۱) لایهٔ واسط شبکه

در فصل اول آموختیم که مسائل مربوط به برقراری ارتباط فیزیکی بین دو ماشین در یک شبکهٔ کامپیوتری که مستقیماً از طریق یک محیط میانی[۱] به هم متصل شده‌اند ، در لایه اول از مدل TCP/IP مطرح می‌شود. این لایه موظف است تدابیری اتخاذ کند تا یک کانال دارای خطا ، به یک خط مطمئن و بدون خطا تبدیل شود. در راستای این وظیفه ، اطلاعاتی که قرار است روی خط ارسال شوند ، در قالب یک "فریم" سازماندهی شده و ابتدا و انتهای آنها با علامتهای ویژه نشانه‌گذاری[۲] می‌شود تا گیرندهٔ اطلاعات بتواند مرز فریمهای متوالی را تشخیص بدهد. همچنین به ابتدا و انتهای هر فریم ، اطلاعات لازم مثل آدرس گیرنده و فرستندهٔ فریم و کدهای کشف خطا اضافه می‌شود. در شبکه‌هائی که از کانال اشتراکی استفاده می‌کنند ، وظیفهٔ جلوگیری از تصادم سیگنال[۳] و مدیریت کانال ، بر عهدهٔ سخت‌افزار این لایه است.

در فصل قبل اشاره شد که از دیدگاه کانال انتقال ، دو دسته شبکهٔ "کانال فراگیر/ اشتراکی" و "کانال نقطه به نقطه" تعریف شده است. پروتکلهای مورد نیاز برای انتقال فریم روی کانالهای نقطه به نقطه ، تفاوت ذاتی با پروتکلهای کانال اشتراکی دارند ، زیرا کانالهای نقطه به نقطه مشکل مدیریت کانال و پدیدهٔ تصادم را نخواهند داشت. در این فصل آن دسته از پروتکلهای شناخته شده و جهانی ، که در لایهٔ "واسط شبکه" از مدل TCP/IP تعریف شده ، بررسی خواهد شد.

برای انعطاف بیشتر در شبکهٔ اینترنت ، که مجموعه‌ای از عناصر غیرهمگن و نامشابه را به هم پیوند زده ، این لایه بسیار باز و منعطف تعریف شده است ، یعنی الزام ویژه‌ای در بکارگیری سخت‌افزار ارتباطی خاص و پروتکل ارتباطی معین ، در این لایه وجود ندارد. ایستگاهی که تصمیم دارد به اینترنت متصل شود باید با بهره‌گیری از یک پروتکل ارتباطی معتبر و نرم‌افزار راه‌انداز مناسب ، به نحوی داده‌های خودش را به شبکه تزریق کند. بنابراین اصرار و اجبار خاصی در استفاده از یک استاندارد خاص در لایهٔ اول از مدل TCP/IP تعیین نشده است.

تقریباً در اکثر شبکه‌های محلی ، ماشینهای شبکه از یک کانال مشترک استفاده می‌کنند. ولی معمولاً دو شبکهٔ مجزا ، با استفاده از مسیریاب و خطوط نقطه به نقطه[۴]

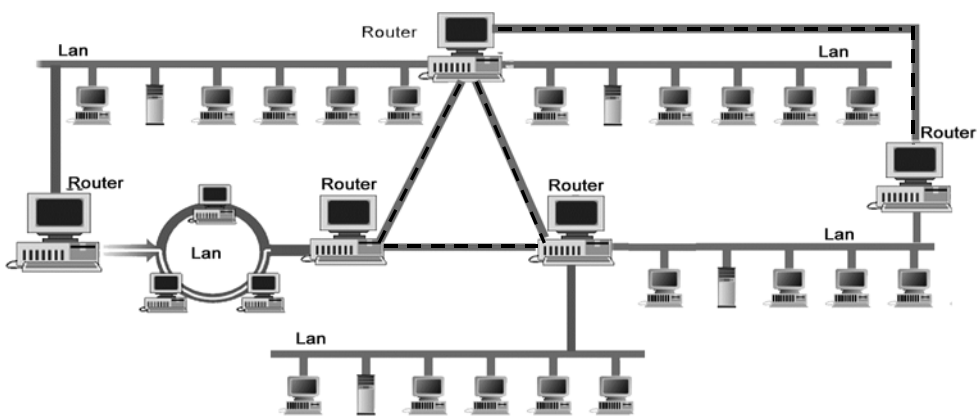
---

۱ Medium (Channel)
۲ Delimiter
۳ Collision
۴ Point to Point

به یکدیگر متصل می‌شوند. منظور از خطوط نقطه به نقطه خطوطی است که ارتباط دو ماشین روبرو را برقرار می‌کنند و هیچ ماشین ثالثی در این کانال سهیم نیست. این خطوط می‌توانند خطوط اجاره‌ای[1] ، خطوط تلفن معمولی ، کانالهای اختصاصی مایکروویو و یا کانالهای ماهواره‌ای باشند. از آنجایی که تمام ارتباطات زیر شبکه ، از طریق مسیریاب (یا مراکز سوئیچ سلول[2]) انجام می‌شود لذا هر یک از این مسیریابها یک (یا تعدادی) خط اختصاصی با دیگر مسیریابها (یا سوئیچها) دارند که به این خطوط اختصاصی در یک اصطلاح عام ، **"لینک"**[3] گفته می‌شود.

به شکل (۱-۲) نگاه کنید. در این شکل ، پنج شبکهٔ محلی متفاوت از طریق مسیریابها به هم متصل شده‌اند. خطوط بین مسیریابها که در این شکل به صورت نقطه‌چین نشان داده شده‌اند ، خطوط نقطه به نقطه و اختصاصی محسوب می‌شوند. بقیهٔ کانالها ، اشتراکی و فراگیر هستند.

یک بسته برای طی مسیر از مبدأ به مقصد ، باید از شبکه‌ها و کانالهای متفاوت عبور کند. با تغییر شبکه و کانال ، ساختار فریم توسط واسط شبکه تعویض می‌شود. چیزی که در طی مسیر و تغییرات مداوم فریم ، تغییر نخواهد کرد و ساختار آن از مبدأ تا مقصد ، استاندارد و بدون تغییر باقی خواهد ماند ، **"ساختمان داده‌ایست که درون فیلدِ داده از این فریمها قرار گرفته و بستهٔ IP نام دارد"**.



شکل (۱-۲) شمای یک شبکهٔ فرضی

---

[1] Leased line
[2] Cell Switchs
[3] Link

در ادامهٔ این فصل ابتدا مسئلهٔ خطا و چگونگی کشف آن را در داده‌ها مطرح می‌کنیم و سپس مشخصات کانالهای فیزیکی مختلف را که مرتبط با لایهٔ واسط شبکه هستند ، به اختصار یادآوری می‌نماییم. سپس به معرفی پروتکلها و استانداردهای تعریف شده در این لایه خواهیم پرداخت.

۱-۱) مختصری در مورد کانالهای انتقال

همانگونه که گفته شد وظیفهٔ سخت‌افزار مخابراتی در لایهٔ واسط شبکه آنست که بدون توجه به نوع و محتوای داده‌ها ، بیتهای داده را بر روی کانال فیزیکی منتقل کند. سخت‌افزار انتقال در این لایه ، بیشتر با مسائل مخابراتی و الکتریکی سروکار دارد. سه جز اصلی این سخت‌افزار ، عبارتند از:

- گیرنده
- فرستنده
- کانال فیزیکی[۱]

مباحث مربوط به گیرنده/فرستنده در محدودهٔ این کتاب نیست ، تنها به معرفی کانالهای ارتباطی که برای اتصال بین ماشینها استفاده می‌شود ، اکتفا می‌کنیم. این کانالها عبارتند از :

- **خطوط تلفن**
- **سیمهای به هم بافته شدهٔ زوجی** (در انواع مختلف مثل UTP[۲] که یک زوج سیم معمولی به هم بافته‌شده است و STP[۳] که زوج سیم معمولی به هم بافته‌شده به همراه یک پوشش آلومینیمی بر روی آنها جهت کاهش اثر نویزهای محیطی بر روی سیم می‌باشد.)
- **کابلهای هم‌محور (کواکسیال)** (در انواع مختلف مثل کابل کواکس ۵۰ اهم ضخیم[۴] ، کابل کواکس ۵۰ اهم نازک[۵] و کابل کوآکس ۷۵ اهم معمولی)
- فیبرهای نوری (در انواع مختلف مثل فیبر تک‌موده و چندموده[۶])
- **کانالهای ماهواره‌ای** : در باندهای فرکانسی مختلف مثل :

  باند **C** : ارسال از زمین به ماهواره در باند 5.925~6.425 GHz

  دریافت از ماهواره در باند 3.7~4.2 GHz

---

۱ Physical Channel
۲ Unshielded Twisted Pair
۳ Shielded Twisted Pair
۴ Tick Coaxial Cable
۵ Thin Coaxial Cable
۶ Mono mode / Multi mode Fiber Optic

باند **Ku** : ارسال از زمین به ماهواره در باند 14.0~14.5 GHz
دریافت از ماهواره در باند 11.7~12.2 GHz
باند **Ka** : ارسال از زمین به ماهواره در باند 27.5~30.5 GHz
دریافت از ماهواره در باند 17.7~21.7 GHz

- **کانالهای رادیویی** (شامل باندهای فرکانسی مختلف مثل UHF ، VHF)
- **امواج طیف نوری** شامل نور مادون قرمز (با استفاده از این امواج که خاصیت نور دارند می‌توان داده‌ها را به فاصلهٔ چند متر عبور داد. این امواج فقط از محیطهای شفاف عبور می‌کنند و بیشتر برای انتقال اطلاعات در فواصل بسیار کوتاه کاربرد دارد. مثلاً در کامپیوترهای کیفی برای ارتباط بی‌سیم با یک کامپیوتر دیگر مناسب است.)

