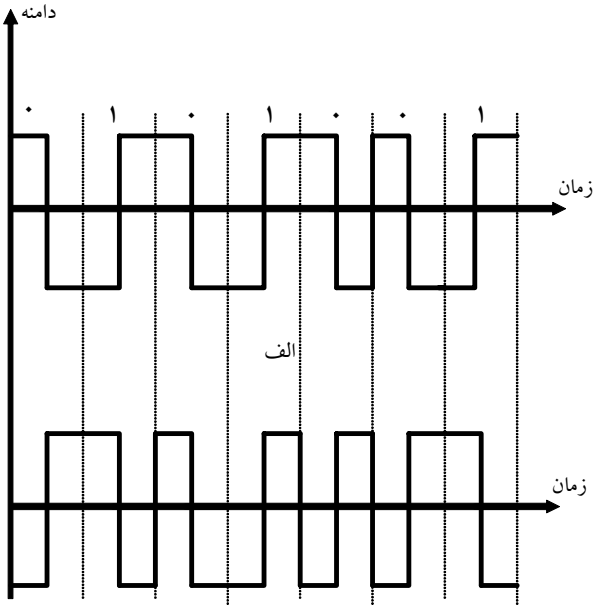


شکل(۲-۸): مثالی از کدینگ NRZ الف)روش NRZ-L ب) روش NRZ-I



شکل (۲-۹): مثالی از روش RZ

یکی از بهترین روش‌های حل مشکل همزمانی، روش دو فاز می‌باشد. در این روش سیگنال در وسط فاصله زمانی هر بیت، تغییر قطبیت داده و از منفی به مثبت ویا بالعکس از مثبت به منفی می رود. دو روش عمده دو فاز عبارتنداز: روش منچستر و روش منچستر تفاضلی. در روش منچستر برای ارسال بیت‌های ۱، قطب سیگنال ارسالی در وسط فاصله زمانی هر بیت از منفی به مثبت تغییر می‌نماید. در حالی‌که برای بیت‌های ۰ قطب سیگنال ارسالی در وسط فاصله زمانی هر بیت از مثبت به منفی تغییر می‌کند . قدرت همزمانی این روش مشابه روش RZ می‌باشد، در حالی‌که در این روش فقط از دو سطح مثبت و منفی استفاده می‌شود . در روش منچستر تفاضلی، چنانچه بیت ارسالی صفر باشد، سطح سیگنال ارسالی در شروع فاصله زمانی بیت تغییر می‌کند. در حالی‌که 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 .



ب

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

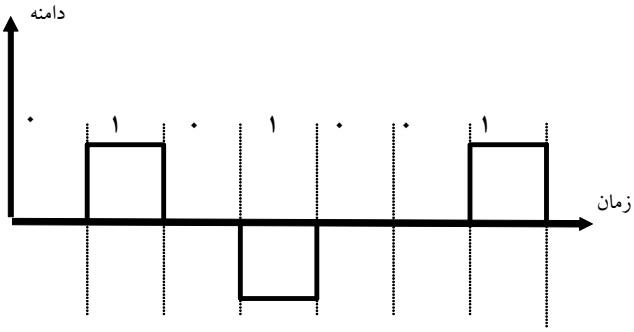
۲-۳-۱-۳- روش دو قطبی

یکی دیگر از روش‌های ارسال سیگنال‌های دیجیتال روش دوقطبی می‌باشد . در این روش مشابه روش RZ از سه سطح مثبت، منفی و صفر استفاده می‌شود. ولی برخلاف روش RZ ، در روش دو قطبی بیت ۰ با سیگنال صفر و بیت ۱ با سیگنال‌هایی با سطح مثبت و یا منفی ارسال می‌شوند. سطح سیگنال ارسالی برای بیت‌های ۱ به‌طور متناوب مثبت و منفی می‌شود .

کدینگ دوقطبی به سه روش AMI[1]، B8ZS[2] و HDB3[3] تقسیم می‌شود. روش AMI ساده‌ترین روش دو قطبی می‌باشد . در این روش بیت۰ با سیگنال با سطح ولتاژ صفر و بیت ۱ با سیگنالی با سطوح ولتاژ مثبت یا منفی ارسال می‌شود . سطح ولتاژ سیگنال ارسالی برای بیت۱ به‌طور متناوب مثبت و یا منفی می‌شود .در شکل (۲-۱۱) مثالی از روش AMI آورده شده است. در روش AMI به دلیل تغییر متناوب سطح سیگنال ارسالی بیت‌های۱، مشکل وجود DC حل می‌شود و همچنین همزمانی هنگام ارسال یک رشته متوالی بیت ۱ حفظ می‌شود، ولی یکی از نقاط ضعف عمدهٔ این روش مشکل بودن همزمانی در گیرنده هنگام ارسال متوالی چندین بیت ۰ می‌باشد. برای رفع این مشکل دو روشB8ZS و HDB3 ارائه شده است .در روشB8ZS برای ارسال ۸ بیت متوالی ۰ بر اساس قطبیت بیت ۱ قبلی از یکی از الگوهای نشان داده شده در شکل (۲-۱۲) استفاده می‌شود . تفاوت اصلی AMI با B8ZS هنگام ارسال متوالی ۸ بیت صفر مشاهده می‌شود. در روش B8ZS گیرنده با مشاهدهٔ تخلف از سطح ولتاژ دریافتی قادر به تشخیص بیت ۰ و۱می‌باشد.

---

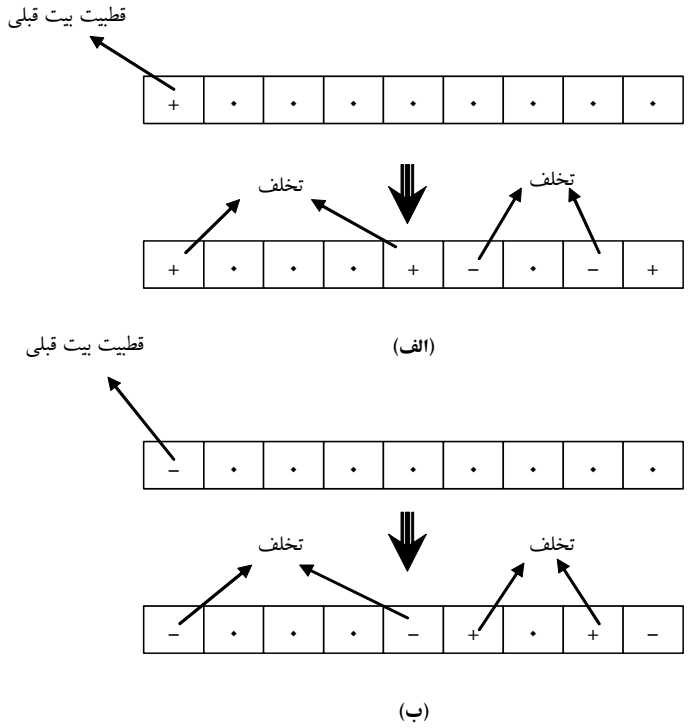
[1] Alternative Mark Inversion
[2] Bipolar 8-Zero Substitution
[3] High Density Bipolar 3



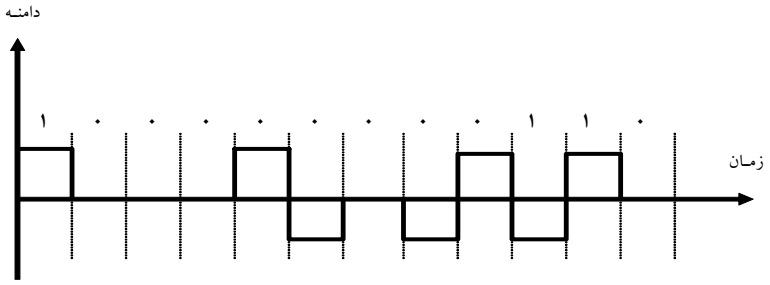
شکل (۲-۱۱): مثالی از روش AMI

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

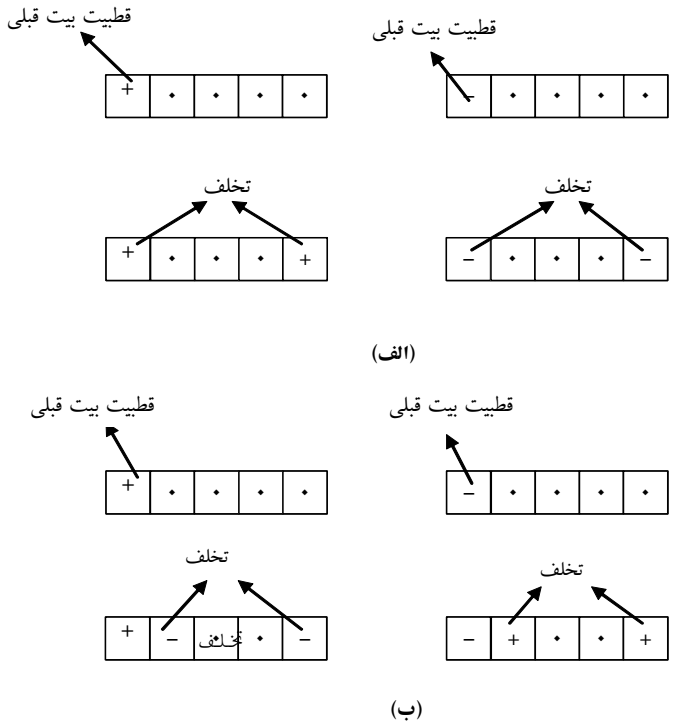
از روش فوق در آمریکا برای حل مشکل همزمانی ارسال چندین بیت ۰ متوالی استفاده می‌شود، در حالی‌که در اروپا و ژاپن برای حل مشکل فوق از روش H DB3 استفاده می‌گردد. در روش HDB3 برای ارسال ۴ بیت متوالی صفربراساس تعداد ۱های ارسالی بعد از آخرین جایگزینی و همچنین بر اساس قطبیت آخرین بیت ۱ از یکی از الگوهای نشان داده شده در شکل (۲-۱۴) استفاده می‌شود .



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

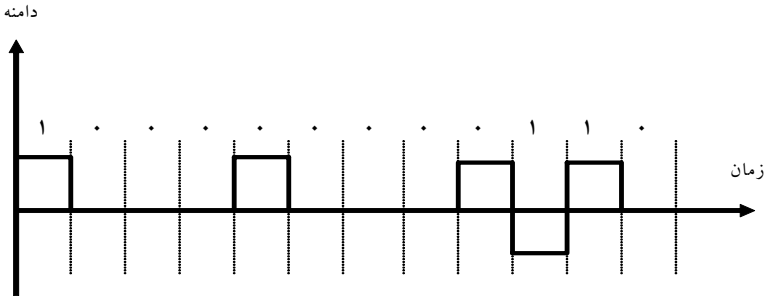


شکل (۲-۱۳): مثالی از روش B8ZS



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 (۲-۵ ۱) مثالی از روش HDB3 آورده شده است .

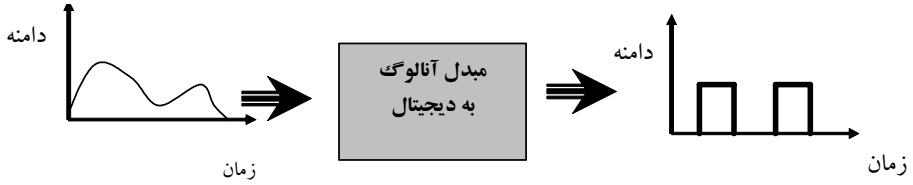


شکل (۲-۱۵): مثالی از روش HDB3

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 اولیهٔ آنا لوگ می‌باشد ولی رسانه انتقال دیجیتال است، استفاده می‌شود.

در شکل (۲-۱۶) مثالی از مبدل آنالوگ به دیجیتال آورده شده است . مطابق با شکل فوق، موج پیوسته آنالوگ به یک سری پالس‌های دیجیتال که نشاندهنده بیت‌های ۰و۱ می‌باشند تبدیل می‌گردند.



شکل (۲-۱۶): تبدیل آنالوگ به دیجیتال

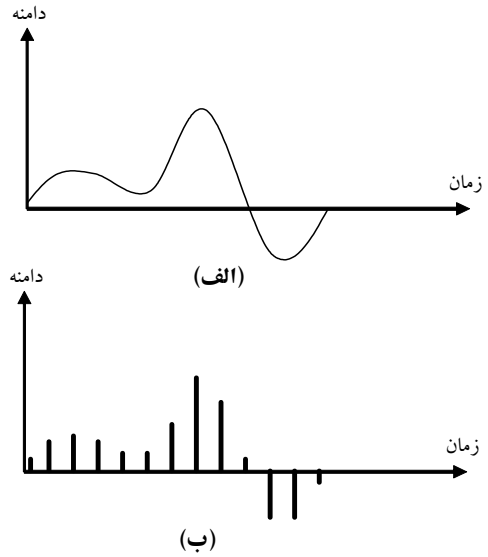
اولین مرحله در تبدیل اطلاعات آنالوگ به دیجیتال مدولاسیون دامنه پالس(PAM[1]) می‌باشد. دراین روش اطلاعات آنالوگ دریافت می‌شوند و بعد از نمونه برداری از آنها یک سری پالس‌های دیجیتال ایجاد می‌گردد. منظور از نمونه برداری، اندازه گیری دامنهٔ سیگنال در فواصل زمانی معین می‌باشد. از روش PAM در سیستم‌های مدولاسیون کد پالس(PCM[2]) که یکی از روش‌های اصلی تبدیل اطلاعات آنالوگ به دیجیتال در شبکه های کامپیوتری است استفاده می‌گردد. مطابق با شکل (۲-۱۷) در فواصل زمانی معین از سیگنال آنالوگ ورودی نمونه‌برداری می‌شود و مقدار این نمونه تا نمونه‌برداری بعدی نگهداری می‌گردد. سیگنال‌های خروجی ازعملیات PAM به تنهایی قابل ارسال نمی‌باشند و هنوز ماهیت آنالوگ دارند. برای تبدیل این سیگنال‌های آنالوگ به سیگنال‌های دیجیتال از روش PCM استفاده می‌شود . در سیستم‌های PCM بعد از نمونه‌برداری از سیگنال به روش PAM سیگنال‌های به‌دست آمده به سطوح مشخصی تقسیم‌بندی می‌شوند که این عملیات سطح بندی [3] نام دارد.

در شکل (۲-۱۸) نمونه‌ای از سیگنال سطح بندی شده که از ۲۵۵ سطح مثبت و منفی استفاده می‌نماید، نشان داده شده است . بعد از عملیات سطح بندی هر یک از سطوح به‌دست آمده به معادل باینری تبدیل می‌شوند. تعداد بیت‌های مورد استفاده در این روش به تعداد سطوح انتخاب شده بستگی دارد. به‌عنوان مثال چنانچه از ۲۵۵ سطح مختلف برای عملیات سطح بندی استفاده شود، به ۸ بیت برای ارسال هر یک از سطوح نیاز می‌باشد.

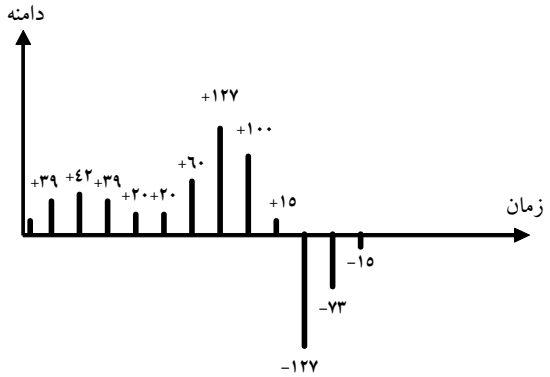
در آخرین مرحلهء یک سیستم PCM رشته بیت‌های به‌دست آمده با استفاده از یکی از روش‌های تبدیل دیجیتال به دیجیتال که در قسمت قبلی توضیح داده شد، به سیگنال‌های دیجیتال مناسب تبدیل شده و ارسال می‌گردند. بنابراین هر سیستم PCM از چهار قسمت اصلی تشکیل شده است که عبارتند از : عملیات PAM ، سطح‌بندی، تبدیل سطوح به معادل باینری[4] و تبدیل اطلاعات دیجیتال به دیجیتال. در شکل (۲-۱۹) قسمت‌های تشکیل‌دهندهٔ یک سیستم PCM نشان داده شده است .

---

[1] Pulse Amplitude Modulation
[2] Pulse Cod Modulation
[3] Quantization
[4] Binary encoding

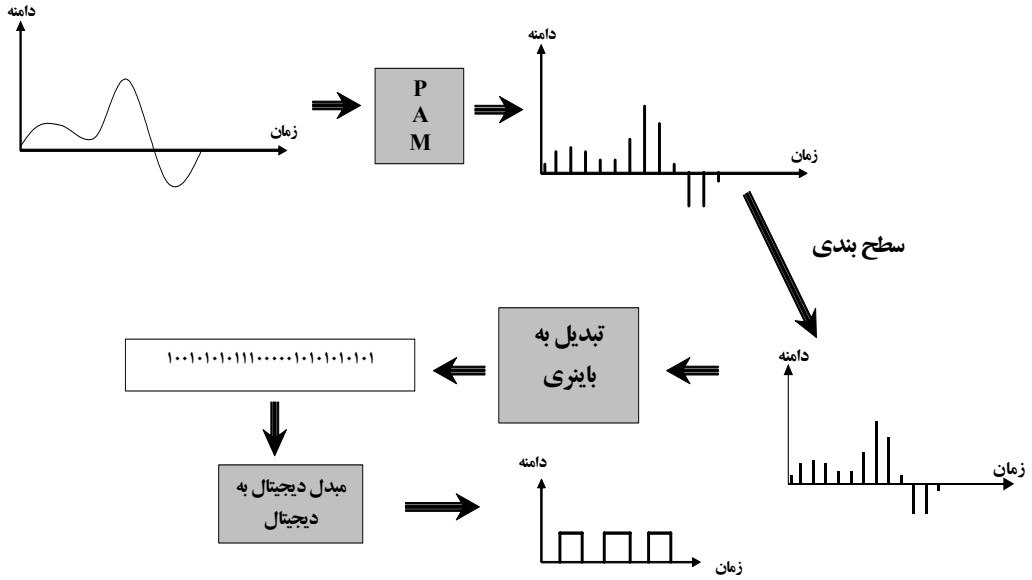


شکل (۲-۱۷): عملکرد PAM : الف) سیگنال اولیه ب) سیگنال نمونه برداری شده



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

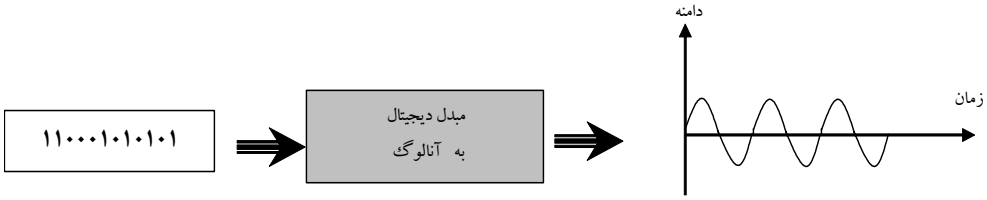
یکی از عوامل مهم در دقت عملیات تبدیل آنا لوگ به دیجیتال، نرخ نمونه برداری و تعداد سطوح مورد استفاده می‌باشد. مطابق با قضیهء نا یکوییست، برای بازسازی سیگنال نمونه برداری شده PAM ، باید نرخ نمونه‌برداری حداقل دو برابر بالاترین فرکانس سیگنال آنا لوگ اولیه باشد. به‌عنوان مثال در انتقال صوت انسان به‌وسیله سیستم PCM ، ازآنجایی‌که بالاترین فرکانس صوت انسان حدود۳۳۰۰ هرتز است، بنابراین به تعداد۶۶۰۰ نمونه درهر ثانیه نیاز است که در عمل برای دقت بیشتر در هر ثانیه ۸۰۰۰ نمونه برداشته می‌شود.



شکل (۲-۱۹): نمونه‌ای از یک سیستم PCM

۲-۳-۳- تبدیل اطلاعات دیجیتال به آنالوگ

از این نوع تبدیل، هنگام ارسال اطلاعات دیجیتال بر روی رسانه های آنا لوگ استفاده می‌شود. به‌عنوان مثال چنانچه دو کامپیوتر از طریق خط تلفن آنا لوگ به یکدیگر متصل شوند، در این صورت از آنجایی‌که اطلاعات کامپیوترها دیجیتال بوده و خطوط آنا لوگ تلفن قادربه ارسال آنها نمی‌باشند، از مبدل‌های دیجیتال به آنا لوگ استفاده می‌شود .در شکل (۲-۲۰) نمونه‌ای از یک سیستم تبدیل دیجیتال به آنا لوگ آورده شده است .

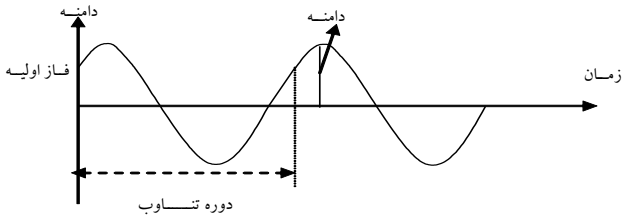


شکل (۲-۲۰): تبدیل دیجیتال به آنالوگ

روش‌های متعددی برای تبدیل اطلاعات دیجیتال به آنا لوگ وجود دارد که در این قسمت به بررسی مهم‌ترین آنها که درشبکه‌های انتقال داده استفاده می‌شوند می پردازیم .

به‌طور کلی یک سیستم آنا لوگ سینوسی به‌وسیلهٔ سه مشخصهٔ اصلی که عبارتند از :دامنه، فرکانس و فاز مشخص می‌شود . در شکل (۲-۲۱) مثالی از یک موج سینوسی که مشخصه‌های فوق در آن نشان داده شده آورده شده است.

چنانچه بخواهیم بیت‌های ۰ و ۱ دیجیتال را در یک موج سینوسی مدوله نماییم، باید یکی از سه مشخصه نامبرده فوق را تغییر دهیم.



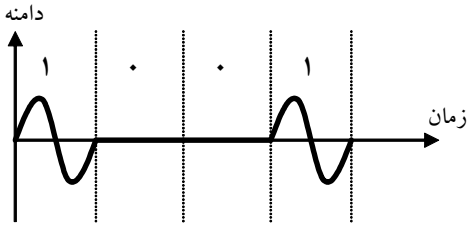
شکل (۲-۲۱): یک موج سینوسی

چهار روش اصلی تبدیل دیجیتال به آنا لوگ که در سیستم‌های انتقال داده استفاده می‌شوند عبارتند از:

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

۲-۳-۳-۱- مدولاسیون ASK

در روشASK دامنهٔ موج سینوسی ارسالی (موج حامل) متناسب با صفر یا یک بودن بیت ارسالی تغییر می‌کند. در شکل (۲-۲۲) مثالی از مدولاسیون ASK آورده شده است .



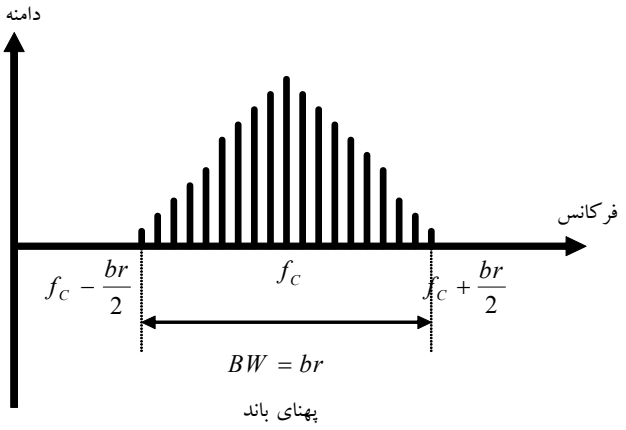
شکل (۲-۲۲): مثالی از مدولاسیون ASK

یکی از بزرگ‌ترین معایب مدولاسیون ASK ، حساسیت زیاد آن به نویز می‌باشد. در ASK سیگنال‌های نویز که از پدیده‌های مختلفی نظیر گرما و یا القای الکترومغناطیسی ناشی می‌شوند، دامنهٔ موج ارسالی را تغییرمی‌دهند، به‌طوری‌که گیرنده ممکن است در تشخیص بیت ۰ و ۱ دچار اشکال شود. در روش متداول ASKکه کلیدزنی قطع و وصل (OOK[5]) نام دارد، برای ارسال بیت صفر سیگنال صفر ولت ارسال می‌شود. در شکل (۲-۲۳) طیف فرکانسی سیگنال ASK نشان

---

[1] Frequency Shift Keying
[2] Amplitude Shift Keying
[3] Phase Shift Keying
[4] Quadrate Amplitude Modulation
[5] On-Off Keying

داده شده است. در این شکل f_c فرکانس سیگنال حامل[1] که همان فرکانس موج سینوسی ارسالی است، می‌باشد. همچنین br نشان‌دهندهٔ نرخ ارسال سمبل در ASK است.

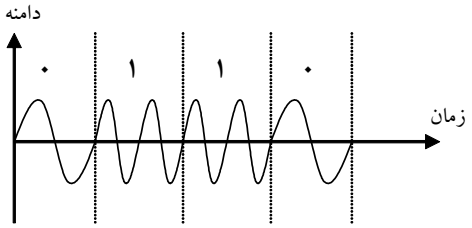


شکل (۲-۲۳): طیف فرکانسی سیگنال ASK

از آنجایی‌که در این مدولاسیون برای هر بیت، یک سمبل (موج سینوسی با دامنه مشخص) ارسال می‌شود، نرخ ارسال سمبل با نرخ ارسال بیت برابر می‌باشد.

۲-۳-۳-۲- مدولاسیون FSK

در مدولاسیون FSK فرکانس سیگنال سینوسی ارسالی متناسب با ۰ و یا ۱ بودن بیت ارسالی تغییر می‌کند. 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 می‌گردد.



شکل (۲-۲۴): مثالی از مدولاسیون FSK

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

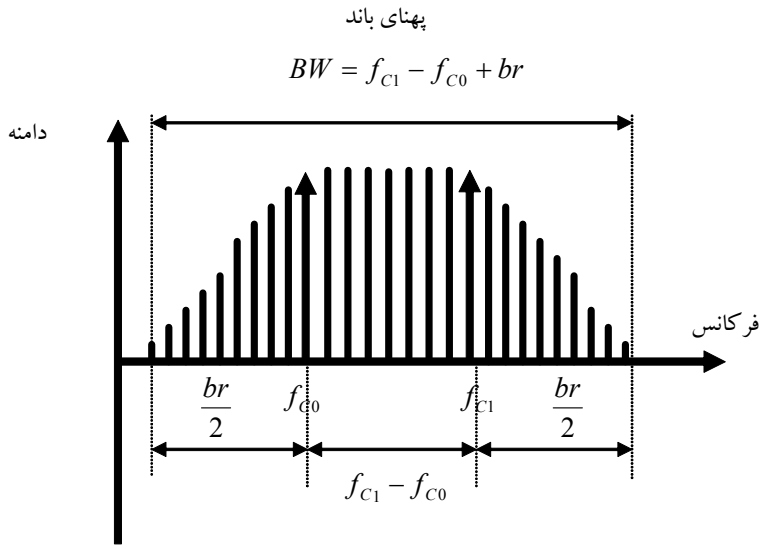
مهم‌ترین برتری FSK به ASK ، مصونیت آن در مقابل نویز می‌باشد. نویزهای کانال‌های مخابراتی فقط دامنهٔ سیگنال را تغییر می‌دهند و فرکانس آن بدون تغییر می ماند، بنابراین گیرنده قادر به تشخیص فرکانس موج دریافتی می‌باشد و نویز کانال در آن اثری ندارد. در شکل (۲-۲۵) طیف فرکانسی سیگنال FSK نشان داده شده است . مطابق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

[1] Carrier

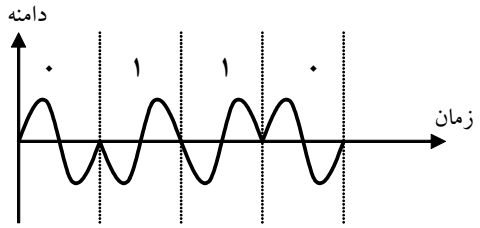
شکل فوق ، پهنای باند FSK برابر با $f_{c1} - f_{c0} + br$ می‌باشد که در آن br نرخ ارسالی سمبل در مدولاسیون FSK است که با نرخ ارسال بیت برابر است .

۲-۳-۳-۳- مدولاسیون PSK

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



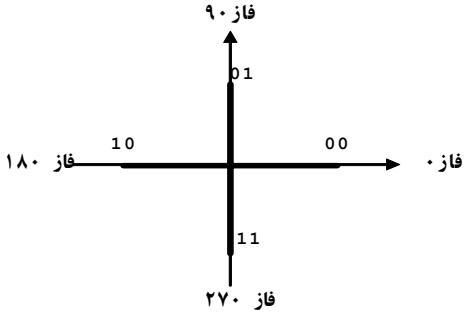
شکل (۲-۲۵): طیف فرکانسی مدولاسیون FSK



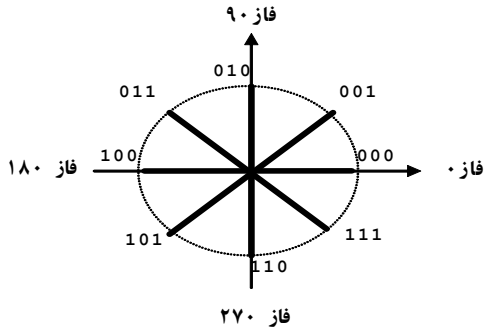
شکل(۲-۲۶): مثالی از مدولاسیون PSK

مطابق با شکل فوق، درمدولاسیون PSK برای ارسال بیت ۰ موج سینوسی با فاز صفر و برای ارسال بیت۱، یک منبع سینوسی با فاز ۱۸۰ درجه ارسال می‌شود. از آنجایی‌که دراین روش از دو فازصفرو ۱۸۰ درجه استفاده می‌گردد، به این روش۲PSK- یا PSK باینری نیز گفته می‌شود . همانند FSK، سیگنال‌های PSK نیز درمقابل نویز از مصونیت بالایی برخوردار می‌باشند .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 به‌وسیلهٔ یک سمبل PSK ارسال نمود که باعث افزایش سرعت ارسال می‌شود. همچنین با افزایش فازهای ارسالی می توان به سرعت‌های بالاتر نیز دسترسی پیدا کرد. در شکل (۲-۲۷) دیاگرام فازی مدولاسیون‌های 4- PSKو 8- PSK که به ترتیب از ۴ و ۸ فاز متفاوت برای ارسال بیت‌ها استفاده می‌کنند نشان داده شده است.

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 می‌باشد. البته در مدولاسیون‌های 4- PSK و 8- PSK ، مقدار br به ترتیب دو برابر و سه برابر نرخ ارسال بیت است.

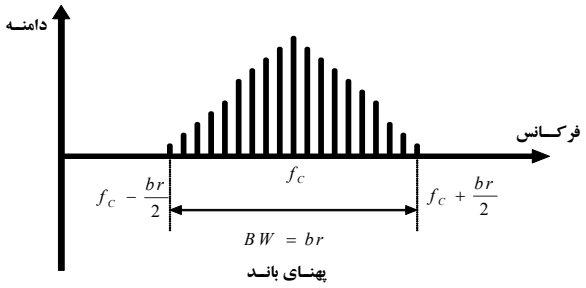


(الف)



(ب)

شکل (۲-۲۷): دیاگرام فازی: الف) مدولاسیون 4- PSK ب) مدولاسیون 8- PSK



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 (به‌ترتیب دامنه، فرکانس و فاز) تغییر می‌نماید و دو مشخصه دیگر ثابت می‌باشند. چنانچه مدولاسیون‌های A SK و PSK با یکدیگر ترکیب شوند، مدولاسیون جدیدی به نام QAM ایجاد می‌شود . در QAM اطلاعات ارسالی هم در فاز و هم در دامنه می‌باشد. در شکل (۲-۲۹) مثالی ازدیاگرام فازی می‌باشد. حالت‌های مختلف QAM آورده شده است . حداقل پهنای باند لازم برای QAM

مشابهASK و PSK می‌باشد. درجدول (۲-۲) رابطهٔ بین نرخ ارسال بیت و نرخ ارسال سمبل درمدولاسیون‌های مختلف نشان داده شده است.

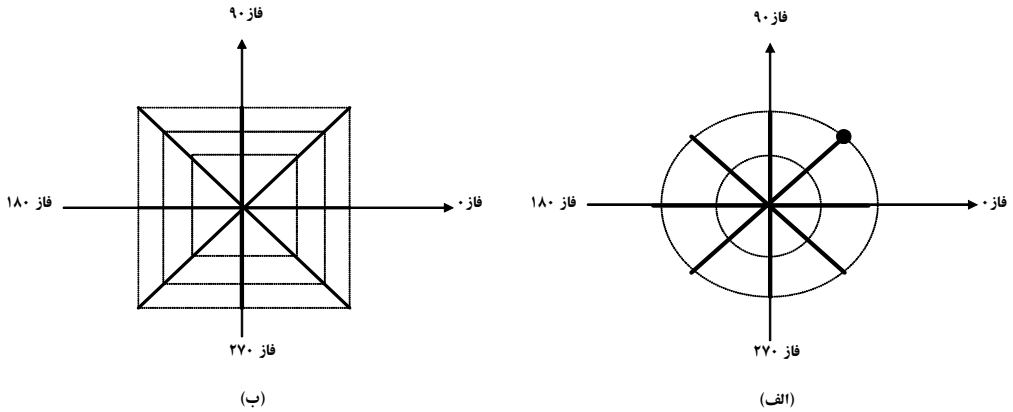
جدول (۲-۲): رابطه بین نرخ ارسال بیت و نرخ ارسال سمبل در مدولاسیون‌های مختلف

نوع مدولاسیون	نرخ بیت	نرخ سمبل
ASK،FSK و PSK۲-	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 سیگنال‌های آنالوگ

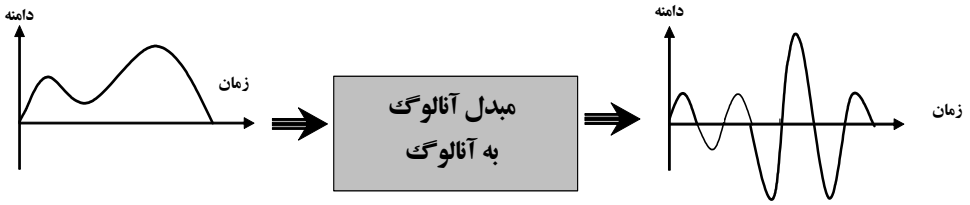
برای ارسال اطلاعات آنا لوگ بر روی رسانه های انتقال آنا لوگ، از مدولاسیون‌های آنالوگ به آنا لوگ استفاده می‌شود. در شکل(۲-۳۰) نمونه‌ای از یک سیستم تبدیل آنا لوگ به آنا لوگ نشان داده شده است . سه روش اصلی برای تبدیل اطلاعات آنا لوگ به سیگنال‌های آنالوگ وجود دارد که عبارتند از :

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



شکل (۲-۲۹): دیاگرام فازی QAM : الف) ۲ دامنه و۸ فاز ب)۴ دامنه و ۸ فاز

[1] Amplitude Modulation
[2] Frequency Modulation
[3] Phase Modulation

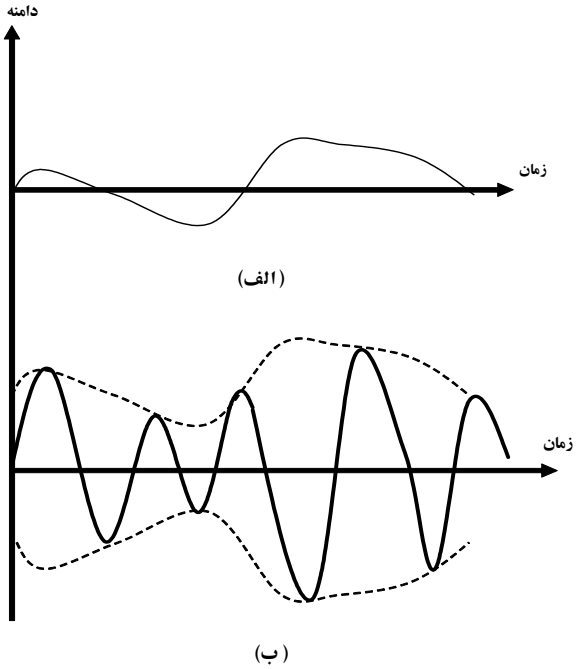


شکل (۲-۳۰): تبدیل آنالوگ به آنالوگ

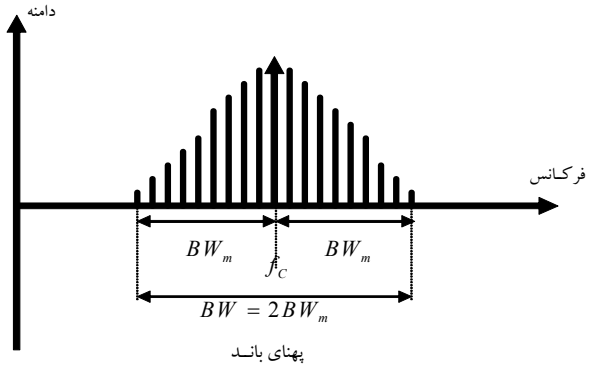
۲-۳-۴-۱- مدولاسیون AM

در ارسال AM ، سیگنال حامل طوری مدوله می‌شود که دامنهٔ آن متناسب با سیگنال پایهٔ ارسالی تغییر می‌کند. فرکانس و فاز سیگنال حامل ثابت می‌باشد و فقط دامنهٔ آن متناسب با دامنه موج پایهٔ ارسالی تغییر می‌کند . 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



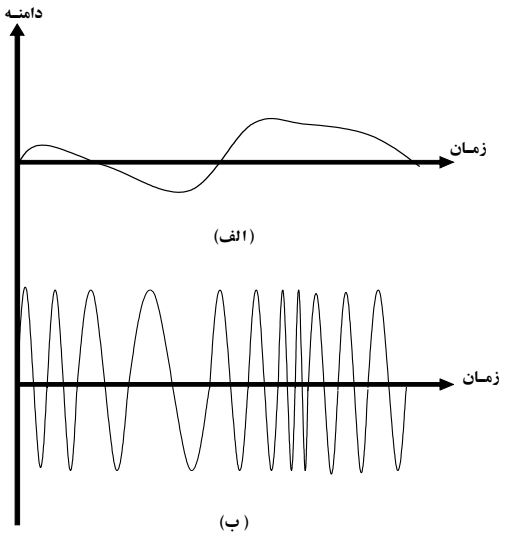
شکل (۲-۳۲): طیف فرکانسی سیگنال AM

مطابق با شکل فوق، پهنای باند سیگنال AM دو برابر پهنای باند سیگنال پایهٔ ارسالی (BW_m) می‌باشد. به‌عنوان مثال پهنای باند سیگنال‌های صوتی، معمولاً حدود ۵ کیلو هرتز است. بنابراین یک ایستگاه رادیویی AM به پهنای باند حدود ۱۰ کیلو هرتز نیاز دارد. در ایستگاه‌های رادیویی AM از فرکانسهای بین ۵۳۰ کیلو هرتز تا ۱۷۰۰ کیلوهرتز استفاده می‌شود. هرایستگاه AM به حدود ۱۰ کیلوهرتز پهنای باند نیاز دارد، بنابراین در محدودهٔ فرکانسی فوق حدود ۱۱۸ ایستگاه رادیو AM قابل استفاده می‌باشد .

۲-۳-۴-۲- مدولاسیون FM

درمدولاسیون FM فرکانس موج حامل ، متناسب با سیگنال ارسالی باند پایه تغییر می‌نماید. در شکل (۲-۳۳) مثالی از مدولاسیون FM آورده شده است . همان‌طور که در شکل (۲-۳۳) مشاهده می‌شود، در سیگنال ارسالی دامنه و فاز ثابت می ماند و فقط فرکانس موج حامل متناسب با سیگنال پایهٔ ارسالی تغییر می‌نماید.

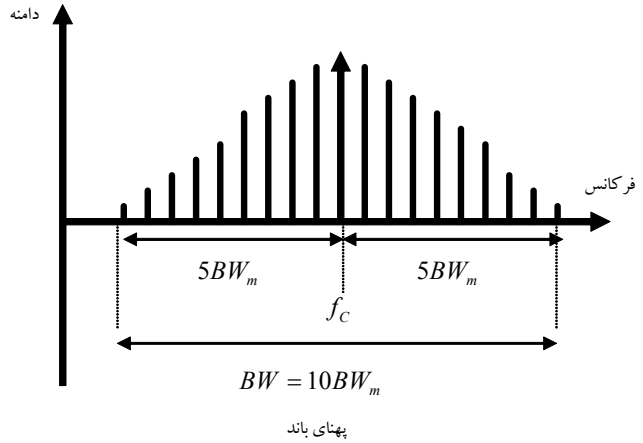
درشکل (۲-۳۴) طیف فرکانسی سیگنالFM نشان داده شده است. سیگنال FM دارای پهنای باند ۱۰ برابر پهنای باند سیگنال پایه ارسالی می‌باشد . به‌عنوان مثال پهنای باند سیگنال صوت استریو حدود ۱۵ کیلو هرتز است، بنابراین هر ایستگاه FM به پهنای باند حدود ۱۵۰ کیلو هرتز نیاز دارد . البته برای جلوگیری از تداخل فرکانسی ایستگاه‌های مجاور FM، ۵۰ کیلو هرتز پهنای باند محافظ نیز در هرایستگاه FM در نظرگرفته می‌شود؛ که در نتیجه هر ایستگاه FMحدود ۲۰۰ کیلو هرتز پهنای باند نیاز دارد. در ایستگاه‌های رادیویی FM از محدودهٔ فرکانسی ۸۸ مگاهرتز تا ۱۰۸ مگاهرتز استفاده می‌شود. از آنجایی‌که هر ایستگاه FM به ۲۰۰ کیلو هرتز پهنای باند نیاز دارد، بنابراین در محدودهٔ فرکانسی فوق حدود ۱۰۰ ایستگاه FM قابل استفاده است.



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

۲-۳-۴-۳- مدولاسیون PM

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



شکل(۲-۳۴): طیف فرکانسی FM

۲-۴- واسطه‌های دیجیتال

برای انتقال اطلاعات دیجیتال کامپیوترها بر روی کانال‌های ارتباطی، نیاز به واسطه‌های دیجیتال می‌باشد. به‌عنوان مثال چنانچه بخواهیم اطلاعات دیجیتال یک کامپیوتر را بر روی خطوط آنالوگ تلفن ارسال کنیم، نیاز به واسط مشخص و همچنین وسیله ای به نام مودم برای انتقال اطلاعات کامپیوتر به خط تلفن داریم .

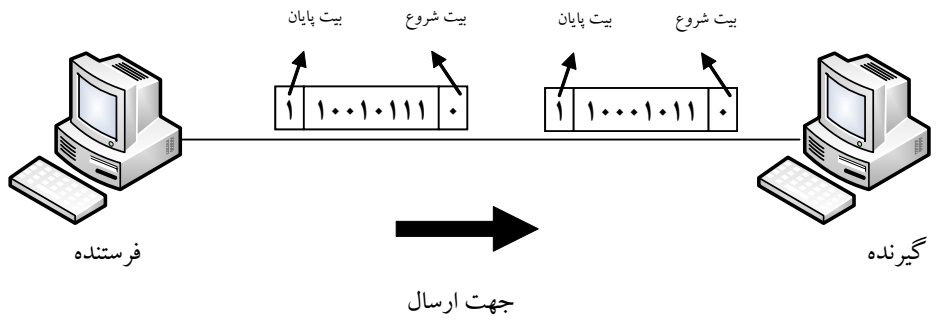
جهت ارسال اطلاعات در کامپیوترها دو روش موازی و سری وجود دارد.در روش ارسال موازی، داده های۰ و۱ باینری به صورت گروه‌های چندبیتی درآمده و یکجا ارسال می‌گردند، که باعث افزایش نرخ ارسال بیت می‌شود. حداکثر ارسال داده ها به روش موازی ۲۵ فوت است . در روش ارسال سری ، داده های ارسالی بیت به بیت یکی پس از دیگری ارسال می‌گردند. بنابراین در این روش تنها به یک کانال ارتباطی نیاز می‌باشد که از مزایای عمدهٔ روش ارسال سری است . ارسال اطلاعات سری به روش غیرهمزمان[1] و همزمان صورت می‌گیرد که به بررسی هر یک از این روش‌ها می پردازیم.

۲-۴-۱- روش غیر همزمان

در این روش زمان‌بندی سیگنال ارسالی مهم نمی‌باشد و داده‌های ارسالی به صورت بایت به بایت ارسال می‌گردند. از آنجایی‌که در روش غیر همزمان سیگنال ساعت[2] عملاً بین فرستنده و گیرنده مبادله نمی‌شود، برای جداسازی و تشخیص داده های ارسالی در گیرنده، فرستنده یک سری بیت‌هایی به هربایت ارسالی اضافه می‌نماید. بدین‌منظور در ابتدای هر بایت یک بیت صفر به‌عنوان بیت شروع[3] و در پایان هر بایت، ۱ یا ۱/۵ و یا ۲ بیت ۱ به‌عنوان بیت پایان[4] اضافه می‌شود. با استفاده از بیت‌های شروع و پایان، عملاً گیرنده قادر به جداسازی بایت‌های ارسالی از یکدیگر می‌باشد. علاوه بر بیت‌های فوق، معمولاً بین هر دو بایت متوالی، کانال ارسال درحالت بی‌کار[5] به‌سر می‌برد. در شکل(۲-۳۵) نمونه‌ای از ارسال غیرهمزمان نشان داده شده است .

---

[۱] Asynchronous
[۲] Clock
[۳] Start bit
[٤] Stop bit
[٥] Idle



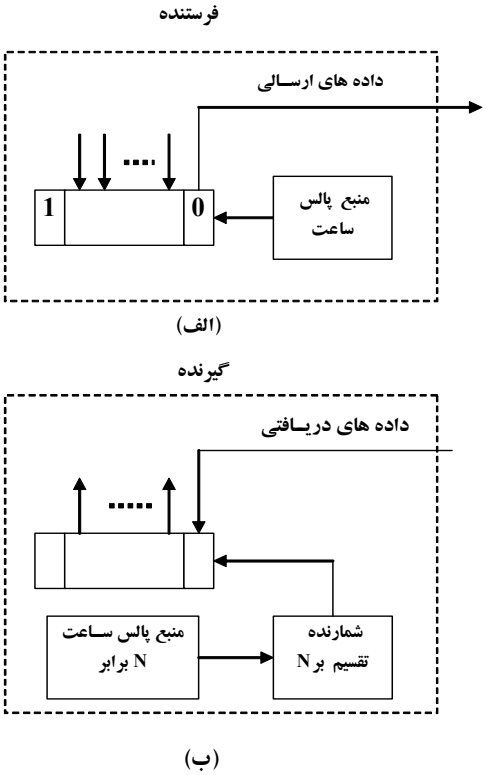
شکل (۲-۳۵): مثالی از ارسال غیرهمزمان

درروش غیرهمزمان، فرستنده و گیرنده از مولد پالس ساعت مستقل از یکدیگر و به طور محلی استفاده می‌نمایند. این روش برای سرعت‌های پایین و درمواردی که ارسال کاراکترها به صورت تصادفی (مثل تایپ کردن برروی صفحه کلید) می‌باشد، استفاده می‌گردد. اضافه کردن بیت‌های شروع و پایان، باعث افزایش بالا سری وکاهش سرعت ارسال روش غیر همزمان می‌گردد.

ساختار فرستنده وگیرنده روش غیرهمزمان درشکل(۲-۳۶) نشان داده شده است. مطابق با این شکل، داده های ارسالی فرستنده داخل یک شیفت رجیستر PISO[1] به صورت موازی قرارمی‌گیرند و به صورت سری با هرپالس ساعت بیت به بیت از آن خارج می‌شوند. درسمت گیرنده، برای اطمینان از صحت دریافت بیت‌ها، از یک منبع پالس ساعت با فرکانس N برابر فرکانس منبع پالس ساعت فرستنده استفاده می‌شود.(معمولاً $N = 16$ اختیار می‌گردد).

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

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

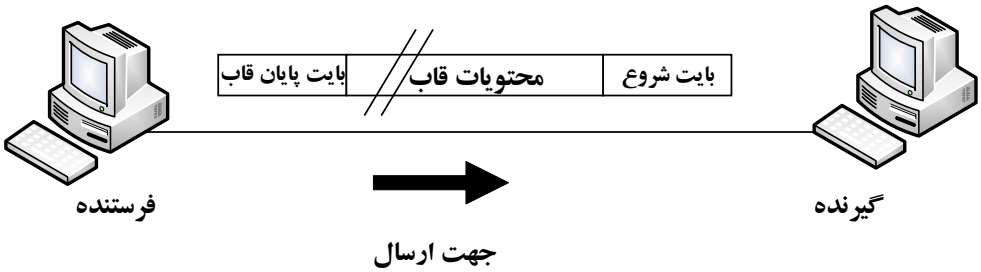


شکل (۲-۳۶): ساختار روش غیرهمزمان الف)فرستنده ب) گیرنده

۲-۴-۲- روش همزمان

در روش همزمان رشته بیت‌های ارسالی به صورت قاب‌هایی به طول مشخص که شامل چندین بیت می‌باشد، ارسال می‌گردند. در این روش بین بایت‌های ارسالی موجود در قاب هیچ‌گونه فاصلهٔ زمانی(که در روش غیر همزمان وجود داشت) وجود ندارد. در شکل ۲-۳۷ نمونه‌ای از ارسال همزمان نشان داده شده است . از این روش برای ارسال حجم زیادی ازداده ها با سرعت بالا استفاده می‌شود.

دراین روش درآغاز و پایان هرقاب از یک یا چند کاراکتر کنترلی خاص که منحصر به فرد بوده و درناحیهٔ داده‌های کاربران وجود ندارد، برای تعیین شروع وپایان هرقاب استفاده می‌شود.



شکل (۲-۳۷): مثالی از ارسال همزمان

ازآنجایی‌که در روش همزمان ازبیت شروع و پایان درهربایت استفاده نمی‌شود و همچنین با توجه به سرعت بالای ارسال دراین روش، برای همزمانی بیت و استخراج صحیح اطلاعات ازهرقاب، نیاز به حفظ همزمانی پالس ساعت درفرستنده و گیرنده حس می‌گردد. بدین‌منظور ازروش‌های کدینگ دیجیتال به دیجیتال نظیر روش منچستر وهمچنین مدار DPLL[1] برای همزمان سازی پالس ساعت گیرنده با فرستنده استفاده می‌شود.

۲-۴-۳- واسط DTE به DCE

در شبکه‌های کامپیوتری به تجهیزاتی نظیر کامپیوترها، چاپگرها و ماشین‌های فاکس، تجهیزات پایانه داده(DTE[2]) گفته می‌شود. همچنین تجهیزاتی مثل مودم که برای ارسال داده‌های DTE ها به کار می‌روند؛ تجهیزات مخابره داده یا تجهیزات پایان‌دهنده 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 می‌گیرد. هر استاندارد مدل خاصی را برای مشخصات مکانیکی، الکتریکی و عملیاتی تعریف می‌نماید. 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-442,EIA-232 و EIA-449 برای ارتباط بین DTE و DCE وضع شده است. یکی از متداول‌ترین و مهم‌ترین استانداردهای واسط DTE به DCE، استاندارد EIA-232 می‌باشد. این استاندارد که تا حد زیادی مشابه استاندارد CCITT V.24است، برای ارتباط یک DTE مثل کامپیوتر به یک DCE نظیر مودم به کار می‌رود که به بررسی آن می‌پردازیم. لازم به توضیح است که مودم وسیله‌ای می‌باشد که امکان انتقال اطلاعات دیجیتال کامپیوترها را از طریق خطوط آنالوگ تلفن فراهم می‌آوردکه درقسمت‌های بعدی به توصیف عملکرد آنها خواهیم پرداخت.

شکل (۲-۳۸): واسط DTE به DCE

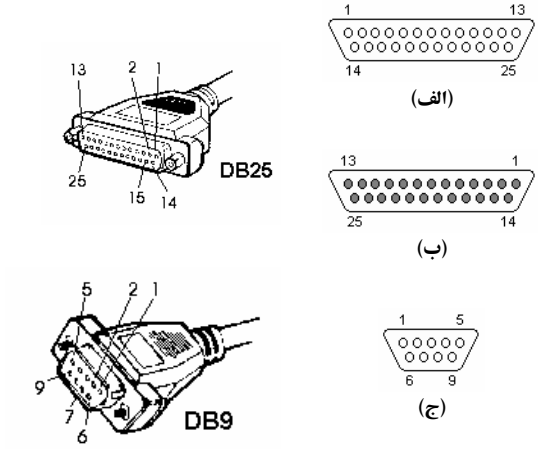
۲-۴-۳-۱- واسط EIA-232

استاندارد EIA-232 (که با نام قبلی آن یعنی RS-232 نیز شناخته‌شده می‌باشد)، دارای دو نوع کانکتور مختلف ۲۵ پین (DB-25) و ۹ پین (DB-9) است. هریک از کانکتورهای فوق نیز دو نوع می‌باشند که عبارتند: از کانکتور نری[4] و کانکتور مادگی[5]. درشکل (۲-۳۹) نمونه‌ای 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

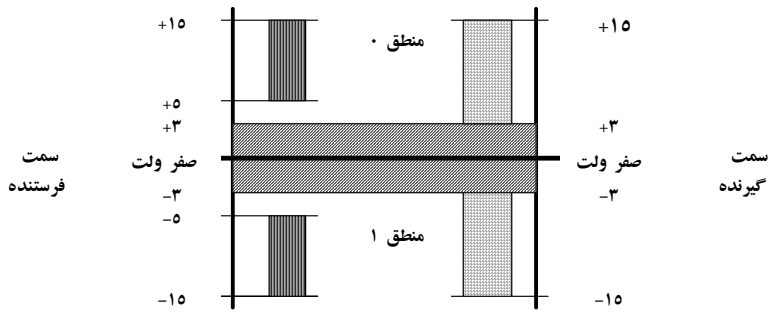
در کانکتور نوع DB-25، از ۲۵ رشته سیم برای تبادل اطلاعات و سیگنال‌های کنترلی استفاده می‌شود. برای ارسال داده‌ها از طریق این کانکتور، بیت ۱ با سطح ولتاژ بین ۳- تا ۱۵- و بیت ۰ با سطح ولتاژی بین ۳+ و ۱۵+ نشان داده می‌شوند. ناحیه بین ۳- تا ۳+ ناحیه غیرمجاز و تعریف‌نشده می‌باشد. در DB-25 فقط از چهار پین آن برای ارسال و دریافت داده‌ها استفاده می‌شود و ۲۱ پین باقی‌مانده برای عملیات کنترلی نظیر کنترل DTE و DCE، زمان‌بندی[1] ، تعیین سطح ولتاژ صفر و عملیات تست استفاده می‌گردد.



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 می‌باشد. مهم‌ترین پین‌های DB-25 به شرح زیر است:

- ***پین شمارهٔ (۲)، داده‌های ارسالی*** [2] : توسط این پین داده‌های ارسالی DTE تحویل DCE می‌شود، تا آنها را ارسال کند.

---

[1] Timing

[2] Transmitted data

- ***پین شمارهٔ (۳)، داده‌های دریافتی***[1] : این پین حاوی داده‌های دریافتی DCE می‌باشد که از طریق آن به DTE ارسال می‌شود.
- ***پین شمارهٔ (۴)، درخواست ارسال*** **DTE (RTS[2])** : با فعال‌شدن این پین، درخواست ارسال داده از طرف DTE به اطلاع DCE رسانده می‌شود.
- ***پین شمارهٔ (۵)، آمادگی ارسال*** **DCE (CTS[3])** : هنگامی‌که DCE درخواست ارسال DTE را دریافت نماید و آمادهء انتقال اطلاعات DTE باشد، با فعال‌کردن این پین آمادگی خود را به اطلاع DTE می‌رساند.
- ***پین شمارهٔ (۶)، آمادگی*** **DCE[4] :** هنگامی‌که DCE آماده کار باشد، این پین فعال می‌شود. معمولاً با روشن‌شدن DCE این پین نیز فعال می‌گردد.
- ***پین شمارهٔ (۷)، زمین مشترک سیگنال***[5]: برای آن‌که 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 می‌شود.
- ***پین شمارهٔ (۸)، آشکارساز سیگنال دریافتی از خط***[6] : هنگامی‌که DCE متوجه وجود سیگنال در خط شود، با فعال‌کردن این پین به اطلاع DTE می‌رساند که داده‌های دریافتی در خط وجود دارند.
- ***پین شمارهٔ (۲۰) آمادگی*** **DTE**[7] : DTE با فعال‌کردن این پین به اطلاع DCE می‌رساند که آماده کار می‌باشد. معمولاً با روشن‌شدن DTE این پین نیز فعال می‌شود.

البته به غیر از پین‌های فوق که شرح مختصری از آنها آورده شد، پین‌های دیگری نیز وجود دارد که از اهمیت کمتری برخوردارند. به همین دلیل با کاهش پین‌های 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 می‌شود. ااامادگی h hhh HH

مرحله ۲- آمادگی:در این مرحله ، آمادگی هر۴ وسیله (دو کامپیوتر و دو مودم)، در طرف فرستنده و گیرنده بررسی می‌شود . بدین‌منظور هر دو کامپیوتر فرستنده و گیرنده اعلام آمادگی خود را از طریق پین شماره ۲۰ به اطلاع مودم می رسانند. مودم‌ها نیز در پاسخ به ارسال پیام فوق، با فعال کردن پین شمارهء ۶ ، اعلام آمادگی متقابل خود را به کامپیوترها می رسانند.

مرحله ۳- برقراری ارتباط: در این مرحله یک اتصال فیزیکی بین مودم‌های فرستنده و گیرنده برقرار می‌شود . بدین‌منظور ابتدا کامپیوتر فرستنده از طریق پین شماره۴، اعلام درخواست خود را برای مودم ارسال می‌دارد و به دنبال آن مودم فرستنده نیز یک سیگنال حامل برای مودم طرف مقابل ارسال می‌کند. وقتی که مودم مقابل سیگنال حامل فوق را در یافت کرد، از طریق پین شمارهٔ ۸ ، وقوع احتمالی ارسال داده را به کامپیوتر متصل به خود اطلاع می‌دهد . کامپیوتر گیرنده نیز با فعال سازی پین شماره ۴ اعلام آمادگی خود را به مودم ارسال می‌دارد و مودم نیز یک سیگنال حامل برای

---

[1] Received data
[2] Request To Send
[3] Clear To Send
[4] DCE ready
[5] Signal ground common return
[6] Received Line Signal Detector
[7] DTE ready

مودم فرستنده ارسال می‌کند . در پاسخ به درخواست ارسال هر دو کامپیوتر، مودم‌های فرستنده و گیرنده نیز از طریق پین شمارهٔ ۵ ، اعلام آمادگی ارسال خود را به اطلاع کامپیوتر می‌رسانند .

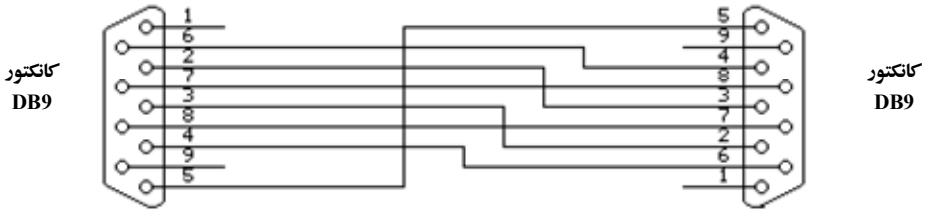
مرحله ۴ – ارسال داده ها :در این مرحله داده های دیجیتال بین دو کامپیوتر فرستنده و گیرنده مبادله می‌شود. بدین‌منظور کامپیوتر فرستنده از طریق پین شمارهٔ۲ داده های ارسالی خود را برای ارسال به مودم تحویل می‌دهد . همچنین از طریق پین شمارهٔ ۲۴ ، سیگنال زمان‌بندی بین کامپیوتر و مودم ارسال می‌شود . داده های ارسالی توسط مودم به صورت سیگنال‌های آنالوگ دریافتی به دیجیتال تبدیل می‌شوند و از طریق پین شماره۳ تحویل کامپیوتر می‌گردند .

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

درشکل (۲-۴۱)، مراحل برقراری ارتباط، ارسال داده ها و قطع ارتباط دریک مودم یک طرفه نشان داده شده است.

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

چنانچه بخواهیم دو DTE را به‌طور محلی بدون استفاده از مودم به یکدیگر متصل نماییم، در این صورت نیاز به کابل نال مودم داریم. در شکل (۲-۴۲) نمونه‌ای از یک کابل نال مودم با استفاده از کانکتورDB9 نشان داده شده است.



شکل (۲-۴۲): کابل نال مودم

۲-۴-۴- مودم

یکی از تجهیزات ارتباطی در شبکه های کامپیوتری مودم می‌باشد . با استفاده از این وسیله امکان تبادل فایل‌ها بین کامپیوترها، اتصال به اینترنت و ارسال و دریافت فاکس فراهم می آید . مودم در حقیقت ترکیبی از دو کلمه مدولاتور[1] و دی مدولاتور[2]می‌باشد . اطلاعات دیجیتال کامپیوترها توسط مودم تبدیل به سیگنال‌های آنالوگ قابل ارسال در شبکهٔ تلفن می‌گردد. درسمت گیرنده نیز، اطلاعات آنالوگ دریافتی تبدیل به اطلاعات دیجیتال می‌شود و تحویل کامپیوتر می‌گردد. بنابراین برای استفاده از مودم نیاز به یک خط تلفن می‌باشد.

مودم‌ها به دو دسته داخلی و خارجی تقسیم می‌شوند . مودم‌های داخلی، در داخل کامپیوتر بر روی یکی از اسلات‌های آن نصب می‌شوند. مودم‌های خارجی، خارج از کامپیوتر می‌باشند و مستقل عمل می‌کنند . این مودم‌ها از طریق کابل سریال RS 232 به کامپیوتر متصل می‌شوند . سرعت مودم‌ها متفاوت می‌باشد و در حدود ۳۰۰۰ تا بالاتر از ۵۶۰۰۰ بیت بر ثانیه است. به غیرازمودم‌های تلفنی ، مودم‌های دیگری نیز وجود دارند که بر روی خطوط استیجاری[3] فعال می‌باشند.

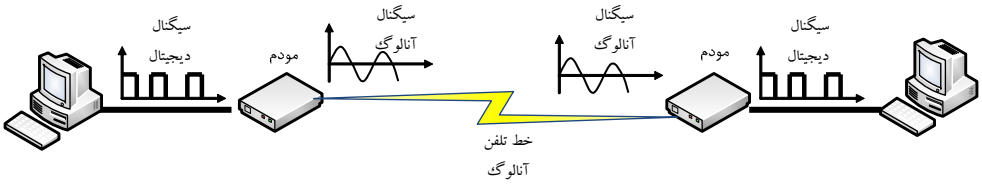
علاوه بر عملیات تبدیل اطلاعات دیجیتال به آنالوگ و بالعکس، هرمودم عملیات دیگری نظیر کنترل خطا و فشرده سازی اطلاعات را نیز بر عهده دارد. در شکل (۲-۴۳) نمونه‌ای از عملیات یک مودم نشان داده شده است .

مودم‌ها از تکنیک‌های تبدیل دیجیتال به آنالوگ نظیرASK , FSK, PSK و QAM استفاده می‌کنند . پهنای باند خطوط تلفن برای انتقال داده‌های دیجیتال حدود ۲۴۰۰ هرتز می‌باشد 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، سرعت‌های متفاوتی برای عملکرد مودم‌ها وجود دارد. درجدول (۲-۳) نرخ بیت ارسالی مودم‌ها بر اساس نوع مدولاسیون و نحوه عملکرد آنها آورده شده است.

امروزه اکثر استانداردهای مودم‌های موجود، براساسITU-T می‌باشند. در جدول (۲-۴) مشخصات برخی از مودم‌های ITU-T آورده شده است.

---

[1] Modulator
[2] Demodulator
[3] leased line



شکل(۲-۴۳): عملیات

مودم

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

نوع مدولاسیون	سرعت ارسال یک طرفه (بیت برثانیه)	سرعت ارسال دو طرفه (بیت برثانیه)
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 برثانیه)
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

بسیاری از مودم‌های امروزه مجهز به نرم افزاری می‌باشند که به‌وسیله آن قادر بـه پـشتیبانی از قابلیـت‌هـای مختلفـی هستند. این نوع مودم‌ها که به نام مودم‌های هوشمند معروف می‌باشـند، بـرای اولـین بـار توسـط شـرکت میکروکـامپیوتری Hayes، معرفی گردیدند . امروزه مودم‌های سازگار با Hayes توسط شرکت های کامپیوتری متعددی وارد بازارمی‌شوند.

مودم‌های هوشمند توسط دستورات AT کنترل و برنامه ریزی می‌شوند . شکل کلی این دستورات به شرح زیر است :

AT دستور [مشخصه‌ها] دستور [مشخصه‌ها] , ...

مهم‌ترین دستورات ATدر جدول (۲-۵) آورده شده است .

جدول (۲-۵): مهم‌ترین دستورات AT

دستور	مفهوم دستور	مشخصه‌ها
A	مودم را در حالت پاسخ گویی قرار می‌دهد	-----
B	مودم را در حالت کاری V.22bisدر سرعت ۱۲۰۰ بیت برثانیه قرار می‌دهد	-----
D	شماره گیری	شماره موردنظر
E	فعال سازی / غیر فعال سازی حالت اکو	۰ یا ۱
H	مودم را در حالت on/off hook قرار می‌دهد	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 شبکه‌های کامپیوتری برای ارسال اطلاعات استفاده مـی‌شـوند توصیف می‌گردند. در حالت کلی دو نوع رسانه انتقال در شبکه‌های کامپیوتری وجود دارد که عبارتند از: رسانه های هـدایت شونده[1] و رسانه های غیرهدایت شونده[2]. چنانچه دو کامپیوتر توسط رسانه های هدایت شونده به یکـدیگر متـصل شـوند، در این صورت یک کانال بین دو کامپیوتر متصل شده به یکدیگر وجود دارد. رسانه هایی نظیر زوج سیم بـه هـم تابیـده شـده[3]، کابل هم محور[4] و فیبر نوری[5] مثال‌هایی از رسانه های هدایت شونده می‌باشند. رسانه های غیرهدایت شونده یـا بـی‌سـیم، از امواج الکترومغناطیسی و بدون استفاده از هادی‌های فیزیکـی بـرای انتقـال اطلاعـات اسـتفاده مـی‌نماینـد. امـواج رادیـویی، مایکرویو، مخابرات سلولی (موبایل) و مخابرات ماهواره‌ای نمونه‌ای از رسانه های غیرهدایت شونده می‌باشند. در زیر به معرفی چند رسانه هدایت شونده می‌پردازیم.

۲-۵-۱- زوج سیم به هم تابیده شده

---

[۱] Guided
[۲] Unguided
[۳] Twisted-pair cable
[٤] Coaxial
[٥] Optical fiber

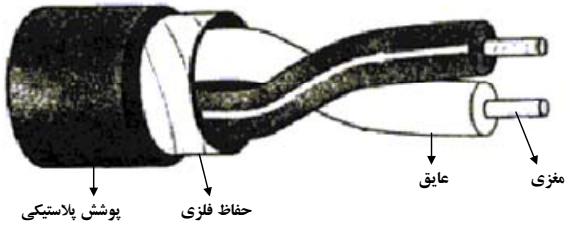
یک زوج سیم به هم تابیده شده شامل دو رشته سیم مسی روپوش‌دار می‌باشد که ضخامت تقریبی هر رشته سیم حدود یک میلی‌متر است. برای کاهش تداخل الکتریکی زوج سیم با زوج سیم‌های مشابه که در نزدیکی آن قرار دارند، این دو رشته سیم به صورت مارپیچ دور هم پیچیده می‌شوند. از این نوع سیم‌ها معمولاً در شبکه‌های تلفن استفاده وسیعی می‌شوند. می‌توان اطلاعات موجود در زوج سیم‌ها را تا چندین کیلومتر ارسال نمود، ولی چنانچه فاصله بیش از حدزیاد باشد باید در بین راه از تقویت‌کننده‌های مناسب استفاده شود.

در مراکزی که به چندین زوج سیم نیاز است؛ مانند تلفن‌کشی مجتمع‌های مسکونی، چندین زوج سیم به هم تابیده به صورت دسته‌هایی جمع می‌شوند و در یک غلاف محافظ قرار می‌گیرند. طیف فرکانسی زوج سیم به هم تابیده شده در محدودهء ۱۰۰ هرتز تا ۵ مگا هرتز می‌باشد. دو نوع زوج سیم به هم تابیده شده وجود دارد که عبارتند از:

- ***زوج سیم به هم تابیده شده بدون حفاظ،*** **(UTP[1])** : این نوع زوج سیم که متداولترین نوع در شبکه‌های انتقال داده امروزه نیز می‌باشد بدون حفاظ و حفاظ خارجی است. ارزانی، انعطاف‌پذیری و نصب آسان این نوع زوج سیم از مزایای عمده آن می‌باشند. از سوی سازمان EIA، ۵ ردهٔ مختلف از کاربردهای UTP تعیین شده است که برای انتقال اطلاعات در سرعت‌های بسیار پایین (رده یک) تا سرعت‌های بالا در حدود ۱۰۰ مگا بیت در ثانیه (رده پنج) به کار می‌روند. متداولترین کانکتورهای UTP، RJ45 می‌باشد که دارای ۸ رشته سیم (۴ زوج UTP) است و در شبکه‌های کامپیوتری کاربرد فراوان دارد.

- ***زوج سیم به هم تابیده شده حفاظ دار*** **(STP[2])** : همانطور که از نام این نوع زوج سیم نیز مشخص می‌باشد، در STP یک حفاظ فلزی به همراه یک پوشش پلاستیکی در اطراف زوج سیم به هم تابیده‌شده قرار می‌گیرد. وجود این حفاظ باعث کاهش نویزپذیری سیم می‌گردد و همچنین از القای متقابل[3] یک سیم برروی سیم دیگر جلوگیری می‌نماید. به خاطر وجود همین حفاظ در STP، قیمت این نوع رشته سیم از UTP بیشتر می‌باشد. در شکل (۲-۴۴) زوج سیم‌های UTP و STP نشان داده شده‌اند.

(الف)



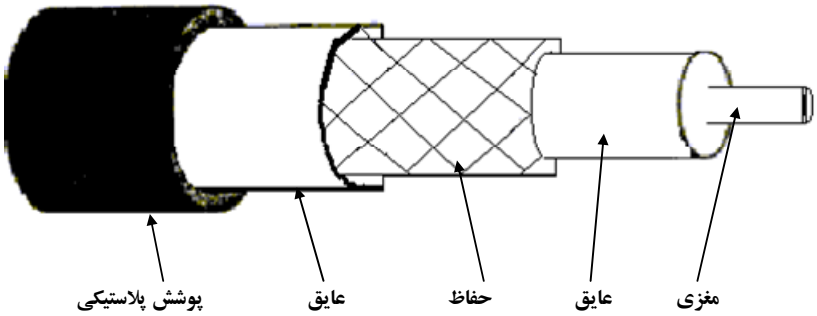
(ب)

[1] Unshielded Twisted-Pair
[2] Shielded Twisted-Pair
[3] 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 مادهٔ 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.



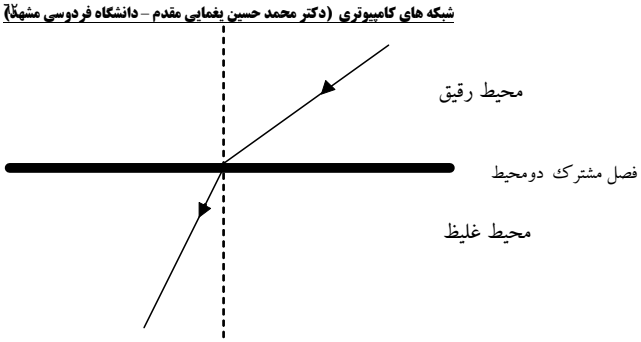
شکل (۲-۴۵): ساختار کابل هم محور

کابل هم‌محور دارای پهنای باند زیادی می‌باشد که در محدوده فرکانسی ۱۰۰ کیلوهرتز تا ۵۰۰ مگاهرتز قرار دارد. البته هرچه طول کابل افزایش یابد، حداکثرسرعت انتقال داده‌ها در کابل کم می‌شود. ۵ نوع متداول از کابل هم‌محوروجود دارند که عبارتند از: RG-9,RG-8 ، 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 وافزایش سرعت، نیاز به رسانه های انتقال با پهنای باند و اطمینان بالا حس گردید. بدین‌منظور فیبر نوری به‌عنوان یک رسانه هدایت شونده مناسب مطرح است. نور یک نوع موج الکترومغناطیسی است که با سرعت ۳۰۰ هزار کیلومتردر ثانیه درخلاء انتشار می‌یابد. در سایر محیط ها، سرعت نور به چگالی محیط بستگی دارد؛ طوری که با افزایش چگالی محیط سرعت نور کاهش می یابد. 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[1] 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 .

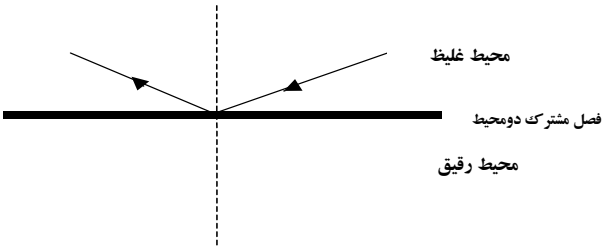
[1] Refraction



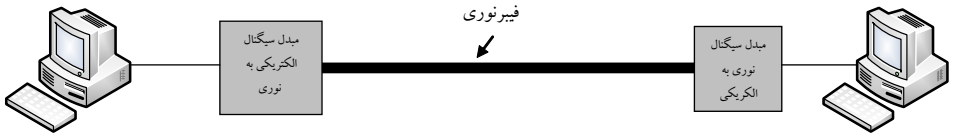
شکل (۲-۴۶):
پدیدهٔ شکست نور

هنگامی که نور از یک محیط غلیظ وارد یک محیط رقیق می‌گردد، زاویهء 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[1] نامیده می‌شود. 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 زاویهٔ انعکاس برابر می‌باشد. فیبر نوری از پدیده انعکاس برای انتقال نور استفاده می‌کند.اطراف فیبر نوری یک بافرمخصوص قرار دارد که آن را در مقابل رطوبت و نم محافظت می‌نماید. در اطراف بافر نیز یک پوشش محافظ قرار می‌گیرد.

در شکل (۲-۴۸) ساختار کلی یک سیستم انتقال نوری نشان داده شده است. در فرستنده از دیودهای نوری (LED[2]) و لیزر برای تبدیل سیگنال‌های الکتریکی به سیگنال‌های نوری استفاده می‌شود . در سمت گیرنده نیز ازگیرنده های نوری مخصوص جهت تبدیل سیگنال نوری به سیگنال الکتریکی استفاده می‌گردد.



شکل(۲-۴۷): پدیده بازتابش کلی



شکل(۲-۴۸): یک سیستم انتقال نوری

در فیبر نوری برای ارسال اطلاعات۰ و ۱ از پالس‌های نور مرئی استفاده می‌گردد.

---

[1] Critical angle
[2] Light Emitting Diode

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

فیبر نوری از دو قسمت اصلی تشکیل شده است که عبارتند از: مغزی[1] و غلاف[2]. هم مغزی و هم غلاف هر دو ازجنس شیشه می‌باشند. ضریب شکست مغزی بیشتر از ضریب شکست غلاف است که این امر باعث پدیده بازتابش کلی در فیبر نوری می‌شود. مطابق با شکل (۲-۴۹) سه نوع مختلف فیبر نوری وجود دارند که عبارتند از:

- ***فیبر نوری چند مود با ضریب شکست پله‌ای[3]:*** در این نوع فیبر، مغزی و غلاف دارای دو ضریب شکست مختلف می‌باشند. قطر مغزی نسبتاً زیاد می‌باشد و این باعث می‌شود که چندین پرتوی نوری مختلف با زاویه‌های تابش گوناگون وارد فیبر شوند. این پرتوهای نوری از مسیرهایی با طول مختلف به مقصد می‌رسند. از آنجایی‌که سرعت انتشار در محیط برای تمام این پرتوها یکسان می‌باشد، بنابراین پرتوی نوری که مسیر کمتری را طی کرده است زودتر از پرتوی نوری که مسیر طولانی را طی نموده است به مقصد می‌رسد. این مسئله باعث اعوجاج در پالس نوری دریافتی در مقصد می‌شود که آشکارسازی آن را با مشکل مواجه می‌سازد.

- ***فیبر نوری چندمود با ضریب شکست تدریجی[4]:*** در این نوع فیبر نیز قطر مغزی نسبتاً زیاد می‌باشد که باعث می‌شود تا پرتوهای نوری مختلف با زوایای تابش گوناگون وارد فیبر شوند. برخلاف فیبرنوری با ضریب شکست پله‌ای، در این نوع فیبر ضریب شکست به‌طور ناگهانی تغییر نمی‌کند بلکه هر چه از محور مرکزی فیبر فاصله می‌گیریم، ضریب شکست به‌طور تدریجی کاهش می‌یابد. این امر باعث می‌شود که پرتوهای نوری که از محور مرکزی فیبر دور هستند و فاصله بیشتری را طی می‌کنند 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 می‌کنند و مسیر کوتکه‌تری را طی می‌کنند با سرعت کمتری به مقصد برسند. بنابراین تدریجی بودن ضریب شکست فیبر، باعث همزمان رسیدن تمام پرتوهای نوری ارسالی فرستنده در گیرنده می‌شود و این امر باعث کاهش اعوجاج پالس نوری در گیرنده می‌شود.

- ***فیبر تک‌مود[5]***: در این نوع فیبر، قطر فیبر تا حد طول موج نور کاهش یافته است و این کاهش باعث می‌شود که پرتوی نور بدون انعکاس و بر روی یک خط مستقیم منتشر شود و به مقصد برسد. بنابراین در فیبر نوری تک‌مود، پالس نوری در مقصد با کمترین اعوجاج دریافت می‌شود و آشکارسازی آن آسان می‌باشد.

نوع فیبر نوری، با توجه به نسبت قطر مغزی آن به قطر غلاف شناخته می‌شود . 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

---

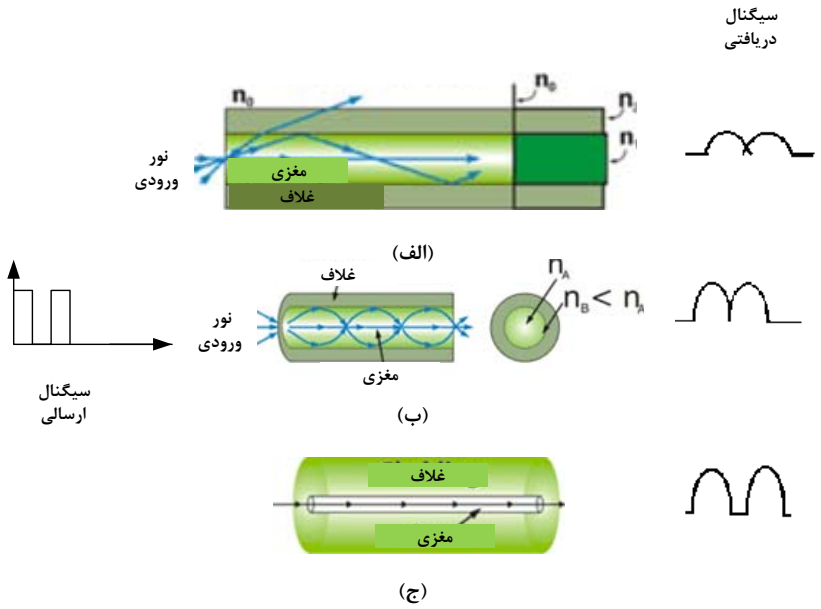
[1] Core
[2] Cladding
[3] Multimode step- index
[4] Multimode graded- index
[5] Single mode

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

درفیبر نوریTight 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 Bufferاغلب 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 داده‌ها با سرعت بسیار بالا مفید می‌باشد. علاوه بر شبکه‌های محلی، از فیبر نوری می توان در شبکه‌های مخابراتی راه دور و شبکه تلفن نیز استفاده کرد. به‌طور خلاصه مزایای فیبر نوری را می توان نویزپذیری کم، تضعیف کم و پهنای باند بسیار بالا دانست. البته فیبر نوری دارای معایبی نیز می‌باشد که مهم‌ترین آنها عبارتند از: هزینه بالا (به‌خصوص در مورد فیبرهای تک‌مود)، نیاز به تخصص بالا در نصب و نگهداری آن و همچنین شکنندگی زیاد.

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



شکل (۲-۴۹): سه نوع فیبر نوری

الف) فیبر چند مود با ضریب شکست پله‌ای ب) فیبر چند مود با ضریب شکست تدریجی ج) فیبر تک مود

جدول (۲-۶): انواع فیبر نوری

نوع فیبر	قطر مغزی (میکرون)	قطرغلاف (میکرون)

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

۲-۵-۴ - امواج رادیویی

امواج رادیوئی که بخشی از طیف امواج الکترومغناطیسی می‌باشند، بر اساس فرکانس به۸ دستهٔ عمده تقسیم می‌شوند که عبارتند از :

_ امواج با فرکانس بسیار پایین (VLF[1]) (۳ الی ۳۰کیلوهرتز)

_ 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 گیگا هرتز)

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

_ امواج با فرکانس شدیداً بالا(EHF[8]) (۳۰ الی ۳۰۰ گیگا هرتز)

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

- انتشار سطحی [9]
- انتشار در قسمت پایین هوای کره(تروفوسفوریک[10])
- انتشار یونوفسفریک [11]
- انتشار در خط مستقیم[12]
- انتشار فضایی [13]

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

---

[1] Very Low Frequency
[2] Low Frequency
[3] Medium Frequency
[4] High Frequency
[5] Very High Frequency
[6] Ultra High Frequency
[7] Super High Frequency
[8] Extremely High Frequency
[9] Surface propagation
[10] Tropospheric propagation
[11] Ionospheric propagation
[12] Line of sight Propagation
[13] Space propagation

در انتشار تروفسفوریک، امواج ارسالی با سطح پایین جو برخورد کرده و منعکس می‌شوند. البته مـی تـوان فرسـتنده و گیرنده را نیز در یک مسیر و در دید یکدیگر قرار داد و امواج رادیوئی را ارسال نمود . سیگنال‌های رادیویی MF از این نـوع انتشار استفاده می‌کنند.

در انتشار یونوسفریک امواج رادیویی فرکانس بالا HF به سطح میانی جو برخورد کـرده و در آن‌جـا بـه سـمت زمـین منعکس می‌گردند.از این نوع انتشار در حالتیکه توان ارسال کم می‌باشـد و فاصـله فرسـتنده و گیرنـده زیـاد اسـت اسـتفاده می‌گردد.

در انتشار درخط مستقیم، سیگنال‌های رادیویی بسیار فرکانس بالای VHF و UHF مستقیماً در یـک خـط راسـت، بین فرستنده و گیرنده منتقل می‌شوند. در این حالت آنتن‌های فرستنده و گیرنده باید دقیقاً در معرض دید مستقیم یکدیگر قرارداشته باشند.

در انتشارفضایی که درمخابرات ماهواره‌ای استفاده می‌شود، امواج رادیویی VHF ، SHF و EHF از جو زمـین عبـور کرده و به‌وسیلهٔ آنتن ماهواره دوباره به سمت زمین منعکس می‌شوند.

۲-۵-۵- امواج مایکروویو

امواج مایکروویو قادر به پیمودن انحنای کره زمین نمی‌باشند، بلکه ارسال و دریافت آنها بر روی خطـوط مـستقیم و در دید یکدیگر می‌باشد. فاصله مستقیمی که امواج مایکروویو قادر به پیمودن آن می‌باشند، بستگی به ارتفاع آنتن دارد، به‌طوری که هرچه آنتن بزرگتر باشد فاصله بیشتری می تواند طی شود. معمولاً آنتن‌های مـایکروویو در نقـاط بلنـد، نظیـر بـرج‌هـا و کوهستان قرارمی‌گیرند. امواج مایکروویو در هرلحظه در یک جهت انتشار می یابند. بنابراین برای برقراری ارتباط دوطرفه نیاز به دو فرکانس متفاوت می‌باشد و برای هر فرکانس فرستنده و گیرندهٔ مخصوصی نیاز می‌باشد. البته می توان هر دو فرستنده و گیرنده را در یک دستگاه به نام فرستنده/گیـرنده ادغام نمود.

برای افزایش برد امواج مایکروویو از تکرار کننده های مناسب استفاده می‌شود . هر تکـرار کننـده، امـواج مـایکروویو را دریافت می‌نماید و پس از تقویت با استفاده از آنتن‌های مناسب امواج را به تکرار کنندهٔ بعدی ارسـال مـی‌کنـد. فاصـلهٔ بـین تکرار کننده‌ها بستگی به فرکانس امواج مایکروویو و همچنین شرایط محیطی دارد . براساس نوع سیستم به کار گرفته شـده، هر تکرار کننده می تواند سیگنال دریافتی را با همان فرکانس و یا با فرکانس متفاوت ارسـال دارد. سیـستم‌هـای مـایکروویو دارای دو نوع آنتن به نام‌های آنتن‌های سهموی[1] وشیپوری[2] می‌باشند.

۲-۵-۶- مخابرات ماهواره‌ای

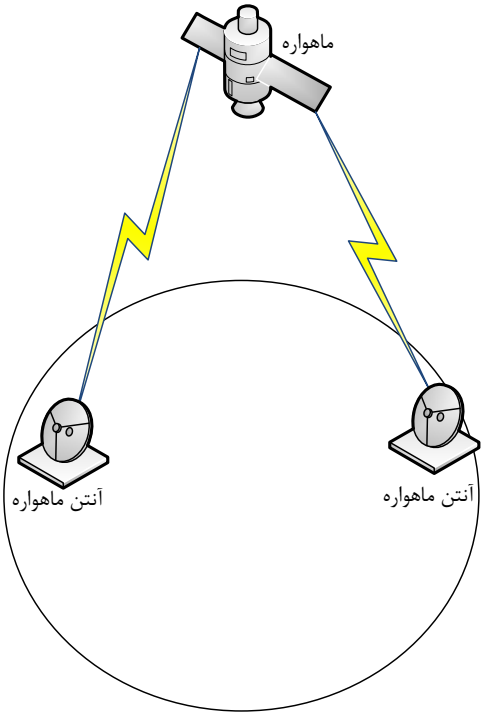
انتشار امواج درسیستم‌های مخابرات ماهواره ای شبیه ارسال امواج مایکروویو، بر روی مسیر مستقیم صورت می‌گیردکه در آن یک ایستگاه زمینی اطلاعات را برای یک ماهواره که دور زمین می چرخد ارسال می‌دارد. اصول سیستم‌های ماهواره‌ای نیز مشابه سیستم‌های مایکروویو می‌باشد که در آن ماهواره مانند یک تکرار کننده عمل می‌کند. در شکل (۲-۵۰) نمونه‌ای از یک سیستم ماهواره نشان داده شده است .

با استفاده از سیستم‌های ماهواره ای از هر نقطه زمین می توان برای هر نقطه دیگر از زمـین اطلاعـات را ارسـال کـرد. بنابراین سیستم‌های مخابرات ماهواره ای از کیفیت ارتباطی بالایی برخوردار هستند . ماهواره به تنهایی قیمت بالایی دارد اما اجاره کردن فرکانسهای ماهواره‌ای و یا اجاره کردن زمانی آن قیمت نسبتاً مناسبی دارد .

---

[1] Parabolic
[2] Horn

برای ارسال مستقیم امواج، باید آنتن‌های فرستنده و گیرنده در دید یکدیگر قرار داشته باشند، در غیر این صورت امکان برقراری ارتباط وجود ندارد. بنابراین ماهواره‌هایی که سریعتر و یا کندتر از زمین حرکت می‌کنند، فقط برای دوره زمانی کوتاهی در طول روز قابل استفاده می‌باشند. برای آن‌که ارتباط دایمی برقرار باشد، ماهواره باید با همان سرعت زمین، دور زمین گردش نماید، طوری‌که نسبت به زمین ثابت باشد. به این نوع ماهواره‌ها، ماهواره‌های ژئوسنکرون[1] می گویند.



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

از آنجایی‌که سرعت مداری حرکت ماهواره‌ها به فاصله آنها از زمین بستگی دارد، بنابراین فقط یک مدار ژئوسنکرون وجود دارد . این مدار در فاصله تقریبی ۲۲ هزار مایلی سطح زمین قرار دارد. یک ماهواره ژئوسنکرون به تنهایی نمی‌تواند کل کره زمین را پوشش دهد؛ بلکه حداقل به۳ ماهواره ژئوسنکرون که در زاویه ۱۲۰ درجه از یکدیگر قرار دارند برای پوشش کل زمین نیاز می‌باشد. فرکانسهای مورد استفاده در مخابرات ماهواره‌ای در محدوده گیگاهرتز می‌باشد. هر ماهواره در دو باند فرکانسی متفاوت اقدام به ارسال و دریافت اطلاعات می‌نماید . ارسال امواج از زمین به ماهواره، کانال بالا [2] و ارسال امواج از ماهواره به زمین، کانال پایین [3] 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 فرکانسی	کانال پایین (برحسب گیگا هرتز)	کانال بالا (برحسب گیگا هرتز)

[1] Geosynchronous
[2] Up link
[3] Down link

C	۳/۷ الی ۴/۲	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 می‌شود. در سیستم تلفن‌های سلولی پس از شناسایی و ردگیری محل کاربر، یک کانال فرکانسی خاص برای مکالمه ایجاد می‌گردد و به کاربر تخصیص داده می‌شود. چنانچه کاربر از محدودهٔ کانال اختصاص یافته به آن خارج شود، سیگنال آن از کانال قبلی به کانال جدیدی منتقل می‌شود.

برای ردگیری کاربران در شبکه های تلفن سلولی، سطح شهر به مناطق کوچکی به نام سلول تقسیم می‌شوند. هر سلول شامل آنتن خاصی می‌باشد و توسط یک دفتر کوچکی اداره می‌شود . هریک از دفترهای فوق به نوبت توسط یک دفترمرکزی به نام دفتر سوئیچینگ تلفن موبایل (MTSO[1]) کنترل می‌شوند.

هر MTSO وظیفه ایجاد هماهنگی لازم بین دفاتر سلولی و اداره‌ء مرکزی تلفن را به عهده دارد. اندازه سلول‌ها 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 سلول‌های کوچکتری نسبت به سایر مناطق استفاده می‌کنند. برای جلوگیری از تداخل بین سلول‌های مجاور توان ارسالی هر سلول به اندازه کافی کم درنظر گرفته می‌شود. تلفن‌های سلولی از روش آنالوگ FM برای برقراری ارتباط بین تلفن متحرک و اداره سلولی استفاده می‌کنند. دو باند فرکانسی ۸۲۴ الی ۸۴۹ مگاهرتز برای ارتباط‌هایی که با تلفن موبایل شروع می‌شود و باند فرکانسی۸۶۹ الی ۸۹۴ مگاهرتز برای ارتباط‌هایی که توسط تلفن‌های ثابت آغاز می‌شود، اختصاص یافته است. فرکانسهای حامل به فاصله ۳۰ کیلوهرتزی از یکدیگر قرار دارند، بنابراین هر باند قادر به پشتیبانی از ۸۳۳ فرکانس حامل می‌باشد. از آنجایی‌که برای هر ارتباط دوطرفه به دو فرکانس حامل نیاز است، درنتیجه در هر باند فرکانسی فقط ۴۱۶ کانال وجود دارد. البته برخی از این کانال‌ها برای عملیات کنترل و برقراری ارتباط رزرو شده‌اند. علاوه بر این برای جلوگیری از تداخل، کانال‌های فوق طوری بین سلول‌ها توزیع شده اند که دو سلول مجاور از کانال یکسان استفاده ننمایند. 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 می‌نماید . به‌دنبال آن تلفن موبایل کل باند فرکانسی را جاروب نموده و به دنبال یک کانال خالی کنترلی می‌گردد. سپس شماره تلفن مخاطب را با استفاده از کانال کنترلی به نزدیکترین اداره سلول ارسال می‌دارد. اداره سلول نیز داده‌های دریافتی را به MTSO ارسال می‌دارد وMTSO نیز داده‌ها را به اداره مرکزی تلفن ارسال می‌کند. چنانچه مخاطب در دسترس باشد، اداره مرکزی تلفن اتصال را برقرار می‌کند و آن را به MTSO ارسال می‌کند. MTSO نیز یک کانال خالی صوتی پیدا نموده و به دنبال آن ارتباط برقرار می‌شود. تلفن موبایل به طور اتوماتیک خود را به کانال جدید وفق می‌دهد و ارتباط صوتی برقرار می‌شود. هنگامی که یک تلفن ثابت مایل به برقراری ارتباط با یک تلفن موبایل می‌باشد، ادارهٔ مرکزی تلفن شماره مخاطب را برای MTSO ارسال می‌کند. MTSO نیز با ارسال پیام‌های جستجو برای هر سلول به دنبال محل تلفن موبایل مخاطب می‌گردد.

[1] Mobile Telephone Switching Office

هنگامی‌که MTSO محل تلفن موبایل مخاطب را پیدا کرد، برای آن یک سیگنال زنگ ارسال می‌دارد و پس از آن‌که 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 مقایسهٔ سیستم‌ها و رسانه های ارسال از ۵ مشخصه کارآیی استفاده می‌شود، این مشخصه‌ها عبارتند از :

- ***هزینه :*** شامل هزینهٔ سرمایه‌گذاری و همچنین هزینهٔ 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 حالی‌که فیبر نوری از امنیت بیشتری برخوردار می‌باشد.

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

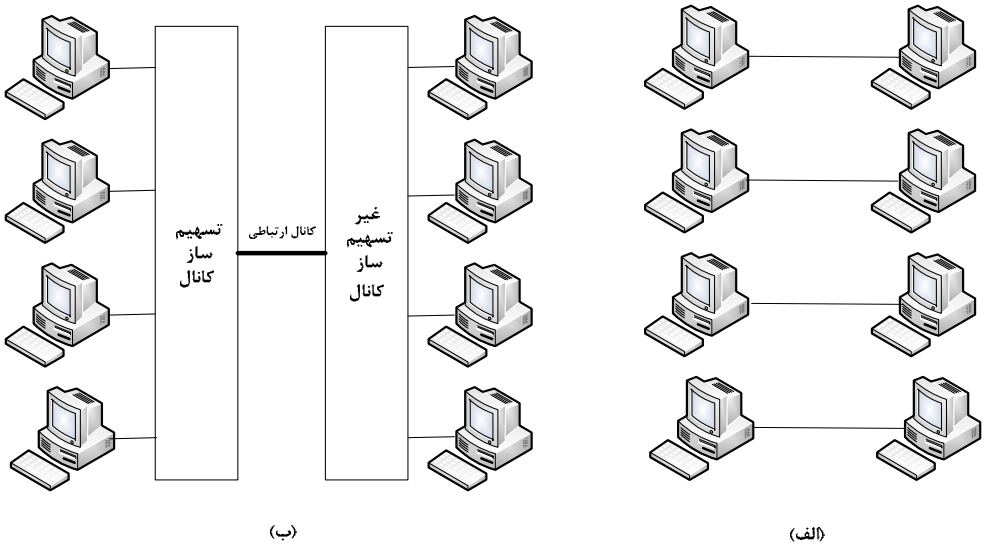
جدول (۲-۸): کارآیی رسانه های ارسال

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

۲-۶- تسهیم سازی

یکی دیگر از وظایف لایهء فیزیکی، تسهیم سازی می‌باشد. هنگامی‌که ظرفیت کانالی که دو وسیله کامپیوتری را به یکدیگر متصل می‌نماید، از ظرفیت مورد نیاز برای ارسال بیشتر باشد، در این صورت می‌توان از کانال به‌طور مشترک استفاده نمود و چندین وسیلهٔ کامپیوتری را از طریق آن به همدیگر متصل کرد. با استفاده از تسهیم سازی، امکان ارسال همزمان چندین کامپیوتر برروی یک کانال فیزیکی مشترک فراهم می‌آید.

طبیعی است که استفاده از تسهیم سازی، و استفادهء مشترک از یک کانال باعث کاهش تعداد کانال‌های مورد نیاز می‌شود و هزینهٔ ارتباطی نیز کاهش می‌یابد. در شکل(۲-۵۱)، نمونه‌ای از یک تسهیم کننده[1] کانال آورده شده‌است. در این مثال، چهار کامپیوتر از طریق یک تسهیم‌کننده کانال که به اختصار به آن MUX گفته می‌شود، به یک کانال مشترک متصل شده‌اند. در سمت گیرنده با استفاده از یک DEMUX جریان اطلاعاتی هریک از کامپیوترها از کانال جدا می‌شود و تحویل گیرنده مربوطه می‌گردد.



شکل (۲-۵۱): نمونه‌ای از کاربرد یک تسهیم کنندهٔ کانال
الف) اتصال مستقیم بدون تسهیم کننده کانال ب) اتصال با استفاده از تسهیم کنندهٔ 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 تقسیم‌بندی می‌شوند. در زیر به بررسی هر یک از روش‌های مختلف فوق می‌پردازیم.

۲-۶-۱- تسهیم سازی فرکانسی(FDM)

این روش یک تکنیک آنالوگ می‌باشد و در مواقعی که پهنای باند کانال از پهنای باند سیگنال‌های ارسالی بیشتر است استفاده می‌شود. در روش FDM هریک از سیگنال‌های ارسالی در فرکانس‌های مختلف حامل مدوله می‌شوند که این

[1] Multiplexer
[2] Time Division Multiplexing
[3] Frequency Division Multiplexing

فرکانس‌های حامل به اندازه کافی از یکدیگر فاصله دارند تا تداخلی در سیگنال‌ها به‌وجود نیاید. در شکل (۲-۵۲) مثالی از عملیات تقسیم فرکانسی کانال نشان داده شده است.

به‌عنوان مثال، یکی از کاربردهای متداول FDM در تلویزیون‌های کابلی می‌باشد. کابل‌های هم‌محور که در سیستم تلویزیون‌های کابلی استفاده می‌شوند دارای پهنای باندی در حدود ۵۰۰ مگاهرتزمی‌باشند. هر کانال تلویزیون در حدود ۶مگاهرتز پهنای باند نیاز دارد. با این حساب هر کابل هم‌محور در حدود۸۳ کانال تلویزیون را سرویس می‌دهد. اما در عمل با توجه به این‌که مقداری از پهنای باند به‌عنوان باند محافظ استفاده می‌شود، تعداد کانال‌هایی که توسط هر کابل هم‌محور سرویس داده می‌شود به مراتب کمتر از ۸۳ می‌باشد.

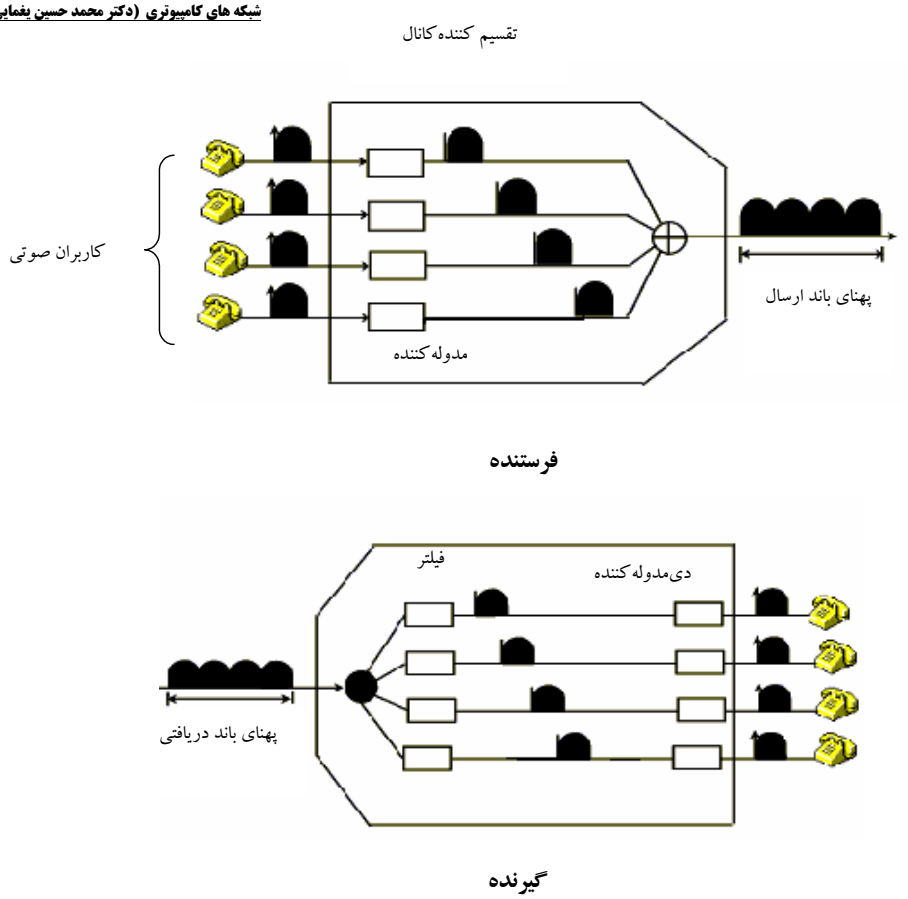
با گسترش تکنولوژی فیبر نوری از روش WDM[1] که مشابه FDM برای ارسال سیگنال‌های نوری است، استفاده می‌شود.

۲-۶-۲- تسهیم سازی زمانی (TDM)

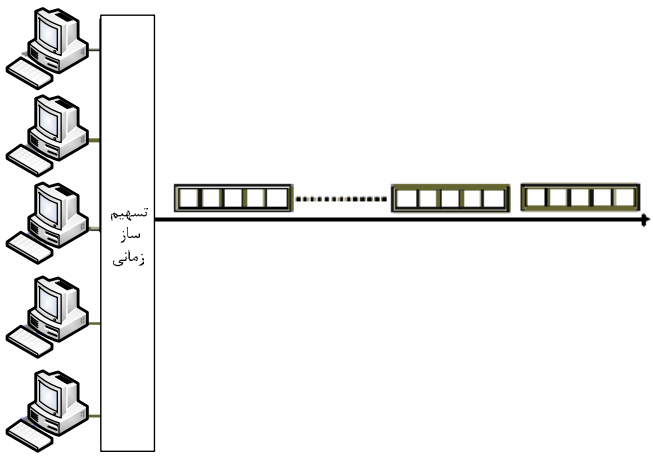
روش TDM یک تکنیک دیجیتال برای تسهیم سازی زمانی کانال بین کاربران می‌باشد و در مواقعی که نرخ ارسال داده کانال ، از نرخ ارسال مورد نیاز هریک از تجهیزات کامپیوتری متصل به کانال بیشتر است، استفاده می‌گردد. در روش TDM همزمان، زمان به برش‌های ثابتی تقسیم‌بندی می‌شود و هر برش زمانی در اختیار یک کاربر قرار می‌گیرد. هر ایستگاه متصل به کانال، فقط در مواقعی که برش زمانی مخصوص آن برسد، اجازه ارسال داده‌ها در کانال را دارد و در سایر زمان‌ها اجازه ارسال از آن سلب می‌شود. در روش TDM همزمان، چنانچه ایستگاهی هیچ داده‌ای برای ارسال در برش زمانی خود نداشته باشد، در این صورت آن برش زمانی بدون استفاده می‌ماند که این امر باعث اتلاف ظرفیت کانال می‌شود 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 می‌باشد. در صورتی‌که همه ایستگاه‌های متصل به کانال دارای سرعت ارسال یکسان باشند، به هریک از آنها در هر قاب یک برش زمانی ثابت می‌رسد. هنگامی‌که نرخ ارسال یک ایستگاه بیشترازسایر ایستگاه‌ها باشد، آن ایستگاه می‌تواند برش‌های زمانی بیشتری در یک قاب را اشغال کند. به‌عنوان مثال اگر سرعت پایه یک سیستم TDM همزمان ۱۲۰۰ بیت بر ثانیه باشد، چنانچه ایستگاهی دارای سرعت ارسال ۴۸۰۰ بیت بر ثانیه باشد، دراین‌صورت آن ایستگاه ۴ برش زمانی را در هر قاب به خود اختصاص می‌دهد. در شکل (۲-۵۳) مثالی از عملکرد یک سیستم تقسیم زمانی همزمان آورده شده است.

[1] Wavelength Division Multiplexing



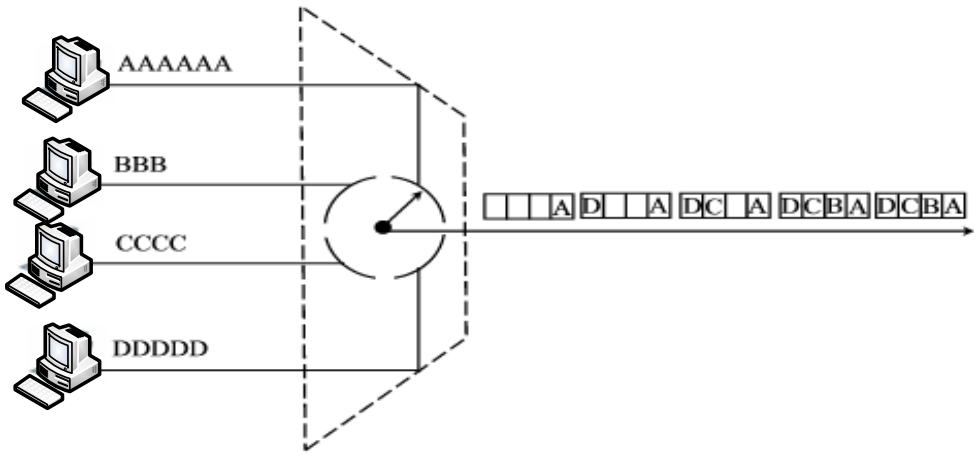
شکل (۲-۵۲): نمونه‌ای از عملیات تقسیم فرکانسی کانال



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. درشکل (۲-۵۴) مثالی از یک سیستم TDM همزمان آورده شده است، که درآن برخی از برش‌های زمانی به دلیل عدم وجود ترافیک ارسالی خالی مانده است .

برای رفع این مشکل، روش TDM غیر همزمان ارائه شده است. در این روش، مجموع سرعت همهٔ ایستگاه‌های 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 می‌باشند، برخلاف روش TDM همزمان تعداد برش‌های زمانی در هر قاب به مراتب از N کمتر می‌باشد. به عبارت دیگردر یک سرعت یکسان کانال، تعداد ایستگاه‌های متصل شونده به کانال در روش TDM غیرهمزمان از روش TDM همزمان بیشتر می‌باشد. تعداد برش‌های زمانی موجود در هر قاب، به وسیله آنالیز آماری ترافیک ورودی هر ایستگاه تعیین می‌شود، از اینرو به این روش، TDM آماری[1] نیز گفته می‌شود.



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 مدت‌ها 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 می‌شوندکه درزیر 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 می‌شود .

به این نوع اتصال دراصطلاح حلقه محلی[2] گفته می‌شود. این سیستم‌ها، شبکه‌های تلفن سوئیچینگ محلی (PSTN[3]) نامیده می‌شوند. سیگنال ارسالی در حلقه محلی از نوع آنالوگ می‌باشد و پهنای باند آن معمولاً از فرکانس صفر تا ۴ کیلو هرتز می‌باشد . در خطوط سوئیچینگ هنگامی که یک مشتری اقدام به شماره گیری می‌کند، مکالمه مورد نظر به

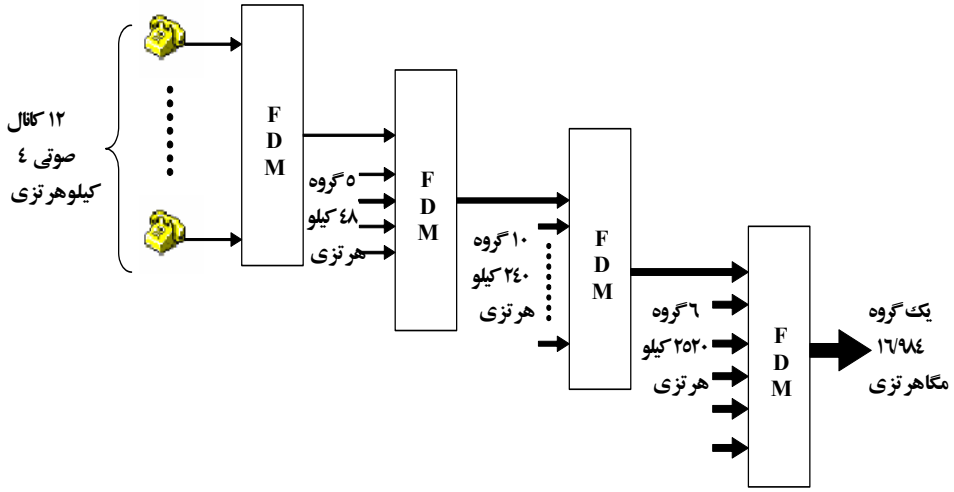
[1] Statistical TDM
[2] local loop
[3] Public Switched Telephone Network

سمت یک یا چند سوئیچ هدایت می‌شود . بعد از انتخاب سوئیچ مناسب، ارتباط بین دو طرف مکالمه از طریق کانال‌های ارتباطی بین سوئیچ‌ها برقرار می‌شود .

- 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 نمی‌باشد.

برای استفاده بهینه ازظرفیت شبکه تلفن، شرکت‌هایی تلفن با استفاده از تسهیم‌سازها سیگنال‌های ورودی را از خطوط پهنای باند پایین به خطوط پهنای باند بالاتسهیم سازی می‌نمایند . معمولاً درخطوط آنالوگ از روش تسهیم‌سازی FDM استفاده می‌شود. نمونه‌ای از سیستم سلسله مراتبی آنالوگ[1] که AT&T از آن استفاده می‌نماید در شکل (۲-۵۵) نشان داده شده است.



شکل (۲-۵۵): نمونه‌ای 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 کیلو هرتز می‌دهند. در سطح بعدی، ۵ گروه با یکدیگر تسهیم سازی می‌شوند و تشکیل یک ابرگروه با ظرفیت ۲۴۰ کیلو هرتز می دهند .هر ابرگروه شامل ۶۰ کانال ۴ کیلوهرتز صوتی می‌باشد . در سطح بعدی ۱۰ ابرگروه با یکدیگر تسهیم سازی شده و تشکیل یک گروه بزرگ[2] می دهند.

هرگروه بزرگ دارای پهنای باند ۲/۵۲ مگاهرتز می‌باشد که می تواند ۶۰۰ کانال صوتی را پشتیبانی نماید. مقداری از پهنای باند هر گروه بزرگ (۱۲۰ کیلوهرتز) به‌عنوان محافظ بین کانال‌های صوتی استفاده می‌شود. در آخرین مرحله، ۶ گروه بزرگ با یکدیگر ترکیب می‌شوند و تشکیل یک گروه بسیار بزرگ[3] می‌دهند.

هر گروه بسیار بزرگ دارای پهنای باند ۱۵/۱۲ مگاهرتزمی‌باشد، اما با در نظر گرفتن باندهای محافظ، هر گروه بسیار بزرگ دارای پهنای باند۱۶/۹۸۴ مگاهرتز می‌باشد، که قادر به پشتیبانی از ۳۶۰۰ کانال صوتی۴ کیلو هرتز است.

---

[1] Analog hierarchy
[2] Master group
[3] Jumbo group

۲-۶-۳-۲- سرویس سوئیچینگ دیجیتال

امروزه اکثر شرکت‌هایی تلفن از سرویس دیجیتال برای سرویس‌دهی به مشترکین خود استفاده می‌کنند. یکی از مزایای عمدهء 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 آنجایی‌که سیگنال ارسالی از نوع دیجیتال است جداسازی آن از نویز آسانتر می‌باشد. یکی دیگر از مزایای ارسال دیجیتا ل هزینه کم آن است. از آنجایی‌که 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[1]
۲- سرویس دادهء دیجیتال DDS[2]
۳- سرویس سیگنال دیجیتال DS[3]

سرویس سوئیچ شده /۵۶ : این سرویس درحقیقت نسخه دیجیتا ل از خطوط سوئیچ شدهء 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 شبکهٔ تلفن معمولی، حتی با داشتن مودم قادر به برقراری ارتباط با مشترک سرویس سوئیچ شده / ۵۶ ، نمی‌باشد . از آنجایی‌که 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[4])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 ازمودم گرانتر است اما به خاطر سرعت بیشتر، کیفیت بالاتر و نویز پذیری کمترخطوط 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 ارائهٔ سرویسی نظیر کنفرانسهای ویدئویی، فاکس سریع، سرویس چند رسانه ای و ارسال داده با سرعت بالا می‌باشند.

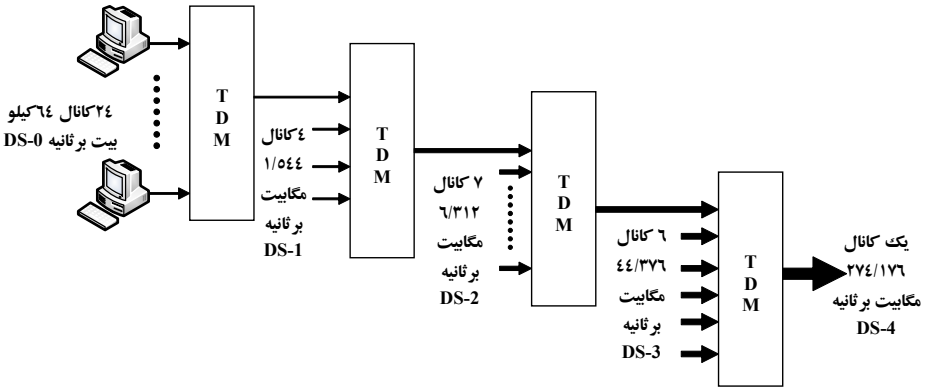
سرویس DDS : این سرویس درحقیقت یک نسخهء دیجیتال از خطوط استیجاری آنالوگ می‌باشد . بنابراین می توان به آن خطوط استیجاری دیجیتال گفت.حداکثر سرعت سرویس DDS مشابه سرویس سوئیچ شده/ ۵۶برابربا ۵۶ کیلو بیت بر ثانیه است . البته در این سرویس کاربران قادر به انتخاب یکی از نرخ‌های ارسال ۲/۴، ۴/۸، ۹/۶، ۱۹/۲ و یا ۵۶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

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

---

[1] Switched/56
[2] Digital Data Service
[3] Digital Signal Service
[4] Digital Service Unit

سلسله مراتبی سیگنال‌های 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 می‌باشند با یکدیگر با استفاده از تسهیم سازی زمانی TDM ترکیب شده و تشکیل یک کانال DS-1 با سرعت ۱/۵۴۴ مگابیت بر ثانیه می‌دهند . در هر کانال DS-1 ، ۸ کیلو بیت بر ثانیه به‌عنوان بالاسری استفاده می‌شود. در مرحله بعدی ۴ کانال DS-1 (۹۶ کانال DS-0) با یکدیگر ترکیب می‌شوند و تشکیل یک کانال DS2 با سرعت ۶/۳۱۲ مگابیت برثانیه می دهند. در مرحلهٔ بعدی ۷ کانالDS-2 (۶۷۲ کانالDS-0) با یکدیگر ترکیب می‌شوند 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 به‌عنوان بالاسری استفاده می‌شود . در مرحله بعدی ۶ کانال DS-3 (۴۰۳۲ کانالDS-0) با یکدیگرترکیب می‌شوند 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 به‌عنوان بالاسری استفاده می‌شود . معمولاً برای پیاده سازی سرویس DS شرکت‌هایی تلفن از خطوط T (T1 تا T4) استفاده می‌کنند . 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

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

خطوط T از نوع دیجیتال می‌باشند و برای ارسال داده های دیجیتال و یا سیگنال‌های صوت و تصویر دیجیتال شده به کار می روند. در مواردی می توان از آنها برای ارسال آنالوگ نیز استفاده نمود. بدین‌منظور سیگنال‌های آنالوگ ابتدا باید نمونه برداری شوند و سپس با روش تسهیم سازی زمانی به اطلاعات دیجیتال تبدیل گردند. کشورهای اروپایی از خطوط E که نسخه‌ای از خطوط T می‌باشد استفاده می‌نمایند . هر دو سیستم از نظر مفهومی مشابه یکدیگر می‌باشند، ولی سرعت‌های ارسال آنها با یکدیگر متفاوت است .

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

جدول (۲-۱۰): نرخ ارسال خطوط E

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

علاوه برسرویس دیجیتال فوق، امروزه شرکت‌هایی تلفن ازسرویس دیگری نظیر ISDN[1]، NET[2] و ATM[3] استفاده می‌نمایند که در فصل‌های بعدی آنها را توضیح خواهیم داد .

۲-۷- فن آوری خط دیجیتال نامتقارن مشترکین(ADSL[4])

روش‌های موجود فعلی برای ارسال و دریافت داده‌ها در سرعت بالا تقریباً پر هزینه می‌باشد. شرکت‌هایی بزرگ برای اتباط‌های راه دور خود معمولاً از خطوط مایکرویو و ماهواره استفاده می‌کنند و برای انتقال داده‌ها و اتباط‌های تلفنی از خطوط گران قیمت T1 و E1 به‌صورت اجاره‌ای بهره می برند. به‌علت هزینه بالای اشتراک خطوط فوق ،شرکت‌هایی متوسط و کوچک قادر به استفاده از فن‌آوری‌های فوق برای اتباط‌های خود نمی‌باشند. بدین‌منظور فن‌آوری ADSL ارائه شده است. با استفاده از خطوط تلفن موجود و با بهره بردن از فن‌آوری ADSL شرکت‌های و فراهم کنندگان سرویس اینترنت قادر به برقراری ارتباط خصوصی با سرعت بالا می‌باشند.

خطوط سیم مسی تلفن برای حمل صوت و یا سیگنال‌های 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 سیگنال‌های فرکانس بالا بر روی خطوط مسی باعث تضعیف انرژی و تداخل می‌گردد که این امر موجب اختلال در ارسال داده می‌شود. به خاطر عدم وجود تضعیف زیاد، فیبر نوری برای ارسال سریع داده های کامپیوتری در فواصل طولانی بسیار مناسبتر از سیم‌های مسی می‌باشد، اما باید توجه نمود که فیبرهای نوری به مراتب گران قیمت تر از سیم‌های مسی می‌باشند. با استفاده از فن آوری ADSL امکان افزایش ظرفیت خطوط مسی برای پشتیبانی از ارسال داده‌های سرعت بالا مانند کنفرانس‌های ویدئویی، سرویس محیط چند رسانه‌ای و دسترسی سریع به اینترنت فراهم می‌آید. در حقیقت ADSL نوع مهمی از خانوادهٔ فن‌آوری خط دیجیتال مشترکین(DSL[5]) می‌باشد. هنگامی‌که مودم و منشعب‌کننده[6] با هم استفاده می‌شوند، فن‌آوری ADSL مطابق با شکل (۲-۵۷) امکان ارائهٔ توأم با هم سرویس تلفن و ارسال داده‌های 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 می‌شود:

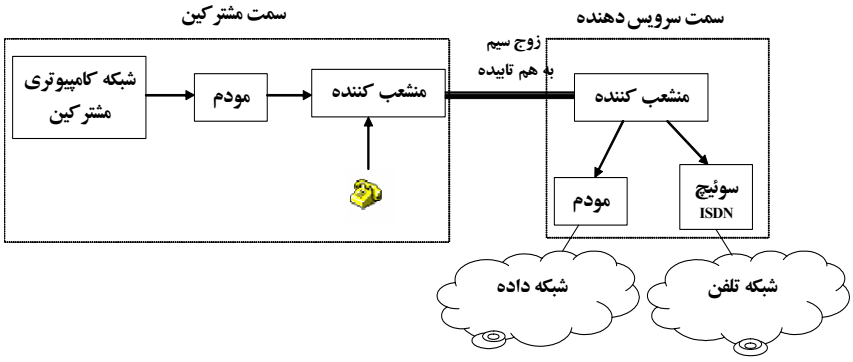
الف) اتباط‌های تلفنی معمولی در فاصله فرکانسی صفر تا ۳۴۰۰ هرتز

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

---

[1] Integrated Services Digital Network
[2] Synchronous Optic NETwork
[3] Asynchronous Transfer Mode
[4] Asymmetric Digital Subscriber Line
[5] Digital Subscriber Line
[6] Splitter

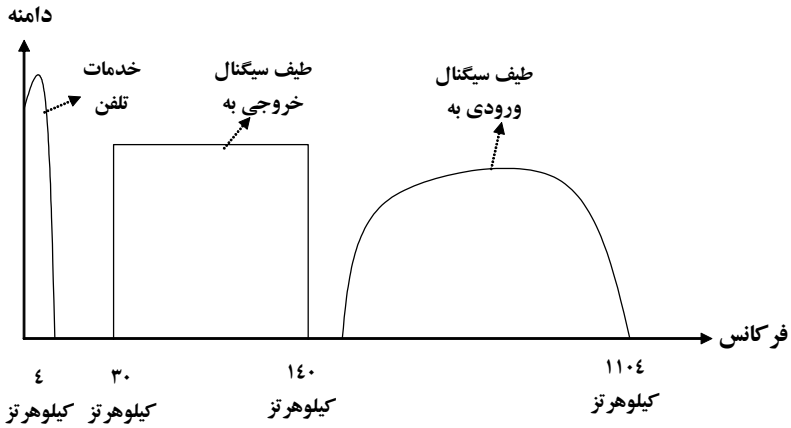
ج) انتقال داده ها به سمت مشتری در حداکثر فرکانس ۱۱۰۴ کیلوهرتز



شکل(۲-۵۷): پیکره بندی ADSL

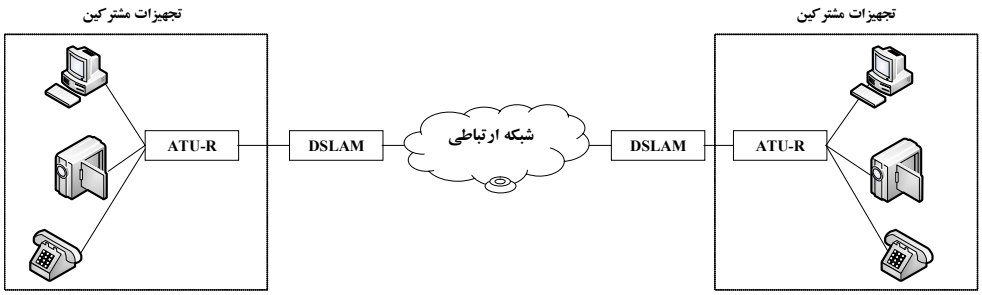
در شکل (۲-۵۸) طیف فرکانسی ADSL نشان داده شده است. از آنجایی‌که در ADSL سیگنال‌های خروجی در محدودهٔ فرکانسی ۳۰ کیلوهرتز تا ۱۴۰ کیلو هرتز و سیگنال‌های ورودی در محدودهٔ فرکانسی تا حداکثر ۱۱۰۴ کیلوهرتز قرار دارند، بنابراین ظرفیت ارسال داده در جهت ارسال ۶۴۰ کیلو بیت بر ثانیه و در جهت دریافت ۶۱۴۴ کیلو بیت بر ثانیه می‌باشد. به‌خاطر تفاوت نرخ ارسال و دریافت در ADSL به این فن آوری ارسال نامتقارن گفته می‌شود. دلیل نامتقارن بودن سرعت ارسال و دریافت در ADSL کاهش القای متقابل می‌باشد.

درسمت مشترکین ADSL یک واحد فرستنده گیرندهٔ ADSL به نام ATU-R قرار می‌گیرد. در سمت شبکهٔ ارتباطی نیز یک تسهیم‌ساز دسترسی به خطوط دیجیتال مشترکین (DSLAM[1]) وجود دارد. با استفاده از یک تسهیم‌ساز فوق؛ امکان جابجایی و هدایت ترافیک‌های ورودی چندین ATU-R وجود دارد. از شبکه های ارتباطی موجود برای ارتباط بین تسهیم کننده های دسترسی به خطوط مشترکین دیجیتال استفاده می‌شود. در شکل (۲-۵۹) نمونه‌ای از پیکربندی شبکه نقطه به نقطهٔ ADSL نشان داده شده است که درآن امکان ارائهٔ سرویس باند وسیع به مشترکین فراهم می‌آید.



شکل(۲-۵۸): طیف فرکانسی سیگنال‌های ADSL

[1] Digital Subscriber Line Access Multiplexer



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

از آنجایی‌که سیم کشی تلفن در اغلب ساختمان‌ها وجود دارد نیازی به کانال‌کشی برای پیاده سازی سرویس ADSL نمی‌باشد. در سرویس ADSL امکان دریافت داده‌ها در سرعت حداکثر ۶۱۴۴ کیلو بیت بر ثانیه وجود دارد که با مقایسهٔ سرعت مودم‌های استاندارد ۵۶ کیلو بیت بر ثانیه به مراتب بیشتر می‌باشد. فن‌آوری ADSL در مقایسه با سایرفن‌آوری‌های موجود نظیر ISDN و خطوط T و E دارای مزایای زیر است :

الف) هزینهٔ نصب و بهره‌برداری ازتجهیزات ADSL بسیار پایین است.

ب) سرعت ارسال و دریافت در ADSL برای سرویسی نظیر ارسال داده‌های سریع و کنفرانسهای ویدئویی بالا می‌باشد.

ج) استفادهٔ از ADSL ساده است. اتصال به اینترنت از طریق ADSL نیاز به هیچ‌گونه شماره‌گیری ندارد.

درجدول (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 برثانیه	۱ مگابیت برثانیه
ITU G.992.1	ADSL (G.DMT)	۱۲ مگابیت برثانیه	۱/۳ مگابیت برثانیه
ITU G.992.1 Annex A	ADSL over POTS	۱۲ مگابیت برثانیه	۱/۳ مگابیت برثانیه
ITU G.992.1 Annex B	ADSL over ISDN	۱۲ مگابیت برثانیه	۱/۸ مگابیت برثانیه
ITU G.992.2	ADSL Lite (G.Lite)	۴ مگابیت برثانیه	۰/۵ مگابیت برثانیه
ITU G.992.3/4	ADSL2	۱۲ مگابیت برثانیه	۱ مگابیت برثانیه
ITU G.992.3/4 Annex J	ADSL2	۱۲ مگابیت برثانیه	۳/۵ مگابیت برثانیه
ITU G.992.3/4 Annex L	RE-ADSL2	۵ مگابیت برثانیه	۰/۸ مگابیت برثانیه
ITU G.992.5	ADSL2+	۲۴ مگابیت برثانیه	۱ مگابیت برثانیه
ITU G.992.5 Annex L[1]	RE-ADSL2+	۲۴ مگابیت برثانیه	۱ مگابیت برثانیه
ITU G.992.5 Annex M	ADSL2+M	۲۴ مگابیت برثانیه	۳/۵ مگابیت برثانیه

پرسش‌های فصل

۱. انواع سیگنال‌های الکتریکی را نام برده و با ذکر یک مثال مشخصات هر یک را توضیح دهید.
۲. طیف فرکانسی و پهنای باند را با ذکر یک مثال توضیح دهید.
۳. ظرفیت کانال، فاصلهٔ بیت نرخ ارسال بیت را تعریف کنید.
۴. انواع روش‌های کدینگ سیگنال‌های الکتریکی را نام ببرید.
۵. انواع روش‌های کدینگ دیجیتال به دیجیتال را نام برده و با رسم شکل هر یک را توضیح دهید.
۶. دو مشکل اصلی روش کدینگ قطبی را تشریح نمایید.
۷. عملکرد روش قطبی را نوشته و انواع آن را تشریح نمایید.
۸. برتری و عیب روش RZ را نسبت به روش NRZ بنویسید.
۹. رشته بیت ۱۱۰۰۱۰۱۰۰۱۱۰۰۱۰۱۰۱ را درنظر بگیرید. شکل موج خروجی حاصل از کدینگ رشته بیت فوق را درحالات زیر رسم نمایید:
۱۰. الف) روش قطبی ب) روش NRZ-I ج) روش NRZ-L د) روش RZ
۱۱. ح) روش منچستر و) روش منچستر تفاضلی ز) روش AMI
۱۲. مشکل اصلی روش AMI را نوشته و راه‌حل‌های موجود برای حل مشکل فوق را تشریح نمایید.
۱۳. رشته بیت ۱۰۰۱۰۰۰۰۰۰۰۰۰۱۰۱۱۰۰۰۰۱ را درنظر بگیرید. شکل موج خروجی حاصل از کدینگ B8ZS و HDB3 را رسم کنید.
۱۴. عملکرد و موارد کاربرد کدینگ آنالوگ به دیجیتال را تشریح نمایید.
۱۵. اساس کار سیستم‌های PCM را تشریح نمایید.
۱۶. عملکرد و مورد استفاده کدینگ دیجیتال به آنالوگ را بنویسد.
۱۷. انواع روش‌های کدینگ دیجیتال به آنالوگ را نام ببرید.
۱۸. شکل موج خروجی حاصل از کدینگ رشته بیت ۱۰۱۰۰۰۱۱۰۱ را به روش‌های زیر رسم نمایید.
۱۹. الف) روش ASK ب) روش FSK ج) روش PSK
۲۰. مدولاسیون‌های ASK و FSK را بایکدیگر مقایسه کرده و برتری هریک را بردیگری بنویسید.
۲۱. برای افزایش سرعت نرخ ارسال بیت در مدولاسیون PSK به چه صورت می توان عمل نمود؟
۲۲. نحوه عملکرد مدولاسیون QAM را نوشته و آن را با روش‌های ASK و PSK مقایسه نمایید.
۲۳. دیاگرام فازی 8-PSK،QAM۱۶- و 32-QAM را رسم کنید.
۲۴. عملکرد، کاربرد و انواع روش‌های تبدیل آنالوگ به آنالوگ را توضیح دهید.
۲۵. چنانچه پهنای باند یک فرستندهء رادیویی AM درمحدودهء فرکانس‌های ۱۰۰ کیلو هرتز الی ۲۰۰ کیلو هرتز باشد، با فرض آن‌که پهنای باند محافظ برابر با ۲ کیلو هرتز بین هر دو ایستگاه رادیویی مجاور درنظر گرفته شود، حداکثر تعداد ایستگاه‌های رادیو AM و فرکانس حامل هریک را به‌دست آورید.
۲۶. مدولاسیون‌های AM، FM و PM را از نظر پهنای باند با یکدیگر مقایسه نمایید.
۲۷. روش ارسال سری و موازی را بایکدیگر مقایسه نمایید.
۲۸. روش ارسال همزمان وغیرهمزمان را توصیف کرده و برتری هر روش را بردیگری بنویسید.

۲۹. ویژگی‌های واسط RS232 را توضیح داده و پین‌های مهم آن را بنویسید.
۳۰. مودم را تعریف کرده و کاربرد آن را توصیف نمایید.
۳۱. مراحل برقراری یک ارتباط مودمی را بارسم شکل توصیف نمایید.
۳۲. موارد استفاده کابل نال مودم را نوشته و ساختار آن را رسم کنید.
۳۳. مودم‌های هوشمند را توضیح دهید.
۳۴. مهم‌ترین 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 قسمت‌هایی تشکیل شده است؟ وظیفه هر قسمت را توضیح دهید.
۳۹. امواج رادیویی از نظر فرکانس به چند دسته تقسیم می‌شوند؟
۴۰. انواع انتشار امواج رادیویی را توضیح دهید.
۴۱. مورد کاربرد سیستم‌های مایکرویو را بنویسید.
۴۲. اساس کارمخابرات ماهواره‌ای و قسمت‌های تشکیل‌دهنده آن را توصیف نمایید.
۴۳. اصول کار سیستم‌های تلفن سلولی را توضیح دهید.
۴۴. مشخصه‌های 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 قسمت‌های مختلف آن را بنویسید.
۴۸. روش TDM همزمان و TDM غیرهمزمان را بایکدیگر مقایسه نمایید.
۴۹. سیستم سلسله مراتبی آنالوگ AT&T را رسم نمایید.
۵۰. عملکرد و موارد کاربردسرویس سوئیچ شده/۵۶ را تشریح نمایید.
۵۱. عملکرد سرویس دادهٔ دیجیتال (DDS) را نوشته و تفاوت آن را باسرویس سوئیچ شده/۵۶ بنویسید.
۵۲. سیستم سلسله مراتبی DS را تشریح نمایید.
۵۳. فن‌آوری ADSL را توضیح داده و مزایای آن را بنویسید.
۵۴. نمودار پهنای باندی سیستم‌های ADSL را رسم نمایید.

فصل سوم

لایهٔ پیوند داده

۳-۱- مقدمه

در این فصل به بررسی لایه پیوند داده و وظایف مهم آن می‌پردازیم. در لایه فیزیکی که در فصل قبل به بررسی آن پرداختیم، داده‌های ارسالی در قالب رشته بیت‌های ۱ و ۰ به سیگنال‌های الکتریکی مناسب تبدیل می‌شوند و وارد محیط انتقال می‌گردند. حال برای کنترل داده‌ها و تعیین این‌که کدام یک از کامپیوترهای متصل به کانال باید داده‌های ارسالی را دریافت دارند، از مکانیسم‌های کنترلی لایه دوم استفاده می‌شود. لایه پیوند داده براساس وضعیت کانال و نحوه اتصال ایستگاه‌ها به یکدیگر، عملیات خود را انجام می‌دهد. مثلاً در کانال‌های دو طرفه امکان ارسال همزمان داده در طرفین کانال وجود دارد، درحالی‌که در کانال‌های یک‌طرفه چنانچه همزمان ایستگاه‌ها اقدام به ارسال نمایند، تداخل به‌وجود می‌آید. 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 داده‌ها در گیرنده، کنترل سرعت ارسال فرستنده و تنظیم آن با سرعت دریافت گیرنده مهم می‌باشد. این عملیات کنترل جریان نام دارد.
- ***کنترل خطا:*** لایه پیوند داده با استفاده از مکانیسم‌های کنترل خطا، متوجه وقوع خطا در کانال ارسالی می‌شود و در این‌صورت اقدامات لازم برای تصحیح خطا و یا درخواست ارسال مجدد داده‌ها را از گیرنده انجام می‌دهد. 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 می‌باشد. برای پی بردن به اهمیت مسئله فوق به مثالی توجه نمایید. فرض کنید که دو کامپیوتر به‌طور مستقیم از طریق یک کانال نقطه به نقطه به یکدیگر متصل شده‌اند. چنانچه کامپیوتر فرستنده با سرعتی بیشتر از آنچه کامپیوتر گیرنده قادر به دریافت آن است، اقدام به ارسال داده‌های خود بنماید، در این‌صورت طبیعی است که بعد از مدتی بافر گیرنده سرریز می‌شود و بعد از آن تمامی داده‌های ارسالی از بین خواهد رفت. یکی از روش‌های معمول برای رفع مشکل فوق، استفاده از روال‌های کنترل جریان می‌باشد. هنگامی‌که بافر گیرنده در آستانه پرشدن است، کامپیوتر گیرنده با ارسال پیامی از فرستنده درخواست می‌نماید که دیگر اطلاعاتی ارسال ننماید تا این‌که دوباره بافر آن خالی شود. در این لحظه گیرنده با ارسال پیام مناسبی به فرستنده از او می‌خواهد که دوباره ارسال اطلاعات را از سر بگیرد. معمولاً گیرنده با دریافت هریک یا هرچند قاب، اقدام به ارسال پیام تصدیق (ACK[1]) مبنی بردریافت صحیح قاب‌ها به فرستنده می‌نماید. با دریافت این پیام تصدیق، فرستنده از دریافت صحیح قاب توسط گیرنده اطمینان حاصل می‌نماید و قادر است سایر قاب‌ها را ارسال کند. در صورتی‌که قاب‌های 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 می‌شود.

دو روش کلی برای کنترل جریان وجود دارد که عبارتند از :

---

[1] Acknowledge

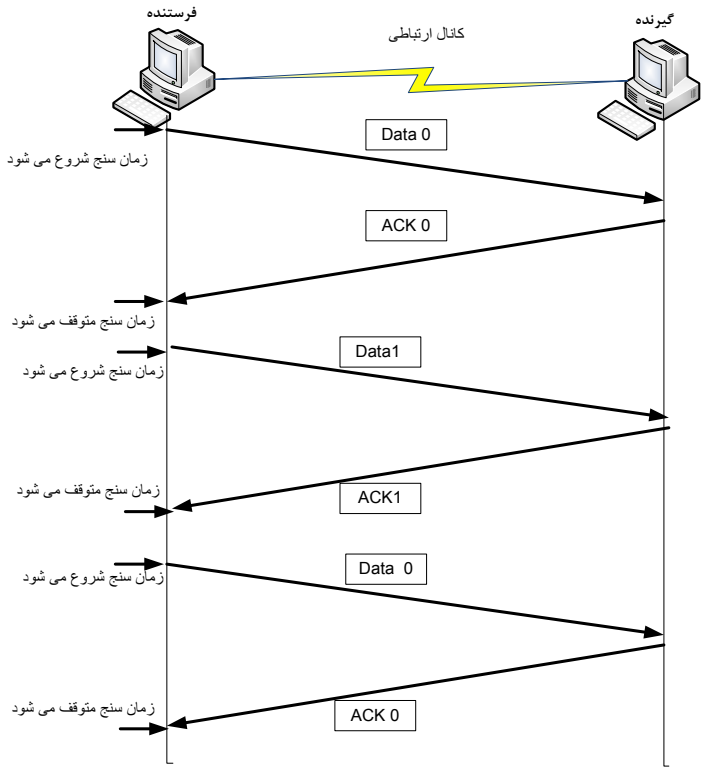
[2] Not-Acknowledge

- روش توقف و انتظار[1]
- روش پنجره لغزان [2]

در ادامه به بررسی هریک از دو روش فوق می‌پردازیم.

۳-۲-۱- روش توقف و انتظار

در این روش با ارسال هر قاب فرستنده منتظر دریافت پیام تصدیق از طرف گیرنده می‌ماند و هنگامی‌که پیام تصدیق قاب قبلی را دریافت نمود، قادر به ارسال قاب جدید می‌باشد. در شکل (۳-۱) مثالی از عملکرد روش توقف و انتظارآورده شده است. از آن‌جایی‌که در این روش، قبل از این‌که قاب بعدی ارسال شود، قاب قبلی بررسی می‌شود و از دریافت صحیح آن در گیرنده اطمینان حاصل می‌گردد، این امر باعث سادگی پیاده‌سازی پروتکل می‌شود که از مزایای عمده روش توقف و انتظار می‌باشد. عیب عمده این روش، بهره‌وری کم آن است. از آن‌جایی‌که با توجه به این‌که 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 می‌شود که در روش فوق، فرستنده باید مدت زیادی بی‌کار بماند که باعث کاهش سرعت و بهره‌وری کانال می‌گردد. نام دیگر روش فوق، ARQ[3] بی‌کار می‌باشد.



شکل(۳-۱) : مثالی از روش توقف و ارسال

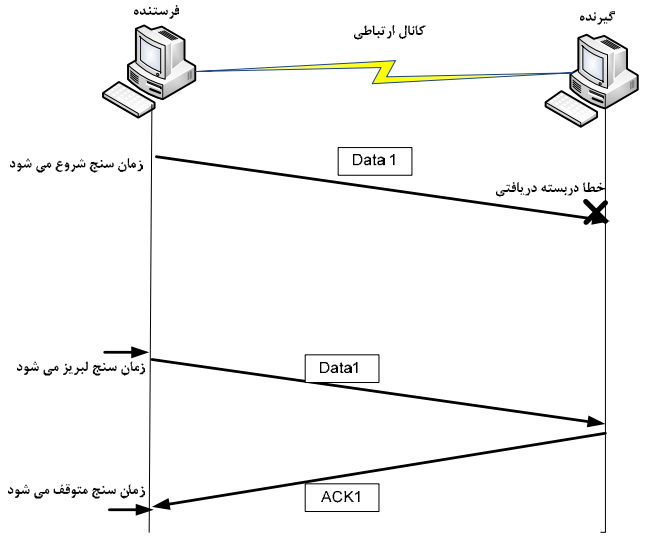
در روش توقف و انتظار با ارسال هر قاب یک زمان‌سنج خاص نیز فعال می‌گردد. چنانچه قبل از اتمام زمان زمان‌سنج، پیام تصدیق قاب ارسالی دریافت شود، در این‌صورت زمان‌سنج قطع می‌شود و قاب بعدی ارسال می‌گردد. ولی چنانچه

---

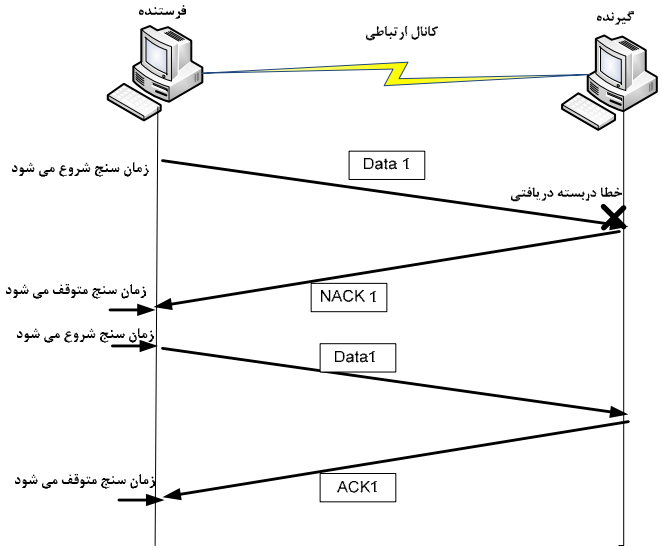
[1] Stop and wait
[2] Sliding window
[3] Automatic Repeat reQuest

زمان‌سنج به پایان رسیده و پیام تصدیق قاب ارسالی دریافت نشود، در این‌صورت فرستنده متوجه بروز مشکلی در سیستم می‌شود و دوباره قاب قبلی را ارسال می‌کند. در این روش تنها به دو شماره قاب (۰ و ۱) نیاز می‌باشد.

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 انتظارآورده 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- بهره وری کانال[1]

[1] Channel utilization

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:

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

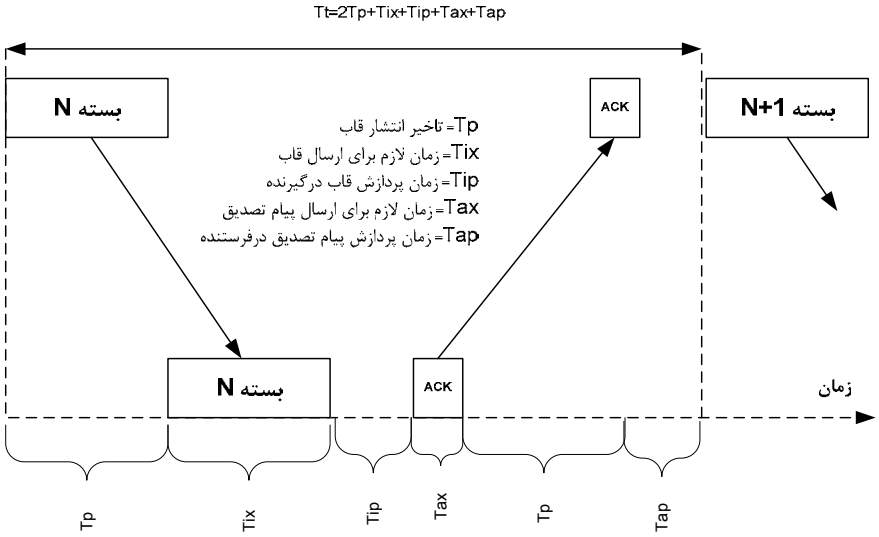
که T_{ix} زمان مورد نیاز فرستنده برای ارسال قاب و T_t برابر T_{ix} بعلاوه مقدار زمانی است که فرستنده برای دریافت پیام تصدیق منتظر می ماند.

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 تقریبا معادل $T_{ix} + 2T_p$ است. از اینرو یک رابطه تخمینی برای U بصورت زیر است :

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

نسبت T_p / T_{ix} معمولا 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 نسبتا کوتاه که مقدار a کمتر از ۱ است ، بهره وری کانال با تقریبا خوب براب 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 ازاینرومقادیر کم a) بالا است اما با افزایش نرخ داده (واز 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

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 دربالا 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 ارسالهای 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 مقدارBER موجود درکانال 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 $N_i P << 1$ ، $P_f = 1-(1-P)^{N_i} \approx N_i P$. 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 فرستند ه 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

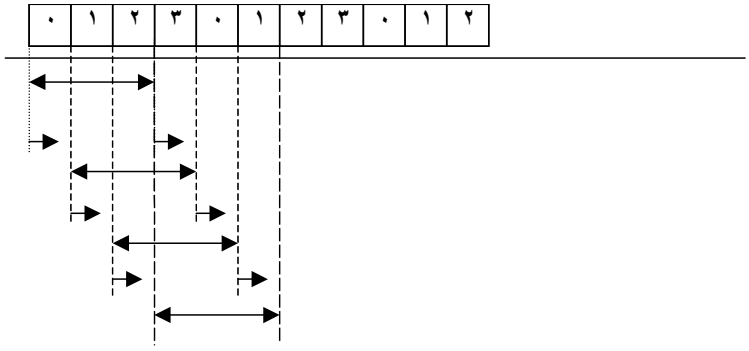
چنانچه فاصله فرستنده و گیرنده از یکدیگر زیاد باشد، در این صورت طولانی بودن این فاصله باعث افزایش تأخیر بین ارسال قاب‌ها و کاهش بهره‌وری از کانال می‌شود. به‌عنوان مثال یک کانال ماهواره با سرعت ۵۰ کیلوبیت بر ثانیه را در نظر بگیرید که تأخیر انتشار رفت و برگشت در آن ۵۰۰ میلی ثانیه است. چنانچه فرستنده یک قاب ۱۰۰۰ بیتی را ارسال دارد با توجه به سرعت کانال ماهواره، ۲۰ میلی ثانیه بعد، ارسال قاب تمام شده است و ۲۷۰میلی ثانیه بعد قاب به‌طور کامل به گیرنده می‌رسد. در صورتی که گیرنده همان لحظه پیام تصدیق ارسال دارد ۵۲۰ میلی ثانیه بعد فرستنده متوجه سالم رسیدن قاب ارسالی خود در گیرنده می‌شود. با این حساب اگر از روش توقف و انتظار استفاده شود، فرستنده در حدود۹۶ (۵۰۰/۵۲۰) درصد از کانال را از دست داده است و فقط از ۴ درصد ظرفیت کانال استفاده می‌نماید. با این مثال متوجه

[1] Bit Error Rate

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 کارآیی سیستم به شدت پایین می آید 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.

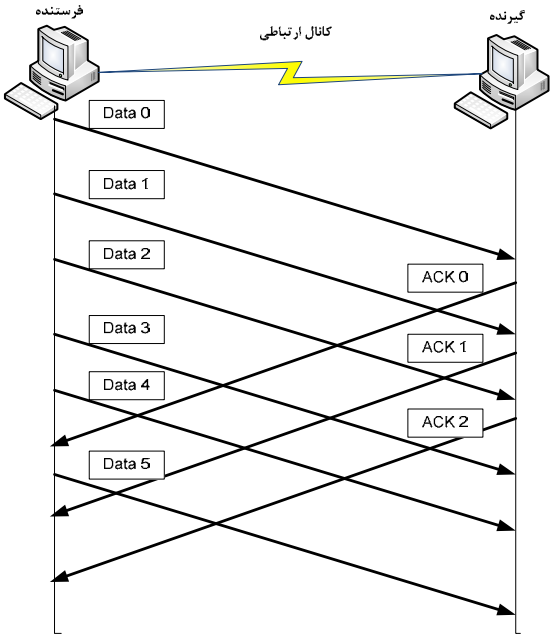
روش پنجره لغزان که با نام ARQ پیوسته نیز نامیده می‌شود، از نظر سرعت و بهره‌وری از کانال به مراتب بهتر از روش قبل می‌باشد. در این روش فرستنده بدون آن‌که منتظر دریافت پیام تصدیق قاب‌های ارسالی قبلی خود باشد، اقدام به ارسال پیوسته قاب‌ها می‌نماید. گیرنده نیز به‌طور دسته جمعی با دریافت چندین قاب، اقدام به ارسال پیام تصدیق می نماید. 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 ...،۰،۱،۲،۳،۴،۵،۶،۷،۰،۱،۲،۳،۴،۵،۶،۷ شماره‌گذاری و ارسال می‌گردند. هنگامی‌که گیرنده پیام تصدیق مبنی بردریافت صحیح یک قاب را ارسال می‌دارد، در پیام فوق شماره قاب بعدی را که انتظار دریافت آن را از گیرنده دارد، ذکرمی نماید. 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، لبه بالایی پنجره یک واحد اضافه می‌شود. هنگامی‌که فرستنده پیام تصدیق مربوط به قاب‌های ارسالی قبلی خود را دریافت کرد، در این حالت لبه 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 =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 شوندو از بین بروند. در این‌صورت فرستنده باید دوباره قاب‌های معیوب را ارسال کند. بنابراین فرستنده نیاز به یک بافر به اندازه طول

پنجره ارسال دارد تا قادر به نگه‌داری قاب‌های ارسالی باشد. هنگامی‌که 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. هنگامی‌که 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 زمان‌سنج فعال می‌شود و چنانچه در مدت زمان فعال‌بودن زمان‌سنج 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 مواجه با خطا وجود دارد که عبارتند از: روش بازگشت به عقب به اندازه N[1] و روش تکرار انتخابی.[2] در زیر به بررسی هریک از این دو روش می‌پردازیم.

۳-۲-۲-۱- روش بازگشت به عقب به اندازه N

در این روش چنانچه ضمن ارسال قاب‌ها خطایی به‌وجود 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.

دراین مثال فرض برآن است که قاب شماره ۲، ضمن ارسال دچار خطا شده‌است. گیرنده تمامی قاب‌های دریافتی بعدی را نادیده می‌گیرد و منتظر می‌ماند تا قاب شماره ۲ را دوباره دریافت کند. هنگامی‌که زمان‌سنج مربوط به قاب شماره

[1] Go back N
[2] Selective repeat

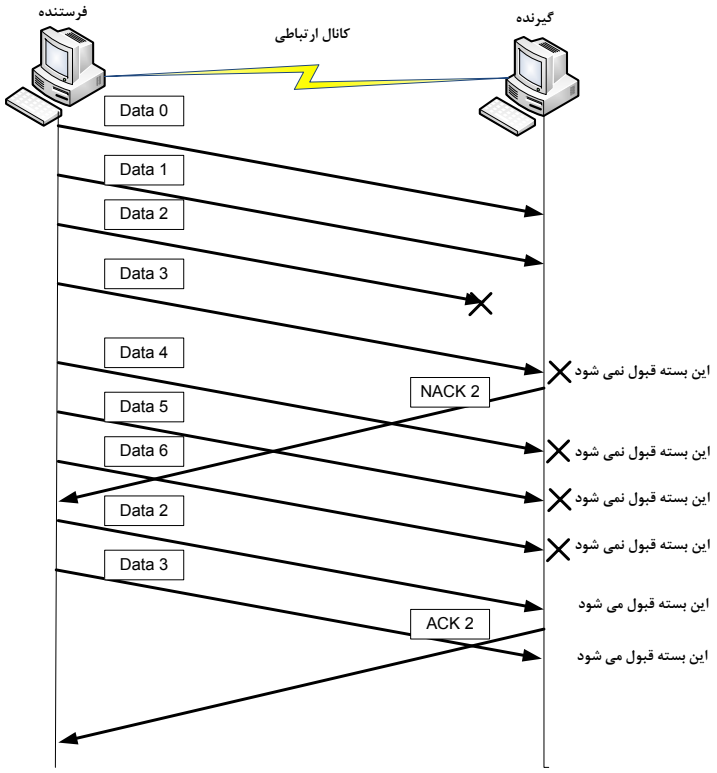
۲ در سمت فرستنده منقضی شود و یا فرستنده پیام NACK دریافت کند، دوباره اقدام به ارسال قاب شماره ۲ و قاب‌های بعد از آن می‌نماید.

۳-۲-۲-۲- روش تکرار انتخابی

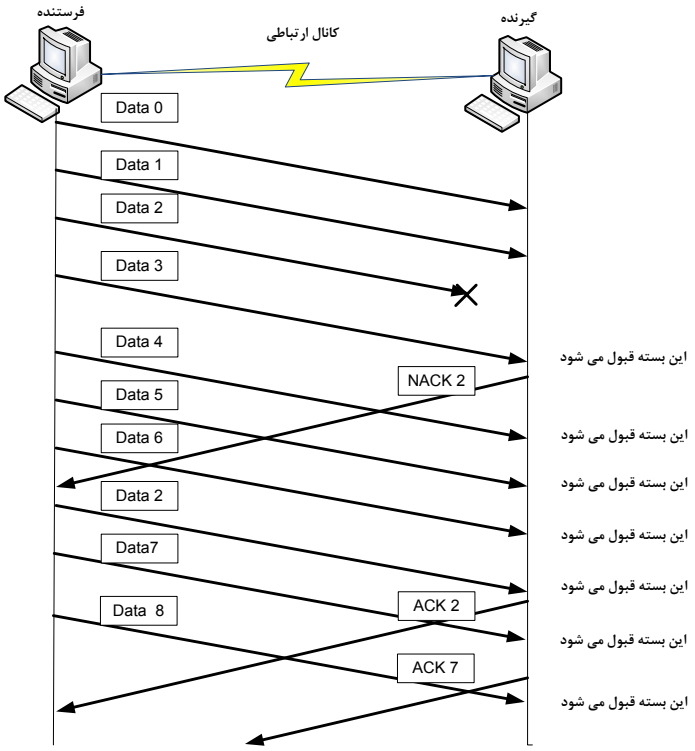
یکی دیگر از استراتژی‌های موجود در هنگام مواجه با خطا در روش پنجره لغزان، تکرار انتخابی قاب‌های معیوب می‌باشد. در این روش چنانچه قابی با خطا مواجه شود وگیرنده آن را دریافت نکند، گیرنده تمامی قاب‌های ورودی بعد از قاب معیوب را دریافت می‌کند و در بافر خود ذخیره می‌نماید و برای قاب معیوب پیام عدم تصدیق ارسال می‌نماید. با دریافت این قاب، فرستنده اقدام به ارسال مجدد قاب معیوب می‌کند و برخلاف روش بازگشت به عقب به اندازه N، نیازی به ارسال مجدد قاب‌های سالم ارسالی بعد از قاب معیوب نمی‌باشد. 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 می‌باشد.

با مقایسه دو روش تکرار انتخابی و بازگشت به عقب به اندازه N، به این نتیجه می‌رسیم که در روش تکرار انتخابی میزان استفاده از ظرفیت کانال زیاد می‌باشد و به عبارتی اتلاف پهنای باند کمتری وجود دارد، ولی در مقابل به فضای بافر زیادی در گیرنده نیاز می‌باشد. روش بازگشت به عقب به اندازه N، دارای میزان بهره‌وری 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



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 نسبتا خوبی بهره وری کانال،U ، تابعی از زمان T_{ix} برای ارسال یک قاب اطلاعاتی و تاخیر انتشاری خط T_p می باشد. بهرحال 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 $k \prec 1+2a$ باشد برابر است با :

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

درفرمول فوق، فرض براین 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. بهرحال ، 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 $K \prec 1+2a$ بدین صورت است :

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

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

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

درروش 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 $K \prec 1+2a$ ، تعداد بارهایی (K-1) که قاب باید ارسال مجدد شود ، $P_f(K-1)$ است. برای هر اتفاقی ، یک تاخیر 1+2a نیز رخ می‌هد. عبارت اصلاح شده برای $K \prec 1+2a$ 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 شبکه‌های محلی

همان‌طورکه درفصل۱ به آن اشاره شد، کانال‌های انتقال را می‌توان به دو نوع عمده تقسیم‌بندی نمود که عبارتند از: کانال‌های نقطه به نقطه و کانال‌های پخشی. شبکه‌های محلی عمدتاً از کانال‌های پخشی برای انتقال اطلاعات کاربران استفاده می‌نمایند. در کانال‌های پخشی، چندین کاربر به‌طور مشترک از یک کانال استفاده می‌کنند. مهمترین مسئله در کانال‌های پخشی، تخصیص مناسب کانال به کاربران و جلوگیری از تداخل قاب‌های ارسالی هر ایستگاه می‌باشد. در شبکه‌های محلی، لایه پیوند داده به دو زیرلایه مختلف تقسیم می‌شود 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 می‌پردازیم.

۳-۳-۱- زیرلایه کنترل دسترسی به محیط

همان‌طور که گفته شد، یکی از مسائل بسیار مهم در شبکه‌های محلی که از کانال‌های پخشی استفاده می‌نمایند، کنترل دسترسی به محیط می‌باشد. این کار توسط زیرلایه کنترل دسترسی به محیط انجام می‌شود. در طراحی مکانیسم‌های 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 :

---

[1] Medium Access Control

[2] Logical Link Control

- ***کنترل مرکزی***[1] : در این روش، یک کنترل‌کننده مرکزی در شبکه وجود دارد که برکل شبکه نظارت دارد. هر ایستگاه قبل از ارسال اطلاعات نیاز به اخذ مجوز از کنترل‌کننده مرکزی دارد. از آن‌جایی‌که تمام ایستگاه‌ها تا اجازه کنترل‌کنندهء مرکزی را دریافت نکنند، حق ارسال اطلاعات به شبکه را ندارند، بنابراین در این روش احتمال تداخل وجود ندارد. پروتکل‌های سوئیچینگ مداری، سرکشی[2] و TDMA[3] از روش کنترل مرکزی استفاده می‌کنند.
- ***کنترل توزیعی***[4] : در این روش هر ایستگاه برای ارسال اطلاعات نیاز به دریافت نشانه دارد. نشانه در بین ایستگاه‌ها توزیع می‌شود. هنگامی‌که ایستگاهی نشانه را دراختیار دارد، اطلاعات خود را ارسال می‌دارد و سپس نشانه را آزاد کرده و آن را به داخل شبکه می‌فرستد تا سایر ایستگاه‌های شبکه با دریافت آن اقدام به ارسال اطلاعات بنمایند. پروتکل‌هایی نظیر حلقه نشانه و گذرگاه نشانه از روش کنترل توزیعی استفاده می‌نمایند.
- **کنترل تصادفی**[5] : در این نوع کنترل، هر ایستگاهی در شبکه قادر به ارسال درهرلحظه دلخواه می‌باشد و نیازی به اخذ نشانه و یا دریافت اجازه از یک ایستگاه مرکزی در شبکه ندارد. پروتکل‌هایی نظیر ALOHA, CSMA/CD[6]، حلقه برش بندی شده[7] و درج ثبات[8] از این روش کنترل استفاده می‌نمایند.

در زیر به بررسی برخی از مهمترین پروتکل‌های ارسال در شبکه‌های پخشی می‌پردازیم.

۳-۳-۱-۱- 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. سیستم‌های اولیهALOHA برروی سیستم‌های پخش رادیویی زمینی پیاده‌سازی گردید ولی بر روی هر محیط دیگری نیز قابل پیاده‌سازی می‌باشد.

پروتکل ALOHA به دو نوع تقسیم می‌شود که عبارتند از:

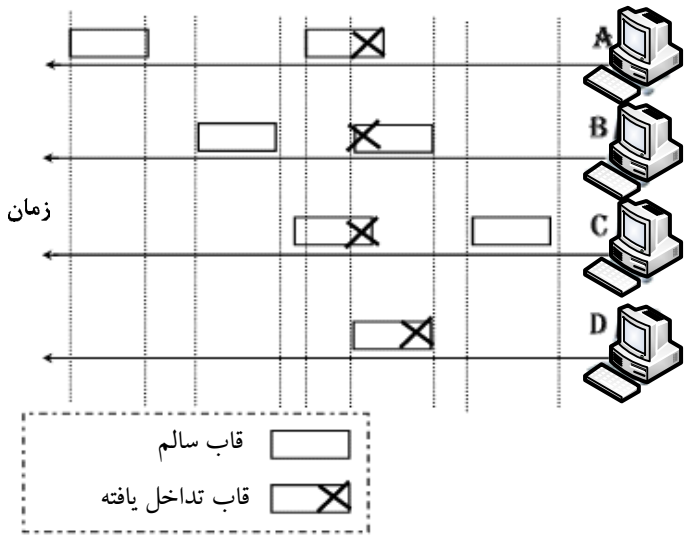
- ***پروتکل* ALOHA *خالص***: در این پروتکل کاربران شبکه اجازه دارند که در هر لحظه دلخواه اقدام به ارسال اطلاعات نمایند. البته مسلماً در این روش امکان تداخل داده‌های ارسالی وجود دارد. برای رفع مشکل تداخل، در این روش هرکاربر بعد از ارسال قاب، کانال را بررسی می‌نماید تا متوجه وقوع تداخل در کانال شود. چنانچه قاب ارسالی با تداخل مواجه شود، فرستنده با بررسی کانال متوجه وقوع تداخل می‌شود و سپس یک زمان تصادفی صبر می‌نماید و دوباره قاب را ارسال می‌دارد. طبیعی است برای کاهش احتمال تداخل دوبارهء قاب ارسالی، فرستنده باید یک زمان تصادفی منتظربماند و سپس دوباره قاب را ارسال دارد چون در غیر این‌صورت دوباره تداخل به‌وجود خواهد آمد. به سیستم‌هایی که چندین کاربر برای دسترسی به یک کانال مشترک با یکدیگر به رقابت می‌پردازند، سیستم‌های رقابتی[9] گفته می‌شود. در شکل (۳-۸) دیاگرام زمانی ارسال قاب‌ها در یک شبکه ALOHA خالص با ۴ کاربرنشان داده شده است. مطابق با این شکل هرگاه دو یا چند قاب همزمان کانال را اشغال نمایند، در این‌صورت تداخل روی خواهد داد و اطلاعات

---

[1] Centralized control
[2] Polling
[3] Time Division Multiple Access
[4] Distributed control
[5] Random control
[6] Carrier Sense Multiple Access/ Collision Detect
[7] Slotted ring
[8] Register insertion
[9] Contention system

از بین می‌رود. حتی اگر اولین بیت یک قاب با آخرین بیت قاب دیگری برروی هم قرار بگیرد، در این‌صورت باز هم تداخل روی داده است و باید دوباره دو قاب ارسال شود.

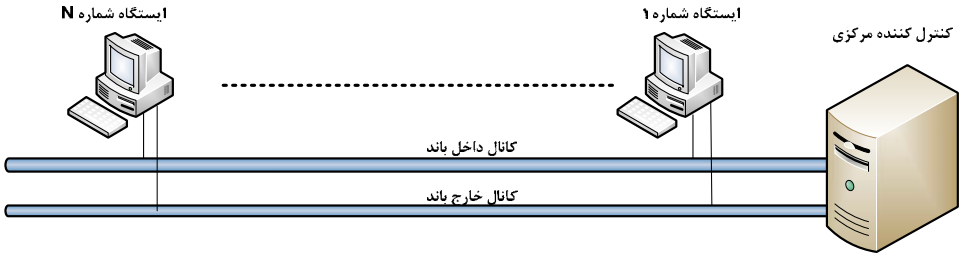
- ***پروتکل* ALOHA *برش بندی شده:*** در سال ۱۹۷۲ جهت افزایش ظرفیت و بهره‌وری بیشتر از کانال، توسط روبرتس، پروتکل ALOHA برش بندی شده ارائه گردید. در این پروتکل زمان به فواصل معین و ثابتی به نام برش تقسیم‌بندی می‌شود. برخلاف روش ALOHA خالص که هر ایستگاه در هر لحظه از زمان قادر به ارسال می‌باشد، در این روش ایستگاه‌ها فقط در لحظات خاصی که همان شروع هر برش می‌باشد، اجازه ارسال اطلاعات را دارند. با آنالیز ریاضی می‌توان 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 می‌باشد.



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

۳-۳-۱-۲- روش سرکشی

در این روش که از نوع کنترل مرکزی کانال می‌باشد، ایستگاه‌های شبکه از طریق دو کانال به یک ایستگاه مرکزی که درحکم کنترل‌کننده کانال می‌باشد متصل می‌شوند. در شکل (۳-۹) مثالی از یک سیستم سرکشی آورده شده است.



شکل (۳-۹): مثالی از پروتکل سرکشی

مطابق شکل فوق، بین ایستگاه‌ها و کنترل‌کننده مرکزی، دو کانال وجود دارد. این دو کانال عبارتند از : کانال خارج باند[1] و کانال داخل باند[2] . از کانال داخل باند برای تبادل اطلاعات و داده‌های ارسالی بین ایستگاه‌ها استفاده می‌شود. برای ارسال پیام‌های کنترلی و نشانه بین ایستگاه‌ها از کانال خارج باند استفاده می‌گردد. پروتکل سرکشی به دو نوع تقسیم می‌شود که به بررسی هریک می‌پردازیم.

- ***پروتکل سرکشی چرخشی[3] :*** در این روش کنترل کننده مرکزی به ترتیب به تک‌تک ایستگاه‌ها از طریق کانال خارج باند خود سرکشی می‌نماید. اگر ایستگاهی که به آن سرکشی شده است، اطلاعاتی برای ارسال داشت، آن را ازطریق کانال داخل باند ارسال می‌دارد و پایان ارسال اطلاعات خود را به کنترل کننده مرکزی گزارش می‌دهد. چنانچه ایستگاهی که به آن سرکشی شده است، داده‌هایی برای ارسال نداشته باشد، کنترل‌کننده مرکزی به‌دنبال ایستگاه بعدی می‌رود. سرکشی به ایستگاه‌ها در این روش منظم و چرخشی می‌باشد. روش کار این پروتکل به این صورت است که در ابتدا ایستگاه مرکزی با ارسال پیام خاصی به اولین ایستگاه از آن می‌خواهد که داده‌های خود را ارسال دارد. ایستگاهی که به آن سرکشی شده است، چنانچه داده‌ای برای ارسال داشته باشد، آنها را از طریق کانال داخل باند ارسال می‌کند و در پایان دوباره نشانه را به کنترل‌کننده مرکزی ارسال می‌دارد. کنترل‌کننده مرکزی با دریافت نشانه، آن را برای ایستگاه دوم ارسال می‌دارد و ایستگاه دوم نیز در پایان ارسال داده‌های خود دوباره نشانه را به کنترل کننده مرکزی ارسال می‌کند. این کار به‌طور چرخشی ادامه دارد و به تمام ایستگاه‌ها از طریق کانال خارج باند سرکشی می‌شود.
- ***پروتکل سرکشی هاب[4]:*** یکی از معایب روش سرکشی چرخشی، آن است که در پایان ارسال هر ایستگاه نشانه دوباره به ایستگاه مرکزی ارسال می‌شود و از آن طریق در اختیار ایستگاه بعدی قرارمی‌گیرد. این مسئله باعث افزایش تاخیر بین ارسال دو ایستگاه متوالی می‌گردد، که این امر نیز باعث کاهش میزان استفاده از کانال و اتلاف ظرفیت کانال می‌شود. برای رفع این مشکل از روش سرکشی هاب استفاده می‌شود. در این روش ایستگاه مرکزی ابتدا نشانه را به بالاترین ایستگاه (ایستگاه شماره N) تحویل می‌دهد. چنانچه ایستگاه شماره N اطلاعاتی برای ارسال داشت، اطلاعات خود را ارسال می‌دارد و در پایان ارسال، نشانه را به ایستگاه مجاور خود (ایستگاه N-1) ارسال می‌کند. این روند آن‌قدر ادامه پیدا می‌کند 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 اختیارگرفتن کانال کاهش می‌یابد و میزان بهره‌وری از کانال افزایش می یابد.

۳-۳-۱-۳- پروتکل تشخیص سیگنال حامل با دسترسی چندگانه (CSMA[5])

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 می‌شود. یکی از متداولترین پروتکل‌های تشخیص سیگنال حامل، پروتکلCSMA است. پروتکل‌های CSMA خود به چندین نوع تقسیم می‌شوند که عبارتند از: پروتکل CSMA صددرصد مصرّ[6] و پروتکل CSMA غیرمصرّ[7].

---

[1] Outband line
[2] Inband line
[3] Roll call polling
[4] Hub polling
[5] Carrier Sense Multiple Access
[6] 1-persistent CSMA
[7] Nonpersistent CSMA

در پروتکل CSMA صددرصد مصّر، هنگامی‌که ایستگاهی اطلاعاتی برای ارسال دارد، ابتدا کانال را بررسی می‌نماید تا مطمئن شود کانال مشغول است یا خیر؟ چنانچه کانال مشغول باشد، تا لحظه آزادشدن کانال، صبر می‌نماید و بعد از آن اقدام به ارسال یک قاب می‌کند. اگر قاب ارسالی با تداخل مواجه شود، در این‌صورت ایستگاه مدت زمانی تصادفی صبر می‌نماید و دوباره اقدام به ارسال قاب می‌کند. از آنجایی‌که در این پروتکل هرگاه ایستگاهی کانال را خالی ببیند با احتمال ۱ اقدام به ارسال قاب می‌نماید، به آن پروتکل CSMA صددرصد مصّر گفته می‌شود.

در کارآیی این پروتکل، تأخیر انتشار تاثیر مهمی دارد. چنانچه دو ایستگاه همزمان اقدام به بررسی کانال بنمایند، در این صورت هر دو متوجه خالی‌بودن کانال می‌شوند. چنانچه یکی ازآنها اقدام به ارسال اطلاعات نماید، این احتمال وجود دارد که قبل از آن‌که 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 می‌شوند و از بین می‌روند. هرچه تأخیر انتشار بیشتر باشد (فاصله ایستگاه‌ها ازهمدیگر زیاد باشد)، در این‌صورت احتمال وقوع تداخل نیز زیاد می‌شود و کارآیی سیستم کاهش می‌یابد.

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 می‌نماید و چنانچه ایستگاه دیگری در حال ارسال نباشد، شروع به ارسال قاب می‌نماید. ولی در صورتی‌که کانال مشغول باشد، آنگاه ایستگاه به‌طور پیوسته وضعیت کانال را بررسی نمی‌نماید تا به محض این‌که کانال آزاد شد اقدام به ارسال قاب کند بلکه در صورتی‌که کانال مشغول باشد، یک زمان تصادفی صبر نموده و بعد دوباره وضعیت کانال را بررسی می‌نماید. ثابت می‌شود که کارآیی این روش نسبت به روش CSMA مصّر به مراتب بهتر است.

نوع دیگری از پروتکل CSMA با نام P CSMA درصد مصّر[1]نیز وجود دارد. از این پروتکل در کانال‌های برش بندی‌شده استفاده می‌شود. روش کار آن به این صورت است که ایستگاهی که می‌خواهداطلاعاتی ارسال دارد، ابتدا کانال را بررسی‌می‌کند و بعد از آن چنانچه متوجه خالی‌بودن کانال گردید، با احتمال P ارسال می‌دارد و با احتمال 1-P ارسال خود را به برش بعدی موکول می نماید. اگر برش بعدی نیز آزاد باشد با احتمال P ارسال می‌کند و با احتمال 1-P ارسال خود را به برش بعدی می‌اندازد. این فرآیند تا زمانی‌که قاب ارسال نشود و یا تا زمانی‌که ایستگاه دیگری شروع به ارسال ننماید، ادامه پیدا می‌کند. با کاهش P ، کارآیی سیستم افزایش می‌یابد و احتمال تداخل کم می‌شود.

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

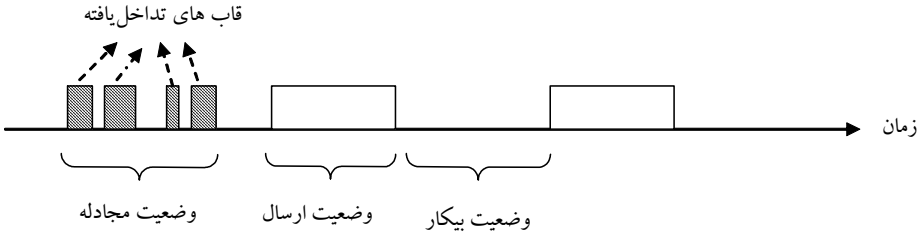
از آن‌جایی‌که در پروتکل‌های CSMA، هیچ ایستگاهی وقتی که کانال مشغول است ارسال نمی‌نماید، بنابراین میزان کارآیی آن نسبت به روش ALOHA به مراتب بیشتر می‌باشد. در پروتکلCSMA/CD، هرگاه دو ایستگاه همزمان شروع به بررسی وضعیت کانال بنمایند، متوجه آزادبودن کانال می‌شوند وهر دو با هم اقدام به ارسال قاب می‌کنند. مسلماً قاب‌های ارسالی با تداخل مواجه می‌شود و از بین می‌روند. چنانچه قاب ارسالی در اولین بیت‌های آن و یا در آخرین بیت‌های 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 می‌نماید. قطع سریع ارسال قاب‌های آسیب دیده باعث صرفه‌جویی درزمان و پهنای باند می‌گردد. در پروتکل CSMA/CD هر ایستگاه مطابق با شکل (۳-۱۰) در یکی از سه وضعیت زیر قرار دارد:

---

[1] P-persistent CSMA

- ***وضعیت ارسال :*** در این وضعیت بدون آن‌که تداخلی گزارش داده شود، ایستگاه در حال ارسال قاب خود می‌باشد و در نهایت با موفقیت این کار را به پایان می‌رساند.
- ***وضعیت مجادله :*** در این وضعیت چند ایستگاه درحال رقابت برای دسترسی به کانال می‌باشند. قاب ارسالی ایستگاه‌ها با یکدیگر تداخل می‌نماید و ایستگاه‌ها یک مدت زمان تصادفی صبرمی‌کنند و دوباره اقدام به ارسال قاب می‌نمایند. این کار آن‌قدر ادامه پیدا می‌کند که بالاخره ایستگاه‌ها موفق به ارسال صحیح قاب شوند.
- ***وضعیت بی‌کار:*** در این وضعیت ایستگاه‌ها قابی برای ارسال ندارند و کانال بلا استفاده و بی‌کار می‌ماند.

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 رسیده‌است.



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

۳-۴- استانداردهای IEEE برای شبکه‌های محلی

یکی ازمراجع معتبر استانداردگذاری در زمینه‌های مرتبط با برق وکامپیوتر، انجمن IEEE می‌باشد. گروه کاری ۸۰۲ وابسته به انجمن IEEE در زمینه استانداردگذاری شبکه‌های محلی فعال است. توسط این گروه استانداردهای متعددی در زمینه شبکه‌های کامپیوترای 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)

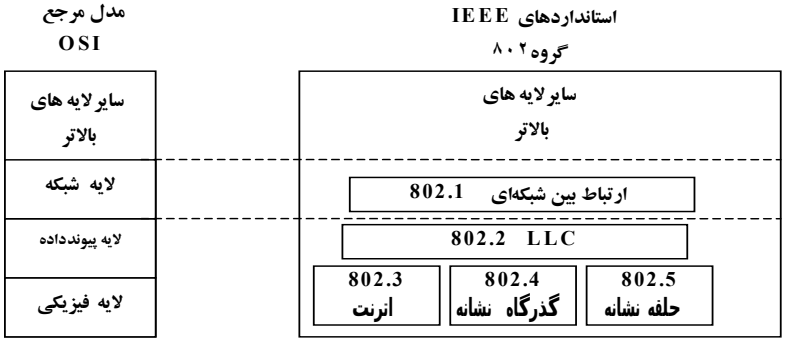
در شکل (۳-۱۱) مدل لایه‌ای شبکه‌های محلی IEEE 802 نشان داده شده است. در زیر به بررسی هر یک از شبکه‌های فوق می‌پردازیم.

۳-۴-۱- شبکه‌های محلی اترنت

شبکه‌های محلی اترنت از روش CSMA/CD صددرصد مصّر استفاده می‌نمایند. در این شبکه‌ها هنگامی‌که ایستگاه قابی برای ارسال دارد، ابتدا وضعیت کانال را بررسی می‌نماید و چنانچه کانال مشغول باشد تا آزادشدن کانال صبر می‌کند ودرصورتی‌که کانال آزاد شد اقدام به ارسال قاب می‌نماید. ایستگاه فرستنده، همزمان با ارسال قاب وقوع تداخل در قاب ارسالی را نیز بررسی می‌کند و چنانچه متوجه وقوع تداخل در قاب ارسالی شود، ارسال قاب را قطع می نماید و یک زمان تصادفی صبر می‌کند و دوباره اقدام به ارسال قاب می‌نماید.

پایه استاندارد اترنت، سیستم ALOHA آقای آبرامسون که در بخش‌های قبلی به بررسی آن پرداختیم می‌باشد که به مرور زمان به آن قابلیت تشخیص حامل نیزاضافه شده‌است.

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



شکل (۳-۱۱) : مدل لایه‌ای شبکه‌های 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 شبکه‌ها از کابل به‌عنوان محیط هادی برای انتقال امواج الکترومغناطیسی استفاده می‌شود. در شبکه‌های اترنت دو نوع کابل موجود است که با نام‌های کابل نرم وکابل سخت شناخته می‌شوند. کابل‌های اترنت نرم بسیار نازک و انعطاف‌پذیر هستند و نسبت به کابل سخت ارزانتر نیز می‌باشند. از این نوع کابل‌ها فقط می‌توان در فواصل کوتاه استفاده نمود. امکان اتصال این دو نوع کابل نیز به یکدیگر وجود دارد.

یکی از مشکلات اساسی در شبکه‌های اترنت، وقوع خرابی و قطعی در کابل می‌باشد. چنانچه کابل شبکه دچار قطعی شود و یا یکی از اتصال‌دهنده‌های آن از محل خود خارج شود، سیگنال‌های ارسالی منعکس می‌شود و شبکه قادر به ادامه فعالیت خود نمی‌باشد. یکی از روش‌های متداول تشخیص قطعی در کابل شبکه آن است که یک پالس الکتریکی در کابل ارسال گردد. هنگامی‌که پالس ارسالی به مانعی برخورد نماید، منعکس می‌شود. با اندازه‌گیری دقیق زمان ارسال پالس و زمان دریافت انعکاس آن، می‌توان دقیقاً محل انعکاس را تعیین نمود و بدین ترتیب متوجه محل قطعی کابل شد. به این روش، انعکاس سنجی زمانی[۱] گفته می‌شود.

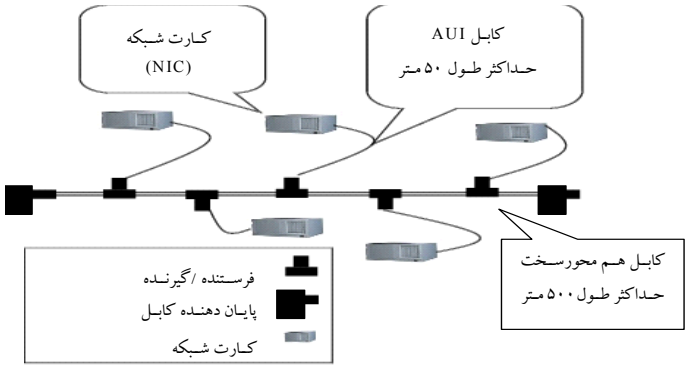
درشکل (۳-۱۲) نحوه کابل‌کشی شبکه‌های اترنت با استفاده از کابل‌های سخت RG-8 نشان داده شده است. همان‌طور که در این شکل نیز دیده می‌شود، هر کامپیوتر شبکه از طریق یک کابل که حداکثر طول آن ۵۰ متر است از طریق وسیله‌ای به نام فرستنده/گیرنده[2] به کابل اصلی شبکه متصل است. درفرستنده/گیرنده تجهیزات الکترونیکی وجود دارد که به‌وسیله آن امکان تشخیص وضعیت سیگنال حامل در کانال و کشف تداخل فراهم می‌آید. هنگامی‌که فرستنده/گیرنده متوجه وقوع تداخل در کابل شبکه می‌شود، سیگنال مشخصی را روی کانال قرار می‌دهد و بدین‌وسیله به همه فرستنده/گیرنده های دیگر از وقوع تداخل اطلاع می‌دهد. کابلی که ایستگاه را به فرستنده/گیرنده متصل می‌نماید حاوی پنج زوج سیم به هم تابیده شده روکش‌دار است. دو زوج سیم فوق برای ورود و خروج داده‌ها به کار می‌روند و دو زوج دیگر به

---

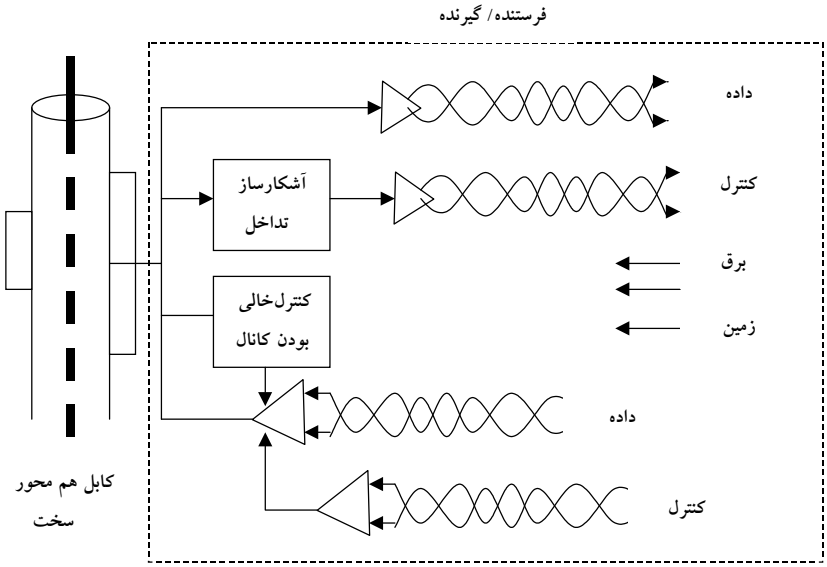
[۱] Time domain reflectometry

[۲] Transceiver(Transceiver مخفف کلمات Transmitter و Receiver می‌باشد)

ورود و خروج سیگنال‌های کنترلی اختصاص دارند. از پنجمین زوج سیم استفاده زیادی نمی‌شود و می‌توان 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. درشکل (۳-۱۳) اجزای داخلی فرستنده/گیرنده نشان داده شده است.