تمام کانالها دارای مشخصه‌ای بنام پهنای باند هستند. در یک عبارت ساده و غیر دقیق ، پهنای باند هر کانال را می‌توان ، توانایی و ظرفیت آن در ارسال اطلاعات با نرخ B بیت در هر ثانیه ، تعریف کرد. بنابراین وقتی گفته می‌شود پهنای باند یک کانال یک مگابیت بر ثانیه (1Mbps) است یعنی با سرعت بالاتر از یک مگابیت بر ثانیه نمی‌توان اطلاعات را سالم به مقصد رساند. در این خصوص رابطهٔ معروفی بنام رابطهٔ شانون وجود دارد:

$$C=B.\log_2(1+S/N)$$

C : ظرفیت کانال بر حسب بیت بر ثانیه
S : متوسط توان سیگنال
N : متوسط توان نویز
B : پهنای باند کانال بر حسب هرتز

به عنوان مثال اگر پهنای باند کانالهای تلفن معمولی را حداکثر 4KHz فرض کنیم و نسبت توان سیگنال به توان نویز بطور تقریبی ۱۰۰۰ باشد ، در چنین حالتی با استفاده از خط تلفن حداکثر ۳۹۰۰۰ بیت در ثانیه را می‌توان انتقال داد و انتقال اطلاعات در بالاتر از این نرخ منجر به خرابی داده‌ها خواهد شد. انتقال یک فایل یک مگابایتی از طریق خط تلفن با این سرعت حدوداً ۲۱۰ ثانیه طول خواهد کشید. در جدول (۲-۲) مشخصات برخی از کانالهای انتقال با یکدیگر مقایسه شده است.

معیار خطا در کانالهای انتقال ، احتمال بروز یک بیت خطا روی کانال تعریف می‌شود؛ یعنی احتمال آنکه در فرستنده بیت ۱ ارسال و در گیرنده اشتباهاً بیت ۰ آشکارسازی بشود.

	پهنای باند	خطا	پیاده سازی	قیمت	توضیح
خطوط تلفن معمولی	کم (حدود 4KHz)	زیاد	ساده	ارزان	از قبل وجود دارد
زوج سیم	متوسط (حدود چند ده تا صد مگاهرتز)	متوسط	ساده	ارزان	برای فواصل کوتاه مناسب است.
کابلهای کواکس	حدود چند صد مگاهرتز	کم	متوسط	متوسط	
فیبرهای نوری	حدود چند گیگا هرتز	بسیار کم	پیچیده	متوسط	بهترین کارآیی
کانالهای ماهواره	حدود چند صد مگاهرتز	متوسط	بسیار پیچیده	گران	در همه جا تحت پوشش
کانالهای رادیویی	حدود چند مگاهرتز	زیاد	نسبتاً پیچیده	نسبتاً گران	در جایی که کابل‌کشی عقلایی نیست مناسب می‌باشد.

جدول (۲-۲) مقایسهٔ مشخصاتِ برخی از کانالهای انتقال

با توجه به آنکه پهنای باند بعضی از کانالها بسیار زیاد است (مثل کانالهای ماهواره‌ای) می‌توان یک کانال فیزیکی را بین چندین ایستگاه تقسیم کرد. این تقسیم باعث می‌شود که از یک کانال مشترک چندین ایستگاه استفاده کنند و هزینه‌های ارتباط کاهش یابد. به عمل تقسیم پهنای باند یک کانال بین چند ایستگاه عمل مالتی‌پلکس یا تسهیم گفته می‌شود. تسهیم به دو روش قابل انجام است:

- تسهیم در میدان فرکانس یا FDM[۱]
- تسهیم در میدان زمان یا TDM[۲]

در روش FDM با فرض آنکه حداکثر N ایستگاه در شبکه وجود داشته باشد ، پهنای باند فرکانسی کانال به N باند مجزا تقسیم می‌شود. هر ایستگاه موظف است در یکی از این باندهای فرکانسی ارسال و دریافت داشته باشد و چون این باند فرکانسی به صورت ثابت ، متعلق به خودش خواهد بود ، هرگونه تصادم و تداخل سیگنال منتفی است.

در روش TDM زمان به بازه‌های کوچکی[۳] تقسیم شده و هر ایستگاه مجاز است فقط در بازهٔ زمانی متعلق به خودش ، اطلاعات را روی کانال بفرستد.

---

۱ Frequency Division Multiplexing
۲ Time Division Multiplexing
۳ Time Slot

روشهای FDM و TDM زمانی کارآمد و مفید خواهند بود که : اولاً تعداد ایستگاهها ثابت و محدود باشد. ثانیاً هر ایستگاه حجم ثابت و در عین حال دائمی ارسال داده بر روی کانال داشته باشد. در شبکه‌های کامپیوتری ایستگاهها از نظر تعداد ، نامشخص و زیادند و ارسال داده‌ها نیز "انفجاری"[1] است. انفجاری بودن ترافیک بدین معناست که ایستگاه در لحظاتی ، بصورت ناگهانی حجم انبوهی از فریمها را برای ارسال روی کانال تولید می‌کند و سپس متوقف شده و تا لحظات متمادی هیچ داده‌ای برای ارسال تولید نمی‌کند. در شبکه‌ها تقاضای ارسال روی کانال پدیده‌ایست تصادفی و هیچ قاعدهٔ از پیش تعیین شده‌ای ندارد. آمارها نشان می‌دهد که انفجاری بودن ترافیک روی شبکه ، نسبت ۱۰۰۰/۱ دارد؛ یعنی :

$$\frac{\text{Peak Traffic}}{\text{Mean Traffic}} = \frac{1000}{1}$$

با این توصیف برای تسهیم کانالهای مشترک باید به سمت روشهای پویا حرکت کرد. در این خصوص پروتکلهای متفاوتی عرضه شده که در این فصل شناخته شده‌ترین آنها را که استانداردهای IEEE 802.x هستند ، معرفی خواهیم کرد.

۲-۱) مختصری در مورد خطا در شبکه‌های کامپیوتری

خطا در خطوط انتقال جزو حقایقی است که به هیچ وجه نمی‌توان بطور کامل آن را برطرف کرد و همیشه جزو مشکلات عمدهٔ سیستمهای مخابراتی بوده است. ماهیت خطا و علل بوجود آمدن آن را می‌توان در موارد زیر خلاصه کرد:

- **نویز حرارتی** : این نویز به دلیل حرکت اتفاقی الکترونها بوجود می‌آید و با افزایش دما ، شدت این نویز هم به صورت خطی تقویت می‌شود. بخصوص در مداراتی مثل تقویت کننده‌های نیمه هادی با ضریب تقویت و بهرهٔ بالا ، تاثیر این نویز حساسیت بیشتری دارد. اثر این خطا کاملا تصادفی است.
- **شوک‌های الکتریکی** : این نوع از نویز بدلیل قطع و وصل کلیدها ، سیمها و سوئیچ‌های الکتریکی یا رعد و برق بوجود آمده و نوعی خطای انفجاری را باعث می‌شود؛ یعنی مجموعهٔ گسترده‌ای از بیتها که روی کانال در جریانند ، به یکباره خراب می‌شوند. به

[1] Bursty Traffic

عنوان مثال اگر یک شوک الکتریکی به اندازه 10ms ادامه یابد و اطلاعات روی کانال با سرعت 1Mbps در جریان باشد ، با فرض آنکه طول متوسط فریمها 1KB در نظر گرفته شود ، این شوک می‌تواند تا ده فریم را بطور کلی نابود کند؛ به این معنا که فرستنده ده فریم را فرستاده ولی گیرنده هیچ فریمی دریافت نکرده است.

- **نویز کیهانی:** این نوع خطاها ناشی از حرکات کیهانی ، کهکشانها ، وضعیت ستارگان و خورشید و امثال آن می‌باشد و تاثیر آن بیشتر بر روی کانالهای رادیوئی است.