شکل (۳-۱۲) : نمونه‌ای 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(NIC[1]) نام دارد، امکان اتصال به شبکه را دارد. کارت شبکه حاوی یک پردازنده الکترونیکی است که به‌وسیله آن عملیات ارسال ودریافت قاب‌ها انجام می‌شود. همچنین عملیاتی نظیر: تشکیل و ایجاد قاب‌های ارسالی و محاسبه مجموع مقابله‌ای برای قاب‌های ارسالی و دریافتی توسط پردازنده انجام می‌شود. برخی از کارت‌های شبکه دارای قابلیت‌های اضافی دیگر نظیر اتصال به کامپیوتر از طریق DMA[۲] و

[۱] Network Interface Card
[۲] Direce Memory Access

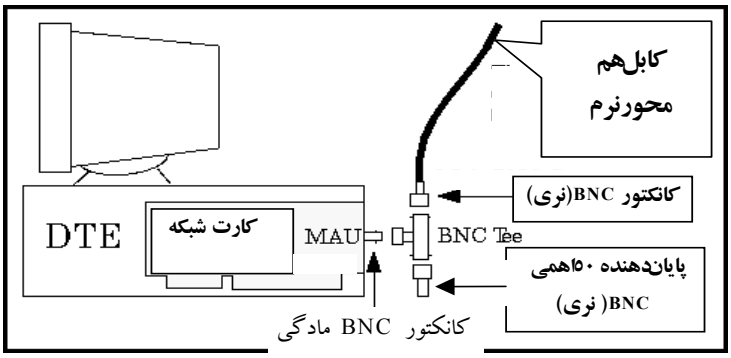
انجام عملیات مدیریت شبکه می‌باشند. هر کارت شبکه از طریق یک واسط اتصال(AUI[1])که یک کانکتور DB-15 مـی‌باشـد، به کابل اترنت سخت متصل می‌شود.

حداکثر طول مجاز کابل اترنت سخت برابر با ۵۰۰ متر می‌باشد. چنانچـه بخـواهیم شـبکه محلـی خـود را بـه فواصـل طولانی‌تری گسترش دهیم، می‌توان چندین کابل شبکه را از طریق تکرارکننده[2] به یکدیگر متصل نمـود. تکرارکننـده‌هـا در لایه فیزیکی عمل می‌نمایند و وظیفه آنها دریافت و تقویت و ارسال دوبارهء قاب‌های دریافتی از یک طـرف بـه طـرف مقابـل می‌باشد. با استفاده از تکرارکننده‌ها می‌توان طول فیزیکی یک شبکه اترنت را افزایش داد، ولی باید توجه نمود کـه بیـشترین فاصله بین فرستنده و گیرنده در یک شبکه اترنت نباید از ۲/۵ کیلومتر بیشتر باشـد، بـدین ترتیـب در یـک شـبکه حـداکثر می‌توان از ۴ تکرارکننده استفاده نمود.

به شبکه‌های اترنت کابل سخت، 10Base5 نیز اطلاق می‌شود که در آن 10 نشان‌دهنده سرعت ارسـال ده مگابیـت بـر ثانیه است و 5 بیانگر حداکثر طول ۵۰۰ متری کابل شبکه می‌باشد. قطرکابل درشبکه‌های 10Base5 حدود نیم اینچ است.

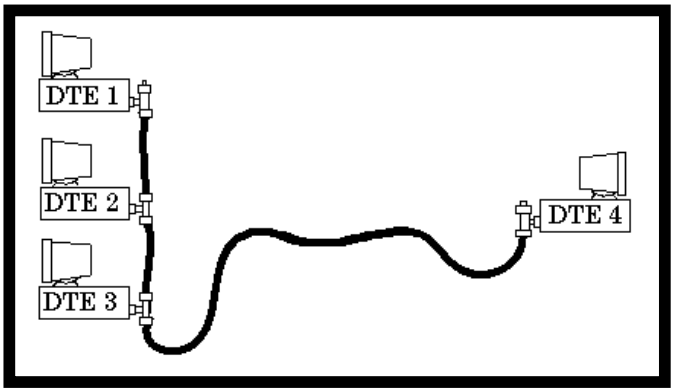
علاوه بر کابل‌های سخت برای شبکه‌های اترنت، می‌توان از کابل‌های نرم نیز بـرای کابـل‌کـشی شـبکه اسـتفاده نمـود. طبیعی است که این نوع کابل‌های شبکه، دارای انعطاف‌پذیری بالا و قیمت پایین‌تری می‌باشند. قطر کابل های نرم حدود ۲۵ صدم اینچ می‌باشد. همان‌طور که در شکل (۳-۱۴) نشان داده شده است، در شبکه‌های اترنت نرم هر کارت شـبکه مـستقیماً 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 مترمی‌باشد و بنابراین تعداد کاربران آن نسبت به شـبکه کابـل سخت کمتر است.

با توجه به ساختار شبکه‌های اترنت نرم، دیده می‌شود که در این نوع شبکه‌ها، فرستنده/گیرنده حـذف شـده اسـت. از کابل‌های هم‌محور RG-58 در شبکه‌های اترنت نرم استفاده می‌شود. هر کارت شبکه از طریق یک کانکتور BNC-T بـه کابـل شبکه متصل می‌گردد. به شبکه‌های اترنت نرم، شبکه‌های 10Base2 نیز گفته می‌شود. این نوع شبکه‌ها نیز مشابه شبکه‌هـای 10Base5 که از کابل‌های سخت استفاده می‌کنند دارای سرعت ۱۰ مگابیت بر ثانیه می‌باشند. برای رفع مـشکل محـدودیت طول کابل در شبکه‌های اترنت نرم، از تکرار کننده استفاده می‌گردد. با استفاده از تکرار کننده امکـان افـزایش طـول شـبکه اترنت نرم وجود دارد. در شکل (۳-۱۶) مثالی از گسترش یک شبکه اترنت با استفاده از تکرار کننده آورده شده است.

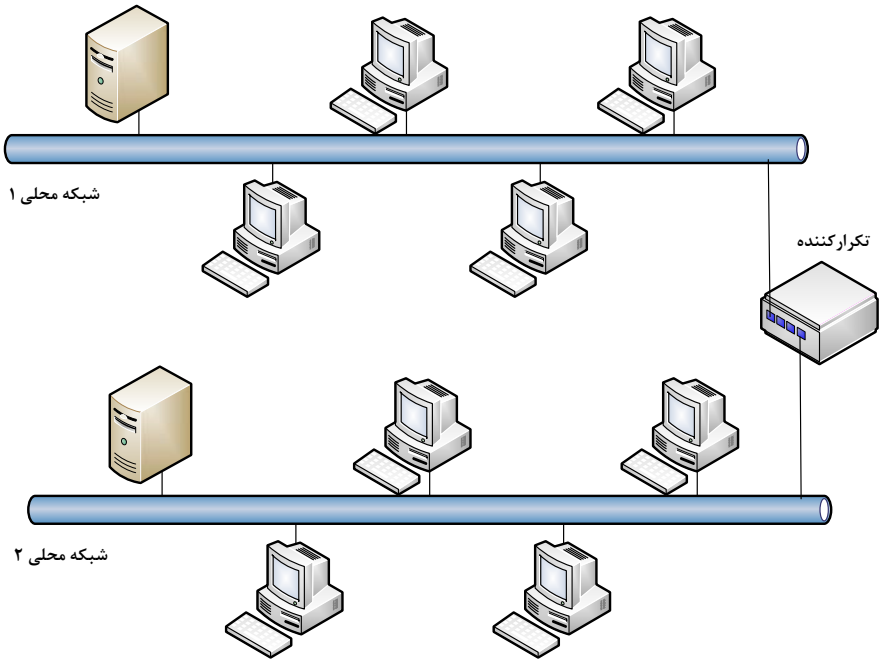


شکل (۳-۱۴): اجزای شبکه اترنت نرم

[1] Attachment Unit Interface
[2] Repeater

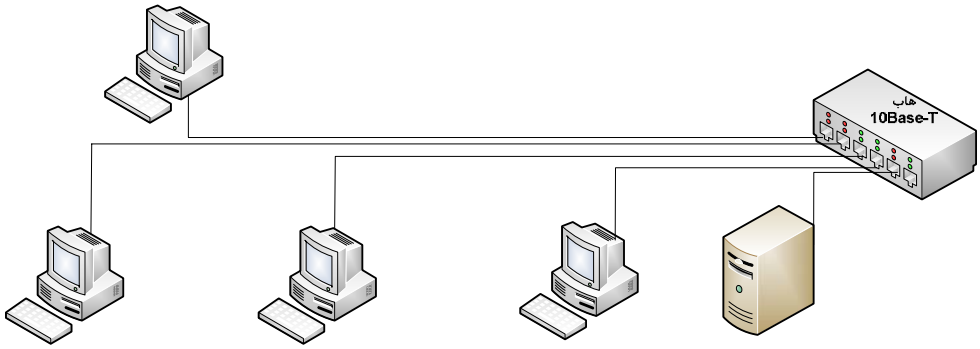


شکل (۳-۱۵): مثالی از کابل کشی شبکه اترنت نرم



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

امروزه شبکه‌های 10Base5 و 10Base2 به تدریج از رده خارج شده‌اند و شبکه‌های اترنت ستاره‌ای (10Base-T,100Base-T) جایگزین آنها گردیده‌اند. در این نوع شبکه‌ها از زوج سیم‌های UTP استفاده می‌شود. سرعت‌های متداول این نوع شبکه‌ها ۱۰ مگابیت بر ثانیه (10Base-T) و ۱۰۰ مگابیت بر ثانیه (100Base-T) می‌باشد. تمام ایستگاه‌های شبکه از طریق یک کابل RJ-45 (که شامل ۴ زوج سیم UTP است) به یک ایستگاه مرکزی که هاب نام دارد متصل می‌شوند. چنانچه یکی از ایستگاه‌های متصل‌شده به هاب قابی را ارسال دارد، در این صورت هاب آن را دریافت می‌کند و آن را به تمام درگاه‌های خروجی خود ارسال می‌دارد. بدین ترتیب قاب ارسالی هر ایستگاه توسط هاب به تمام ایستگاه‌های دیگر نیز ارسال می‌شود. در شکل(۳-۱۷)، نمونه‌ای از یک شبکه ستاره‌ای با استفاده از هاب نشان داده شده است.

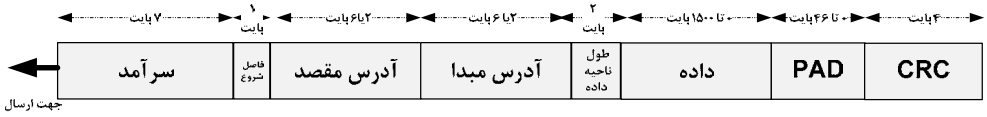


شکل(۳-۱۷) :یک شبکه محلی ستاره‌ای از نوع 10Base-T

در شبکه‌های ستاره‌ای حداکثر طول کابل RJ-45 که ایستگاه‌های شبکه را به هاب متصل می‌نماید، برابر با ۱۰۰ متر می‌باشد. یکی از مهمترین مزایای شبکه‌های محلی ستاره‌ای این است که چنانچه خرابی در یکی از کابل‌های RJ-45 رخ دهد، فقط همان ایستگاه از کار می‌افتد و سایر ایستگاه‌های شبکه به کار خود ادامه می‌دهند.

۳-۴-۱-۱- ساختار زیرلایه MAC در اترنت

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



شکل(۳-۱۸) : ساختار قاب‌های MAC **استاندارد اترنت**

همان‌طورکه در این شکل دیده می‌شود، فیلدهای زیر در ساختار قاب های اترنت وجود دارند.

- ***فیلد سرآمد***[1]: این فیلد ۷ بایتی حاوی الگوی بیتی ۱۰۱۰۱۰۱۰ می‌باشد و برای همزمان‌سازی ساعت فرستنده با ساعت گیرنده مورد استفاده قرار می‌گیرد.
- ***فیلد فاصل شروع*** (**SFD**[2]) : این فیلد که حاوی بایت ۱۰۱۰۱۰۱۱است نشان‌دهنده شروع قاب می‌باشد.
- ***فیلد آدرس‌های مقصد و مبدأ :*** توسط این فیلدهای ۲ یا ۶ بایتی آدرس‌های فرستنده و گیرنده قاب مشخص می‌شود. معمولاً استاندارد اترنت با سرعت ۱۰ مگابیت بر ثانیه از آدرس‌های ۶ بایتی استفاده می‌نماید. توسط بالاترین بیت در فیلد آدرس گیرنده، نوع آدرس مشخص می‌گردد. چنانچه آدرس از نوع گروهی باشد این بیت حاوی ۱ است و برای آدرس‌های معمولی بیت فوق صفر می‌باشد. به‌وسیله مکانیسم آدرس‌دهی گروهی این امکان وجود دارد که به چندین ایستگاه که در یک گروه قرار گرفته‌اند، قاب‌هایی را ارسال نمود. چنانچه تمام بیت‌های فیلد آدرس مقصد حاوی بیت ۱ باشد، در این‌صورت تمامی ایستگاه‌های شبکه، قاب ارسالی را دریافت می‌نمایند که به این حالت، آدرس‌دهی داده‌پراکنی گفته می‌شود. از دومین بیت بالا(بیت شماره ۴۶) برای تفکیک آدرس‌های

[1] Preamble
[2] Start Field Delimeter

محلی از آدرس‌های جهانی استفاده می‌شود. آدرس‌های محلی توسط مدیران شبکه تعیین می‌شود و در خارج از شبکه اهمیت و معنایی ندارند. ولی آدرس‌های جهانی در دنیا واحد بوده و از سوی سازمان IEEE تعیین می‌شوند. با ۴۶ بیت باقیمانده از فیلد آدرس، می‌توان تعداد ۷۰/۰۰۰/۰۰۰/۰۰۰/۰۰۰ آدرس جهانی تولید نمود که هر ایستگاه در جهان به‌طور انحصاری قابل آدرس‌دهی یکتا می‌باشد.

- ***فیلد طول ناحیه داده :*** از این فیلد برای تعیین دقیق طول ناحیه داده که می‌تواند صفر تا ۱۵۰۰ بایت باشد، استفاده می‌شود.
- ***فیلد* PAD*:*** برای آن‌که بتوان قاب‌های سالم را از قاب‌های آشغال که از تداخل قاب‌های دیگر به‌وجود می‌آیند، جداسازی نمود، بایدحداقل طول قاب‌های ارسالی ۶۴ بایت باشد. چنانچه طول قاب‌های ارسالی از۴۶ بایت کمتر باشد به تعداد بایت کمتر از ۴۶ در ناحیه PAD بایت صفر اضافه می‌گردد تا طول قاب به حداقل مقدار خود برسد.
- ***فیلد داده:*** این فیلد متغیر که دارای طول ۰تا ۱۵۰۰ بایت می‌باشد، حاوی اطلاعات لایه بالاتر است که باید در قالب قاب‌هایی به درون شبکه ارسال شود.
- ***فیلد* CRC*:*** این فیلد که دارای ۴ بایت طول می‌باشد، برای اطمینان از صحت قاب دریافتی به کار می‌رود. چنانچه ضمن ارسال قاب در شبکه برخی از بایت‌های فیلد داده از بین بروند، در این‌صورت گیرنده با بررسی فیلد CRC دریافتی با CRC ای که خود بدست می‌آورد، متوجه وقوع خطا در قاب دریافتی می‌شود. از کدهای CRC 32 برای این فیلد استفاده می‌شود.

همان‌طور که قبلاً نیز اشاره شد، بعد از هر بار تداخل در قاب ارسالی، ایستگاه فرستنده مدت زمان تصادفی صبرمی نماید و دوباره قاب را ارسال می‌دارد. الگوریتم کار به این صورت است که در اولین تداخل، ایستگاه به‌طور تصادفی یکی از اعداد 0,T را انتخاب می‌کند و به آن اندازه صبر می نماید و سپس دوباره اقدام به ارسال قاب می‌کند. چنانچه برای بار دوم تداخلی رخ دهد، ایستگاه فرستنده یکی از اعداد 0,T,2T,3T را انتخاب می‌کند و به آن اندازه صبر می‌نماید و سپس اقدام به ارسال مجدد قاب می‌کند. به‌طور کلی بعد از i بارتداخل، فرستنده یکی از زمان‌های $0,T,2T,...,(2^i-1)T$ را انتخاب نموده و به آن اندازه صبر می‌کند و دوباره اقدام به ارسال قاب می‌نماید. البته بعد از رسیدن به ۱۰ تداخل، دیگر دامنه اعداد تصادفی افزایش نمی‌یابد و یکی از زمان‌های بین 0,T,2T,...,1023T انتخاب می‌شود. پس از ۱۶ بار تداخل فرستنده تسلیم می‌شود و دیگر از ارسال قاب صرفنظر می‌نماید. به این الگوریتم، الگوریتم عقب‌گرد توانی دودویی[1] می‌گویند. طبیعی است که با افزایش محدوده اعداد تصادفی که ایستگاه باید به اندازه آن صبر نماید، احتمال بروز تداخل کاهش می‌یابد. متغیر زمانی T نشان‌دهنده حداکثر تأخیر انتشاردرکانال می‌باشد.

۳-۴-۱-۲ - اترنت سریع[2]

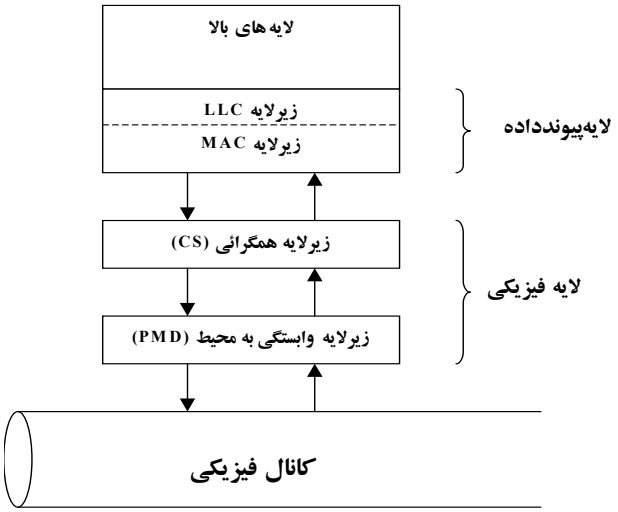
با پیشرفت خدمات جدید در شبکه‌های کامپیوترای، سرعت شبکه‌های اترنت معمولی برای تبادل اطلاعات کافی به نظر نمی رسد. تعدادی از شرکت‌های کامپیوترای معتبر با ارائه توافق نامه‌ای و تصویب IEEE در سال ۱۹۹۵ استاندارد اترنت سریع (IEEE 802.3U) را تصویب کردند. در این استاندارد که توسعه یافته اترنت معمولی است، سرعت مبادلهء داده ها،۱۰۰ مگابیت برثانیه می‌باشد. درشکل (۳-۱۹) ساختار لایه ای پروتکل اترنت سریع نشان داده شده است. باتوجه به این شکل ، در

---

[1] Binary exponential backoff

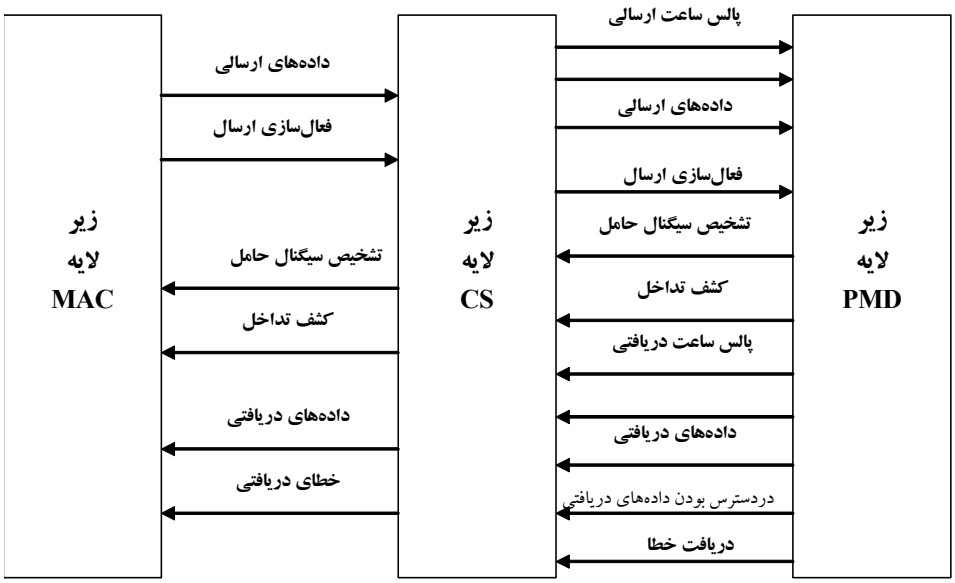
[2] Fast Ethernet

شبکه‌های اترنت سریع، لایه فیزیکی به دو زیرلایه به نام های زیرلایه همگرائی (CS[1]) و زیرلایه وابسته به محیط فیزیکی (PMD[2]) تجزیه می‌شود.



شکل (۳-۱۹): ساختار لایه ای اترنت سریع

زیرلایه همگرایی موظف به فراهم آوری واسط لازم بین زیرلایه MAC و زیرلایه PMD می‌باشد. بااستفاده از این زیرلایه، می‌توان با شفافیت لازم در MAC برای استفاده از کانال‌های مختلف درلایه فیزیکی دستیابی داشت. درشکل (۳-۲۰)، سیگنال‌های موجود درواسط زیرلایه CS با زیرلایه MAC و همچنین زیرلایه PMD با زیرلایه CS نشان داده شده است.

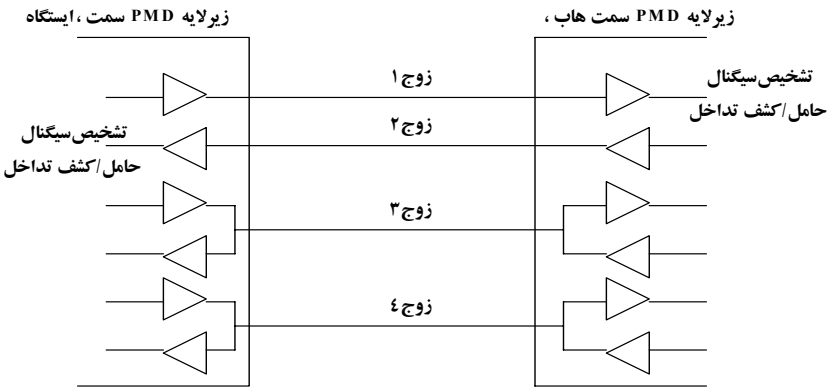


شکل(۳-۲۰): سیگنال‌های موجود درواسط زیرلایه CS با زیرلایه MAC و زیرلایه PMD با زیرلایه CS

[1] Convergence Sublayer
[2] Physical Medium-dependent Sublayer

درشبکه‌های 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 می‌شود. استاندارد اترنت سریع دارای انواع مختلفی می‌باشد که عبارتند از:

- **100Base-T4** : در این نوع شبکه از ۴ زوج سیم UTP بین هر ایستگاه و هاب استفاده می‌شود. از زوج سیم های شماره ۳ و ۴ برای ارسال و دریافت داده ها استفاده می‌گردد. درهریک از زوج سیمهای به‌کاررفته، ارسال به‌صورت یک‌طرفه انجام می‌شود. 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 می‌شود. درشکل (۳-۲۱)، زوج سیم‌های 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 می‌گردد.
- **100Base-FX** : در این استاندارد از دو رشته فیبر نوری برای اتصال هر ایستگاه به هاب استفاده می‌شود. استاندارد 100Base-FX ا ز 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 می‌شود.



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

۳-۴-۱-۳- گیگابیت اترنت

با پیشرفت فن‌آوری 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 می‌نماید می‌توان 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 سریع‌تر از اترنت پایه است، می‌باشد. این استاندارد با اترنت سریع و اترنت پایه سازگاری دارد، و می‌توان از آن به‌عنوان شبکه شالوده دراتصال شبکه‌های محلی استفاده نمود.

توسط سازمان IEEE استاندارد IEEE 802.3Z برای شبکه‌های گیگابیت اترنت تصویب گردید. گیگابیت اترنت برای اتصال سوئیچ‌های شبکه‌های اترنت پایه و سریع به یکدیگر و برقراری یک شبکه شالوده سریع به کار می رود. ساختار قاب‌های این استاندارد مشابه اترنت پایه است و از پروتکل CSMA/CD استفاده می‌نماید. استاندارد گیگابیت اترنت از عملکرد یک‌طرفه ودوطرفه پشتیبانی می‌کند. در این استاندارد از فیبرنوری و زوج سیم UTP برای مبادله اطلاعات استفاده می‌گردد. زیر لایه سری کننده/غیرسری کننده که در مدل لایه ای گیگابیت اترنت دیده می‌شود، وظیفه تبدیل اطلاعات موازی لایه بالاتر به اطلاعات سری و بالعکس را به عهده دارد.

در شبکه‌های اترنت گیگابیت از روش کد گذاریB8/B10 استفاده می‌شود. در این روش کد گذاری که برای ارسال اطلاعات در محیط فیبر نوری به‌کار می رود اطلاعات از۸ بیت به ۱۰ بیت تبدیل شده و ارسال می‌گردند.

همان‌طور که گفته شد استاندارد گیگابیت اترنت هر دو عملکرد یک‌طرفه و دو طرفه را پشتیبانی می نماید. در حالت یک‌طرفه از پروتکل CSMA/CD و درحالت دو طرفه از پروتکل IEEE 802.3X استفاده می‌شود. در گیگابیت اترنت حداقل طول قاب های ارسالی۵۱۲ بایت می‌باشد. برخی از پروتکل های فیزیکی گیگابیت اترنت عبارتند از1000Base-LX، Base-SX 1000 ، 1000Base-CX و1000Base-T. 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	فیبرنوری تک مودیا چند مود	۲ مترتا ۵ کیلومتر	
	1000 Base-CX	سیم مسی	۲۵ متر	
IEEE 802.3ab	1000 Base-T	کاتگوری 5 و5E سیم UTP	۱۰۰ متر	۱۹۹۹

از استاندارد گیگابیت اترنت جهت افزایش سرعت اتصال به خدمات دهنده های شبکه، اتصال سوئیچ‌ها به یکدیگرو اتصال سوئیچ‌ها به خدمات دهنده‌ها استفاده می‌شود. همچنین با استفاده از گیگابیت اترنت می‌توان برنامه های کاربردی نظیر مدل سازی ۳ بعدی، انیمیشن سازی CAD/CAM ، تصویربرداری پزشکی، پیاده‌سازی خدمات محیط‌های چندرسانه ای و بسیاری ازکاربردهای دیگر اینترنت و اینترانت را که پهنای باند زیادی نیاز دارند، پیاده‌سازی نمود.

۳-۴-۱-۴- ده گیگابیت اترنت

از ۲۷ سال پیش که فن‌آوری اترنت ارائه شد، این فن‌آوری تاکنون تحول‌های زیادی جهت برآورده کردن نیازهای شبکه‌های سوئیچ بسته ای یافته است. به خاطر مزایایی نظیر هزینه پیاده سازی کم، قابلیت اطمینان بالا و نصب و نگه‌داری آسان، فن‌آوری اترنت به شدت مورداستقبال قرارگرفته است. با افزایش سرعت شبکه‌ها و ارائه خدمات جدیدتر، فن‌آوری اترنت نیز تکامل یافته است و خود را با سرعت‌های بالا وفق داده است.

استاندارد گیگابیت اترنت که در بالا به آن اشاره شد، در شبکه‌های خصوصی وهمچنین شبکه‌های عمومی استفاده می‌شود. باتوسعه این فن‌آوری، استفاده اترنت از شبکه‌های محلی به شبکه‌های شهری توسعه یافته است. اخیراً استاندارد اترنت۱۰ گیگابیت برثانیه ارائه شده است. با استفاده از این استاندارد امکان ارسال ترافیک داده ای سریع و همچنین خدمات جدیدی نظیر ویدئوی متحرک فراهم شده‌است. استاندارد اترنت۱۰ گیگا بیت از چند جنبه با استاندارد اترنت پایه متفاوت است. دراین استاندارد فقط ازفیبر نوری استفاده می‌شود وهمچنین عملیات ارسال به‌صورت کاملا دوطرفه است. بنابراین دراین استاندارد هیچ‌گونه تداخلی بین قاب ها به‌وجود نمی‌آید. هر چند اترنت ۱۰گیگا بیت ازسرعت بسیار بالایی نسبت به اترنت پایه برخوردار است، اما از نظرساختار قاب‌ها تا حد زیادی مشابه آن می‌باشد. سرمایه گذاری بر روی اترنت۱۰ گیگابیت بر ثانیه و استفاده وسیع از آن هنوز مطمئن نمی‌باشد. قابلیت ارتباط اترنت۱۰ گیگابیت باسایر فن‌آوری های شبکه نظیرSONET 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:

۱. این فن‌آوری 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 شبکه‌ها به عنوان یک راه حل واحد و منحصربه فرد و نه به‌عنوان یک راه حل ثانویه استفاده نمود.

از نظر اقتصادی، باید نصب و توسعه شبکه‌های اترنت ۱۰ گیگابیت برای مشتریان مقرون به صرفه باشد. از سوی سازمان IEEE استاندارد IEEE 802.3ae جهت شبکه‌های اترنت ۱۰ گیگابیت وضع شده است. در این شبکه‌ها، 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 می‌باشد استفاده می‌شود.

دراین استاندارد، مشابه استاندارد اترنت سریع، لایه فیزیکی به دو زیر لایه PMD و CS تجزیه می‌شود. فرستنده/ گیرنده های نوری نمونه ای از PMD می‌باشند.توسط زیرلایه CS نحوه کدگذاری و عملیات تسهیم‌سازی توصیف می‌شود. در استاندارد 802.3ae دو نوع لایه فیزیکی پیشنهاد شده است که عبارتند از: لایه فیزیکی برای شبکه‌های محلی[1] و لایه فیزیکی برای شبکه‌های گسترده[2].

در شبکه‌های اترنت ۱۰ گیگابیت از واسط XAUI استفاده می‌شود. کلمه AUI از استاندارد اترنت پایه گرفته شده است. همچنین حرف X نشان دهنده سرعت ۱۰ گیگابیت بر ثانیه می‌باشد. علاوه بر واسط XAUI واسط XGMII در شبکه‌های اترنت ۱۰ گیگا بیت استفاده می‌گردد. این واسط دارای ۷۴ پین می‌باشد که برای اتصال کارت شبکه به محیط فیزیکی استفاده می‌شود.

در اترنت ۱۰ گیگابیت فقط از کانال‌های فیبر نوری از نوع چند مد یا تک مد استفاده می‌شود. با استفاده از این کانال‌ها می‌توان حداکثر تا ۴۰ کیلومتر را بدون نیاز به تکرار کننده اطلاعات ارسال نمود. هر دو واسط موجود برای شبکه‌های محلی و گسترده از یک زیر لایه PMD یکسان استفاده می‌کنند.

کاربردهای اترنت ۱۰ گیگابیت

فن‌آوری اترنت، متداول‌ترین و کاملترین فن‌آوری در شبکه‌های محلی می‌باشد. با توسعه فن‌آوری اترنت و پیدایش ۱۰ گیگابیت اترنت، امکان استفاده از برنامه های کاربردی با پهنای باند بالا در شبکه‌های محلی فراهم می‌شود.

مشابه فن‌آوری اترنت ۱ گیگابیت، در اترنت ۱۰ گیگابیت نیز امکان استفاده از کانال‌های فیبر نوری تک مد و چند مد وجود دارد. در شبکه‌های اترنت ۱۰ گیگابیت در حالتی که از فیبر تک مد استفاده می‌شود، حداکثر فاصله بین ایستگاه‌های شبکه۴۰کیلومتر می‌باشد در حالی که در شبکه‌های اترنت ۱ گیگابیت این فاصله ۵ کیلومتر است. به این دلیل استفاده از اترنت ۱۰ گیگابیت برای اتصال شبکه‌های محلی شرکت ها که دارای چندین شبکه محلی در سطح شهر می‌باشند مناسب‌تر از اترنت ۱ گیگابیت می‌باشد.

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

---

[1] LAN PHY
[2] WAN PHY

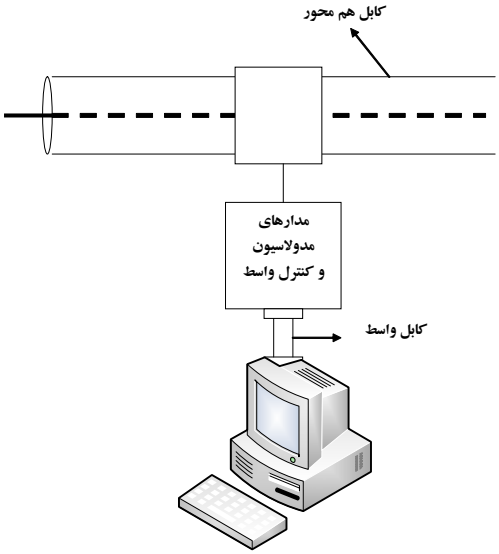
می‌توان برای پیاده سازی شالوده شبکه‌های شهری استفاده کرد. با استفاده از این فن‌آوری می‌توان همان‌طورکه گفته شد، فاصله کانال‌های شبکه را تا ۴۰ کیلومتر افزایش داد. از فن‌آوری اترنت ۱۰ گیگابیت در شبکه‌های گسترده نیز استفاده می‌شود. به عنوان مثال فراهم کنندگان خدمات اینترنت ،از شبکه‌های اترنت۱۰ گیگابیت برای اتصال سریع ونسبتاً ارزان به شبکه اینترنت استفاده می‌کنند.همچنین می‌توان از این فن‌آوری برای اتصال شبکه‌های محلی دور از هم از طریق شبکه گسترده استفاده نمود.

۳-۴-۲- شبکه گذرگاه نشانه (IEEE 802.4)

با وجود این‌که امروزه استاندارد اترنت به‌طور وسیعی در مراکز دانشگاهی و ادارات استفاده می‌شود، ولی یک عیب عمده در آن وجود دارد. در شبکه‌های اترنت امکان اولویت‌گذاری در قاب‌های ارسالی وجود ندارد؛ از این‌رو نمی‌توان از آن برای کاربردهای زمان حقیقی[1] استفاده نمود. در این راستا از سوی شرکت جنرال موتورکه در زمینه اتوماسیون کارخانجات فعال است، استاندارد گذرگاه نشانه مطرح گردید. درشکل (۳-۲۲)، نحوه اتصال ایستگاه ها در شبکه گذرگاه نشانه به کابل هم محورنشان داده شده است.

واحد مدولاسیون و واسط فیزیکی که درشکل فوق نشان داده شده است ، موظف به انجام عملیات زیراست:

- 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

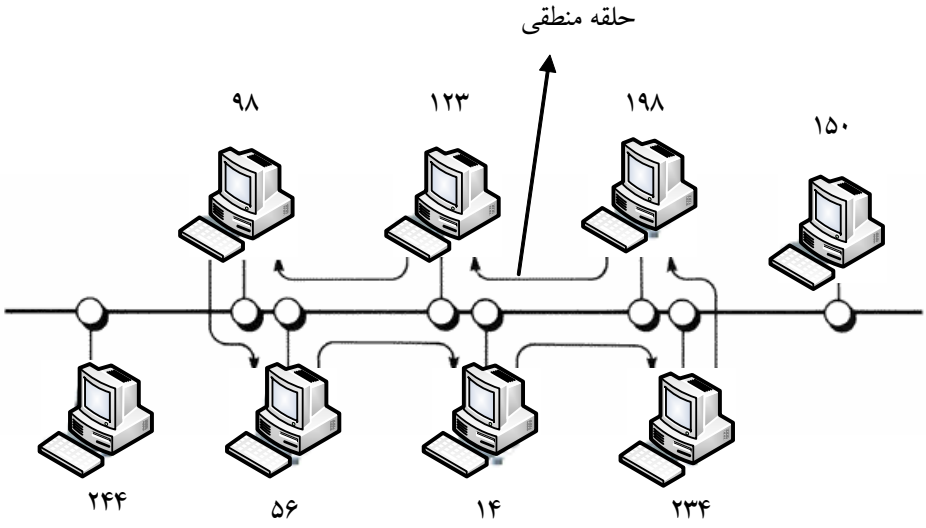
شبکه‌های گذرگاه نشانه دردو حالت کاری عمل می نمایند که عبارتند از: حالت کاری باند پهن[2] وباند حامل[1].در حالت کاری باند حامل، داده های ارسالی با استفاده ازمدولاسیونFSK به‌صورت سیگنال‌های سینوسی تبدیل می‌شوند. بسامد سیگنال حامل برای بیت ۰، دوبرابربسامد حامل برای بیت ۱ می‌باشد.

[1] Real time

[2] Broadband

در این استاندارد، ایستگاه‌های شبکه از طریق یک گذرگاه مشترک به یکدیگر متصل می‌شوند. ایستگاه‌های شبکه تشکیل یک حلقه منطقی می‌دهند به‌طوری که هر ایستگاه آدرس ایستگاه سمت چپ خود را می‌داند. هنگامی‌که حلقه منطقی به‌وجود می‌آید، ایستگاهی که دارای بالاترین آدرس است قادر به ارسال قاب می‌باشد. پس از آن‌که ارسال قاب‌های ایستگاه فرستنده پایان یافت، ایستگاه مزبور با ارسال یک قاب کنترلی خاص به نام نشانه ، امکان ارسال را در اختیار همسایه‌اش برروی حلقه منطقی می‌گذارد. بعد از آن‌که ایستگاه، نشانه را به همسایه منطقی خود ارسال نمود، برای اطمینان ازدریافت صحیح آن توسط همسایه، برای مدت زمان معینی به کانال گوش فرامی‌دهد وچنانچه دراین مدت عبورقاب سالمی ازکانال را تشخیص ندهد، متوجه خراب شدن و یا گم شدن نشانه شده و دوباره آن رابرای همسایه منطقی خود ارسال می دارد.

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



شکل (۳-۲۳) : شبکه گذرگاه نشانه

همان‌طور که در شکل فوق نیز دیده می‌شود، در شبکه‌های گذرگاه نشانه، ترتیب فیزیکی قرارگرفتن ایستگاه‌ها در روی گذرگاه مشترک اهمیتی ندارد. هنگامی‌که یک ایستگاه، قابی را ارسال می‌کند، آن قاب در هر دو طرف کانال منتشر می‌شود و تمام ایستگاه‌های دیگر آن را دریافت می‌دارند، ولی تنها ایستگاهی که آدرس گیرنده قاب ارسالی با آدرس آن مطابقت دارد قاب را دریافت می‌کند. در پایان ارسال هر ایستگاه، قاب در اختیار همسایه منطقی ایستگاه قرار می‌گیرد. احتمال این‌که در یک حلقه منطقی تمام ایستگاه‌های شبکه عضویت نداشته باشند وجود دارد. به‌عنوان مثال در شکل (۳-۲۳)، فقط ایستگاه‌های به آدرس ۱۴،۵۶،۹۸،۱۲۳،۱۹۸و۲۳۴داخل حلقه منطقی می‌باشند. هنگامی‌که حلقه منطقی فعال می‌شود، می‌توان 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 زمان‌سنج و ۱۲ متغیر داخلی می‌باشد. در شبکه‌های فوق کابل‌های هم‌محور ۷۵ اهمی که بیشتر در سیستم‌های تلویزیون کابلی کاربرد دارند استفاده می‌شود. سرعت‌های متداول این نوع شبکه‌ها عبارتند از ۱،۵ و ۱۰ مگابیت برثانیه.

---

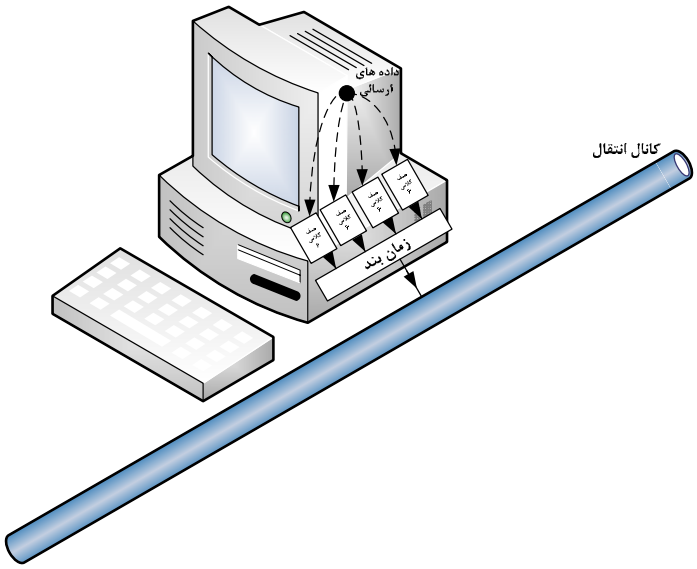
[1] Carrierband

هنگامی‌که برای اولین بار حلقه منطقی تشکیل می‌شود، ایستگاه‌ها به ترتیب آدرس فیزیکی (کارت شبکه) خود در حلقه قرار می‌گیرند. مبادله نشانه نیز از ایستگاه‌های با آدرس بالا به سمت ایستگاه‌های با آدرس کم صورت می‌گیرد. هرگاه ایستگاهی نشانه را در اختیار قرار گرفت، فقط برای مدت محدودی اقدام به ارسال قاب می‌نماید و بعد از آن‌که مدت زمان آن تمام شد، باید نشانه را در اختیار ایستگاه دیگر قرار دهد. چنانچه ایستگاهی که نشانه را در اختیار دارد داده‌هایی برای ارسال نداشته باشد، آنگاه به‌سرعت نشانه را آزاد می‌کند و به ایستگاه مجاور خود بر روی حلقه منطقی تحویل می‌دهد.

درشبکه‌های گذرگاه نشانه، هرایستگاه به‌طور داخلی به چهار زیر ایستگاه دیگر تقسیم‌بندی می‌شود. هر زیر ایستگاه داخلی قادر به ارسال یک کلاس خاص ترافیک می‌باشد. چهار کلاس ترافیک با اولویت‌های ۰،۲،۴ و۶ در شبکه‌های گذرگاه نشانه وجود دارند که کلاس صفر کمترین اولویت و کلاس ۶ بالاترین اولویت را در اختیار دارد. نحوه استفاده از۴ کلاس ترافیکی فوق به‌صورت زیر می‌باشد:

- ***کلاس۶:*** پیام های اورژانسی و بسیارمهم نظیرآلارم‌های هشداردهنده وعملیات کنترلی حساس ازکلاس ۶ که بالاترین اولویت را دارا می‌باشد، استفاده می‌کنند.
- ***کلاس۴ :*** 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 داده‌ها به‌منظور واقعه‌نگاری[1] ازکلاس اولویت ۲ استفاده می نمایند.
- ***کلاس ۰:*** پیام های مربوط به انتقال فایل دارای کمترین اولویت بوده و ازکلاس اولویت ۰ استفاده می‌کنند.

هنگامی‌که از لایه بالاتر(زیرلایه LLC) قابی برای ارسال تحویل زیرلایه MAC می‌گردد، ابتدا قاب دریافتی از نظر اولویت بررسی می‌شود و سپس به یکی از زیرایستگاه‌های ۰ تا ۶ ارسال می‌گردد و در آنجا در یک صف قرار می‌گیرد تا نوبت ارسال آن فرا برسد. در شکل (۳-۲۴) زیرایستگاه‌های موجود در یک ایستگاه شبکه گذرگاه نشانه نشان داده شده است.

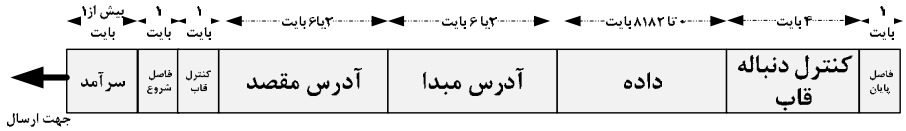


شکل(۳-۲۴) : زیرایستگاه‌های موجود در یک ایستگاه شبکه گذرگاه نشانه

[1] Logging

هرایستگاه برای کنترل ارسال قاب ها دارای دو زمان‌سنج می‌باشد که عبارتند از: زمان‌سنج نگـه‌داری نـشانه (THT[1]) و زمان‌سنج نگه‌داری نشانه برای کلاس اولویت بالا(HP-THT[2]). هنگامی‌که یک ایستگاه شبکه نشانه را در اختیارمی‌گیـرد، آنـرا به زیرایستگاه شماره ۶ تحویل می‌دهد. این زیرایستگاه حداکثر بـه انـدازه مـدت زمـان زمـان‌سـنجHP-THT، قادربـه ارسـال قاب‌های بااولویت بالا می‌باشد. حداکثر مدت زمانی که ایستگاه قادربه نگه‌داری نشانه و ارسال قاب‌های خود می‌باشـد توسـط زمان‌سنجTHT مشخص می‌شود. بنابراین درشبکه‌های گذرگاه نشانه، هرزیرایستگاه برای مدت زمان معینـی قـادر بـه ارسـال داده‌ها می‌باشد و هنگامی‌که زمان‌سنج هر زیرایستگاه لبریز شد، نـشانه از آن سـلب مـی‌شـود و بـه زیرایـستگاه بعـدی داده می‌شود. از آن‌جایی‌که کلاس‌های ۶ و ۴ به ترتیب دارای اولویت بیشتری نسبت به کلاس‌های دیگر می‌باشند، مدت زمـانی که زمان‌سنج در اختیار کلاس ۶ است بیشتر از سایر کلاس‌ها می‌باشد. بدین ترتیـب زیـرکلاس صـفر کمتـرین فرصـت ارسال قاب‌های خود را پیدا می‌نماید.

چنانچه زیر ایستگاهی تمام قاب‌های خود را ارسال دارد، دیگر نیازی به نشانه ندارد و زمان باقی مانده خـود را تحویـل زیرایستگاه بعدی می‌دهد. با توجه به اولویت بالایی که زیرکلاس ۶ دارد، از آن می‌توان برای ارسال داده‌هـای زمـان حقیقـی مثل صوت و تصویر استفاده کرد. در شکل (۳-۲۵) ساختار قاب‌های گذرگاه نشانه نشان داده شده است.



شکل (۳-۲۵) : ساختار قاب‌های گذرگاه نشانه

همان‌طور که در این شکل نیز دیده می‌شود، درقاب‌های گذرگاه نشانه فیلدهای زیر موجود است:

- ***فیلد سرآمد:*** حداقل طول این فیلد یک بایت می‌باشد و مشابه استاندارد اترنت از آن بـرای همزمـان‌سـازی سـاعت های فرستنده وگیرنده استفاده می‌شود.
- ***فیلدهای فاصل شروع و فاصل پایان:*** از این فیلدها برای تعیین محدوده شروع و پایان قاب‌ها استفاده می‌گردد.
- ***فیلد کنترل قاب:*** برای جداسازی قاب‌های داده‌ای از قاب‌های کنترل شبکه از این فیلد تک‌بایتی استفاده می‌شـود. توسط این فیلد اولویت قاب‌های داده‌ای قابل تعیین می‌باشد. همچنین چنانچه بیت خاصـی در ایـن فیلـد فعـال باشـد، گیرنده قاب ملزم به ارسال پیام تصدیق مبنی بر دریافت صحیح یا نادرست قاب است. نوع قاب‌های کنترلی توسـط ایـن فیلد مشخص می‌شود. انواع مختلف قاب‌های کنترلی عبارتند از: قاب‌های واگذاری نشانه و قاب‌های نگه‌داری حلقـه کـه به‌وسیله آن امکان ورود و خروج ایستگاه جدید به حلقه وجود دارد.
- ***فیلدهای آدرس مبدأ و آدرس مقصد:*** توسط این فیلدها مشابه آنچه که در استاندارد اترنت گفته شد، آدرس‌های مبدأ و مقصد قاب ارسالی مشخص می‌شود.
- ***فیلد داده:*** این فیلد حاوی داده‌های زیرلایه LLC است که باید توسط قاب‌های MAC تحویل مقصد شود. طول ایـن فیلد متغیر می‌باشد و چنانچه از آدرس‌های دو بایتی استفاده شود، این فیلد حداکثر دارای طول ۸۱۸۲ بایت خواهد بود ولی در صورت استفاده از آدرس‌های ۶ بایتی حداکثر طول این فیلد ۸۱۷۴ بایت است.

---

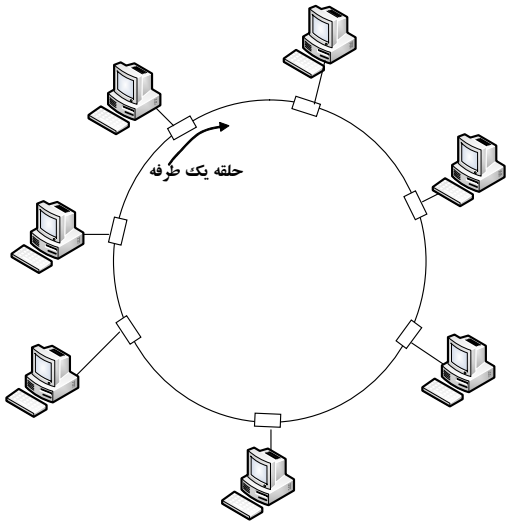
[1] Token Hold Timer

[2] High-Priority Token Hold Timer

- ***فیلد کنترل دنباله قاب:*** این فیلد که مشابه فیلد کد افزونگی چرخشی (CRC) استاندارد اترنت می‌باشد، برای تشخیص و رفع خطاهای احتمالی در انتقال قاب‌ها به کار می‌رود.

۳-۴-۳- شبکه حلقه نشانه(IEEE 802.5)

در این استاندارد مطابق با شکل (۳-۲۶)، تمام ایستگاه‌ها از طریق یک حلقه مشترک به یکدیگر متصل می‌شوند. البته یک حلقه را می‌توان به‌صورت مجموعه‌ای از کانال‌های نقطه به نقطه تصور نمود و برای پیاده‌سازی آن از محیط‌هایی نظیر زوج سیم به هم تابیده شده، کابل هم‌محوروفیبر نوری استفاده کرد. هنگامی‌که تمام ایستگاه‌های موجود در حلقه بی‌کار هستند، یک نشانه درحلقه درحال چرخش می‌باشد. وقتی که ایستگاهی قصد ارسال یک قاب را داشته باشد، ابتدا نشانه را تصرف می نماید وآن را از حلقه خارج می‌سازد وسپس اقدام به ارسال اطلاعات می‌کند. از آن‌جایی‌که فقط یک نشانه در شبکه به‌صورت آزاد وجود دارد، بنابراین امکان تداخل از بین می‌رود. طول فیزیکی حلقه و سرعت آن باید طوری باشد که حداقل یک قاب نشانه به‌طور کامل درحلقه جریان داشته باشد.



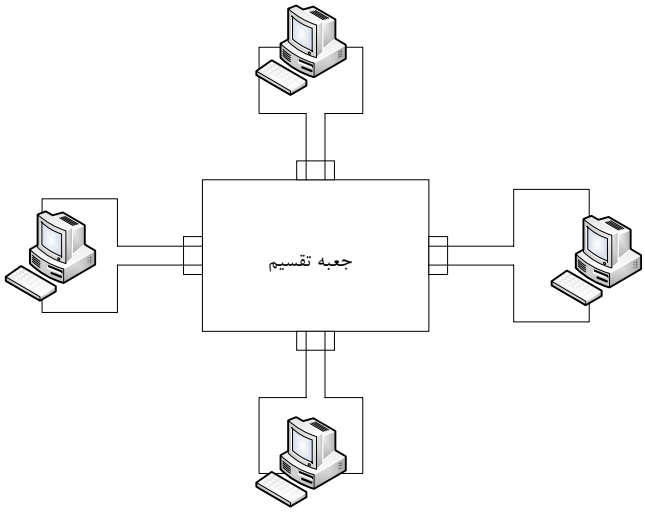
شکل (۳-۲۶) : شبکه حلقه نشانه

در شبکه‌های حلقه نشانه، از کانال‌های فیزیکی از نوع زوج سیم‌های STP در سرعت‌های ۱،۴ و۱۶ مگابیت بر ثانیه استفاده می‌شود. یکی از مشکلات اصلی شبکه‌های حلقه نشانه این است که چنانچه کابل شبکه در محلی قطع شود، کل شبکه از کار می‌افتد. برای رفع این مشکل از جعبه تقسیم استفاده می‌شود. در این روش ایستگاه‌ها از نظر منطقی تشکیل یک حلقه می‌دهند 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 می‌شوند. در شکل(۳-۲۷)، نمونه‌ای از شبکه حلقه نشانه با استفاده از جعبه تقسیم نشان داده شده است.

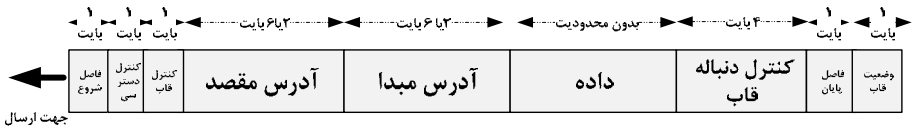
در داخل جعبه چندین کلید وجود دارد که وظیفه آنها اتصال یا قطع اتصال یک ایستگاه از حلقه می‌باشد. چنانچه حلقه قطع شود و یا ایستگاهی از کار بیفتد، کلید آزاد می‌شود و در نتیجه ایستگاه از حلقه خارج می‌گردد. می‌توان کلیدهای فوق را به‌وسیله نرم‌افزار کنترل نمود، که در این‌صورت امکان عیب‌یابی اتوماتیک شبکه فراهم می‌آید. هنگامی‌که حلقه از هرگونه ترافیکی خالی باشد، یک نشانه ۳ بایتی به‌طور مداوم در حلقه می‌چرخد تا این‌که ایستگاهی نشانه را دریافت دارد و آن را تصرف کند. در شبکه‌های حلقه نشانه هر ایستگاهی که قاب را ارسال نموده است، خود موظف به خارج‌نمودن آن

ازحلقه می‌باشد. بدین ترتیب هرقاب ارسالی یک دور در حلقه می‌چرخد و سپس توسط خود فرستنده از حلقه حذف می‌شود. هر ایستگاهی که نشانه را در اختیار دارد، قادر به ارسال قاب به مدت ۱۰ میلی‌ثانیه می‌باشد. البته این زمان قابل تغییر است. بعد از اتمام ارسال قاب‌ها، نشانه دوباره توسط ایستگاه تولید می‌شود و وارد شبکه می‌گردد.

درشبکه‌های حلقه نشانه، هر شبکه دارای یک ایستگاه ناظر[۱] می‌باشد که از آن برای نظارت بر حلقه استفاده می‌شود. ازایستگاه ناظر برای پاک‌سازی حلقه از قاب‌های مخدوش و انجام اقدامات لازم در هنگامی‌که حلقه قطع می‌شود، استفاده می‌گردد. جهت اطمینان از گم‌شدن احتمالی نشانه، هر ناظر شبکه دارای یک زمان‌سنج می‌باشد که در صورت لبریزشدن آن، متوجه گم‌شدن نشانه می‌شود. در شکل(۳-۲۸)، ساختار قاب‌های حلقه نشانه نشان داده شده است.



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



شکل(۳-۲۸) : ساختار قاب‌های حلقه نشانه

همان‌طور که در این شکل نیز دیده می‌شود، در قاب‌های حلقه نشانه فیلدهای زیر موجود می‌باشد:

- ***فیلد فاصل شروع[۲] و فاصل پایان[۳] :*** از این فیلدها برای نشان دادن شروع و پایان هر قاب استفاده می‌شود.
- ***فیلد کنترل دسترسی[۴]:*** این فیلد شامل بیت‌هایی برای رزرو نشانه و نظارت بر حلقه می‌باشد.
- ***فیلد کنترل قاب:*** برای جداسازی قاب‌های داده‌ای از قاب‌های کنترلی از این فیلد استفاده می‌شود.
- ***فیلدهای آدرس مبدأ و مقصد:*** این فیلدها مشابه فیلدهای موجود دراستانداردهای اترنت وگذرگاه نشانه برای تعیین آدرس فرستنده و گیرنده قاب‌ها به‌کار می‌روند.

---

[۱] Monitoring station
[۲] Start delimiter
[۳] End delimiter
[۴] Access control

- ***فیلد داده:*** این فیلد حاوی داده‌های لایه بالاتر می‌باشد. در طول این فیلد هیچ‌گونه محدودیتی وجود ندارد.
- ***فیلد کنترل دنباله قاب:*** این فیلد مشابه با فیلد موجود در قاب‌های اترنت وگذرگاه نشانه برای بررسی و اطمینان از صحت قاب دریافتی در مقصد به کار می‌رود. ازروش CRC برای کنترل خطا استفاده می‌شود.
- ***فیلد وضعیت قاب[1]:*** دراین فیلد دو بیت به نام‌های بیت‌های A و C موجود است که از آنها برای اطمینان از دریافت صحیح قاب ارسالی توسط مبدأ درگیرنده استفاده می‌شود. چنانچه مقصد در شبکه موجود نباشد و یا هنوز ایستگاه خاموش باشد، دو بیت A و C صفر می‌باشند. 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 به‌طور صحیح دریافت نموده است. بدین ترتیب فرستنده با بررسی وضعیت بیت‌های فوق، هنگامی‌که قاب ارسالی خود را دوباره دریافت می‌کند، متوجه دریافت ویا عدم دریافت صحیح قاب در مقصد می‌شود.

۳-۵- پروتکل DQDB

توسط گروه۸۰۲ سازمان IEEE ،استاندارد 802.6 که با نام DQDB نیز شناخته می‌شود، برای استفاده در شبکه‌های شهری ارائه گردید. همان‌طور که از نام این استاندارد شناخته می‌شود DQDB ازساختار متشکل از دو گذرگاه مشترک استفاده می‌نماید. هر ایستگاه در شبکه به دو گذرگاه مشترک متصل می‌باشد. نحوه دسترسی به گذرگاه مشترک فوق به‌وسیله مکانیسمی بنام صفهای توزیع شده انجام می‌گیرد.

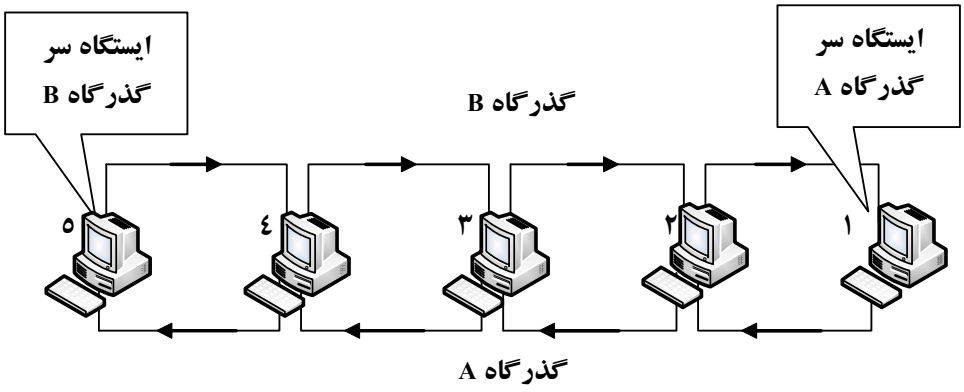
در شکل (۳-۲۹) توپولوژی یک شبکه DQDB نشان داده شده است. مطابق با شکل فوق دو گذرگاه مشترک یک‌طرفه به‌نام A و B در شبکه وجود دارند. تمام ایستگاه‌های شبکه به‌طور مستقیم به هر دو گذرگاه مشترک A و B متصل می‌باشند. ترافیک ارسالی در گذرگاه‌های مشترک فوق یک‌طرفه می‌باشد. جهت ترافیک در یک گذرگاه مشترک بر خلاف جهت ترافیک در گذرگاه مشترک دیگر می‌باشد. ارتباط بین ایستگاه‌ها در شبکه‌های DQDB به‌وسیله جریان ترافیکی در گذرگاهها مشخص می‌شود. به عنوان مثال در گذرگاه A شکل (۳-۲۹) ایستگاه‌های ۱ و ۲ نسبت به ایستگاه۳ بالاجریان[2] و ایستگاه‌های ۴ و ۵ نسبت به ایستگاه ۳، پایین جریان[3] می‌باشند. همچنین در گذرگاه مشترک B نیز ایستگاه‌های ۱ و ۲ نسبت به ایستگاه۳ پایین جریان وایستگاه ۴ و۵ نسبت به ایستگاه ۳، بالا جریان می‌باشند.

۳-۵-۱- ارسال برش‌های زمانی

در شبکه‌های DQDB ارسال اطلاعات از طریق برشهای زمانی ۵۳ بایتی انجام می‌گیرد. ایستگاه سرگذرگاه مشترک موظف به ایجاد برش زمانی خالی برای استفاده در گذرگاه مشترک می‌باشد. نرخ ارسال ایستگاه‌ها بستگی به تعداد برشهای زمانی ایجاد شده در ثانیه دارد. برش زمانی خالی درگذرگاه مشترک به سمت پایین حرکت می‌نماید تا این‌که یک ایستگاه فرستنده داده‌ها را درون برش زمانی قرار دهد. گیرنده نیز با توجه به آدرس خود اقدام به برداشتن داده از برش زمانی می‌نماید.

---

[1] Status field
[2] Upstream
[3] Downstream



شکل (۳-۲۹): مثالی از شبکه DQDB

همان‌طور که گفته شد از آن‌جایی‌که در شبکه DQDB از دو گذرگاه مشترک استفاده می‌شود، ایستگاه فرستنده بایدازطریق گذرگاه مشترکی داده‌های 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) داده‌هایی را ارسال نماید، از گذرگاه مشترک B استفاده می‌کند.

۳-۵-۲- رزرو برش‌های زمانی

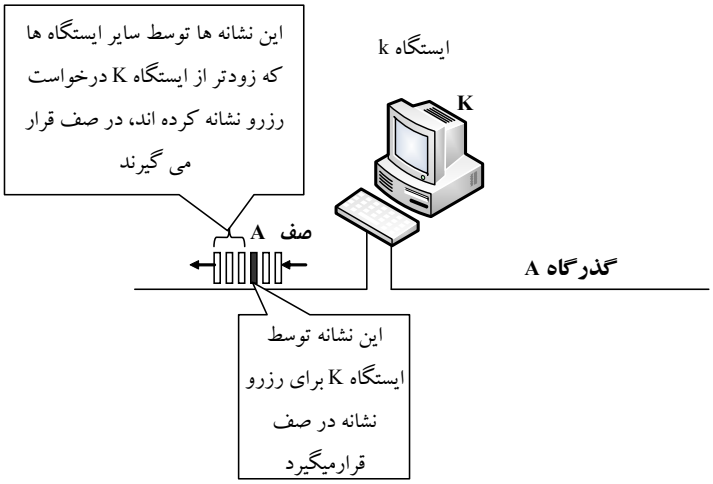
برای ارسال داده‌ها در شبکه‌های DQDB هر ایستگاه باید منتظر ورود یک برش زمانی خالی باشد. از آن‌جایی‌که برشهای زمانی خالی از طرف ایستگاه سرگذرگاه مشترک به سمت پایین تولید می‌گردد، بنابراین ایستگاه‌هایی که نزدیکتر به ایستگاه سر می‌باشند شانس بیشتری برای دسترسی به برشهای زمانی خالی در گذرگاه مشترک دارند. چنانچه برای مشکل فوق راه حل مناسبی ارائه نگردد، کیفیت خدمات درایستگاه‌های پایین جریان به شدت کاهش می‌یابد.

برای حل مشکل فوق از عملیات رزرو برش زمانی استفاده می‌شود. هر ایستگاه درصورتی اجازه استفاده از برش زمانی خالی را دارد که قبلاً آن را رزرو کرده باشد. از آن‌جایی‌که جهت ارسال در گذرگاههای مشترک یک‌طرفه می‌باشد، هر ایستگاه برای رزور یک برش زمانی در یک گذرگاه مشترک از گذرگاه مشترک دوم استفاده می‌نماید. با فعال نمودن یک بیت مشخص در هر برش زمانی عملیات رزروانجام می‌گیرد.

۳-۵-۳ - صف‌های توزیع شده

برای انجام عملیات رزرو برش زمانی و ردگیری عملیات رزرو سایر ایستگاه‌ها، درهرگذرگاه مشترک در شبکه‌های DQDB ، هر ایستگاه به دو صف نیاز دارد. برای گذرگاه مشترکA، صف A و برای گذرگاه مشترک B ، صف B در نظر گرفته می‌شود. عملکرد صف‌ها به‌صورت FIFO می‌باشند.

هنگامی‌که ایستگاهی درخواست رزرو برش زمانی را ارسال می‌کند، تمام ایستگاه‌های دیگر که درخواست فوق را دریافت می‌دارند، آن را به صف خود اضافه می‌نمایند. با عبور هر برش زمانی خالی یکی از محتویات صف کاهش می‌یابد. چنانچه خود یک ایستگاه بخواهد داده‌هایی را ارسال نماید، ابتدا درخواست رزرو برش زمانی خود را از طریق گذرگاه مشترک دوم ارسال می‌کندو سپس درصف یک علامت که نشان دهنده درخواست رزرو خود ایستگاه می‌باشد قرار می‌دهد. شکل(۳-۳۰) عملیات رزرو در صف را نشان می‌دهد.

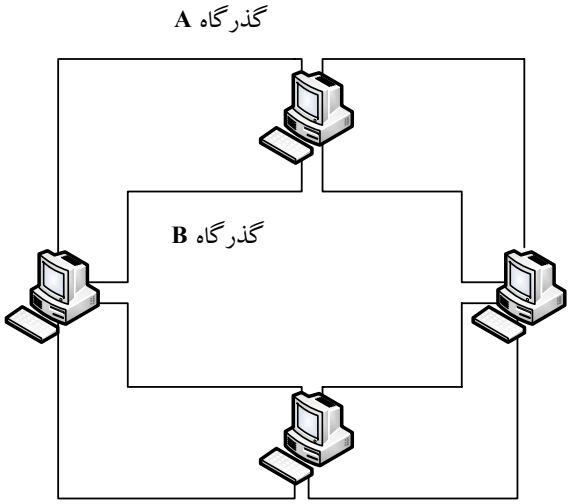


شکل(۳-۳۰): مثالی از رزرو نشانه درشبکه DQDB

با عبور هر برش زمانی خالی یکی از محتویات صف کم می‌شود.چنانچه نشانه مشخص کننده رزرو ایستگاه در صف به ابتدای صف رسید، نوبت ارسال خود ایستگاه فرا رسیده است. در این حالت باعبور اولین برش زمانی خالی، ایستگاه داده‌های خود را درآن قرار می‌دهد و آن را ارسال می‌دارد.

۳-۵-۴ - ساختار حلقه

می‌توان پروتکل DQDB را به‌صورت حلقه نیز پیاده‌سازی نمود که در شکل (۳-۳۱) نمونه‌ای از این ساختار نشان داده شده است. در این حالت یک ایستگاه نقش هر دو ایستگاه شروع و پایان را عمل می‌نماید. یکی از مزایای این ساختار، قدرت آن در مواجه با خرابی در کانال است.



شکل (۳-۳۱) : ساختار حلقه ای DQDB

۳-۵-۵- لایه‌های DQDB

توسط سازمان IEEE زیرلایه‌های MAC و لایه فیزیکی برای DQDB تعریف شده است. زیرلایه MAC موظف به تجزیه قاب‌های ورودی از زیرلایه LLC به تکه‌های ۴۸ بایتی می‌باشد. این زیر لایه به هر تکه ۵ بایت سرآیند اضافه می‌نماید و قاب‌های ۵۳ بایتی ایجاد می‌کند.

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 می‌باشد برای کنترل دسترسی به گذرگاه مشترک استفاده می‌شود. این فیلد به ۵ زیر فیلد زیر تجزیه می‌شود.
  - **بیت B**: چنانچه این بیت ۱ باشد، نشان دهنده وجود داده در برش زمانی است. درصورتی‌که این بیت صفر باشد برش زمانی خالی می‌باشد.
  - **بیت ST**: توسط این بیت دو نوع برش زمانی مشخص می‌گردد که یکی از آنها برای ارسال قاب های داده و دیگری برای ارسال اطلاعات همزمانی به‌کار می‌رود.
  - **بیت R** : از این بیت برای رزرو برش زمانی استفاده می‌شود.
  - **فیلد PRS** : این فیلد دو بیتی هنگامی‌که ایستگاه مقصد محتویات برش زمانی ورودی خود را خواند صفرمی‌گردد.
  - **فیلد RQ**: این فیلد سه بیتی توسط ایستگاهی که می‌خواهد عملیات رزرو برش زمانی را انجام دهد مقدار دهی می‌شود. توسط این سه بیت می‌توان ۸ سطح اولویت تعریف نمود.
- ***فیلد آدرس:*** این فیلد ۲۰ بیتی حاوی مشخص کننده کانال مجازی (VCI[1]) که درشبکه‌های شهری و گسترده استفاده می‌شود، می‌باشد. هنگامی‌که از شبکه‌های DQDB به‌صورت شبکه‌های محلی استفاده می‌شود،تمام بیت های این فیلد۱ است. برای حمل آدرسهای فیزیکی، سرآیندهای دیگری به قاب‌ها اضافه می‌شود.
- ***فیلد نوع:*** این فیلد دو بیتی نوع داده‌های موجود در قاب را مشخص می‌نماید. داده‌های موجود در ۴۸ بایت قاب‌های DQDB می‌تواند داده‌های کاربر، داده‌های مدیریت و نظیر آن باشد.
- ***فیلد اولویت:*** توسط این فیلد دو بیتی اولویت برش زمانی مشخص می‌شود.
- ***فیلد CRC.*** این فیلدحاوی کد افزونگی چرخشی می‌باشد که از آن برای تشخیص یک یا چند بیت خطا و تصحیح یک بیت خطا درسرآیند استفاده می‌شود.

۳-۶- شبکه SMDS

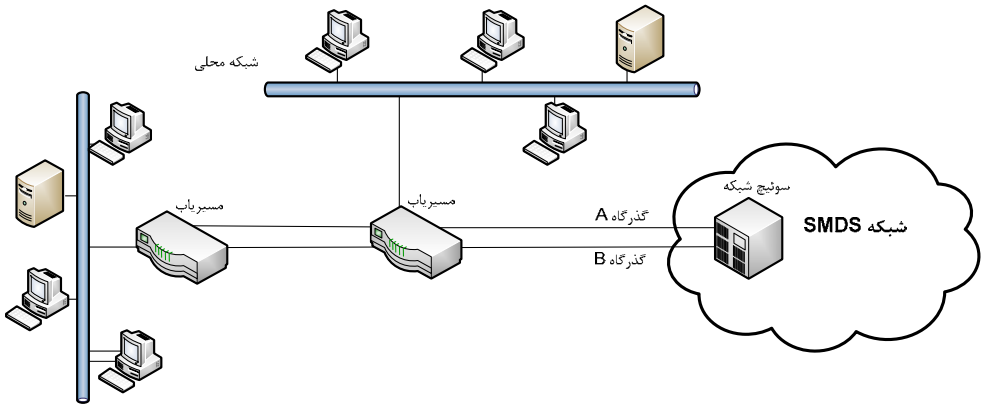
یکی دیگر از استانداردهای شبکه‌های شهری، SMDS می‌باشد که از آن برای برقراری ارتباط با سرعت بالا استفاده می‌شود. یکی از موارد استفاده SMDS ،اتصال شبکه‌های محلی سازمانها که در نقاط مختلف یک شهر قرار دارند به یکدیگراست. قبل از پیدایش SMDS اتصال بین شبکه‌های محلی فوق به سختی انجام می‌شد و اغلب از خدمات شبکه تلفن سوئیچ شده و DDS استفاده می‌گردید. از آن‌جایی‌که اکثر شبکه‌های محلی دارای نرخ ارسال بالای ۱۰ مگابایت بر ثانیه می‌باشند، استفاده ازشبکه تلفن وخدمات آن برای اتصال شبکه‌های محلی به یکدیگر راه حل مناسبی نمی‌باشد. یکی دیگر از روش‌های مناسب، استفاده از خطوط T1 با سرعت ۱/۵۴۴ مگابیت بر ثانیه و یا خطوط T3 با سرعت ۴۴/۷۳۶ مگابیت بر ثانیه می‌باشد. استفاده از این خطوط تا حدی مشکل سرعت اتصال شبکه‌های محلی به یکدیگر را حل می‌نماید ولی باید

[1] Virtual Channel Identifier

توجه نمود که هزینه خطوط فوق بسیار زیاد است. از طرف دیگر ترافیک داده ارسالی شبکه‌های محلی شرکتها به‌طور دائمی وجود ندارد و بنابراین از تمامی ظرفیت خطوط بهره‌برداری کامل نمی‌شود.

برای حل مشکلات فوق از فن‌آوری SMDS استفاده می‌گردد. SMDS از نوع سوئیچینگ بسته‌ای داده گرام می‌باشد که برای حمل ترافیکهای شبکه شهری با سرعت بالا بسیار مفید است. این فن‌آوری به‌وسیله یک سری استانداردهایی که توسط مرکز تحقیقاتیBellcore پیشنهاد گردید و توسط خدمات دهنده های شبکه‌های مخابراتی به‌طورمناسب تغییر و توسعه یافت، توصیف می‌شود.

اتصال شبکه‌های محلی به شبکه SMDS از طریق مسیریاب‌ها صورت می‌پذیرد. دسترسی به شبکه SMDS از طریق پروتکل واسط SMDS (SIP[1]) که مبتنی بر DQDB است انجام می‌پذیرد. شبکه‌های محلی کاربران از طریق مسیریاب ودوگذرگاه مشترک مطابق با آنچه که در شکل (۳-۳۲) نشان داده شده است، به شبکه SMDS متصل می‌شوند.



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 می‌باشد و نیازی به صف ندارد. ولی درصورتی‌که چندین شبکه محلی مشتریان به شبکه SMDS متصل شود، در این حالت به تمامی قابلیت‌های DQDB نیاز می‌باشد.

استانداردهای SMDS به روشنی نحوه پیاده‌سازی شبکه را مشخص نمی‌کند، بلکه فراهم‌کنندگان خدمات SMDS درانتخاب فن‌آوری شبکه برای حمایت از خدمات مورد نیازخود آزاد می‌باشند. پیش بینی می‌شود که در آینده نزدیک نرخ ارسال در شبکه‌های SMDS به بالاتر از ۶۰۰ مگابیت بر ثانیه برسد.

۳-۷- شبکه FDDI

شبکه FDDI یک پروتکل شبکه محلی می‌باشد که توسط سازمان‌های ANSI و ITU-T استاندارد شده است. نرخ ارسال شبکه‌های FDDI ، ۱۰۰ مگابیت بر ثانیه می‌باشد، که به مراتب بالاتر از نرخ شبکه‌های اترنت و گذرگاه نشانه و حلقه نشانه است. درهنگام ارائه FDDI فقط کانال فیبر نوری قادر به تامین سرعت ارسال ۱۰۰ مگابیت برثانیه بود، ولی امروزه باکمک زوج سیم‌های مسی نیز می‌توان به این سرعت دسترسی پیدا نمود. به نسخه سیم مسی از شبکه‌های FDDI ، CDDI[۲] گفته می‌شود.

---

[1] SMDS Interface Protocol

[۲] Copper Distributed Data Interface

شبکه FDDI مبتنی بر مبادله نشانه می‌باشد. در شبکه‌های حلقه نشانه هر ایستگاه فقط هنگامی‌که نشانه را دریافت نمود، قادر به ارسال یک قاب می‌باشد. اما در شبکه‌های FDDI دسترسی به شبکه محدود به زمان می‌باشد و هر ایستگاه تا هنگامی‌که محدودیت زمانی به آن اجازه می‌دهد، 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 می‌باشند و در مقابل، کلمه غیرهمزمان به اطلاعاتی اشاره می‌کند که به زمان حساس نمی‌باشند. هر ایستگاهی که نشانه را در اختیار می‌گیرد ابتدا قاب‌های همزمان خود را ارسال می‌دارد و چنانچه از زمان ارسال آن چیزی باقی مانده باشد، قاب‌های غیرهمزمان ارسال می‌شوند.

۳-۷-۱- رجیسترهای FDDI

در FDDI برای کنترل چرخش نشانه و دسترسی عادلانه ایستگاه‌های شبکه به کانال، ازسه رجیستر زمانی استفاده می‌گردد. بنابراین هر ایستگاه در FDDI دارای سه رجیستر زمانی می‌باشد که برای کنترل حلقه به‌کار می‌رود. مقادیر این رجیسترها با راه افتادن حلقه تنظیم می‌گردد و درتمام مدت کارکرد شبکه ثابت می‌مانند. 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 داده‌های همزمان را دارد مشخص می‌نماید. مقداراین رجیستر برای ایستگاه‌های شبکه متفاوت می‌باشدودرهنگام راه اندازی حلقه مقداردهی می‌گردد.

رجیستر TTRT مشخص کننده زمان متوسط مورد نیاز برای یک دور چرخش نشانه می‌باشد. مقدار این رجیستر برای تمام ایستگاه‌ها یکسان است که در هنگام راه اندازی حلقه تعیین می‌شود. از آن‌جایی‌که این رجیستر مقدار متوسط زمان چرخش یک دور نشانه درحلقه را مشخص می‌کند، ممکن است مقدار واقعی بیشتر یا کمتر از محتوای این رجیستر باشد.

مقدار رجیستر AMT دو برابر مقدار رجیسترTTRT است. زمان چرخش نشانه درحلقه 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- زمان‌سنج‌های FDDI

در شبکه FDDI هر ایستگاه برای مقایسه زمان واقعی با مقادیر موجود در رجیسترهای فوق نیاز به یک سری زمان‌سنج دارد. زمان‌سنج‌های فوق قابل مقداردهی و آغاز دوباره می‌باشند که مقدار آنها توسط ساعت سیستم کم می‌شود.

دو زمان‌سنجدر شبکهFDDI به‌کار می‌روند که عبارتند از: زمان‌سنج TRT و زمان‌سنج THT . زمان‌سنج TRT مقدار زمانی یک دور چرخش نشانه درحلقه را اندازه گیری می‌کند. هرایستگاه مدت زمان سپری شده بین دو مشاهده متوالی نشانه درشبکه را با استفاده از زمان‌سنج TRT اندازه گیری می نماید. باید توجه نمود که زمان فوق شامل مدت زمان لازم برای ارسال قاب‌های ایستگاه‌هایی که نشانه را دراختیار می گیرند نیز می‌باشد. طبیعی است که درصورتی‌که در شبکه بار ترافیکی کمی موجود باشد، دراین‌صورت مقدار زمان‌سنج TRT بسیار کم است.

درصورتی‌که ایستگاهی قاب‌هایی برای ارسال داشته باشد، با دریافت نشانه مقدار جاری TRT را از مقدار موجود در رجیستر TTRT کم نموده و حاصل را در زمان‌سنج THT قرار می‌دهد. مقدار حاصل در زمان‌سنج THT نشان دهنده حداکثر زمان مجاز برای ایستگاه که قادر به ارسال قاب‌های منتظر خود است، می‌باشد. در صورتی‌که مقدار THT مثبت باشد، ایستگاه قادربه ارسال قاب‌های منتظر خود است؛ ولی چنانچه مقدار THT منفی باشد، ایستگاه قادر به ارسال قاب‌های منتظر

---

[1] Synchronous Allocation
[2] Target Token Rotation Time
[3] Absolute Maximum Time

خود نمی‌باشد و باید به‌سرعت نشانه را آزاد نماید. تا زمانی که THT مثبت است، ایستگاه قادر به ارسال قاب‌های غیرهمزمان می‌باشد. هنگامی‌که زمان‌سنج فوق صفرشد، ایستگاه باید نشانه را رها نماید.

۳-۷-۳- مشخصات الکتریکی FDDI

FDDI از یک مکانیسم کدگذاری ویژه به نام 4B/5B استفاده می‌کند. در این سیستم هر ۴ بیت داده تبدیل به یک کد ۵ بیتی می‌شوند و سپس با استفاده از روش کد گذاری NRZ-I ارسال می‌گردند. 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 به۵ بیت تبدیل می‌کند؛ طوری‌که بیشتر از ۲ بیت صفر متوالی در آن نباشد. در جدول (۳-۲) کدگذاری 4B/5B نشان داده شده است. از سایر کدهای ۵ بیتی باقی‌مانده که در جدول (۳-۲) وجود ندارند، برای مصارف کنترلی که در جدول (۳-۳) نشان داده شده است استفاده می‌شود.

جدول (۳-۲): کدگذاری 4B/5B در FDDI

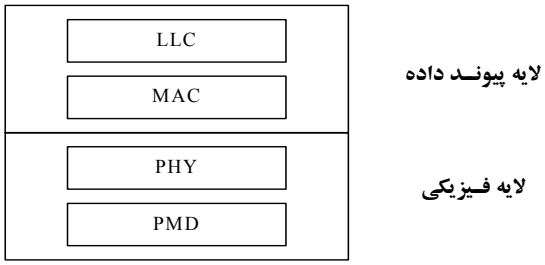
رشته بیت ورودی	رشته بیت رمزشده
۰۰۰۰	۱۱۱۱۰
۰۰۰۱	۰۱۰۰۱
۰۰۱۰	۱۰۱۰۰
۰۰۱۱	۱۰۱۰۱
۰۱۰۰	۰۱۰۱۰
۰۱۰۱	۰۱۰۱۱
۰۱۱۰	۰۱۱۱۰
۰۱۱۱	۰۱۱۱۱
۱۰۰۰	۱۰۰۱۰
۱۰۰۱	۱۰۰۱۱
۱۰۱۰	۱۰۱۱۰
۱۰۱۱	۱۰۱۱۱
۱۱۰۰	۱۱۰۱۰
۱۱۰۱	۱۱۰۱۱
۱۱۱۰	۱۱۱۰۰
۱۱۱۱	۱۱۱۰۱

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[1])
۱۱۰۰۰	J (مورد استفاده درفاصل شروع)
۱۰۰۰۱	K (مورد استفاده در فاصل شروع)
۰۱۱۰۱	T (مورد استفاده در فاصل پایان)
۱۱۰۰۱	S (تنظیم)
۰۰۱۱۱	R (آغاز دوباره)

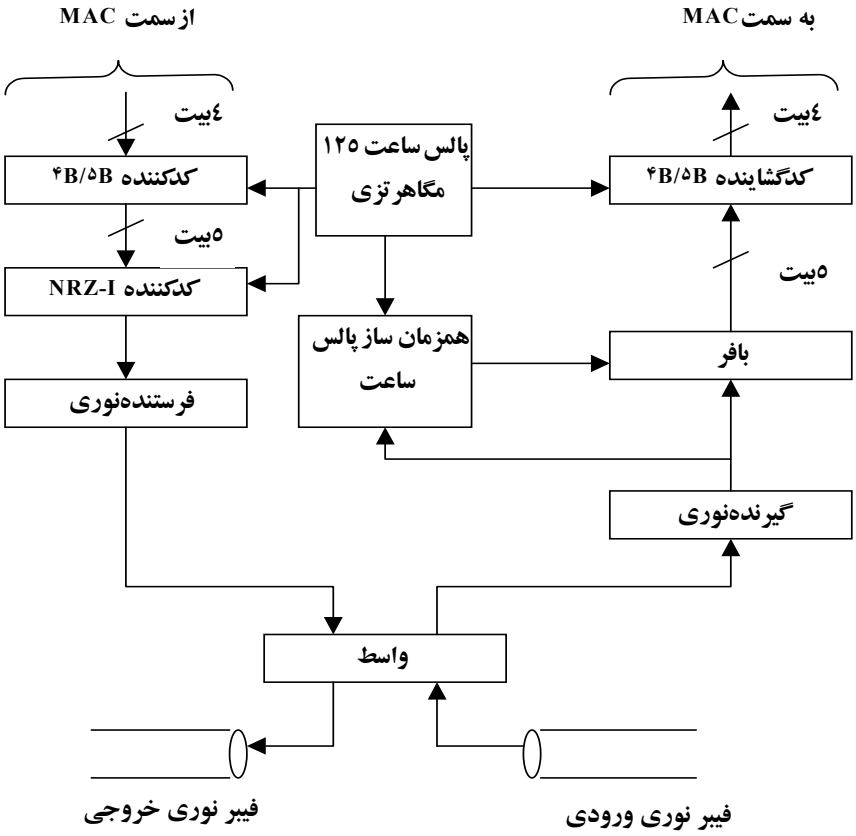
[1] Halt

در شکل (۳-۳۳) ساختار لایه‌ای FDDI نشان داده شده است. همان‌طور که در شکل دیده می‌شود. لایه فیزیکی FDDI ، به دو زیر لایه PHY و PMD تجزیه می‌شود. همچنین لایه پیوند داده، در FDDI ، از دو زیرلایه LLC و MAC تشکیل شده است. زیر لایه LLC در FDDI ، مشابه زیرلایه LLC تعریف شده در پروتکل IEEE 802.2 است. همچنین زیرلایه MAC در FDDI مشابه زیرلایه فوق در شبکه حلقه نشانه است، با این تفاوت که ساختار قاب‌های FDDI با قاب‌های حلقه نشانه متفاوت است.



شکل (۳-۳۳) : ساختار لایه ای FDDI

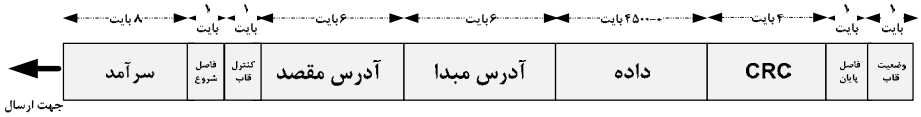
درشکل (۳-۳۴) بلوک دیاگرام واسط فیزیکی درFDDI نشان داده شده است.



شکل (۳-۳۴) : ساختار واسط فیزیکی FDDI

در شکل (۳-۳۵) ساختار قاب‌های MAC ، در شبکه FDDI نشان داده شده است. مطابق شکل فوق در قاب‌های FDDI فیلدهای زیر موجود می‌باشد.

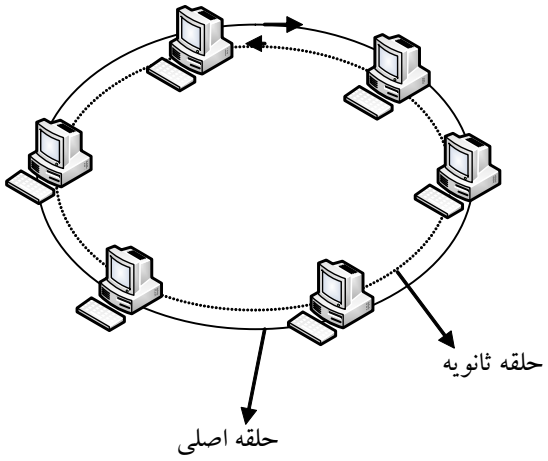
- ***فیلد سرآمد:*** این فیلد ۸ بایتی برای همزمانی پالس ساعت گیرنده با فرستنده به کار می‌رود.
- ***فیلد فاصل شروع:*** این فیلد نشان دهنده شروع قاب FDDI می‌باشد که به‌صورت کدهای متوالی J و K که در جدول (۳-۳) آورده شده است، می‌باشد.
- ***فیلد کنترل قاب :*** این فیلد نشان دهنده نوع قاب است.
- ***فیلد آدرس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



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

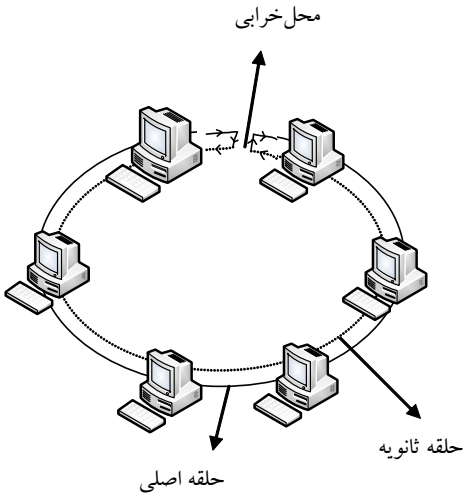
۳-۷-۳-۱- زیر لایه PMD

توسط زیر لایه PMD ، اتصال‌های لازم و تجهیزات الکترونیکی شبکه FDDI تعریف می‌گردد . مشخصات این زیر لایه، براساس این‌که محیط ارسال فیبرنوری و یا کابل مسی باشد، تعیین می‌شود. همان‌طور که در شکل (۳-۳۶) دیده می‌شود، FDDI از دو حلقه به نام‌های حلقه اصلی و حلقه ثانویه استفاده می‌کند. چنانچه حلقه اصلی دچار اشکال گردد، ازحلقه ثانویه استفاده می‌شود.



شکل (۳-۳۶): حلقه ها در شبکه‌های FDDI

شکل (۳-۳۷) ساختار حلقه FDDI بعد از وقوع خرابی در حلقه اصلی را نشان می‌دهد. هر ایستگاه شبکه از طریق دو درگاه فیبرنوری که بر روی کانکتور واسط محیط (MIC[1]) نصب می‌شود، به حلقه‌های اصلی و ثانویه متصل می‌گردد.