ساده ترین روش کشف خطا ، اضافه کردن بیت توازن به داده‌هاست. در این روش به ازای هر بایت از اطلاعات یک بیت توازن اضافه می‌شود؛ این بیت باید به گونه‌ای انتخاب و اضافه شود که مجموع تعداد بیتهای ۱ ، همیشه زوج یا فرد باشد.

مثال:

بایت اصلی :	01101001
بیت توان فرد	Odd Parity 1 01101001
بیت توان زوج	Even Parity 0 01101001

بنابراین گیرنده می‌تواند با بررسی بیت توازن ، خطای احتمالی را کشف کند ، ولی این روش در صورتی موثر است که تعداد خطاهای رخ داده زوج نباشد.

روش **Checksum** : در این روش تمام بایتهای یک فریم که باید توسط فرستنده ارسال شود ، با هم جمع (یا XOR) شده و یک بایت به نام Checksum بدست می‌آید. این بایت در انتهای فریم به مقصد ارسال می‌شود. در مقصد مجدداً بایت Checksum محاسبه و سپس مقایسه می‌شود. این روش در صورتی قادر به کشف خطا است که تعداد خطاهای رخ داده در بیتهای هم ارزش زوج نباشد.

کدهای کشف خطای CRC[1] : در روش CRC ، به ازای مجموعه ای از بیتها (مثلا ۵۱۲۰ بیت یا ۱۰۲۴۰ بیت ...) تعدادی بیت کنترلی به نام CRC محاسبه و به انتهای فریم اضافه می‌شود. مبنای محاسبهٔ کدهای CRC با استفاده از تقسیم چندجمله‌ای است که روش محاسبهٔ آن با ارائهٔ یک مثال توضیح داده شده است :

[1] Cyclic Redundancy Check

دادهٔ اصلی : 11100101

7	6	5	4	3	2	1	0
1	1	1	0	0	1	0	1

ابتدا از روی دادهٔ اصلی یک چندجمله‌ای تولید می‌شود. نمایش ریاضی چند جمله‌ای بدینصورت است که بیتها از راست به چپ ضرایب یک چند جمله‌ای قرار می‌گیرند که توان هر جمله را موقعیت بیت در رشته مشخص می‌کند. بدین صورت داده به صورت یک چند جمله‌ای نمایش داده خواهد شد. رشتهٔ بیت در این مثال برای سادگی عملیات ، هشت بیتی فرض شده است ، ولی در عمل این رشته می‌تواند دهها هزار بیت طول داشته باشد.

$$D(X)=1 * x^7 + 1 * x^6 + 1 * x^5 + 0 * x^4 + 0 * x^3 + 1 * x^2 + 0 * x + 1$$
$$D(X)= x^7 + x^6 + x^5 + x^2 + 1$$

برای تولید کد CRC ، چند جمله‌ای D(X). x^n بر یک **"چندجمله‌ای مولد"** که بین گیرنده و فرستنده توافق می‌شود و اختیاری است ، تقسیم می‌گردد. (n بالاترین توان چندجمله‌ای مولد است.) تقسیم در مبنای ۲ انجام می‌شود ، یعنی ضرایب جملاتِ با توان مساوی با هم XOR خواهد شدو تفریق معنا ندارد. باقیماندهٔ تقسیم به عنوان کدهای کنترل خطا در انتهای داده‌ها ارسال خواهند شد.

مولد CRC = $X^2+1 \rightarrow 101$

Data = $x^7+x^6+x^5+x^2+1 \xrightarrow{*X^2} X^9 + X^8 + X^7 + X^4 + X^2$

$X^9 + X^8 + X^7 + X^4 + X^2 \,|\, X^2+1$

باقیمانده : $+1 = 01$

در روشی که بخواهیم بصورت باینری (به جای چند جمله‌ای) کد CRC را حساب کنیم ، به تعداد بزرگترین توان جملهٔ مولد ، در سمت راست رشتهٔ داده صفر اضافه می‌کنیم. بنابراین در مثال بالا باید دو صفر به سمت راستِ داده اضافه شود. سپس داده‌ای که به آن صفر اضافه شده است ، بر چند جمله ای مولد تقسیم می‌شود. در تقسیم به نکات زیر باید توجه داشت:

۱- تقسیم از این لحاظ با تقسیم معمولی متفاوت است که شما باید از سمت چپ بیتهای باقیمانده را صفر کنید.

۲- جمع در مبنای ۲ و به صورت XOR انجام می‌شود.

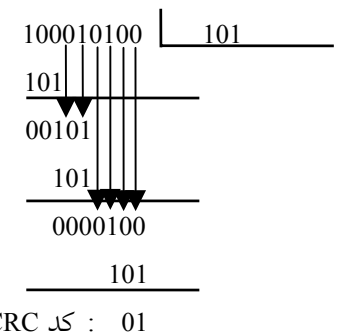
۳- نهایتاً بیتهای باقیماندهٔ تقسیم در سمت راست بیتهای داده قرار می‌گیرد. مثال:

```
1 1 1 0 0 1 0 1 0 0 | 101
1 0 1               | 11010001
  1 0 0
  1 0 1
    1 0 1
    1 0 1
      0 0 0 1 0 0
          1 0 1
            0 1   کد CRC
```

مثال :

Data = $X^6 + X^2 + 1$

CRC Generator = $X^2 + 1$



مثالی از مولدهای شناخته شده و استاندارد CRC

CRC-12 = $X^{12} + X^{11} + X^3 + X^2 + 1$

CRC-16 = $X^{16} + X^{15} + X^2 + 1$

CRC-CCITT = $X^{16} + X^{12} + X^5 + 1$

کدهای محاسبه شدهٔ CRC معمولا در انتهای اطلاعات ارسال خواهد شد و پس از دریافت اطلاعات در گیرنده ، مجدداً کدهای CRC برای داده‌ها محاسبه می‌شوند و نتیجه با کد ارسالی CRC مقایسه می‌گردد و در صورت عدم تطابق ، خطایی در داده‌ها وجود دارد و داده‌ها فاقد

اعتبار است. اگر مولد CRC مناسب انتخاب شود ، احتمال آنکه خطایی بروز کند ولی گیرنده قادر به کشف آن نباشد ، کمتر از 0.002 است.

دقت کنید که عمل محاسبهٔ کدهای CRC و همچنین بررسی خطا از طریق تراشه‌های سخت‌افزاری انجام می‌شود تا سرعت عمل بالا برود. این تراشه‌ها بسادگی و از طریق شیفت‌رجیسترهای فیدبک‌دار و گیتهای منطقی ساده مثل XOR پیاده می‌شود.

۲) استانداردهای انتقال روی خطوط نقطه به نقطه

در این بخش دو پروتکل ارتباطی برای برقراری یک لینک بین دو ماشین نقطه به نقطه معرفی می‌شود. این دو پروتکل (بالاخص پروتکل دوم یعنی PPP) زمینه ساز برقراری ارتباط میلیونها نفر در سراسر دنیا با شبکهٔ اینترنت هستند ، چراکه بسیاری از کاربران اینترنت بوسیلهٔ مودم و از طریق خطوط تلفن معمولی به اینترنت متصل می‌شوند که کانالی نقطه به نقطه محسوب می‌شود. معمولاً یکسری از موسسات ارائه‌دهندهٔ خدمات اینترنت که از این به بعد آنها را ISP[1] می‌نامیم ، خدمات اتصال به شبکه اینترنت را برای عموم فراهم می‌کنند. این مراکز ، تعدادی خط تلفن و مودم در اختیار دارند که مشترکین آنها می‌توانند از طریق مودم شماره گیری کرده و پس از برقراری ارتباط ، از خدمات شبکهٔ اینترنت برخوردار شوند.[2] گذشته از ISPهای تجاری ، دانشگاهها و موسسات نیز به کاربران مخصوص خودشان به همین روش سرویس می‌دهند.

سوال آنست که داده‌ها چگونه بین دو ماشین نقطه به نقطه مبادله می‌شوند و چه تمهیداتی برای برقراری یک لینک سریال روی این خطوط اندیشیده شده است.

۲-۱) پروتکل SLIP[3]

این پروتکل در سال ۱۹۸٤ توسط ریک آدامز برای اتصال ایستگاههای Sun به وسیلهٔ یک خط سریال مثل خط تلفن ، ابداع شد. این پروتکل که مستندات آن در RFC-1055 تشریح شده است ، فوق‌العاده ساده و در عین حال سریع است. روش کار بدین صورت است که به محض آنکه یک ایستگاه تمایل داشت اطلاعاتی را ارسال

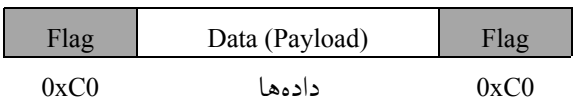
---

[1] Internet Service Providor

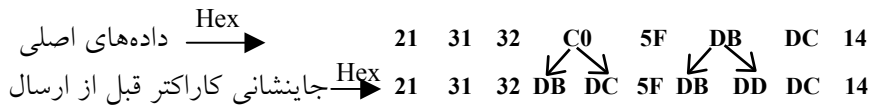
[2] درآمریکا معروفترین آنها AOL , MSN یا همان America online ، Compuserv ، Prodigy هستند.

[3] Serial Line IP

نماید ، علامت مشخصهٔ یک بایتی0xC0 را روی خط ارسال می‌کند و پشت سر آن داده‌ها را روی خط منتقل می‌نماید. برای مشخص کردن انتهای فریم ، پس از ارسال آخرین بایت داده‌ها مجدداً 0xC0 را روی خط می‌گذارد. بنابراین قالب هر فریم در این پروتکل به صورت زیر است :



در ساختار این فریم ، هیچ نکته قابل توضیحی وجود ندارد مگر آنکه بررسی شود اگر در درون قسمت داده‌ها ، کاراکتر 0xC0 وجود داشته باشد ، چه تمهیدی برای جلوگیری از اشتباه در انتهای فریم اندیشیده شده است. پروتکل SLIP برای حل این اشکال از روش "جاینشانی کاراکتر"[1] استفاده کرده است ، یعنی قبل از ارسال داده‌ها روی کانال هرگاه کاراکتر 0xC0 درون داده‌ها پیدا شود ، با دو کاراکتر متوالی (0xDB,0xDC) جایگزین خواهد شد. در ضمن برای آنکه این مشکل مجدداً برای زوج کاراکتر (0xDB,0xDC) تکرار نشود تمام کاراکترهای 0xDB با زوج (0xDB,0xDD) عوض خواهد شد. در چنین حالتی ضمن آنکه داده‌ها در مقصد قابل بازیابی به شکل اصلی هستند ، کاراکتر 0xC0 در درون فیلد داده وجود نخواهد داشت. برای آشنایی با این روش به مثال زیر دقت کنید.



با کمی دقت به قالب فریم در پروتکل SLIP ، متوجه خواهیم شد که این پروتکل از مسائل متعددی رنج می‌برد:

- در این پروتکل هیچ گونه کد کشف خطا گنجانیده نشده است و مسئلهٔ کشف خطاهای احتمالی به لایه‌های بالاتر محول شده است.

[1] Character stuffing

♦ در درون فیلد داده از فریم پروتکل SLIP ، فقط بسته‌های IP قرار می‌گیرد ، در حالی که امروزه در بعضی از شبکه‌ها مثل Novel یا Apple Talk ، ایستگاهها قادرند از طریق خطوط سریال و پروتکلهائی به غیر از IP با ایستگاههای راه دور ارتباط برقرار کنند و SLIP در این شبکه‌ها قابل استفاده نیست.

♦ چون دو ماشین که از طریق پروتکل SLIP با هم ارتباط برقرار می‌کنند دو مرکز رو در رو (نقطه به نقطه) محسوب می‌شوند ، این دو ایستگاه باید آدرسهای IP ثابت و شناخته شده‌ای داشته باشند ولیکن امروزه ارتباطی مورد نیاز است که وقتی یک ماشین میزبان به شبکه وارد شد ، قبل از هر گونه تبادل اطلاعات ابتدا هویت او تائید شده و سپس یک IP موقت به آن تخصیص داده شود. (آدرس IP را بعداً تشریح می‌کنیم.) نهایتاً پس از ختم ارتباط ، آن آدرس IP آزاد شده و برای ماشین دیگری در نظر گرفته شود. پروتکل SLIP چنین ویژگی را پشتیبانی نمی‌کند.

♦ پروتکل SLIP فقط برقرار کننده ارتباط را بعنوان ماشین معتبر می‌شناسد و هیچ راهی برای تائید و احراز هویت کاربر برقرارکننده ارتباط فراهم نکرده است و امنیت شبکه به مخاطره می‌افتد.

♦ متأسفانه بسیاری از سیستمهای عامل از SLIP پشتیبانی نمی‌کنند بهمین دلیل این پروتکل جای خود را به پروتکل جدید تری به نام PPP داده است که در ادامه آنرا معرفی می‌نمائیم. با تمامی معایب گفته شده بدلیل آنکه فریم SLIP فیلدهای سرآیند زیادی ندارد و یک ارتباط بدون انجام مراحل گوناگون ، برقرار می‌شود ، لذا این پروتکل بسیار سریع است.

۲-۲) پروتکل PPP[1]

این پروتکل که مستندات آن در RFC-1661 تا RFC-1663 آمده است دارای قالب فریم زیر است:

1 Byte	1 Byte	1 Byte	1 or 2 byte	Variable	2 or 4	1 Byte
Flag 01111110	Address 11111111	Control 00000011	Protocol	Payload	Checksum	**Flag 01111110**

با یک نگاه ساده و بدون هیچگونه توضیحی به قالب فریم بالا می‌توان متوجه شد که در این پروتکل بسیاری از معایب SLIP رفع شده است. قبل از آنکه

[1] Point to Point Protocol

مشخصات دقیق فریم PPP توضیح داده شود ، بررسی می‌کنیم که وقتی از طریق یک خط سریال نقطه‌به‌نقطه (مثل خط تلفن) می‌خواهید به اینترنت متصل شوید چه اتفاقاتی رخ می‌دهد تا یک ارتباط موفقیت‌آمیز برقرار شود:

در مرحله اول ماشین به کمک مودم شماره‌گیری می‌کند و پس از آنکه مودم طرف مقابل اتصال تلفن را وصل کرد ، ابتدا لازم است یکسری بسته‌های اطلاعاتی کنترلی به نام LCP[۱] بین طرفین رد و بدل شود. فریمهای LCP حاوی اطلاعاتی درون فیلد داده هستند که پارامترهای پروتکل PPP را بصورت توافقی ، انتخاب و تنظیم می‌نمایند (مهمترین بسته‌های LCP در ادامه معرفی خواهد شد). سپس یک سری پارامترهای لایهٔ بالاتر یعنی پروتکل لایهٔ شبکه تنظیم می‌شود. این پارامترها توسط بسته‌هایی که NCP[۲] نامیده می‌شوند ، تنظیم شده و طرفین بر روی این پارامترها توافق می‌کنند. به عنوان مثال کامپیوتر شما که قبل از برقراری ارتباط دارای آدرس IP نیست می‌تواند در هنگام برقراری ارتباط با ISP از طریق رد و بدل کردن فریمهای NCP ، یک IP موقت بگیرد و آدرس IP خودش را تنظیم کند. پس از ختم ارتباط ، آن آدرس IP آزاد شده و می‌تواند به مشترک دیگری اختصاص داده شود. در ضمن در ابتدای برقراری ارتباط طول فیلد داده ، فیلد کشف خطا ، فیلد پروتکل و وجود یا عدم وجود فیلدهای آدرس و کنترل ، توافق می‌شود. به مجموعه این مراحل ، فاز **مذاکره**[۳] گفته می‌شود. سپس مبادلهٔ فریمها آغاز می‌شود. در قسمت فیلد داده[۴] از پروتکل PPP ، می‌تواند بسته‌های IP یا بسته‌های پروتکلهای شناخته شده قرار بگیرد.

حمل بسته‌های مورد نظر ادامه خواهد یافت تا طرفین بر سر ختم ارتباط به توافق برسند. در هنگام ختم ارتباط مجدداً بسته‌های NCP رد و بدل می‌شوند تا همدیگر را از پایان ارتباط مطلع کنند.سپس مجدداً یکسری فریمهای LCP مبادله می‌شود تا طرفین بصورت توافقی ارتباط فیزیکی خودشان را قطع بنماید و خط آزاد شود.

با دقت در قالب فریم PPP مشخص است که ابتدا و انتهای فریم با علامت هشت بیتی 01111110 (0x7E) تعیین می‌شود و بالطبع چنین الگویی نباید در درون اطلاعات وجود داشته باشد. در ضمن برای پیشگیری از اشتباهات ناشی از وجود کاراکترهای کنترلی ASCII ، در این پروتکل وجود کاراکترهای با کد زیر ۳۲ در داده‌ها نیز

---

۱ Link Control Protocol
۲ Network Control Packet
۳ Negotiation Phase
۴ Payload

غیرمجازند. بـهمین دلیـل در ایـن پروتکـل ، در هنگـام وجـود چنیـن الگوهـای غیرمجـاز در درون داده‌ها ، عمل "جاینشانی کـاراکتر" بـه صـورت زیـر انجـام می‌شـود:

بجای کاراکتر با کد 0x7E ، زوج کاراکتر 0x7D-0x5E قرار می‌گیرد.