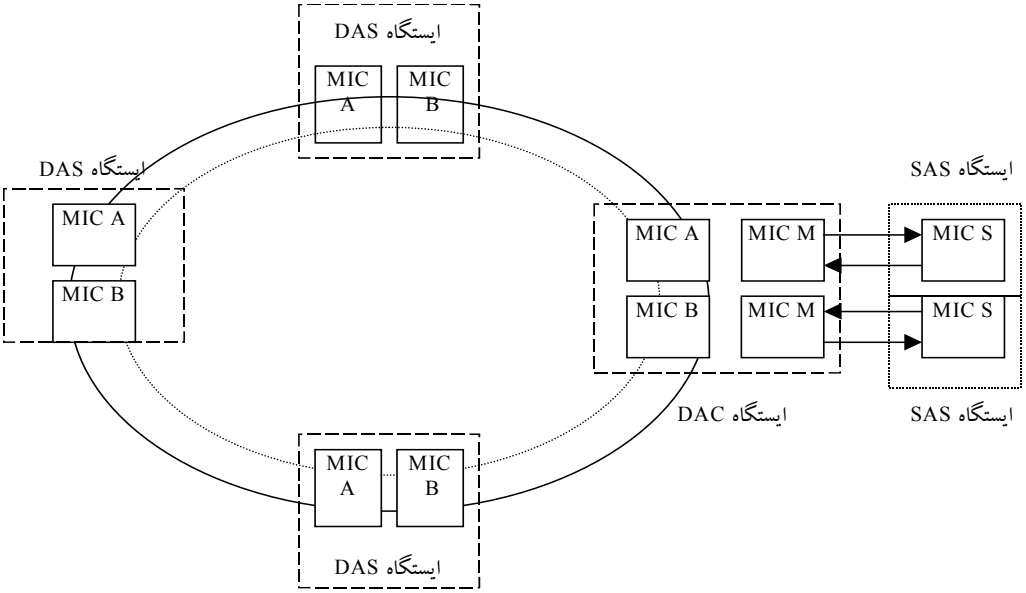


شکل (۳-۳۷) : ساختار حلقه‌های FDDI **بعد از وقوع خرابی**

در FDDI ، سه نوع ایستگاه وجود داردکه عبارتند از: ایستگاه‌های DAC[2]، DAS[3] وSAS[4] . در شکل (۳-۳۸) این نوع ایستگاه ها نشان داده شده است . ایستگاه‌های از نوع DAS ، دارای دو MIC می‌باشند که از طریق آنها به هر دو حلقه اصلی و ثانویه متصل می‌باشند. چنانچه خطایی درحلقه اصلی به‌وجودآید، ایستگاه‌های DAS به‌طوراتوماتیک ارسال اطلاعات را از

[1] Medium Interface Connector
[2] Dual Attachment Concentrator
[3] Dual Attachment Station
[4] Single Attachment Station

طریق MIC دوم خود که به حلقه ثانویه متصل است ادامه می دهند. اکثرایستگاه‌های کاری، خدمات دهنده های شبکه و میکروکامپیوترهای شبکه FDDI به‌صورت DAS عمل می‌کند . ایستگاه‌های SAS فقط یک MIC دارند و بنابراین فقط می‌توانند به یک حلقه متصل شوند. این ایستگاه‌ها به جای آن‌که مستقیماً به حلقه FDDI وصل شوند، به نودهای میانی DAC متصل می‌گردند . ایستگاه DAC موظف به فراهم سازی اتصال به هر دو حلقه شبکه می‌باشد. چنانچه ایستگاهی معیوب گردد، برای جلوگیری از قطع حلقه، ایستگاه از حلقه کنار زده می‌شود.



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

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

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

جدول (۳-۴): مقایسه انواع فن‌آوری‌های شبکه‌های 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	۱۰و ۱۶ مگابیت بر ثانیه	بله
FDDI	عبور نشانه	۶ بایت	4B/5B	۱۰۰ مگابیت برثانیه	بله

۳-۱۰- پروتکل‌های لایه پیوند داده

پروتکل‌های لایه پیوند داده به دو دسته تقسیم می‌شوند که عبارتند از: پروتکل‌های همزمان و پروتکل‌های غیرهمزمان. در پروتکل‌های غیرهمزمان هر بایت به همراه بیت های شروع و پایان، دررشته بیت ارسالی انتقال می‌یابد؛ اما در

پروتکل‌های همزمان کل رشته بیت ارسالی در قالب قاب‌هایی با طول مشخص ارسال می‌گردد. اکثرمودم‌های امروزی از پروتکل‌های غیرهمزمان استفاده می‌کنند،که برخی از مهمترین این پروتکل‌ها عبارتند از Xmodem، Ymodem، Zmodem، Blast و Kermit. پروتکل‌های غیرهمزمان از پیچیدگی زیادی برخوردار نمی‌باشند و پیاده‌سازی آنها نسبتاً ساده وکم خرج می‌باشد. دراین پروتکل‌ها همان‌طور که قبلاً اشاره گردید هر بایت ارسالی به همراه بیت شروع، بیت پایان و بیت توازن ارسال می‌شود. درپروتکل‌های غیرهمزمان، گیرنده باید شروع و پایان هر بایت را با کمک بیت‌های شروع و پایان تشخیص دهد.

پروتکل‌های همزمان از سرعت بسیار بالایی نسبت به پروتکل‌های غیرهمزمان برخوردار می‌باشند. بدین علت از این پروتکل‌ها اغلب در شبکه‌های محلی، شبکه‌های شهری و شبکه‌های گسترده استفاده می‌شود. پروتکل‌های همزمان به دو دسته مختلف به نام پروتکل‌های کاراکترگرا[1] و پروتکل‌های بیت گرا[2] تقسیم‌بندی می‌شوند. تفاوت عمده دو روش فوق، درنحوه همزمانی درکاراکتر و قاب می‌باشد. پروتکل های کاراکترگرا برای ارسال حجم زیادی از اطلاعات نظیر فایل های اسکی استفاده می‌شوند. ازآنجایی‌که درپروتکل های ارسال همزمان، به اول و آخر هربایت، بیتهای شروع و پایان اضافه نمی‌شود، بنابراین برای نیل به همزمانی کاراکتر و قاب، ازکاراکترهای خاصی دراول و آخر قاب برای نشان دادن شروع وپایان هر قاب استفاده می‌شود. درشکل (۳-۳۹) نمونه ای از پروتکل کاراکتر گرا نشان داده شده است.

SYN	SYN	STX	داده	ETX

شکل (۳-۳۹) : نمونه ای ازیک قاب پروتکل کاراکترگرا

مطابق با شکل فوق، درپروتکل های کاراکترگرا، درابتدای قاب ازدوبایت SYN برای همزمان سازی گیرنده با شروع قاب ارسالی استفاده می‌گردد. کاراکتر STX[3] برای تعیین شروع قاب و کاراکتر ETX[4] برای مشخص سازی پایان قاب استفاده می‌شوند. گیرنده با تشخیص کاراکتر SYN، وارد مد شکار شده ومنتظر دریافت کاراکترSTX می‌شود. بعد از تشخیص کاراکترSTX، گیرنده تا دریافت کاراکتر ETX، بایت به بایت اطلاعات موجود درقاب را دریافت می‌کند. یکی از مشکلات این روش، امکان وجود بایت ETX درقسمت داده قاب می‌باشد. با توجه به این‌که اطلاعات موجود درناحیه داده قاب پروتکل های کاراکترگرا ازلایه های بالاتر دریافت می‌شود، این امکان وجود دارد که دراین ناحیه کاراکتری با کد مشابه با ETX وجود داشته باشد. دراین صورت گیرنده آن را با کاراکتر ETX پایان قاب اشتباه تشخیص داده، که موجب عدم تشخیص درست اطلاعات می‌شود. برای حل این مشکل، مطابق با آنچه که درشکل (۳-۴۰) نشان داده شده است، درابتدا و انتهای هرقاب، قبل از کاراکترهای کنترلی STX و ETX، از کاراکتر DLE استفاده می‌گردد. همچنین چنانچه درناحیه داده های قاب، کاراکترDLE جزو اطلاعات ارسالی باشد، قبل از آن نیز یک DLE دیگراضافه می‌شود. به این روش ، میان گذاری بایت[5] گفته می‌شود.

SYN	SYN	DLE	STX	داده	DLE	ETX

[1] Character oriented
[2] Bit oriented
[3] Start of Text
[4] End of Text
[5] Character stuffing

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

با توجه به این‌که درروش کاراکترگرا از عملیات میان‌گذاری بایت برای جلوگیری از اشتباه گیرنده درتشخیص نادرست انتهای قاب استفاده می‌شود، این روش برای ارسال فایل های باینری چندان از کارآیی بالایی برخوردار نمی‌باشد. 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 می‌باشند. دراین پروتکل‌ها شروع و پایان هرقاب، بایک کاراکتر خاص به نام کاراکتر پرچم[۱] مشخص می‌گردد. درشکل (۳-۴۱) نمونه ای از ساختار قاب درپروتکل‌های بیت‌گرا نشان داده شده است.

پرچم پایان	**داده**	**پرچم شروع**

شکل (۳-۴۱) : نمونه ای از ساختارقاب درپروتکل های بیت گرا

دلیل نام‌گذاری این پروتکل به بیت گرا، این است که دراین پروتکل رشته بیت دریافتی بیت به بیت برای تشخیص کاراکتر پرچم شروع، کاراکترهای ناحیه داده قاب و پرچم پایان جستجو می‌گردد. برای کمک به عملیات همزمان سازی درسمت گیرنده، فرستنده قبل از ارسال قاب، اقدام به ارسال بایت های idle (با کد ۰۱۱۱۱۱۱۱) 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 دربین داده های کاربر می‌باشد. دراین صورت این امکان وجود دارد که گیرنده آن را با پرچم نشان دهنده پایان قاب اشتباه بگیرد. برای حل این مشکل ازروش درج صفر استفاده می‌شودکه در ادامه این فصل هنگام توصیف پروتکل HDLC توضیح داده خواهد شد.

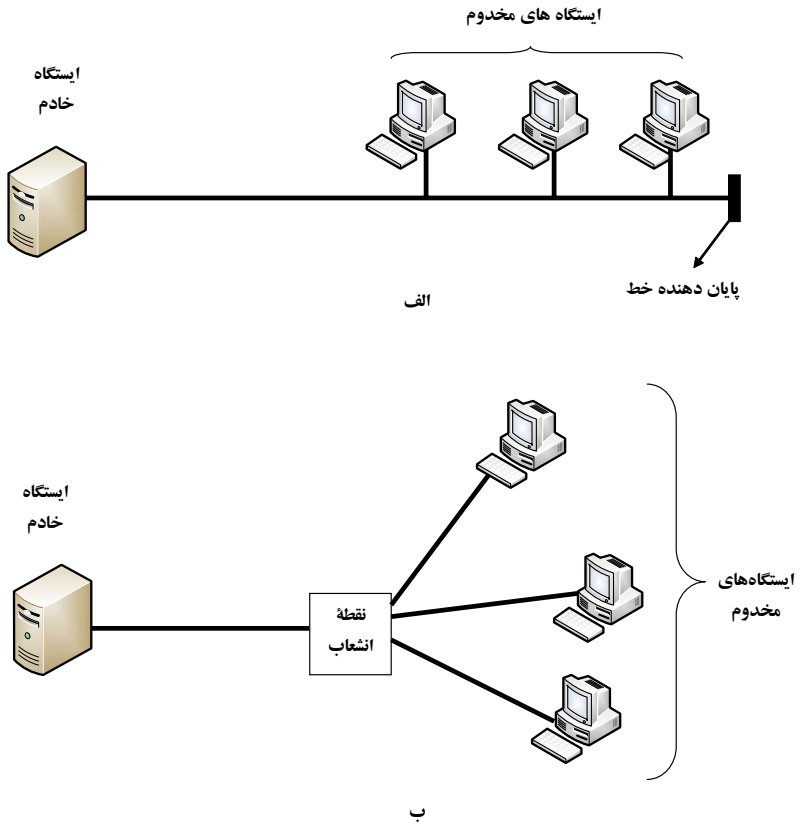
دو پروتکل متداول همزمان عبارتند از: پروتکل ارتباط همزمان باینری (BSC[2]) و پروتکل HDLC. پروتکل BSC از نوع کاراکترگرا می‌باشد و پروتکل HDLC به‌صورت بیت گرا عمل می‌نماید.

۳-۱۰-۱- پروتکل BSC

پروتکل BSC ، یکی از متداولترین پروتکل‌های کاراکترگرا می‌باشد که در سال ۱۹۶۴ توسط شرکت IBM ارائه گردید. از این پروتکل در اتصالهای نقطه به نقطه و نقطه به چند نقطه می‌توان استفاده نمود. پروتکل BSC به‌صورت ارسال یک‌طرفه عمل می‌کندو از روش کنترل جریان توقف و انتظاراستفاده می‌نماید. ازپروتکل BSC معمولاً برای کاربردهای چند نقطه ای که درآن یک ایستگاه خادم[۳] با چندین ایستگاه مخدوم[۴] در ارتباط است استفاده می‌شود. 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



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 نمی‌کند. در جدول(۳-۵) لیست کاراکترهای کنترلی که در پروتکل BSC استفاده می‌شود آورده شده است.

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

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

۳-۱۰-۱-۱- قاب‌های BSC

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 درمواردی 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.

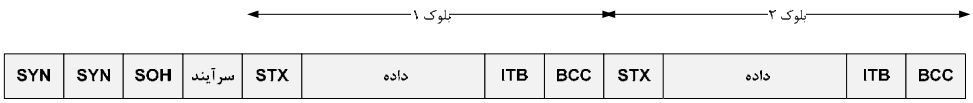
SYN	SYN	STX	داده	ETX	BCC

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

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

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



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

با توجه به این‌که پروتکل BSC از روش یک‌طرفه استفاده می‌کند، بعد از پایان ارسال قاب، کنترل کانال از فرستنده به گیرنده منتقل می‌شود. چنانچه پیام ارسالی بسیار طولانی باشد به‌طوری‌که در داخل یک قاب به تنهایی گنجانده نشود، می‌توان پیام ارسالی را به چندین قاب کوچکتر تجزیه نمود و آنها را ارسال کرد.

همان‌طور که اشاره گردید از قاب‌های کنترلی برای تبادل اطلاعات کنترلی نظیر برقراری و حذف ارتباط، کنترل جریان و کنترل خطا بین دو طرف ارتباط استفاده می‌شود. در شکل (۳-۴۵) ساختار قاب‌های کنترلی در BSC نشان داده شده است.

SYN	SYN	سایر کاراکترهای کنترلی	BCC

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

۳-۱۰-۱-۲- شفافیت داده‌ها[1]

در ابتدا ازپروتکل BSC برای تبادل داده‌های متنی استفاده می‌گردید. امروزه در بسیاری از کاربردها، داده‌های ارسالی از نوع باینری می‌باشند. چنانچه داده‌های ارسالی باینری باشند، این احتمال وجود دارد که یک یا چند بایت در داده‌های ارسالی مطابق با کاراکترهای کنترلی BSC باشند. در این حالت گیرنده در تشخیص و جدا سازی کاراکترهای کنترلی با کاراکترهای داده دچار اشتباه می‌شود. به عنوان مثال چنانچه در رشته بیت ارسالی فرستنده بایت ۰۰۰۰۰۰۰۱ قرار داشته باشد، گیرنده آن را با کاراکتر کنترلی ETX اشتباه خواهد گرفت. از طرفی دیگر یک پروتکل خوب و موفق باید به‌صورت شفاف عمل کند و هیچ‌گونه محدودیتی در رشته بیت ارسالی وضع ننماید. بدین منظورهمان‌طور که قبلاً توضیح داده شد، برای حفظ شفافیت داده‌های ارسالی در BSC از روش میان‌گذاری بایت استفاده می‌شود. در این روش چنانچه در داده‌های ارسالی بایت‌های کنترلی موجود باشد، قبل از کاراکتر STX و ETX دو کاراکتر کنترلی DLE قرار داده می‌شود. گیرنده با مشاهده اولین کاراکتر DLE متوجه می‌شود که در داده‌های ارسالی بایت‌های کنترلی وجود دارد و بدین ترتیب تا دریافت دومین

[1] Data transparency

کاراکترDLE از تمام بایت‌های کنترلی دریافتی صرف‌نظر می‌کند. در شکل (۳-۴۶) نمونه‌ای از علمیات میان‌گذاری بایت نشان داده شده است.

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

۳-۱۰-۲ - پروتکل HDLC

در پروتکل‌های کاراکترگرا بیت‌های ارسالی به‌صورت الگوهای از قبل تعریف شده گروه بندی می‌شوند و تشکیل کاراکتر می‌دهند. در مقایسه با پروتکل‌های کاراکترگرا، پروتکل‌های بیت‌گرا قادربه گنجاندن اطلاعات بیشتر در قاب‌های کوتاه‌تر و اجتناب از مشکل شفافیت داده می‌باشند. در طی چند سال گذشته پروتکل‌های بیت گرای متعددی ارائه شده است که از میان آنها می‌توان به پروتکل هایSDLC ، HDLC ،پروتکل‌های LAP و پروتکل‌های شبکه‌های محلی اشاره نمود. اغلب پروتکل‌های بیت گرا توسط شرکت‌های خصوصی جهت پشتیبانی از محصولات آنها ارائه شده است.

یکی از مهمترین پروتکل‌های بیت‌گرا ،HDLC می‌باشد که توسط سازمان ISO طراحی گردیده است و به عنوان پایه اغلب پروتکل‌های بیت گرای امروزی شناخته می‌شود. 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 می‌باشد تایید کرد. با تایید استاندارد HDLC توسط ISO، سایر مراجع استاندارد گذاری نظیر ITU-T اقدام به تصویب پروتکل‌هایی نظیر پروتکل‌های LAP (LAPB , LAPD , LAPM و LAPX) نمودند. تمامی این پروتکل‌ها توسعه یافته پروتکل HDLC می‌باشند. همچنین پروتکل‌های Frame relay و PPP که توسط ITU-T و ANSI توسعه یافتند، بر اساس HDLC طراحی شده‌اند. بنابراین با توجه به اهمیت HDLC به بررسی این پروتکل می‌پردازیم.

پروتکل استاندارد HDLC ، یک پروتکل اتصال گرا می‌باشد که قادر به عملکرد یک‌طرفه و دو طرفه بر روی خطوط نقطه به نقطه و نقطه به چند نقطه می‌باشد. ایستگاه‌ها در پروتکل HDLC ، به سه دسته اولیه[۱] ثانویه[۲] و ترکیبی[۳] تقسیم‌بندی می‌شوند. ایستگاه اولیه در HDLC اقدام به ارسال پیام‌های دستور به ایستگاه‌های ثانویه می‌نماید. ایستگاه‌های ثانویه نیز در جواب به پیام دستور اقدام به ارسال پیام پاسخ می‌نمایند. به‌عنوان مثال ارتباط کامپیوتر با پایانه، نمونه‌ای از ارتباط ایستگاه اولیه به ایستگاه ثانویه در HDLC می‌باشد. ایستگاه ترکیبی قادر به ارسال پیام‌های دستور و پاسخ‌های آنها نیز می‌باشد.

بر اساس جهت مبادله اطلاعات، ایستگاه‌های ترکیبی در HDLC می‌توانند هم به‌صورت ایستگاه اولیه و هم به‌صورت ایستگاه ثانویه عمل نمایند. در HDLC ایستگاه‌های اولیه، ثانویه و ترکیبی به سه صورت مختلف پیکره‌بندی می‌شود این سه ترکیب مختلف عبارتند از غیربالانس، متقارن و بالانس. در شکل (۳-۴۷) این سه نوع پیکره‌بندی HDLC نشان داده شده

---

[۱] Primary
[۲] Secondary
[۳] Combined

است. در پیکره‌بندی غیربالانس که به پیکره‌بندی خدمات دهنده/ خدمات گیرنده نیز نامیده می‌شود، یک ایستگاه به‌صورت اولیه و سایر ایستگاه‌ها به‌صورت ثانویه عمل می‌نمایند. پیکره‌بندی غیربالانس هم به‌صورت نقطه به نقطه و هم به‌صورت نقطه به چند نقطه عمل می‌کند.

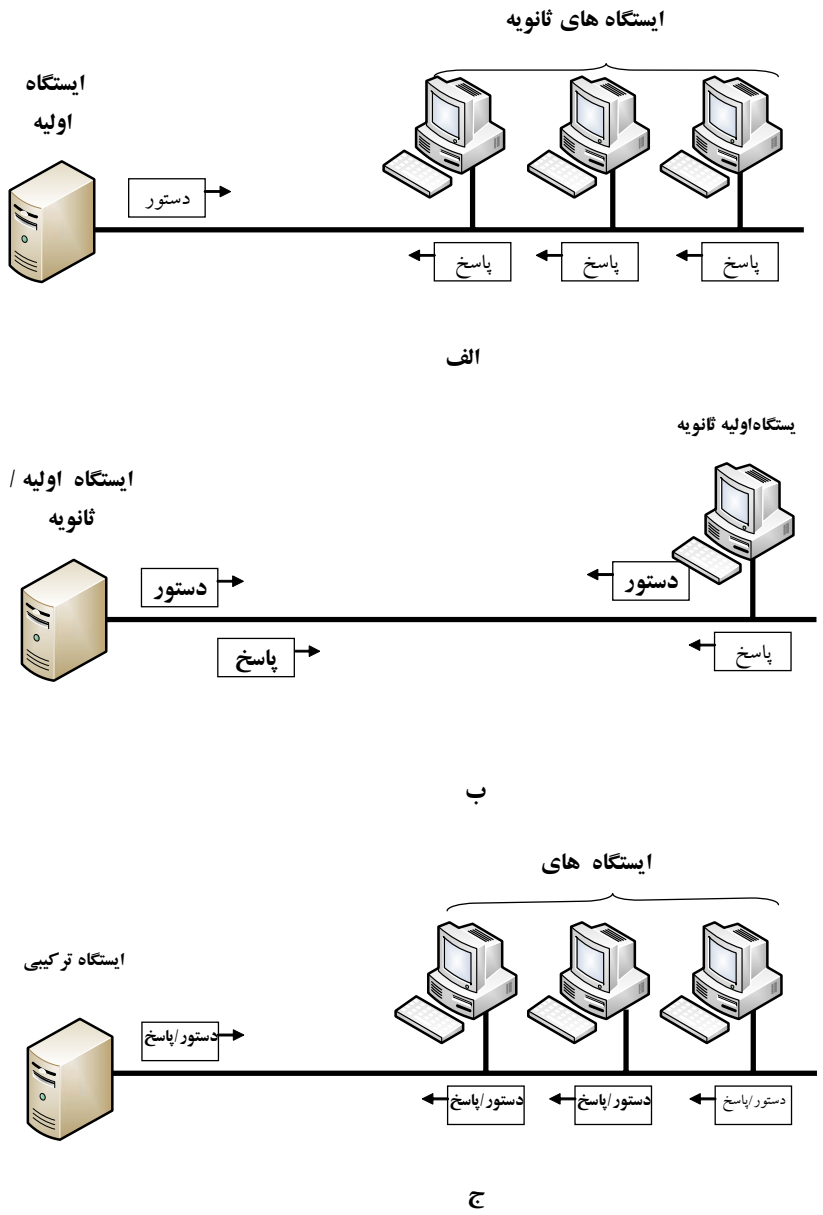
در پیکره‌بندی متقارن، هر ایستگاه فیزیکی به‌طور منطقی از دو ایستگاه اولیه و ثانویه تشکیل شده‌است. کانال‌های مجزایی ایستگاه‌های اولیه و ثانویه را به یکدیگر متصل می‌نمایند. این نوع پیکره‌بندی مشابه پیکره‌بندی غیربالانس می‌باشد. با این تفاوت که کنترل کانال و جهت ارسال پیام‌های دستور و پاسخ می‌تواند بین دو ایستگاه فیزیکی تغییر نماید.

در پیکره‌بندی بالانس هر دو ایستگاه در اتصال‌های نقطه به نقطه از نوع ایستگاه ترکیبی می‌باشند. برخلاف پیکره‌بندی متقارن در این نوع پیکره‌بندی فقط از یک کانال برای اتصال ایستگاه‌ها استفاده می‌شود. جهت ارسال پیام در کانال توسط هر دو ایستگاه قابل کنترل می‌باشد. پروتکل HDLC قادر به پشتیبانی از پیکره‌بندی بالانس چند نقطه‌ای نمی‌باشد، ولی سایر انواع پیکره‌بندی که اشاره گردید توسط HDLC پشتیبانی می‌شود.

برای کنترل کانال در HDLC سه مد ارتباطی متفاوت بین ایستگاه‌ها وجود دارند که عبارتند از:

- مدپاسخ 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



شکل(۳-۴۷): انواع پیکره‌بندی در پروتکل HDLC

الف) غیربالانس ب) متقارن ج) بالانس

- **NRM**: این مد ارتباطی در پیکره‌بندی غیربالانس به‌کارمی رود. در این مد، 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 می‌باشد. از کانال‌های نقطه به نقطه و یا چند نقطه دراین مد ارتباطی استفاده می‌شود.
- **ARM** : این مد ارتباطی در پیکره‌بندی غیربالانس به کارمی رود. در این مد، ایستگاه ثانویه هنگامی‌که کانال خالی می‌باشد، قادر به ارسال اطلاعات بدون مجوز از ایستگاه اولیه است. در این حالت تمام اطلاعات ارسالی ایستگاه‌های ثانویه، حتی بین خودشان باید از طریق ایستگاه اولیه عبور داده شود. دراین مد ارتباطی از کانال‌های دوطرفه نقطه به نقطه استفاده می‌شود.

- **ABM**: در مد ABM تمام ایستگاه‌ها یکسان می‌باشند و بنابراین ایستگاه‌های ترکیبی که به‌صورت نقطه به نقطه به یکدیگر متصل شده‌اند، استفاده می‌شوند. هر کدام از ایستگاه‌های ترکیبی بدون نیاز به کسب مجوز قادر به ارسال می‌باشند. دراین مد ارتباطی از کانال‌های دوطرفه نقطه به نقطه استفاده می‌شود. در جدول (۳-۶) ارتباط بین مدهای فوق و انواع ایستگاه‌های HDLC نشان داده شده است.

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

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

۳-۱۰-۲-۱- قاب‌های HDLC

جهت فراهم سازی انعطاف پذیری لازم برای پشتیبانی انواع مدهای HDLC، سه نوع قاب به نامهای قاب‌های اطلاعاتی، قاب‌های نظارتی و قاب‌های بدون شماره وجود دارد. درشکل (۳-۴۸) انواع قاب‌های HDLC نشان داده شده است. از قاب‌های اطلاعاتی برای ارسال داده‌های کاربر و اطلاعات کنترلی مربوط به داده‌های کاربر استفاده می‌شود. از قاب‌های نظارتی برای مبادله اطلاعات کنترلی، کنترل جریان و کنترل خطا استفاده می‌گردد. قاب‌های بدون شماره برای مدیریت سیستم به‌کار می‌روند.

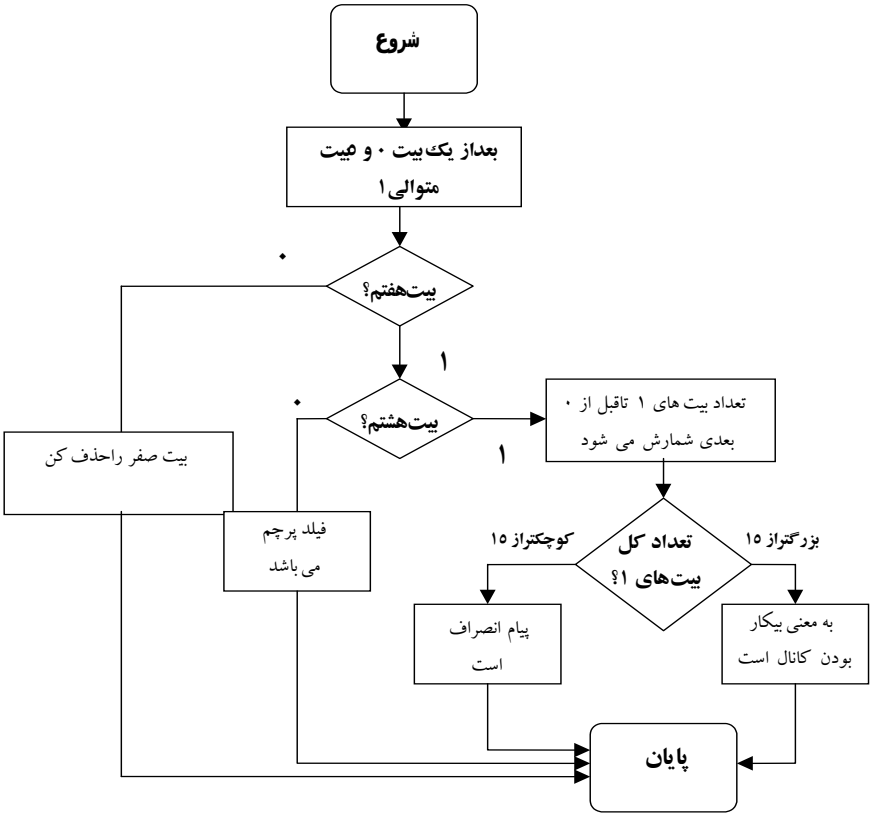
شکل(۳-۴۸): انواع قاب ها در پروتکل HDLC
الف) قاب‌های اطلاعاتی ب) قاب‌های نظارتی ج) قاب‌های بدون شماره

همان‌طور که در شکل ۳-۴۸ دیده می‌شود قاب‌های HDLC از فیلدهای زیر تشکیل شده اند:

- فیلد پرچم: ***فیلد پرچم در HDLC ،که شامل رشته بیتی ۰۱۱۱۱۱۱۰ می‌باشد، شروع و پایان قاب را مشخص می‌کندو برای همزمانی فرستنده با گیرنده استفاده می‌شود. برای تضمین عدم وجود فیلد پرچم در بخش داده قاب‌های HDLC ، از عملیات درج صفراستفاده می‌شود. درسمت فرستنده، بعد از هر۵ بیت ۱ متوالی یک بیت ۰ اضافه می‌گردد. به عنوان مثال رشته بیت۰۱۰۱۱۱۱۱۱۰۱۰ تبدیل به رشته بیت ۰۱۰۱۱۱۱۱۰۱۰۱۰ می‌شود. در سمت گیرنده نیز ۰ بعد از ۵ بیت ۱ حذف می‌شود. در شکل (۳-۴۹)***

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

- فیلد آدرس: ***دومین فیلد در قاب‌های HDLC، مشخص‌کننده آدرس ایستگاه که می‌تواند ایستگاه اولیه یا ایستگاه ثانویه باشد، است. درحالتی که فرستنده قاب،ایستگاه اولیه باشد، فیلد آدرس مشخص کننده آدرس ایستگاه ثانویه که بایدپیام را دریافت نماید، است؛ ولی درحالتی که ایستگاه ثانویه فرستنده قاب است، فیلد آدرس، مشخص کننده آدرس ایستگاه ثانویه که فرستنده قاب است، می‌باشد.***



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

- *فیلد کنترل:* **از این فیلد که دارای یک یا دو بایت است، برای مدیریت جریان ترافیکی استفاده می‌شود. بر اساس نوع قاب، محتویات فیلد کنترل متفاوت است. چنانچه اولین بیت فیلد کنترل صفر باشد، قاب از نوع اطلاعاتی است. درصورتی‌که دو بیت اول فیلد کنترل ۱۰ باشند، قاب از نوع نظارتی می‌باشد و چنانچه دو بیت اول در فیلد کنترل ۱۱ باشند، قاب از نوع بدون شماره می‌باشد. فیلد کنترل درهرسه نوع قاب HDLC ، شامل بیتی به نام بیت P/F[1] می‌باشد. این بیت برای دو منظور متفاوت استفاده می‌شود و در صورتی معتبر است که مقدار آن ۱ باشد. هنگامی‌که قاب از سمت ایستگاه اولیه به سمت ایستگاه ثانویه ارسال می‌گردد، این بیت مفهوم سرکشی می‌دهد و در صورتی‌که قاب از سمت ثانویه به اولیه ارسال شود، مفهوم آن پایان است. فیلد کنترل در قاب‌های اطلاعاتی شامل دو فیلد سه بیتی N(S)**

[1] Pool/Final

و N(R) می‌باشد. این دو فیلد برای کنترل جریان استفاده می‌شوند. N(S) نشان دهنده شماره قاب ارسالی و N(R) نشان دهنده شماره قابی که ایستگاه، انتظار دریافت آن را از طرف مقابل دارد، می‌باشد. با توجه به این‌که در قاب‌های نظارتی، هیچ‌گونه داده‌ای مبادله نمی‌شود، بنابراین فیلد کنترل در قاب‌های نظارتی فقط حاوی فیلد N(R) می‌باشد. در قاب‌های نظارتی فیلد کنترل شامل دو بیت فیلد کد نیز می‌باشند که از این دو بیت برای حمل اطلاعات کنترل خطا استفاده می‌شود. قاب‌های بدون شماره نه حاوی N(S) و نه حاوی N(R) می‌باشند بنابراین از آنها نه برای ارسال داده و نه برای ارسال پیام تصدیق استفاده می‌شود. در عوض قاب‌های بدون شماره حاوی دو فیلد دو بیتی و سه بیتی به‌عنوان کد می‌باشند که از آنها برای مشخص نمودن نوع قاب بدون شماره و عملیات آن استفاده می‌شود.

- *فیلد اطلاعات:* **یکی دیگر از فیلدهای موجود در قاب‌های HDLC ، فیلد اطلاعات می‌باشد که برای حمل داده‌های کاربر در قاب‌های اطلاعاتی و داده‌های مدیریت شبکه در قاب‌های بدون شماره استفاده می‌شود. طول فیلد اطلاعات در شبکه‌های مختلف، متغیر می‌باشد ولی معمولاً در هر شبکه طول این فیلد ثابت است. باید توجه نمود که قاب‌های نظارتی شامل هیچ‌گونه فیلد اطلاعاتی نمی‌باشند.**
- ***فیلد کنترل ترتیب قاب* (FCS):** از این فیلد دو یا چهار بایتی به منظور تشخیص خطا در قاب‌های HDLC استفاده می‌شود.

۳-۱۰-۲-۲- انواع قاب‌های HDLC

همان‌طور که اشاره شد HDLC دارای سه نوع قاب اطلاعاتی، نظارتی و بدون شماره می‌باشد. از قاب‌های نظارتی برای ارسال پیام تصدیق، کنترل جریان و کنترل خطا استفاده می‌گردد. نوع هر قاب نظارتی توسط دو بیت کد مشخص می‌شود. در جدول (۳-۷) انواع قاب‌های نظارتی آورده شده‌اند.

جدول(۳-۷): انواع قاب‌های نظارتی درHDLC

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 قاب‌های نظارتی در HDLC عبارتند از:

- ***قاب RR:*** از این قاب برای چهارعمل متفاوت استفاده می‌شود که عبارتند از:

الف) تصدیق: هنگامی‌که گیرنده هیچ داده‌ای برای ارسال نداشته باشد، برای تصدیق دریافت سالم قاب‌های ورودی از این قاب استفاده می‌کند. در این حالت فیلد N(R) در قسمت کنترل قاب نشان دهنده شماره قاب بعدی که گیرنده منتظر دریافت آن است می‌باشد.

ب) سرکشی: هنگامی‌که ایستگاه اولیه اقدام به ارسال قاب RR که در آن بیت P/F برابر ۱ است می‌کند عملاً از ایستگاه ثانویه سؤال می‌نماید که آیا داده‌ای برای ارسال دارد یا خیر؟

ج) پاسخ منفی به سرکشی: هنگامی‌که قاب RR توسط ایستگاه ثانویه با بیت P/F مساوی ۱ارسال شود، به‌وسیله آن ایستگاه ثانویه به ایستگاه اولیه اعلام می‌دارد که هیچ داده‌ای برای ارسال ندارد.

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

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

- ***قاب RNR:*** از این قاب‌ها برای سه منظور متفاوت به‌صورت زیر استفاده می‌شود:

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

ب) انتخاب: هنگامی‌که ایستگاه اولیه بخواهد داده‌ای را برای ایستگاه ثانویه ارسال دارد با ارسال یک قاب RNR که بیت P/F آن ۱ می‌باشد، ایستگاه ثانویه را مطلع می‌سازد. با ارسال این قاب عملاً به ایستگاه ثانویه گفته می‌شود که داده‌های خود را برای ایستگاه اولیه ارسال نکند.

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

- ***قاب REJ:*** سومین نوع قاب‌های نظارتی قاب REJ می‌باشد. گیرنده هنگامی‌که هیچ داده‌ای برای ارسال نداشته باشد، از این قاب به عنوان یک پیام تصدیق منفی در حالت کنترل خطا به‌صورت بازگشت به عقب به اندازه N استفاده می‌کند. 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 به‌صورت رد انتخابی استفاده می‌شود. این قاب توسط گیرنده به فرستنده ارسال می‌شود 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.

قاب‌های بدون شماره

از این قاب‌ها برای مبادله اطلاعات مدیریت جلسه و اطلاعات کنترلی بین ایستگاه‌ها استفاده می‌شود. برخلاف قاب‌های نظارتی، قاب‌های بدون شماره، حاوی فیلد اطلاعات می‌باشند؛ اما از این اطلاعات فقط برای مدیریت سیستم استفاده می‌شود و هیچ‌گونه داده کاربردرآن وجود ندارد. انواع قاب‌های بدون شماره توسط فیلدهای ۵ بیتی کد مشخص می‌شود. حداکثر می‌توان ۳۲ قاب بدون شماره مشخص نمود. از این قاب‌ها برای عملیاتی نظیر تنظیم مد، مبادله بدون شماره، قطع اتصال، مقدار دهی اولیه و سایر موارد دیگر استفاده می‌شود. درجدول (۳-۸) انواع قاب‌های بدون شماره آورده شده است.

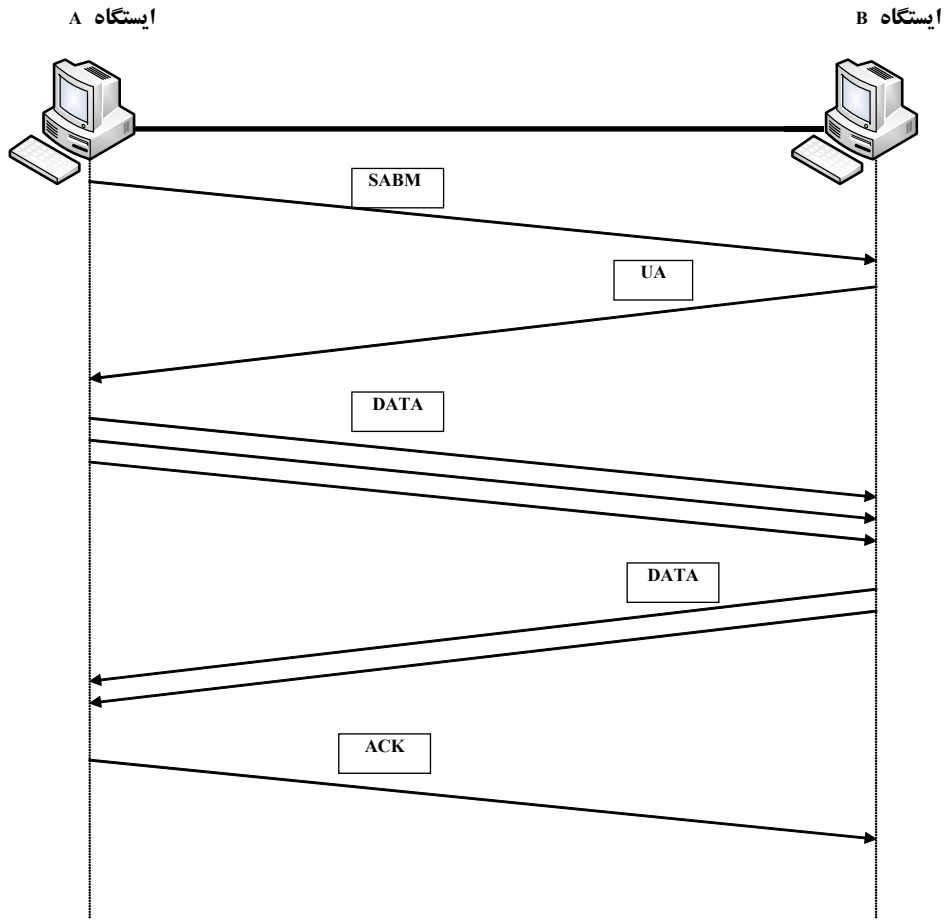
در شکل (۳-۵۰) مثالی از ارتباط همتا به همتا بین دو ایستگاه A و B با استفاده از پروتکل HDLC آورده شده است. مطابق با این شکل، ابتدا ایستگاهA برای برقراری ارتباط درحالت بالانس غیرهمزمان (ABM) یک قاب بدون شماره (SABM) برای ایستگاه B ارسال می‌دارد. در قاب ارسالی بیت P برابر۱ می‌باشد که نشان دهنده این است که ایستگاه A خواهان کنترل جلسه و ارسال زودتراست. در پاسخ، ایستگاهB با ارسال قاب بدون شماره از نوع UA که بیت F آن ۱می‌باشد، درخواست A را می‌پذیرد. از آن‌جایی‌که با توافق دو طرف حالت ارسال به‌صورت بالانس غیرهمزمان است، بنابراین هردو ایستگاه از نوع ترکیبی می‌باشند و بیت P/F اعتبارخود را از دست می‌دهد. بعد از تنظیم حالت ارتباط، دوایستگاه برای یکدیگرقاب‌های اطلاعاتی ارسال می‌دارند.

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

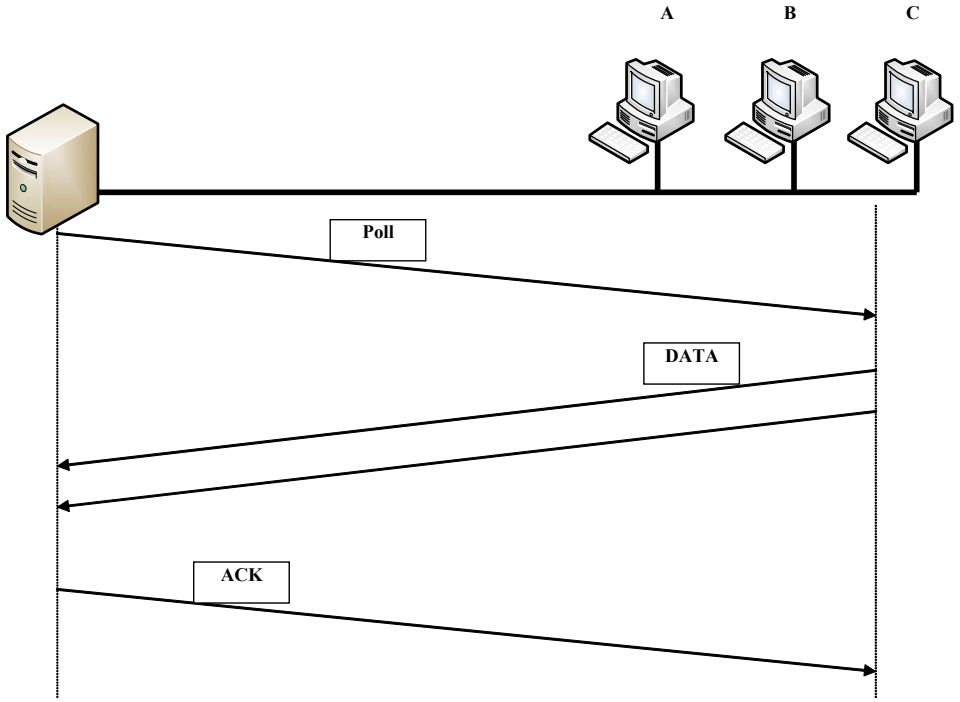
دستور/ پاسخ	عملیات
SNRM	تنظیم حالت NRM
SNRME	تنظیم حالت NRM (توسعه یافته)
SARM	تنظیم حالت ARM
SARME	تنظیم حالت ARM (توسعه یافته)
SABM	تنظیم حالت ABM
SABME	تنظیم حالت ABM (توسعه یافته)
UP	سرکشی بدون شماره
UI	اطلاعات بدون شماره
UA	پیام تصدیق بدون شماره
RD	درخواست قطع ارتباط
DISC	قطع ارتباط
DM	حالت قطع
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 می‌خواهد که داده‌های خود را ارسال دارد. ایستگاه A دو قاب به شماره‌های ۰ و ۱ برای ایستگاه اولیه ارسال می‌کند. در آخرین قاب ارسالی بیت F مساوی ۱ می‌باشد که نشان دهنده پایان ارسال اطلاعات است. ایستگاه اولیه با ارسال یک قاب نظارتی از نوع RNR به ایستگاه A اعلام می‌دارد که قاب‌های شماره ۰ و۱ آن را دریافت نموده است.



شکل (۳-۵۰): مثالی از برقراری ارتباط همتابه همتا درحالت ABM در HDLC



شکل (۳-۵۱) : مثالی از عملیات سرکشی دراتصالات 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 زمان‌سنج در روش توقف و انتظار توضیح دهید.
۴. معایب و مزایای روش توقف وانتظار را بنویسید.
۵. روش پنجره لغزان را با ذکر مثالی توصیف نمایید.
۶. تفاوت روش‌های بازگشت به عقب به اندازه N و روش تکرار انتخابی را توضیح دهید.
۷. علت استفاده از زمان‌سنج برای هر قاب در روش پنجره لغزان را بنویسید.
۸. برتری و نقاط ضعف روش پنجره لغزان را نسبت به روش توقف وانتظار تشریح نمایید.
۹. وظیفه زیر لایه کنترل دسترسی به محیط (MAC) را درشبکه‌های محلی بنویسید.
۱۰. انواع روش های کنترل دسترسی به محیط را نام برده و هریک را توضیح دهید.
۱۱. ویژگی‌های 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 صددرصد مصّر،P درصد مصّر و غیرمصّر را توضیح داده و بایکدیگرمقایسه نمایید.
۱۶. درپروتکل P CSMA ، درصد مصّر با افزایش مقدار P، نحوه تغییرات میزان تداخل و بهره وری از کانال را توضیح دهید.
۱۷. عملکرد پروتکل CSMA/CD وتفاوت آن را با CSMA توضیح دهید.
۱۸. سه وضعیت کاری پروتکل CSMA/CD را نام برده و توضیح دهید.
۱۹. استانداردهای IEEE برای شبکه‌های 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 دراترنت توضیح دهید.
۲۳. عملکرد شبکه‌های 100BaseT را توضیح داده و برتری‌های آن را نسبت به اترنت معمولی تشریح نمایید.
۲۴. کاربرد کابل AUI درشبکه‌های اترنت سخت را توضیح داده و تعداد زوج سیم‌های آن و عملکرد هر زوج سیم را توصیف کنید.
۲۵. وظایف کارت شبکه (NIC) را درشبکه‌های اترنت توضیح دهید.
۲۶. نحوه گسترش شبکه‌های 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 زیرلایه MAC اترنت را نوشته و عملکرد هر فیلد آن را توصیف نمایید.
۲۹. الگوریتم عقب‌گرد توانی دودوئی دراترنت را تشریح نمایید.
۳۰. برتری وجنبه های تمایز اترنت سریع را با اترنت پایه توصیف نمایید.
۳۱. وظایف زیرلایه های PMD و CS را دراترنت سریع بنویسید.
۳۲. انواع استانداردهای اترنت سریع را توصیف نمایید.

۳۳. استانداردهای مختلف گیگا بیت اترنت را نوشته و بایکدیگر مقایسه نمایید.
۳۴. کاربردهای فن‌آوری ۱۰گیگابیت 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 درشبکه‌های گذرگاه نشانه توصیف نمایید.
۳۷. کلاس های ترافیکی مختلف شبکه‌های گذرگاه نشانه و کاربرد هرکلاس ترافیکی را توصیف نمایید.
۳۸. کاربرد زمان‌سنجهای THT و HP-THT را درشبکه گذرگاه نشانه توصیف کنید.
۳۹. تفاوت اساسی که درساختارقاب‌های MAC استاندارد اترنت وگذرگاه نشانه وجود دارد، راذکرنمایید.
۴۰. عملکرد جعبه تقسیم و علت استفاده از آن را درشبکه‌های حلقه نشانه توصیف نمایید.
۴۱. عملکرد ایستگاه ناظر را درشبکه‌های حلقه نشانه توصیف نمایید.
۴۲. کاربرد فیلد وضعیت درساختارقاب‌های MAC شبکه‌های حلقه نشانه را بنویسید.
۴۳. عملکرد ایستگاه‌های پایین جریان، بالا جریان و سر را در شبکه‌های DQDB توصیف نمایید.
۴۴. نحوه عملیات رزرو برش زمانی را درشبکه‌های DQDB توصیف کنید.
۴۵. عملکرد فیلد دسترسی را درساختار قاب‌های DQDB تشریح نمایید.
۴۶. ساختار شبکه‌های SMDS را توصیف نمایید.
۴۷. رجیسترهای FDDI را نام برده وکاربرد هر رجیستر را تشریح نمایید.
۴۸. کاربرد زمان‌سنجهای FDDI را توصیف نمایید.
۴۹. وظایف زیرلایه های PHY و PMD را درشبکه‌های FDDI تشریح نمایید.
۵۰. عملکرد ایستگاه‌های DAC، DAS وSAS را درشبکه‌های FDDI تشریح نمایید.
۵۱. تفاوت پروتکل‌های کاراکترگرا و بیت گرا را بایکدیگر بنویسید.
۵۲. نحوه عملیات میان گذاری بایت را درپروتکل BSC توصیف نمایید.
۵۳. قاب‌های مختلف پروتکل BSC را نام برده و بایکدیگر مقایسه نمایید.
۵۴. ایستگاه‌های اولیه، ثانویه و ترکیبی را درHDLC توصیف نموده تفاوت آنها را با یکدیگر بنویسید.
۵۵. سه مد کاری پاسخ طبیعی (NRM)، پاسخ غیرهمزمان (ARM) ومد با لانس شده غیرهمزمـان (ABM) را درHDLC با یکدیگر مقایسه نمایید.
۵۶. انواع قاب‌های HDLC را نام برده وعملکرد هریک را توصیف نمایید.
۵۷. نحوه عملیات درج صفر را درپروتکل HDLC توصیف کنید.

فصل چهارم

شبکه های بیسیم

۴-۱- مقدمه

فن‌آوری کامپیوتر در چند سال اخیر در زمینه های مختلفی نظیرحجم و قدرت پردازش اطلاعات، ابعاد فیزیکی قطعات کامپیوتر وکاهش قیمت محصولات کامپیوتر، پیشرفت سریعی داشته است. یکی از جنبه‌های پیشرفت سیستم‌های کامپیوتر، قابلیت حمل[1] آنها می‌باشد. امروزه با استفاده ازکامپیوترهای کیفی، کاربران می‌توانند درهرنقطه از دنیا به آخرین اطلاعات دسترسی داشته باشند.

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

امروزه شبکه‌های محلی بیسیم به عنوان یک سیستم همه منظوره که می‌توانند جایگزین مناسبی برای شبکه‌های سیمی باشند، شناخته می‌شوند. در شبکه‌های محلی با سیم، معمولاً ۴۰ درصد کل هزینه نصب شبکه، هزینه کابل کشی آن می‌باشد و چنانچه شبکه نیاز به تغییری داشته باشد، کابل‌کشی باید تغییر نموده که این امر باعث افزایش هزینه می‌گردد. طبیعی است در شبکه‌های محلی بیسیم، هزینه کابل کشی وجود ندارد و در صورت نیاز، ساختار شبکه به راحتی قابل تغییر می‌باشد. از این شبکه‌هادرمحیطهای مختلفی نظیر دفاتر کار، کارخانجات، آزمایشگاههای تحقیقاتی و دانشگاه‌ها می‌توان استفاده نمود. با استفاده از شبکه‌های محلی بیسیم، کاربران شبکه بدون این‌که به نقطه خاصی متصل شوند، قادر به استفاده از منابع مشترک شبکه می‌باشند. همچنین مدیران شبکه قادر به توسعه و تغییر شبکه خود بدون نیاز به سیم کشی می‌باشند.

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 طرحهای مدولاسیون دیجیتال امروزی، تکنیکهای قدیمی مدولاسیون از عرض باند بطور مؤثر استفاده نمی کردند. در آمریکا ، سازمان FCC[2] 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 آژانسهای 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، فرکانسهای بالای ۲۰ گیگاهرتز از جنبه تجاری اهمیت یافتند. فرکانسهای زیر ۲۰ گیگاهرتز نیز می توانند کاربران بیشتری را در سرعتهای بالاتر (اصولاً بواسطه تکنیکهای مدولاسیون دیجیتال و فشرده سازی) پشتیبانی نمایند. افزون بر این فن آوریهای جدید، تغییر در خط مشیهایی که در صدور مجوزفرکانس 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.

درچند سال اخیر ، دولت آمریکا و برخی از دولتهای اروپایی، سرویسهای بیسیم جدیدی را به بازار عرضه نمودند. در میان این فن آوریها می توان از سرویس ماهواره ای پخش مستقیم (DBS[3])، سرویسهای ارتباط شخصی یا PCS (تلفن سلولی دیجیتال نسل دوم)، سرویس توزیع چندنقطه ای محلی(LMDS) ، سرویس توزیع چندنقطه ای چندکاناله (MMDS) ، طیف

---

[1] Portability
[2] Federal Communications Commission
[3] Direct Broadcast Satellite

تلویزیونی دیجیتال، ماهواره های مدارکمLEO ، 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 درچند 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. بعلاوه 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. درنهایت 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 وارتباط پذیری کمی می باشند. سئوال 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 درمورد 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 ازطیف 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

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

فرکانسهای پایین طیف امواج رادیویی به آسانی منتشر نمی شوند. فرکانسهای بالاتر بیشتر شبیه نورمرئی عمل می نمایند. فرکانسهای بالاتر همانند نور مادون قرمز یا نورمرئی 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 درنهایت 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 .*
- ***مقدارعرض 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[1] ، 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[2]** : 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 درآن است که ارتباط محاوره ای و دوطرفه با افزایش شعاع مؤثر، کاهش می یابد. شعاع مؤثربزرگ 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.

---

[1] Sectorization
[2] Footprint

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

ازفرکانس (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 باMMDS 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

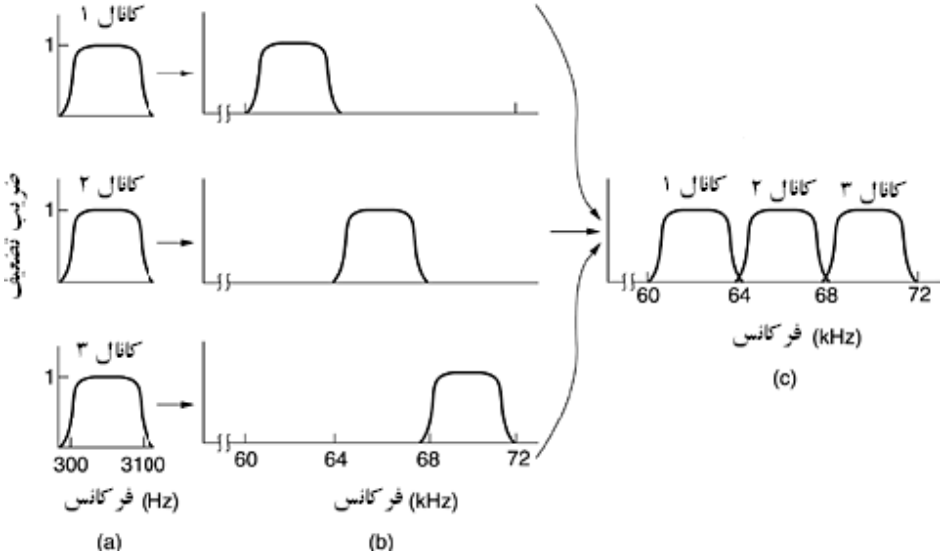
۴-۳- ارتباطات نقطه به نقطه و نقطه به چند نقطه

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 ازکاربران 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.

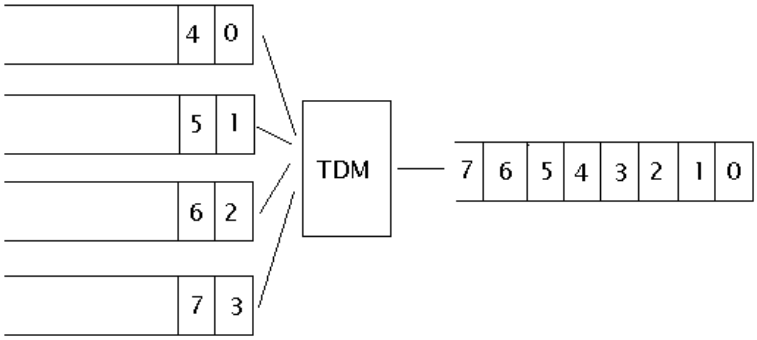
دریک سیستم نقطه به چند نقطه ، یک فرستنده اطلاعات رادر مسیرجریان پایین به چندین گیرنده ارسال می نماید. هنوز برسر استفاده ازتکنیک تسهیم سازی فرکانسی و تسهیم سازی زمانی بمنظور نائل شدن به یک عملکرد ارتباطی دوطرفه بحث وجود دارد.

همانطور که درشکل (۴-۱) نشان داده شده است، مدل قبلی، استفاده ازفن آوری تسهیم سازی فرکانسی می باشدکه طیف موجود را به دوکانال مجزا تقسیم می کند : یکی برای مسیرجریان بالا و دیگری برای مسیرجریان 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. ازتکنیک تسهیم ساز زمانی،گاهی اوقات بعنوان عملکرد ping-pong نام برده می شود. درشکل (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، ازفرکانسهای۸۲۴ مگاهرتز تا ۸۴۹ مگاهرتز استفاده می شود. اما هنگامی که به مکالمه روی تلفن سلولی گوش فرا می دهید از فرکانسهای۸۶۹ 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.

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 درپی 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 وسرویسهای 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 شبکه‌های 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 حدوده ۱/۵۴ مگابیت برثانیه(T1) می باشد، درحالیکه شبکه‌های گسترده سلولی در آمریکای شمالی از مرز۲/۵۴ مگابیت برثانیه گذشته اند. درضمن یک شبکه محلی بیسیم مبتنی بر استاندارد802.11a دارای سرعت۵۴ مگابیت برثانیه می باشد و فن آوری بیسیم باند پهن قدرت ارسال ۱ گیگابیت برثانیه 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. شبکه‌های بی‌سیم دستگاههای ارتباطی را آزادگذاشته 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

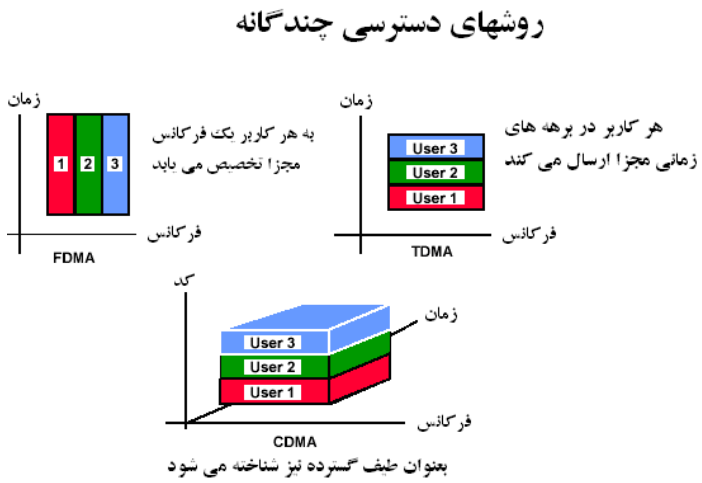
دستگاهها	شبکه ها	کاربرد ها
Web phone	WAN	ارسال و دریافت پیغام
Handheld	LAN	مرورگر اینترنت
Pager	PAN	محاوره
PORTAL	-	ارسال صدا
PC	-	وب
Appliance	-	ارتباطات

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 وWeb 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 ونرخ ارسال داده بایکدیگرتفاوت دارند. شبکه های ماهواره ای[1] نیز جزو شبکه های بیسیم هستند اما ارتباطات دوطرفه ماهواره ای در حال حاضر بسیارگران است.

[1] Satellite Networking (SAN)

در شبکه های بیسیم مجموعه متنوعی از برجهای مخابراتی، دکلهای سلولی، ایستگاههای پایه ونقاط 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 وشبکه های شخصی را با استفاده از اینترنت جهانی خواهند داشت.

شبکه های بیسیم در چگونگی عملکرد طیف، اختصاص طیف و استفاده از طیف فرکانسی درشرایط سلولی وموبایل 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 درنهایت 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 باند۸۰۰ 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 برصحبت، می شنوند. باندهای سلولی، بمنظورتضمین دسترسی مالک این باند، نیازبه مجوز دارند. یک اپراتور بایک مجوزبیسیم یک رابط هوایی[1] همانند CDMA ، FDMA و TDMA انتخاب می کندکه این تکنیکها امکان استفاده از حداکثر تعداد مشترکین را فراهم می نمایند. درشکل (۴-۳) روش های دسترسی چند گانه درشبکه های بیسیم نشان داده شده است.



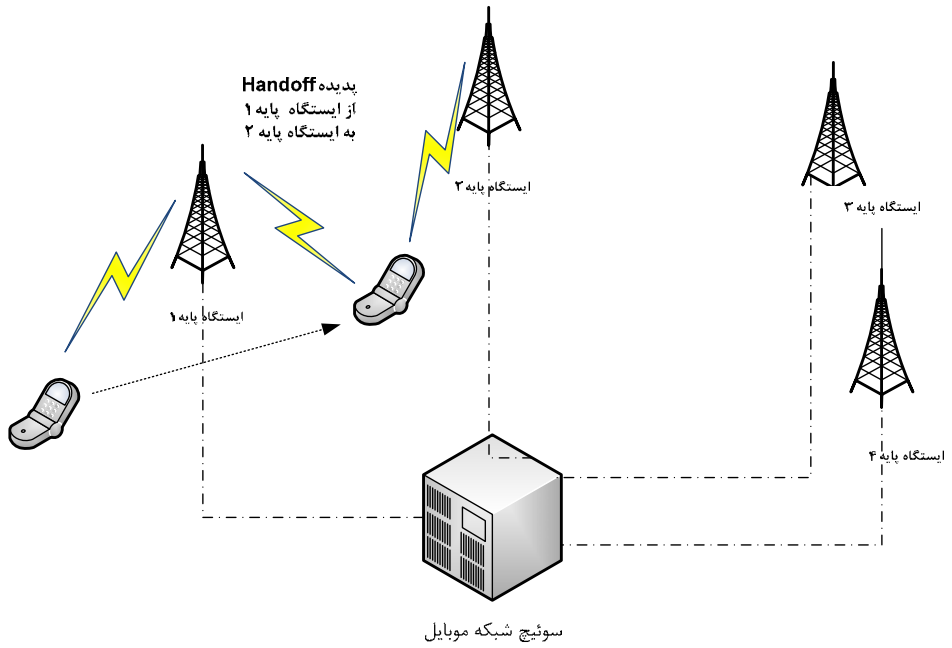
شکل(۴-۳): مقایسه تکنیک های FDMA&TDMA&CDMA

رابط هوایی یک پروتکل ارسال رادیویی برای دستگاههای ارتباطی و ایستگاههای پایه می باشد. این طیف معمولاً گران بوده بطوریکه اروپایی ها بیش از صدمیلیارد دلار در۲۰ سال اخیر برای مجوزهای نسل سوم هزینه نمودند. از طرف دیگر بعضی از بخشهای این طیف همانند طیف۲/۴ گیگاهرتزکه به باند ISM[2] معروف است و باند ۵/۷ گیگاهرتز که به نام U-NII[3] معروف می باشد نیاز به مجوزندارد. 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

کوچکتر تقسیم می کنند و درهر 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 سلولیA به برج سلولیB 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 بیسیم802.11 حرکت می کند، نیز به این سرویس نیاز دارد. درشکل (۴-۴) مثالی از این سرویس نشان داده شده است.



شکل (۴-۴) : سرویسhandoff

کلیه شبکه های بیسیم از امواج رادیویی استفاده می نمایند، لذا برج‌های مخابراتی و دستگاههای ارتباطی هر دو دارای آنتن می باشند. فرستنده گیرنده های بیسیم به آنتن ا متصل گشته و سیگنالهای 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 دستگاههای ارتباطی آماده برقراری ارتباط باشند، برج ارتباطی کانال کنترلی رابه کانالهای ارسال می فرستد. دوکانال عمده برای تلفن های شبکه گسترده ، کانالهای 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 قرمزو 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 ماشینهای مجاور با یکدیگر ارتباط داده ای بر مبنای یک شبکه بیسیم برقرار نمایند. یک تلفن وب بیسیم بعنوان یک آنتن برای یک کامپیوترlaptop مجاور کار می کند، مجموعه‌ای از ماشینهای سازگار با یکدیگر ازطریق پروتکل discovery ، نرم افزارهای خود را تعریف می‌نمایند. اغلب به این مجموعه فدراسیون دستگاههای ارتباطی می گویند. پروتکلdiscovery وظیفه مبادله اطلاعات مربوط به هویت دستگاهها و قابلیتهای سرویس دهی بین دستگاهها را دارد. این پروتکل همچنین به معنای در دسترس بودن اطلاعات بطور بیسیم خواهد بود. ارسال مادون

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.

۴-۴-۳- شبکه های محلی بیسیم

شبکه خانگی و تجاری بیسیم قدرتمند دوطرفه، شبکه محلی نام دارد و از حروف اختصاری WLAN[1] برای بیان آن استفاده می شود . یک شبکه محلی بیسیم می تواند منطقه‌ای 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 درتلفنهای سلولی برحسب کیلوبیت برثانیه می باشد.

محبوبترین استاندارد، اترنت بیسیم(IEEE802.11b) با محدوده تحت پوشش ۱۰۰ متر می باشد و سرعت ارسال آن ۱۱مگابیت 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. شبکه‌های محلی بیسیم دارای مزایای عمده زیر هستند.

- ***قابلیت جابه‌جا پذیری[۲]:*** کاربران محلی شبکه‌های بیسیم در هر نقطه ای از شبکه، قادر به دسترسی به اطلاعات شبکه می‌باشند. طبیعی است این امکان در شبکه‌های با سیم دیده نمی‌شود.
- ***نصب سریع وآسان:*** نصب شبکه‌های محلی بیسیم به سرعت و به آسانی امکان پذیر است و برخلاف شبکه‌های محلی سیم دار نیاز به صرف وقت و هزینه برای کابل کشی نمی‌باشد.
- ***انعطاف پذیری در نصب[۳]:*** شبکه‌های محلی بیسیم به راحتی قابل گسترش می‌باشند و با انعطاف‌پذیری بالا می‌توان این نوع شبکه‌ها را پیاده سازی نمود.
- ***کاهش هزینه ها:*** هر چند تجهیزات مورد نیاز شبکه‌های محلی بیسیم به مراتب بیشتر از شبکه‌های محلی سیم دار است ولی هزینه نصب، نگه‌داری و توسعه این شبکه‌ها کمتر از شبکه‌های محلی سیم‌دار می‌باشد، بنابراین در دراز مدت هزینه این شبکه‌ها کمتر از شبکه‌های با سیم خواهد بود.
- ***مقیاس پذیری[۴]:*** شبکه‌های محلی بیسیم جهت ارضاء نمودن نیازهای موجود در شبکه، قادر به پیاده سازی با ساختار متنوعی می‌باشند. پیکره‌بندی این شبکه‌ها به راحتی قابل تغییر است و همچنین توسعه و گسترش آنها آسان می‌باشد.

برخی از کاربردهای مهم شبکه‌های محلی بیسیم به شرح زیراست:

---

[1] Wireless LAN
[۲] Mobility
[۳] Flexibility
[٤] Scalability

الف) در بیمارستانها، پزشکان و پرستارها با استفاده از یک کامپیوتر قابل حمل کیفی قادر به اتصال به شبکه‌های محلی بیسیم می‌باشند و بدین ترتیب در هر نقطه از بیمارستان و درهرلحظه می‌توانند از اطلاعات پزشکی موجود در شبکه استفاده نمایند.

ب) گروه های حسابداری و شرکت های مشاوره ای با استفاده از امکانات شبکه‌های محلی بیسیم با سرعت بالا قادر به انجام وظایف خود می‌باشند.

ج) دانشجویان دانشگاهها با استفاده از امکانات شبکه‌های محلی بیسیم در هر نقطه از دانشگاه قادر به ورود به شبکه اینترنت و همچنین استفاده از منابع کتابخانه می‌باشند.

د) مدیران شبکه‌های کامپیوترای در محیط‌های متغیر، با استفاده از شبکه‌های محلی بیسیم بالاسری مورد نیاز برای توسعه و تغییرات در شبکه‌های کامپیوترای را به شدت کاهش می‌دهند.

ه) سایت‌های آموزشی در سازمان های حرفه ای و همچنین دانشجویان دانشگاه ها با استفاده از شبکه‌های محلی بیسیم به راحتی قادر به دسترسی اطلاعات و مبادله اطلاعات و آموزش از راه دور می‌باشند.

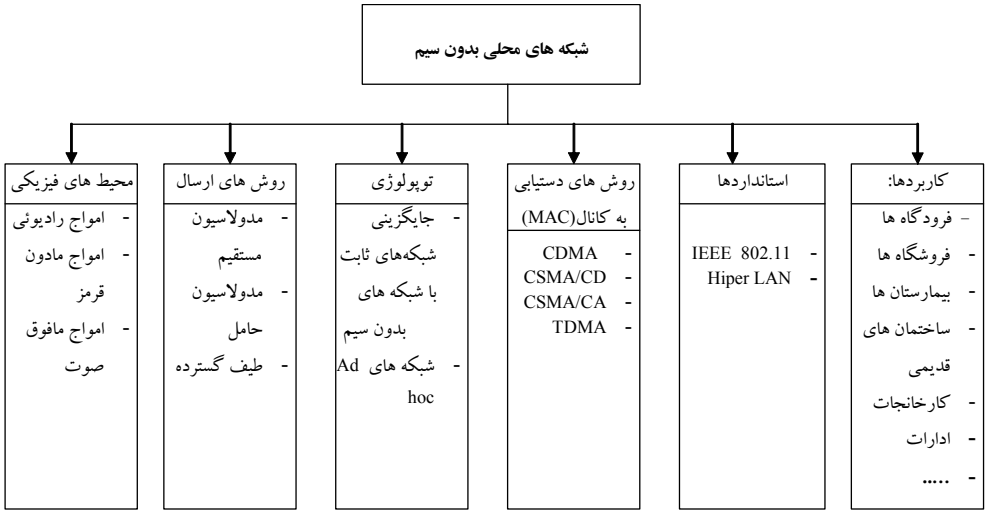
و) مدیران شبکه‌های کامپیوترای برای نصب شبکه‌های محلی کامپیوترای در ساختمان‌های قدیمی ومستهلک بدون نیاز به اعمال تغییرات در ساختمان ، قادر به نصب شبکه‌های محلی بیسیم می‌باشند .

ز) کارمندان شعبات مختلف اداره ها با نصب و پیکره‌بندی مناسب شبکه‌های محلی بیسیم، نیاز به سیستم اطلاعات مدیریت اطلاعاتی (MIS[1]) محلی ندارند؛ بلکه به راحتی قادر به استفاده از سیستم مدیریت اطلاعات شعبه مرکزی خود می‌باشند.

ن) کارگران انبارها و کارخانجات با استفاده از امکانات شبکه‌های محلی بیسیم، قادر به مبادله اطلاعات با بانک اطلاعاتی مرکزی خود می‌باشند و بدین وسیله بهره وری بیشتری قابل دست‌یابی می‌باشد .

ی) مقامات و مدیران اجرایی با استفاده از شبکه‌های محلی بیسیم در جلسات خود قادر به تصمیم‌گیری‌های سریع و فوری از طریق دستیابی به اطلاعات موجود در شبکه می‌باشند.

فنآوری ها و مسائل مختلف مربوط به شبکه های محلی بیسیم درشکل (۴-۵) نشان داده شده است.



شکل (۴-۵): فن‌آوری ها و مسائل وابسته به شبکه‌های محلی بیسیم

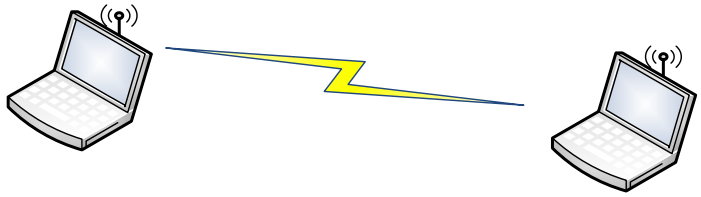
[1] Management Information System

۴-۴-۳-۱- عملکرد شبکه‌های محلی بیسیم

امروزه استفاده از امواج رادیویی در پیاده سازی شبکه‌های محلی بیسیم بر سایر روش‌های موجود ترجیح داده می‌شود. در این شبکه‌ها داده های ارسالی کاربران به‌صورت حامل‌های رادیویی ارسال می‌شوند و گیرنده به خوبی قادر به دریافت و تشخیص آنها می‌باشد. در سمت فرستنده، داده‌های دیجیتالی ارسالی به وسیله عملیات مدولاسیون به امواج رادیویی مناسب تبدیل می‌شوند و ارسال می‌گردند. چنانچه حاملهای 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 می‌کندکه با کمک این فیلتر،داده های هر کاربر دریافت می‌شوند وسایر بسامدهای ورودی فیلتر می‌گردند. هریک از ایستگاه‌های موجود در شبکه‌های محلی بیسیم مجهز به فرستنده/ گیرنده رادیویی می‌باشدکه درحقیقت نقطه دسترسی کاربر به شبکه است. هر یک از نقاط دسترسی فوق قادر به پشتیبانی از چندین کاربرمی‌باشند. آنتن‌های متصل به نقاط دسترسی شبکه، معمولاً در ارتفاع بالایی نصب می‌شوند تا تمام کاربران قادربه دریافت و ارسال سیگنال‌های رادیویی باشند. کاربران انتهایی شبکه‌های محلی بیسیم از طریق آداپتورهای مخصوص که برروی کامپیوترهای شخصی قابل حمل نصب شده اند، به شبکه متصل می‌گردند. آداپتورهای فوق از طریق آنتن های مخصوص ارتباط کاربران را از طریق فرستنده/گیرنده به شبکه برقرار می‌سازند.

۴-۴-۳-۲- ساختار شبکه‌های محلی بیسیم

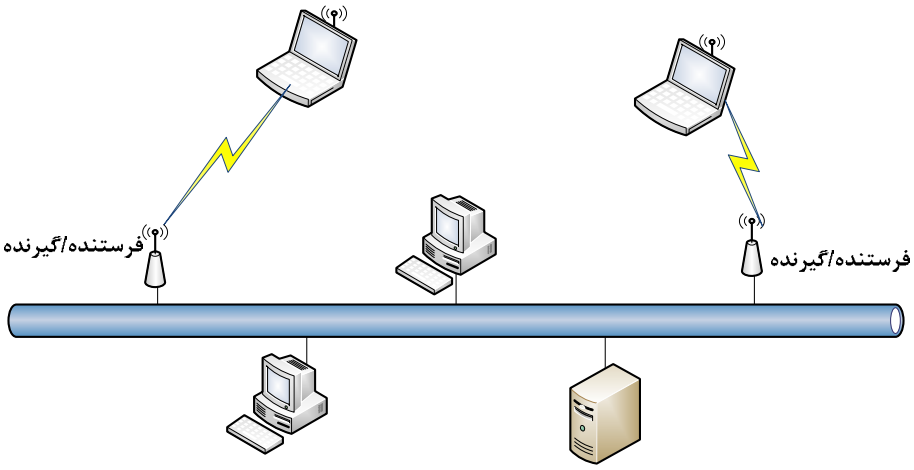
شبکه‌های محلی بیسیم به دو صورت ساده و پیچیده قابل پیاده سازی می‌باشند. در ساده ترین حالت چنانچه دو کامپیوتر مجهز به آداپتور رادیویی در فاصله معقولی از یکدیگر قرار داشته باشند، قادر به پیاده سازی شبکه بیسیم همتا به همتا می‌باشند. طبیعی است که چنین شبکه ای نیاز به مدیریت ندارد. هر کامپیوتر در حکم یک خدمات گیرنده شبکه است و قادر به استفاده از منابع خدمات گیرنده های دیگر می‌باشد، 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.



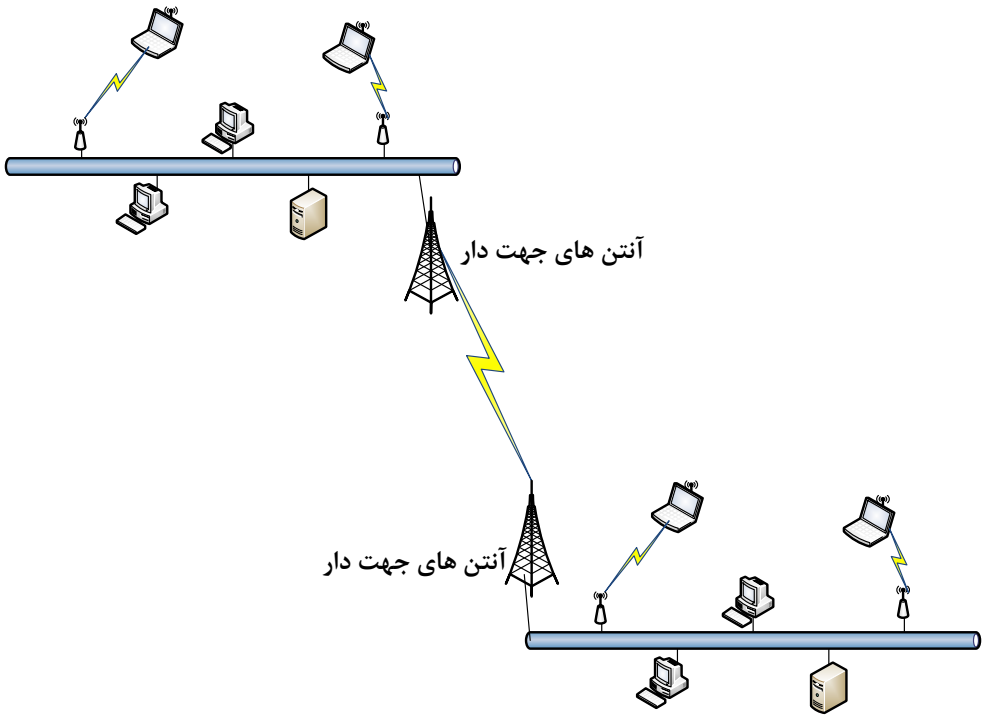
شکل (۴-۶): نمونه ای ازیک شبکه بیسیم همتا به همتا

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 این‌که می‌تواند از منابع خدمات گیرنده دیگر استفاده کند، قادربه استفاده از منابع خدمات دهنده شبکه نیزمی‌باشد. هر فرستنده/گیرنده، قادر به خدمات دادن به ۱۵ الی ۵۰ خدمات گیرنده می‌باشد. فاصله هر خدمات گیرنده تا فرستنده/گیرنده حداکثر بین ۵۰۰ تا ۱۰۰۰ فوت می‌باشد. بنابراین در شبکه‌های وسیع‌تر نیاز به چندین فرستنده/گیرنده می‌باشد. در شکل(۴-۷) نمونه ای از یک شبکه محلی بیسیم با استفاده از چندین فرستنده/گیرنده نشان داده شده است.

در طراحی شبکه‌های 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 ازهم قرار دارند را به یکدیگر متصل نماییم، از آنتن های جهت‌دارکه به فرستنده/گیرنده شبکه متصل می‌شوند استفاده می‌گردد. در شکل(۴-۸) نمونه ای از اتصال دو شبکه محلی بیسیم با استفاده از آنتن‌های جهت‌دار 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

۴-۴-۳-۱- فن‌آوری‌های شبکه‌های محلی بیسیم

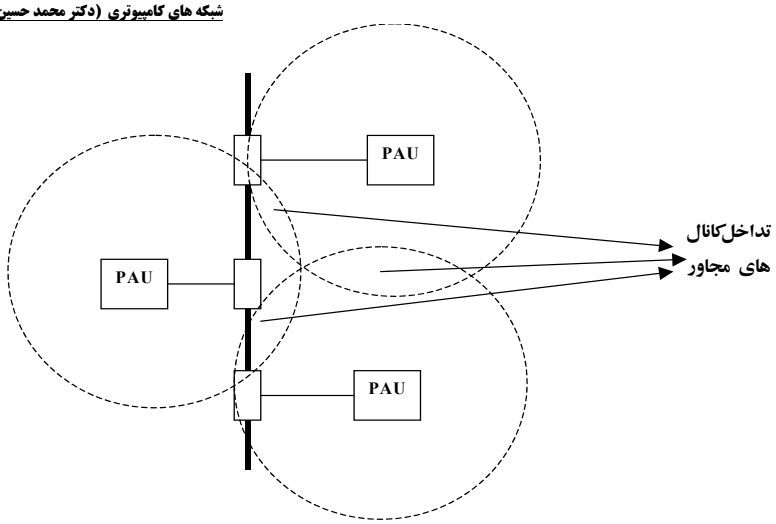
برای پیاده سازی ارتباط بیسیم بین دونقطه، فن‌آوری های مختلفی ارائه شده است. هر یک از این فن‌آوری‌ها دارای مزایا و محدودیت های خاص خود می‌باشند. برخی از این فن‌آوری‌ها عبارتند از : استفاده از امواج رادیویی و مایکروویو ، استفاده از امواج مافوق صوت[1] و استفاده از سیگنال‌های نوری. در زیر به بررسی مختصر هر یک از این روش‌ها می‌پردازیم.

امواج رادیویی

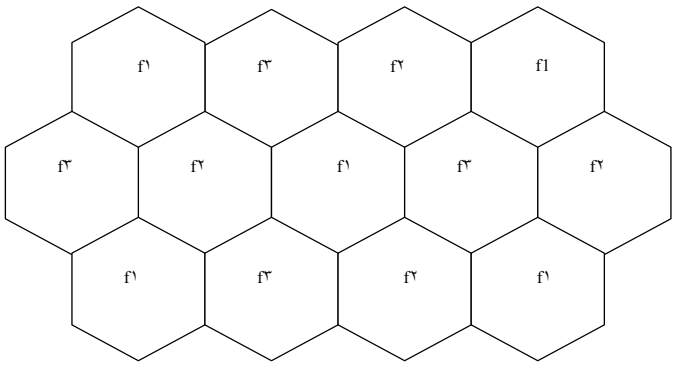
در فن‌آوري امواج راديويي ازدو روش باند باريك و طيف گسترده[2] استفاده مي‌شود. در سيستم‌هاي راديويي باند باريك، داده هاي كاربران بر روي باند بسامدي مشخصي ارسال و دريافت مي‌گردند. از آن‌جايي‌كه پناي باند تخصيص يافته در اين روش فقط به اندازه عبور اطلاعات مي‌باشد، بنابراين به اين روش باند باريك گفته مي‌شود. با هماهنگ ساختن دقيق كاربران در بسامدهاي مختلف، از وقوع تداخل بين كانال‌هاي مخابراتي جلوگيري مي‌شود. در سيستم‌هاي راديويي براي جلوگيري از وقوع تداخل، هر كاربر داراي يك فيلتر خاص مي‌باشد كه با كمك آن، اطلاعات ارسالي و دريافتي خود را از ساير ين جدا مي‌كند. از ديد كاربران، يكي از معايب عمده اين روش نياز به اخذ مجوز بسامدي براي پياده سازي شبكه‌هاي بي‌سيم مي‌باشد.

یکی ازمشکلات روش رادیویی، تداخل امواج می‌باشد. دراین شبکه‌ها، پهنای باند موجود به تعدادی زیرباند تقسیم می‌شود. برای جلوگیری ازتداخل، زیربانده‌ای مجاور ازبسامدهای متفاوت استفاده می‌نمایند. درشکل (۴-۹) مثالی از تخصیص بسامد برای یک سیستم بیسیم آورده شده است. براساس این شکل، از سه بسامد f2،f1 و f3 درشبکه استفاده شده است. تخصیص بسامد، طوری انجام می‌گیرد که سلول های مجاوریکدیگر ازبسامدهای متفاوت استفاده کنند.

[1] Ultrasonic
[2] Spread spectrum



الف

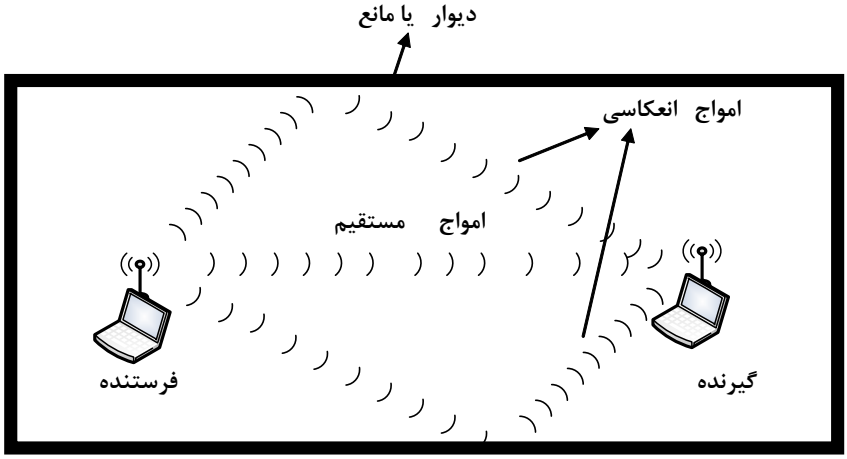


ب

شکل (۴-۹) مثالی از شبکه بیسیم با سه زیر باند الف) تداخل امواج ب) تخصیص کانال

یکی دیگر از مشکلات سیستم‌های رادیویی، مشکل چند مسیره[1] است. درشبکه‌های بیسیم و درهرلحظه از زمان، گیرنده سیگنال‌های متعددی از جهت‌های مختلف که از یک فرستنده واحد به آن می‌رسد را دریافت می‌دارد. این پدیده باعث تداخل بین سمبل‌ها (ISI[2]) می‌شود. درشکل (۴-۱۰) مثالی از پدیده چند مسیره آورده شده است.

[1] Multi path
[2] Inter symbol Interference

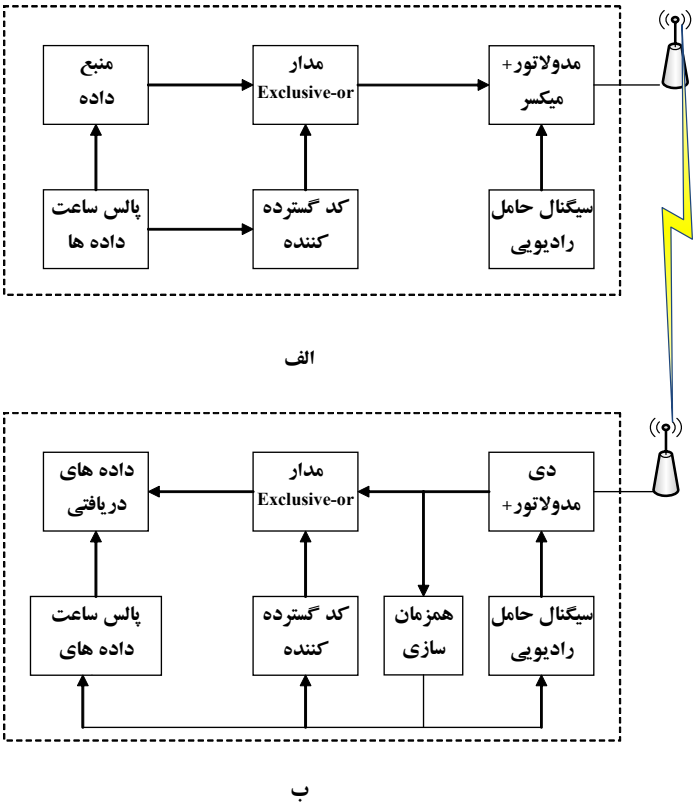


شکل (۴-۱۰) : مثالی از پدیده چند مسیره

براي حل مشكل چند مسيره ، درگيرنده ها از تكنيكي به نام يكنواخت‌سازي[1] استفاده مي‌شود. براساس اين تكنيك، سيگنال‌هاي انعكـاس يافته از سيگنال دريافتي مستقيم، كم شده و سيگنال حاصل به گيرنده وارد مي‌شود. بيشتر سيستم‌هاي بي‌سيم امروزه از فن‌آوري طيـف گسترده استفاده مي‌كنند. اين روش يك تكنيك بسامدهاي راديويي مي‌باشد كه اغلب در كاربردهاي نظامي براي پياده‌سازي يك سيـستم ارتباطي مطمئن و امن استفاده مي‌گردد. در اين فن‌آوري بين استفاده بينه از پناي باند و قابليت اطمينان بالا يك مصالحه انجام مي‌گيرد. در اين روش براي رسيدن به امنيت بالا سيگنال‌هاي ارسالي در تمام پناي باند موجود پخش مي‌شوند كه اين امر باعث نياز به پناي باند زيـاد مي‌گردد. چنانچه گيرنده مشخصه‌هاي فرستنده را داشته باشد، قادر به جمع‌آوري اطلاعات ارسالي از ميان سيگنال‌هاي نويز خواهد بود.

دو نوع روش مختلف برای پیاده سازی سیستم‌های طیف گسترده وجود دارند که عبارتند از : روش پـرش بـسامدی(FH[2]) و روش رشته بیتی مستقیم(DS[3]). در روش DS برای هر رشته بیت ارسالی یک الگوی بیتی اضافی که در اصطلاح چیپ نامیده می‌شود تولید می‌گردد. هر چه طول این چیپ بیشتر باشد احتمال بازیابی داده های اصلی بیشتر خواهـد بـود. درشـکل (۴-۱۱) بلوک دیاگرام فرستنده و گیرنده روش DS نشان داده شده است.

[1] Equalization
[2] Frequency hopping
[3] Direct sequence

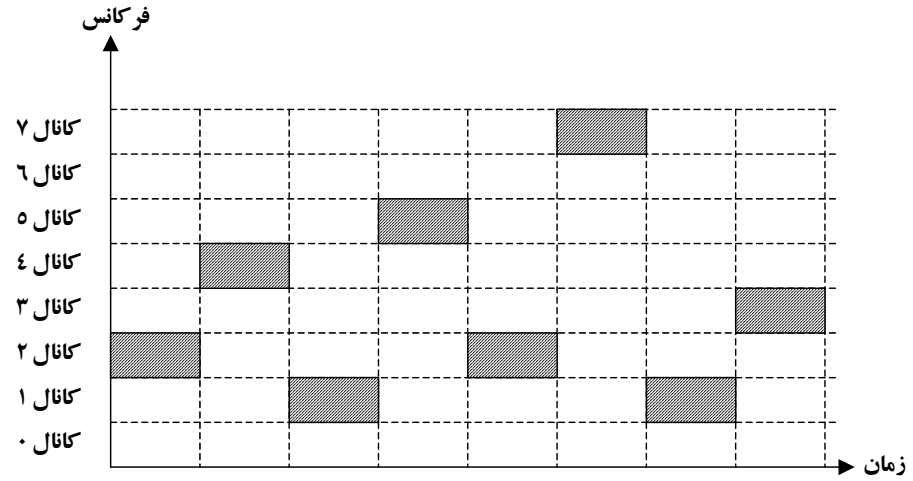


شکل (۴-۱۱): بلوک دیاگرام روش DS الف) فرستنده ب) گیرنده

مطابق با شکل فوق، درسمت فرستنده ابتدا داده های ارسالی به‌وسیله مدار Exclusive-or با یک رشته بیت تولید شده توسط کد گسترده کننده، به یک رشته بیت طولانی تصادفی تبدیل می‌شوند. خروجی مدار Exclusive-or به واحد مدولاتور و میکسر ارسال می‌شود. دراین واحد رشته بیت تصادفی تولید شده که داده های اصلی در دل آنها وجود دارد، به‌صورت امواج رادیویی تبدیل می‌شوند و درتمام باند بسامدی موجود گسترده می‌شوند. بدین صورت گیرنده های غیرمجاز قادر به جداسازی داده های ارسالی نخواهند بود.

درسمت گیرنده، سیگنال‌های رادیویی دریافتی با کمک دی مدولاتورو میکسر به‌صورت رشته بیت درمی‌آیند. رشته بیت دریافتی وارد مدار Exclusive-or می‌گردد و درآنجا با کمک کد گسترده‌کننده، داده‌های اصلی فرستنده استخراج می‌شود.

در روش FH با یک الگوی مشخص که هم فرستنده و هم گیرنده قادر به تشخیص آن می‌باشند، بسامد سیگنال ارسالی باگذشت زمان تغییرمی نماید. به هریک از بسامدهای ارسالی، یک کانال گفته می‌شود. در شکل (۴-۱۲) عملکرد روش FH نشان داده شده است. دراین مثال از هشت کانال بسامدی مختلف استفاده می‌شود. همان‌طور که درشکل نیز مشاهده می‌شود، بسامد کانال ارسالی فرستنده با گذشت زمان و براساس یک الگوی مشخص تغییر می نماید. تغییرات فوق نسبت به نرخ ارسال داده ها، می‌تواند خیلی سریع ویا خیلی کند صورت گیرد. چنانچه تغییرات بسامد سیستم FH نسبت به زمان کند باشد، همزمانی گیرنده با فرستنده به سادگی قابل دست‌یابی است.

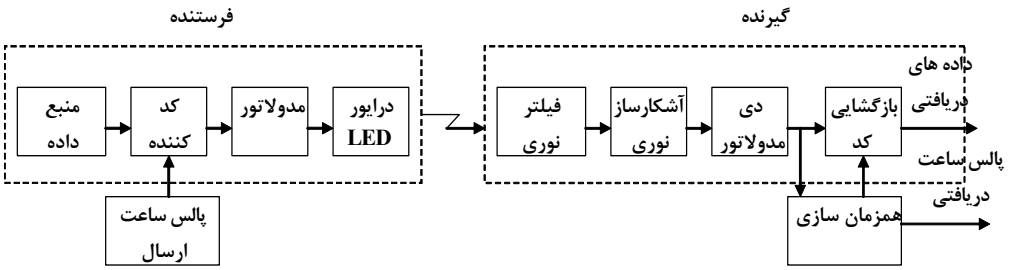


شکل (۴-۱۲): مثالی از روش FH با هشت کانال بسامدی

امواج مادون قرمز

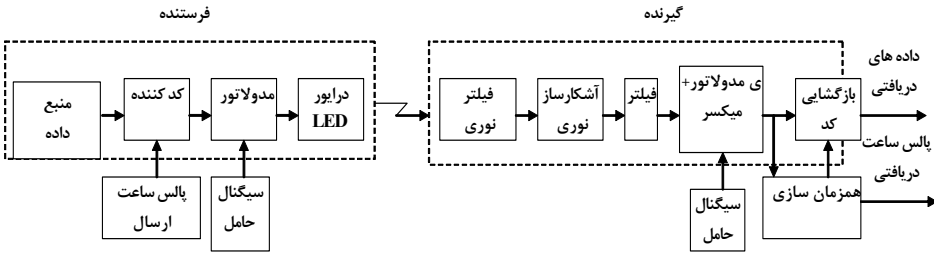
قبل از این‌که فن‌آوری فیبرنوری به‌طور گسترده مورد استفاده قرار گیرد، نیمه هادی های نوری مانند دیودهای لیزری و دیودهای نوری در حوالی دهه ۷۰ گسترش فراوانی پیدا کردند. امروزه از تجهیزات الکترونیک نوری که در طول موج‌های ۸۴۰ تا ۹۵۰ نانومتر کار می‌کنند، در کاربردهایی نظیر کنترل از راه دور سیستم‌ها و هدفون‌های بیسیم استفاده می‌شود. همچنین می‌توان از این فن‌آوری در شبکه‌های محلی بیسیم نیز استفاده نمود. این فن‌آوری دارای مشکلاتی نظیر قدرت انتشار امواج نوری و تداخل امواج و همچنین نویزهای موجود در محیط می‌باشد. به خاطر سرعت و انتشار بر روی خط مستقیم از دیودهای لیزری برای ارتباط کامپیوترای بین دو ساختمان استفاده می‌شود. برای سیستم‌های داخل ساختمان معمولاً از دیودهای نوری که دارای قدرت و سرعت کمتری می‌باشند استفاده می‌گردد. از آن‌جایی‌که سیگنال‌های مادون قرمز قادر به عبور از موانعی نظیر دیوارها و دربها نمی‌باشند، بنابراین فرستنده و گیرنده نوری باید در دید یکدیگر قرارداشته باشند. در این فن‌آوری، مشکل محدودیت بسامدی و تداخل امواج که در روش امواج رادیویی وجود دارد دیده نمی‌شود واستفاده ازآن در محیط‌هایی که تداخل امواج الکترومغناطیسی زیاد می‌باشد مناسب است. فن‌آوری امواج مادون قرمز نسبت به امواج رادیویی ارزان‌تر می‌باشد.

سیستم‌های مادون قرمز به دوصورت 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.درشکل (۴-۱۳) بلوک دیاگرام کلی فرستنده و گیرنده مادون قرمز نشان داده شده است.



شکل (۴-۱۳) : بلوک دیاگرام فرستنده و گیرنده مادون قرمز (روش مدولاسیون مستقیم)

درروش مدولاسیون سیگنال حامل که بلوک دیاگرام آن درشکل (۴-۱۴) نشان داده شده است، برای نیل به سرعت بالا مشابه سیستم‌های رادیویی از تکنیک‌های مدولاسیون سیگنال حامل نظیرFSK و PSK استفاده می‌گردد.



شکل (۴-۱۴) : بلوک دیاگرام فرستنده و گیرنده مادون قرمز (روش مدولاسیون حامل)سیگنال

در هردو فن‌آوری امواج رادیویی و امواج مادون قرمز، از محیط های پخشی استفاده می‌شود. درشبکه‌های محلی بیسیم از استانداردهای مختلف نظیر: CDMA[1]،CSMA/CD،CSMA/CA،TDMA و FDMA[2] برای کنترل دسترسی به کانال ارتباطی استفاده می‌گردد.

۴-۴-۳-۲- 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 معادل۵,۵ تا ۱۱ مگابیت برثانیه به بازار معرفی شد. این استاندارد برای پیاده سازی شبکه بیسیم در لایه های فیزیکی و دسترسی به شبکه طراحی شده است . موسسه WECA[3] وظیفه معرفی و بررسی تجهیزاتی که با این استاندارد مطابقت دارند را برعهده دارد. اصطلاح WiFi[4] 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 ۵ GHz

802.11b: استاندارد شبکه بیسیم در محدوده۲,۴ 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 : استانداردکیفیت سرویس درشبکه های محلی بیسیم

802.11f: استاندارد بررسی ارتباطات نقاط دسترسی در 802.11

802.11g: استاندارد ارتباط سریع تر در 802.11

---

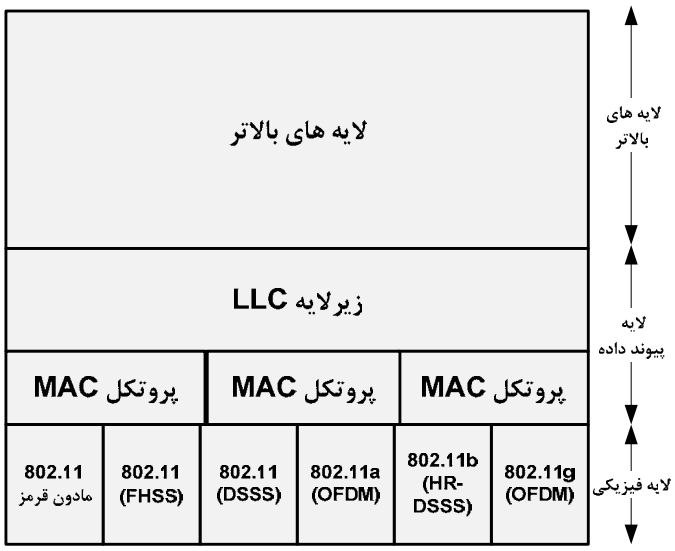
[1] Code-Devision Multiple Access
[2] Frequency Devision Multiple Access
[3] Wireless Ethernet Compatibility Alliance
[4] Wireless fidelity

802.11h: استاندارد مربوط به بالا بردن انتخاب کانال ها وتوان کنترلی

802.11i: استاندارد بررسی امنیت و احراز هویت در 802.11

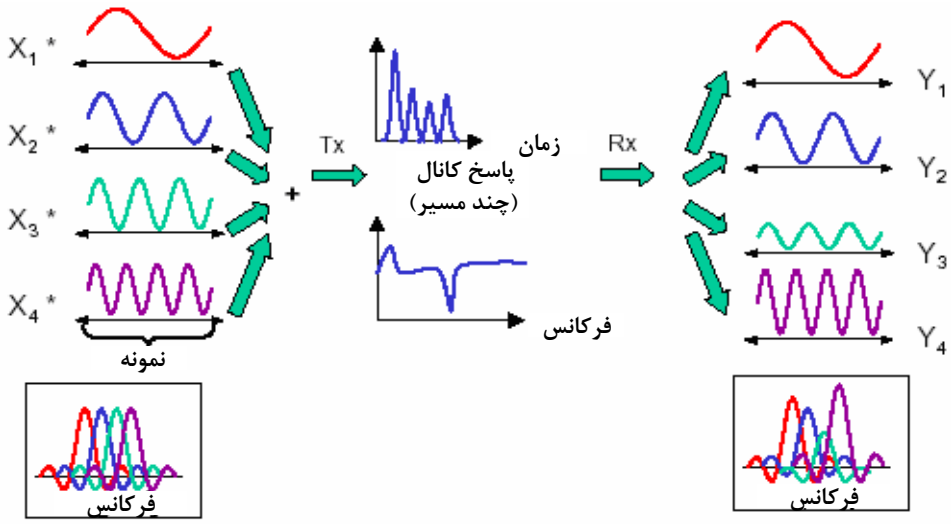
پشته پروتکل 802.11

کلیه پروتکلهای 802 ساختار تقریباً مشابهی دارند. لایه فیزیکی پشته پروتکل 802.11 متناظر با لایه فیزیکی OSI است،اما لایه پیوند داده ها در پروتکلهای 802 به دو یا چند زیر لایه تقسیم می شود. در 802.11 زیرلایه MAC (کنترل دستیابی رسانه) چگونگی تخصیص کانال را مشخص می کند. دربالای آن زیر لایه LLC (کنترل پیوند منطقی) قراردارد که وظیفه اش پنهان کردن انواع رسانه های 802 می باشد. درشکل (۴-۱۵) ساختار پشته استاندارد های 802.11 نشان داده شده است.



شکل(۴-۱۵) : پشتهٔ پروتکلهای 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 دیگراز رادیوی بردکوتاه استفاده می کنند که تکنیک هایی به نام FHSS و DSSS درآن ها به کار می رود . در سال ۱۹۹۹ نیز روشهای OFDM و HR- DSSS با سرعتهای 54Mbps و 11Mbps معرفی شدند. در سال ۲۰۰۱ دومین تلفیق OFDM معرفی شدکه باند فرکانس آن متفاوت از اولی بود.از نظر تکنیکی این ها به لایه فیزیکی تعلق دارند. درشکل (۴-۱۶) تلفیق فرکانسی OFDM نشان داده شده است.



شکل (۴-۱۶) : تلفیق فرکانسی OFDM

۴-۵- ملاحظات مشتریان شبکه‌های محلی بیسیم

هر چند شبکه‌های محلی بیسیم از انعطاف پذیری بالا در نصب و پیکره‌بندی برخوردار می‌باشند، اما مشتریان این شبکه‌ها باید فاکتورهای زیررا توجه داشته باشند:

- ***محدوده پوشش:*** در شبکه‌های محلی بیسیم، محدوده پوشش شبکه به عواملی مانند نوع تجهیزات استفاده شده، توان ارسالی ومسیر انتشار امواج بستگی دارد. برخورد امواج رادیویی با اشیایی نظیر ساختمانها، دیوارها، فلزات و حتی مردم باعث پراکندگی انرژی می‌شود که این مسأله محدوده پوشش سیستم را کاهش می‌دهد. اکثر سیستم‌های بیسیم از امواج رادیویی به خاطر قابلیت نفوذ ناپذیری آنها در دیوارها و سایر موانع استفاده می‌کنند. به‌طور نمونه شبکه‌های محلی بیسیم محدوده جغرافیایی بین ۱۰۰ تا ۳۰۰ فوت را پوشش می دهند.
- ***گذردهی[1]:*** مشابه شبکه‌های محلی سیم دار، گذردهی شبکه‌های محلی بیسیم نیز بستگی به نوع محصول دارد. عواملی که گذردهی را محدود می‌نمایند عبارتند از : تعداد کاربران، فاکتورهای انتشار، نوع سیستم شبکه محلی بیسیم مورد استفاده وگلوگاه موجود در نقطه اتصال شبکه بیسیم به شبکه سیم‌دار محلی. اکثرشبکه‌های محلی بیسیم تجاری دارای سرعت ۱/۷ مگابیت برثانیه می‌باشند. کاربران شبکه‌های محلی اترنت وحلقه نشانه، هنگامی‌که از شبکه‌های محلی بیسیم استفاده می‌کنند، به‌طور محسوس کاهشی در کارآیی شبکه حس نمی‌کنند. شبکه‌های محلی بیسیم، از گذردهی مناسب برای اغلب خدمات متداول شبکه‌های محلی سیم دار برخوردارمی‌باشند.
- ***جامعیت و قابلیت اطمینان:*** قابلیت اطمینان فن‌آوری شبکه‌های 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 می‌شود، ولی با طراحی مناسب شبکه‌های محلی بیسیم می‌توان این مشکل رابرطرف نمود.
- ***سازگاری با شبکه‌های موجود:*** اکثر شبکه‌های محلی بیسیم قادر به اتصال به شبکه‌های سیم‌دار اترنت یا حلقه نشانه می‌باشند. ازآنجایی‌که نودهای شبکه‌های محلی بیسیم همانند نودهای شبکه‌های محلی سیم‌دار مدیریت و پشتیبانی می‌شوند بنابراین امکان سازگاری و اتصال این شبکه‌ها با شبکه‌های موجود فعلی وجود دارد.

---

[1] Throughput

- ***سازگاری تجهیزات شبکه‌های محلی بیسیم با یکدیگر*** :یکی از نکات مهمی که مشتریان باید به آن توجه داشته باشند، آن است که سیستم‌های شبکه‌های محلی بیسیم مربوط به فروشنده های مختلف، ممکن است سازگار با یکدیگر نباشند. سه دلیل مهم این امرعبارتند از:

الف) ممکن است هر فروشنده از فن‌آوری مختلفی استفاده نمایند که سازگار با فن‌آوری سایرتجهیزات فروشنده ها نباشد.

ب) ممکن است سیستم‌های مختلف از باندهای بسامدی مختلفی استفاده نمایند، که در این‌صورت قادر به ارتباط با یکدیگر نمی‌باشند.

ج) ممکن است تجهیزات شبکه‌های محلی بیسیم فروشندگان مختلف، با وجود استفاده از فن‌آوری 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 وشبکه‌های محلی بیسیم را نظارت می نماید. سایر کشورها نیز اداره هایی برای این کار دارند. فروشندگان سیستم‌های شبکه‌های 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 شبکه‌های محلی بیسیم برای استفاده از مزایای آن نیاز به اطلاعات زیادی ندارند. برنامه های کاربردی موجود در شبکه‌های محلی سیم دار، به راحتی قابل استفاده در شبکه‌های محلی بیسیم می‌باشند. نصب و راه اندازی شبکه‌های محلی بیسیم به دلیل عدم نیاز به کابل کشی آسان است. همچنین بعد از نصب تجهیزات شبکه‌های محلی بیسیم، امکان جابجایی آنها از یک محل به محل دیگر وجود دارد.
- ***امنیت:*** ازآنجایی‌که ریشه اولیه فن‌آوری شبکه‌های محلی بیسیم از کاربردهای نظامی نشأت گرفته است، بنابراین امنیت این سیستم‌ها بسیار بالا می‌باشد. برای گیرنده های غیرمجاز دریافت اطلاعات ارسالی سایر کاربران مجاز، عملاً بسیار مشکل و پیچیده است. در سیستم‌های شبکه‌های محلی بیسیم، از تکنیکهای رمزنگاری پیچیده ای برای افزایش امنیت شبکه استفاده می‌شود.
- ***هزینه:*** پیاده‌سازی یک شبکه محلی بیسیم، دارای هزینه هایی جهت نصب نقاط دسترسی و همچنین آداپتورهای کاربران می‌باشد. تعداد نقاط دسترسی مورد نیاز دریک شبکه، به محدوده جغرافیایی پوشش شبکه و همچنین تعداد و نوع کاربران بستگی دارد. آداپتورهای شبکه‌های 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 شبکه‌های محلی بیسیم هزینه های کابل کشی و نصب آن وجود ندارد.

ب) از آن‌جایی‌که شبکه‌های محلی بیسیم به سادگی قادر به حرکت، اضافه کردن، کاهش و یا تغییر کاربران می‌باشند، بنابراین هزینه های اضافی اجرایی کاهش می یابد.

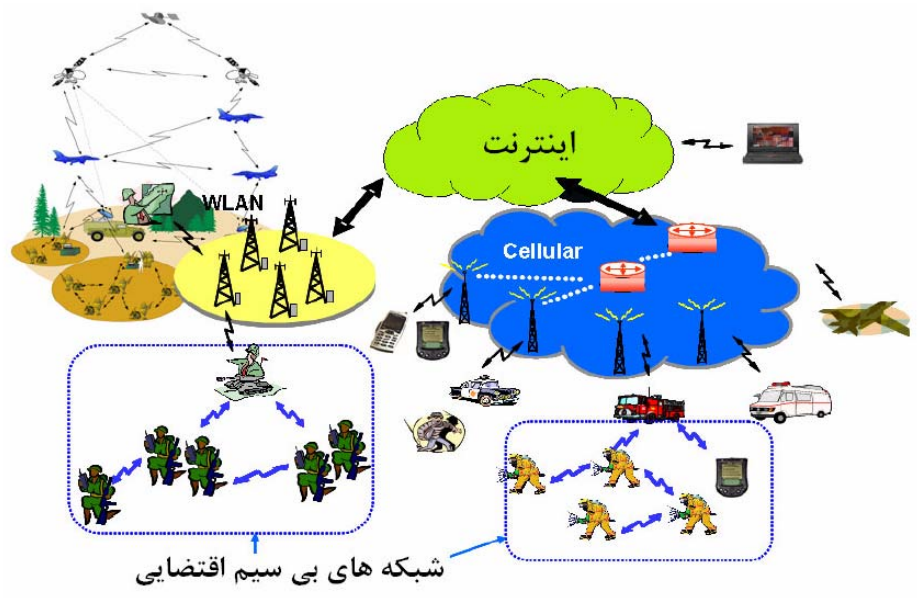
- ***مقیاس پذیری:*** در شبکه‌های محلی بیسیم، امکان توسعه شبکه با اضافه کردن نقطه دسترسی به شبکه به آسانی فراهم می آید.
- **سلامتی** : توان خروجی از سیستم‌های شبکه‌های محلی بیسیم بسیار کم است. این توان خیلی کمتر از توان خروجی از تلفن‌های موبایل سلولی می‌باشد.

۴-۶- شبکه‌های بیسیم اقتضایی (MANET[1])

[1] Mobile Adhoc NETworks

شبکه‌های بیسیم اقتضایی، مجموعه‌ای از نودهای بیسیم است که می‌توانند به طور پویا درهرمکان و درهر زمان بدون استفاده از هرزیر ساخت شبکه‌ای تشکیل شده و بایکدیگر درارتباط باشند. این شبکه ها یک سیستم خود مختار می‌باشند که نودهای سیار توسط کانال های بیسیم به هم متصل شده‌اند 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 اقتضائی مجهز به آنتن های فرستنده و گیرنده بیسیم همه جهتی (پخش فراگیر)[1] هستند. درهر لحظه، وابسته به مکان نود ها و الگوهای پوشش فرستنده و گیرنده آنها، یک ارتباط بیسیم چندگامی بین نود ها وجود دارد. این توپولوژی اقتضائی ممکن است با گذشت زمان به سبب جابجائی نود ها تغییر کند. درشکل(۴-۱۷) نمونه ای از کاربردهای مختلف شبکه های بیسیم اقتضایی نشان داده شده است.

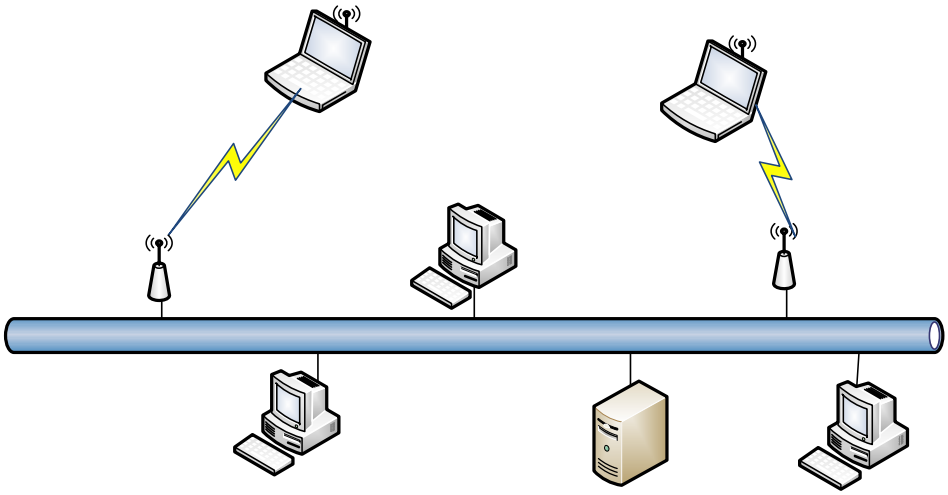


شکل (۴-۱۷): نمونه ای از کاربردهای شبکه های بیسیم اقتضایی

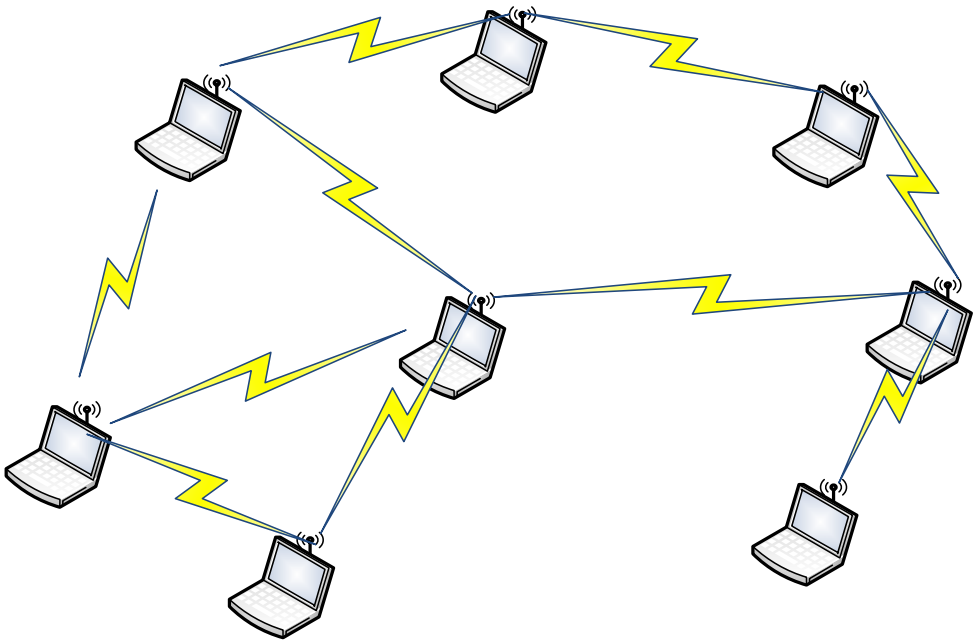
بطور کلی دو رویکرد مجزا برای ارتباط واحدهای سیار بیسیم با یکدیگر وجود دارد که عبارتند از:

- **ساختار یافته** : شبکه های بیسیم سلولی هستند که در آن دستگاه های سیار بااستفاده 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 سیارمی باشد. یک شبکه بیسیم اقتضائی 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 .

[1] Broadcast



شبکه بیسیم ساختار یافته



شبکه بیسیم اقتضایی بی ساختار

شکل(۴-۱۸): انواع شبکه های بیسیم

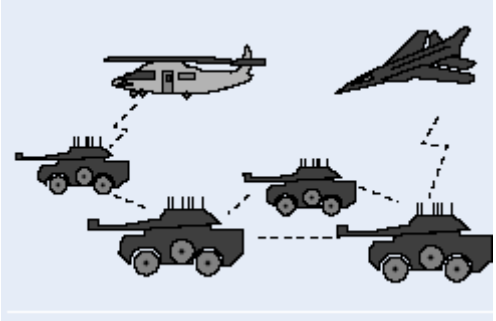
۴-۶-۱- کاربرد شبکه های اقتضائی بیسیم

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،

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.

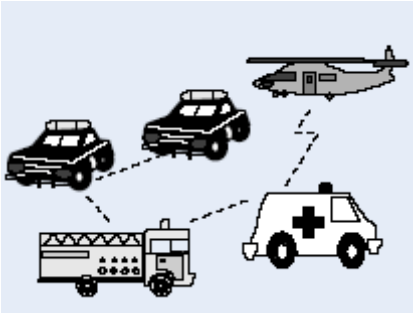


شکل(۴-۱۹): کاربرد نظامی شبکه های اقتضایی

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 اعضاء به اشتراک بگذارند. کاربرد دیگر ممکن است در شبکه های شخصی (PAN) [1] باشد زمانی که می خواهیم برای تبادل اطلاعات، بین چند دستگاه کامپیوتری مستقیما ارتباط برقرار کنیم، شبکه های شخصی یک زمینه کاربرد نویدبخش ازشبکه های بیسیم اقتضائی در تکنولوژی آینده می باشند.

ج) عملیات نجات/ اضطراری : شبکه های بیسیم اقتضائی می توانند در عملیات های نجات/ اضطراری ، برای کمک به پرسنل در حال امداد رسانی در حوادثی مانند اطفاء حریق ، زلزله ، سیل و ... مورداستفاده قرار گیرند. عملیات نجات/ اضطراری همیشه در جائیکه 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 اقتضائی در عملیات های پلیسی نیز استفاده می گردند. شکل (۴-۲۰) مثالی از کاربرد در عملیات نجات/اضطراری را نشان می دهد.

[1] Personal Area Networks



شکل(۴-۲۰): کاربرد شبکه های اقتضایی سیار در عملیات نجات/اضطراری

انواع ترافیک در شبکه‌های بیسیم اقتضایی کاملاً متفاوت از ترافیکهای موجود در شبکه های بی‌سیم معمولی که دارای زیر ساخت می‌باشند است. این ترافیک ها شامل موارد زیر می باشند:

- **ترافیک های همتا به همتا**: ارتباط بین دو نود که یک پرش بین آنها قرار می‌گیرد. این نوع ترافیک شبکه معمولاً ثابت است.
- **ترافیک های انتها به انتها:** ارتباط بین دو نود فراتر از یک پرش 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 می‌مانند یا احتمالا به صورت گروهی حرکت می‌کنند. این نوع ترافیک شبیه ترافیک استاندارد شبکه است.
- **ترافیک های پویا:** هنگامی اتفاق می‌افتد که نودها به طور پویا و تصادفی حرکت می‌کنند. مسیرها بایددوباره تشکیل شوند که پیامد آن اتصال نودها به صورت ضعیف[1] می‌باشد.

۴-۶-۲- ویژگی های شبکه های اقتضائی بیسیم

شبکه های اقتضائی بیسیم دارای ویژگی ها و مشخصات مختص به خود می باشند. چندین ویژگی برجسته شبکه های اقتضائی عبارتند از :

الف) توپولوژی شبکه پویا: از آنجا که در شبکه های اقتضائی نود ها سیار هستند و می توانند آزادانه حرکت کنند، توپولوژی شبکه ممکن است بسرعت و غیر قابل پیش بینی تغییر کند و در نتیجه ارتباطات بین ترمینال ها نیز با زمان تغییر کند. شبکه بیسیم اقتضائی 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 اقتضائی نه تنها درون شبکه اقتضائی 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 اقتضائی 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 وغیره ، اغلب کمتر از بیشترین نرخ انتقال رادیویی است.

[1] loosed

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 : معمولا 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 دائما تغییر می کند و خطاهای ارتباطی موقتی وتغییرات 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[1] مبتنی بر مسیریابی واکنشی[2] 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) [3] : 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

ج) ارتباطات بین شبکه ای [1]: علاوه بر ارتباطات درون یک شبکه اقتضایی، در بسیاری از حالات نیاز به ارتباط بین شبکه ای بین شبکه بیسیم اقتضائی 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 مواجه 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 خوهد یافت.

و) مسیریابی درشبکه 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 معمولا از لحاظ انرژی و قابلیتهای 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 وکاربرد هریک را ذکر نمایید.
۲. منظور از شعاع موثر سرویس درشبکه های بیسیم را توضیح دهید.
۳. کاربرد تسهیم سازی فرکانسی را درشبکه 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 شبکه‌های محلی بیسیم را تشریح نمایید.
۷. موارد کاربرد شبکه‌های محلی بیسیم را بنویسید.
۸. مشکلات عمده فن‌آوری امواج رادیویی و روش های حل آنها را درشبکه‌های محلی بیسیم توصیف نمایید.
۹. عملکرد روش DS را درشبکه‌های محلی بیسیم تشریح نمایید.
۱۰. عملکرد روش FH را درشبکه‌های محلی بیسیم تشریح نمایید.
۱۱. روش مدولاسیون سیگنال حامل و روش مدولاسیون مستقیم را درسیستم‌های بیسیم با فن‌آوری امواج مادون قرمز تشریح نمایید.
۱۲. ساختارشبکه‌های محلی بیسیم همتا به همتا را تشریح نمایید.
۱۳. فاکتورهای مهم انتخاب شبکه‌های محلی بیسیم را ازدیدگاه مشتریان ذکرنمایید.
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

۱۶. تفاوت شبکه های MANET ساختار یافته وبی 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.

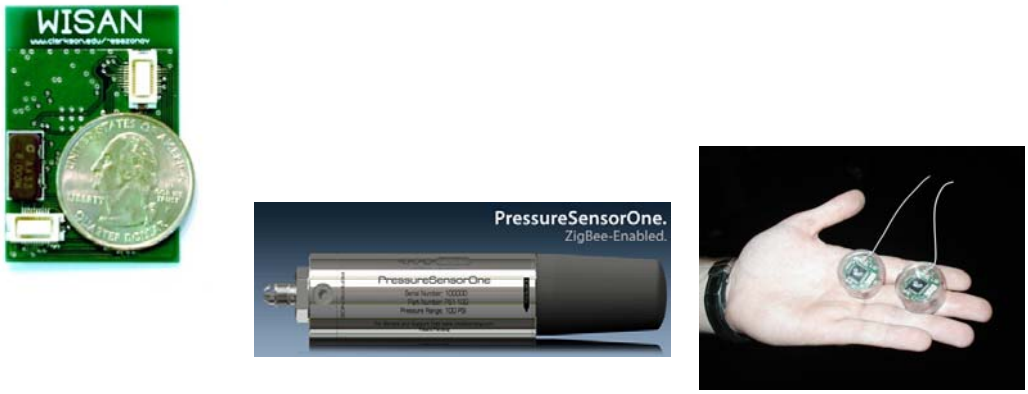
فصل پنجم

شبکه های حسگر بیسیم[1]

۵-۱- مقدمه

پیشرفتهای اخیر در کوچک سازی، طراحی مدارهای کم مصرف و تجهیزات ارتباطی بیسیم ساده وکم مصرف و نیز توسعه شرکت های تولید کننده منابع انرژی کوچک به همراه کاهش هزینه های تولید کارخانه ای موجب ایجاد دیدگاه فنآوریکی جدیدی با نام شبکه های حسگر بیسیم گردید. پیشرفت فنآوری 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 نظیردما، نور، لرزش، صدا، تابش، رطوبت و ... استفاده می شود. یک شبکه حسگر از تعداد زیادی نود های حسگر تشکیل شده که بصورت متراکمی در اطراف پدیده فیزیکی مورد نظر پخش شده اند. نکته مهم در مورد شبکه های حسگر بیسیم این است که نیاز نیست مکان حسگرها کاملا 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. خصوصیاتی 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.
درشکل (۵-۱) نمونه ای از حسگرهای مختلف نشان داده شده است.

[1] Wireless Sensor Networks (WSNs)



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 هایMANET 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 هایMANET 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 فنآوری 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.

- **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[1] 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 وخصوصیات 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

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.

۵-۴- گذشته، حال وآینده شبکه های حسگر

همانند بسیاری دیگر از فناوری‌ها، کار بر روی شبکه‌های حسگر از کارهای نظامی و دفاعی آغاز شد. در طول جنگ سرد، دولت آمریکا، حمایت از پروژه‌ای به نام سیستم نظارت صوتی[1] را بر عهده گرفت. در این پروژه با قرار دادن تعدادی حسگر در نقاط استراتژیک زیر اقیانوس، سعی در تشخیص نفوذ و ردیابی زیر دریایی‌های شوروی داشتند.

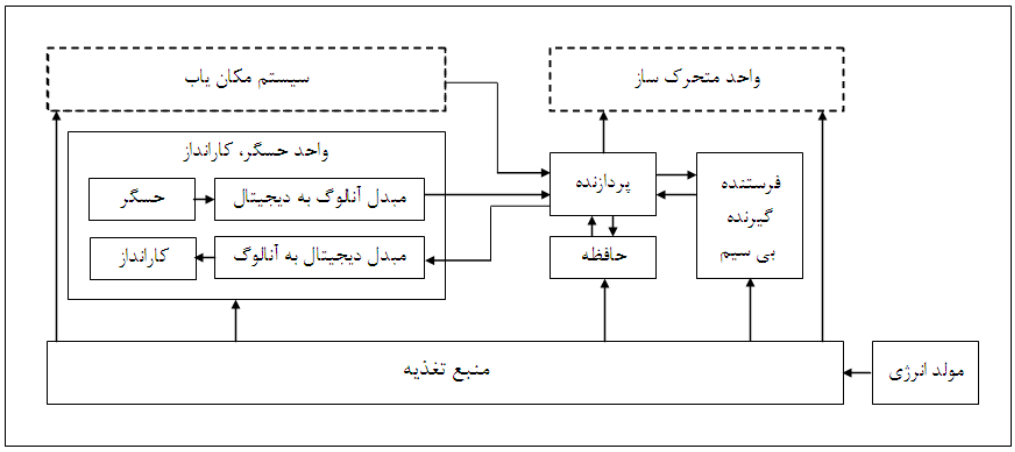
کار بر روی شبکه‌های حسگر بطور جدی از سال ۱۹۸۰ و با پروژه شبکه‌های حسگر توزیع شده در آژانس پروژه‌های تحقیقات دفاعی پیشرفته آمریکا آغاز شد. پروژه WINS در سال ۱۹۹۳ و با همکاری دانشگاه کالیفرنیا و مرکز علوم شرکت Rockwell شروع شد. این پروژه در سال ۱۹۹۸ به یک محصول تجاری تبدیل شد.در حدود سال ۱۹۹۹ دانشگاه برکلی دو پروژه تحقیقاتی بر روی شبکه‌های حسگر آغاز کرد. پروژه PicoRadio و پروژه Smart Dust یک پروژه کاملا بلند پروازانه بود و هدف آن ساختن گره‌های حسگری با ابعاد یک میلیمتر مکعب بود که البته به موفقیت‌هایی هم رسید. برای داشتن تصور بهتر از ابعاد یک حسگر می‌توان گفت که این حسگرها چنان کوچک هستند که می‌توانند همانند گرد و غبار بوسیله جریان هوا جابجا شوند.

در سال‌های اخیر پروژه‌های بسیار دیگری مانند پروژه µAMPS 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.

شبکه‌های حسگر یکی از فن‌آوری‌های نوینی است که بسیاری از دانشمندان عقیده دارند، آینده بشر را تغییر خواهد داد. این فنآوری به خاطر مزایا و کاربردهای بسیاری که در زمینه‌های مختلف دارد، جزء فن‌آوری‌های استراتژیک بسیاری از کشورها محسوب می‌شود. در دسامبر ۱۹۹۹ مجله Business Week شبکه‌های حسگر جز یکی از مهم‌ترین فن‌آوری‌های 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 می‌شود که تعداد گره‌های حسگر در سال ۲۰۱۰ به ۴۶۵ میلیون برسد و این در حالی است که در سال ۲۰۰۳ تعداد گره‌های 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)

شکل(۵-۲): اجزاء یک نود حسگر

علاوه بر اجزاء ذکر شده، بسته به کاربرد مورد نظر اجزاء دیگری نیز دریک نود حسگروجود 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 معمولا دارای سیستم تعیین محل می باشند. محرک[1] 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 درنظر 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 شئ، 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 حسگرکارانداز: به نودی گفته می شود که مجهز به حسگر و کارانداز باشد.

[1] Mobilizer

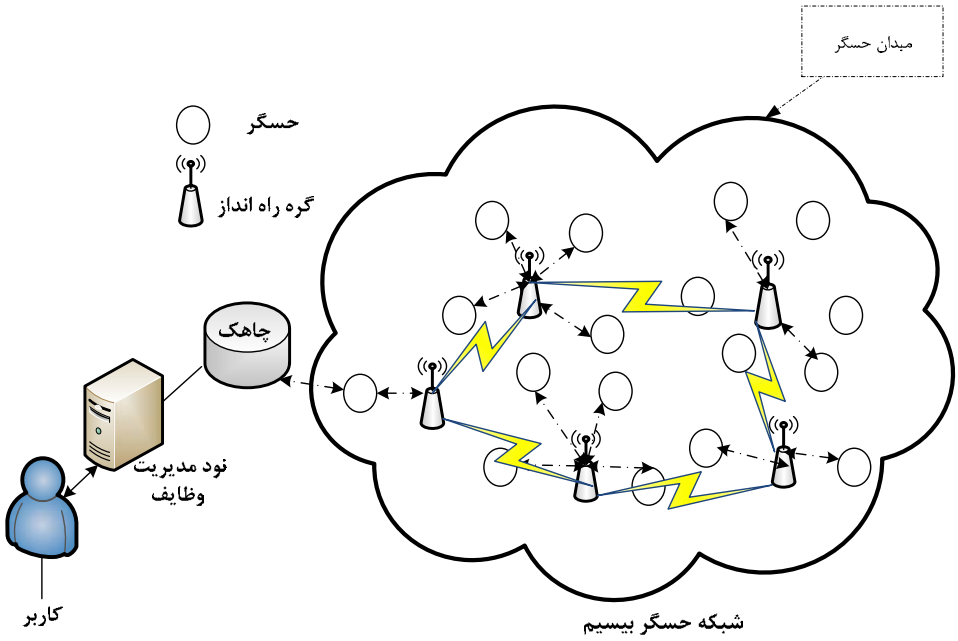
شبکه حسگر : شبکه ای که فقط شامل نود های حسگر باشد. این شبکه نوع خاصی از شبکه حسگر می باشد. در کاربردهایی که هدف جمع آوری اطلاعات و تحقیق در مورد یک پدیده می باشد ، استفاده می شود؛ مانند مطالعه بر روی گردبادها وسایرپدیده های محیطی.

میدان حسگر،کارانداز: ناحیه کاری که نود های شبکه حس وکار 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[1] 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(۵-۳) 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.

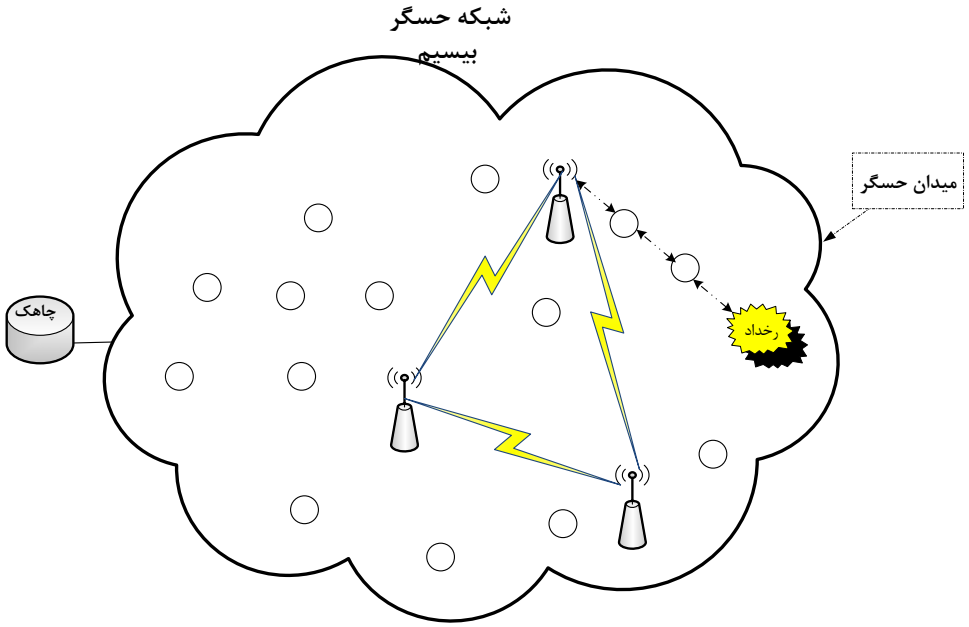


شکل(۵-۳): ساختار کلی یک شبکه حسگر

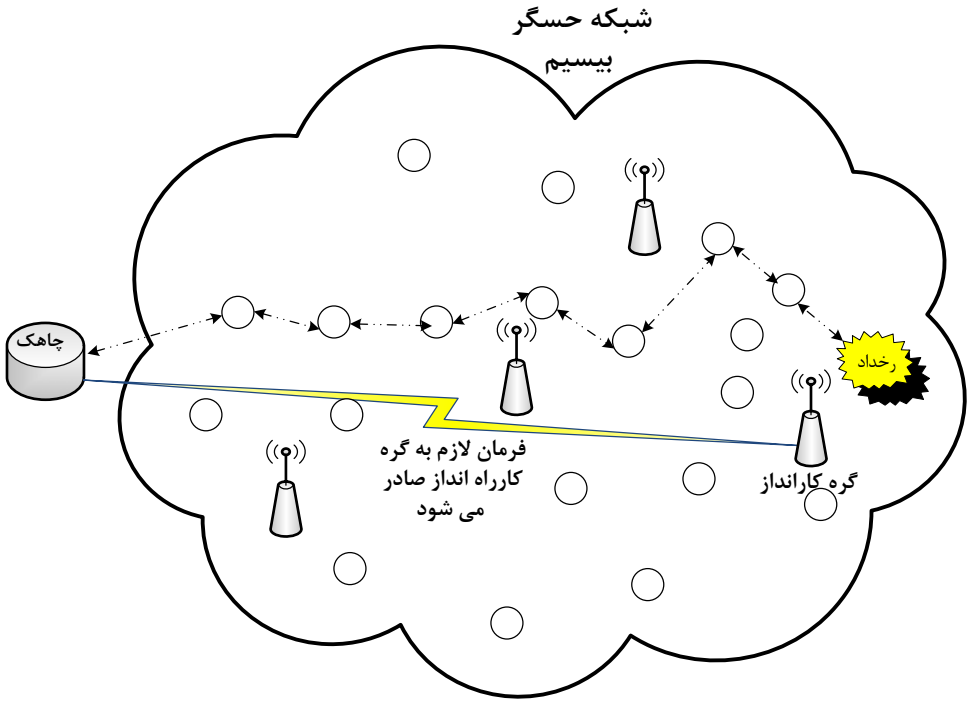
ساختار خودکار : حسگر هایی که یک رخداد یا پدیده را تشخیص می دهند، داده های دریافتی را به نود های کارانداز جهت پردازش و انجام واکنش مناسب ارسال می کنند. نود های کارانداز مجاور با هماهنگی یکدیگر تصمیم گیری کرده و عمل می نمایند. در واقع هیچ کنترل متمرکزی وجود ندارد و تصمیم گیری ها بصورت محلی انجام میشود. شکل(۵-۴) ساختار شبکه های حسگر خودکار را نمایش می دهد.

[1] Task manager node

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

از طرف دیگر در کاربردهای خاصی ممکن است از ساختار بخش بندی شده یا سلولی استفاده شود که در هر بخش یک سردسته[1] وجود دارد که داده های نود های دستهٔ خود را به چاهک ارسال می کند. در واقع هر سردسته مانند یک دروازه[2] 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 دلائلی نظیر: مکان، قابلیت دسترسی، انرژی موجود، بروز خطا در نود، وجزئیات 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 تجمیع داده ها از چندین حسگر است. زمانیکه قصد همگرایی در یک یا چند چاهک ،

---

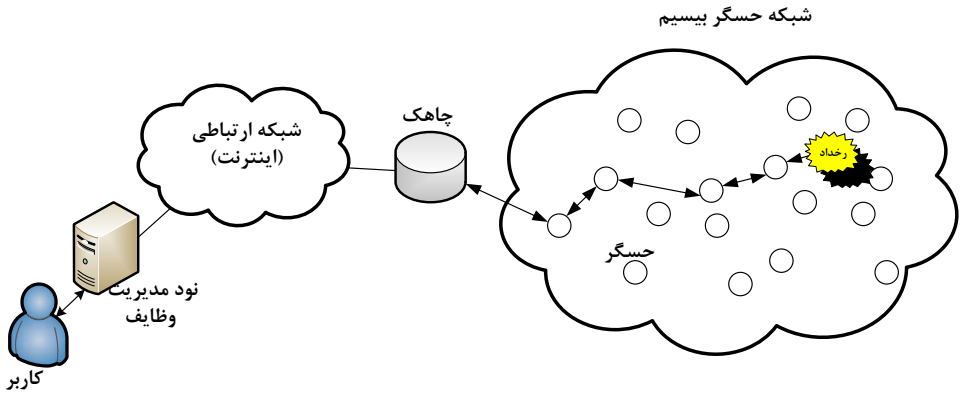
[1] Cluster head
[2] Gateway

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، سرویسهایی که شبکه های حسگر بیسیم در سطح شبکه ارائه می کنند هنوز کاملا 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 درشکل(۵-۶) نشان داده شده است، پخش می گردند.



شکل(۵-۶): نود های حسگر که در منطقه هدف پخش شده اند

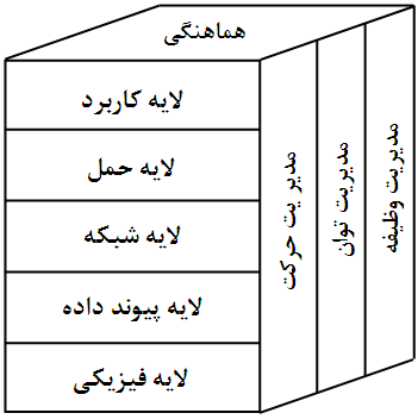
هر کدام از نود های مورد نظر توانایی جمع آوری داده ها و مسیریابی آنها به نود چاهک و کاربر نهایی را دارند. داده ها از طریق معماری چند پرشی همانطور که در شکل (۵-۶) نمایش داده شده است، مسیریابی و ارسال می گردند. نود چاهک ممکن است از طریق ماهواره یا اینترنت با نود مدیریت وظایف ارتباط برقرار نماید.

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 پیونددداده 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 برروی مصرف انرژی داشته باشد و حداقل تداخلات را برای همه پخشی

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.

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 عملیاتهای 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 خصوصیاتی مانند مسیریابی داده محور، نیاز به پروتکل های مختلف در لایه حمل دارد. در نتیجه این نیازمندیها احساس نیاز به پروتکلهای لایه حمل جدید را افزایش می دهد.

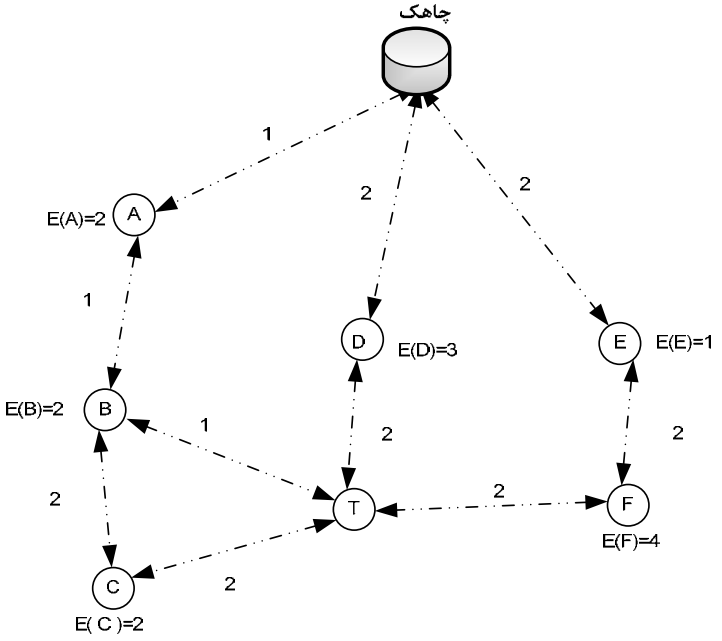
۵-۹-۳- لایه شبکه

نود های شبکه بصورت متراکمی در نزدیکی محلهای مورد بررسی گسترده می گردند. نیاز به پروتکل های مسیریابی بیسیم چند پرشه میان نود چاهک و دیگر نود ها دراین لایه به خوبی حس می شود. پروتکل های مورد استفاده در شبکه هایMANET 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 اکثرا داده محور می باشند.
- تجمیع داده ها تنها زمانی که مانعی برای تلاش جمعی نود های حسگر نباشد کارا می باشد.

- شبکه حسگری که دارای آدرس دهی مبتنی بر خصوصیات و آگاه از مکان[1] 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 درشکل(۵-۸) را درنظر بگیرید. دراین شکل نود T نود مبدا حس کننده پدیده می باشد. اعداد نشان داده شده برروی هر لینک رادیویی، نشان دهنده میزان انرژی لازم برای ارسال پیام ازطریق آن لینک می باشد. مقدار تابع E() نشان دهنده میزان انرژی باقیمانده درنود مورد نظر می باشد. به عنوان مثال E(B)=2 نشان دهنده این مطلب است که درنود 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=۴ و α=۳
- مسیر ۲: T-C-B-A-Sink و PA=۶ و α=۶
- مسیر ۳: T-D-Sink و PA=۳ و α=۴
- مسیر ۴: T-F-E-Sink و PA=۵ و α=۶

PA نشان دهنده انرژی موجود و α بیانگرانرژی مورد نیاز برای ارسال بسته از طریق مسیر مورد نظر می باشد. انتخاب مسیر مناسب از بین مسیرهای موجود، می تواند برمبنای یکی از اصول زیر باشد:

- مسیری با حداکثر انرژی موجود: مسیری که حداکثر انرژی موجود را دارد را انتخاب می نماییم. PA نهایی مسیر 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 بعلاوه 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 شرائط مسیر ۴ را به عنوان مناسبترین مسیر از نظر میزان انرژی موجود انتخاب می نماییم.

[1] - Location awareness

- 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:

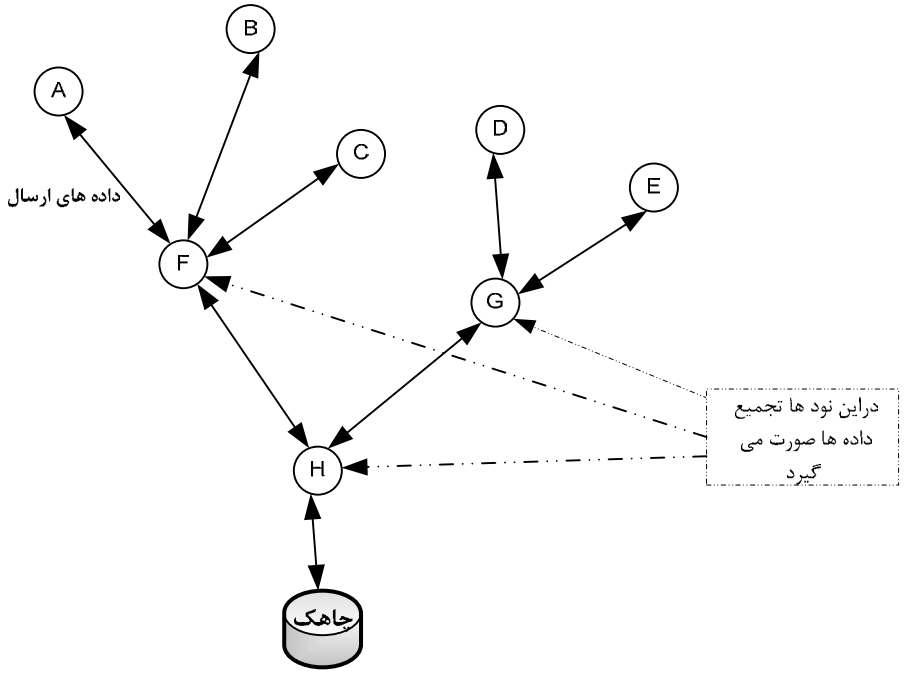
- نود چاهک درخواست ها را توزیع نماید.

- 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[1] تکنیکی برای حل مشکل تشابه و حجم زیادداده 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



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[1] 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 هایMAC 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 پروتکلهای قدیمی لایه پیوند داده، بصورت کامل برای شبکه های حسگر مناسب نمی باشند. در سیستمهای 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 باندی 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

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. پروتکلهای 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- فنآوریهای جاسازی شده[1] 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 وکوچک 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 تقریبا 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

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 غالبا 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[1] 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 فنآوری 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 فنآوری 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.
درشبکه 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 مواردر 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 درشبکه 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 بایتی 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 باطری 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.

[1] - Microelectromechanical

یکی از مهمترین سیستم های عامل درشبکه 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 فنآوری 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 نسبتا پیچیده ای استفاده می کند.
معمولا پردازنده ARM مدیریت فرستنده و گیرنده Bluetooth را برای ارسال بسته ها از طریق پورت سریال بر عهده دارد. در iMote، TinyOS 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 تجمیع، 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 نماید. 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 آنرا 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، کاملا 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 واقعا 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

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 وافزایش 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 راکم می کنند. این موارد با رفتار برنامه های کاربردی سطح بالا هماهنگ می گردد. بعنوان مثال، نمونه گیری داده با نرخی 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 بکار گیری 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

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 آنرا 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 شرائط، 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 کاملا 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 آنرا 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 اتفاقهای 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

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 می‌دهد.

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 مستقیما بر روی کارایی شبکه موثر می باشد.

۵-۱۳-۷- نرخ نمونه گیری موثر[1]

در شبکه جمع آوری داده، نرخ نمونه گیری داده اولین پارامترکارایی 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

[1] Effective sample rate

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 مستقیما 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 کاراتر 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 شرائط 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 کاملا از بین خواهد رفت. به منظور حفظ امنیت، کلید بایستی به نحوی در نود ها ذخیره شود که بازیابی آن تقریبا 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، کاملا 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

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 بلادرنگ 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 درداده 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 فنآوری شبکه های حسگر بیسیم می باشند کاهش در هزینه هر نود به معنی خرید تعداد نود بیشتر، افزاش 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

دراین بخش به بررسی برخی از حسگرهای موجود که توسط شرکت های معتبر فعال دراین زمینه ارائه شده است می پردازیم.

۵-۱۵-۱- گره حسگر MICAz

یکی از اولین و معروف‌ترین شرکت‌هایی که برای کار در زمینه شبکه‌های حسگر بوجود آمد شرکت Crossbow است. این شرکت نودهای گوناگونی را برای کاربردهای مختلف شبکه‌های حسگر تولید می‌کند. 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 حسگردارای مشخصات زیر است:

- یک پردازنده ۸ بیتی Atmel ATMega

- 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

درشکل (۵-۱۰) نمونه ای از گره های حسگر MICAz نشان داده شده است.

شکل (۵-۱۰): نمونه ای از گره حسگر MICAz وMICAz 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).

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 می‌شود.
از سوی دیگر شبکه طراحی شده باید ناحیه‌ای به مساحت صدها تا هزاران کیلومتر مربع را پوشش دهد. با وجود تعداد کم نودهای حسگرموجود در این ناحیه ، در بسیاری از مواقع برقراری ارتباط بین نودها امکان پذیر نیست.
برای مسیریابی بسته‌ها در ZebraNet دو پروتکل مختلف پیشنهاد شده است، پروتکل اول یک پروتکل flooding ساده است و پروتکل دوم پروتکلی بر مبنای تاریخچه[1] است.
ارسالflooding یک الگوریتم ساده برای مسیریابی درشبکه های حسگر بیسیم است. دراین پروتکل هرنود بسته‌های خود را برای تمام همسایه‌ها ارسال می کند. به این ترتیب می‌توان با احتمال بالایی از رسیدن بسته‌ها به مرکز مطمئن بود. گر چه ارسال سیل آسا مطمئن‌ترین 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 می‌شود که مشخص کننده میزان موفقیت آن نود در ارتباط با چاهک و ارسال داده‌ها به آن است. در ابتدا مقدار این عدد صفر است. نودها بطور متناوب همسایه‌های خود را مورد بررسی قرار می‌دهند. هنگامی که نودی در همسایگی چاهک قرار می‌گیرد یک واحد به مقدار عدد فوق افزوده می‌شود. هنگامی که نودی به تعداد دفعات مشخصی نتواند در همسایگی خود چاهک را پیدا کند، یک واحد از مقدار این عدد کسر می‌شود. برای فرستادن یک بسته به مرکز به این صورت عمل می‌شود که اگر چاهک به عنوان یکی از همسایه‌ها پیدا شود، بسته مستقیما به چاهک فرستاده می‌شود ولی اگر این طور نباشد بسته به نودی فرستاده می‌شود که بزرگترین عدد (بیشترین احتمال همسایگی با چاهک در گذشته نزدیک) را دارد. به این ترتیب سعی می‌شود 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 می‌توان نودهای حسگر به اندازه یک میلیمتر مکعب ساخت؟ اندازه این نودها آنقدر کوچک است که مانند ذرات گرد غبار می‌توانند 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 چالش‌ها و فرصت‌های بسیاری را در دنیای شبکه‌های حسگر پیش رو قرار می‌دهد.
قسمت عمده حجم پیشنهاد شده برای این نود ها را منبع تغذیه آن تشکیل می‌دهد. در حال حاضر در هر میلیمتر مکعب ازباتری‌های موجود، حداکثر حدود ۱ ژول انرژی می‌توان ذخیره کرد. به همین خاطردراینجا با محدودیت بسیار شدید انرژی روبرو هستیم. درطرح پیشنهاد شده، همچنین قسمت‌های 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 می‌کند.

[1] History based

در حال حاضر و با توجه به تکنولوژی‌های موجود، ساخت حسگرها و پردازنده‌ای 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 شبکه‌های 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 داده‌ها انتخاب کرده‌اند.

۵-۱۵-۴- دانشگاه های فعال درزمینه شبکه های حسگر

در حال حاظر تحقیقات در زمینه شبکه‌های حسگر در بسیاری از دانشگاه‌ها و مراکز تحقیقاتی جهان انجام می‌شود. از میان این دانشگاه‌ها، دانشگاه برکلی با انجام تحقیقاتی که منجر به تولید گره‌های حسگر سری mica و سیستم عامل TinyOS شده است را می‌توان پیش گام تحقیقات در این زمینه دانست. همچنین در تعداد کمی از دانشگاه‌های جهان، درسی با عنوان شبکه‌های حسگر ارائه می‌شود. از آن جمله می‌توان به دانشگاه‌های 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 مختصرا توضیح دهید.
۳. برخی از کاربردهای شبکه های حسگر بیسیم را نام ببرید.
۴. به غیراز کاربردهای ذکر شده دراین فصل، طرحی پیشنهاد کنید که درآن بتوان از شبکه های حسگر بیسیم استفاده نمود.
۵. معماری داخلی هر نود حسگر را رسم کرده واجزای آن را توضیح دهید.
۶. خصوصیات اصلی که یک نود درشبکه های حسگر بیسیم باید داشته باشد را توضیح دهید.
۷. با رسم شکل، ساختار شبکه ای حسگر را کشیده و انواع نودهای موجود درآن را تشریح کنید.
۸. نحوه توزیع و قراردادن نودها را درشبکه های حسگر بیسیم توصیف کنید.
۹. پشته پروتکل شبکه های حسگر بیسیم را رسم کرده و عملکرد هرلایه را به اختصار بنویسید.
۱۰. با رسم یک شکل، مسیریابی آگاه از انرژی درشبکه های حسگر بیسیم را توضیح دهید.
۱۱. منظور از تجمیع و آمیزش داده ها درشبکه 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 دراین 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
لایهٔ شبکه

۶-۱- مقدمه

در این فصل به بررسی لایه شبکه و وظایف آن می‌پردازیم. همان‌طور که در فصل اول به آن اشاره شد، لایه شبکه که سومین لایه در مدل مرجع OSI می‌باشد، موظف به هدایت بسته‌ها از مبدأ به سمت مقصد است. بدین‌منظور لایه شبکه باید از توپولوژی شبکه در لایه‌های پایین‌تر مطلع باشد تا بتواند بهترین مسیر ممکن را به سمت مقصد پیدا نماید. به‌طور خلاصه وظایف اصلی لایه شبکه عبارتند از:

- ارائه سرویس به لایه بالاتر از خود(لایه حمل)
- مسیریابی بسته‌ها از مبدأ به مقصد
- کنترل ازدحام
- ارتباط بین شبکه‌ای

در زیر به بررسی هر یک از وظایف فوق می‌پردازیم.

۶-۲- سرویس لایه شبکه به لایه حمل

همان‌طور که می‌دانیم در مدل لایه‌ای، هر لایه موظف به ارائه سرویس مناسب به لایه بالاتر از خود می‌باشد. لایه شبکه، نیز موظف به فراهم‌آوردن سرویس لازم برای لایه حمل می‌باشد. در طراحی سرویس لایه شبکه بایدسرویس مستقل ازفن‌آوری شبکه طراحی شود. همان‌طور که قبلاً اشاره شد در هر لایه شبکه در مدل OSI دو نوع سرویس می‌تواند موجود باشند که عبارتند از: سرویس اتصال‌گرا و سرویس بی‌اتصال. لایه شبکه نیز قادر به ارائه هر دو نوع سرویس ذکرشده به لایه حمل می‌باشد.

در سرویس اتصال‌گرا ابتدا کاربر با ارسال پیام خاصی به شبکه ، از آن درخواست برقراری اتصال به یک مقصد خاص می‌کند. چنانچه شبکه منابع کافی در اختیار داشته باشد، با درخواست کاربر موافقت می‌کند و یک مسیر مشخص از مبدأ به مقصد برای کاربر فراهم می‌آورد. به این مسیر به‌وجود آمده دراصطلاح مدار مجازی گفته می‌شود. بسته‌های ارسالی فرستنده

به ترتیب از این مسیر ارسال می‌شوند تا این‌که ارسال اطلاعات به اتمام برسد. بعد از اتمام ارسال اطلاعات، مسیر مجازی به‌وجودآمده از بین می‌رود. به خاطر به‌وجود آمدن یک مسیر اولیه بین مبدأ و مقصد، تمامی بسته‌ها به ترتیب از این مسیر عبور می کنند و به مقصد تحویل داده می‌شوند. بنابراین ترتیب بسته‌ها در سرویس اتصال‌گرا، حفظ می‌شود. همچنین لایه شبکه در سرویس اتصال‌گرا موظف به کنترل سرعت و کنترل جریان داده‌ها از مبدأ به مقصد می‌باشد. در شبکه‌های اتصال‌گرا این احتمال وجود دارد که در شبکه چندین مسیر مجازی موجود باشد، در این صورت برای مشخص‌نمودن این‌که بسته ورودی به کدام مدار مجازی موجود در شبکه اختصاص دارد، از یک فیلد به نام شناسه اتصال استفاده می‌شود.

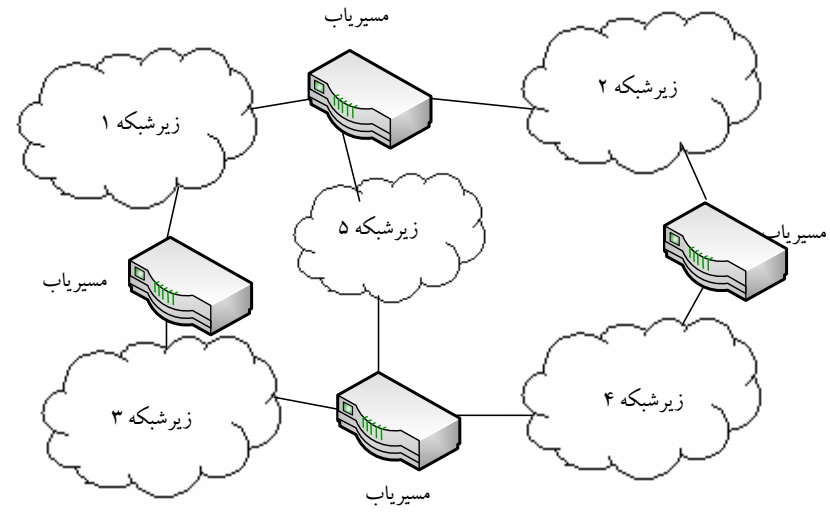
درسرویس بدون اتصال، فرستنده بدون هیچ‌گونه عملیات اولیه‌ای، اقدام به ارسال قاب‌های خود می‌کند. در این صورت قاب‌های ارسالی به‌طور مستقل پردازش می‌شوند و این احتمال وجود دارد که از مسیرهای متفاوتی به مقصد ارسال گردند. بنابراین ممکن است که ترتیب بسته‌ها در مقصد از بین برود. با مقایسه سرویس اتصال‌گرا با سرویس بی‌اتصال می‌توان به این نتیجه رسید که سرویس اتصال‌گرا پیچیدگی بیشتری نسبت به سرویس بی‌اتصال دارند. چنانچه یک شبکه در سطح لایه سوم از سرویس اتصال‌گرا استفاده نماید، به آن شبکه مدار مجازی گفته می‌شود. همچنین شبکه‌هایی که از سرویس بی‌اتصال استفاده می‌نمایند، شبکه‌های داده‌گرام نامیده می‌شوند. در زیر به مقایسه این دو نوع شبکه از جنبه‌های مختلف می‌پردازیم:

- ***آدرس‌دهی:*** با توجه به این‌که در شبکه‌های مدارمجازی ابتدا قبل از ارسال داده‌ها، یک مسیر مشخص بین مبدأ و مقصد به‌وجود می‌آیدوسپس داده‌های ارسالی از این مسیر راهی مقصد می‌شوند، بنابراین در شبکه‌های مدار مجازی به آدرس مبدأومقصد فقط در فاز برقراری اتصال اولیه نیاز می‌باشد و بعد از آن از یک مشخص‌کننده اتصال برای تعیین مدار مجازی هر بسته استفاده می‌شود. بسته‌های ارسالی در شبکه‌های داده‌گرام به‌طور مستقل پردازش می‌گردند و مسیریابی می‌شوند بنابراین در تمامی‌بسته‌های ارسالی فوق به آدرس مبدأ و مقصد نیاز می‌باشد.
- ***اطلاعات وضعیت شبکه :*** همان‌طور که گفته شد در شبکه‌های مدار مجازی این احتمال که چندین مدار مجازی مختلف در شبکه فعال باشند زیاد است. برای تمایز بسته‌های ورودی و تعیین مدار مجازی هر بسته، از یک مشخص‌کننده اتصال در هر بسته استفاده می‌شود. همچنین نودهای میانی شبکه دارای جداولی می‌باشند که در آنها اطلاعات تمام مدارهای مجازی قرار دارد. بنابراین در شبکه‌های مدار مجازی اطلاعات وضعیت شبکه ذخیره می‌شود؛ در حالی‌که در شبکه‌های داده‌گرام این اطلاعات ثبت نمی‌گردد.
- ***مسیریابی:*** در شبکه‌های مدار مجازی هنگام برقراری اتصال اولیه مسیریاب‌های شبکه با توجه به آدرس فرستنده و گیرنده اقدام به مسیریابی و انتخاب بهترین مدارمجازی ممکن بین مبدأ و مقصد می‌نمایند. بعد از آن‌که مدار مجازی به‌وجود آمد همه بسته‌های ارسالی متعلق به یک مدار مجازی خاص، از طریق فیلد مشخص‌کننده اتصال از مدار مجازی مشخص شده عبورمی کنند تا به مقصد برسند. در شبکه‌های داده‌گرام با توجه به این‌که هر بسته مستقل از بسته‌های دیگر پردازش می‌شود، هر بسته ورودی به‌طور جداگانه مسیریابی می‌شود.
- ***خراب‌شدن یک نود :*** در شبکه‌های مدار مجازی چنانچه یکی از نودهای میانی شبکه از کار بیافتد، در این صورت تمامی‌مدارهای مجازی عبوری از آن از بین می‌روند، در حالی‌که در شبکه‌های داده‌گرام با خراب‌شدن یک نود، سایر نودهای شبکه بسته‌های ورودی را از طریق نودهای دیگر به سمت مقصد هدایت می‌کنند.
- ***کنترل ازدحام:*** در شبکه‌های مدار مجازی چنانچه بافر کافی برای نودهای میانی شبکه در نظر گرفته شود، کنترل ازدحام به سادگی انجام می‌گردد؛ در حالی‌که کنترل ازدحام در شبکه‌های داده‌گرام مشکل تر از شبکه‌های مدار مجازی می‌باشد.

- ***پیچیدگی:*** شبکه‌های مدار مجازی بیشترین پیچیدگی را درسطح لایه شبکه دارند درحالی‌که درشبکه‌های داده‌گرام بیشترین پیچیدگی در سطح لایه حمل می‌باشد.

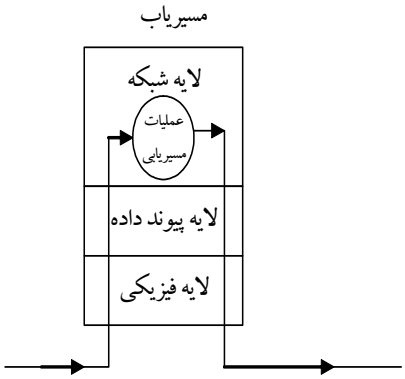
۶-۳- مسیریابی

در طی چند سال اخیر میزان تقاضا برای شبکه‌های 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 می‌گردد. با استفاده از مسیریاب های شبکه امکان دسترسی به شبکه جهانی اینترنت و سرویس آن فراهم می‌آید. در شکل (۶-۱) نمونه ای از اتصال زیر شبکه‌های مختلف از طریق مسیریاب های شبکه نشان داده شده است. درون زیرشبکه‌ها از پروتکل های مختلفی نظیر Ip ، Ipx ، X.25 ، XNS ، .... استفاده می‌شود . هرمسیریاب برای انجام عملیات مسیریابی از پروتکل های مسیریابی مانند : OSPF, RIP ,IS-IS و ... استفاده می‌کند.



شکل (۶-۱): اتصال شبکه‌های مختلف با کمک مسیریاب به یکدیگر

مسیریاب‌های شبکه در سطح لایه سوم مدل مرجع OSI عمل می نمایند. لایه شبکه داده‌های لایه حمل را دریافت نموده و با افزودن سرآیندهای مناسبی نظیر آدرس منطقی مبدأ و مقصد، آن را به لایه پایین تر تحویل می‌دهد. در شکل (۶-۲) مدل لایه ای مسیریاب نشان داده شده است.

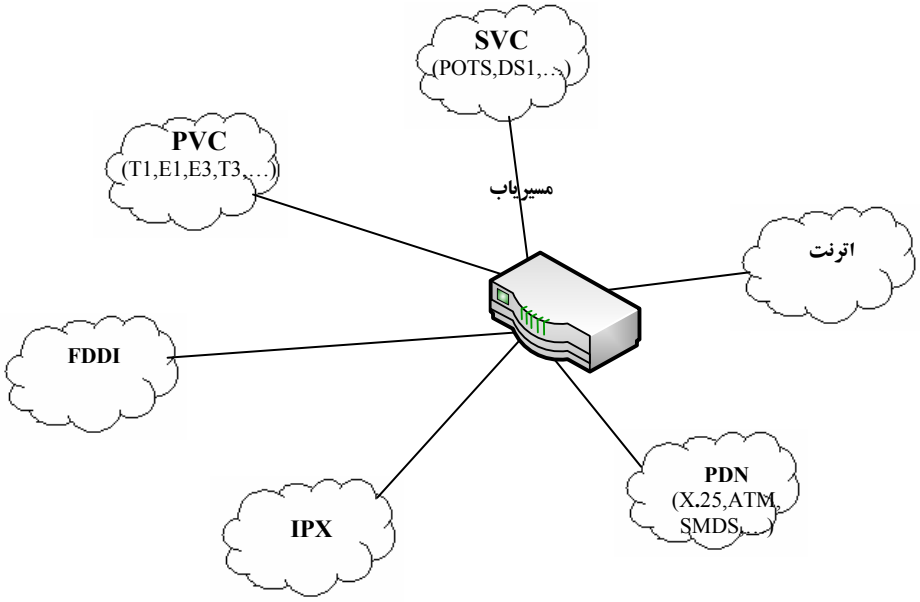


شکل (۶-۲): مدل لایه ای یک مسیریاب شبکه

مسیریاب‌های شبکه، عملیات فیلترینگ و هدایت به جلو بسته‌های ورودی را انجام می‌دهند. از مسیریاب‌ها می‌توان به‌عنوان یک تکرارکننده و یا پل نیز استفاده نمود. به غیرازهدایت بسته‌ها از مبدأ به مقصد، هر مسیریاب قادر به ارائه سرویس ارزش افزوده دیگری نیز می‌باشد 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 فن‌آوری مختلف شبکه می‌باشد .هر مسیریاب شبکه، برای هدایت بسته‌ها به مقصد از الگوریتم‌های مسیریابی استفاده می‌کند. هر چند اجزای هر الگوریتم مسیریابی با یکدیگر متفاوت می‌باشد اما تمام آنها دارای اهداف مشخص زیر می‌باشند:

- ***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[۳]:*** چنانچه توپولوژی شبکه تغییر نماید، الگوریتم مسیریابی باید دوباره بهترین مسیر را به‌دست آورد.
- ***سادگی پیاده سازی:*** الگوریتم مسیریابی باید حتی الامکان پهنای باند شبکه را اشغال ننماید و بالاسری پردازش کمی داشته باشد.



شکل(۶-۳): فن‌آوری های مختلف مسیریاب

۶-۳-۱- الگوریتم‌های مسیریابی

---

[۱] Traffic sequencing

[۲] Security filtering

[۳] Robustness

مهمترین وظیفه لایه شبکه، مسیریابی و راهبری بسته‌های اطلاعاتی از ماشین مبدأ به ماشین مقصد است. در بیشتر زیرشبکه‌ها، بسته‌های 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 بسته‌ها به آن مسیر هدایت شوند. الگوریتم مسیریابی، بخشی از نرم‌افزار لایه شبکه است؛ که موظف به تصمیم‌گیری درباره کانال خروجی یک بسته ورودی و هدایت آن درکانال فوق می‌باشد. درشبکه‌های داده گرام برای هر بسته ورودی باید این تصمیم‌گیری صورت گیرد؛ چرا که دراین شبکه‌ها ممکن است بهترین مسیر به‌طور دایم تغییر کند. در شبکه‌های مدارمجازی، یافتن مسیر فقط در فاز برقراری ارتباط انجام می‌شود. در هر صورت، آنچه که در مسیریابی مهم است : صحت، سادگی، پایداری، قدرت ، شفافیت و بهینه بودن مسیرانتخابی می‌باشد.

شاید بتوان گفت پایداری، مهمترین هدف برای الگوریتم مسیریابی است. البته لازم به ذکر است که ممکن است درمواردی دراهداف فوق تداخل پیش بیاید و این اهداف با یکدیگر متضاد باشند اما در هرصورت می‌توان به سطحی رسید که تمام اهداف تا حدودی برآورده شوند.

الگوریتم‌های مسیریابی را می‌توان به دو گروه عمده تقسیم کرد: الگوریتم‌های غیروفقی والگوریتم‌های وفقی. الگوریتم‌های غیروفقی، تصمیم‌های مسیریابی خود را بر اساس ترافیک و توپولوژی جاری شبکه انجام نمی‌دهند، بلکه انتخاب مسیر از هر نود به نود دیگر، زمانی که شبکه راه‌اندازی می‌شود صورت می گیرد. به اینگونه مسیریابی، مسیریابی ایستا نیز گفته می‌شود.

الگوریتم‌های وفقی، تصمیمات مسیریابی خود را با تغییر توپولوژی و غالباً ترافیک، تغییر می‌دهند. این الگوریتم ها، اطلاعات مسیریابی را به نحوی متفاوت با الگوریتم‌های ایستا به‌دست می‌آورند و نیز مسیر خود را زمانی که بار ترافیکی و یا توپولوژی شبکه تغییر می‌کند، تغییر می‌دهند. به این الگوریتم‌ها، الگوریتم‌های پویا نیز گفته می‌شود.

۶-۳-۱-۱- الگوریتم‌های ایستا

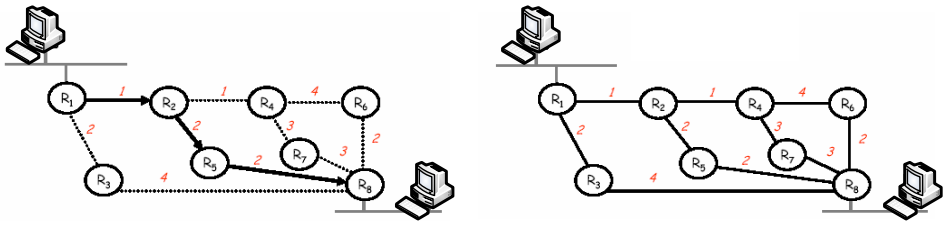
برای تشریح الگوریتم‌های مسیریابی، زیر شبکه به‌صورت یک گراف درنظرگرفته می‌شود که هر نود آن یک مسیریاب است و هریال، معرف یک کانال ارتباطی است. برخی از مهمترین الگوریتم‌های مسیریابی ایستا در شبکه‌های کامپیوتری به شرح زیر می‌باشند:

- ***الگوریتم کوتاهترین مسیر***[1]:در این الگوریتم، هدف یافتن کوتاهترین مسیر موجود بین مبدأ و مقصد می‌باشد که این کوتاهترین مسیر تعابیر متفاوتی می‌تواند داشته باشد واین تعابیر بر اساس معیارهای مختلف صورت می گیرد. مثلاً میتوان از معیار تعداد پرش‌هایی که باید در طی مسیر از آنها گذشت استفاده نمود. براساس این معیارها به هر یال گراف شبکه، یک برچسب نسبت داده می‌شود که از این برچسبها برای محاسبه کوتاهترین مسیر استفاده می‌گردد. برچسب های موجود برروی هریال شبکه معرف مشخصه‌های گوناگونی نظیر فاصله، پهنای باند، متوسط ترافیک، هزینه ارتباطی، متوسط طول صف و تاخیراندازه گیری شده می‌باشند. با اجرا شدن الگوریتم کوتاهترین مسیر برروی مسیریاب های شبکه ، فاصله همه نودهای دیگر بامسیریاب جاری مشخص می‌شود. یکی از مهمترین الگوریتم‌های مسیریابی کوتاهترین فاصله، الگوریتم Dijestra می‌باشد. درشکل (۶-۴) مثالی از الگوریتم فوق آورده شده است. دراین شکل کوتاهترین مسیر بین کامپیوتر میزبان A و کامپیوتر میزبان B از طریق مسیریاب های R1-R2-R5-R6 می باشد.
- ***الگوریتم سیل***[2]: الگوریتم ایستای دیگری که در این‌جا معرفی می‌شود، الگوریتم سیل است. در این الگوریتم هر نود شبکه هر بسته اطلاعاتی دریافتی خود را به کلیه درگاه‌های 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

[1] Shortest path

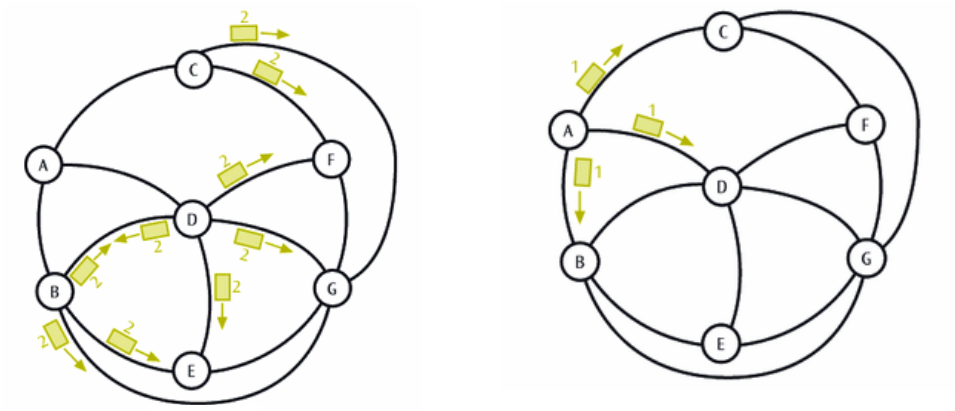
[2] Flooding

اطلاعاتی، یک فیلد در قسمت سرآیند وجود دارد که حاوی یک شمارنده می‌باشد. هر بار که بسته ای به یک نود می رسد و نود می خواهد آن را منتشر کند، یکی ازمقدار این فیلد کم می‌شود. زمانی که مقدار فیلد فوق به صفر رسید، نود دریافت‌کننده بسته از انتشار آن جلوگیری می‌کند. درحالت ایده آل مقدار اولیه این شمارنده باید برابر با تعداد پرش‌های 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 می‌کند. یک روش دیگر برای جلوگیری ازانتشار بی‌خودی بسته‌ها این است که هر بسته دارای یک شماره سریال خاص خود باشد. هرنود شبکه که یک بسته ورودی را منتشر می سازد، شماره سریال آن را در حافظه خود ذخیره می‌کند. با ورود بسته جدید ابتدا شماره سریال آن با شماره سریال بسته‌های موجود درحافظه مقایسه می‌شودو درصورت عدم تطابق، بسته ورودی منتشر می‌گردد. البته باید از مکانیسم‌های کنترلی برای جلوگیری از رشد بیش از حد لیست شماره سریال های بسته‌ها در حافظه های نودهای میانی شبکه استفاده نمود. درشکل (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

۶-۳-۱-۲- الگوریتم‌های پویا

در بیشتر شبکه‌های کامپیوتری امروزی، از الگوریتم‌های مسیریابی پویا به جای الگوریتم‌های ایستا استفاده می‌شود. دو الگوریتم مسیریابی پویای بردارفاصله[1] و وضعیت لینک[2] ازاهمیت زیادی در شبکه‌های کامپیوتری برخوردار می‌باشند که به بررسی آنها می پردازیم.

الگوریتم مسیریابی بردار فاصله

در این الگوریتم هرمسیریاب یک جدول (یک بردار)، که نشان دهنده بهترین مسیر شناخته شده تا هر مقصد و نحوه رسیدن به آن مقصد است را ذخیره می‌کند. این جداول با تبادل اطلاعات بین همسایه‌ها به روزآوری می‌شوند. این الگوریتم با نامهای دیگری نظیر الگوریتم مسیریابی توزیع شده بل من- فورد والگوریتم فورد-فوجستون نیز شناخته می‌شود . الگوریتم فوق اولین الگوریتم مسیریابی استفاده شده درشبکه آرپانت می‌باشد. الگوریتم مسیریابی[3] RIP که امروزه در شبکه جهانی اینترنت استفاده می‌شود، از روش مسیریابی بردار فاصله استفاده می‌کند. بسیاری از شرکت‌های تولید کننده مسیریاب، نظیرشرکت Apple Talk و Cisco نیز از فرم پیشرفته این الگوریتم درمسیریاب های خود استفاده می کنند. الگوریتم مسیریابی بردار فاصله یک الگوریتم وفقی‌می‌باشد که در آن هر مسیریاب شبکه به‌طور متناوب در فواصل زمانی معین جدول مسیریابی خود را برای دیگر مسیریاب‌های شبکه ارسال می‌کند. هر مسیریاب با دریافت جداول مسیریابی از مسیریاب‌های مجاورخود، اقدام به روزآوری جدول مسیریابی خودمی‌کند. طبیعی است که بعد از مدتی، جدول مسیریابی کلیه مسیریاب‌های شبکه به روزآوری می‌شود و بدین ترتیب هر مسیریاب، کل شبکه را شناسایی‌می‌کند.

به‌عنوان مثال برای درک بیشتر این الگوریتم شبکه نشان داده شده در شکل (۶-۶) را در نظر بگیرید. دراین شکل هفت شبکه مختلف از طریق مسیریاب‌های A,B,C,D,E و F به یکدیگر متصل شده‌اند. در شروع کار شبکه، هرمسیریاب فقط شبکه‌هایی را که به آنها اتصال مستقیم داردمی‌شناسد. در مثال فوق، ارزش عددی هر لینک ۱می‌باشد. به عبارت دیگر مسیریاب‌های شبکه در انتخاب مسیر، مسیری را که دارای کمترین پرش می‌باشد، در نظرمی‌گیرند.

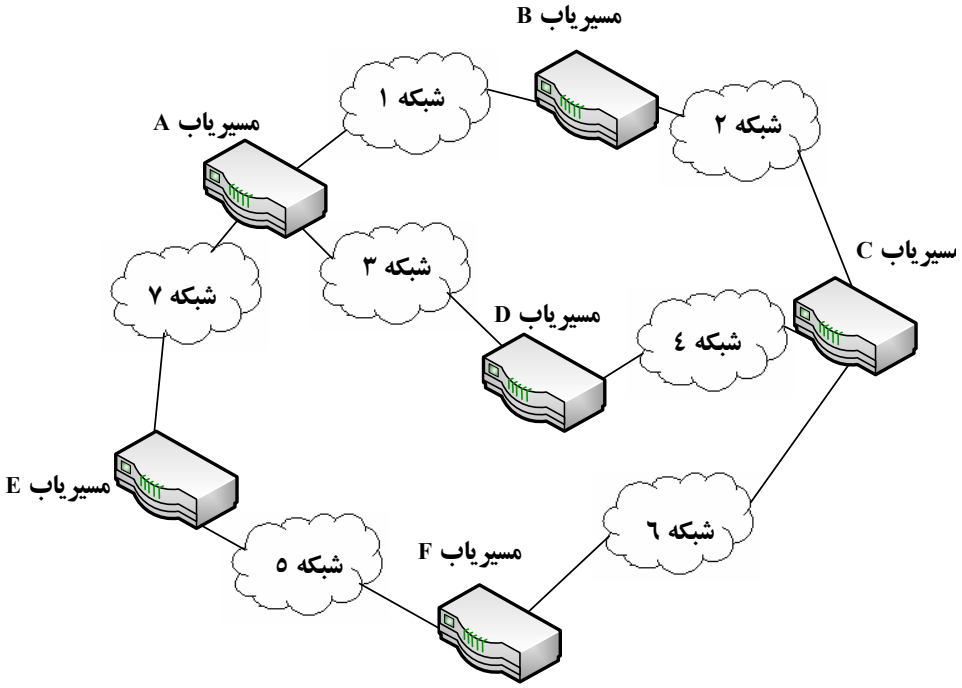
در شکل (۶-۷) نحوه به روزآوری جداول مسیریابی مسیریاب‌های شبکه نشان داده شده است. دیده می‌شود که بعدازگذشت مدتی، تمامی مسیریاب های شبکه ازوضعیت شبکه مطلع شده وجدول مسیریابی خود را کامل می‌نمایند. البته بعد از این‌که جداول مسیریابی شبکه کامل شد، مسیریاب‌های شبکه همچنان به‌طور متناوب هر چند وقت یک بار اقدام به ارسال جداول مسیریابی خود به یکدیگرمی‌نمایند. بدین ترتیب اگر تغییری در شبکه رخ دهد، نزدیکترین مسیریاب متوجه تغییرمی‌شود و بعد از مدتی تمام مسیریاب های شبکه از بروز تغییر فوق آگاه می‌شوند.

---

[1] Distance vector routing

[2] Link state routing

[3] Routing Information Protocol



شکل(۶-۶): یک شبکه نمونه برای توصیف مسیریابی بردار فاصله

زمـــان ۰

مســـیریاب A

مسیریاب بعدی	فاصله	شبکه مقصد
–	۱	۱
–	۱	۷
–	۱	۳

مســـیریاب B

مسیریاب بعدی	فاصله	شبکه مقصد
–	۱	۱
–	۱	۲

مســـیریاب C

مسیریاب بعدی	فاصله	شبکه مقصد
–	۱	۲
–	۱	٤
–	۱	٦

مســـیریاب D

مسیریاب بعدی	فاصله	شبکه مقصد
–	۱	۳
–	۱	٤

مســـیریاب E

مسیریاب بعدی	فاصله	شبکه مقصد
–	۱	۵
–	۱	۷

مســـیریاب F

مسیریاب بعدی	فاصله	شبکه مقصد
–	۱	۵
–	۱	٦

زمـــان T

مسیریاب بعدی	فاصله	شبکه مقصد
–	۱	۱
–	۱	۷
–	۱	۳
B	۲	۲
D	۲	٤
E	۲	۵

مسیریاب بعدی	فاصله	شبکه مقصد
–	۱	۱
–	۱	۲
A	۲	۳
A	۲	۷
C	۲	٤
C	۲	٦

مسیریاب بعدی	فاصله	شبکه مقصد
–	۱	۲
–	۱	٤
–	۱	٦
B	۲	۱
D	۲	۳
F	۲	۵

مسیریاب بعدی	فاصله	شبکه مقصد
–	۱	۳
–	۱	٤
A	۲	۱
A	۲	۷
C	۲	۲
C	۲	٦

مسیریاب بعدی	فاصله	شبکه مقصد
–	۱	۵
–	۱	۷
A	۲	۱
A	۲	۳
F	۲	٦

مسیریاب بعدی	فاصله	شبکه مقصد
–	۱	۵
–	۱	٦
E	۲	۷
C	۲	۲
C	۲	٤

زمـــان 2T

مسیریاب بعدی	فاصله	شبکه مقصد
–	۱	۱
–	۱	۷
–	۱	۳
B	۲	۲
B	۳	٦
E	۲	۵
D	۲	٤

مسیریاب بعدی	فاصله	شبکه مقصد
–	۱	۱
–	۱	۲
A	۲	۳
A	۲	۷
C	۲	٤
C	۳	۵
C	۲	٦

مسیریاب بعدی	فاصله	شبکه مقصد
–	۱	۲
–	۱	٤
–	۱	٦
B	۲	۱
D	۲	۳
F	۳	۷
F	۲	۵

مسیریاب بعدی	فاصله	شبکه مقصد
–	۱	۳
–	۱	٤
A	۲	۱
A	۲	۷
C	۲	۲
C	۳	۵
C	۲	٦

مسیریاب بعدی	فاصله	شبکه مقصد
–	۱	۵
–	۱	۷
A	۲	۱
A	۲	۳
A	۳	۲
A	۳	٤
F	۲	٦

مسیریاب بعدی	فاصله	شبکه مقصد
–	۱	۵
–	۱	٦
E	۲	۷
C	۲	۲
E	۳	۱
E	۳	۳
C	۲	٤

شکل(۶-۷): مراحل تکمیل جدول مسیریابی شبکه نشان داده درشکل (۶-۶)

مسیریابی وضعیت لینک

مسیریابی وضعیت لینک، یک جایگزین مناسب با قابلیت انعطاف پذیری بالاتر و قدرت بیشتراز مسیریابی بردار فاصله است که منشأ پیدایش آن شبکه آرپانت می‌باشد. استفاده از این الگوریتم درچند سال اخیرگستردگی زیادی یافته است، به‌طوری که امروزه در اینترنت هم از این نوع مسیریابی استفاده وسیعی می‌شود. دو مشکل عمده روش مسیریابی بردار فاصله، باعث گردید که امروزه از مسیریابی وضعیت لینک در شبکه جهانی اینترنت استفاده وسیعی شود. نخست این‌که در مسیریابی بردار فاصله، معیارمحاسبه تاخیرطول صف می‌باشد و الگوریتم هیچ توجهی به پهنای باندخطوط برای ارزیابی تاخیر ندارد. مساله دوم این‌که همگرا شدن الگوریتم بردارفاصله وقتی که مکانیسمهای شناسایی حلقه های مسیریابی نیز استفاده می‌شوند طولانی می‌باشد. به‌علت وجود دو مشکل فوق در مسیریابی بردار فاصله، مسیریابی وضعیت لینک جایگزین آن گردید. امروزه شکلهای متنوعی از این نوع مسیریابی به‌طور گسترده در شبکه‌های کامپیوتری استفاده می‌شود.