بجای کاراکتر با کد 0x7D ، زوج کاراکتر 0x7D-0x9D قرار می‌گیرد.

بجای کـاراکتر بـا کدهـای زیـر ۳۲ ابتـدا بیـت ششـم از آن کـاراکتر معکـوس شـده و سـپس کـاراکتر 0x7D قبـل از آن اضافـه می‌شـود. مثـلاً کـاراکتر بـا کـد 0x0A بصـورت 0x7D-0x2A تبدیـل و ارسـال می‌شـود.

حال فیلدهای فریـم را در ایـن پروتکـل بررسـی می‌نمـاییم:

- **Address Field** : تمامـاً ۱ اسـت و طبعـاً بعنـوان یـک آدرس فـراگـیر تلقـی شـده و ایستگاه مقابل موظف است چنین فریمـی را بپذیـرد. (ایـن فیلـد عمـلاً زائـد اسـت.)

- **Control Field** : ایـن فیلـد در مـورد فریمـهای عـادی مقـدار 00000011 دارد کـه نشـان دهنـده آن اسـت کـه ایـن فریـم شـماره‌گـذاری شـده نیسـت[1] و در نتیجـه ، طرفیـن برای فریمـهای یکدیگـر پیغـام ACK پـس نخواهنـد فرسـتاد. وقتـی کـه یـک فریـم PPP در حـالت عـادی بسـته‌های IP را حمـل می‌کنـد هـر دو فیلـد "آدرس " و "کنـترل" ثـابت و عملاً زائد هستند زیرا کنـترل جریـان داده‌هـا در لایـهٔ سـوم انجـام می‌شـود. البتـه می‌تـوان از ایـن پروتکـل در حـالت شـماره‌گـذاری شـده فریمـها را ارسـال کـرد کـه در اینجـا بـه آن نخواهیـم پرداخـت زیـرا در شـبکهٔ اینـترنت کـاربرد چندانـی نـدارد. (مسـتندات آن در REC-1663 آمده اسـت) شـاید سـئوال کنیـد در هنگـام حمـل بسـته‌های IP ، دو فیلـد ثـابت و زائد "آدرس" و "کنترل" چـرا بایسـتی ارسـال شـوند؟ پاسـخ آن اسـت کـه طرفیـن ارتبـاط بـا اسـتفاده از بسـته‌های LCP می‌تواننـد توافـق کننـد کـه در ادامـهٔ ارتبـاط ایـن دو فیلـد حذف شوند. نکته ای که بـاید بـه آن دقـت داشـته باشـید آن اسـت کـه ایـن پروتکـل بـرای یـک اتصـال نقطـه بـه نقطـه تعریـف شـده و بـرای ارتباطـات چنـدگانـه[2] صـادق نیسـت و بهمین دلیل حل بسیاری از مسـائل در چنیـن ارتبـاطی سـاده خواهـد بـود.

- **Protocol** : عددی که در این فیلد قرار می‌گیرد مشخص‌کنندهٔ آنست کـه بسـتهٔ درون فیلـد داده ، مربوط به چه پروتکلی در لایهٔ بالاتر است؛ یعنی پس از دریـافت فریـم ، محتـوای فیلـد

---

[1] Unnumbered Frame
[2] Multidrop

دادهٔ آن برای پردازشهای بعدی باید به کدام پروسس در لایهٔ بالاتر تحویل شود.(مثلاً پروتکلهایی مثل IP ، IPX و ...) در ضمن این عدد می‌تواند مشخص کند که درون فیلد داده ، یک بستهٔ NCP یا LCP قرار دارد.

0xC021 : درون فریم ، بستهٔ LCP قرار دارد.

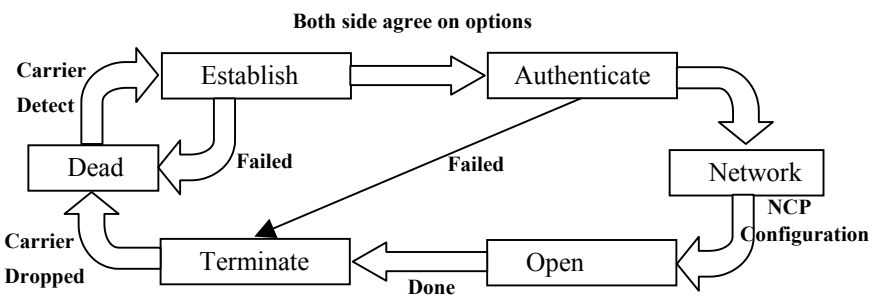
0x8021 : درون فریم ، بستهٔ NCP قرار دارد.

0x0021 : درون فریم ، بستهٔ IP قرار دارد.

- **Payload** : در این فیلد یک بستهٔ مربوط به لایهٔ بالاتر حمل می‌شود. محدودیتی بر روی طول این فیلد وجود ندارد ، ولی اندازهٔ آن توافقی است و در ابتدای برقراری ارتباط بین طرفین توافق می‌شود. در هنگام برقراری ارتباط که هنوز طرفین ارتباط ، روی اندازهٔ مشخصی توافق نکرده‌اند، سایز پیش فرض برای این فیلد ۱۵۰۰ بایت می‌باشد.
- **Checksum** : این فیلد برای کشف خطاهای احتمالی در فریم است و در حالت پیش فرض ۲ بایتی است ولی می‌توان بصورت ٤ بایتی بین طرفین ارتباط توافق کرد.

همانگونه که اشاره شد پروتکل PPP اجازه داده است که درون فیلد داده از هر فریم ، بسته‌های متفاوتی (از لحاظ پروتکل تولید کننده در لایهٔ بالاتر) قرار بگیرد ، بهمین دلیل این انعطاف را دارد که در شبکه‌های گوناگونی بکار گرفته شود.

در شکل (۳-۲) مراحل برقراری و ختم یک ارتباط در پروتکل PPP به صورت یک نمودار حالت تصویر شده است.



شکل (۳-۲) مراحل برقراری و ختم یک ارتباط در پروتکل PPP

شرح "نمودار حالتِ"[۱] شکل (۳-۲) در زیر آمده است :

♦ حالت Dead نشان می‌دهد که خط آزاد است و هیچ سیگنال معتبری روی کانال احساس نمی‌شود.

♦ حالت Establish بدین معناست که روی خط سیگنال معتبری مشاهده شده و یک اتصال فیزیکی برقرار گردیده است ولیکن طرفین ، پارامترهای خود را برای برقراری یک ارتباط تنظیم نکرده‌اند ، بهمین دلیل یک سری بسته‌های LCP بین طرفین رد و بدل شده تا پارامترهای لینک تنظیم شوند. (پارامترهایی مثل اندازهٔ فیلدها)

♦ حالت Authenticate ، مرحلهٔ بررسی و تائید هویت شروع کنندهٔ ارتباط خواهد بود. اگر یکی از طرفین ، هویت و مشخصات طرف مقابلش را تصدیق نکرد ، ارتباط قطع می‌شود.

♦ حالت Network : در این حالت بسته‌های NCP برای تنظیم پیکربندی پروتکل لایهٔ بالاتر (لایه شبکه) مبادله می‌شوند. پس از تنظیمِ پیکربندی لازم همه چیز برای برقراری یک ارتباط آماده است.

♦ حالت Open : در این حالت ، شرایط برای مبادله و انتقال اطلاعات آماده می‌شود.

♦ حالت Terminate : در این حالت که پس از اتمام مبادلهٔ اطلاعات صورت می‌گیرد ، طرفین با مبادله بسته‌های LCP ، بر سر ختم ارتباط به توافق می‌رسند.

♦ حالت Dead : هر گاه مبادله اطلاعات به اتمام رسید و طرفین با ختم ارتباط موافقت کردند ، کانال به حالت غیرفعال تبدیل شده و عملاً هیچ سیگنال حاملِ معتبری روی آن ارسال نخواهد شد.

۱-۲-۲) برخی از بسته‌های مهم LCP

بسته‌های LCP بسیار متنوعند و برای دسترسی به جزئیات دقیق آن بایستی به RFC-1661 مراجعه کرد. در جدول (٤-۲) برخی از این بسته‌ها بصورت اجمالی معرفی شده است. در این جدول ، علامت I[۲] به معنای یکی از طرفین است که به دیگری پیشنهادی را عرضه می‌کند و علامت R[۳] پاسخ‌دهنده به پیشنهاد دهنده است.