در مسیریابی وضعیت لینک هر مسیریاب بایدمراحل زیر را اجرا نماید:

۱- همسایگانش را شناسایی نماید و آدرس شبکه آنها را یاد بگیرد.

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 واین بسته اطلاعاتی را به کلیه مسیریاب‌های دیگر ارسال کند.

۴- کوتاهترین مسیر تا هر یک از مسیریاب های دیگر را حساب کند.

طبق آنچه که در شماره ۳ گفته شده است، هر مسیریاب موظف به ساختن یک بسته اطلاعاتی است، که این بسته اخبار وضعیت لینک(LSA[1]) نامیده می‌شود. پس ازآن‌که ساخت LSA در مسیریاب کامل گردید، نوبت به ارسال آن به دیگر مسیریاب‌ها است که این‌کار به عهده یک پردازه به نام سیل می‌باشد. در واقع ایده اصلی عملکرد این پردازه ازهمان روش مسیریابی سیل که در بخش الگوریتم‌های ایستا گفته شد، گرفته شده است. پردازه سیل باید سریع و قابل اعتماد باشد. بعد ازگذشت چند دوره زمانی، پایگاه‌های داده وضعیت لینک درمسیریاب ها همگرا و یکسان خواهند شد. هر چه الگوریتم بهتر باشد این زمان همگرایی کوتاهترخواهد بود. زمان همگرایی در الگوریتم فوق به میزان تأخیر انتشاردر شبکه نیز بستگی دارد. بعد از همگرائی پایگاه‌های داده به کمک آن بهترین مسیر برای رسیدن به سایر نودها محاسبه می‌شود که دراصطلاح به این مرحله محاسبه مسیرگفته میشود. در مرحله محاسبه مسیرغالباً از الگوریتم‌های کوتاهترین فاصله نظیر Dijestra استفاده می‌شود. به همین جهت گاهی به پروتکل‌های وضعیت لینک، پروتکل‌های مبتنی بر کوتاهترین مسیرنیزگفته میشود. البته به غیر از الگوریتم کوتاهترین فاصله، می‌توان ازالگوریتم‌های دیگرنیز استفاده نمود.

یکی از مسائل مهم در الگوریتم وضعیت لینک، بروز آوری LSA ها است. هر مسیریاب شبکه، زمانی که در محیط محلی اش تغییری رخ میدهد، LSA های خود را به روز درمی‌آورد. مدت زمانی که طول می کشد تا مسیریاب متوجه بروز تغییرات در محیط محلی اش شود، تأثیرزیادی در واکنش یک پروتکل وضعیت لینک به تغییرات شبکه دارد. ممکن است توسط دیگر پروتکل‌های درحال اجرا درمسیریاب‌های شبکه، تغییرات در محیط عملیاتی محلی هرمسیریاب تشخیص داده شود. در بسیاری از پروتکل‌های وضعیت لینک، به‌طورمتناوب هرمسیریاب نشانه "سلام" را به دیگرهمسایگانشان می فرستد تا بدین‌وسیله متوجه غیبت احتمالی یک مسیریاب همسایه گردد. برای کسب اطمینان بیشتر، اکثر پروتکل‌های وضعیت لینک به‌طور متناوب LSA های خود را حتی وقتی‌که در شبکه تغییری رخ نداده باشد هم به روز درمی‌آورند.

در محاسبه مسیرمی‌توان از روش‌های مسیریابی متنوعی نظیر مسیریابی پرش به پرش[2] و مسیریابی مبدأ[3] استفاده نمود. هر دو پروتکل فوق درالگوریتم مسیریابی وضعیت لینک حمایت می‌شوند. در مسیریابی پرش به پرش، بسته‌های ارسالی با استفاده از آدرس گیرنده بسته به سمت مقصد هدایت می‌شوند. دراین روش بسته ورودی به هرمسیریاب (پرش) که می‌رسد، آن مسیریاب به‌طور مستقل از سایر مسیریاب‌ها و با توجه به جدول مسیریابی خود وآدرس مقصد بسته، اقدام به مسیریابی بسته می‌کند. در روش مسیریابی پرش به پرش احتمال وقوع حلقه های مسیریابی زیاد می‌باشد.

برای درک بهتر پروتکل مسیریابی وضعیت لینک، به ذکر یک مثال می پردازیم. به عنوان مثال شبکه نشان داده شده درشکل (۶-۸) (الف) را درنظر 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, ACDBE وجود دارد. بدیهی است که بهترین مسیر موجود مسیرABDE می باشدکه دارای هزینه کمتر از سایر مسیرها است. مراحل الگوریتم وضعیت لینک به شرح زیر است:

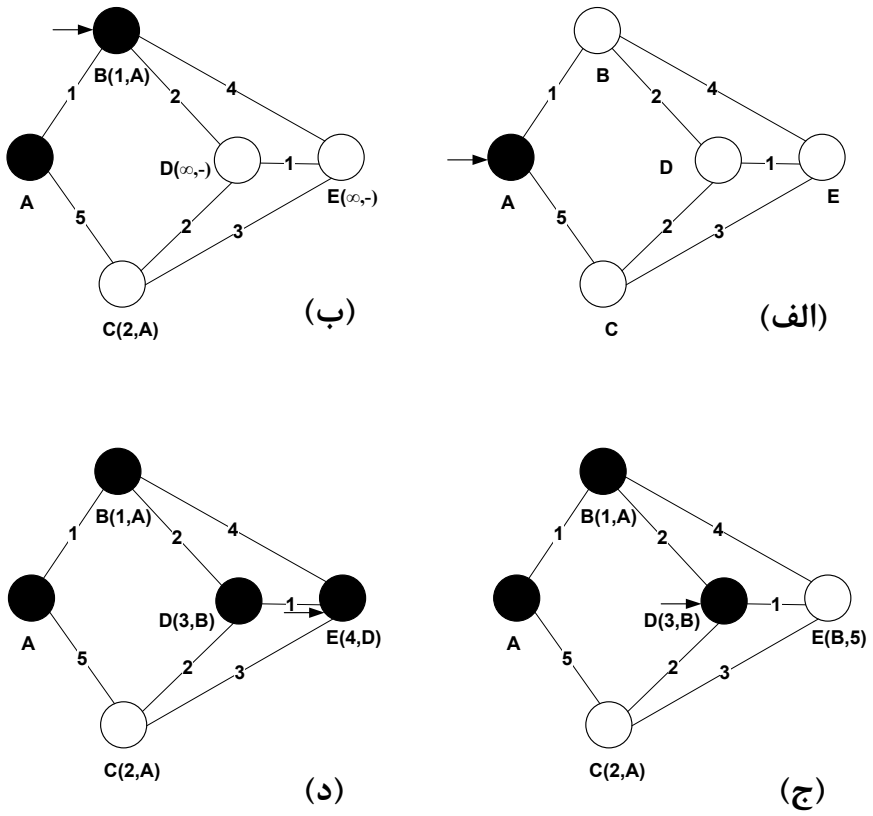
---

[1] Link State Advertisement

[2] Hop by hop routing

[3] Source routing

۱. ابتدا نود مبدا A به عنوان نود شروع انتخاب شده و وضعیت آن دائمی می شود. نودهای دائمی درشکل بـه صـورت دایره پررنگ نشان داده می شوند. نودهایی که دائمی نشده اند با دایره خالی نشان داده شده اند.
۲. با توجه به شکل، ازبین نودهای B وC که ارتباط مستقیم به نود شروع A دارند، نود B به عنوان نود بعدی درمسیر انتخاب می شود. این نود درمقایسه با نود C دارای فاصله کمتری تا نود مبدا A است. وضـعیت نـود B بـه صـورت 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 بدسـت مـی آینـد. بـا توجه به شکل فوق نودهایD وE به نود B متصل بوده ولی نود D دارای فاصله کمتری تا B بوده و بنـابراین ایـن 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 انتخـاب می شود.
۵. با توجه به اینکه نود E نود مقصد می باشد، بنابراین الگوریتم خاتمه یافته و مسیر ABDE بـا فاصـله برابـر بـا ۵ بدست می آید.



شکل(۶-۸): مثالی از مسیریابی وضعیت لینک

۶-۴- کنترل ازدحام

یکی دیگر از وظایف مهم لایه شبکه کنترل ازدحام‌می‌باشد. هنگامی‌که تعداد بسته‌های ارسالی کاربران به شبکه بیش از حد زیاد باشد، در این صورت بافر اکثر نودهای شبکه پرمی‌شود و پس از آن نودهای شبکه قادر به ارائه سرویس مطلـوب بـه کاربران خودنمی‌باشند. در یک شبکه کامپیوتری، تعداد بسته‌های تحویل داده شده به مقصد، متناسب بـا تعـداد بـسته‌هـای

ارسالی‌می‌باشد. چنانچه بسته‌های ارسالی بیش از ظرفیت شبکه باشند، در این صورت نودهای شبکه قادر به تحمل انبوه بسته‌های ورودی نمی‌باشند و بدین ترتیب بسته‌های ورودی از بین می‌روند که این امر مشکل ازدحام و ازدحام را بدتر و بدتر می‌کند. چنانچه ترافیک ورودی به شبکه بیش ازحد زیاد باشد، در این صورت کارآیی شبکه به شدت افت می‌کند و تقریباً هیچ بسته‌ای به مقصد نمی‌رسد.

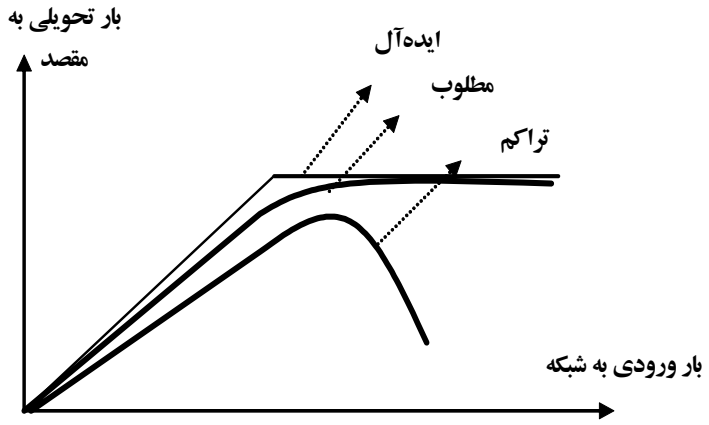
عوامل مختلفی باعث ایجاد ازدحام در شبکه‌های کامپیوتری می‌شوند. اولین عامل موثر در ایجاد ازدحام در نودهای شبکه، سرعت پردازش پایین نودهای شبکه می‌باشد. چنانچه نودهای میانی شبکه سرعت پردازش کمی‌داشته باشند، در این صورت تمامی بافرهای میانی شبکه لبریزمی‌شوند.

دومین دلیل ایجاد ازدحام در شبکه‌های کامپیوتری، کند بودن سرعت لینک‌های خروجی هر نود می‌باشد. به عبارت دیگر چنانچه نرخ ورود ترافیک به نودهای شبکه، بیشتر از ظرفیت خطوط خروجی باشد، احتمال وقوع ازدحام زیاد می‌باشد.

چنانچه در شبکه، ازدحام به‌وجود آید، بافرهای میانی شبکه لبریز می‌شوند و باگذشت زمان درصورتی‌که اقدام مناسب انجام نشود، وضعیت ازدحام بدترمی‌گردد. اگر بسته ارسالی فرستنده در بافرهای میانی شبکه از بین برود، فرستنده بعد از مدتی دوباره اقدام به ارسال بسته فوق می‌کند؛ که این امر باعث افزایش شدت ازدحام‌می‌شود. با توجه به این‌که فرستنده با ارسال هر بسته، آن را درحافظه خود ذخیره می‌سازد تا درصورت نیاز دوباره آن را ارسال نماید، چنانچه ازدحامی در شبکه به وقوع پیوندد، بسته‌های ارسالی فرستنده از بین رفته و بدین ترتیب فرستنده هیچگاه نمی‌تواند بافر خود را خالی نماید.

باید توجه نمود که کنترل ازدحام با کنترل جریان متفاوت می‌باشد. کنترل ازدحام به روال‌های لازم جهت کنترل تمام نودهای شبکه و بافرهای میانی آنها برای جلوگیری از کاهش کارآیی شبکه دلالت دارد؛ در حالی‌که کنترل جریان فقط بین دو نقطه انجام می‌شود و هنگامی‌که یک فرستنده سریع به یک گیرنده کند، داده‌هایی را ارسال می‌دارد از کنترل جریان برای تعدیل سرعت ارسال فرستنده و تنظیم آن با سرعت دریافت گیرنده استفاده‌می‌شود.

در شکل (۶-۹) نمودار تعداد بسته‌های تحویل داده شده در مقصد برحسب تعداد بسته‌های ارسالی به شبکه رسم شده است. همان‌طور که در این شکل دیده‌می‌شود، با افزایش تعداد بسته‌های ارسالی به شبکه، تعداد بسته‌های تحویل داده شده در مقصد نیز افزایش‌می‌یابد. چنانچه بسته‌های ارسالی از حدی بیشتر شوند، شبکه با ازدحام مواجه می‌گردد و قادر به ارائه کارآیی مطلوب خودنمی‌باشد.



شکل(۶-۹): تاثیر ازدحام برکارآیی شبکه

۶-۵- ارتباط بین شبکه‌ای

یکی دیگر از وظایف مهم لایه شبکه ، ارتباط بین شبکه‌ای می‌باشد. همان‌طور که در فصل اول به آن اشاره شد، شبکه‌های کامپیوتری دارای مزایای متعددی می‌باشند. شبکه‌سازی و اتصال شبکه‌های کامپیوتری به یکدیگر نیز دارای مزایای زیادی است. در راستای ایجاد یک شبکه وسیع جهانی، اتصال شبکه‌ها به یکدیگر و ایجاد یک شبکه بزرگتر دارای مزایا و اهداف متعددی می‌باشد.

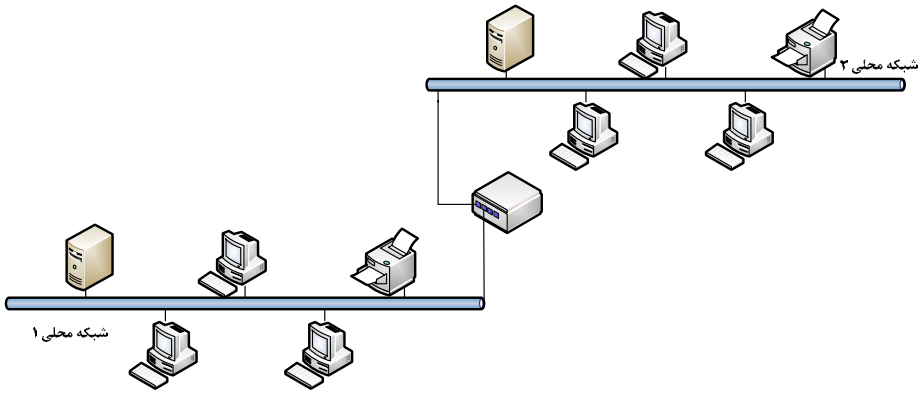
اتصال یک یا چند شبکه و ایجاد یک شبکه بزرگتر واتصال آنها به یکدیگر را ارتباط بین شبکه‌ای گویند. چنانچه فرستنده وگیرنده یک بسته در دو شبکه متفاوت با پروتکل‌های غیریکسان قرارداشته باشند، در این صورت لزوم تبدیل بسته‌ها از یک پروتکل به پروتکل دیگر و استفاده از تجهیزات خاص ارتباط بین شبکه‌ای حس‌می‌شود. به شبکه‌هایی که از اتصال چند شبکه به یکدیگر به‌وجود می آید، دراصطلاح internet گفته می‌شود. البته باید توجه نمود که شبکه جهانی Internetنمونه کاملی از یک internet است که درآن میلیون‌ها کامپیوتر به یکدیگر متصل شده‌اند.

اتصال شبکه‌ها به یکدیگر و ایجاد یک شبکه وسیعتر در رده‌های مختلفی قابل انجام‌می‌باشد که عبارتند از:

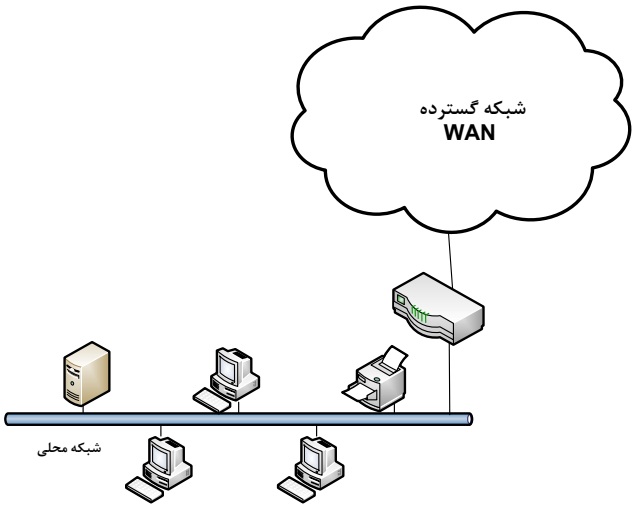
- ***اتصال*** LAN ***به*** LAN: دراین حالت دو شبکه محلی مستقیماً با کمک تجهیزات ارتباط بین شبکه ای به یکدیگر متصل می‌شوند. به‌عنوان مثال اتصال دوشبکه محلی دریک ساختمان به یکدیگرنمونه ای از اتصال LAN به LAN می‌باشد.
- ***اتصال*** LAN ***به*** WAN: دراین حالت یک شبکه محلی به یک شبکه گسترده اتصال می‌یابد. برقراری اتصال فوق به تجهیزات ارتباط بین شبکه‌ای نیاز دارد. به‌عنوان مثال اتصال شبکه محلی یک دانشگاه به اینترنت نمونه ای از اتصال LAN به WAN است.
- ***اتصال*** WAN ***به*** WAN: دراین حالت دو شبکه گسترده ازطریق تجهیزات مناسب به یکدیگر متصل شده و قادربه تبادل اطلاعات با یکدیگر می‌باشند. اتصال شبکه دیتای یک کشور به شبکه جهانی اینترنت، نمونه ای از این نوع اتصال می‌باشد.
- ***اتصال دو*** LAN ***از طریق یک یا چند*** WAN: در این حالت دو شبکه محلی که درفاصله دور از یکدیگر قرارگرفته اند، از طریق امکانات ارتباط بین شبکه ای با کمک یک شبکه گسترده به یکدیگر متصل می‌شوند. اتصال دو شبکه محلی یک سازمان ازطریق شبکه مخابرات نمونه ای از این نوع اتصال است.

درشکل (۶-۱۰) مثالی ازانواع اتصال فوق آورده شده است.

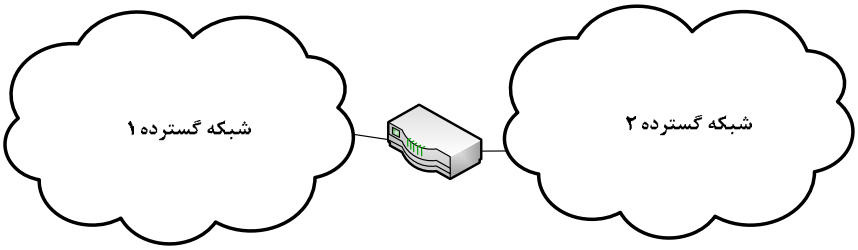
جهت اتصال دو شبکه به یکدیگر از تجهیزات ارتباط بین شبکه‌ای استفاده می‌شود. براساس این‌که دو شبکه‌ای که به یکدیگر متصل می‌شوند، درچه لایه‌هایی با یکدیگر مشترک و در چه لایه‌هایی با یکدیگر متفاوت هستند، از تجهیزات متفاوتی برای اتصال آنها به یکدیگر استفاده‌می‌شود. در زیر به بررسی مهمترین تجهیزات ارتباط بین شبکه‌ای می‌پردازیم.



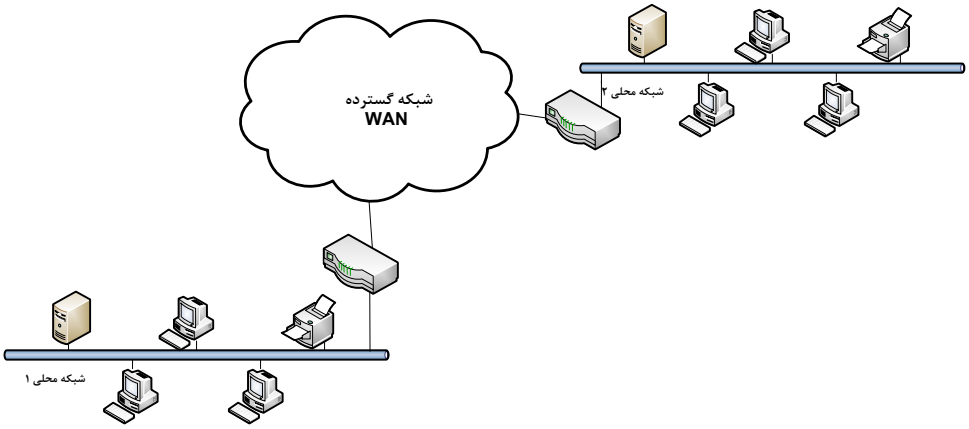
(الف)



(ب)



(ج)



(د)

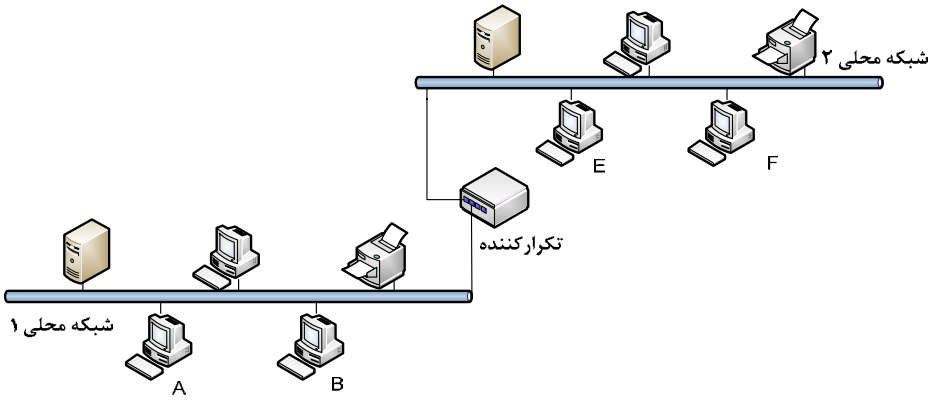
شکل (۶-۱۰) اتصال شبکه‌ها به یکدیگر

الف) اتصال LAN به LAN ب) اتصال LAN به WAN

ج) اتصال WAN به WAN د) اتصال LAN به LAN از طریق WAN

۶-۵-۱- تکرارکننده

یک تکرارکننده درسطح لایه فیزیکی عمل می‌کند و جهت گسترش شبکه‌های محلی استفاده می‌شود. همان‌طورکه درفصل قبل نیز اشاره شد، چنانچه کابل شبکه بیش ازحد طولانی باشد، دراینصورت سیگنال ارسالی درکابل تضعیف می‌شود و دیگر قابل دریافت درگیرنده نمی‌باشد. برای رفع این مشکل از تکرارکننده استفاده می‌گردد. درشکل (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 می‌شوند، در حقیقت جزئی از یک شبکه واحد می‌باشند. مطابق با شکل فوق چنانچه به‌عنوان مثال ایستگاه A قابی را برای ارسال به ایستگاه B ، وارد شبکه نماید، تمامی‌ایستگاه‌های شبکه ازجمله E و F نیز این قاب را دریافت می‌دارند. به عبارت دیگر تکرارکننده هیچ‌گونه هوشمندی در فیلترنمودن ترافیک از خود نشان نمی‌دهد و کلیه ترافیک‌های ورودی به خود را عبور می‌دهدو به طرف مقابل ارسال‌می‌دارد.



شکل (۶-۱۱) : اتصال دو قسمت مختلف شبکه توسط یک تکرارکننده

۶-۵-۲- پل

یک پل درهر دو سطح لایه فیزیکی و پیوند داده از مدل لایه‌ای OSI عمل می‌کند. توسط یک پل امکان تقسیم بندی یک شبکه بزرگ به قطعات کوچکتر فراهم می‌آید. برخلاف تکرارکننده، پل‌ها قابلیت فیلترنمودن ترافیک‌های ورودی را به خود دارند. پل آدرس مقصد قاب ورودی را بررسی می‌کند و درصورتی‌که آدرس گیرنده قاب درطرف دیگرپل قرار داشته باشد، اجازه عبور بسته را می‌دهد ولی در غیراینصورت ازعبور بسته جلوگیری می‌کند.

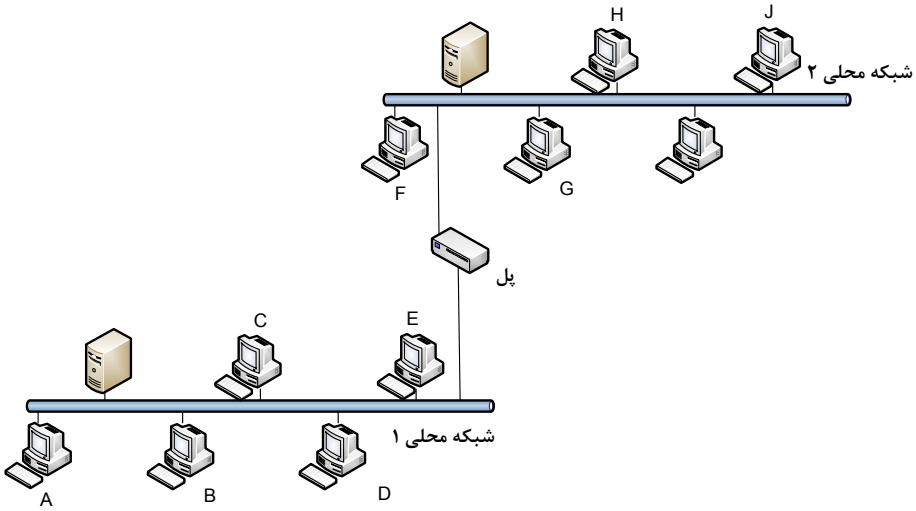
با توجه به نحوه عملکرد پل، می‌توان نتیجه گرفت که یکی از مزایای عمده آن قابلیت فیلترنمودن ترافیک و جلوگیری از ارسال ترافیک‌های ناخواسته به سایر قسمت‌های یک شبکه‌می‌باشد. در شکل (۶-۱۲) مثالی ازدوشبکه که با استفاده از پل به یکدیگر متصل شده‌اند آورده شده است. به‌عنوان مثال در این شکل، چنانچه ایستگاه A قابی‌را به مقصد ایستگاه D ارسال دارد، با توجه به این‌که فرستنده و گیرنده قاب در یک شبکه قرار دارند، پل متوجه شده و اجازه عبور قاب را ازخود نمی‌دهد؛ ولی چنانچه مقصد قاب ارسالی A، ایستگاه G باشد، قاب از پل عبور می‌کند.

هر پل برای انجام صحیح عملیات فیلترنمودن بسته‌ها، بایدحاوی یک جدول آدرس باشد که تمامی آدرس‌های فیزیکی ایستگاه‌های موجود در شبکه را دارا می‌باشد. با توجه به این‌که جدول مسیریابی آدرس فوق به چه صورت ایجاد و مدیریت شود، سه نوع مختلف از پل وجود دارند که در زیر به بررسی آنهامی‌پردازیم:

- ***پل ساده :*** این نوع پل، ساده‌ترین و ارزانترین نوع پل می‌باشد. در این نوع پل، جدول آدرس ایستگاه‌ها باید به‌صورت دستی توسط یک اپراتور واردگردد. طبیعی است که جدول فوق ثابت می‌باشد و درصورتی‌که یک ایستگاه

جدید به شبکه اضافه شود، جدول آدرس باید به‌روزآوری 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 به‌صورت خودکار اقدام به تولید جدول آدرس‌می‌کند. روش ایجاد جدول آدرس به اینصورت است که پل با شروع به کار شبکه و ارسال قاب بین ایستگاه‌های شبکه، اقدام به آموزش وفراگیری آدرس‌های فیزیکی هر یک از ایستگاه‌های شبکه می‌کند. در ابتدای راه‌اندازی شبکه، جدول آدرس‌های پل آموزش گیرنده خالی می‌باشد، ولی با گذشت زمان این جدول تکمیل می‌شود. با توجه به قدرت بالای این نوع پل و توانایی ایجاد جداول آدرس به‌صورت خودکار، قیمت پل‌های آموزش گیرنده به مراتب بیشتر از پل‌های ساده می‌باشد.
- ***پل چندین درگاهه [1]:*** سومین نوع پل، پل چندین درگاهه می‌باشد. این نوع پل که خود می‌تواند از نوع ساده و یا آموزش گیرنده باشد، دارای چندین درگاه می‌باشد ومی‌توان به‌وسیله آن چندین شبکه مختلف را به یکدیگر متصل نمود.



شکل (۶-۱۲): اتصال دو شبکه مختلف به یکدیگر به‌وسیله پل

۶-۵-۳- مسیریاب

یکی دیگر از مهمترین تجهیزات ارتباط بین شبکه‌ای، مسیریاب‌های شبکه می‌باشد. مسیریاب‌ها به آدرس‌های شبکه دسترسی دارند و با کمک نرم‌افزار مسیریابی خود، قادر به محاسبه و انتخاب بهترین مسیر بین مبدأ و مقصد می‌باشند. هرمسیریاب شبکه در سطح لایه سوم مدل مرجع OSI عمل می‌کند و با دریافت یک بسته از یکی از درگاه‌های ورودی خود و با پردازش بر روی سرآیند بسته‌های لایه سوم، آدرس گیرنده بسته را تعیین می‌کند و سپس با کمک جدول مسیریابی خود، مسیر مناسب برای ارسال بسته به مقصد را به‌دست‌می‌آورد. در شکل (۶-۱۳) مثالی از نحوه اتصال چندین شبکه به‌وسیله مسیریاب‌های شبکه آورده شده است.

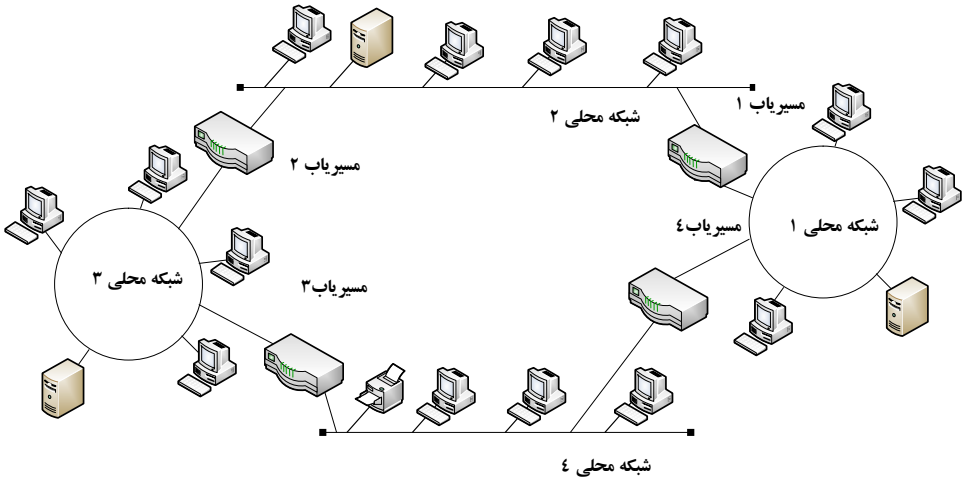
۶-۵-۴- دروازه[2]

---

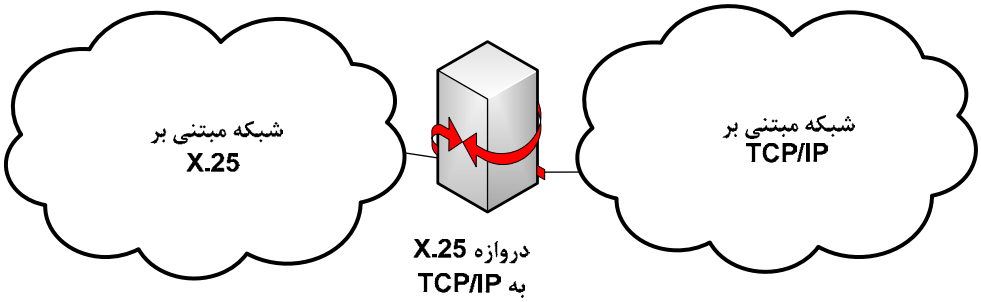
[1] Multiport bridge

[2] Gateway

مطابق با شکل (۶-۱۴) یک دروازه در سطح تمام ۷ لایه OSI عمل می‌کند. یک دروازه درحقیقت به‌صورت یک مبدل پروتکل عمل می‌کند. هنگامی‌که بخواهیم دو شبکه کاملاً متفاوت را که دارای معماری‌های مختلف هستند به یکدیگر متصل نماییم، از دروازه استفاده‌می‌شود. به‌عنوان مثال چنانچه بخواهیم یک شبکهTCP/I P را به یک شبکهX.25 متصل نماییم، با توجه به این‌که این دو شبکه دارای معماری‌های مختلف هستند و پروتکل‌های 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 مسیریاب



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 شبکه‌های مخابراتی به حساب می آید. شبکه ISDN قادر به برقراری اتصال‌های انتها به انتها برروی خطوط دیجیتال می‌باشد. بسیاری از شرکتهای مخابرات کشورها اقدام به جایگزینی شبکه آنالوگ موجود خود با شبکه کاملاً دیجیتال ISDN کرده‌اند. بدین ترتیب دراین شبکه‌ها امکان برقراری ارتباطات محلی و بین المللی با سرعت بالا و کیفیت خوب فراهم می‌آید.

در شبکه‌های ISDN ، کاربران قادر به ارسال اطلاعات داده،صوت، تصویر و فاکس بر روی یک شبکه دیجیتال واحد می‌باشند. هدف اصلی ISDN فراهم سازی سرویس دیجیتال یک پارچه برای کاربران می‌باشد. این سرویس به ۳ دسته کلی سرویس حامل[۱] ، تله سرویس و سرویس تکمیلی[۲] تقسیم بندی می‌شوند.

سرویس حامل، محیطی فراهم می‌آورند که در آن کاربران قادر به ارسال اطلاعات صوت و تصویر و داده بدون آن‌که شبکه، محتوای اطلاعات را تغییر دهد می‌باشند. در این‌گونه سرویس، شبکه اطلاعات موجود در بسته‌ها را پردازش نمی‌کند، بنابراین هیچ گونه تغییری در محتوای آنها ایجاد نمی‌شود. این سرویس متعلق به ۳ لایه اول مدل مرجع OSI می‌باشند. برای پیاده سازی سرویس حامل می‌توان از شبکه‌های سوئیچینگ مداری، سوئیچینگ بسته ای،Frame Relay یا Cell Relay استفاده نمود.

در سرویس تله سرویس، شبکه ممکن است محتویات بسته‌های دریافتی را پردازش و یا تغییر دهد. این سرویس مطابق با لایه ۴ الی ۷ مدل مرجع OSI می‌باشند. سرویس فوق متکی بر امکانات سرویس حامل هستند و برای برآورده کردن نیازهای کاربران، بدون آن‌که آنها ازجزئیات پردازش درشبکه 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 تله‌سرویس اضافه می نمایند. نمونه‌ای از این سرویس عبارتند از: سرویس شارژینگ معکوس ، انتظار مکالمه و تبادل پیام که تماماً در شرکت‌های تلفنی امروزی استفاده می‌شوند.

۶-۶-۱- تاریخچه ISDN

شبکه‌های مخابراتی اولیه تماماً به‌صورت آنالوگ عمل می‌کردند و از آنها برای ارسال اطلاعات آنالوگ نظیر صوت استفاده می‌شده است. با پیدایش پردازشهای دیجیتال، مشتریان علاوه بر صوت، محتاج به مبادله داده گردیدند. دراین زمینه مودم برای مبادله پیام‌های دیجیتال برروی خطوط آنالوگ موجود طراحی و ساخته شد.

به منظور کاهش هزینه‌ها و بهبود کارآیی شبکه، شرکت‌های تلفنی با حفظ سرویس آنالوگ خود به تدریج شروع به افزودن فن‌آوری دیجیتال به شبکه‌های 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 می‌نمودند و مشتریانی که از سرویس دیجیتال برای مبادله اطلاعات دیجیتال استفاده می کردند.

با توجه به این‌که درآن مقطع زمانی، مشتریان گروه اول برجسته ترین و بیشترین مشتریان شرکت‌های تلفنی را تشکیل می دادند، بنابراین بیشترسرویس پیشنهادی شرکتهای تلفنی همچنان آنالوگ باقی ماند. با گذشت زمان و پیدایش شبکه‌های دیجیتال، مشتریان علاقمند به استفاده از انواع شبکه‌های داده گردیدند.

به منظور برآورده کردن این نیازها شرکت‌های تلفن اقدام به ایجاد شبکه‌های مجتمع دیجیتال نمودند. یک شبکه مجتمع دیجیتال مجموعه ای از شبکه‌ها می‌باشد که برای برآورده کردن نیازهای مختلف کاربران طراحی شده است. برای دسترسی به شبکه‌های مجتمع دیجیتال از کانال‌های سرعت بالای دیجیتال که به‌صورت زمانی بین کاربران تقسیم می‌شوند، استفاده می گردد.

هر چندامروزه خطوط دیجیتالی نظیر DDS، DSS و غیره موجود می‌باشد، ولی همچنان برخی مشترکین از خطوط آنالوگ استفاده می نمایند.

---

[۱] Bearer services

[۲] Supplementary services

شبکه‌های ISDN سرویس مشترکین را با شبکه‌های مجتمع دیجیتال ترکیب می نمایند. سرویس دیجیتال به مراتب کارآمدتر و انعطاف پذیرتر از سرویس آنالوگ می‌باشند. به منظور دستیابی به مزایای شبکه‌های مجتمع دیجیتال ، خطوط آنالوگ موجود با خطوط دیجیتال جایگزین می‌شوند. در این حالت صوت آنالوگ درمبدأ تبدیل به دیجیتال می‌شود و نیازی به حامل‌های آنالوگ ندارد. بنابراین امکان ارسال داده، صوت، تصویر و فاکس بر روی شبکه‌های دیجیتال فراهم می‌شود.

در شبکه‌های ISDN تمام سرویس مشتریان از آنالوگ به دیجیتال تبدیل می‌شوند. به خاطر انعطاف پذیری بالای این شبکه‌ها، امکان دسترسی کاربران به سرویس درخواستی وجود دارد. هر کاربر از طریق یک خط دیجیتال به اداره مرکزی ISDN متصل می‌شود. سرعت خطوط دیجیتال متناسب با نیازهای کاربران ، متفاوت می‌باشد.

برای دسترسی به انعطاف پذیری بیشتر، خطوط دیجیتال بین مشتریان و شبکه ISDN به کانال‌هایی با اندازه‌های متفاوت تقسیم بندی می‌شود. در ISDN ، سه نوع کانال وجود دارد که هریک دارای نرخ ارسال متفاوتی هستند. این۳ کانال عبارتند از: کانالB (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 می‌باشد که با کمک آن کابران قادر به ارسال هر گونه اطلاعات دیجیتال به‌صورت دو طرفه با حداکثر نرخ ارسال ۶۴ کیلو بیت بر ثانیه می‌باشند. به‌عنوان مثال از کانالB می‌توان برای مبادله داده‌های دیجیتال، صوت دیجیتال و یا سایر اطلاعات کم‌سرعت استفاده کرد. با استفاده از تسهیم‌سازها می‌توان داده‌های چندین منبع مختلف را به‌صورت یک‌جا بر روی خطوط ارسال کرد.

کانال‌های D ، باتوجه به نیاز کاربران می‌توانند دارای سرعت ۱۶ یا ۶۴ کیلوبیت برثانیه 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 شبکه‌های ISDN سیگنال‌های کنترلی از کانال مخصوص خود(کانال D) استفاده می کنند. به این حالت، سیگنالینگ کانال مشترک گفته می‌شود، زیرا کانالD اطلاعات سیگنالینگ تمام مشتریان موجود در یک مسیر را حمل می‌کند.

کانال‌های H برای دسترسی به سرعت‌های بالاتر نظیر ۳۸۴ کیلوبیت بر ثانیه (H_0) ، ۱۵۳۶ کیلو بیت بر ثانیه (H_{11}) و ۱۹۲۰ کیلو بیت بر ثانیه (H_{12}) استفاده می‌شوند. با استفاده از این نرخ‌های ارسال می‌توان برنامه های کاربردی سرعت بالا نظیر تصاویر زنده ویدیویی وکنفرانس‌های صوتی وتصویری راه دور را پیاده‌سازی نمود.

واسط های کاربران به شبکه‌های دیجیتال درحال حاضر به دو نوع واسط نرخ پایه (BRI[1]) و واسط نرخ اولیه (PRI[2]) تقسیم بندی می‌شوند. متناسب با سرعت مورد نیاز کاربران می‌توان ازهر یک از این دو نوع واسط استفاده کرد. واسط نرخ پایه از دوکانال B و یک کانال ۱۶ کیلو بیتی D تشکیل شده است. بنابراین مجموع نرخ کانال پایه ۱۴۴ کیلو بیت ثانیه می‌باشد.برای عملکرد مناسب این کانال نیاز به ۴۸ کیلوبیت بر ثانیه بالاسری اضافی می‌باشد، بنابراین نرخ کلی این کانال ۱۹۲کیلوبیت بر ثانیه است. از این نوع کانالها در کاربردهای سرعت پایین استفاده می‌شود.

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 می‌شود؛ بنابراین نرخ کلی این کانال ۱/۵۴۴ مگابیت برثانیه است. با توجه به سرعت بالای این واسط ها، از آنها درکاربردهای سرعت بالا نظیر اتصال شبکه‌های محلی به یکدیگر استفاده می‌گردد. واسط های PRI سازگار با خطوط T_1 می‌باشند. البته در اروپا واسط های فوق شامل ۳۰ کانال B و ۲ کانال D است. بنابراین نرخ

[1] Basic Rate Interface

[2] Primary Rate Interface

کلی آن ۲/۰۴۸ مگابیت بر ثانیه می‌باشد که سازگار با خطوط E_1 است.برای نیازهای تخصصی‌تر سایر ترکیب‌های مختلف نظیر $3H_0+D$ ، $4H_0+D$ و $H_{12}+D$ استفاده می‌گردد.

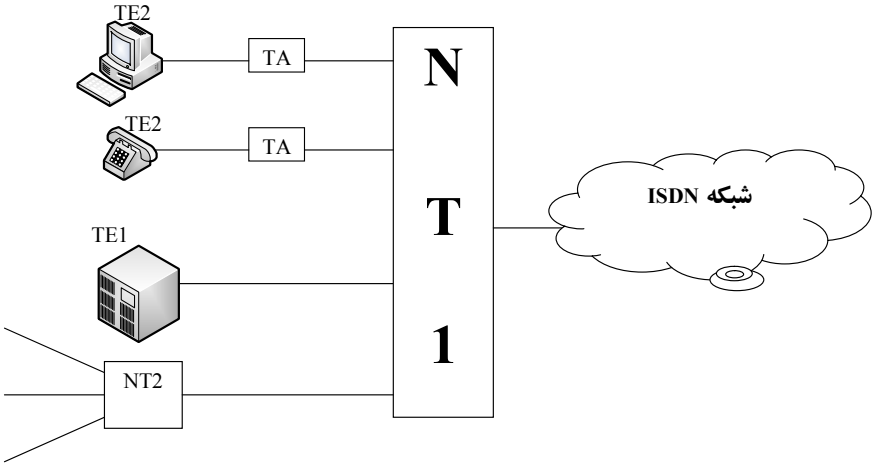
در شبکه‌های ISDN تجهیزاتی که برای اتصال کاربران به شبکه در نرخ ارسال پایه و یا نرخ ارسال اولیه استفاده می‌شوند، براساس وظایفی که برعهده آنها است به گروه های عملیاتی متفاوتی تقسیم می‌شوند. از میان این گروه ها، مشتریان تجهیزات ویژه ای را که به بهترین شکل، مناسب نیازهای آنها می‌باشد انتخاب می‌کنند.

درشبکه‌های ISDN با استفاده از وسایل وتجهیزات انتخاب شده کاربر، گروه‌های عملیاتی قابل پیاده‌سازی می‌باشند. این گروه‌های عملیاتی عبارتند از پایان دهنده‌های شبکه (نوع ۱و۲) ، تجهیزات پایانه (نوع ۱و۲) و آداپتورهای پایانه. یک پایان دهنده شبکه نوع ۱(NT1[۱]) به‌عنوان پایان‌دهنده الکتریکی و فیزیکی شبکه ISDN به تجهیزات کاربر عمل می‌کند. در NT1 رشته داده‌های ارسالی کاربران به‌صورت قاب‌های مشخصی تبدیل می‌شود و سپس برروی خطوط دیجیتال ارسال می‌گردد. عملیات NT1 مشابه عملیات لایه فیزیکی در مدل مرجع OSI می‌باشد. پایان دهنده شبکه نوع ۲ (NT2[۲]) عملیات لایه های فیزیکی، پیوند داده و شبکه را در مدل مرجع OSI انجام می‌دهد. توسط NT2 عملیات مختلفی نظیر تسهیم سازی (لایه ۱) کنترل جریان (لایه ۲) و بسته بندی (لایه ۳) انجام می‌شود. در حقیقت NT2 عملیات پردازش سیگنالها را بین تجهیزات تولید کننده داده و NT1 انجام می‌دهد.

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 می‌کند. به هر وسیله ای که استاندارد ISDN را حمایت نماید، نظیر تلفن دیجیتال، پایانه های داده، تجهیزات صوت مجتمع و فاکس دیجیتال، TE1 اطلاق می‌شود.

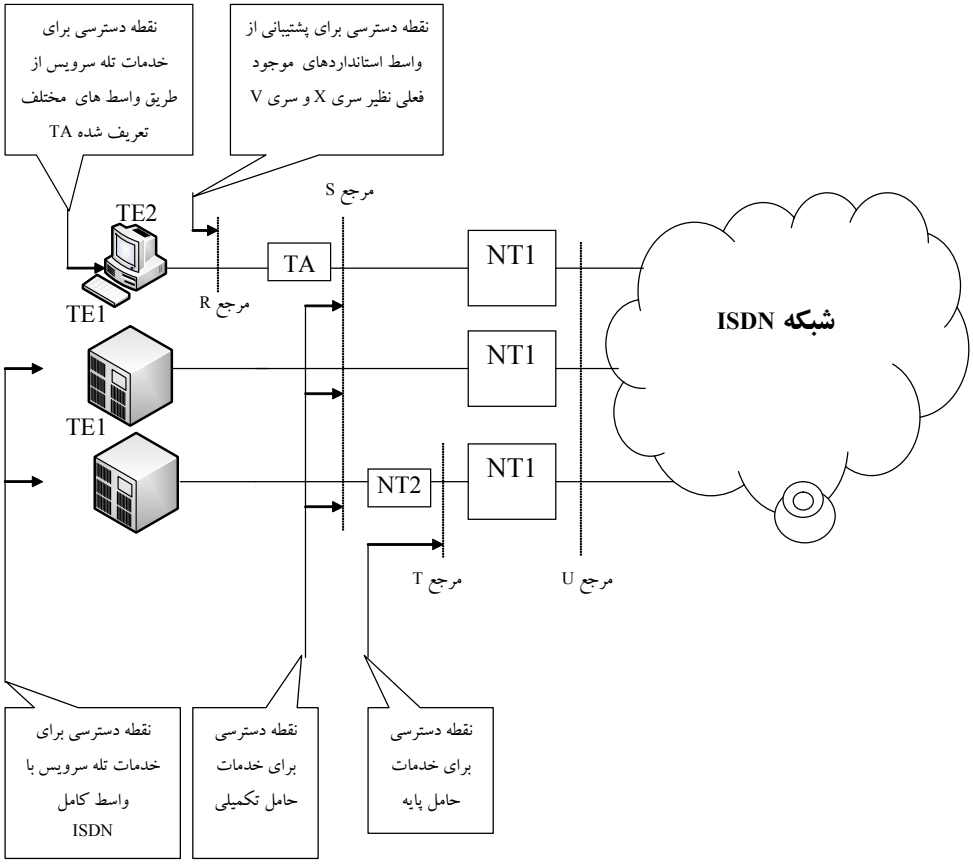
تجهیزات پایانه نوع ۲ (TE2[۴])، شامل وسایل غیر ISDN نظیر: پایانه ها، ایستگاه های کاری و کامپیوتر میزبان می‌باشد. تجهیزات TE2 مستقیماً سازگار با ISDN نیست، بلکه برای اتصال آنها به شبکه ISDN نیاز به تجهیزات خاصی به نام آداپتورهای پایانه (TA[۵]) می‌باشد. در شکل(۶-۱۵) مثالی از گروه بندی عملیاتی TE1، TE2، TA ، NT1 و NT2 آورده شده است.



[۱] Network Terminator 1
[۲] Network Terminator 2
[۳] Terminal Equipment 1
[۴] Terminal Equipment 2
[۵] Terminal Adapter

شکل (۶-۱۵): گروه های عملیاتی ISDN

در شبکه‌های ISDN واسط بین دو گروه عملیاتی ISDN که قبلاً توضیح داده شد، توسط نقاط مرجع خاصی با نام نقاط مرجعR ، S، T وU شناخته می‌شود. 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 NT2 و NT1 و نقطه مرجع U واسط بین NT1 و شبکه ISDN را مشخص می‌کند.



شکل (۶-۱۶): نقاط مرجع ISDN

۶-۶-۲- لایه های ISDN

سازمان ITU-T از مدل توسعه یافته ای به‌عنوان 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 وصفحه مدیریت تعریف شده است. صفحه کاربر عملیات کانال B و H را تعریف می‌کند (اتصال کاربر به کاربر). صفحه کنترل، عملیات کانال سیگنالینگ D و صفحه مدیریت ، عملیات مدیریت دو صفحه دیگر را انجام می‌دهد. تمام این سه صفحه به ۷ لایه مطابق با مدل مرجع OSI تقسیم می‌شوند. 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.

شکل (۶-۱۷): مدل لایه ای ISDN

مطابق با شکل (۶-۱۸) در سطح لایه فیزیکی هر دو صفحه مشابه یکدیگر هستند. دراین لایه از نرخ ارسال پایه و اولیه استفاده می‌شود. در سطح لایه پیوند داده، صفحه کاربر از پروتکلLAP-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. دراین لایه درصفحه کنترل از پروتکل کنترل مکالمه Q.931 استفاده می‌شود. از سوی ISDN برای لایه های بالاتر (لایه های ۴ الی ۷) در صفحه کاربر پروتکل خاصی تعریف نشده است، بلکه پروتکل ها براساس انتخاب کاربرتعیین می‌شود. همچنین در لایه های بالاتر در صفحه کنترل از پروتکل های سیگنالینگ انتها به انتها استفاده می‌گردد.

۶-۶-۲-۱- لایه فیزیکی

استاندارد فیزیکی ISDN توسط دو استانداردITU_T ،I.430 و I.431 تعریف شده است. در این دو استاندارد، تمام جنبه های واسط های BRI و PRI توصیف شده اند. مهمترین جنبه های توصیف شده دراین استاندارد عبارتند از: مشخصات فیزیکی و الکتریکی واسط های R,S,T و U ، روش کد گذاری، نحوه تسهیم سازی کانال و منبع تغذیه.

واسط R توسط ISDN تعریف نشده است و کاربر می‌تواند ازهمه 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 دهنده‌های۴، ۶ و یا ۸ سیمه استفاده می‌شود.سیم های موجود در واسطS مطابق با جدول (۶-۲) استفاده می‌گردند.

کانال D	کانال B
سیگنالینگ انتها به انتهای کاربر	لایه های ٦،٥،٤و٧ انتخاب کاربر
لایه شبکه کنترل مکالمه (Q.931)	لایه شبکه X.25 و...
لایه پیوند داده LAPD	لایه پیوند داده LAPB و...
لایه فیزیکی BRI و PRI	لایه فیزیکی BRI و PRI

شکل (۶-۱۸): لایه های ISDN برای کانال های B وD

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

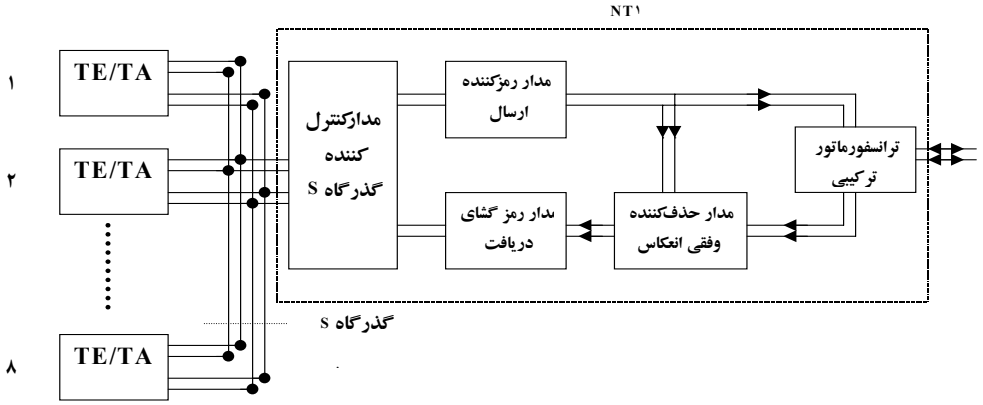
در ISDN از روش کدگذاری AMI استفاده می‌گردد. در واسط U و درهرجهت یک کابل زوج سیم به هم تابیده شده استفاده می‌شود. در این واسط مکانیسم 2B1Q که بر خلاف AMI به جای استفاده از دو سطح سیگنال، از ۴ سطح سیگنال استفاده می‌کند، تعیین شده است.

براساس فاصله بین وسیله ارسال داده تا NT1 از توپولوژی ستاره یا گذرگاه مشترک در BRI استفاده می‌شود. در اتصال‌های نقطه به نقطه تجهیزات کاربران می‌توانند تا فاصله هزار متری از NT1 قرار داشته باشند. در اتصال‌های چند نقطه حداکثر فاصله کانال می‌تواند ۲۰۰ متر باشد. چنانچه در کانال‌های چند نقطه، ایستگاه‌ها در انتهای کانال متمرکز گردند؛ در این حالت تاخیر انتشار برای همه آنها یکسان خواهد بود و می‌توان طول کانال را به ۵۰۰ متر افزایش داد. حداکثر امکان اتصال ۸ ایستگاه به NT1 وجود دارد. درهرلحظه فقط دو ایستگاه قادر به دسترسی به کانال B می‌باشند.

درشکل (۶-۱۹) ساختار واسط کاربر به شبکه درلایه فیزیکی ISDN نشان داده شده است. مطابق با این شکل بین تجهیزات کاربر و شبکه از یک زوج سیم به هم تابیده شده استفاده می‌گردد. با توجه به این‌که ارسال به‌صورت کاملاً دوطرفه

می‌باشد، بنابراین نیاز به یک ترانسفورماتور ترکیبی[1] می‌باشد. توسط ترانسفورماتورترکیبی، سیگنال دریافتی ازخط از سیگنال ارسالی جدا شده و به مدارگیرنده تحویل داده می‌شود. ازآن‌جا که عملیات جداسازی فوق به‌صورت ایده‌آل انجام نمی‌گردد، 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[2] می‌باشد. برای آن‌که مدار حذف کننده انعکاس فوق به‌صورت ایده آل عمل کند، نباید بین سیگنال ارسالی با سیگنال دریافتی هیچ‌گونه همبستگی[3] موجود باشد. برای جلوگیری ازایجاد همبستگی درسیگنال ارسالی و دریافتی، ازمدار رمز کننده[4] درسمت ارسال و رمزگشا[5] در سمت دریافت استفاده می‌شود. این مدار اقدام به درهم ریختن رشته بیت ارسالی می‌کند و بدین‌ترتیب رشته بیت ارسالی به‌صورت کاملاً تصادفی تبدیل می‌شود.

همان‌طور که درشکل (۶-۱۹) مشاهده می‌شود، تجهیزات TE و TA ازطریق دو زوج سیم (یک زوج برای ارسال و یک زوج برای دریافت) به NT1 اتصال می یابند. درISDN ، این امکان وجود داردکه حداکثر ۸تا تجهیزات TE/TA به یک NT1 اتصال یابند.



شکل (۶-۱۹): واسط کاربر به شبکه درISDN

از روش CSMA برای دسترسی به کانال D استفاده می‌شود. هنگامی که ایستگاهی به کانال D دسترسی یافت، قادر به درخواست کانال B می‌باشدو چنانچه کانال B آزاد موجود باشد اتصال برقرارخواهد شد.

در واسط های PRI از۲۳ کانال B و یک کانال D استفاده می‌شود. در این واسط ها نیز نقاط مرجع U,T,S,R تعریف می‌گردند. نقاط مرجع S,R در این حالت مشابه نقاط متناظر در واسط BRI می‌باشند. نقطه مرجع T مشابه نقطه مرجع S می‌باشد، که در آن از روش کدگذاری B8ZS استفاده می‌شود. واسط U نیز در PRI مشابه BRI می‌باشد، با این تفاوت که از نرخ ارسال ۱/۵۴۴ مگابیت بر ثانیه استفاده می‌گردد.

---

[1] Hybrid transformer
[2] Echo canceler
[3] Correlation
[4] Scrambler
[5] Descrambler

۶-۶-۲-۲- لایه پیوند داده

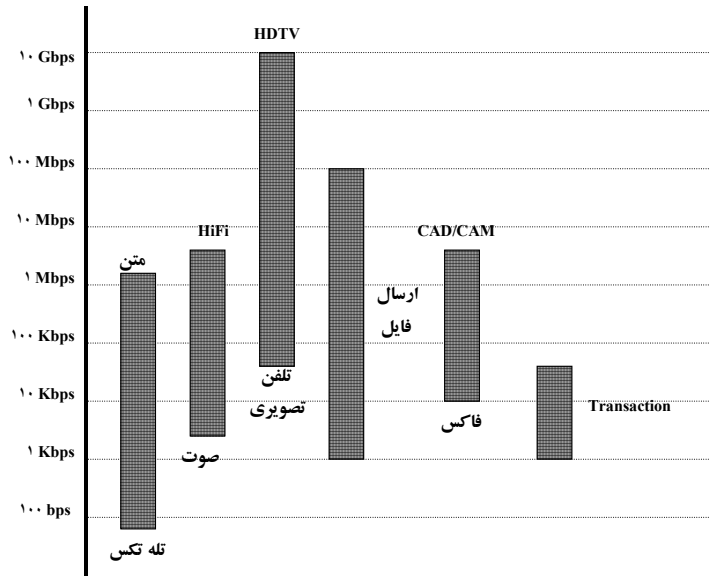
کانال‌های D,B (صفحه کاربر و صفحه کنترل) از پروتکل‌های پیوند داده متفاوتی استفاده می نمایند. همان‌طور که قبلاً گفته شد کانال B از پروتکل LAPB و کانال D از پروتکل LAPD استفاده می‌کند. LAPD مشابه پروتکل HDLC می‌باشد با این تفاوت که در آن تغییرات خاصی انجام گرفته است.

۶-۶-۲-۳- لایه شبکه

هنگامی که با استفاده از کانال D اتصال اولیه به‌وجود آمد، صفحه کاربر با استفاده از پروتکل هایی مانند سوئیچینگ مداری،X.25 و یا سایر پروتکل‌ها اقدام به ارسال اطلاعات بین کاربران می‌کند.

۶-۶-۳- ISDN باند پهن(BISDN[1])

هنگامی که برای اولین بار ISDN مطرح شد، سرعتهای ۶۴ کیلو بیت بر ثانیه تا ۱/۵۴۴ مگابیت بر ثانیه برای برآوردکردن نیازهای ارسال آن زمان کافی بود. با توسعه شبکه‌های کامپیوتری و ارائه سرویس جدیدتر، سرعت‌های فوق کافی نمی‌باشد. ازاین رو استاندارد ISDN باند پهن ارائه گردید. در این استاندارد، اتصال بین کاربر و شبکه تا سرعت۶۰۰ مگا بیت بر ثانیه می‌تواند افزایش یابد. درشکل(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 سیستم های آنالوگ تلفن ایجاد نمود. پیدایش BISDN درحقیقت انقلاب بزرگی در فن‌آوری مخابرات به حساب می‌آید. در BISDN به جای استفاده از کابل‌های فلزی، از محیط‌های ارسال جدیدی نظیر فیبر نوری استفاده می‌شود.

[1] Broadband ISDN

BISDN قادربه ارائه دونوع سرویس به کاربران خود می‌باشد که عبارتند از: سرویس تاثیر متقابل[1] و سرویس توزیعی[2].

در سرویس تاثیر متقابل یک یا دو مشتری با یک سرویس دهنده در ارتباط متقابل می‌باشند. این نوع سرویس خود به سه دسته زیر تقسیم می‌شوند:

- ***سرویس محاوره ای[3]:*** این نوع سرویس ، مبادله دوطرفه به‌صورت زمان حقیقی را پشتیبانی می‌کند. از این سرویس زمان حقیقی در تلفن، تلفن های تصویری، کنفرانس های ویدئویی، ارسال داده و نظیر اینها استفاده می‌شود.
- ***سرویس پیامی[4]:*** دراین نوع سرویس اطلاعات به‌صورت ذخیره و هدایت به جلو مبادله می‌شوند. این نوع سرویس به‌صورت دوطرفه هستند، که درآن یک مشتری از مشتری مقابل درخواست اطلاعات می‌کند. ممکن است اطلاعات درخواستی در همان لحظه حاضر نباشد و درخواست‌کننده مدتی منتظر پاسخ بماند. پست صوتی[5]، پست داده[6] وپست ویدئویی [7] نمونه ای از این نوع سرویس می‌باشد.
- ***سرویس بازیافتی[8]:*** از این نوع سرویس برای بازیافت اطلاعات از یک منبع مرکزی به نام مرکز اطلاعات استفاده می‌شود. این سرویس مشابه کتابخانه ها باید اجازه دسترسی عمومی به کاربران را فراهم آورند. در این سرویس، اطلاعات توزیع نمی‌شوند مگر آن‌که درخواستی برای آن از جانب مشتریان دریافت شود.

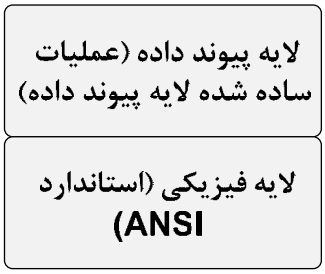
سرویس توزیعی به‌صورت یک طرفه از طرف سرویس دهنده به سمت مشتریان می‌باشند و برخلاف سرویس تاثیر متقابل، مشتریان قادر به ارسال درخواست برای دستیابی به سرویس مورد نظر خود نمی‌باشند. این نوع سرویس به دو صورت : تحت کنترل کاربر، و بدون کنترل کاربر قابل پیاده سازی می‌باشند. درسرویس توزیعی بدون کنترل کاربر، بدون آن‌که کاربر درخواستی برای سرویس و زمان پخش آنها داشته باشد، سرویس از سوی سرویس دهنده بین کاربران توزیع می‌شود. برنامه های تلوزیونی، نمونه ای از این سرویس می‌باشند. سرویس توزیع تحت کنترل کاربر، به‌صورت چرخشی به کاربر ارسال می‌شود.این نوع سرویس به‌صورت متناوب تکرار می‌شوند تا این‌که کاربر قادر به دریافت آنها در زمانهای دلخواه خود باشد. پخش برنامه های آموزشی[9] و تلوزیون پولی، نمونه ای از این نوع سرویس می‌باشد. به‌عنوان مثال در تلوزیون پولی، یک برنامه خاص در زمان های معینی پخش می‌شود، کاربر برای مشاهده این برنامه باید تلوزیون خود را در زمان های خاصی که این برنامه پخش می‌شود، روشن کند.برای پیاده سازی سرویس BISDN از فن‌آوری ATM که در بخش‌های بعدی توضیح داده می‌شوداستفاده می‌گردد.

---

[1] Interactive services
[2] Distributive services
[3] Conversational services
[4] Messaging services
[5] Voice mail
[6] Data mail
[7] Video mail
[8] Retrieval services
[9] Educational broadcasting

۶-۷- شبکه Frame Relay

در شبکه‌های frame relay ، جهت افزایش سرعت عملیات پردازش و هدایت قاب‌های لایه دوم، کلیه عملیات لایه شبکه و بخشی از عملیات لایه پیوند داده حذف شده است. بنابراین در مقایسه با شبکه‌های X.25 که دارای ۳ لایه می‌باشند، شبکه‌های 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 شبکه‌های frame relay ، درسطح لایه پیوند داده از نسخه ساده شده پروتکل HDLC استفاده می‌شود. جهت سادگی و افزایش سرعت، عملیات کنترل جریان و کنترل خطای پیشرفته که در HDLC استاندارد وجود دارد، در شبکه‌های frame relay استفاده نمی‌شود.

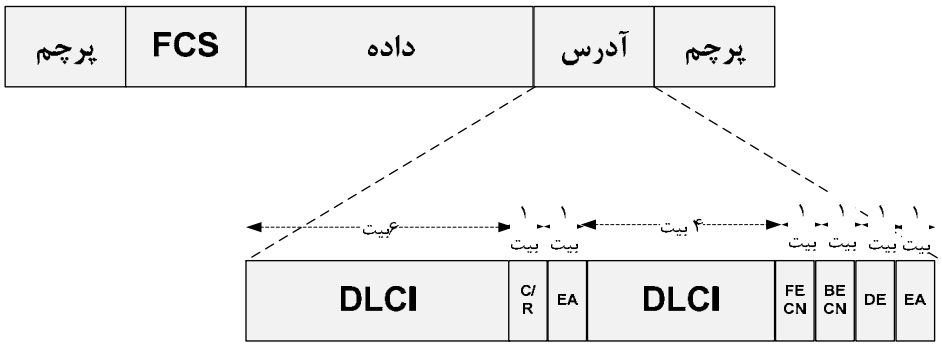
در شکل (۶-۲۲) ساختار قاب‌های لایه دوم در frame relay نشان داده شده است. همان‌طور که دراین شکل نیز دیده می‌شود، ساختار این قاب ها مشابه ساختار قاب‌های HDLC می‌باشد. فیلدهای پرچم، FCS و اطلاعات در قاب‌های frame relay مشابه فیلدهای فوق در HDLC می‌باشند، اما فیلد های آدرس و کنترل در قاب‌های frame relay با یکدیگر ترکیب شده و فیلد آدرس را تشکیل می‌دهند. در فیلد آدرس زیر فیلدی به نام "مشخص کننده اتصال لایه پیوند داده" (DLCI[1]) وجود دارد، که از آن برای هدایت قاب‌های frame relay استفاده می‌شود. با توجه به ساختار قاب‌های frame relay، در فیلد آدرس، زیر فیلدهای زیر موجود می‌باشد:

- ***فیلد DLCI***: این فیلد که به دو تکه۶ و۴ بیتی تقسیم شده است(مجموعاً ۱۰ بیت)، برای مشخص کردن اتصال لایه پیوند استفاده می‌شود.
- ***فیلد دستور/پاسخ (C/R[2])*** : ازاین فیلد برای تعیین این‌که قاب ارسالی از نوع دستور یا پاسخ است استفاده می‌شود.
- ***فیلد آدرس توسعه یافته (EA[3])*** : این بیت مشخص می‌کند 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 وچنانچه 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 وفیلد دوم برابر با ۱ می‌باشد. چنانچه برنامه کاربردی به آدرس بیشتر از دو بایت نیاز داشته باشد، در این صورت هر دو فیلد EA برابرصفر می‌باشند و یک بایت سوم آدرس اضافه می‌شود که در آن ۷ بیت نشان دهنده آدرس و بیت هشتم که همان فیلد EA است، برابر با ۱ می‌باشد.

---

[1] Data Link Connection Identifier
[2] Command/Response
[3] Extended Address

- ***فیلد اعلام صریح ازدحام در مسیر پیشرو(FECN[1]):*** چنانچه در نودهای میانی شبکه ازدحام رخ دهد، در این صورت این فیلد ۱ می‌شود، که نشان دهنده این است که در مسیر عبور قاب‌ها از مبدأ به مقصد ازدحام رخ داده است. گیرنده با مشاهده فعال بودن این بیت متوجه می‌شود که در داخل شبکه، ازدحام رخ داده است و متوجه می‌شودکه این احتمال وجود دارد که به خاطر ازدحام قاب‌های بعدی با تأخیردریافت شوند.
- ***فیلد اعلام صریح ازدحام در مسیر پسرو(BECN[2]):*** برای اعلام وقوع ازدحام در مسیرمخالف مسیری که قاب ها از آن عبور می کنند، این بیت فعال می‌شود. گیرنده بافعال کردن این فیلد به فرستنده در خصوص وقوع ازدحام هشدار می‌دهد.
- ***فیلد شایستگی حذف*** (**DE[3]**) : از این بیت برای تعیین اولویت قاب استفاده می‌شود. در شرایط بحرانی که ازدحام در شبکه رخ داده است، با استفاده از این فیلد قاب‌های ارسالی اولویت بندی شده و آنهائی‌که اولویت کمتری دارند درمعرض حذف قرار می گیرند. قاب‌هایی که فیلد DE آنها ۱ است اولویت بیشتری نسبت به قاب‌های با فیلد DE برابر با صفر دارند.



شکل (۶-۲۲): ساختار قاب‌های frame relay

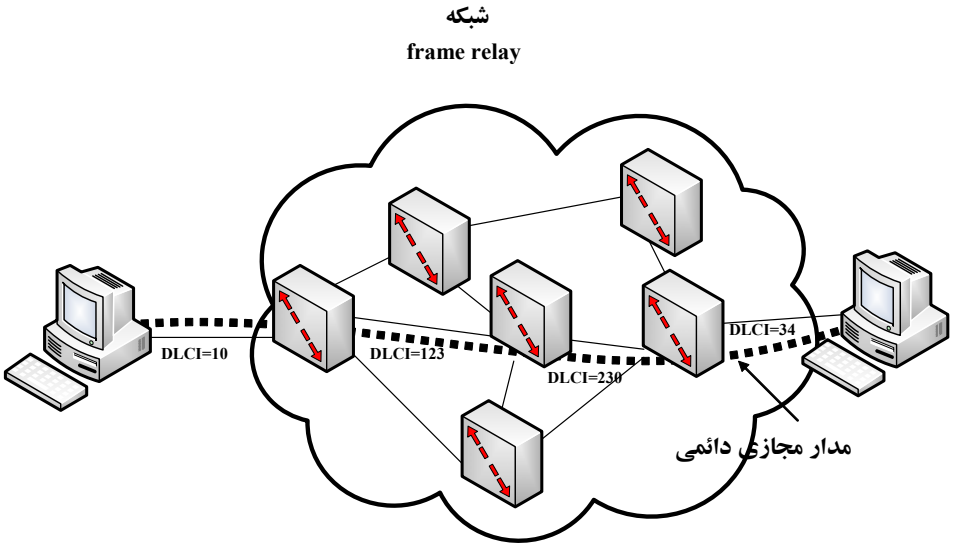
۶-۸-۲- عملکرد frame relay

شبکه‌های Frame relay از اتصال‌های مدارمجازی دایمی (PVC[4]) استفاده می کنند. برای مشخص کردن مدارمجازی دایمی از فیلد DLCI استفاده می‌شود. با توجه به این‌که طول ناحیه DLCI برابر با ۱۰ بیت می‌باشد، حداکثر می‌توان ۱۰۲۴ مدارمجازی دایمی مختلف ایجاد نمود. چنانچه بایت سوم آدرس نیز در سرآیند قاب‌های frame relay قرارگیرد، در این‌صورت می‌توان حداکثر تعداد مدارهای مجازی دایمی شبکه را افزایش داد. در شکل (۶-۲۳) مثالی از کاربرد فیلد DLCI نشان داده شده است.

هریک از سوئیچ‌های شبکه‌های frame relay دو وظیفه عمده به عهده دارند که عبارتند از: کنترل خطا (با استفاده از فیلدFCS موجود در هرقاب) وسوئیچینگ و هدایت قاب‌ها با استفاده از فیلد DLCI موجود در سرآیند قاب‌ها. هریک از سوئیچ‌های میانی شبکه، برای هدایت قاب‌ها از مبدأ به مقصد، دارای یک جدولDLCI می‌باشند. 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 می‌گردد.

---

[1] Forward Explicit Congestion Notification
[2] Backward Explicit Congestion Notification
[3] Discard Eligibility
[4] Permanent Virtual Circuit



شکل (۶-۲۳): مثالی از ایجاد مدارهای مجازی دایمی با استفاده از فیلد DLCI

یکی دیگر ازعملیات هرسوئیچ در شبکه‌های frame relay، کنترل ازدحام می‌باشد. همان‌طورکه قبلاً اشاره گردید، در سرآیند قاب‌های frame relay، دو بیت به نام‌های بیت FECN و بیت BECN وجود دارند، که از آنها برای کنترل ازدحام در شبکه استفاده می‌شود. 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 می‌دهد. گیرنده نیز با دریافت قاب‌هایی که بیت FECN آنها ۱ است، قاب‌هایی با بیت BECN برابر با ۱ به فرستنده اولیه ارسال می دارد و به آن درمورد وقوع ازدحام درشبکه خبر می‌دهد.

۶-۸- شبکه ATM

فن‌آوری ATM، از سوی انجمن ATM به‌عنوان یک فن‌آوری جدید برای پیاده‌سازی سرویس BISDN ارائه گردید و توسط سازمان ITU_T مورد تصویب قرار گرفت. درفن‌آوری ATM اهداف زیر مورد توجه می‌باشد:

- استفاده از محیط‌های ارسال بسیار سریع به ویژه فیبر نوری
- ایجاد یک شبکه انعطاف‌پذیر که قادر به اتصال به سایر شبکه‌ها باشد
- استفاده از ATM به‌عنوان یک شبکه شالوده با قیمت ارزان برای اتصال شبکه‌های مختلف به یکدیگر
- توانایی برقراری ارتباط با سایر شبکه‌های موجود در دنیا
- پیاده‌سازی ATM به‌صورت اتصال‌گرا برای دستیابی به مزایای شبکه‌های اتصال‌گرا
- پیاده‌سازی قسمت‌های مختلف آن به‌صورت سخت‌افزاری و نرم‌افزاری برای افزایش سرعت

هرچند بسیاری از اهداف فوق هنوز به‌طور کامل به تحقق نرسیده است، ولی تلاش‌های زیادی در راستای رسیدن به اهداف فوق در دست انجام است. در شبکه‌های سوئیچینگ بسته‌ای ، اطلاعات کاربران در قالب بسته‌هایی به طول متغیر

ارسال می‌شود، درحالی‌که درشبکه‌های ATM، اطلاعات ارسالی کاربران در قالب بسته‌هایی به طول ثابت ۵۳ بایت ارسال می‌گردد. به علت کوچک بودن بسته‌های ارسال در ATM، به آنها سلول[1] گفته می‌شود.

در ATM با توجه به طول کم هر سلول، پردازش هر سلول در نودهای میانی در زمان بسیار کمی‌صورت می‌گیرد و همچنین تأخیر ارسال در شبکه‌های ATM، بسیار ناچیز است.

ATM یک نوع شبکه اتصال‌گرا است که در آن قبل از ارسال داده‌ها، یک مدار مجازی بین مبدأ و مقصد به‌وجود می‌آید و سپس سلول‌های متعلق به هر پیام، به‌طور کامل از طریق یک مدار مجازی به مقصد ارسال می‌شود و در گیرنده نیز به ترتیب دریافت می‌شود. در شبکه‌های ATM، از سوئیچینگ لایه دوم برای هدایت و مسیریابی سلول‌ها استفاده می‌شود. در ATM ارسال اطلاعات کاربران به‌صورت غیرهمزمان انجام می‌شود. مفهوم غیرهمزمان بودن ATM آن است که داده‌های تولیدی کاربران به‌طور مستقل تولید می‌شوند و لزومی‌در رعایت یک زمان بندی خاص‌نمی‌باشد. با توجه به این‌که در ATM از کانال‌های سریع و مطمئن استفاده می‌شود، احتمال خرابی سلول‌ها بسیار کم می‌باشد. در ATM، توانایی تصحیح یک بیت خطا در سلول‌های ارسالی وجود دارد و نیازی به ارسال دوباره سلول نمی‌باشد. همچنین از روال‌های پیچیده کنترل ازدحام و کنترل جریان استفاده نمی‌شود. شکل (۶-۲۴) نشان‌دهنده مدل لایه‌ای ATM است.

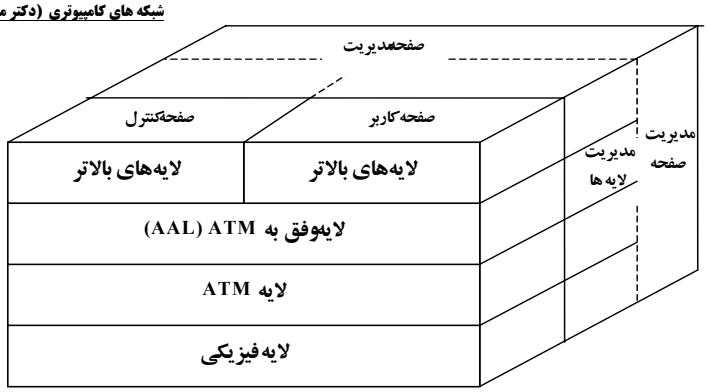
فن‌آوری ATM دارای ویژگیهای زیر می‌باشد:

- ***عدم نیاز به کنترل خطا و کنترل جریان به‌صورت لینک به لینک:*** در شبکه ATM چنانچه در کانال ارتباطی خطایی به‌وجود آید، عملیات کنترل خطا به‌صورت لینک به لینک انجام نمی‌شود. با توجه به این‌که معمولاً از کانال‌های فیبر نوری که از کیفیت بالایی برخوردار هستند در شبکه ATM استفاده می‌شود، احتمال خرابی کانال در ATM بسیار کم است. بنابراین کنترل خطا در ATM بصورت انتها به انتها انجام می‌گردد.
- ***فن‌آوری ATM اتصال گرا است:*** در این شبکه ابتدا بین فرستنده و گیرنده یک مدار مجازی به‌وجود می‌آید، سپس داده‌های ارسالی به‌طور کامل از این مدار عبور می‌کند و بعد از اتمام داده‌ها مدار مجازی از بین می‌رود.
- ***کاهش سرآیند :*** در ATM عملیات پردازش بر روی سرآیند کاهش یافته است، بنابراین سرعت پردازش سرآیندهای ATM بسیار زیاد است.
- ***طول کم :***طول بسته‌های ATM بسیار کوچک است (۵۳ بایت) بنابراین بافرهای میانی شبکه ATM کاهش می‌یابد و تأخیر صف در شبکه کم می‌گردد.
- ***حمایت از انواع ترافیک ها:*** شبکه ATM قادر به ارائه انواع سرویس صوت، ویدئو و داده می‌باشد.

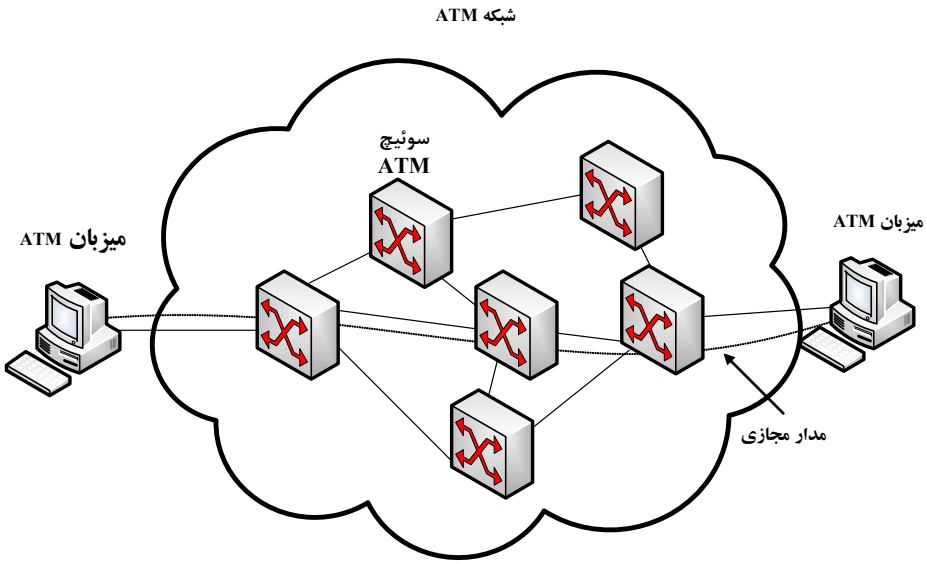
همان‌طور که در شکل (۶-۲۵) دیده می‌شود، در شبکه‌های ATM برای هر کاربر انتها به انتها یک مسیر مجازی به‌وجود می آید و با کمک تسهیم‌سازهای ATM ترافیک ارسالی کاربران با یکدیگر ترکیب می‌شوند و وارد شبکه ATM می‌شوند. هر شبکه ATM از دو جزء اصلی تشکیل شده است که عبارتند از: کامپیوترهای میزبان و سوئیچ‌های شبکه. کامپیوترهای میزبان به‌وسیله آداپتورهای ATM و با کمک کانال فیزیکی که ارتباط آن‌را به سوئیچ‌های شبکه برقرار می سازد، به شبکه ATM متصل می‌باشند. در شبکه‌های ATM برای برقراری ارتباط بین دو کامپیوتر میزبان از اتصال‌های مجازی استفاده می‌شود. نقطه انتهایی اتصال‌های مجازی فوق کامپیوترهای میزبان ATM می‌باشند.

---

[1] Cell



شکل (۶-۲۴) : مدل لایه‌ای ATM



شکل(۶-۲۵): یک اتصال انتها به انتها در ATM

سوئیچ ATM که در داخل شبکه نصب می‌شود، دارای چندین درگاه ورودی و خروجی می‌باشد، که ارتباط آن را به کامپیوترهای میزبان ATM و سایر سوئیچ‌های ATM برقرار می‌سازد. سلول‌های ورودی به سوئیچ‌های ATM بر اساس فیلد مشخص کننده اتصال، که درسرآیندهای سلول‌های ATM قرار دارند به درگاه خروجی مناسب ارسال می‌شوند.

در ATM دونوع اتصال وجود دارد که عبارتند از: اتصال‌های دایمی (PVC) و اتصال‌های سوئیچینگ (SVC). در اتصال‌های PVC یک مدار مجازی دایمی بین فرستنده و گیرنده موجوداست. برای برقراری این نوع اتصال‌ها نیازی به روال‌های سیگنالینگ نمی‌باشد. این نوع اتصال‌ها مشابه خطوط استیجاری در شبکه تلفن هستند. در اتصال‌های SVC برای ایجاد مدارمجازی بین مبدأ و مقصد از روال‌های سیگنالینگ استفاده می‌شود. در ATM چهار نوع پیام سیگنالینگ وجود دارد که عبارتند از:

برقراری ارتباط: *از این پیام‌ها برای پایه گذاری و برقراری ارتباط مدارهای مجازی SVC بین فرستنده و گیرنده استفاده می‌شود. در ATM پنج پیام اصلی برای برقراری ارتباط وجود دارد که عبارتند از: برقراری ارتباط، پیشرفت ارتباط [1] ، اتصال ، گوش به زنگ [2] و گواهی اتصال [3].در شکل (۶-۲۶) مثالی از مراحل برقراری ارتباط در ATM با استفاده از پیام‌های فوق آورده شده است.*

بررسی وضعیت ارتباط: *در شبکه‌های ATM برای بررسی وضعیت ارتباط‌های موجود از پیام‌های: اعلام وضعیت [4] ، بررسی وضعیت [5] و آگاهی دادن [6] استفاده می‌شود. توسط کاربر یا شبکه برای دریافت وضعیت ارتباط‌های موجود از پیام بررسی وضعیت استفاده می‌گردد. در پاسخ به پیام فوق، پیام اعلام وضعیت ارسال می‌شود. برای نمایش اطلاعات وضعیت ارتباط از پیام آگاهی دادن استفاده می‌گردد.*

قطع ارتباط: *در شبکه‌های ATM بعد از برقراری ارتباط و ارسال اطلاعات، مدار مجازی به‌وجود آمده باید قطع گردد. بدین‌منظور از پیام‌های زیر استفاده می‌شود:*

پیام رها سازی: این پیام توسط کاربر برای درخواست قطع ارتباط و یا توسط شبکه برای اعلام قطع مدار مجازی ارسال می‌گردد.

پیام تکمیل رهاسازی: در پاسخ به درخواست قطع ارتباط، کاربر یا شبکه پیام فوق را ارسال می‌کند و به‌دنبال آن مدار مجازی قطع می‌شود و مرجع ارتباط آزاد می‌شود.

پیام آغاز دوباره: این پیام توسط کاربر یا شبکه ارسال می‌شود و نشان دهنده درخواست آغاز دوباره یک VCC مشخص و یا تمامی VCC های موجود می‌باشد.

پیام‌های مربوط به ارتباط‌های نقطه به چند نقطه [7]: به‌طور کلی در شبکه‌های ATM دو نوع اتصال وجود دارد که عبارتند از: اتصال‌های نقطه به نقطه و اتصال‌های نقطه به چند نقطه. در اتصال‌های 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 می‌باشد. کاربر ریشه با کمک روال‌های استاندارد سیگنالینگ با اولین کاربر برگ ارتباط برقرار می‌سازد. بعد از برقراری ارتباط کاربر ریشه با اولین کاربر برگ، از پیام‌های زیر برای برقراری ارتباط با سایر کاربران برگ استفاده می‌شود:

پیام افزودن کاربرجدید [8]: از این پیام برای اضافه کردن یک کاربر جدید به اتصال موجود استفاده می‌شود.

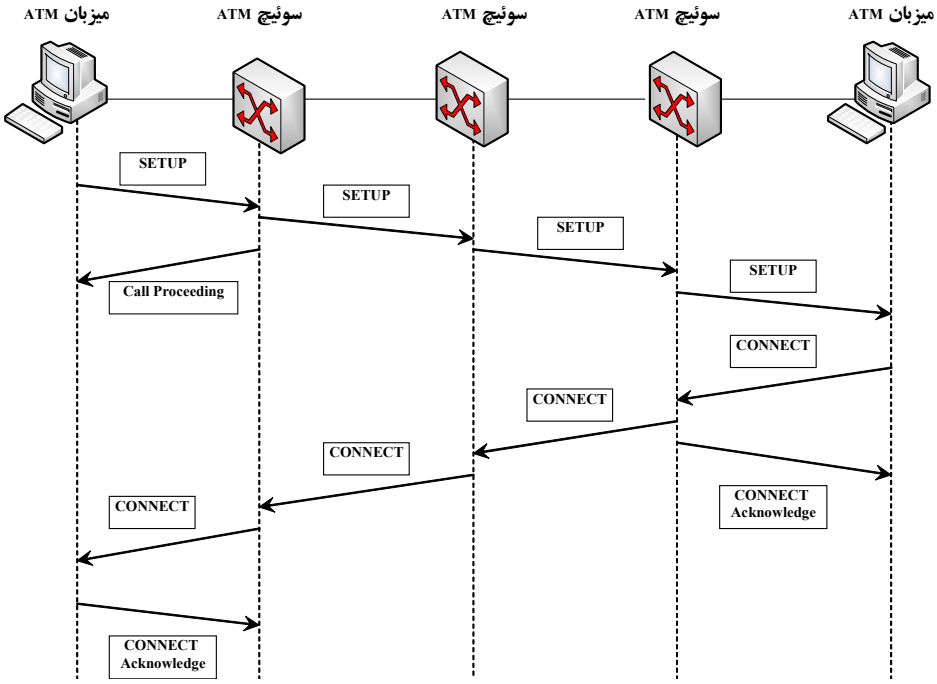
پیام گواهی افزودن کاربر جدید [9]: در پاسخ به پیام افزودن کاربر جدید، این پیام که نشان دهنده پاسخ مثبت به عملیات افزودن کاربر جدید به اتصال موجوداست، ارسال می‌گردد.

پیام رد افزودن کاربر جدید [10]: در پاسخ به پیام افزودن کاربرجدید، این پیام که نشاندهنده پاسخ منفی به عملیات افزودن کاربر جدید به اتصال موجوداست، ارسال می‌گردد.

---

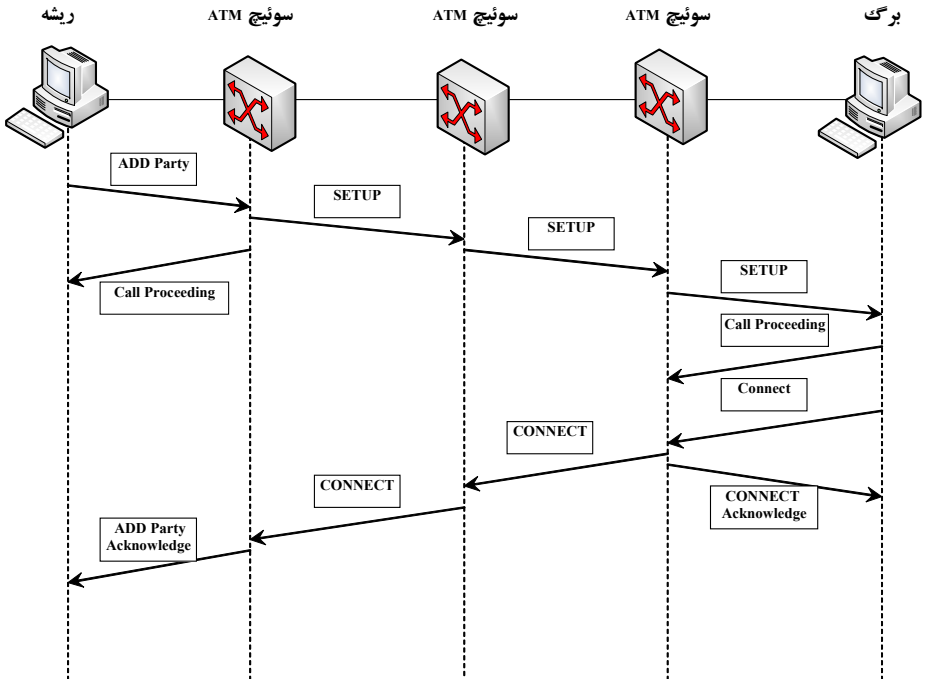
[1] Call proceeding
[2] Alerting
[3] Connect acknowlege
[4] Status
[5] Status enquiry
[6] Notify
[7] Point to multi-point
[8] Add party
[9] Add party acknowledge
[10] Add party reject

- ***پیام حذف کاربر***[1]: جهت حذف یک کاربر در اتصال موجود از این پیام استفاده می‌شود.
- ***پیام گواهی حذف کاربر***[2]: در پاسخ به پیام حذف کاربر، این پیام ارسال می‌گردد که نشان دهنده عملیات موفق حذف یک کاربر از اتصال موجود است.



شکل (۶-۲۶): مثالی از برقراری ارتباط در ATM

[1] Drop party
[2] Drop party acknowledge



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 می‌باشد که عبارتند از: زیرلایه همگرایی ارسال (TC[1]) و زیرلایه وابسته به محیط فیزیکی. در توصیه نامه‌های G.703 وG.957 سازمان ITU-T این زیرلایه 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 سلول‌های ATM می‌باشد. علاوه بر عملیات فوق این زیرلایه وظیفه تبادل سلول‌های مدیریتی (OAM[2]) با لایه مدیریت را بر عهده دارد.

در لایه فیزیکی ATM، محیط ارسال و نحوه کدگذاری بیت‌های ارسالی مشخص می‌شود. استانداردهای SONET وSDH از مهمترین استانداردهای لایه فیزیکی در ATM می‌باشند. در ATM از کانال‌های فیزیکی مطمئن و سریع استفاده می‌شود که برخی از مهمترین این کانال‌هاعبارتند 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)

---

[1] Transmission Convergence
[2] Operation And Maintenance

- کانال SONET OC-3 (باسرعت 155.52Mb/s)
- کانال STS-3c/STM-1 (با سرعت 622.08 Mb/s)
- کانال SONET OC-12 (با سرعت 2488.32 Mb/s)

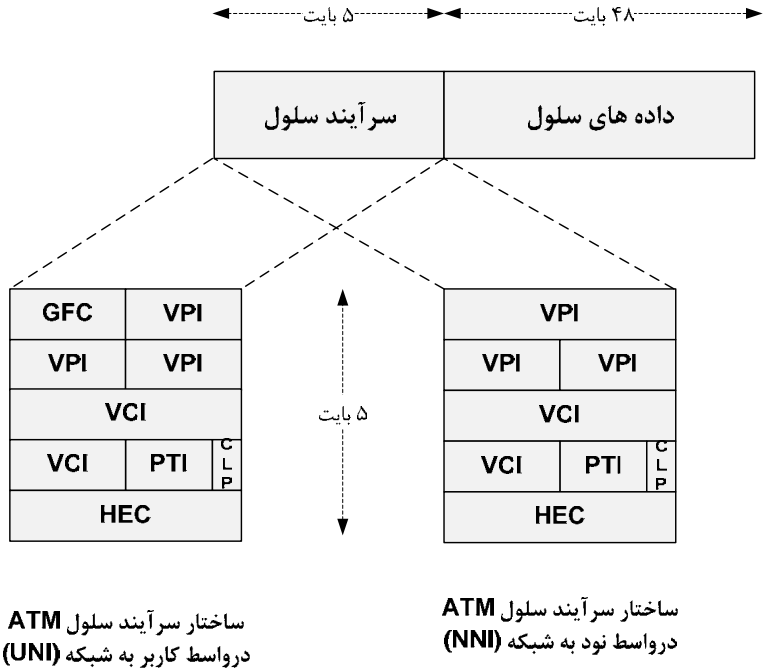
درجدول (۶-۳) برخی از استانداردهای واسط های الکتریکی و نوری مورد استفاده درشبکه های ATM آورده شده است.

جدول (۶-۳): استانداردهای واسط های الکتریکی و نوری مورد استفاده درATM

واسط های الکتریکی	واسط نوری	سرعت ارسال (برحسب مگابیت برثانیه)
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-*n*	**OC-*n***	***n**51.840**
…	**…**	**…**
STS-256	**OC-256**	**13271.040**

۶-۹-۲- لایه ATM

در شبکه‌های ATM، لایه ATM که دومین لایه می‌باشد، عهده‌دار وظایفی نظیر مسیریابی و سوئیچینگ ، مدیریت ترافیک و تسهیم سازی کانال می‌باشد. لایه ATM، بسته‌های به طول ۴۸ بایت را از لایه بالاتر خود دریافت می‌کند و با اضافه کردن ۵ بایت سرآیند، سلول‌هایی به طول ۵۳ بایت تولید می‌کند و آنها را ارسال می‌کند. در شکل(۶-۲۸) ساختار سلول‌های ATM و فیلدهای موجود درآن نشان داده شده است.

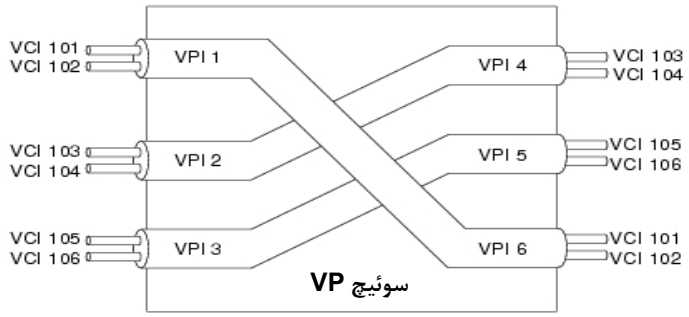


شکل(۶-۲۸) : ساختار سلول‌های ATM

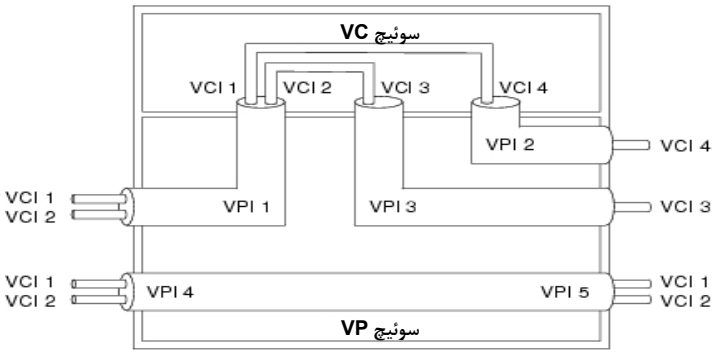
در سرآیند سلول‌های ATM فیلدهای زیر موجود است:

- ***فیلد GFC***[1] : از این فیلد برای کنترل جریان در واسط کاربر به شبکه (UNI[2]) استفاده می‌شود.
- ***فیلد* VPI *و* VCI**: از این فیلدها برای مشخص‌نمودن مدار مجازی استفاده می‌شود. درشکل (۶-۲۹) نمونه ای از کاربرد فیلدهای فوق نشان داده شده است. ارزش مقادیر موجود دراین فیلدها محلی بوده و از هرسوئیچ به سوئیچ دیگر تغییر می کند. سوئیچ های ATM براساس نوع برخورد آنها با فیلد VPI/VCI به دودسته سوئیچ های VP وسوئیچ های VP/VC تقسیم بندی می شوند. سوئیچ های VP فقط مقدار فیلد VPI سلول های ATM راتغییر داده و مقدار VCI آنها را تغییر نمی دهنددرحالیکه سوئیچ های VP/VC هردو فیلد VPI/VCI را تغییر می دهند. درشکل (۶-۲۹) نمونه ای از این دونوع سوئیچ نشان داده شده است.

[1] Generic Flow Control
[2] User Network Interface



(الف)



(ب)

شکل (۶-۲۹): نمونه ای از سوئیچ های ATM (الف) سوئیچ VP (ب) سوئیچ V/VC

- ***فیلد* PT** : توسط این فیلد سه بیتی نوع داده‌های موجود در سلول‌های ATM مشخص می‌شود. سلول‌های ATM، می‌توانند از نوع داده‌های کاربر، مدیریتی و یا کنترل شبکه باشند.
- ***فیلد* CLP[1]** : از این بیت برای کنترل ازدحام در ATM و تعیین نوع اولویت بسته‌ها استفاده می‌شود. بسته‌های با اولویت بالا دارای CLP=0 و بسته‌های کم اهمیت دارای CLP=1 می‌باشند. هنگامی‌که در سوئیچ‌های میانی شبکه، ازدحامی رخ دهد و بافرهای سوئیچ‌ها در آستانه پرشدن قرار گیرند، بسته‌های کم اولویت (CLP=1) از بین می‌روند و بسته‌های مهم (CLP=0) قبول می‌شوند.
- ***فیلد* HEC[2]**: از این فیلد برای تشخیص و تصحیح تک بیت خطا که ممکن است در سرآیند سلول‌های ATM رخ دهد استفاده می‌شود.

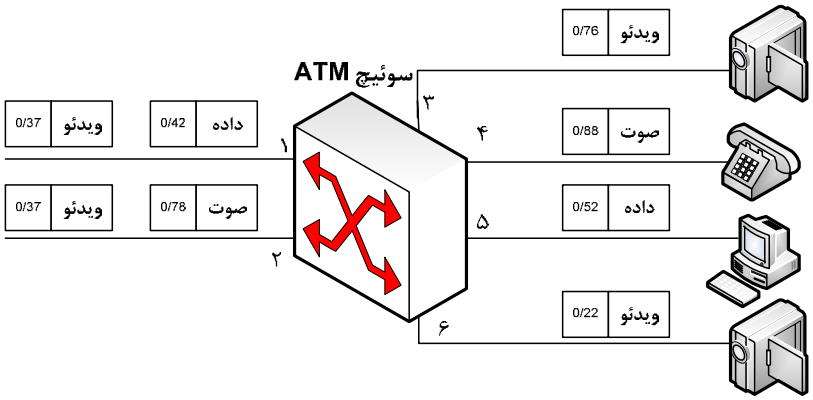
پس از برقراری اتصال وایجاد مدارمجازی، انتقال اطلاعات صورت می گیرد. فرستنده مقدار VPI/VCI تخصیص یافته خود را درداخل فیلد مربوطه موجود درسرآیند سلول های ATM قرار داده و به سمت سوئیچ شبکه ارسال می دارد. سوئیچ شبکه با استفاده از جدول اتصال که درفاز برقراری اتصال ایجاد شده است، اقدام به مسیریابی سلول ها و 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 درمسیریابی سلول ها جلوگیری می شود. به عنوان مثال عملکرد سوئیچ ATM نشان داده شده درشکل (۶-۳۰) را درنظر بگیرید. دراین شکل ترافیک های ویدئو دردرگاه شماره ۱ دارای مقدار VPI/VCI برابر با 0/37 می باشند و طبق جدول

[1] Cell Loss Priority
[2] Header Error Correction

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 درجدول (۶-۴) می باشد.

جدول (۶-۴): جدول اتصال سوئیچ ATM نشان داده شده درشکل(۶-۳۰)

شماره درگاه ورودی	مقدار VPI/VCI ورودی	شماره درگاه خروجی	مقدار VPI/VCI 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 (۶-۳۰) : مثالی از عملکرد یک سوئیچ ATM

۶-۹-۳- لایه AAL[1]

لایه AAL در ATM به دو زیر لایه SAR[2] و CPCS[3] تجزیه می‌شود. در زیرلایه SAR بسته‌های دریافتی از لایه بالاتر به پیام‌های ۴۸ بایتی تجزیه می‌گردند. زیرلایه CPCS که به لایه بالاتر از AAL بستگی دارد، عملیات اضافه نمودن سرآیند را انجام می‌دهد. لایه AAL فقط در سمت کاربر انتهایی قرار دارد و سوئیچ‌های شبکه فاقد لایه فوق می‌باشند.

شبکه ATM، ۴کلاس مختلف سرویس را پشتیبانی می‌کند که این سرویس توسط مشخصه‌های اصلی زیر مشخص می‌گردند:

۱) ***ارتباط زمانی:*** برخی از سرویس شبکه ATM از نوع زمان حقیقی می‌باشند و نیاز به حفظ ارتباط زمانی بین مبدأ و مقصد دارند. به‌عنوان مثال سرویس صوت ۶۴ کیلوبیت بر ثانیه PCM از این نوع می‌باشند. در مقابل برخی از سرویس شبکه نظیر انتقال فایل بین کامپیوترها نیازی به حفظ ارتباط زمانی ندارند.

---

[1] ATM Adaptation Layer
[2] Segmentation AND Reassembly
[3] Common Part Convergence Sublayer

۲) ***نرخ ارسال:*** برخی از سرویس شبکه دارای نرخ ارسال ثابت می‌باشند و برخی از سرویس دیگر دارای نرخ ارسال متغیر هستند.

۳) ***نحوه اتصال:*** سرویس شبکه‌های ATM به دو دسته اتصال گرا و بدون اتصال تقسیم بندی می‌شوند.

در جدول(۶-۴) انواع کلاس‌های AAL و وابستگی آنها به مشخصه‌های فوق نشان داده شده است.

جدول(۶-۴) : انواع کلاسهای AAL در شبکه‌های 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 ویدیوئی
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 لایه‌های AAL

لایه AAL در ATM به ۴ نوع تقسیم‌بندی می‌شوند که عبارتند از: AAL1 ، AAL2 ، AAL3/4 و AAL5 . AAL1مخصوص ارسال اطلاعات با نرخ ثابت می‌باشد. در AAL1 ارتباط زمانی بین مبدأ و مقصد حفظ می‌شود و از آن برای کاربردهایی که به تأخیر حساس هستند، نظیر ارسال صوت و ویدئو استفاده می‌شود. در AAL1 عملیات خطایابی در مقصد انجام می‌گردد. AAL2 کلاسهای B ترافیک‌های ATM را پشتیبانی می‌کند. به خاطر سادگی و بالاسری کم AAL5 و همچنین عدم شناخت کامل رفتار ترافیک‌های متغیر با زمان هنوز به‌طور کامل استاندارد نشده است.AAL3/4 برای ترافیک های کلاس‌های C و D مناسب می‌باشد. در AAL3/4 سرعت ارسال اطلاعات متغیر است و اطلاعات زمانی بین مبدأ ومقصد ارسال نمی‌گردند. دو نوع مد کاری برای AAL3/4 وجود دارد که عبارتند از: مد مطمئن و مد نامطمئن. درحالت کاری مطمئن، کنترل خطا و کنترل جریان بین مبدأ و مقصد انجام می‌شود و بنابراین بسته‌ها به‌طورسالم به مقصد تحویل داده می‌شوند. درحالت کاری نامطمئن امکان معیوب رسیدن بسته‌ها به مقصد وجود دارد.AAL5 مشابه با AAL3/4 می‌باشد و مشابه با آن دارای دو مد مطمئن و نامطمئن است. در AAL5 هیچ‌گونه سرآیندی توسط زیرلایه SAR به بسته اضافه نمی‌شود، بنابراین زمان پردازش سرآیند کم شده است. AAL5 توسط انجمن ATM استاندارد گردیده است. به غیر از انواع AALکه در بالا به آن اشاره گردید،یک نوع لایه AAL دیگر به نام SAAL[2] نیز وجود دارد که از آن برای ایجاد یک محیط مطمئن جهت تبادل اطلاعات سیگنالینگ بین کاربران استفاده می‌شود.

۶-۱۰- شبکه‌های خصوصی مجازی (VPN[3])

درچند ساله اخیر، شرکت‌های چندملیتی به مزایای استفاده اشتراکی از داده ها از طریق شبکه‌های کامپیوتری گسترده پی برده اند. امروزه با استفاده از فن‌آوری VPN ها امکان استفاده از مزایای استفاده اشتراکی داده ها برای کلیه

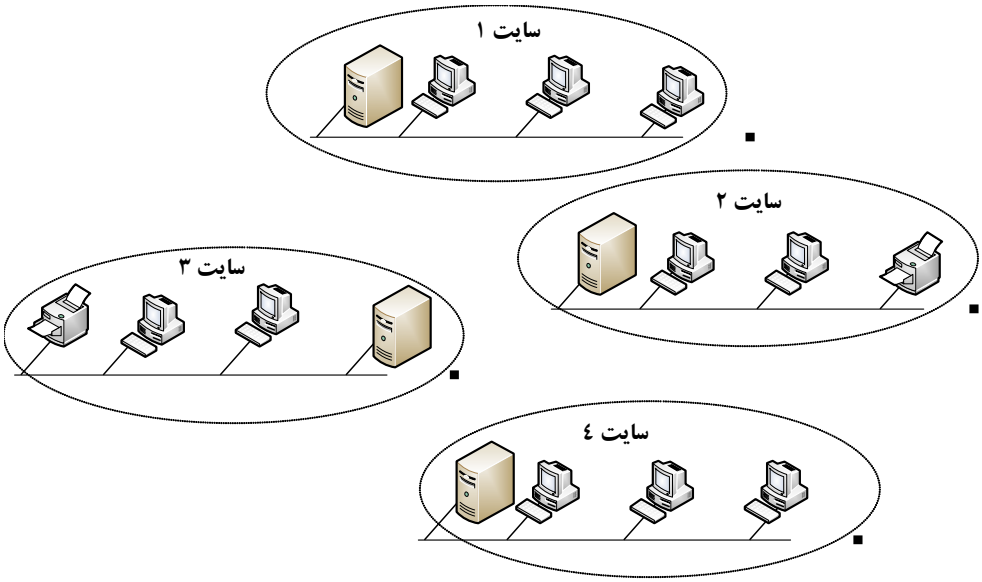
---

[1] Time relation

[2] Signaling AAL

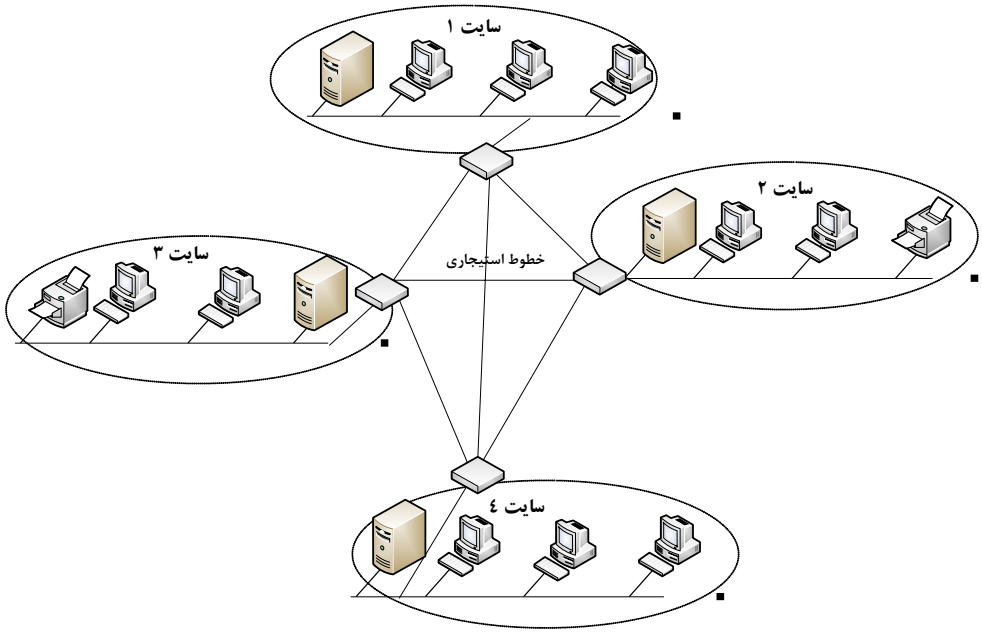
[3] Virtual Private Network

شرکت‌ها، حتی شرکت‌های کوچک فراهم شده است. درحالت عادی، چنانچه شرکتی دارای سایت‌های کامپیوتری متعـدد در نقاط مختلفی از دنیا باشد، امکان استفاده اشتراکی از داده ها بین شعبات مختلف شرکت وجود ندارد. به‌عنوان مثال در شکل (۶-۳۱) چهار سایت کامپیوتری مختلف یک شرکت که در نقاط گوناگون قرار دارند، نشان داده شده است.



شکل(۶-۳۱) : سایت‌های کامپیوتری مجزا ازیکدیگر

به خاطرعدم وجود اتصال های لازم بین سایت‌های کامپیوتری فوق، امکان استفاده اشتراکی از داده ها برای سایت‌های کامپیوتری وجود ندارد. با استفاده از خطوط استیجاری، مبادله مستقیم داده ها بین کامپیوترهای مختلف سایت‌های کامپیوتری فراهم می آید. این مسئله در شکل (۶-۳۲) نشان داده شده است.



شکل(۶-۳۲) : اتصال سایت‌های کامپیوتری مجزا ازیکدیگربه‌وسیله خطوط استیجاری

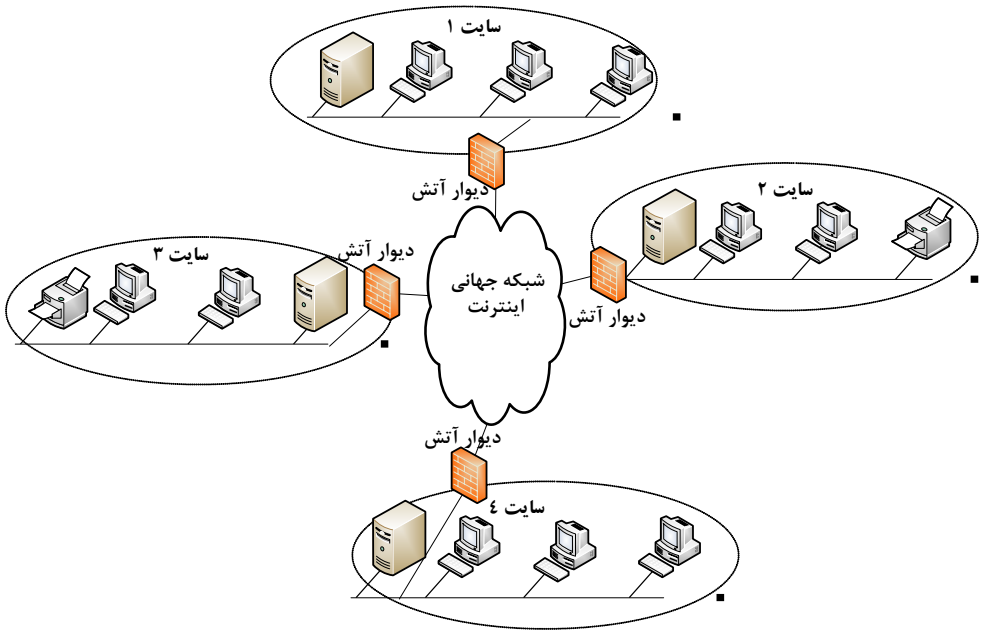
حتی بعد ازگسترش اینترنت و امکان استفاده از آن به خاطر قیمت پایین‌تر نسبت به خطوط استیجاری، به خاطر مشکلات امنیتی موجود دراتصال‌های اینترنتی، شرکت‌ها همچنان مایل به استفاده از خطوط گران قیمت استیجاری برای مبادلات داده‌های خود بودند. اخیراً با استفاده از فن‌آوری VPN، امکان مبادلات تجاری امن بین کامپیوترهای شبکه با استفاده از بستر اینترنت فراهم شده است.

VPN ها قادر به برقراری اتصالات خصوصی تونل بین سایت‌های کامپیوتری مختلف شرکت‌ها در بستر اینترنت می‌باشند. تونل‌های فوق درست مشابه خطوط استیجاری می‌باشند 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 می‌شوند.

برخلاف خطوط استیجاری گران قیمت، با استفاده از رمزنگاری‌های قوی داده‌های کامپیوترها به‌طور امن از طریق VPN ها مبادله می‌شود، طوری که نه تنها نفوذگران اینترنت بلکه خود ISP ها نیز قادر به استراق سمع داده‌ها نخواهند بود.

امروزه سازمان‌های 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 شرکت‌ها از افراد خارجی غیرمجاز نمی‌باشند.

مطابق با شکل (۶-۳۳) دیواره های آتشین مدرن، بدون آن‌که امنیت داده‌های سایت‌های کامپیوتری به خطر بیافتد قادر به برقراری ارتباط‌های VPN بین سایت‌های مختلف می‌باشند. فن‌آوری های مدرن VPN با استفاده از روش‌های رمزنگاری جدید قادر به اتصال سایت‌های کوچک و بزرگ به یکدیگر از طریق اینترنت می‌باشد طوری که کاربران راه دور به همان کیفیت کاربران محلی قادر به استفاده از منابع شبکه می‌باشند. به‌عنوان مثال کاربران راه دور مشابه کاربران محلی قادر به استفاده از داده‌های موجود درسرویس دهنده‌های وب هستند.



شکل(۶-۳۳) : اتصال سایت‌های کامپیوتری مجزا ازیکدیگربه‌وسیله VPN

با استفاده از رمزنگاری، امکان مخفی سازی اطلاعات محرمانه نظیر رمز عبور و داده‌های داخل پست‌های الکترونیکی وجود دارد.رمزنگاری VPN شامل دوقسمت است که عبارتند از:

- الگوریتم رمز نگاری
- کلید رمزنگاری

معمولاً الگوریتم رمزنگاری دانش عمومی بوده وهمه از روش آن آشنا هستند، ولی کلید رمزنگاری همواره مخفی می‌باشد. الگوریتم‌های رمزنگاری نوین مثل DES[1]، ازکلید رمز ۱۱۲ بیتی یا بیشتر استفاده می‌کنند. امنیت داده‌های رمز شده به امنیت کلید رمز بستگی دارد. هنگامی که دو سایت در مورد پیاده‌سازی VPN به توافق رسیدند، کلیدهای رمز خود را بین یکدیگر مبادله می کنند. علاوه برکاهش هزینه های VPN نسبت به خطوط استیجاری، درVPN ها با استفاده از ارتباط های مطمئن امکان تبادل داده‌های تجاری و محرمانه وجود دارد. VPN های مدرن امروزه نیازی به فن‌آوری های محرمانه ندارند، بلکه با استفاده از سخت افزارها و نرم افزارهایی که به راحتی قابل نصب می‌باشند، امکان استفاده از VPN وجود دارد. همچنین نصب VPN نیازی به تغییر درپیکره بندی سرویس دهنده های شبکه ندارد. سربار اضافی عملیات رمزنگاری VPN درشبکه به دیواره‌های آتش و مسیریاب‌های شبکه منتقل می‌شود و به سرویس دهنده شبکه بار اضافی تحمیل نمی‌شود.

۶-۱۰-۱- پروتکل امنیتی اینترنت (Ipsec[2])

امروزه دراکثر محصولات VPN، از پروتکل امنیتی Ipsec برای افزایش اطمینان شبکه استفاده می‌شود. Ipsec از فن‌آوری امنیتی کامل و جامعی استفاده می‌کند. Ipsec برای برنامه های کاربردی موجود امکانات محافظتی شفافی فراهم می آورد، طوری‌که بدون نیاز به اعمال تغییرات نرم‌افزاری در برنامه‌های کاربردی موجود، امکان محافظت پیام‌های آنها وجود دارد. درشکل (۶-۳۴) جایگاه پروتکل Ipsec درمعماری TCP/IP نشان داده شده است.

لایه کاربرد
TCP/IP
پروتکل IPsec
درایور کارت شبکه
کارت شبکه

شکل(۶-۳۴) : جایگاه پروتکل Ipsec

Ipsec برای تمام پیام های ارسالی، سه قابلیت حافظتی زیر را فراهم می سازد:

---

[1] Data Encryption Standard
[2] Internet Protocol Security

- رمزنگاری
- تصدیق هویت[1]
- حفظ تمامیت و درستی داده ها[2]

همان‌طور که قبلاً اشاره شد، رمزنگاری باعث پنهان ساختن محتویات پیام می‌گردد. تصدیق هویت باعث می‌شود که هویت فرستنده پیام مورد تایید و تصدیق گیرنده قرار گیرد. حفظ تمامیت و درستی داده ها، مانع دست‌کاری کردن تمام یا بخشی از پیام توسط افراد غیرمجاز می‌شود. این سه قابلیت حافظتی Ipsec مانع از دزدی و سرقت داده ها می‌شود.

براساس میزان گستردگی شبکه، نحوه استفاده از محصولات Ipsec متفاوت می‌باشد. سایت‌های بزرگ از پروتکل Ipsec که درداخل دیواره آتشین قرار دارد، برای محافظت اتصال‌های اینترنتی خود استفاده می کنند. سایت‌های کوچکتر می‌توانند از پروتکل Ipsec که داخل مسیریاب شبکه مخفی شده است، استفاده نمایند. کاربران انفرادی در ادارات کوچک و یا منازل می‌توانند از نسخه های رومیزی[3]، پروتکل Ipsec برروی کامپیوترهای خود استفاده کنند. تنها درصورتی‌که ترافیک ورودی به شبکه از یک کاربر و یا سایت مورد تأیید تولید شده باشد،Ipsec اجازه ورود آن را به شبکه سازمان می‌دهد.

سیر تکاملی Ipsec

امروزه Ipsec، به یکی از مهمترین پروتکل های امنیتی رایج مورد استفاده درصنعت تبدیل شده است. درسال ۱۹۸۰ آژانس امنیتی ملی آمریکا[4]، به منظور توسعه و ایجاد پروتکل های همه‌منظوره امنیتی شبکه، شروع به اجرای پروژه‌ای به نام SDNS[5] 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 Ipv4وفق داده شد. درسال ۱۹۹۰، پروتکل Ipsec ارائه گردید.

بعد ازآن تحقیقات ومطالعات زیادی برای تجدید نظر و توسعه و تکامل بیشتر پروتکل Ipsec انجام شد. پروتکل IKE[6] برای مدیریت اتوماتیک کلیدهای رمزنگاری در Ipsec مورد تأیید قرار گرفت. تمام بازنگری‌های اعمال شده برروی پروتکل Ipsec از طریق کمیته های استاندارد گزاری کنترل و نظارت می‌شود.

Ipsec قادر به استفاده دردیواره های آتشین و مسیریاب‌های متعدد می‌باشد. برای بررسی سازگاری محصولات، اکثر تولیدکنندگان دیواره آتشین و مسیریاب‌های شبکه اقدام به برگزاری آزمایش‌های تست سازگاری محصولات خود می نمایند. امروزه از Ipsec درسیستم عامل‌های ویندوز ۲۰۰۰ استفاده می‌شود.

پیاده سازی Ipsec VPN

شکلهای مختلف پیاده سازی Ipsec VPN به‌صورت زیر می‌باشد:

- سایت به سایت
- سرویس گیرنده /سرویس دهنده

---

[1] Authentication
[2] Integrity protection
[3] desktop
[4] National security agency
[5] Secure Data Network System
[6] Internet Key Exchange

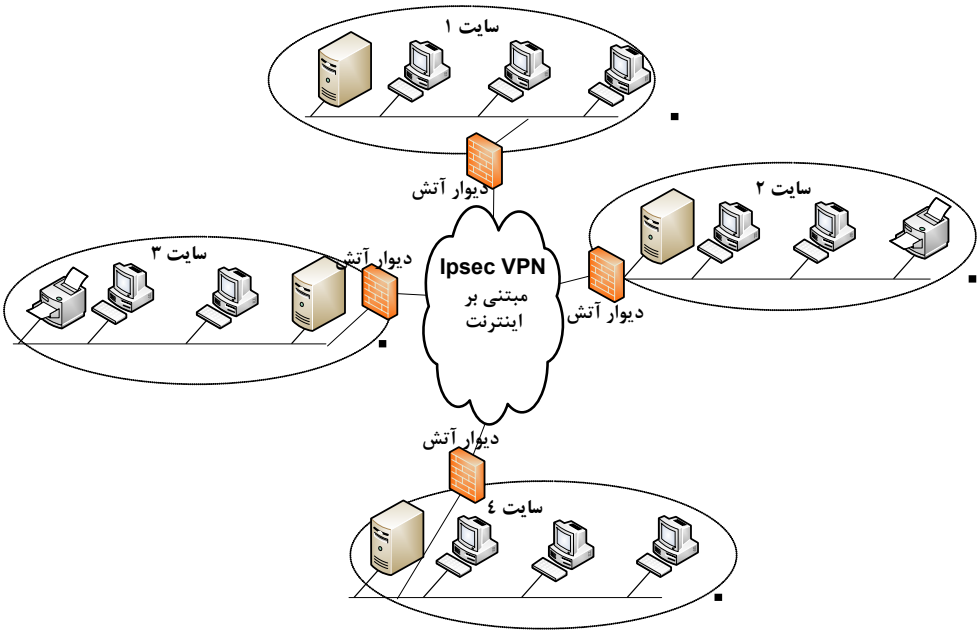
- ترکیب هردو روش

VPN های سایت به سایت از دو یا چند سایت جدا از هم که با استفاده از VPN به یکدیگر متصل شده و از داده‌های یکدیگر به‌صورت اشتراکی استفاده می کنند، تشکیل شده است.VPN های مبتنی برمدل سرویس گیرنده/ سرویس‌دهنده از تعدادی کاربر راه دور که از طریق اینترنت به سایت مرکزی (سرویس دهنده) متصل هستند، تشکیل می‌شوند.

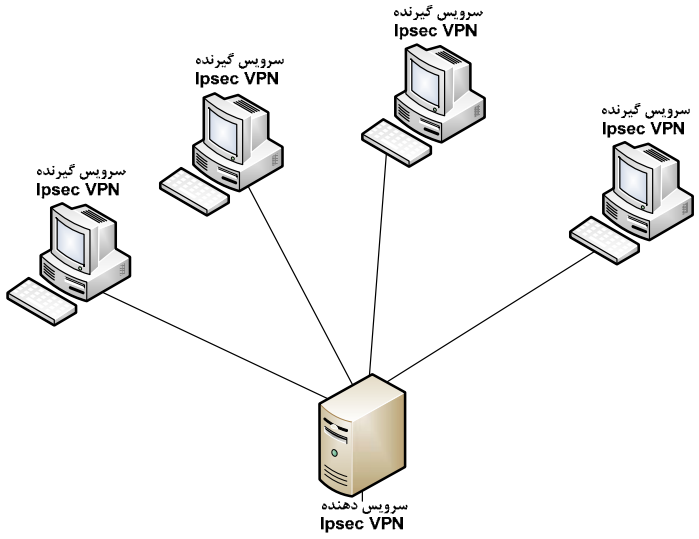
مطابق با شکل (۶-۳۵) در VPN های سایت به سایت، هرسایت ازطریق یک دیواره آتشین به اینترنت اتصال یافته است. ازدیواره آتشین به همراه Ipsec برای محافظت داده‌های مبادله شده بین سایت‌ها استفاده می‌شود.

برای برقراری VPN های سایت به سایت، هرسایت نیاز به اتصال اینترنت به همراه دیواره‌های آتشین با قابلیت Ipsec VPN دارد. برای برقراری اتصال‌های رمز شده مطمئن بین سایت ها، براساس پروتکل IKE، سایت‌ها باید اعتبارنامه های رمزنگاری خود را بین یکدیگر مبادله نمایند.

درشکل (۶-۳۶) ساختار VPN های مبتنی بر مدل سرویس گیرنده/سرویس دهنده نشان داده شده است. دراین ساختار یک سایت VPN با استفاده از پروتکل Ipsec اقدام به برقراری ارتباط‌های مطمئن با یک یا چند سرویس گیرنده انفرادی می‌کند. هردوطرف سرویس دهنده و سرویس گیرنده باید مجهز به نرم افزار Ipsec باشند.



شکل(۶-۳۵) : اتصال سایت‌های کامپیوتری مجزا از یکدیگر به‌وسیله Ipsec VPN مبتنی بر اینترنت



شکل(۶-۳۶): VPN از نوع سرویس گیرنده/سرویس دهنده

پرسش‌های فصل

۱. چهار وظیفه اصلی لایه شبکه را نام ببرید.

۲. شبکه‌های داده گرام و شبکه‌های مدارمجازی را از جنبه‌های مختلف با یکدیگر مقایسه نموده و برتری هریک را بردیگری توضیح دهید.

۳. ویژگی‌های اصلی الگوریتم‌های مسیریابی را نام برده وتوضیح دهید.

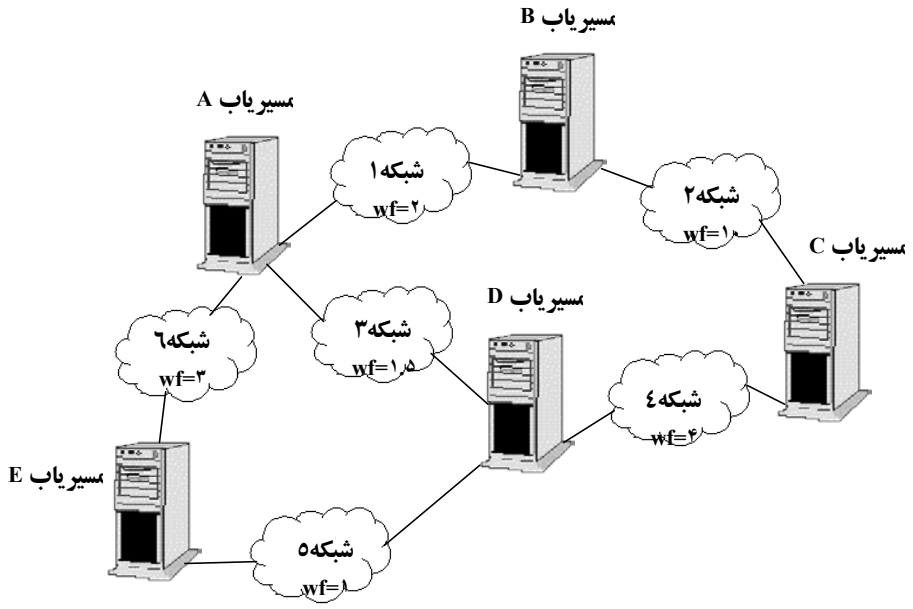
۴. الگوریتم‌های مسیریابی ایستا را نام برده و نحوه عملکرد هریک را به اختصار توضیح دهید.

۵. برتری الگوریتم‌های مسیریابی پویا را برالگوریتم‌های مسیریابی ایستا تشریح کنید.

۶. نحوه عملکرد الگوریتم مسیریابی بردار فاصله را توضیح دهید.

۷. درشبکه زیر مراحل ایجاد و تکمیل جداول مسیریابی هر مسیریاب را با استفاده از الگوریتم مسیریابی بردار فاصله توصیف کنید.(ارزش عددی هرلینک با wf[1] نشان داده شده است)

[1] Weight factor



۸. نحوه عملکرد الگوریتم مسیریابی وضعیت لینک را توضیح دهید.
۹. نقاط ضعف و قوت دو الگوریتم مسیریابی بردار فاصله و وضعیت لینک را بایکدیگر مقایسه کنید.
۱۰. مفهوم ازدحام درشبکه‌های کامپیوتری را نوشته و دلایل ایجاد آن را توصیف کنید.
۱۱. مفهوم ارتباط بین شبکه ای را توضیح دهید.
۱۲. رده های مختلف اتصال شبکه‌ها به یکدیگر را نوشته و از هریک مثالی ذکر کنید.
۱۳. عملکرد تکرارکننده را دراتصال شبکه‌ها به یکدیگر توضیح دهید.
۱۴. عملکرد پل را دراتصال شبکه‌ها به یکدیگر توضیح دهید.
۱۵. برتری پل را نسبت به تکرار کننده توضیح دهید.
۱۶. انواع پل را نوشته و عملکرد هریک راتوضیح دهید.
۱۷. عملکرد مسیریاب را در اتصال شبکه‌ها به یکدیگر توضیح دهید.
۱۸. عملکرد دروازه را در اتصال شبکه‌ها به یکدیگر توضیح دهید.
۱۹. سه دسته کلی سرویس را درشبکه‌های ISDN نام برده و هریک را توضیح دهید.
۲۰. انواع کانال‌های ISDN و سرعت هریک را بنویسید.
۲۱. عملکرد TE2،TE1،NT2،NT1 و TA را درISDN توضیح دهید.
۲۲. با رسم شکل جایگاه نقاط مرجع R,S,T و U را درISDN بنویسید.
۲۳. مدل لایه‌ای ISDN را نوشته و پروتکل‌هایی را که در هرلایه استفاده می‌شود را توضیح دهید.
۲۴. ساختار واسط کاربر به شبکه در لایه فیزیکی ISDN را با رسم شکل توصیف کنید.
۲۵. برتری B-ISDN را برISDN نوشته و موارد کاربرد آن را توضیح دهید.
۲۶. انواع سرویس ارائه شده توسط B-ISDN را توضیح دهید.
۲۷. ساختار قاب‌ها رادر frame relay نوشته و عملکرد هر فیلد آن‌را توضیح دهید.
۲۸. با ذکر یک مثال نحوه ایجاد اتصال بین دو کامپیوتر را درشبکه‌های frame relay توضیح دهید.
۲۹. اهدافی را که در طراحی فن‌آوری ATM مد نظر بوده است، نام ببرید.

۳۰. ویژگی‌ها و مزایای عمده ATM را بنویسید.
۳۱. انواع اتصال‌ها را درATM نوشته و نحوه ایجاد مدارمجازی درآن را توضیح دهید.
۳۲. مفهوم آسنکرون بودن ATM را توصیف کنید.
۳۳. کاربرد سیگنالینگ در ATM را نوشته و انواع پیام‌های آن را توضیح دهید.
۳۴. برای برقراری اتصال‌های نقطه به چند نقطه درATM از چه پیام‌هایی استفاده می‌شود؟
۳۵. ویژگی‌های لایه فیزیکی در ATM را نوشته و انواع کانال‌های فیزیکی را که درATM استفاده می‌شود نام ببرید.
۳۶. ساختارسلول‌های ATM را رسم نموده و عملکرد هریک از فیلدهای موجود درسرآیند سلول‌های ATM را توضیح دهید.
۳۷. انواع کلاس‌های سرویس پشتیبانی شده لایه AAL درATM را نوشته و مشخصه‌های مشخص سازی این سرویس را توضیح دهید.
۳۸. عملکرد شبکه‌های خصوصی مجازی را توضیح دهید.
۳۹. پروتکل امنیتی Ipsec را دراینترنت توصیف کنید.
۴۰. قابلیت‌های محافظتی Ipsec را توضیح دهید.
۴۱. روش‌های مختلف پیاده سازی Ipsec VPN را توصیف کنید.

فصل هفتم

معماری TCP/IP

۷-۱- تاریخچه TCP/IP

برای اولین بار درسال 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[1]) ، 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. درسال ۱۹۶۵ آقای Lawrence Roberts از دانشگاه MIT اقدام به اتصال کامپیوتری در Massachusetts آمریکا به کامپیوتردیگری درایالت کالیفرنیا این کشور و از طریق خطوط تلفنی نمود. درسال ۱۹۶۶ این شخص تجربه عملی فوق را به DARPA منتقل نمود. در سال ۱۹۶۸ DARPA قرارداد همکاری با شرکت BBN برای پیاده‌سازی نرم‌افزار شبکه

[1] Deffence Advance Research Project Agency

آرپانت که از قدیمیترین شبکه‌های سوئیچینگ بسته‌ای می‌باشد، منعقد ساخت. بسیاری از مراکز تحقیقاتی و دانشگاه‌ها و پایگاه‌های نظامی از شبکه آرپانت برای پیاده‌سازی و آزمایش پروژه‌های تحقیقاتی خود استفاده کردند.
درسال 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. درسال ۱۹۷۰ مراکز دیگری شامل دانشگاه MIT، دانشگاه Harvard ، شرکت های BBN و SDC به شبکه فوق اضافه شدند. به دنبال آن درسال ۱۹۷۱، آزمایشگاه هایLincoln دانشگاه MIT و دانشگاه های Carnegie-Mellon وCase-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 به‌عنوان بخشی از شبکه دفاعی ملی (DNN) استفاده کرد.
دردهه ۷۰، معماری TCP/IP توسط فردی به نام Bob Kahn درشرکت BBN ارائه گردید و بعدها توسط Vint Cerf دردانشگاه Stanford و دیگران توسعه یافت. درسال ۱۹۸۰ وزارت دفاع آمریکا معماری فوق را جایگزین پروتکل قدیمی NCP[1] درشبکه خود نمود. این معماری درسال 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 نام‌های میلنت و آرپانت شد. شبکه آرپانت به‌عنوان یک شبکه تحقیقاتی و آزمایشگاهی باقی ماند و میلنت برای کاربردهای نظامی و انتقال داده‌های محرمانه استفاده گردید. هر دو شبکه از بستر سخت‌افزاری یکسانی برای تبادل اطلاعات استفاده می‌کردند و امکان تبادل اطلاعات بین این دو شبکه وجود داشت. از شبکه آرپانت به‌عنوان یک شبکه پایه و اساسی برای پیاده‌سازی شبکه جهانی اینترنت استفاده شد. شبکه آرپانت دارای ۵۰ مینی‌رایانه مدل C30 و C300 ساخت شرکت BBN بود که از آن به‌عنوان سوئیچ‌های شبکه استفاده می‌شد. شبکه آرپانت دارای وسعت زیادی بود و تقریباً سراسر آمریکا و اروپای غربی را گسترش می داد. در ابتدای راه‌اندازی شبکه آرپانت اغلب ازکانال‌های خطوط اجاره‌ای با سرعت ۵۶ کیلوبیت برثانیه استفاده می‌گردید، ولی امروزه از کانال‌های با سرعت بالاتر برای اتصال نودهای شبکه اینترنت استفاده می‌شود. 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 می‌دهد. درسال ۱۹۸۶ شبکه NSFNET[2] با استفاده از کانال های ۵۶ کیلوبیت برثانیه درایالت متحده آمریکا توسعه یافت.
در شکل (۷-۱) مدل لایه‌ای و معماری TCP/IP که از آن به‌عنوان معماری شبکه جهانی اینترنت استفاده می‌شود، نشان داده شده است. یکی از قابلیت‌های عمده TCP/IP ، امکان استفاده از آن در اتصال شبکه‌ها به یکدیگر جهت ایجاد یک شبکه وسیعتر می‌باشد. با استفاده از معماری TCP/IP امکان اتصال چندین شبکه محلی و ایجاد یک شبکه وسیعتر فراهم می‌آید. معماری TCP/IP قبل از مدل لایه‌ای مرجع OSI به‌وجود آمد و بنابراین لایه‌های TCP/IP به‌طور کامل با لایه‌های OSI مطابقت ندارند.
همان‌طور که در شکل (۷-۱) نیز مشاهده می‌شود، در معماری TCP/IP از پنج لایه فیزیکی، پیوند داده، شبکه، حمل و لایه کاربرد استفاده می‌شود. می‌توان گفت که لایه کاربرد در TCP/IP معادل سه لایه جلسه، ارائه و کاربرد در مدل OSI می‌باشد. در سطح لایه حمل در مدل TCP/IP از دو پروتکل TCP[3] و UDP[4] و در سطح لایه شبکه از پروتکل اینترنت (IP[5])استفاده می‌شود. یکی از مزایای بسیار عمده معماری TCP/IP که باعث گسترش و محبوبیت آن شده است، این

[1] Network Control Protocol
[2] National Science Foundation Network
[3] Transmission Control Protocol
[4] User Datagram Protocol
[5] Internet Protocol

است که در این معماری هیچ استاندارد و پروتکل خاصی برای لایه‌های اول و دوم وضع نشده است. این امر باعث می‌شود که به‌راحتی بتوان از TCP/IP برروی فن‌آوری‌های مختلف لایه فیزیکی استفاده کرد. در سطح لایه کاربرد، از پروتکل‌های کاربردی مانند FTP،SNMP[1]،DNS[2]،TELNET و SMTP[3] استفاده می‌شود.

<table>
<tr><td>ping</td><td>telnet & rlogin</td><td>FTP</td><td>SMTP</td><td>SNMP</td><td>Trace Route</td><td rowspan="2">لایه کاربرد</td></tr>
<tr><td>DNS</td><td>TFTP</td><td>BOOTP</td><td>RIP</td><td>OSPF</td><td>….</td></tr>
<tr><td colspan="2">TCP</td><td colspan="2">UDP</td><td colspan="2">ICMP</td><td>لایه حمل</td></tr>
<tr><td colspan="6">IP</td><td>لایه شبکه</td></tr>
<tr><td colspan="3"></td><td colspan="2">LLC</td><td colspan="2">HDLC PPP</td><td rowspan="2">لایه پیونددداده</td></tr>
<tr><td>اترنت</td><td>802.3</td><td>X.25</td><td>حلقه نشانه</td><td>frame relay</td><td>ATM</td><td>SMDS …</td></tr>
<tr><td colspan="2">فیبرنوری</td><td>UTP</td><td>کابل هم محور</td><td colspan="2">مایکروویو</td><td>ماهواره</td><td>لایه فیزیکی</td></tr>
</table>

شکل (۷-۱): معماری TCP/IP

۷-۲- نیاز به آدرس‌های IP

درشبکه های کامپیوتری، با اتصال چند شبکه به یکدیگر، شبکه اینترنت ایجاد می شود. باید توجه نمودکه شبکه جهانی اینترنت که درآن 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 آدرسهایIP، 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 برآن باید مراقب بود که آدرس IP با آدرسهای IP نود های دیگر آن بخش شبکه سازگار باشد. هنگام پیاده سازی معماری TCP/IP برروی یک شبکه، یکی از کارهایی که باید انجام شود انتخاب و پیکره بندی درست آدرسهای IP است. دو نسخه فعلی از پروتکلIP 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. پروتکلIP نسخه۶ که پروتکل نسل بعدی است، برای جایگزینی IP نسخه ۴ طراحی شده است. پروتکلIP 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 ازمقادیرعددی یا اسمی استفاده نمود. آدرسهای شبکه مشخص کننده های نقطه دسترسی به سرویس[4]در لایه شبکه مدل مرجع هستند. این آدرسها، آدرسهای SAP شبکه(NSAP[5]) نام دارند ومی بایست برای همه پروتکل هایی که در لایه شبکه مدل مرجع ارتباط برقرارمی کنند، یکتا باشند.

---

[1] Simple Network Management Protocol
[2] Domain Name System
[3] Simple Mail Transfer Protocol
[4] Service Access Point (SAP)
[5] Network SAP

در سطح لایه شبکه مدل مرجعTCP/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 اسامی نمادین کارآمدتر است و این دلیل دیگری است که چرا مقادیر عددی برای آدرسهای شبکه مناسبتر از اسامی نمادین هستند. به طور کلی لایه های بالاتر مدل مرجعTCP/IP مایل به استفاده ازآدرسهای 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. اگرN 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.

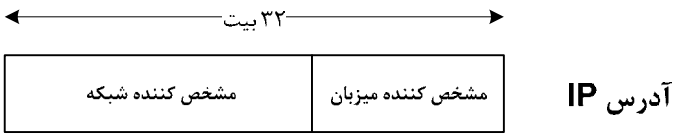
معماری TCP/IPروی انواع مختلف سخت افزار شبکه قابل اجرا می باشد. برای مثال اترنت، شبکه حلقوی و FDDI از آدرسهای فیزیکی ۴۸ بیتی استفاده می کنند. بقیه انواع سخت افزار شبکه ممکن است از آدرس های ۸ بیتی، ۱۶ بیتی و یا ۳۲ بیتی استفاده کنند. با استفاده از آدرس های منطقی به جای آدرس های فیزیکی، پروتکل اینترنت مجبور 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 $۲^{۳۲}$ 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 درشکل (۷-۲) دیده می شود، آدرس IP دارای طول کلی چهار بایت می‌باشد که از دو قسمت عمده تشکیل شده است و عبارتند از:

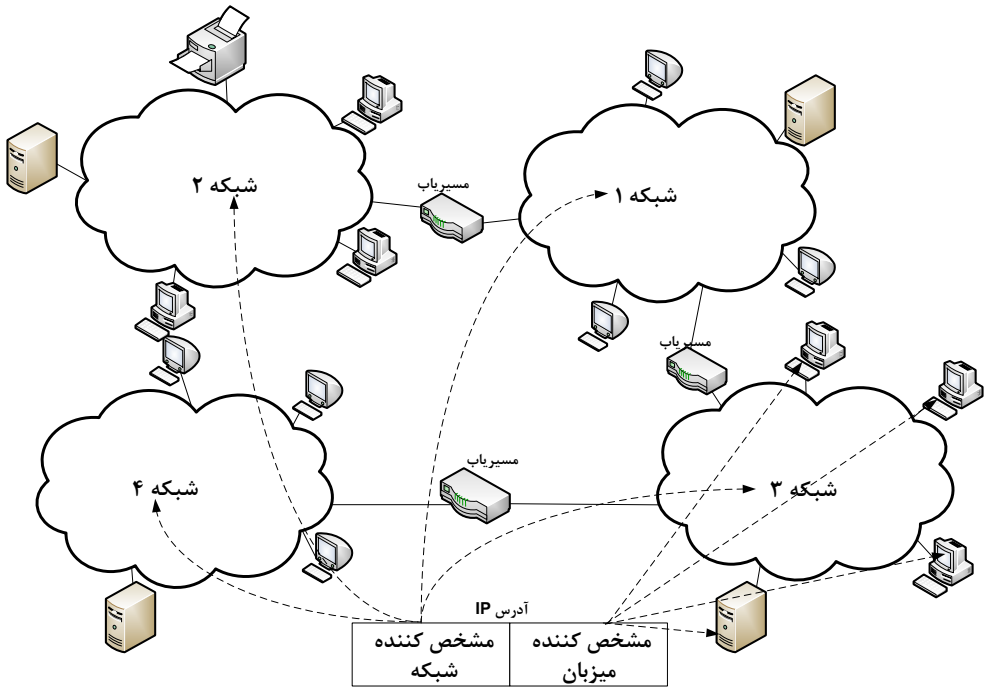
- بخش مشخص‌کننده شبکه (netid[1])
- بخش مشخص‌کننده میزبان (hostid[2])



شکل (۷-۲): استفاده از آدرس IP برای شناسایی شبکه و میزبان

[1]Network identifier
[2]Host identifier

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 وباعث 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 اندکه درشکل (۷-۴) نشان داده شده است. کلاسD برای عملیات چندپخشی رزرو شده است. این کلاس از آدرسهای IP، توسط پروتکلهای مخصوصی برای انتقال پیامها به یک گروه انتخابی از نودها

استفاده می شود. کلاس E برای استفاده های آینده رزرو شده است. جدول(۷-۱) تعداد شبکه هاوتعداد میزبانهایی که درهر 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 وبزرگ مناسبند. شبکه های کلاس C برای سازمان های کوچک مناسبند. درشبکه 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 دهدهی نمایش داده می شوند. اعداد دهدهی بوسیله نقطه از هم جدا می شوند. این نوع نمایش آدرس، نشانه گذاری دهدهی نقطه دار نامیده می شود. در زیر یک آدرس IP در شکل دودویی و نشانه گذاری دهدهی نقطه دار آن نشان داده شده است.

آدرس IP = ۱۰۰۱۰۰۰۰ ۰۰۰۱۰۰۱۱ ۰۱۰۰۱۰۱۰ ۱۱۰۰۱۰۰۱

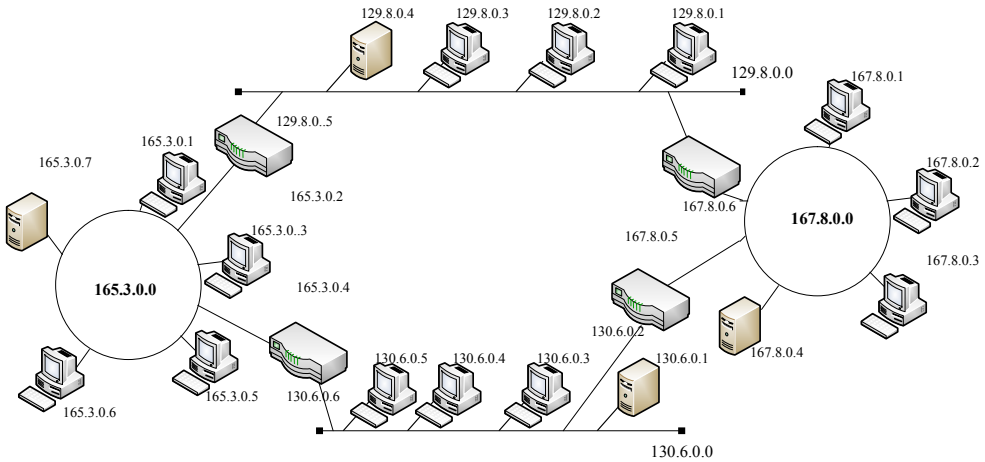
آدرس IP = 144.19.74.201

جدول(۷-۲)، بازه مقادیر اولین عدد دهدهی یک آدرس IP را در نشانه گذاری دهدهی نقطه دار نشان می دهد. با استفاده از این جدول کلاس آدرس IP را به آسانی با بررسی اولین عدد دهدهی آدرس IP می توان مشخص کرد.

جدول(۷-۲): تشخیص کلاس آدرس IP از اولین عدد دهدهی

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

درشکل (۷-۵) مثالی از تخصیص آدرس های IP دریک شبکه اینترنت نشان داده شده است.



شکل (۷-۵) : مثالی از آدرس‌های IP در یک شبکه اینترنت

۷-۴- آدرسهای IP خاص

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

دراین آدرس، فیلدشماره 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 معمولا زمانی استفاده می شودکه یک نود شبکه سعی می کند تا آدرس IP 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 ازمقدار 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، آدرسIP خود را از پاسخ BOOTP بدست آورد دیگرازآدرس 0.0.0.0 استفاده نمی کند. آدرس 0.0.0.0 در جداول مسیریابی نیز استفاده می شود تا ورودیهای شبکه را برای آدرسIP 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 آدرسIP مقصد استفاده نمی شود.

۷-۴-۲- آدرس 0.hostid

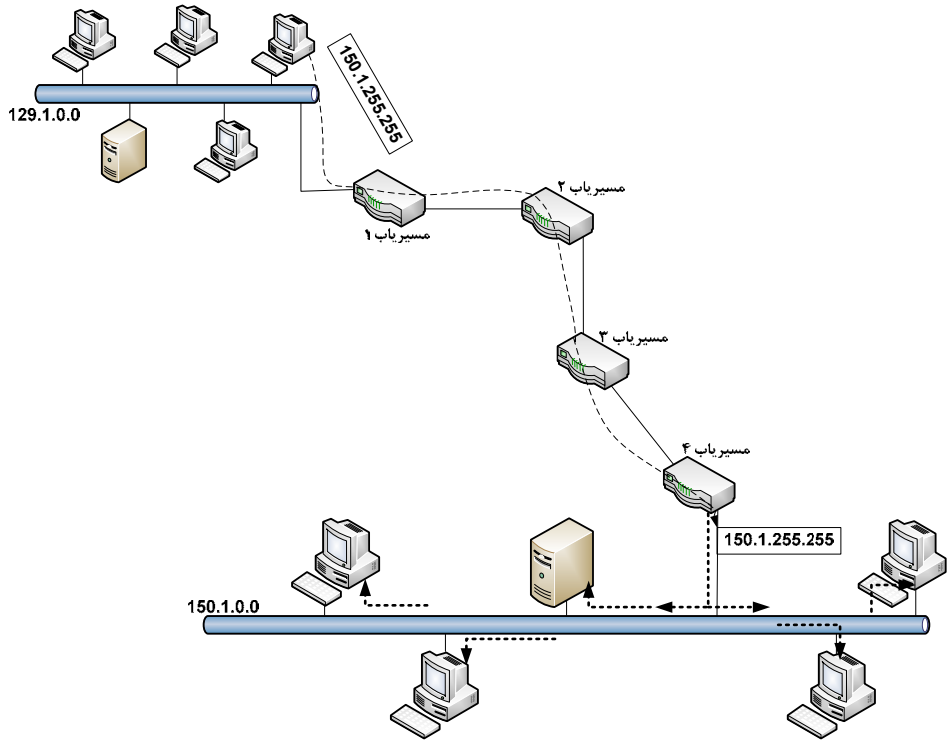
این آدرس به معنی شماره میزبان در "این شبکه" است. اگر یک نود در شبکه ای بسته ای را دریافت کند که شماره شبکه در آدرس IP مقصد صفر باشداما شماره میزبان موجود درآدرس مقصد با آن نود مطابقت داشته باشد، نود بسته را خواهد پذیرفت. گیرنده مقدار صفر را در شماره شبکه به معنی این شبکه تفسیر می کند.

۷-۴-۳-آدرس netid.255

این آدرس همه پخشی مستقیم[1]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 پخشی مستقیم توسط همه نود های شبکه دیده می شود. بنابراین به عنوان مثال برای شماره شبکه 137.53، آدرس همه پخشی 137.53.255.255 خواهد بود.

پیام های همه پخشی مستقیم به یک شبکه خاص فرستاده می شوند که شماره آن شبکه در فیلد شماره شبکه آدرسIP مقصد مشخص می شود. مسیریابهای شبکه، قادر به پیش بردن بسته های همه پخشی 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 درشکل (۷-۶) دیده می شود، آدرس های همه پخشی مستقیم از مسیریاب های میانی شبکه عبور کرده و در شبکه مقصد به همه میزبان ها به صورت همه پخشی ارسال می شوند. دراین مثال، ایستگاهی درشبکه بالا به آدرس شبکه 129.1.0.0 بسته همه پخشی 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 پخشی مستقیم است. بنابراین با استفاده از قابلیت همه پخشی لایه ۲، بسته دریافتی را به همه میزبان های شبکه ارسال می دارد.

[1] Directed broadcast



شکل (۷-۶): 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 دربخش خاص آدرس مقصد قراردهد. اگر همه پخشی در یک شبکه محلی مورد نظرباشد، 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 بیتهای 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 شدکه عدد ۱۲۷ که باید دربازه مقادیر کلاسA باشد، درمجموعه آدرس های کلاس A استفاده نمی شود. این عدد برای قابلیت برگشت حلقه رزرو شده است. آدرس برگشت حلقه یک آدرس مخصوص است. درخیلی 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 . ابزارPing یک بسته ICMP را به یک آدرسIP مقصد می فرستد و لایه IP در آن آدرس به آن پاسخ می دهد. درفصل 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. ازتک 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 ازنودها 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 مستقیما 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 دربازه 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 معمولا 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 دریک 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 دارندیا خیر؟ میزبانهایی که به یک گروه چندپخشی می پیوندند یا آن را ترک می کنند از پروتکل مدیریت گروه اینترنت[1](IGMP) برای گزارش عضویتشان 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 جاریشان در فواصل معین نیزدارند. این

[1] Internet Group Management Protocol(IGMP)

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، ازتوانایی سخت افزاری چند پخشی شبکه های محلی استفاده می شود.

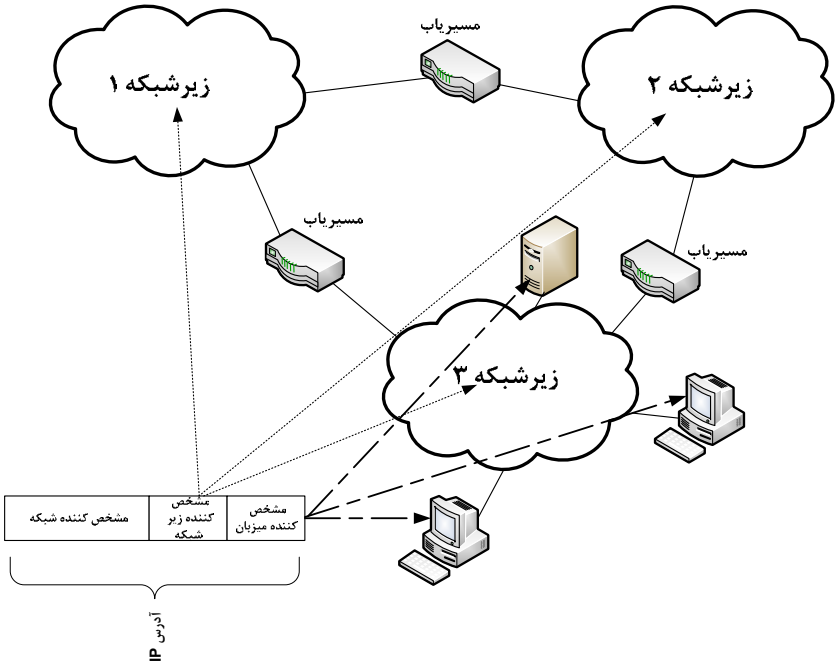
۷-۵- زیر شبکه سازی

آدرس هایIPV4 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 درآنها بود. برای حل مشکل اتلاف فضای آدرس IP، مفهوم زیر شبکه سازی درسال ۱۹۸۵ مطرح گردید.

زیر شبکه ها با استفاده از یک شماره شبکه، امکان اتصال چندین شبکه را به یکدیگرممکن می سازند. همانطور که قبلا ذکر شد، آدرس شبکه برای همه میزبان های داخل یک شبکه یکسان است. معمولا 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 ۲۴بیت 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 درجدول مسیریابی داشته باشیم، میتوان با استفاده از یک رکورد مجرد جدول مسیریابی همه میزبان های در یک شبکه را خلاصه کرد. این رکوردجدول 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 آدرسIP مقصد موجود دربسته 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 کلا $۲^{۱۶}$ 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 کل۶۵۵۳۶ شماره میزبان ممکن، تنها از دو شماره میزبان نمی توان استفاده کرد. بنابراین درکل۶۵۳۵۴ میزبان باقی می ماند.

استفاده ازقابلیت 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.



شکل(۷-۷): زیر شبکه و شماره های زیر شبکه

مسیریاب های موجود بین زیرشبکه 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 کارآیی شبکه
- ساده سازی مدیریت
- ساختار دهی مجدد یک شبکه داخلی بدون اثر گذاشتن شبکه های خارجی
- بهبود بخشیدن امنیت

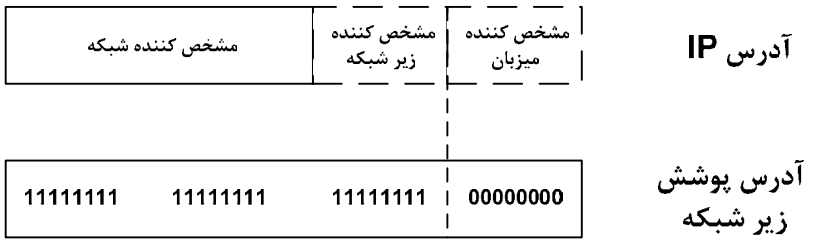
۷-۵-۱- پوشش زیر شبکه[1]

پوشش زیر شبکه بوسیله مسیریابها و میزبانهای زیر شبکه به منظورتشخیص 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 دهدکه برابر 255.255.255.0 می باشد.

[1] Subnet mask



شکل (۷-۸): نمایش پوشش زیر شبکه

از آنجاییکه درقالب بسته های IP کلاس B فضای مشخص کننده میزبان برابر با ۱۶ بیت می باشد، بنابراین درحالت 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 تعداد۱های موجود درآدرس پوشش زیرشبکه فوق، می توان دریافت که فضای مشخص کننده میزبان درآدرس 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، آدرسIP 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 (اینترانت ها)

درسال 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 دراین شبکه ها را می توان به گروه های زیر کلاس بندی کرد:

- میزبانهایی که نیاز به دستیابی به میزبانهایی درسازمانهای تجاری دیگر یا اینترنت ندارند.
- میزبانهایی که نیاز به دستیابی به سرویسهای خارجی محدودی مانند e-mail،FTP , remote login Netnews و غیره دارند که می توان با استفاده از دروازه لایه کاربرد این دستیابی رافراهم نمود.
- میزبانهایی که نیاز به دستیابی درسطح لایه شبکه به شبکه خارج از سازمان تجاری دارند. این نیازمندی ازطریق 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 درهمان شبکه خصوصی اعتبار داشته و ازدنیای 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

تجاری برای اتصال به شبکه داخلی خود به اینترنت از دروازه های لایه کاربرد (مانند دیواره آتش[1]) استفاده می کنند. شبکه داخلی معمولا 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[2] آدرس های IP تخصیص داده می شود. نهاد IANA توسط ICANN[3] اداره می شود.ICANN یک شرکت غیرانتفاعی کالیفرنیای آمریکا می باشد که درسال 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 10.255.255.255 تا 10.0.0.0
- ۱۶ شبکه کلاسB از آدرس172.31.255.255 تا 172.16.0.0
- ۲۵۶ شبکه کلاس C از آدرس 192.168.255.255 تا 192.168.0.0

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 ووسایل 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[4])

سیستم NAT آدرس های IP شبکه محلی را به آدرسهای یکتا برای استفاده بر روی اینترنت تبدیل می کند. هرچنداین 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 پروتکلهایTCP/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 ازدید اینترنت پنهان می دارد. از سوی دیگر اینترنت، کل شبکه را به صورت یک دستگاه ساده می بیند که به اینترنت متصل می باشد.

---

[1] Firewall
[2] Internet Assigned Numbers Authority
[3] Internet Corporation for Assigned Names and Numbers
[4] Network Address Translation

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 سرویس 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 سرویس دهنده هایی هستند که به یک درخواست خاص پاسخ می دهند. این روش برای توزیع بار یک سرویس دهنده پرترافیک برروی یک سری سرویس 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 هرکدام 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. پروتکلPPTP 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 سرویس داخل شبکه باید از پراکسی استفاده کرد.
- یک ارتباط همیشه دوطرفه است: وقتی یک سرویسگیر با یک سرویس دهنده ارتباط برقرار می کند، یک ارتباط از سرویس دهنده به سمت سرویسگیر نیز ایجاد می شود. برقراری ارتباط با بعضی سرویس دهندهها، مثلاً یک وب سایت ، ممکن است منجر به بروز مشکلات امنیتی در شبکه شود. ازآنجا که روی تمام ارتباطات ایجاد شده از طرف شبکه داخلی نمی توان کنترل داشت بهتر است برای هر سرویس از پراکسی استفاده کرد تا محتویات بسته هایی که وارد شبکه می شوند کنترل شود.

۷-۷- ابر شبکه سازی

تکنیک زیر شبکه سازی در سال ۱۹۸۵ برای استفاده کار امد 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 کلاسB کاملا خوب کار می کند، اما این قالب های آدرس شبکه خیلی عمومی بوده و به سرعت درحال 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 کلاسC عملی نباشد. مخصوصا 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 درحال استفاده و روبه اتمام می باشند. این پدیده که نشان دهنده اتمام فضای آدرس می باشد، پدیده ROADS[1] خوانده می شود. با وجود اینکه آدرسهای کلاس A و کلاس B روبه اتمام می باشند، ولی هنوزتعداد 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 کاررا 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، ابرشبکه سازی نام دارد. درحقیقت ابرشبکه 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 ازفضای 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 ۳۲تایی آدرس کلاس C استفاده کنند.یک شبکه کلاس B تا ۶۵۵۳۴ میزبان را پشتیبانی می کند اما در این مثال ۵۷۵۳۵= ۸۰۰۰-۶۵۵۳۴ آدرس بکار نخواهد رفت. بنابراین با تخصیص بهینه تعداد آدرس های مورد نیاز با استفاده از روش ابرشبکه سازی، امکان استفاده بهینه از فضای آدرس های IP فراهم شده و از هرگونه اتلاف درفضای آدرس های IP جلوگیری می شود.

تکنیک ابر شبکه سازی برای استفاده ارائه دهندگان سرویس اینترنت(ISP[2]) برای تداوم اتصال اینترنت طراحی شده است. معمولا 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 ازسازمانهای تجاری که به آنها بلوک های آدرس کلاس C انتساب داده شده است از ابرشبکه سازی استفاده می کنند. ابرشبکه 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 ازطرف 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 ۲۵۶تایی از آدرس های کلاس C می باشد. بنابراین مسیریاب های شبکه،

[1] Running Out of ADderss Space
[2] Internet Service Provider
[3] Classless Inter Domain Routing

درجدول مسیریابی خود به جای استفاده از یک رکورد، از ۲۵۶ رکورد استفاده می نمایند. این امر افزایشی را در تعداد ورودی های جدول مسیر یابی 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 نیازداشته باشد، با عوض کردن این آدرسها با آدرسهای کلاس C به حافظه ای برابر با ۵۱۲=۲۵۶*۲ مگابایت نیاز دارد.

برای رفع مشکل فوق، از تکنیک مسیر یابی 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 ابرشبکه، برای پیشوند یکسان همه آدرس های کلاس C شامل۱است 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 درفضای 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 111111111=200.1.191.255

نشانه گذاری دیگری که می توان برای بلوک های CIDR استفاده به شرح زیر است:

تعداد بیتهای پیشوند مشترک / پایین ترین آدرس در بلوک

تعداد بیتهای پیشوند مشترک، بیانگر تعداد ۱های 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 آدرسIP 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 ۴زیاد 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.

برای رفع مشکل فوق، موسسه استانداردگذاری اینترنت (IETF[1]) تصمیم به طراحی پروتکل اینترنت نسل بعدی گرفت که به عنوانIPng یا IP نسخه ۶ (IPV6) شناخته می شود. یکی ازاهداف طراحی IPV6 استفاده ازآدرسهای ۱۲۸ بیتی می باشدکه 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 بیتهای 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 وارتباط 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.

پروتکلIPV6 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. طراحانIPV6 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 کاراکتردونقطه (:) 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 درآدرس 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 درآدرس های IPv6 را می توان حذف نمود وبه جای آن "::" جایگزین کرد. بنابراین آدرس IPV6 پیش را می توان به صورت زیر نوشت :

48A6::DA3:3F: 1

نمایش IPV6 آدرس IPV4 170.1.1.1 به صورت زیر می باشد:

0:0:0:0:0:0: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 درمدل 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 باذکر 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. دریک 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 زیرشبکه 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 دراینترنت

لایه شبکه درمعماری TCP/IP شامل چند پروتکل مهم می باشد. دراین فصل به بررسی پروتکل های این لایه شامل : پروتکل ARP[1]، پروتکل RARP[2] 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. همانطورکه درفصل 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 ازآنجاییکه پروتکل IP درلایه سوم قراردارد، طبق روال ارسال داده درمعماری لایه ای شبکه، انتقال بسته های لایه سوم مستلزم استفاده از امکانات لایه دوم می باشد. بنابراین ازآنجاییکه بسته های IP دردل 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 درکامپیوترمقصد، 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.
درمعماری TCP/IP از پروتکل DNS[3] برای نگاشت بین آدرس های اسمی که دربرنامه های کاربردی استفاده می شوند و آدرس های IP که درسطح 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[4] نیز گفته می شود) از آدرس IP استفاده می شود.سوالی که اینجامطرح می شوداین 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 هرکامپیوتر شبکه، دارای جدولی باشد که درآن جدول آدرس IP و آدرس MAC همه کامپیوتر های شبکه نوشته شده است. هرگاه کامپیوتری نیاز به آدرس MAC کامپیوتردیگری 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 درصورت تغییر آدرس MAC یک ایستگاه (به عنوان مثال درهنگامی که کارت شبکه یک کامپیوتر عوض شود) باید رکورد مربوط به آن کامپیوتر جداول مربوط به سایر کامپیوتر ها نیز عوض شودکه این کار نیاز به صرف هزینه و وقت زیاد است.

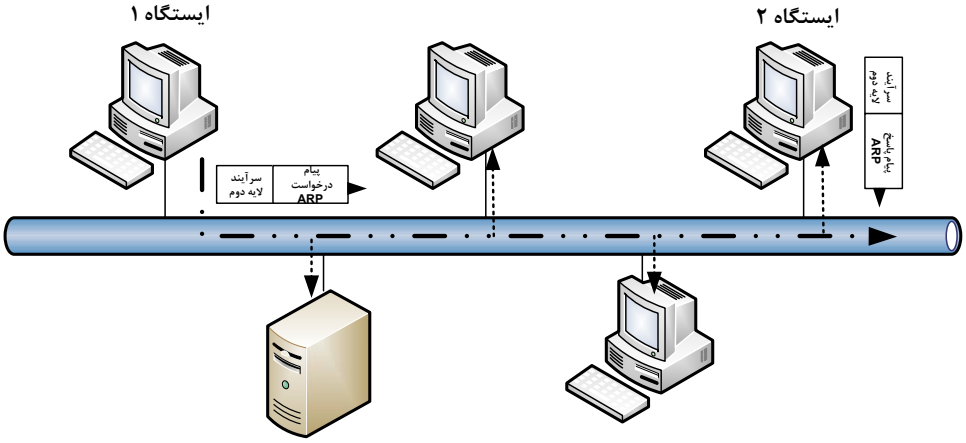
---

[1] Address Resolution Protocol
[2] Reverse Address Resolution Protocol
[3] Domain Name System
[4] Medium Access Control

این روش پیکره بندی دستی TCP/IP برای تعریف انطباق بین آدرس های IP و آدرس های MAC درگذشته 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. دراین شکل فرض می شودکه ایستگاه ۱ می خواهد داده ای را برای ایستگاه ۲ ارسال دارد. بدین منظور باید ابتدا آدرس MAC ایستگاه ۲را بدست آورد.



شکل(۸-۱): عملکرد ARP

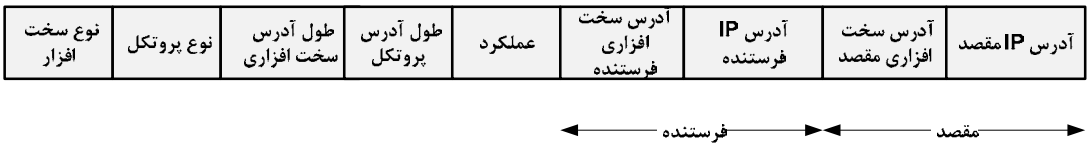
ایستگاه ۱ یک قاب همه پخشی MAC را که پیام درخواست ARP نامیده می شود، به شبکه می فرستد .پیام درخواست ARP شامل آدرس IP و آدرس MAC میزبان فرستنده یعنی ایستگاه ۱ و آدرس IP میزبان مقصد یعنی ایستگاه ۲ است . پیام درخواست ARP شامل یک فیلد خالی برای آدرس سخت افزاری مقصد یعنی ایستگاه ۱ است .همه نود ها در شبکه فیزیکی پیام در خواست همه پخشیARP را دریافت می کنند. سایر نود هاییکه قاب همه پخشی را دریافت می کنند ، آدرس IP خود را با آدرس IP موجود درقاب درخواست ARP مقایسه می نمایند. تنها میزبانی که همان آدرس IP خواسته شده در پیام در خواست ARP را دارد، به درخواست فوق پاسخ می دهد. اگر ایستگاه ۲ در شبکه موجود باشد، آدرس سخت افزاری خود را درفیلد خاصی درپیام فوق قرار داده و به آن پاسخ می دهد. به پیام ارسالی، پیام پاسخ ARP می گویند. بعد از آنکه ایستگاه۱ پاسخ ARP را دریافت کرد، دریک جدول خاص به نام جدول حافظه پنهان ARP که درحافظه اصلی خود نگهداری می کند، زوج آدرس IP و سخت افزاری ایستگاه ۲ را قرار می دهد. درصورتیکه درآینده نیاز به ارسال مجدد به ایستگاه ۲ باشد، ابتدا ایستگاه۱ محتوای این جدول را جستجوکرده و درصورت نیافتن آدرس سخت افزاری ایستگاه ۲ روال درخواست ARP را انجام می دهد. محتویات جدول فوق، یک زمان زندگی خاصی دارندکه دراکثر 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.

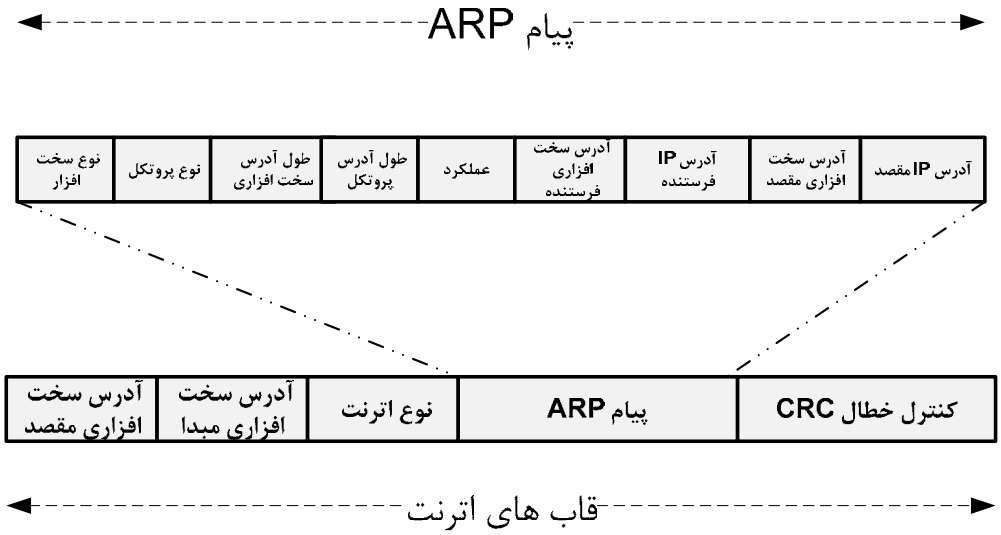
درهنگام ارسال پیام درخواست ARP ازآنجاییکه آدرس سخت افزاری مقصد هنوز معلوم نیست، بنابراین درخواست فوق درلایه دوم به صورت همه پخشی ارسال شده طوری که همه میزبان های شبکه بتوانند آنرا دریافت نمایند. پاسخ ARP که توسط نود مقصد فرستاده می شود یک قاب همه پخشی نیست، زیرا نود گیرنده درخواست ARP، آدرس سخت افزاری فرستنده پیام فوق را درفیلد خاصی درپیام فوق بدست آورده و درهنگام پاسخ دهی به درخواست فوق، قاب پاسخ را به صورت تک پخشی ارسال می دارد. فرض عملکرد پروتکلARP این است که شبکه فیزیکی زیرین توانایی همه پخشی را پشتیبانی می کند که در مورد شبکه های محلی مانند اترنت ، شبکه حلقوی ، FDDI ،ARCnet صدق می کند.

۸-۱-۲- ساختاربسته 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 . بعدا" برای شبکه های محلی دیگر مانندشبکه های محلی IEEE802 توسعه داده شد . پیام هایARP در قالب قاب های لایه پیوند داده بسته بندی می شود . شکل(۸-۳) مثالی از یک بستهARP را نشان میدهد که در یک قاب اترنت جاسازی شده است.



شکل(۸-۲): قاب 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 دربسته ARP است. این فیلد که دوبایت طول دارد (بایت ۸ بیتی) نشان دهنده نوع سخت افزار شبکه است. مقدار ۱در فیلد نوع سخت افزار نشان دهنده یک شبکه اترنت

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 ARP	توصیف
۰	اترنت ۱۰ مگابیت برثانیه
۲	اترنت آزمایشی ۳ مگابیت برثانیه
۴	حلقه نشانه
۵	Chaos Net
۶	شبکه های IEEE 802
۷	ARCNET
۱۴	SMDS
۱۵	Frame Relay
۱۶و۱۹و۲۱	ATM
۱۷	HDLC
۱۸	Fiber Channel

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 مقدارعدد مبنای شانزده۸۰۰ برای فیلد نوع پروتکل استفاده می شود. فیلدطول آدرس سخت افزاری بر حسب بایت است. این فیلد ۱بایت 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 دهدکه آدرس سخت افزاری آن ۸ بایت است. بنا براین مقدار فیلد طول آدرس سخت افزاری برای شبکه های اترنت ۸ است.

فیلد طول آدرس پروتکل، طول آدرس پروتکل مورد استفاده درلایه 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 (درمبنای 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 ونشان دهنده این است که آیا بسته فعلی یک بسته درخواست ARP و یا یک بسته پاسخ ARP است. البته به غیر از این دوبسته، 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

۶	پیام پاسخ DRARP
۷	پیام خطای DRARP
۸	پیام درخواست InARP
۹	پیام پاسخ InARP
۱۰	پیام ARP NAK

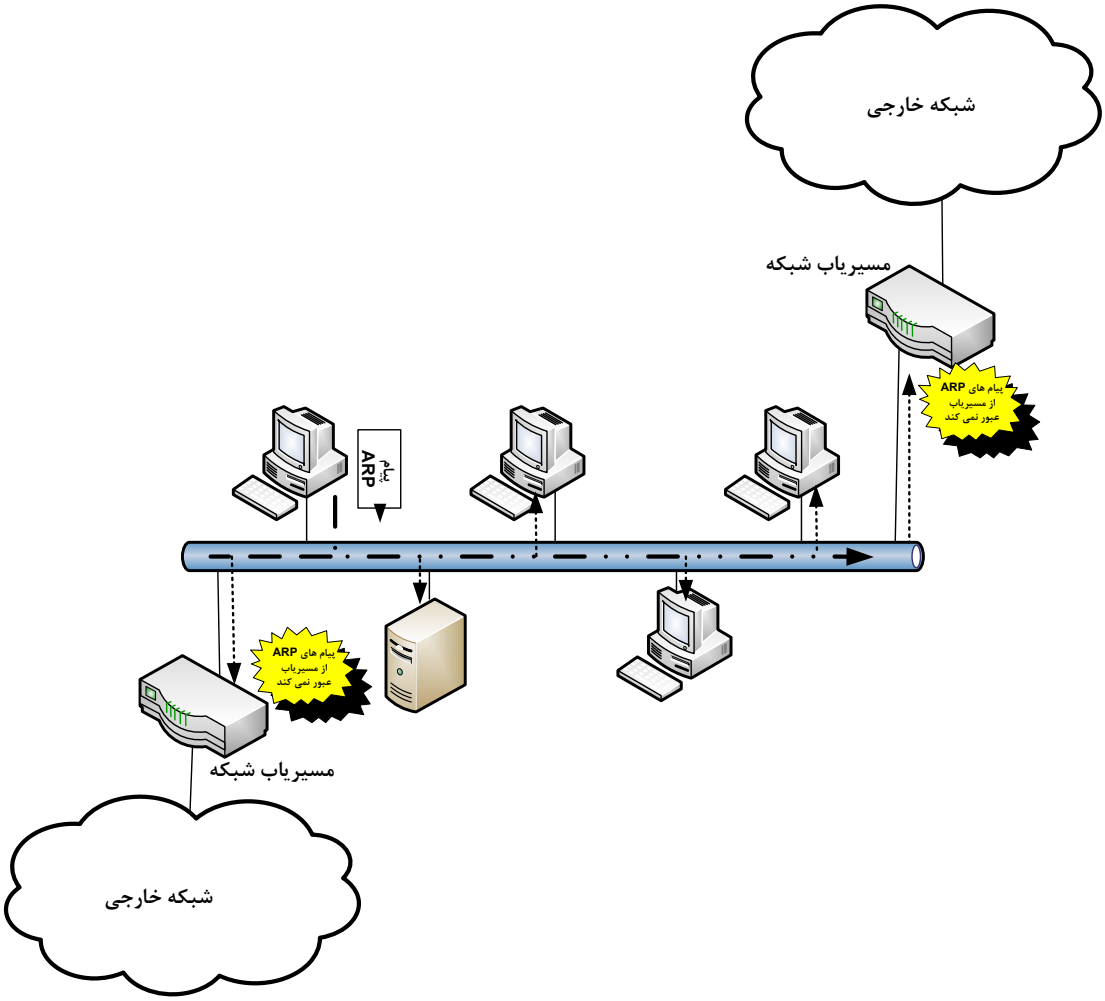
فیلد آدرس سخت افزاری فرستنده، نشان دهنده آدرس سخت افزاری نود فرستندهٔ درخواست ARP است. فرستنده، آدرس سخت افزاری خود را با خواندن آن از کارت شبکه بدست آورده و این فیلد را پر می کند. آدرس IP فرستنده نشان دهنده آدرس IP نود فرستنده درخواست ARP است. فرستنده، آدرس IP خود را با خواندن از یک فایل پیکره بندی یا خواندن حافظه پنهان خود که شامل اطلاعات پیکره بندی شبکه است بدست می آورد و درفیلد 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 معمولا بیتهای ۱ یا بیتهای صفر دارد. آدرس سخت افزاری مقصد می تواند آدرس همه پخشی سخت افزار باشد که آن را برای بعضی از جنبه های پیاده سازی مناسب می سازد.
فیلد آدرسIP مقصد در بسته درخواست ARP دربرگیرنده آدرسIP 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 آن۲ 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 درپیام درخواست ARP است. نود مقصد آن را با بررسی فیلد آدرس IP فرستنده در درخواست ARP بدست می آورد.

هنگامی که کامپیوتر مقصد دریک 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 شودرا پیدا کند.
در مورد شبکه های همه پخشی از پروتکلARP برای یافتن آدرس سخت افزاری نود مقصد استفاده می شود. پروتکلARP به عنوان بخشی از ماژول IP در شبکه هایی که نیاز به تجزیه آدرس دارند، مانند شبکه های محلی همه پخشی (اترنت ، شبکه حلقوی و غیره) پیاده سازی می شود. مطابق شکل (۸-۴)، پروتکل ARP توسط پروتکل IP بسته بندی نمی شود

بلکه مستقیما 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 درشکل(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 مقصدرا جستجو نموده و آن را به ماژول ARP برمی گرداند.



شکل (۸-۴):محدودیت ARP در بخش شبکه محلی

درصورتیکه 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 قبلا ذکر شد، پاسخ ها و درخواست های ARP به بخش شبکه محلی محدود شده و از مرزمسیریاب عبور نمی کنند.