---

[۱] State Diagram
[۲] Initiator
[۳] Responder

نام بسته	جهت	عملکرد
Configure Request	I ⟶ R	لیستی از گزینه‌ها و مقادیر را برای تنظیم ، پیشنهاد می‌کند.
Configure Ack	I ⟵ R	مشخص می‌کند که تمامی پیشنهادات پذیرفته شد.
Configure Nack	I ⟵ R	برخی از پارامترها و گزینه‌ها پذیرفته نشد.
Configure Reject	I ⟵ R	برخی از پارامترها قابل بحث و توافق نیستند.
Terminate Request	I ⟶ R	تقاضا برای خاتمه و قطع ارتباط
Terminate Ack	I ⟵ R	موافقت برای قطع ارتباط و کانال
Code-Reject	I ⟵ R	تقاضایی رسیده است که شناسایی و فهم نمی‌شود.
Echo Request	I ⟶ R	لطفاً عیناً همین بسته را پس بفرستید!
Echo Reply	I ⟵ R	بسته پس فرستاده شد! (پاسخ بستهٔ Echo Request)
Discard Request	I ⟶ R	لطفاً این بسته را ندیده بگیرید. (حذف کنید.)
Protocol Reject	I ⟵ R	پروتکلی را تعیین کرده‌اید که تشخیص داده نمی‌شود.

جدول (٤-٢) برخی از بسته‌های LCP

- **Configure Request** : یکی از طرفین ، فهرستی از پارامترها و گزینه‌ها را برای توافق به طرف مقابل عرضه می‌کند. بعنوان مثال می‌توان بر سر اندازهٔ فیلد داده (Payload) ، بودن یا نبودن دو فیلد آدرس و کنترل در خلال ارسال بسته‌های IP (با ارسال این بسته) ، توافق کرد.
- **Configure Ack** : در پاسخ به لیست پارامترهای پیشنهاد شده ، با ارسال این بسته اعلام می‌شود که همهٔ آنها پذیرفته شده و مورد توافق قرار گرفته است.
- **Configure Nack** : برای مخالفت و ابراز عدم توافق بر روی برخی از پارامترهای پیشنهاد شده ، این بسته پس فرستاده می‌شود و در ضمن پارامترهای جدیدی پیشنهاد می‌شود.
- **Configure Reject** : در پاسخ به پیشنهادات عرضه شده ، طرف مقابل با ارسال این بسته ، یکسری از پارامترها را که قابل بحث و توافق نیستند ، مشخص می‌کند. این پارامترها باید بصورت پیش فرض در نظر گرفته شده یا چشمپوشی شود.
- **Terminate Request** : با این بسته یکی از طرفین ، تقاضای پایان دادن به ارتباط را اعلام می‌نماید.

- **Terminate Ack** : با این بسته در پاسخ به تقاضای ختم ارتباط ، طرف مقابل پذیرش ختم ارتباط را اعلام می‌کند.
- **Code-Reject** : هر گاه یکی از طرفین پارامترها و پیشنهاداتی را دریافت کند که آنها را تشخیص نداده یا منظور طرف مقابل را متوجه نشود ، این بسته را در پاسخ به آن ارسال می‌نماید.
- **Echo Request** : یکی از طرفین ارتباط از دیگری می‌خواهد که این بسته را گرفته و مجدداً به خودش برگرداند.
- **Echo Reply** : در پاسخ به تقاضای Echo Request ، طرف مقابل این بسته را پس می‌فرستد.

دو بستهٔ فوق برای عملیات اشکال زدایی و تست ارتباط و همچنین تخمین زمان رفت و برگشت و محاسبهٔ تاخیر کاربرد دارد.

- **Discard Request** : این بسته که می‌تواند توسط هر یک از طرفین ارتباط ارسال شود ، در طرف مقابل نادیده گرفته می‌شود. در حقیقت این بسته نیز برای اشکال‌زدایی فنّی از شبکه به کار می‌رود. (بعنوان مثال یک ایستگاه که نمی‌داند آیا داده‌هایش روی سیم منتقل می‌شود یا خیر ، می‌تواند با ارسال این بسته موضوع را بررسی کند.)
- **Protocol Reject** : همانگونه که در توضیح قالب فریم پروتکل PPP مشخص شد ، درون فیلد Protocol (یعنی فیلد چهارم) شمارهٔ پروتکلی قرار می‌گیرد که بستهٔ درون فیلد داده توسط آن پروتکل تولید و ارسال شده است و در طرف مقابل نیز باید تحویل پروسهٔ متناظر با همان پروتکل شود. اگر یکی از طرفین شمارهٔ پروتکل را تشخیص ندهد ، نمی‌داند با بسته درون فیلد داده چکار کند. در این حالت ضمن حذف آن بسته در پاسخ به ارسال کنندهٔ آن ، بستهٔ Protocol Reject را ارسال می‌کند.

در مورد بسته‌های NCP فعلاً مطلبی مطرح نمی‌کنیم ولی همین قدر کافی است که بدانید با استفاده از این بسته‌ها ، می‌توان پارامترهای دینامیکی لایهٔ بالاتر را پیکربندی کرد.

۳) استانداردهای واسط شبکه‌های محلی با کانال اشتراکی

در بخش قبلی با دو پروتکل انتقال فریم روی خطوط نقطه به نقطه آشنا شدیم. در این بخش به شبکه‌های متکی به کانالهای مشترک و استانداردهای آنها خواهیم پرداخت. انجمن بین‌المللی مهندسین برق و الکترونیک (IEEE) به عنوان بزرگترین سازمان علمی و تحقیقاتی جهان در زمینهٔ برق ، الکترونیک و کامپیوتر در بسیاری از زمینه‌ها اقدام به تدوین استانداردهای جهانی نموده است که در این بین استانداردهای سری IEEE 802.x در ارتباط با شبکه‌های کامپیوتری تدوین شده‌اند. این استانداردها در خصوص انتقال اطلاعات روی کانال مشترک و مدیریت کانال هستند ، لذا در لایهٔ اوّل از مدل TCP/IP مطرح می‌شوند.[۱] این استانداردها بعداً توسط کمیتهٔ ISO پذیرفته شد و مجدداً تحت نام ISO 8802 معرفی گردید. در این بخش برخی از استانداردهای IEEE سری 802 را توضیح خواهیم داد.

IEEE 802.1 یک پروتکل شبکه نیست بلکه استانداردی شامل یکسری تعاریف ، تشریح برخی از روشها و مقدمه‌ای در مورد مجموعهٔ استانداردها است. همچنین طریقهٔ دسترسی به سرویس‌های تعریف شده در هر استاندارد و نکات فنی در مورد پروتکلهایی که IEEE برای شبکه‌ها ارائه کرده ، در این استاندارد تشریح شده است.

IEEE 802.2 یک زیرلایه به نام LLC[۲] تعریف کرده است تا اولاً جزئیات سخت‌افزاری و توپولوژی شبکه را پنهان کند؛ (یعنی با استفاده از این زیرلایه ، شبکه‌های محلی با توپولوژیهای متفاوت همگی از لحاظ سرویسهایی که به لایهٔ بالاتر ارائه می‌دهند ، یکسان‌سازی خواهند شد.) ثانیاً با استفاده از این زیرلایه سرویس انتقال فریمها مطمئن خواهد شد ، به گونه‌ای که ضمن شماره‌گذاری فریمها ، برای آنها پیغام تصدیق (Ack) مبادله شده و بر روی جریان فریمها نظارت می‌شود.[۳] در این فصل به زیرلایهٔ IEEE 802.2 نخواهیم پرداخت زیرا در شبکهٔ اینترنت به خدمات این زیرلایه احتیاجی نیست و کنترل جریان ونظارت بر مبادلهٔ مطمئن داده‌ها به لایهٔ سوم محول شده است.

۳-۱) IEEE 802.3 : استاندارد شبکه‌های محلی باس

این استاندارد برای شبکه‌های کانال مشترک با توپولوژی باس تعریف شده است. در این استاندارد ، مدیریت کانال به روش CSMA/CD[۴] انجام می‌شود. یعنی هرگاه

---

[۱] این استانداردها ، لایهٔ اوّل و لایهٔ دوّم از مدل ISO را پیاده‌سازی می‌کند.

[۲] Logic Link Control

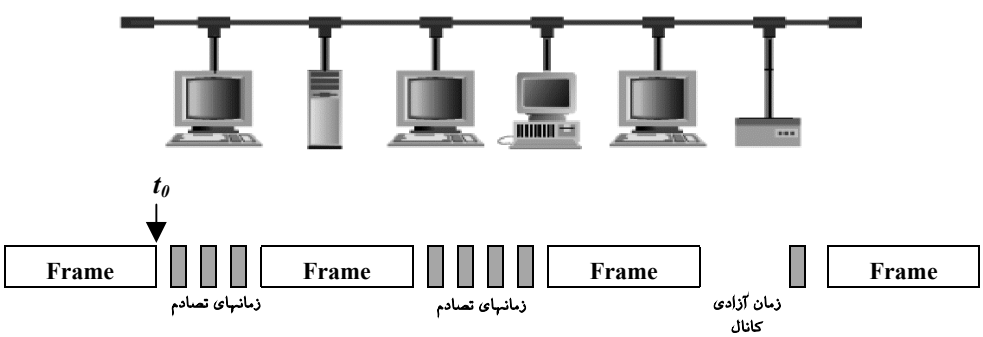
[۳] Flow Control

[۴] Carrier Sense Multiple Access / Collision Detection

ایستگاهی تقاضای ارسال فریم داشته باشد ابتدا به کانال گوش می‌دهد تا تشخیص بدهد آیا روی کانال ، سیگنال معتبر و حامل داده وجود دارد یا آنکه کانال آزاد است. اگر کانال خالی بود ارسال خود را آغاز می‌نماید ولی اگر روی کانال سیگنالی معتبر وجود داشت که نشان می‌داد ایستگاه دیگری در حال ارسال است ، صبر می‌کند و ضمن بررسی مداوم کانال ، مترصد می‌ماند تا کانال آزاد شود. (یعنی صبر می‌کند تا ایستگاه در حال ارسال ، کار ارسال فریمش را به اتمام برساند.) پس از آزاد شدن کانال ، ایستگاه شروع به ارسال فریم خود روی کانال می‌نماید ، ولی احتمال دارد در این لحظه "تصادم سیگنال" اتفاق بیفتد ، زیرا ممکن است ایستگاههای دیگری نیز برای آزاد شدن کانال منتظر مانده باشند و همگی با آزاد شدن خط اقدام به ارسال فریم خود بنمایند. برای کشف سریع تصادم ، ایستگاهها موظفند در حین ارسال فریم ، به سیگنال خط گوش بدهند تا قادر باشند به محض بروز تصادم ، عمل ارسال فریم را سریعاً متوقف کنند. در این استاندارد کشف تصادم به صورت سخت‌افزاری و آنالوگ انجام می‌شود تا بروز تصادم سریعاً کشف شود. (روش آنالوگ در کشف تصادم می‌تواند از طریق اندازه‌گیری توان خروجی فرستنده یا اندازه‌گیری طول پالسها پیاده‌سازی شده یا تلفیقی از هر دو باشد.)

هر گاه ایستگاهی که شروع به ارسال می‌کند با تصادم مواجه شود ، موظف است بطور تصادفی یک عدد تولید کرده و بر اساس آن مدت زمانی را صبر کند و مجدداً به خط گوش بدهد. با توجه به آنکه تمام ایستگاههائی که موجب بروز تصادم شده‌اند به اندازهٔ یک زمان تصادفی صبر خواهند کرد ، لذا آن ایستگاهی که زمان تصادفی انتظارش کمتر از بقیه است ممکن است در مرحلهٔ بعد موفق به ارسال شود. (روال تولید عدد تصادفی و زمان انتظار در ادامه تشریح خواهد شد.)

برای بررسی بیشتر روش CSMA/CD به شکل (۵-۲) دقت کنید.



شکل (۵-۲) بررسی روش CSMA/CD در مدیریت کانال

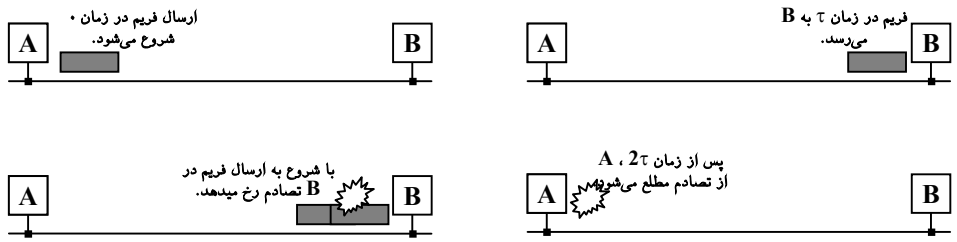
در شکل (۵-۲) یک ایستگاه ارسال فریم خود را در زمان t_0 به اتمام رسانده و در این لحظه کانال آزاد شده است. حال موقع ارسال فریم ایستگاههایی است که تقاضا برای ارسال دارند. در این لحظه چند ایستگاه بطور همزمان اقدام به ارسال فریم کرده‌اند و تصادم بوجود آمده است. ایستگاههای تصادم کننده به اندازهٔ یک زمان تصادفی از تلاش برای تصرف کانال کنار می‌کشند و نهایتاً پس از چند مرحله "رقابت"[1] یکی از ایستگاهها موفق به تصرف کانال خواهد شد. زمانهایی که بصورت منقطع بین زمان دو فریم نشان داده شده ، لحظاتی است که ایستگاهها برای تصرف کانال تلاش کرده‌اند ولی تصادم پیش آمده است.

در CSMA/CD هر گاه ایستگاهی از تصادم آگاه شود با تولید سیگنال نویز روی کانال ، به بقیه ایستگاهها کمک می‌کند تا بتوانند به سرعت از بروز تصادم مطلع شوند. سوال مهم آنست که اگر دو ایستگاه دقیقاً در زمان t_0 شروع به ارسال نمایند ، چقدر طول می‌کشد تا تصادم کشف شود؟ جواب این سوال از برخی جهات حیاتی است.

مدت زمان کشف تصادم به پارامتر تاخیر انتشار[2] سیگنال بستگی دارد.[3] در یک شبکهٔ باس اگر تاخیر انتشار سیگنال در کل کانال ، τ ثانیه باشد ، در بدترین حالت به اندازهٔ 2τ **ثانیه** طول می‌کشد تا تصادم کشف شود. به شکل (۶-۲) نگاه کنید. در این شکل فرض شده که ایستگاه A با خالی دیدن کانال شروع به ارسال فریم بنماید. تا رسیدن سیگنال منتشر شده به ایستگاه B در انتهای کانال ، τ ثانیه طول می‌کشد. اگر در همین لحظه ایستگاه B با خالی دیدن کانال شروع به ارسال فریم خود کند ، تصادم پیش خواهد آمد. با کشف سریع تصادم ، ایستگاه B شروع به تولید نویز می‌کند و τ ثانیهٔ دیگر طول خواهد کشید تا ایستگاه A از این قضیه مطلع شده و ارسال فریم را قطع کند. این زمان تلف شده در شبکه‌های کامپیوتری بسیار زیاد است. به عنوان مثال اگر طول کانال را هزار متر و نرخ ارسال را 100Mbps در نظر بگیریم ، در زمان 2τ که معادل ده میکروثانیه است ، ایستگاه A ، هزار بیت از فریم خود را ارسال کرده که بدلیل عدم اطلاع از تصادم باید آنرا مجدداً ارسال کند. این زمان جزو زمان تلفاتی کانال محسوب می‌شود. اگر تصادم چند مرحله ادامه یابد ، این زمان تلفاتی به مراتب راندمان کانال را بدتر خواهد کرد.

---

[1] Contention
[2] Propagation delay
[3] **تاخیر انتشار سیگنال در کانالهای مسی ۵ میکروثانیه و در کانالهای نوری یا رادیوئی ۳/۳ میکروثانیه در هر هزارمتر است.**



شکل (٦-٢) مراحل کشف تصادم

در روش CSMA/CD پس از آنکه ایستگاهی بدون تصادم موفق به تصرف کانال شد ، دیگر هیچگاه در خلال ارسال ، تصادم پیش نخواهد آمد و تمام برخوردها بین زمان ارسال دو فریم اتفاق می‌افتد. این زمان که "زمان رقابت" نامیده می‌شود روی راندمان کانال تاثیر منفی دارد. با بالا رفتن تعداد ایستگاهها یا ترافیک آنها ، تعداد تصادمها نیز بصورت تصاعدی زیاد شده و راندمان کانال بصورت بحرانی کاهش خواهد یافت. در ضمن هنگامی که طول کانال زیاد شود ، تاخیر انتشار و به تبع آن زمان رقابت نیز افزایش می‌یابد ، لذا این استاندارد فقط برای شبکه‌های محلی با طول کانال کم و نرخ ارسال پایین مناسب است. بطور کلّی راندمان کانال در این استاندارد به پارامترهای زیر بستگی دارد :

- F : طول فریم بر حسب بیت
- B : پهنای باند کانال
- C : سرعت انتشار
- L : طول کانال
- e : عدد نپرین (.....2.718)

$$\text{راندمان کانال} = \frac{1}{1+\frac{2.e.B.L}{C.F}}$$

با دقت در رابطه بالا مشهود است که :

- با کاهش طول فریم راندمان کانال کاهش می‌یابد.
- با افزایش طول کانال راندمان کانال کاهش می‌یابد.
- با افزایش نرخ ارسال راندمان کانال کاهش می‌یابد.