نوع پروتکل (IP)	آدرس پروتکل (آدرس های IP)	آدرس سخت افزاری	شماره واسط	برچسب زمانی

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 پخشی 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 در خواست 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 برشبکه با کمک پروتکلARP

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 درقاب های ARP می توان اطلاعات مفیدی درمورد پروتکل های لایه سوم موجود درشبکه بدست آورد. هنگامی که سیستم نظارتی شبکه، یک پیامARP رادریافت 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.

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 نمودکه 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 بستهARP نشان دهنده درخواستARP باشد وآدرس پروتکل مقصد با آدرس پروتکل ایستگاه ناظرمطابقت کند، ایستگاه ناظر نیزیک پاسخ ARP را مانند هر نود مقصد دیگر می فرستد.

۸-۱-۴- مهلت های زمانی[1] 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 درشبکه 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 دراین 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، دراین صورت پشت یک مرز مسیریاب است . دراین حالت آدرس IP نود نقل مکان کرده حتی اگر آدرس سخت افزاری همان باقی بماند، باید تغییر کند. ازآنجاییکه انتقال پیام های ARP از مرزیک مسیریاب امکان پذیرنمی باشد، بنابراین فرض می شود که نود جدید خاموش شده یا غیر قابل دسترس 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، دراین صورت ورودی مربوط به آن رکورد درجدول ARPپنهان 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 نآدرست 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 دریک شبکه TCP/IP مشکل فیزیکی ایجاد شود، ترمیم در لایه های پائین انجام می گردد. ماژول 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 بیافتد. 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

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 ازترافیک شبکه ایجاد می کند که به قابلیت دسترسی به سایر نود های شبکه اثرمنفی 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 وپردازش 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 وباعث کند کردن آن نود می شود. در نتیجه همه نود های شبکه به نظر کند میشوند.
همه پخشی های تکراری ARP ، درشبکه هایی که بوسیله پل از یکدیگر جدا شده اند، وضعیت را بدتر نیز می نماید. دراین 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 درشبکه 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 درنظر بگیرید که دو سرویس گیرنده TCP/IP به نامهای ایستگاه ۱ و ایستگاه ۲ درآن 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 ۱و۲ 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 درشبکه منتشرکند. 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 IP	آدرس سخت افزاری
144.19.74.1	B

همچنین جدول حافظه پنهان ARP برای ایستگاه ۱ به شرح زیر است :

آدرس IP	آدرس سخت افزاری

144.19.74.102	A

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. بدینمنظورایستگاه 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 پروتکلARP، 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، ایستگاه۲ 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 IP	آدرس سخت افزاری
144.19.74.1	C

جدول حافظه پنهان ARP برای ایستگاه ۲ به شرح زیر است :

آدرس IP	آدرس سخت افزاری
144.19.74.102	A

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. متاسفانه این آدرس آدرس سخت افزاری ایستگاه ۲ است و داده به ایستگاه ۲ فرستاده میشود. ایستگاه ۱در 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 هرصورت برنامه کاربردی فوق که تا مدتی پیش خوب کار می کرده است، ممکن است به طور ناگهانی از کاربیافتد.

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 درسرویس 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 کنیدکه 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 پخشی

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، هردو 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 دهنده۲ 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 IP	آدرس سخت افزاری
144.19.74.1	C

جدول حافظه پنهان ARP سرویس دهنده۲:

آدرس IP	آدرس سخت افزاری
144.19.74.1	C

جدول حافظه پنهان ARP ایستگاه:

آدرس IP	آدرس سخت افزاری
144.19.74.102	B

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، درسرویس دهنده ۲ نداشته باشد، اتصال پذیرفته نمی شود. درصورتیکه شناسه کاربر و کلمه رمزعبوردر هر دو سرویس دهنده یکسان باشد، کاربر به سرویس دهنده اشتباه متصل می شود. دراین حالت این امکان وجود دارد که کاربربه 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

دربسیاری از نسخه های معماری TCP/IP، هرکامپیوتر درهنگام راه اندازی یک درخواست ARP را درشبکه منتشر می نماید. دراین پیام، آدرس IP مقصد موجود درپیام درخواست ARP مساوی با آدرس IP نود ارسال کننده پیام می باشد. هدف از ارسال پیام درخواست ARPفوق، کشف این مطلب است که آیا نودی با آدرس IP تکراری وجود دارد یا خیر؟ درصورتیکه نودارسال کننده پیام، درپاسخ به درخواست فوق، پیام پاسخ ARP دریافت نماید، بدین معنی است که نوددیگری با آدرس IP نود فرستنده وجود دارد و این نشان دهنده وجود آدرس های IP تکراری درشبکه می باشد. درصورت وقوع این حالت، نودی که متوجه وجود آدرس تکراری درشبکه شده است، باید به نحوه مناسب تکراری بودن آدرس فوق را به اطلاع برساند.

با توجه به اینکه قاب های ARP از مسیریاب 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 مسیریاب 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- پروتکلRARP

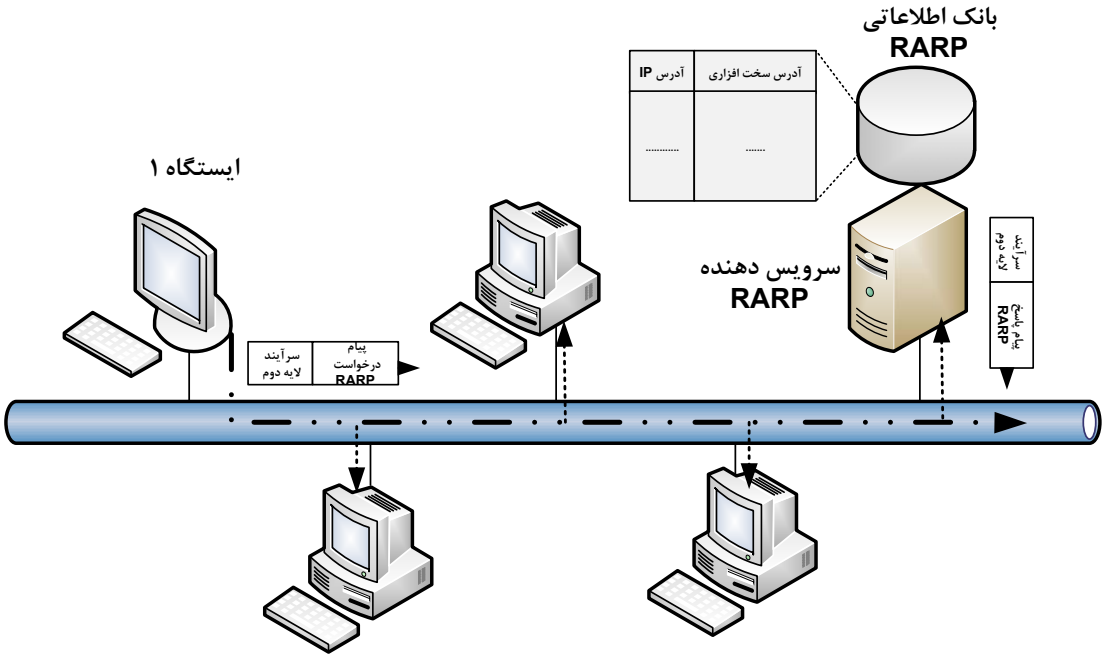
هنگام توصیف عملکرد پروتکل ARP فرض براین بود که هر نود، آدرس IP خود را می داند. سوالی که مطرح می شود این است که چگونه یک نود آدرس IP خود را بدست می آورد؟ می توان آدرس IP نود رادرانباره محلی آن که معمولا یک فایل است، ذخیره نمود. اسم و محل آن فایل به پیاده سازی TCP/IP و سیستم عامل بستگی دارد. با این وجود 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.
معمولا 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. معمولا 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 به صورت یک قاب همه پخشی لایه پیوند داده ارسال می شود. بدین منظور از پروتکل RARP استفاده می شود. اطلاعاتی که توسط پروتکلRARP 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- عملکردپروتکل RARP

در پروتکلRARP ، نودی که می خواهد آدرس IP خود را کشف کند (سرویس گیرنده RARP)، یک پیام درخواست را به نام پیام درخواست RARP درشبکه 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 درلایه پیوند داده همه پخشی می شود. همه نود های موجود درشبکه 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. معمولا

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 RARPمطابقت 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 ازپیام 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. دراین مثال فرض براین است که ایستگاه شماره ۱، آدرس IP ندارد. بدینمنظور پیام درخواست RARP به صورت همه پخشی درلایه ۲ ارسال می دارد. این پیام به سرویس دهنده RARP می رسد. سرویس دهنده با جستجو دربانک 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 درپیام های درخواست و پاسخ RARP به شرح زیر می باشد:

پیام درخواست RARP

آدرس سخت افزاری مقصد درلایه دوم = همه پخشی

آدرس سخت افزاری مبدا درلایه دوم= آدرس سخت افزاری سرویس گیرنده RARP (ارسال کننده پیام)
فیلدEther Type موجود درقاب های پروتکل پیوند داده لایه دوم = 8035 hex
فیلد عملکرد موجود دربسته درخواست RARP = ۳ (نشان دهنده پیا م درخواستRARP)
آدرس سخت افزاری فرستنده موجوددربسته درخواستRARP = آدرس سخت افزاری سرویس گیرندهRARP (ارسال کننده پیام)
آدرسIP فرستنده موجود دربسته درخواستRARP = نامشخص است. معمولا از 0.0.0.0 استفاده می شود.
آدرس سخت افزاری مقصد موجود دربسته درخواستRARP = آدرس سخت افزاری سرویس گیرنده RARP
آدرسIP مقصد موجود دربسته درخواستRARP = نامشخص

پیام پاسخ RARP

آدرس سخت افزاری مقصد درلایه دوم= آدرس سخت افزاری سرویس گیرنده RARP
آدرس سخت افزاری مبدا درلایه دوم= آدرس سخت افزاری سرویس دهنده RARP
فیلدEther Type موجود درقاب های پروتکل پیوند داده لایه دوم = 8035 hex
فیلد عملکردموجود دربسته های RARP = ۴ (پاسخ RARP)
آدرس سخت افزاری فرستنده موجود دربسته پاسخ RARP= آدرس سخت افزاری سرویس دهنده RARP .
آدرس IP فرستنده موجود دربسته پاسخ RARP = آدرس IP سرویس دهنده RARP .
آدرس سخت افزاری مقصد موجود دربسته پاسخ RARP= آدرس سخت افزاری سرویس گیرنده RARP.
آدرسIP مقصد موجود دربسته پاسخ RARP = آدرس IP سرویس گیرنده RARP (این جواب است)

در خیلی از پیاده سازیهایTCP/IP، پروتکل RARP به طور اتوماتیک توسط ماژول ARP یا ماژول IP فراهم نشده بلکه باید به عنوان یک فرایند جداگانه درکامپیوتری که به عنوان سرویس دهنده RARP عمل می کند، اجرا گردد.

۸-۲-۲- مشکلات RARP

درصورتیکه 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. دراین 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 دردسترس 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. دراین حالت سرویس گیرنده های RARP زیادی به ارسال در خواست های همه پخشی RARP به طور نامحدود ادامه می دهند به امید اینکه سرویس دهنده RARP درنهایت 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

رای دستیابی مطمئن تر به سرویس های RARP ، ازچندین 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 قرارگرفته وسایرپاسخ های RARP دیگر حذف می شوند. برای جلو گیری 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 درنظر 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 وفقط 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.

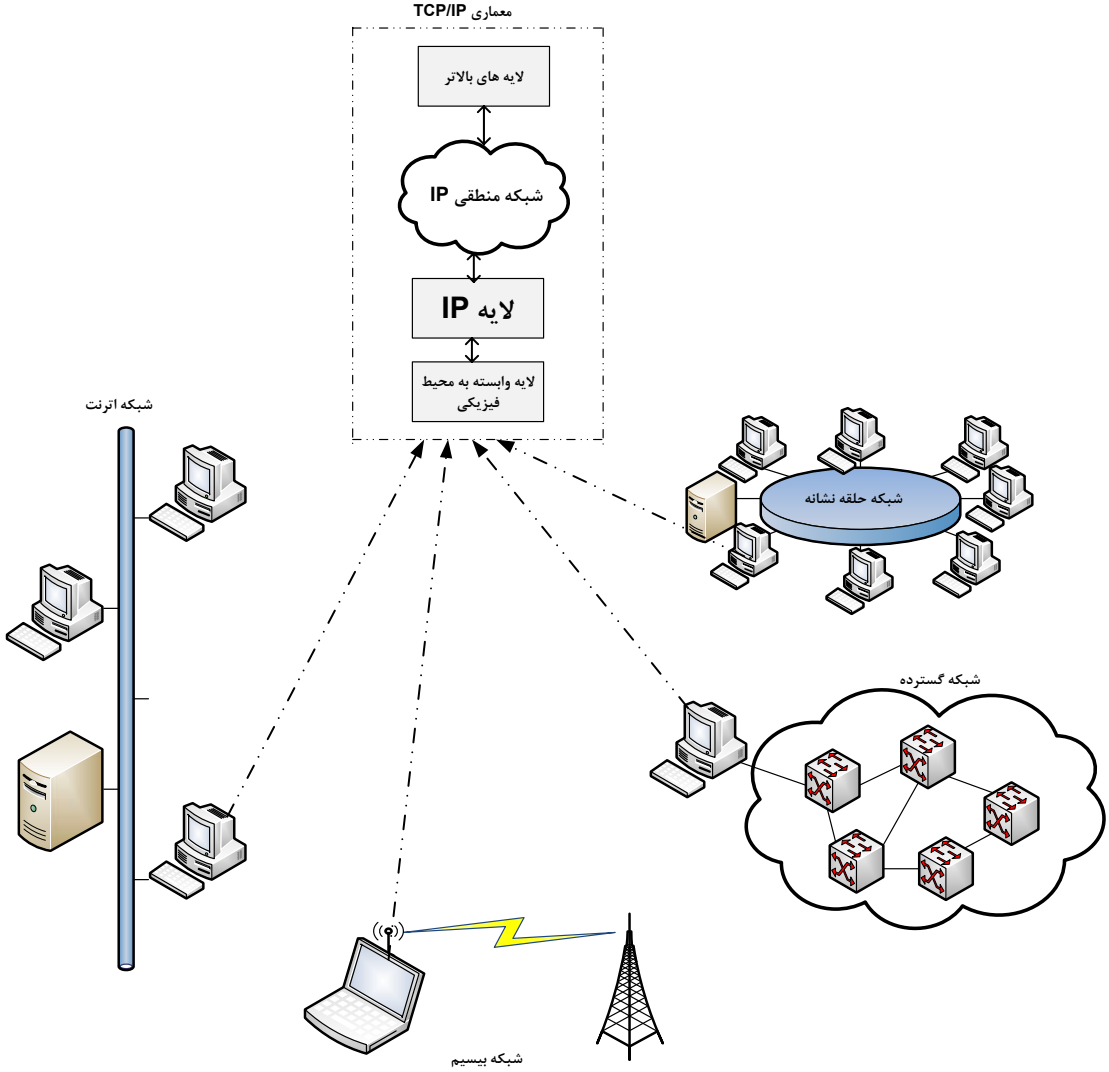
۸-۳- پروتکل اینترنت (IP)

با استفاده ازپروتکل 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 ویا 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 تاخیرکم و گذردهی مناسب را انتظاردارند. 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. لایهIP 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 رانشان می دهد. درتمامی این شبکه ها میزبان هایی وجود دارند که از معماری TCP/IP استفاده می نمایند. دراین 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 درلایه 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 ازنوع ۴ مگابیت برثانیه، ۴۴۴۰ بایت است. این اندازه برای شبکه حلقوی IEEE802.5

[1] Maximum Transfer Unit

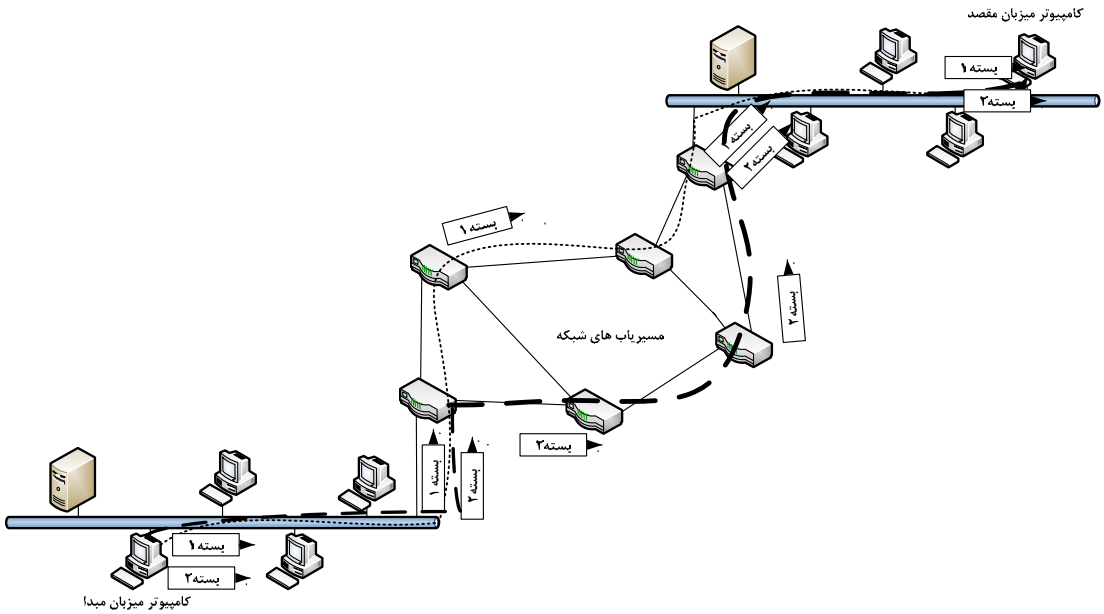
۱۶مگابیت برثانیه، ۱۷۹۴۰ بایت می باشد. درشبکه هایX.25 اندازه MTU اختیاری بوده و در بازه ۶۴ بایت تا۴ کیلو بایت قابل تغییر است. باید توجه داشت که حداقل طول یک بسته IP نمی تواند از ۵۷۶ بایت کمتر باشد.

پروتکل IP بدون اتصال بوده که هر بسته درآن 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 برروی شبکه های فیزیکی مختلف

درشکل(۸-۸) مثالی از مسیریابی بسته ها دریک شبکه IP نشان داده شده است.



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. درپروتکل IP هر بسته مستقل از بقیه بسته ها مسیر یابی می شود. هربسته شامل آدرسIP مقصد و آدرسIP فرستنده می باشد.

مسیریاب های میانی شبکه با استفاده از آدرس IP مقصد، بسته هایIP 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 شبکهIP در صورت نیاز می توانند یک بسته بزرگ را تکه سازی نمایند.

پروتکلIP 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

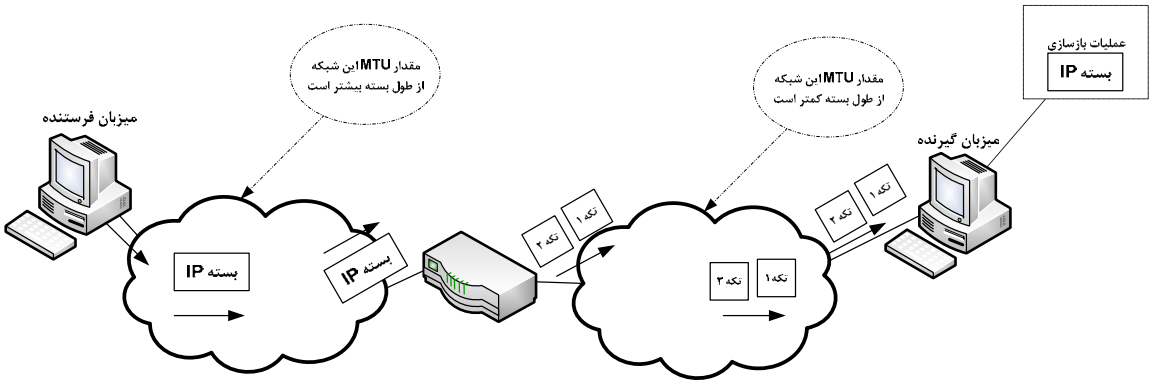
نوع شبکه	اندازه MTU
اترنت	۱۵۰۰بایت
IEEE 802.3	۱۴۹۲ بایت

شبکه حلقوی IEEE 802.5	۴۴۴۰ بایت تا ۱۷۹۴۰ بایت (بستگی به سرعت ارسال در شبکه دارد)
FDDI	۴۳۵۲ بایت
IEEE 802.4	۸۱۶۶ بایت
SMDS	۹۱۸۰ بایت

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 کارامدی 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 ازاندازه 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، بیشترباشد 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 قادربه 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 درکامپیوتر میزبان درمقصد انجام می شود. هرگز مسیر یابهای میانی شبکه عملیات فوق را انجام نمی دهند.



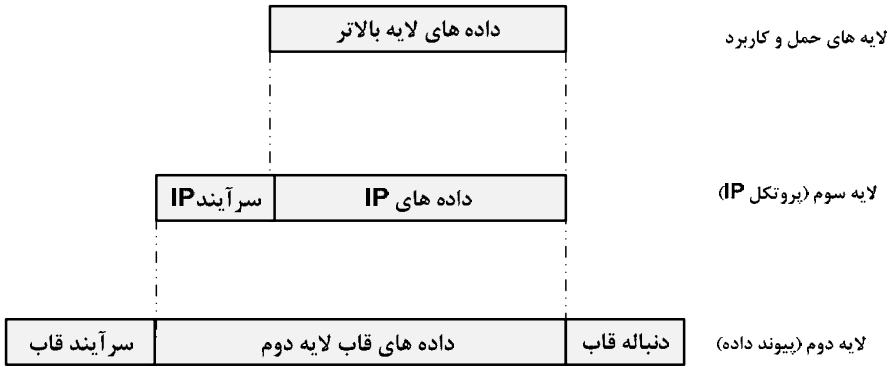
شکل(۸-۹): تکه سازی بسته IP

هنگامی که میزبان B نیاز به پاسخ به میزبان A داشته باشد دراین صورت اندازه بسته را طوری تنظیم می کند تا از اندازه MTU شبکه B تجاوز نکند. بسته هی ارسالی از میزبان C به میزبان A می تواند بدون هیچ تکه سازی تحویل داده شود. با این وجود، مسیریاب های میانی شبکه سعی نمی کنند که برای افزایش کارآیی انتقال، بسته های کوچکتر را با یکدیگر ترکیب نموده و یک بسته بزرگتر ایجاد نمایند. باید به این نکته توجه نمود که درشبکه های IP بسته های تکه شده فقط در مقصد سر هم می شوند.

۸-۳-۲- قالب بسته IP

همانطور که درشکل (۸-۱۰) نشان داده شده است، بسته های IP از دو قسمت تشکیل شده اند که عبارتند از: سرآیندIP 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 فیلد هایی برای کمک به تشخیص تکه ها، درون بسته اصلی باشد.
- اندازه بسته: ازآنجاییکه 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 فیلد های اختیاری برای مشخص کردن امکانات IP استفاده شده برای امنیت، مسیریابی مبدا و غیره باشد. این عامل اندازه طول سرآیند IP را متغیر می سازد. بنابراین اندازه واقعی بستهIP باید درسرآیند IP نشان داده شود.

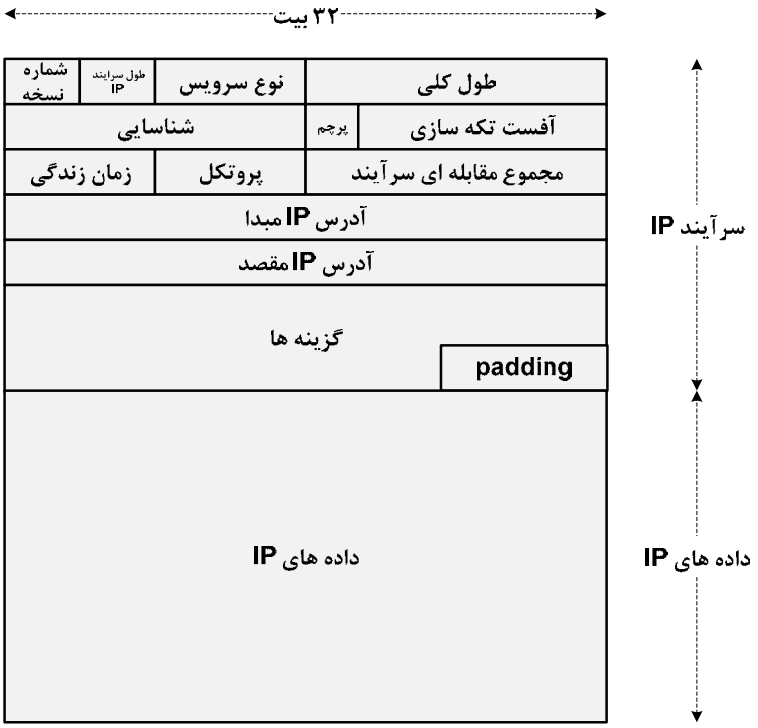


شکل(۸-۱۰): نحوه بسته سازی داده ها درمعماری TCP/IP

کمترین طول سرآیند IP ۲۰ بایت است. چون درسرآیندIP، فیلدی برای امکانات اضافی درنظر گرفته شده است، بنابراین طول سرآیند ممکن است بیشتراز۲۰ 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. همچنینRFC 1349 استفاده فیلد نوع سرویس را با جزئیات کامل در سرآیند IP توصیف می کند.

۸-۳-۲-۱- فیلد شماره نسخه

مطابق با شکل (۸-۱۱)، فیلد شماره نسخه درسرآیند بسته های IP دارای ۴ بیت طول می باشد و نشان دهنده شماره نسخه پروتکل IP است. این امرتوانایی 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 مقدارفیلد 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 افزارIP 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): مقادیرمختلف شماره نسخه IP

شماره نسخه	توصیف
۰ و ۱۵	رزرو
۱-۳ و ۱۰-۱۴	انتصاب داده نشده است
۴	پروتکل فعلی اینترنت (IPV4)

۵	پروتکل آزمایشی Stream IP
۶	پروتکل آتی اینترنت (IPV6)
۷	پروتکل اینترنت TP/IX
۸	پروتکل اینترنت P
۹	پروتکل TUBA

پروتکل Stream IP، یک پروتکل آزمایشی است که برای تضمین سرویس انتها به انتها دراینترنت استفاده می شود. این پروتکل در RFC 1819 توصیف شده است .پروتکلTP/IX ، پروتکل 'P" و TUBAهمه 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. پروتکلSIP از آدرس دهی ۶۴ بیتی استفاده می کند و نحوه گذر بین IPV4 و آدرس دهی طولانی تر را توصیف می کند. پروتکلSIP درRFC 1710 توصیف شده است. پروتکل TP/IX، یک پروتکل قدیمی بوده که پایه معماری مشترک برای اینترنت گردید. پروتکل TUBA در RFC 1347 ، RFC1526 ، RFC 1561 توصیف شده است

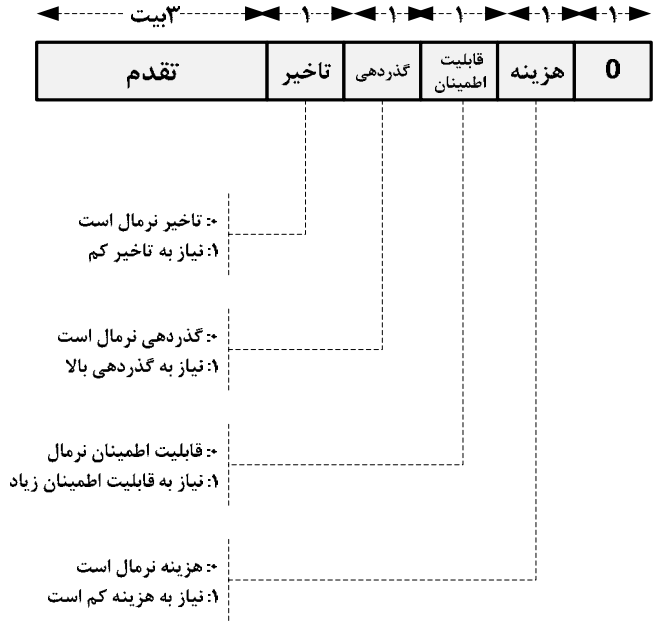
۸-۳-۲-۲- فیلد طول سرآیند اینترنت (IHL)

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. دراین حالت امکانات اضافی دربسته IP وجود ندارد. حداکثرطول سرآیندبسته های IP با درنظر 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[1](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.

[1] Type of Service



شکل(۸-۱۲): ساختار فیلد نوع سرویس برای بسته های IP

۳ بیت اول، مقدارترتیب تقدم همراه با بسته IP را نشان می دهد. فیلد ترتیب تقدم ۳ بیت طول دارد وکدینگ آن در جدول (۸-۵) نشان داده شده است.

جدول(۸-۵): مقادیرزیرفیلد ترتیب تقدم درفیلد نوع سرویس

مقدارتقدم	توصیف
۰۰۰	تقدم عادی
۰۰۱	تقدم دارای اولویت
۰۱۰	تقدم فوری
۰۱۱	تقدم آنی
۱۰۰	تقدم برتر از آنی
۱۰۱	تقدم بحرانی
۱۱۰	تقدم کنترل بین شبکه ای
۱۱۱	تقدم کنترل شبکه

از۴ بیت بعدی که به دنبال فیلدترتیب تقدم درساختار فیلد نوع سرویس می آیند، برای نشان دادن نوع سرویس درخواستی استفاده می شود. این کدها همان طور که در جدول (۸-۶) نشان داده شده اند به صورت زیر تفسیر شده اند.

جدول(۸-۶): کدهای نوع سرویس

کد	توصیف
۱۰۰۰	نیاز به تاخیر کم
۰۱۰۰	نیاز به حداکثر گذردهی
۰۰۱۰	نیاز به حداکثر قابلیت اطمینان

۰۰۰۱	نیاز به کمترین هزینه
۰۰۰۰	سرویس معمولی

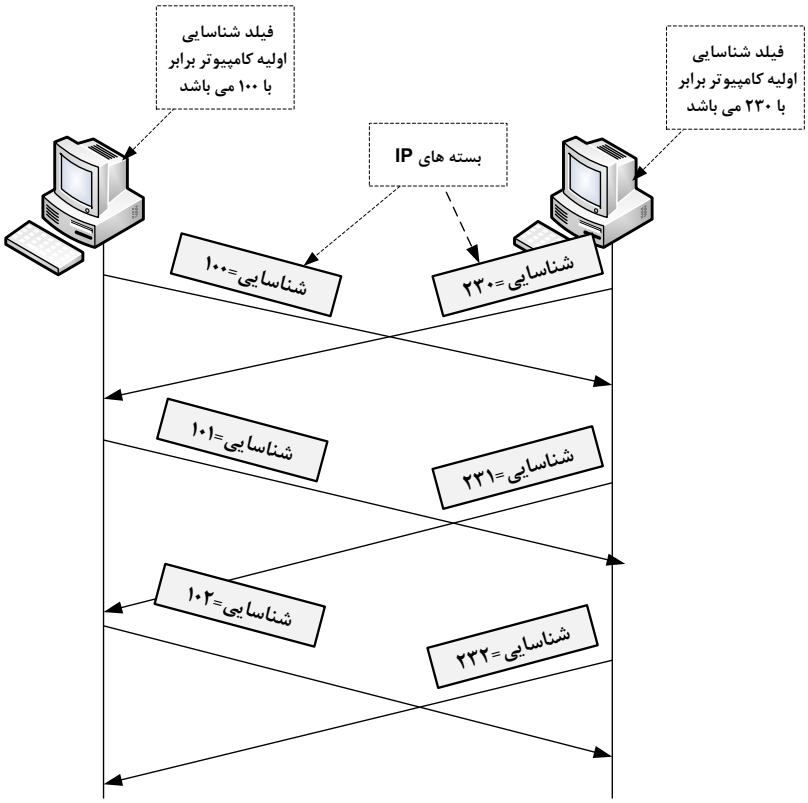
آخرین بیت فیلد نوع سرویس همواره برابر با ۰ می باشد و برای استفاده در آینده رزرو شده است.

۸-۳-۲-۴- فیلد طول کلی

فیلد طول کلی نشان دهنده طول بسته IP شامل سرآیند IP وداده بر حسب بایت می باشد. این فیلد ۱۶ بیت طول دارد و بسته را به حداکثر اندازه ۶۵۵۳۵ بایت محدود می کند. ازآنجائیکه معمولا 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 عبورمی باشند. همچنین چنانچه بسته های IP به بزرگی ۶۵۵۳۵ بایت باشند دراین صورت طراحی با فرهای ارسال درفرستنده وهمچنین بافرهای مسیریاب های میانی کارآمد نیست. معمولاً اندازه بسته برای اغلب شبکه ها و میزبانها بندرت از KB ۱۶ تجاوز میکند. همه نود های IP باید توانایی دریافت بسته هایی را با طول حداقل ۵۷۶ بایت داشته باشند. همانطور که قبلا 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، درابتدای اتصال از یک مقدار اولیه به عنوان شماره بسته استفاده می کنند. همانطور که درشکل (۸-۱۳) نشان داده شده است، با ارسال هر بسته جدید، یکی به مقدار این فید 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.



شکل (۸-۱۳): مثالی از کاربرد فیلد شناسایی

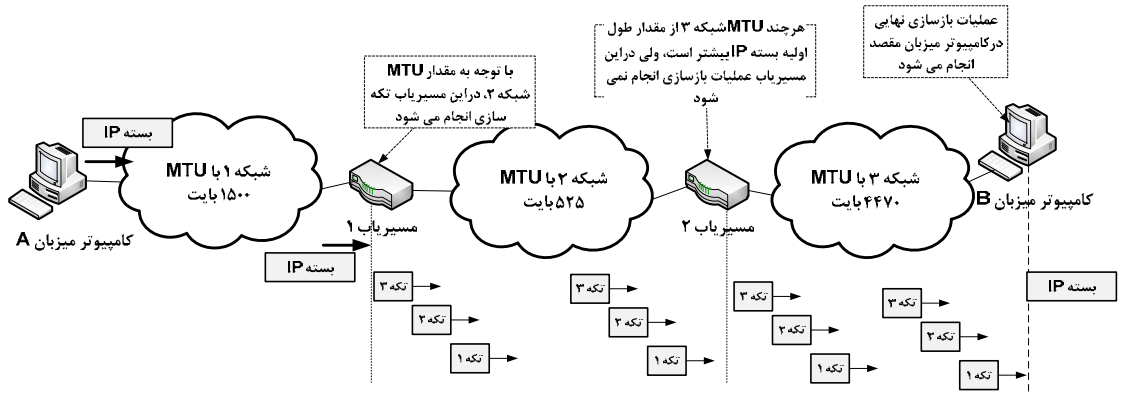
فیلد شناسایی۱۶ بیت طول دارد که این امر اجازه می دهد تا بسته ها از ۰ تا ۶۵۵۳۵ شماره گذاری شوند. فیلد شناسایی دراصل برای شناسایی تکه های بسته IP که متعلق به یک بسته IP اصلی خاص هستند، استفاده می شود. باید توجه نمود که درهنگام تکه سازی یک بسته IP به تکه های کوچکتر، مقدار این فیلد درتمام تکه های IP تغییرنکرده 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 با۱ 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 بستهIP درنودهای میانی جلوگیری شود. به عنوان مثال برنامه boot strap که در Rom کامپیوتراجرا 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 با۱باشد، گیرنده متوجه خواهد شد که تمام تکه های بسته اصلی هنوز نیامده اند وتکه 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.

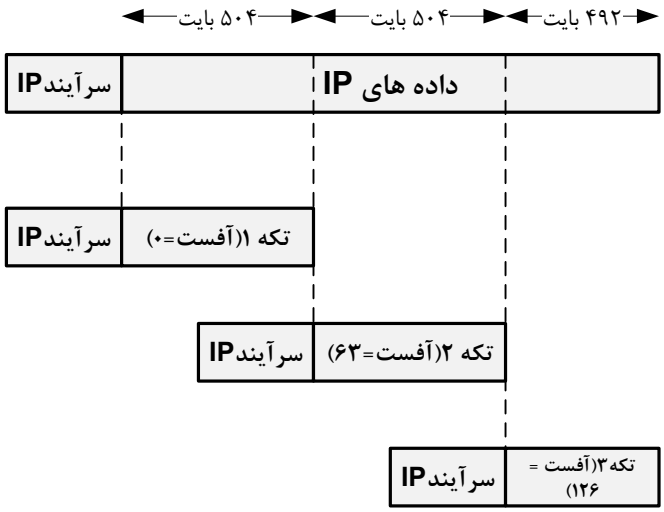
درادامه با ذکر یک مثال نحوه تکه سازی در پروتکل IP را توضیح می دهیم. شبکه نشان داده شده درشکل (۸-۱۴) را در نظر بگیرید که درآن یک میزبانA در شبکه۱ بسته های IP را به میزبانB در شبکه ۳ می فرستد. مقدار MTU درشبکه های۱و۲و۳ به ترتیب ۱۵۰۰ ، ۵۲۵ ، ۴۴۷۰ بایت است. مسیریاب ۱ شبکه های۱ و ۲ را به هم پیوند می دهد و 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 مسیریاب ۱ با این بسته مواجه می شود، قبل از این که بسته را به شبکه ۲ارسال نماید، باید آن راتکه سازی کند. دلیل این امرآن است که اندازهMTU شبکه ۲کوچکتر از اندازه بسته می باشد. اندازه تکه هاطوری انتخاب می شوند که بسته های تکه شده داخل MTU شبکه۲ که ۵۲۵ بایت است جا شوند.



[1] Don't Fragment
[2] More Fragment

شکل(۸-۱۴): مثالی ازنحوه تکه سازی درIP

فیلد افست تکه سازی ،مکان داده مربوط به آغاز بسته اصلی را نشان می دهد. این فیلد ۱۳ بیت طول دارد. با بررسی قالب سرآیندIP ، به این نتیجه می توان رسید که تنها ۱۳ بیت فضا برای این فیلد درنظر گرفته شده است. ازآنجاییکه 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 ضریبی از۸ بایت است وهمواره 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 سر آیند IP که ۲۰ بایت است، ۵۰۵ بایت برای اندازه تکه حاصل می شود. ازآنجائیکه 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 IP اصلی است. این امر مشخص می کند که تکه IP به یک بسته IP اصلی خاص تعلق دارد. مقادیر تنظیمات پرچم و افست تکه سازی بسته هایIP تکه سازی شده درجدول (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

برای این که گیرنده قادر به بازسای 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 کندکه 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 برابربا۱ 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، هرتکه در مسیر های جداگانه احتمالی به سمت مقصدحرکت 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. درصورت از بین رفتن یک بسته، پروتکل های لایه بالا مانند TCP متوجه شده و درخواست ارسال مجدد بسته گم شده ازمقصد را می نمایند. گیرنده بسته هایIP 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 سایرتکه 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 درپی 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، ازآنجاییکه 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- فیلدزمان زندگی(TTL[1])

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. درهر 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 فیلدTTL دریک 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 ازیک 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

درمسیریاب IP می باشد. چون پردازش فوق زمان بر می باشد، بنابراین بسیاری از مسیریاب ها برای سادگی مقدار TTL را از ۱کم می کنند. به خاطر این امر فیلد TTL نشان دهنده حداکثر تعداد پرش های مجاز یک بسته درشبکه 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 نشاند دهنده فاصله بی نهایت می باشد. سایر نکات مهم برای فیلد TTL به صورت زیر است:

- یک میزبان نباید یک بستهIP را با مقدارفیلد 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 قطرشبکه باشد. منظور از قطر شبکه، طولانی ترین مسیر ممکن از مبدابه مقصد است. البته دراکثر موارد مقدار منطقی TTL برابر با دوبرابر قطر فوق تنظیم می شود.
- لایه IP باید ابزاری را برای لایه حمل فراهم کند تا بتوان فیلد TTL هر بسته ارسالی راتنظیم نمود. هنگامی که از یک مقدار TTL ثابت استفاده می شود، مقدارفوق باید قابل پیکره بندی باشد. متاسفانه خیلی از پیاده سازی ها، قادر به تعیین مقدار اولیه TTLنبوده واز 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 رادریافت کند، استفاده می شود. به عبارت دیگر از این فیلد برای تسهیم سازی و غیرتسهیم سازی داده به پروتکل های لایه بالا استفاده می شود. به عنوان مثال مقدار فیلد پروتکل برای پروتکل TCP برابر با۶ است. این مقدار برایUDP برابر با ۱۷ و برای ICMP برابر با۱ است. هنگامیکه پروتکلIP درسمت گیرنده متوجه شد که مقدار فیلد فوق دربسته دریافتی برابربا۶ است، می فهمد که داده های موجود دربسته 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 ماژولICMP تحویل داده شود .

۸-۳-۲-۹- فیلد مجموع مقابله ای سرآیند[1]

این فیلد فقط برای بررسی خطای احتمالی در سرآیند IP استفاده می شود. مکمل۱تمام مقادیر۱۶ بیتی موجود درسرآیند IP با هم جمع می شود (بجز خود فیلد مجموع مقابله ای سرآیند)، سپس مکمل ۱مجموع حساب می شود. مقدار حاصل جمع فوق، برابر با مقدار مجموع مقابله ای سرایند بوده و درفیلد مناسب قرار می گیرد. از آنجاییکه فیلد TTL در هر مسیر یاب کاهش می یابد وباعث تغییرات درسرآیند IP می شود، بنابراین مقدار سرآیند درهر مسیریاب تغییر کرده و این باعث می شود که مقدار مجموع مقابله ای در هر مسیریاب دوباره حساب شود. شواهد نشان می دهد که این مکانیزم درتشخیص خطاهای انتقال بسته مناسب است.

۸-۳-۲-۱۰- آدرس های IP مبدا و مقصد

[1] Cheak sum

آدرسIP مبدا وآدرسIP مقصد، آدرس های IP ۳۲ بیتی نودهای مبدا و مقصد هستند. از آنجاییکه شبکه های IP از نوع بدون اتصال می باشند، هربسته به صورت مستقل پردازش و مسیریابی شده و بنابراین نیاز است که درهربسته 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

ازفیلد گزینه برای فراهم سازی برخی امکانات اضافی درپروتکل 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 درانتهای گزینه قرار دارد. چنانچه طول فیلد گزینه مضربی از ۴ بایت نبود، به مقدار کافی درناحیه padding بیت صفر اضافه می شود تا فیلد گزینه مضربی از ۳۲ بیت باشد. درصورتیکه فیلد گزینه مضربی از ۳۲ بیت باشد، نیازی به فیلد padding وجود ندارد. درادامه به بررسی گزینه های مهم IP می پردازیم.

۸-۳-۳- گزینه های IP[1]

پروتکل IP دارای یکسری امکانات اضافی برای انجام برخی عملیات اختیاری می باشد. ازآنجاییکه این امکانات اختیاری بوده و الزامی دراستفاده آنها نمی باشد، با عنوان گزینه های IP شناخته می شوند. گزینه های IP به شرح زیر است :

- امنیت
- ثبت مسیر
- مسیریابی مبدا دقیق[2]
- مسیریابی مبدا ضعیف[3]
- 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. درصورت لزوم، می توان از مقادیر پرکننده صفر برای رساندن طول گزینه به مضرب 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 درگزینه است که از آن برای تعیین نوع گزینه استفاده می شود. فیلد نوع گزینه شامل سه فیلد زیر می شود:

- پرچم کپی شده (۱بیت)
- کلاس گزینه (۲ بیت)
- شماره گزینه (۵ بیت)

---

[1] IP Options
[2] Strict Source Routing
[3] Loose Source Routing

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، بیانگز آن اشت 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. کد۰ به منظور کنترل شبکه وکد۲ برای اشکال زدایی واندازه گیری به کار می رود. کد۱و۳ 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 وبه 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 بایت رااشغال نموده وبایت 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 بایت 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 مسیرتهیه 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	درپروتکل 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 مسیرتعیین 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 :

۸-۳-۳-۱- انتهای لیست گزینه و گزینه های بدون عملکرد

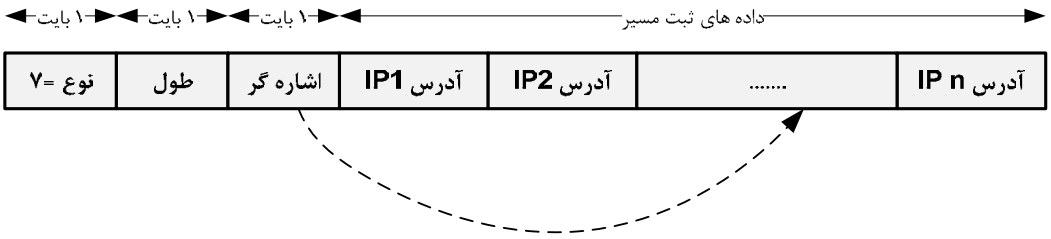
تنها گزینه های تک بایتی، گزینه های انتهای لیست گزینه و گزینه بدون عملکرد می باشند. انتهای لیست گزینه، یک گزینه تک بایتی حاوی بیتهای صفراست. این گزینه، انتهای لیست گزینه را نشان می دهد. این گزینه در انتهای لیست همه گزینه ها و نه درانتهای هر گزینه استفاده می شود. گزینه فوق، درصورتی که انتهای گزینه ها از 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 داردکه 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 وبرای ثبت آدرس IP مسیر یاب هایی که بسته IP را به مقصد پیش می برند، استفاده می شود. دراین گزینه، لیست مسیریاب هایی که بسته ازآنهاعبورکرده 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 درگزینه فوق، بایت اشاره گر می باشد. این فیلد اشاره کننده به محلی است که باید نود دریافت کننده این گزینه، آدرس IP خود را درآن 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 وجودندارد. به عبارت دیگرفیلد ثبت داده پر شده است. اگر لیست ثبت داده پر باشد، مسیریاب 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 ازطول گزینه نباشد، لیست ثبت داده پر نیست و محل های خالی دردسترس می باشد. مسیریاب، 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 مسیریابی است که از طریق آن باید این بسته پیش برده شود. هم فرستنده و هم گیرنده باید با استفاده و پردازش اطلاعات ثبت مسیرموافق باشند. فرستنده، گزینه ثبت مسیر و فضای کافی برای ثبت آدرس های IP مسیریاب های میانی را به بسته IP اضافه می کند. گیرنده با پردازش لیست آدرس

های IP ثبت شده در فیلد ثبت داده، اطلاعات مفیدی از مسیریاب های موجود درشبکه بدست می آورد. اگر گیرنده با پردازش داده های ثبت مسیر موافق نباشد، این اطلاعات توسط گیرنده نادیده گرفته می شود.

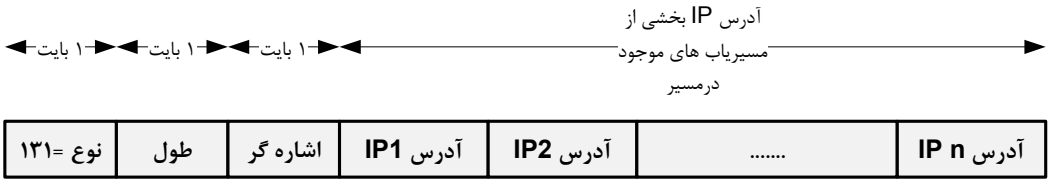
درشبکه های IP دونوع متفاوت از مسیریابی وجود دارد. مسیریابی پرش به پرش و مسیریابی مبداء. درمسیریابی پرش به پرش، درهر نود عملیات مسیریابی انجام شده و بهترین پرش بعدی برای تحویل بسته به مقصد تعیین می شود. سپس بسته برای رسیدن به مقصد نهایی، تحویل پرش بعدی می شود. این عملیات درهمه پرش های بعدی انجام می شود تانهایتا بسته به مقصد برسد. درمسیریابی 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 دیگردر مسیریابی مبدا ، فرستنده مسیری راکه بسته بایددر 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 بسیارمفید 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 دریک 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.

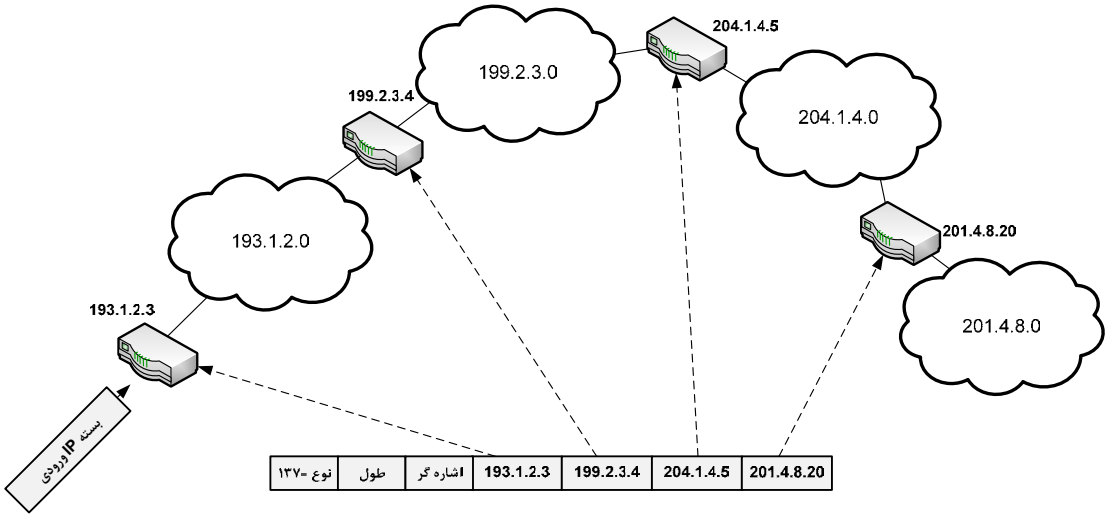
در گزینه مسیریابی مبدا دقیق که درشکل (۸-۱۷) نشان داده شده است، فرستنده رشته ای از آدرس های IP نودهایی را که باید دقیقا در پیش بردن بسته از آنها استفاده شود، را همراه بسته ارسال می نماید. مسیر بین دو آدرسIP متوالی موجود در لیست مسیریابی مبدا، فقط می تواندشامل یک شبکه فیزیکی خاص باشد و امکان وجود نودهای میانی بین آنها وجود ندارد. اگر مسیر یاب های میانی نتوانند مسیرتعیین شده توسط این گزینه را دقیقا دنبال کنند، بسته حذف می شود.

شکل(۸-۱۷): ساختارمسیریابی مبدا دقیق

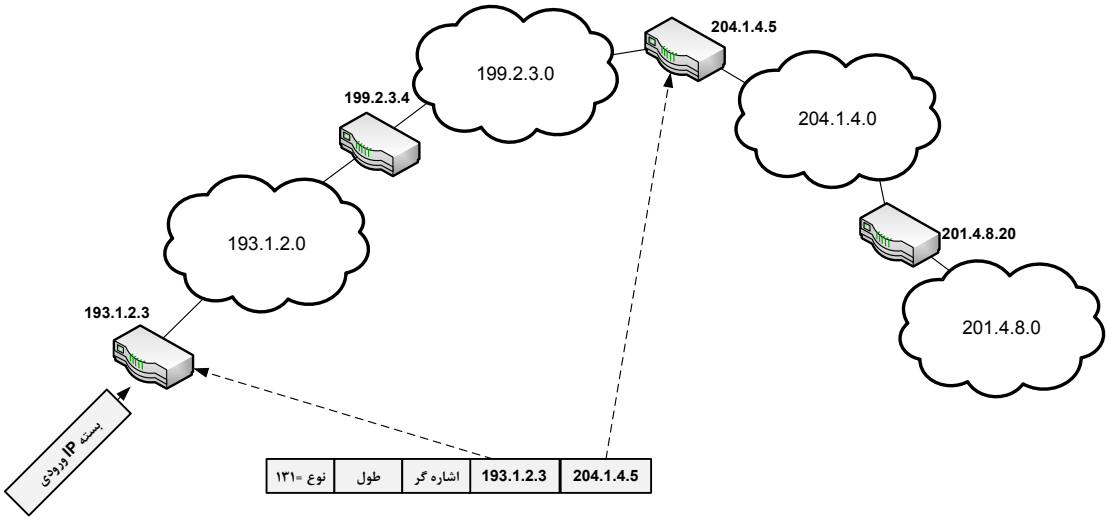
مطابق با شکل (۸-۱۸)، در مسیریابی مبدا ضعیف، فرستنده رشته ای از آدرس های IP نودهایی را که باید در پیش بردن یک بسته دنبال شوند، درپیام ارسالی اضافه می نماید. برخلاف مسیریابی مبدا دقیق، درمسیریابی مبدا ضعیف، ممکن است مسیر بین دو آدرس IP متوالی شامل هر تعداد مسیریاب باشد. شکل (۸-۱۹) مقایسه بین مسیریابی مبدا دقیق و ضعیف را نشان می دهد.



شکل (۸-۱۸): ساختار مسیریابی مبدا ضعیف



مثالی از مسیریابی دقیق

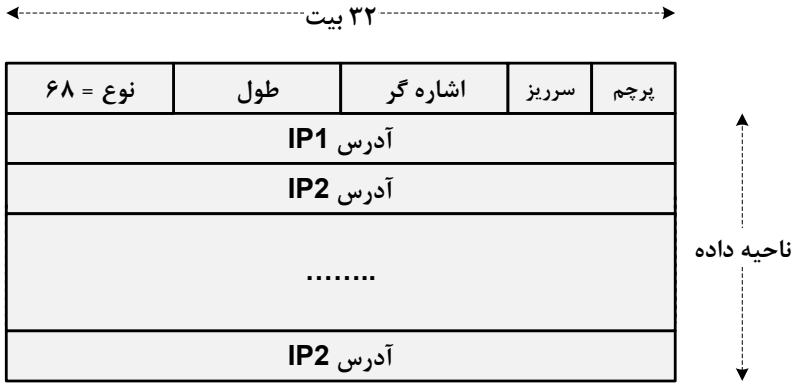


مثالی از مسیریابی ضعیف

شکل (۸-۱۹): مقایسه مسیریابی مبدا دقیق ومسیریابی مبدا ضعیف

۸-۳-۳-۴- برچسب زمانی اینترنت

از این گزینه برای ثبت زمان دریافت هر بسته IP درمسیریاب های درون شبکه استفاده می شود. چنانچه بخواهیم که زمان دریافت هربسته و همچنین آدرس مسیریاب هایی که بسته IP را دریافت می کنندرا 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 بر چسب زمانی اینترنت را نشان میدهد.



شکل (۸-۲۰): ساختارگزینه بر چسب زمانی اینترنت

درگزینه برچسب زمانی اینترنت، فیلد نوع گزینه ۶۸ است. فیلد طول گزینه، تعداد کل بایت های موجود درگزینه رانشان می دهد. هر ورودی در فیلد داده گزینه، شامل دو مقدار ۳۲ بیتی آدرسIP مسیریاب و بر چسب 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 سرریز۴ بیت طول دارد ونشان دهنده تعداد مسیریاب هایی است که به دلیل کوچکی زیاد فیلد داده، نمی توانند برچسب زمانی را درناحیه مربوطه قرار دهند. حداکثر مقدار فیلد سرریز ۱۵ است. اگر فضای کافی برای درج یک برچسب زمانی کامل در ناحیه داده وجود نداشته باشد ویا شماره سرریز از ۱۵ تجاوز کند، بسته IP اشتباه در نظر گرفته شده و حذف می شود. دراینصورت یک پیام ICMP از نوع خطا درپارامتر، به فرستنده ارسال می شود. فیلد پرچم، قالب اطلاعات در فیلد داده را کنترل می کند.

۸-۴- پروتکل ICMP[1]

همانطور که درقبل اشاره شد، پروتکل اینترت از نوع بدون اتصال و بدون گارانتی می باشد. بنابراین پروتکلIP سعی نمی کند تا تحویل مطمئن بسته ها را ضمانت کند بلکه این کاررا به پروتکل های لایه بالا مانند پروتکل TCP واگذار می نماید. بااین 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 1256, RFC792, RFC950, RFC 1812, RFC, 1122 و RFC 1191.

به دلیل بدون اتصال و بدون تضمین بودن پروتکل IP، احتمال اینکه بسته های IP با خطا مواجه شوند زیاداست.

درشبکه های IP، فرستنده بسته های IP را ارسال نموده وآنها را به زیرلایه های شبکه زیرین تحویل می دهد. فرستنده راهی برای دانستن مشکلات احتمالی که ممکن است در ارسال بسته رخ بدهد ندارد. معمولا خطاها و مشکلات احتمالی موجود دربسته های IP درمسیریاب های میانی کشف و گزارش می شود. برخی از مشکلاتی که ممکن است درهنگام ارسال بسته های IP با آنها مواجه شویم عبارتند از:

- اتمام پارامتر زمان زندگی (TTL) در بسته به خاطر وجود حلقه مسیریابی درشبکه.

[1] Internet Control Message Protocol

- 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 مسیریاب شبکه.

در هر یک از این موارد، ازپروتکل 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 کاررا 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 کاررا انجام می دهند. بنابراین درسطوح مختلفی از پیاده سازی پروتکل ICMP درنودهای شبکه وجود دارد.

هم مسیریاب های میانی شبکه و هم میزبان های IP قادر به تولید وارسال پیام های ICMP می باشند. مسیریاب های شبکه درهنگام مواجه با مشکلاتی که باعث عدم توانایی آنها درپیش بردن بسته های دریافتی شود، اقدام به ارسال پیام های ICMP می نمایند. درحالیکه میزبان های شبکه، چنانچه با مشکلاتی نظیرعدم 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 درشبکه 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 کاررفته 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 ۰است. 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.

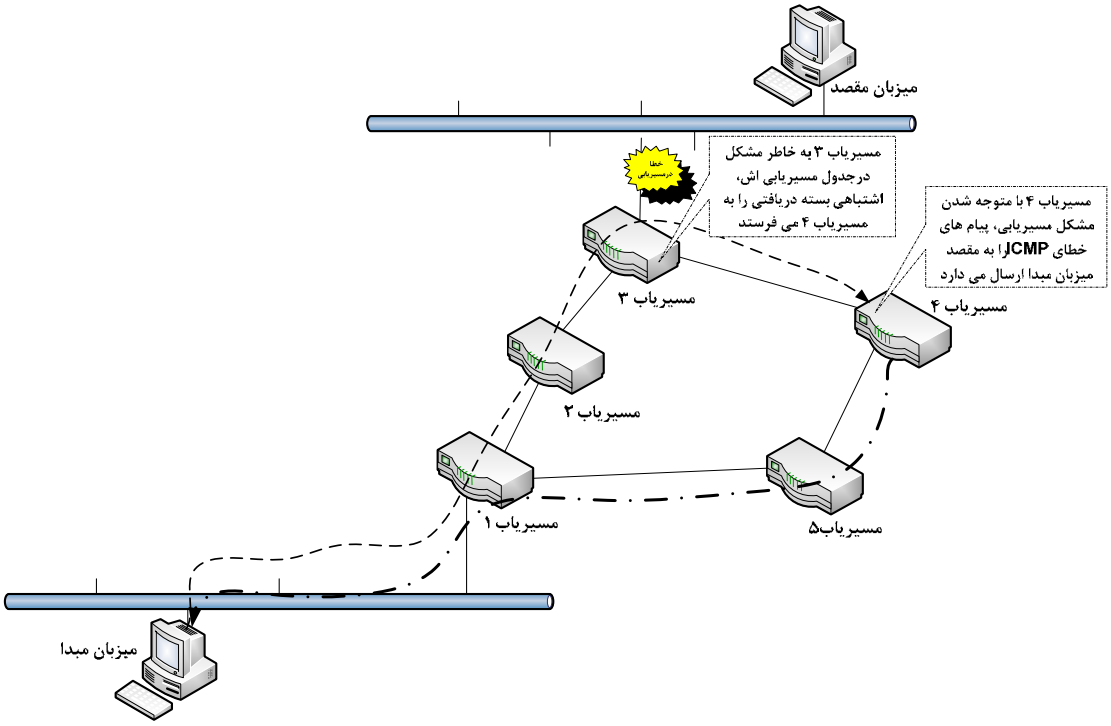
علاوه بر موارد فوق، پروتکلICMP نباید در مورد مشکلات ایجاد شده ذیل پیامی ارسال دارد:

- مسیریابی یا تحویل پیام های ICMP: اگر پیام های خطای ICMP در مورد پروتکلICMP 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 کندکه 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 پیونددادهه 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.

- بسته هایی با آدرس مبدائی 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 بستهIP 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 ازمیزبان مبدا به میزبان مقصد فرستاده شده است و مسیری شامل مسیریاب های ۱،۲ و۳ را طی می کند.

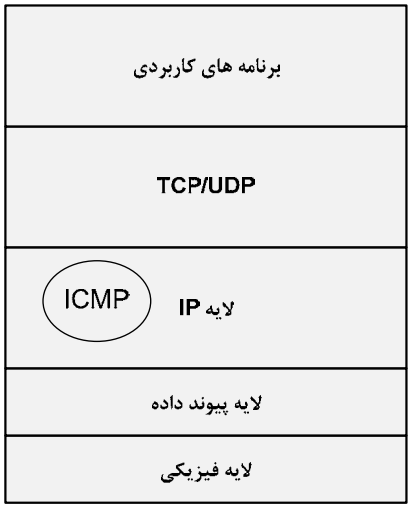


شکل (۸-۲۱): مثالی از کاربردپیام ICMP

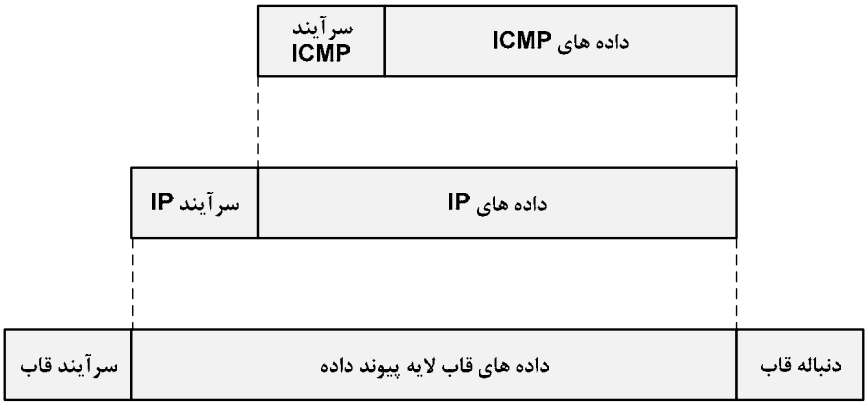
فرض کنید مسیریاب ۳ اطلاعات نادرستی درباره مقصد در جدول مسیریابی خود دارد و اشتباها به جای میزبان مقصد، بسته را به مسیر یاب ۴ ارسال می کند. مسیریاب ۴که متوجه وقوع خطا درشبکه شده است، یک پیام ICMP درباره مسیریابی نادرست به فرستنده پیام می فرستد. با توجه به اینکه پیام های ICMP فقط به مبدا تولید کننده بسته IP ارسال می شوند، بنابراین مسیریاب ۴ نمی تواند پیامی را به مسیریاب۳ درباره دلیل مشکل فوق ارسال دارد. دراین مثال، میزبان مبدا هیچ نقشی درخطای بوجود آمده نداشته است وبنابراین 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 هایIP فقط دو فیلد آدرس شامل آدرسIP 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 مبدااصلی ارسال می گردند. بنابراین درمثال فوق هنگامی که

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 دراین 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 درایجاد مشکل فوق نقشی نداشته است و دلیل مشکل اخیرنیست بلکه دلیل مشکل مبدأ یا یکی از مسیریاب های میانی است. بنابراین ارسال پیام ICMP به مبدا تنها انتخاب منطقی است. به هرحال ارسال پیام ICMP به مبدا از اصلا نفرستادن هیچ پیامی بهتر است.

ازآنجاییکه پیام های ICMP باید در اینترنت توسط مسیریاب ها حمل شوند، باید این پیام ها راتوسط پروتکلIP 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 وآن 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

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 نیازپروتکل 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 ازپروتکل 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 دوردردسترس 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 ویا به خاطر ازدحام درمسیریاب های میانی حذف شوند. اگردرپردازش 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:

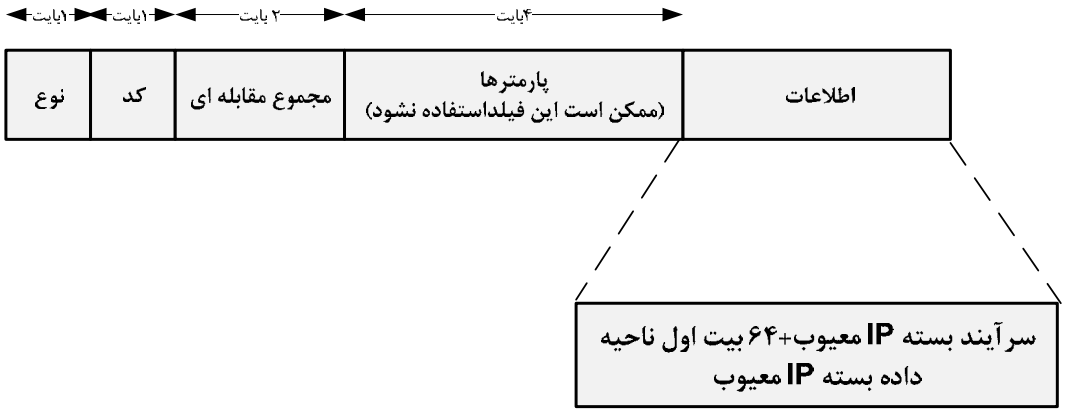
- echo : به عنوان یک تشخیص برای تعیین کردن دسترس پذیری به یک نود IP بکار می رود.
- غیرقابل دسترس بودن مقصد : برای اعلام غیر قابل دسترس بودن نود IP مقصد به کار می رود.
- فرو نشاندن مبدا[1] : برای نشان دادن مشکل ازدحام درشبکه و درخواست از مبدا برای کاهش سرعت ارسال به کار می رود.
- تغییرمسیر[2]: بوسیله مسیر یاب های میانی شبکه برای آگاهی دادن از وجود یک مسیر جایگزین استفاده می شود.
- تخطی زمانی[3]: برای اعلام صفرشدن مقدار فیلد TTL سرآیند IP به کار می رود.
- مشکل پارامتر[4] : برای نشان دادن یک مشکل دریکی از پارامترهای بسته IP به کار می رود.
- برچسب زمانی[5]: برای اندازه گیری زمان در اینترنت استفاده میشود .
- پوشش آدرس[6] : برای به دست آوردن اطلاعات پوشش زیر شبکه استفاده می شود.

۸-۴-۳- ساختار پیام های ICMP

ساختار پیام های ICMP درشکل (۸-۲۴) نشان داده شده اند. اولین بایت در سرآیند ICMP فیلد نوع می باشدکه 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



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

مقدارفیلد نوع	توصیف
۰	پاسخ Echo
۱،۲،۷و۳۷-۲۵۵	انتساب داده نشده است
۲	انتساب داده نشده
۳	مقصد غیر قابل دسترس است
۴	فرو نشاندن 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 مسیرمیزبان قابل حمل
۳۳	IPV6 Where- Are- You

۳۴	IPV6 I- Am – Here
۳۵	درخواست ثبت قابل حمل
۳۶	پاسخ ثبت قابل حمل

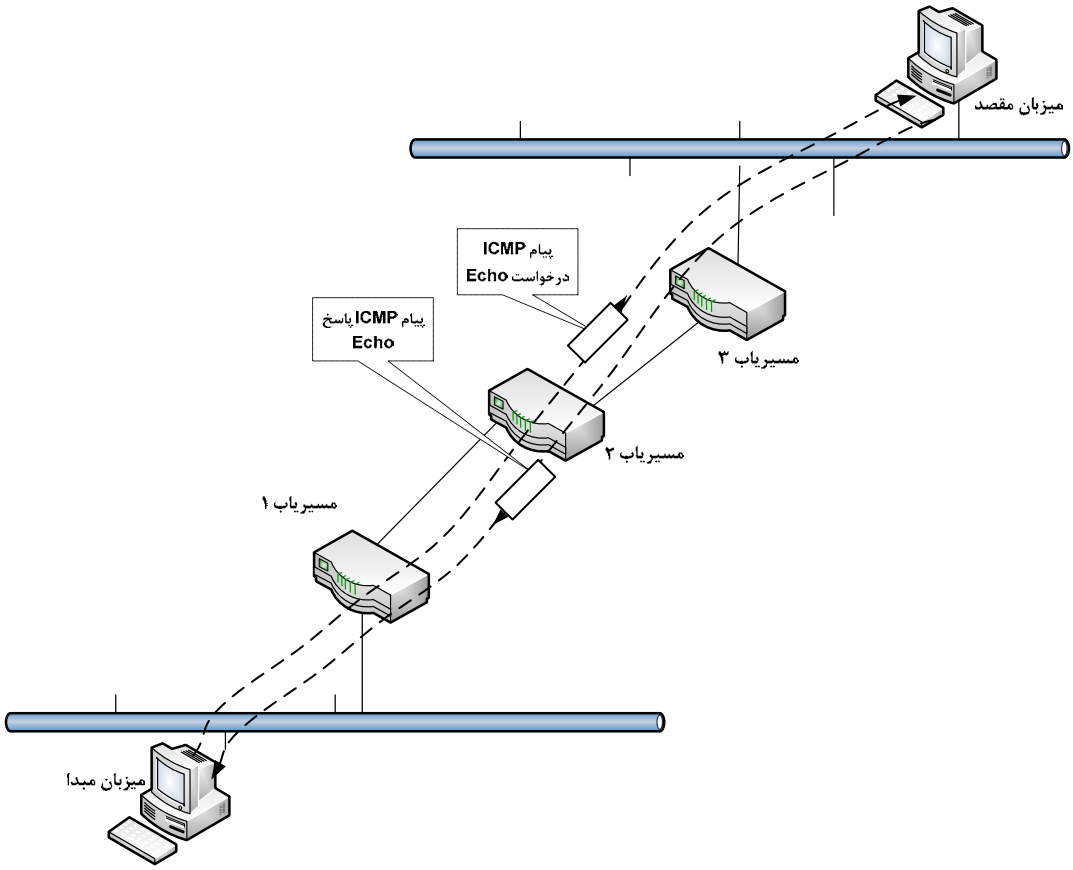
جدول (۸-۱۰): فیلدهای کد ICMP

نوع	کدها	توصیف
۰(پاسخ echo)	-	کد ندارد
۲۵۵-۱،۲،۷،۳۷	-	انتساب داده نشده است
۳ (غیرقابل 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
	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
۴ (فرو نشاندن مبدا)	-	کد ندارد
۵ (تغییر مسیر)	۰	تغییر مسیر بسته به خاطر شبکه (یا زیر شبکه)
	۱	تغییرمسیر 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 اطلاعا ت)	-	کد ندارد
۱۶(پاسخ اطلاعات)	-	کد ندارد
۱۷(درخواست پوشش آدرس)	-	کد ندارد
۱۸(پاسخ پوشش آدرس)	-	کد ندارد

دو بایت بعدی فیلد مجموع مقابله است که برای بررسی خطا دربسته ICMP به کار می رود. فیلد بررسی خطای فوق فقط شامل پیام ICMP بوده و سرآیند بستهIP را دربرنمی گیرد. الگوریتم بررسی خطا همان الگوریتم بررسی خطا یی است که برای پروتکل IP استفاده می شود. ۴ بایت بعدی شامل پارامتر های 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 برنداشته 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 درپیام های ICMP این است که بتوان آدرسIP مقصد ومبدا 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 درفصل 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. درادامه به توصیف برخی از مهمترین پیام های ICMP می پردازیم.

۸-۴-۳-۱- پیام ICMP Echo

یکی از پراستفاده 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. درپیام 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 ترآن در سیستم انتقال بین مبدا و مقصد درست کار می کنند. اگر بین مبدا و مقصد هر تعداد مسیریاب میانی وجود داشته باشد، با دریافت پیام پاسخ Echo مشخص می شود که مسیریاب های فوق قادر به مسیریابی بین مبدا و مقصد هستند. نود IP ای با کمک امکان PING دردسترس بودن آن بررسی می شود، یک میزبان یا یک مسیریاب می باشد. شکل (۸-۲۵) مثالی از چگونگی عملکرد PING را نشان می دهد.



شکل(۸-۲۵): استفاده از پیام های درخواست / پاسخ ICMP Echo

۸-۴-۳-۲-پیام ICMP در دسترس نبودن مقصد

همانطور که قبلا 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، معمولا به وسیله مسیریاب های شبکه شناسایی می شود. هنگامی که یک مسیریاب قادر به تحویل بسته به مقصد نباشد، یک پیام ICMP دردسترس نبودن مقصد را به فرستنده ارسال می دارد. پیام ICMP ارسالی فوق، فرستنده را از دلیل تحویل ناموفق آگاه کند. دراین پیام، مقدار فیلد نوع ۳ است که نشان می دهد این یک پیام ICMP ازنوع 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. درادامه به بررسی مفهوم هریک از مقادیر فیلد کد آورده شده درجدول فوق می پردازیم.

هنگامی که شبکه مشخص شده در آدرس مقصد IP قابل دسترس نباشد، مقدار کد۰ (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 راکه این خطا را تولید کرده است مشخص می کند.

مقدار کد ۱ (میزبان در دسترس نیست) به وسیله مسیریابی تولید می شود که مستقیما 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 پروتکلARP انجام شده توسط مسیریاب برای پیدا کردن آدرس سخت افزاری مقصد موفقیت آمیز نبوده است. همچنین این احتمال وجود دارد که میزبان مقصد به

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. درمواردی 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 ویک 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 وآدرس 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 ازیک پیام ICMP با نوع ۳ و با کد ۰ (در دسترس نبودن شبکه) استفاده می نماید.

درصورتیکه مسیریاب میانی شبکه با کمک لایه پیوند خود متوجه عدم وجود میزبان مقصد شود، از پیام ICMP با مقدارکد ۷ (میزبان مقصد ناشناخته است) استفاده می نماید. به عنوان مثال چنانچه لایه پیوند مسیریاب ازطریق 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 بامقدار کد ۸(میزبان مبدا جدا شده است) استفاده می نماید. البته RFC ۱۸۱۲ توصیه می کندکه مسیریاب های شبکه از کد خطای فوق استفاده ننمایند و در عوض ازیکی 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.

مدیرشبکه می تواند به دلایل مختلف از ارسال بسته ها توسط مسیریاب های شبکه و ازطریق 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 ازطریق مسیرخاصی پردازش شود. دراین حالت از بسته های ICMP نوع ۳ و کد ۹ و ۱۰ (ارتباط با شبکه/ میزبان مقصداز طرف مدیریت ممنوع شده است)،

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 مسیریاب های میانی شبکه قادر به تامین نوع سرویس درخواست شده درفیلد نوع سرویس موجود درسرآیند IP بسته ها باشد، نمی تواند بسته را به شبکه یا میزبان مقصد پیش ببرد. دراین حالت یک بسته ICMP با نوع۳ وکد های۱۱،۱۲ (شبکه/ میزبان مقصد برای نوع سرویس دردسترس نیست) ارسال می شود. کد۱۱ نشان دهنده این است که شبکه مقصد برای مقدارکیفیت سرویس درخواستی در دسترس نیست درحالیکه کد ۱۲ نشان می دهد که میزبان مقصد برای کیفیت سرویس درخواستی دردسترس 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 خاطردلایل امنیتی انجام شده و اولین خط دفاع در برابر کاربران متخاصم است. دراین 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 میزبان)، توسط مسیریاب اولین پرش به میزبان فرستنده ارسال می شوند. مسیریاب اولین پرش، اولین مسیریابی است که بسته برای رسیدن به مقصد خود باید از آن عبور کند. این پیام ICMP نشان دهنده این 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 مسیریاب های میانی شبکه تولید میشود. مدیر شبکه این امکان را دارد که درجدول مسیریابی نودهای میانی شبکه، حداقل تقدم مورد نیاز برای عبوربسته ها از یک مسیرخاص را تعیین کند. اگر بسته ارسالی با مقدار تقدم پائین تر از آنچه درجدول مسیریابی مشخص شده است، ارسال گردد دراین صورت بسته ها قادر به عبور از این مسیر نبوده و ناگزیر باید حذف شوند. دراین حالت یک پیام ICMP با کد ۱۵(تقدم در اثر عمل نمی کند) به سمت مبدا ارسال می شود.

۸-۴-۳-۳-پیام ICMP فرونشاندن مبدا

ازآنجاییکه شبکه های IP بدون اتصال می باشند، درهنگام 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 مقصددر 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 کندوبدین ترتیب از فرستنده ها درخواست می کند که سرعت ارسال خود را کاهش دهند.
اگرقرارباشد برای هر بسته ای که مسیریاب به خاطر پر بودن بافر های حافظه خود آن را حذف می کند یک پیام فرو نشاندن مبدا ارسال شود، دراین 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، درپیاده سازی های پیشرفته پروتکل ICMP، پیام های فرو نشاندن مبدا، فقط به مبداء هایی ارسال می شودکه بیشترین بسته ها را تولید می کنند. همچنین دربرخی از پیاده سازی ها، مسیریاب ها به جای این که صبر کنند تا بعد ازپرشدن بافر،پیام ICMP فرونشاندن مبدا ICMP ارسال نمایند، هنگامی

که بافر در حال پر شدن است، ارسال پیام های فوق را شروع کرده تا بدینوسیله از سرریزشدن بافر های خود جلو گیری 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؟ متاسفانه هیچ پیام ICMP برای لغو یا معکوس کردن پیام فرو نشاندن 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، پروتکلTCP نسبت به زمانی که باید نرخ ارسال را افزایش دهد، آگاهی دارد. این قابلیت دربخش کنترل جریان TCP پیاده سازی شده است که درفصل های بعدی آن را توصیف خواهیم نمود.

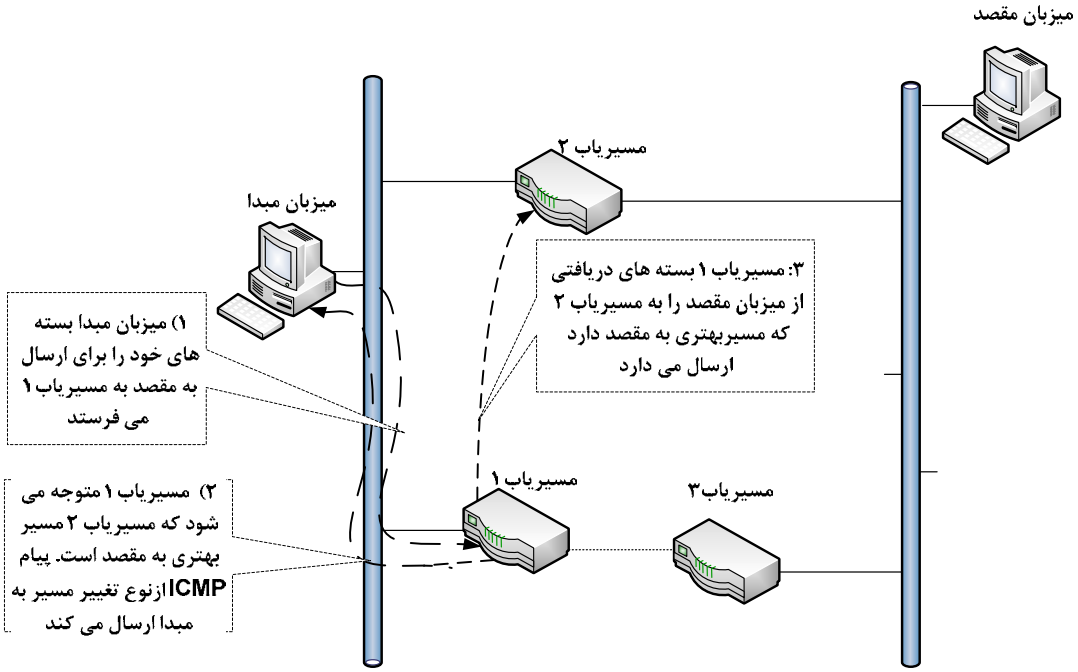
درساختار پیام های فرو نشاندن مبداء، مقدار فیلد نوع برابر با ۴ است. فیلدکد برابر با صفربوده و از فیلد۴ بایتی پارامتر استفاده نشده و همواره صفر است.

۸-۴-۳-۴-پیام ICMP تغییر مسیر

هنگامی که یک مسیریاب شبکه بسته ای را برای ارسال دریافت نماید ولی تشخیص دهد که مسیریاب دیگری مسیر بهینه تری برای ارسال بسته به سمت مقصد دارد، اقدام به ارسال پیام ICMP تغییر مسیر می نماید. مسیریاب ها اطلاعات مسیریابی را در شبکه با استفاده از پروتکلهای مسیریابی با یکدیگر رد و بدل می کنند. بنابراین مسیریاب های شبکه، همواره اطلاعات بهینه یا اطلاعات نزدیک به بهینه را درباره مسیرهای شبکه دارند. از طرف دیگراطلاعات مسیریابی میزبان ها بسیار کم بوده و قابل مقایسه با مسیریاب ها نمی باشد. معمولا یک میزبان شبکه آگاهی کمی نسبت به شبکه داشته و فقط مسیریاب های پرش بعدی خود را می شناسد. مسیریاب های پرش بعدی، مسیر یابهایی هستند که یک پرش از میزبان مبدا فاصله دارند. بنابراین میزبان مبدا و مسیریاب های پرش بعد مستقیما به یک شبکه متصل شده اند.

میزبان های شبکه معمولا دارای مسیریاب پیش فرض می باشندکه از آن برای پیش بردن بسته های ارسالی به مقصد هایی که صریحا در جدول مسیریابی میزبان لیست نشده است، استفاده می شود. جدول مسیریابی، در ناحیه داده پیکره بندی مانند یک فایل در میزبان نگه داشته می شود. با توجه به اینکه مسیریاب های شبکه مجهز به پروتکل های مسیریابی می باشند، درصورت وقوع تغییر درتوپولوژی شبکه، قادر به شناسایی مسیرهای جدید هستند. معمولا میزبان های شبکه در مبادلات پروتکل مسیریابی به طور مستقیم شرکت نمی کنند. در نتیجه میزبان ها از تغییرات توپولوژی آگاه نبوده و ممکن است جداول مسیریابی آنها شامل اطلاعات بهینه برای دستیابی به یک مقصد نباشد.

به عنوان مثال، شبکه نشان داده شده درشکل (۸-۲۶) را درنظر بگیرید. دراین شکل، مسیریاب جدید R2 به شبکه اضافه شده است. این مسیریاب جدید دارای یک مسیر بهینه تری برای دستیابی به میزبان مقصد B است. از آنجاییکه میزبان A هنوز متوجه اضافه شدن مسیریاب جدید R2 به شبکه نشده است، بنابراین برای پیش بردن بسته هایش به مقصد B همچنان از مسیریاب R1 استفاده می نماید. اگر مسیریاب R1 تشخیص دهدکه مسیریاب R2 مسیر بهینه تری به مقصد دارد ، یک پیام ICMP تغییر مسیر به فرستنده ارسال می کند. همچنین بسته را به مسیریاب بهینه تر یعنی R2 ارسال می دارد.



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 پیامICMP 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 با۵ است. همچنین مقادیر فیلد کد دراین پیام ها، قبلا در جدول (۸-۱۰) نشان داده شده بود. دربسته های ICMP تغییر مسیر، فیلدی برای نمایش آدرسIP مسیریاب بهینه درنظر گرفته شده است.

۸-۴-۳-۵-پیام هایICMP 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، دربازه های متناوب ۷ تا ۱۰ دقیقه توسط مسیریاب ها فرستاده می شوند. همچنین از این پیام ها می توان درپاسخ به پیامICMP 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 TTLموجود دربسته های IP به صفر رسید، مسیریاب 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 دریک حلقه مسیریابی قرارگرفت، هر بار که مسیریاب بسته را دریافت می نماید حداقل ۱ واحد فیلد TTL را کاهش می دهد. درنهایت 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 معمولا مجهز به یک زمان سنج بازسازی می باشندکه 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 مبداء ارسال می گردد.

مقدار فیلد نوع درساختارپیام 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 مسیریاب های میانی شبکه تولید شده است درحالیکه کد۱ نشان دهنده اتمام زمان سنج بازسازی بسته ها درمیزبان مقصد می باشد. پیام های ICMP تخطی زمانی توسط میزبان های شبکه تولید می شوند.

۸-۴-۳-۷-پیام ICMP مشکل پارامتر

چنانچه مسیریاب و یا میزبان شبکه متوجه مشکلی درپارامترهای سرآیندIP 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 دراین پیام، محل و نوع پارامتری که دارای مشکل است، درسرآیند IP مشخص می شود. مقدار فیلد کد برابر با ۰ ،۱ ویا ۲ می باشد. کد ۰ بیانگر این است که اشاره گر موجود درپیام ICMP مشکل پارامتر محل خطا را نشان می دهد. کد ۱ نشان دهنده نادرست بودن یکی از امکانات موجود درسرآیند IP است و نهایتا کد ۲ نشان دهنده این است که طول بسته IP نادرست است. بنابراین درصورتیکه پیام فوق با کد ۱ ارسال شود، ازفیلد اشاره گراستفاده ای نمی شود.

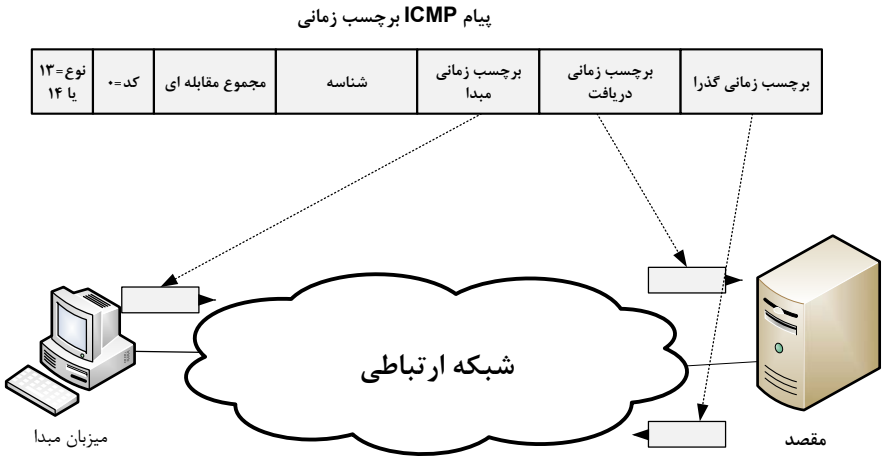
۸-۴-۳-۸-پیام ICMPدرخواست برچسب زمانی/پاسخ برچسب زمانی

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 NTP[1] نیز برای همزمان سازی ساعت نودهای شبکه نیز استفاده نمود، اما استفاده از پیام هایICMP درخواست برچسب زمانی/پاسخ برچسب زمانی به مراتب ساده تر است.

درساختار 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

ساعت جهانی اندازه گیری می شود. درساختار پیام های فوق، سه فیلد برای درج برچسب زمانی درنظر گرفته شده است که عبارتند از: برچسب زمانی مبداء، برچسب زمانی دریافت و برچسب زمانی گذرا. برچسب زمانی مبدا، توسط مبداء فرستنده پیام مقداردهی می شود. گیرنده ، به محض دریافت پیام فوق مقدار زمان جاری خود را درفیلد برچسب زمانی دریافت قرارمی دهد. بعد از پردازش بسته دریافتی، درپاسخ به آن، پیام پاسخ ارسال می شود. دراین حالت، گیرنده مقدار برچسب زمانی جاری را درفیلد برچسب زمانی گذرا قرار داده و ارسال می دارد. شکل (۸-۲۷) مثالی از نحوه مقدار دهی برچسب زمانی دراین پیام ها نشان داده شده است.



شکل (۸-۲۷): مثالی از نحوه پرنمودن فیلدهای برچسب زمانی

۸-۴-۳-۹-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 را ۱۶ است. فیلد کد همواره ۰ است.

۸-۴-۳-۱۰-پیام های ICMP درخواست پوشش آدرس/پاسخ پوشش آدرس

درفصل قبلی، مفهوم زیر شبکه سازی و آدرس های پوشش زیرشبکه توصیف شدند. میزبان های شبکه برای بدست آوردن پوشش زیر شبکه، از پیام ICMP درخواست پوشش آدرس استفاده می کنند. دراین پیام ها مقدار فیلد نوع برابر با ۱۷ می باشد. همچنین درپاسخ به پیام درخواست فوق، پیام ICMP پوشش آدرس با مقدار فیلد نوع برابر با ۱۸ ارسال می شود.
میزبان درخواست کننده آدرس پوشش زیرشبکه، درخواست خود را مستقیما به آدرس مسیریاب شبکه ارسال می دارد. درحالتیکه میزبان فوق، آدرس مسیریاب را نداند، درخواست را به صورت همه پخشی درشبکه 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.

۲. ساختار بسته های ARP را رسم نموده و کاربرد هرفیلد آن را بنویسید.
۳. محدودیت های پروتکل ARP را ذکر کنید.
۴. به چه علت پیام درخواست ARP به صورت همه پخشی ارسال می شود؟
۵. آیا پیام پاسخ ARP نیز به صورت همه پخشی 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 درشکه های پل بندی شده توضیح دهید.
۱۰. فرض کنید که دریک شبکه دو ایستگاه کاری وجود دارند که هر دو آدرس197.12.35.67 دارند. آدرس های MAC دو ایستگاه فوق به ترتیب A وB می باشد. این دو ایستگاه همزمان اقدام به برقراری همزمان یک جلسه Telnet با یک سرویسگر به آدرس IP 197.12.35.99 وآدرس سخت افزاری C می نمایند. به طور کامل توضیح دهید که دراین 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 سرویس دهنده های اصلی و ثانویه RARP چیست ؟ توصیف کنید چگونه یک سرویس 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 دهیدکه مشکل ناشی از گم شدن بسته ها درمعماری 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 کنیدکه نرم افزار IP موجود دریک مسیریاب 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 سرویس 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 کارمی روند، ذکر کنید.
۲۱. کاربرد فیلد TTL را دربسته های IP بنویسید؟
۲۲. مزایا و معایب بازسازی بسته های درمسیریاب 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 افست تکه سازی مشخص کنید .

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 مسیریاب 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 مبدادقیق را ذکر کنید.

۲۸. با ذکر یک مثال تفاوت مسیریابی مبداء ضعیف با مسیریابی مبداءدقیق 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 هستنداستفاده می شود یا خیر؟ جواب خود را توجیه کنید .

۳۵. درچه 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 ICMPباشد. 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 هرفیلد 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 بارسم 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 فرونشاندن 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 نشاندن 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 پیا مهای ICMP که برای کشف مسیریاب استفاده می شود بحث کنید. مزایای این روش بر سایر تکنیک ها چیست ؟

۴۹. درچه حالت هایی پیام ICMP تخطی اززمان فرستاده می شود ؟

۵۰. چه هنگامی پیام ICMP مشکل پارامتر ارسال می شود ؟

۵۱. کاربرد پیام های ICMP درخواست / پاسخ پوشش آدرس چیست ؟ سایر پروتکل های دیگر که می توانند برای این مقصود استفاده شوند چیست ؟