مشخصات فیزیکی استاندارد IEEE 802.3 بطور خلاصه عبارت است از :

- سرعت : ۱۰ مگابیت بر ثانیه
- کدینگ : "منچستر"

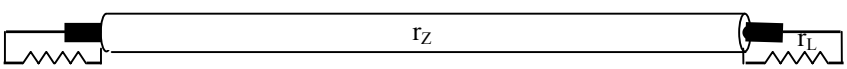
در کدینگ منچستر برای ارسال بیتهای صفر و یک از شکل موجهای زیر استفاده می‌شود :

استفاده از این شکل موجها ، بدلیل لبه‌ای که یقیناً در وسط هر بیت وجود دارد ، به سنکرون شدن ایستگاهها کمک می‌کند.

- سطوح ولتاژ : ± 0.85 V
- کانال : کابل کواکس ۵۰ اهم یا زوج سیم
- حداکثر طول کانال : ۵۰۰ متر با کابل کوآکس ضخیم و ۱۸۵ متر با کابل کوآکس نازک و ۱۰۰ متر با زوج سیم. (برای افزایش طول کابل به "تکرارکننده"[1] نیاز است. با استفاده ازتکرارکننده حداکثر طول کابل تا ۲/۵ کیلومتر قابل افزایش است.[2])

در شبکه‌های با توپولوژی باس ، اگر انتهای کابل باز باشد سیگنال منتشر شده در درون کابل پس از برخورد به سطح مقطع انتهایی آن ، بازتاب شده و ضمن بازگشت با اختلاف فاز ۱۸۰ درجه ، باعث تداخل با سیگنالهای ارسالی و نهایتاً خرابی بیتها خواهد شد. اگر انتهای کابل با یک مقاومت $\mathbf{r_L}$ اهمی بسته شده باشد ، میزان انعکاس سیگنال در درون کانال طبق رابطهٔ زیر محاسبه می‌شود :

$$\frac{\mathbf{r_Z - r_L}}{\mathbf{r_Z + r_L}}$$



برای آنکه میزان انعکاس سیگنال به صفر برسد باید $r_L=r_Z$ باشد. بهمین دلیل در این استاندارد که کابل کوآکس ۵۰ اهمی بکار رفته است باید یک مقاومت انتهایی (مقاومت ترمیناتور) ۵۰ اهمی در انتهای کانال بسته شود.

---

[1] Repeater

[2] **تکرار کننده ابزاری است که پس از دریافت بیتها از روی خط ، آنها را مجدداً روی خروجی خود تولید می‌کند و و این عمل باعث تقویت سیگنال و حذف نویز خواهد شد.**

قالب فریمهای داده در استاندارد IEEE 802.3 بصورت زیر است :

7 Byte	1 Byte	2 or 6 Byte	2 or 6 Byte	2 Byte	0~1500 Byte	0~46	4 Byte
Preamble	**Start of Frame Delimiter**	**Destination Address**	**Source Address**	**Length of Data Field**	**Data**	**Pad**	**CRC**

- **Preamble** : ابتدا ایستگاهی که توانسته است بدون تصادم کانال را صاحب شود ، ۷ بایت الگوی 10101010 را روی خط می‌گذارد و چون طریقه ارسال بیتها "منچستر" است ، این ۷ بایت با فرکانس 10MHz بمدت 5.6 میکروثانیه باعث سنکرون شدن تمام گیرنده‌ها با فرستنده خواهد شد.
- پس از این ۷ بایت ، فرستنده **"علامت ابتدای فریم"**[1] را با الگوی 10101011 ، روی خط می‌گذارد. این بایت نقطهٔ شروع فریم را مشخص می‌کند.
- هر فریم دارای دو فیلد آدرس است. طبق استاندارد IEEE 802.3 این آدرسها می‌توانند ۲ بایتی یا ٦ بایتی باشند. (امروزه این آدرسها ٦ بایتی هستند.)

این فیلدها که به نام آدرسهای MAC مشهورند ، عبارتند از :

- آدرس گیرندهٔ فریم (مقصدِ فریم) : همهٔ ایستگاهها به خط گوش می‌دهند و ایستگاهی که آدرس خود را روی خط ببیند فریم را دریافت خواهد کرد.
- آدرس فرستندهٔ فریم (مبدأ فریم)

تبصره :

- با ارزشترین بیتِ آدرس برای آدرس شخصی هر ایستگاه 0 است (لزوماً)
- با ارزشترین بیتِ آدرس برای آدرسهای گروهی 1 است. بقیه بیتها شماره گروه را تعیین می‌کند.
- اگر همه بیتهای فیلد آدرس مقصد ۱ باشد ، فریم برای تمامی ایستگاههای شبکه است و باید توسط همهٔ آنها دریافت و پردازش شود. (ارسال فراگیر و همگانی[2])

- **فیلد Lenght Of Data Field** : مقدار این فیلد مشخص می‌کند که چند بایت اطلاعات در فیلد داده وجود دارد.
- **فیلد Data** : در این فیلد حداقل صفر بایت و حداکثر ۱۵۰۰ بایت داده قرار می‌گیرد.

---

[1] Start Delimiter
[2] Boradcasting

- **فیلد PAD** : طبق استاندارد IEEE 802.3 ، فریمهای ارسالی حداقل باید ٦٤ بایت طول داشته باشند. بنابراین اگر اندازهٔ کل فریم ، از ٦٤ بایت کمتر بود باید در قسمت PAD آنقدر صفر اضافه شود تا طول فریم به ٦٤ بایت برسد. دلیل وجود این فیلد آنست که طول فریم نباید آنقدر کم باشد که قبل از زمان 2τ (بدترین حالتِ زمان کشف تصادم) ارسال آن به پایان برسد وگرنه ممکن است فرستنده قبل از اطلاع از تصادم ارسال فریم خود را تمام کند. در این استاندارد با در نظر گرفتن حداکثر ۲۵۰۰ متر طول کانال ، زمان 2τ تقریباً معادل ۲۵ میکروثانیه خواهد شد. در این ۲۵ میکروثانیه با سرعت 10 Mbps می‌توان ۲۵۰ بیت (معادل ۳۲ بایت) ارسال کرد که برای اطمینان ، حداقل طول هر فریم ٦٤ بایت انتخاب شده است.
- در انتهای فریم یک کد کشف خطا از نوع CRC-32 جهت بررسی صحت فریم ، اضافه شده است.

به گونه‌ای که اشاره شد در هنگام بروز تصادم هر ایستگاه اقدام به تولید یک عدد تصادفی کرده و بر اساس آن مدت زمانی را صبر می‌کند و مجدداً به خط گوش خواهد داد. روش تولید عدد تصادفی برای انتظار ، از یک الگوریتم خاص تبعیت می‌کند:
در اولین تصادم هر ایستگاه بطور تصادفی یکی از اعداد صفر یا یک را تولید می‌کند. در صورت تولید عدد ۱ ، معادل ۵۱۲ میکروثانیه صبر می‌کند و سپس به خط گوش می‌دهد تا در صورت خالی بودن ارسال را شروع نماید.
در هنگام دومین تصادم متوالی ، ایستگاه بطور تصادفی یکی از اعداد صفر تا سه را تولید می‌کند.
در هنگام سومین تصادم متوالی ، بطور تصادفی یکی از اعداد صفر تا هفت را تولید می‌کند.
در هنگام ***n***امین تصادم متوالی ، بطور تصادفی یکی از اعداد 0 تا $(2^n - 1)$ را تولید می‌کند.

ایستگاه موظف است به ازای عدد تصادفی تولید شده بر مبنای ۵۱۲ میکروثانیه ، منتظر مانده و سپس مجدداً خط را بررسی کند. بعنوان مثال اگر پس از ده تصادم پیاپی ، عدد تصادفی تولید شده ۱۰۰ باشد ، ایستگاه موظف است ۱۰۰×۵۱۲ میکروثانیه (۵۱/۲ میلی ثانیه) منتظر بماند.
پس از ١٦ تصادم پیاپی ، سخت‌افزار شبکه ، یک خرابی جدّی را به کاربر هشدار می‌دهد و پیگیری و کشف علت مسئله برعهده لایه‌های بالاتر است. این روش ، **"الگوریتم عقب‌گرد توانی"**[1] نامیده می‌شود.

[1] Binary Exponential Backoff

شرکت‌های DEC ، Xerox و Intel یک پیاده‌سازی عملی از این استاندارد را که به نام **اترنت**[1] مشهور است ، ارائه کرده‌اند. اترنت کاملاً سازگار با IEEE 802.3 است با این تفاوت که ساختار فریم در اترنت با یک اختلاف جزئی به صورت زیر است :

8 Byte	6 Byte	6 Byte	2 Byte	64~1500 Byte	4 Byte
Preamble	**Destination Address**	**Source Address**	**Frame Type**	**Data**	**CRC**

در این فریم ، فیلد Frame Type ، نوع بسته‌ای را که در درون فیلد داده حمل می‌شود ، مشخص می‌نماید.

محصولات مبتنی بر این استاندارد به دلیل ارزان بودن و سادگی نصب ، راه‌اندازی و نگهداری ، برای سالیان سال از پررونق‌ترین سخت‌افزارهای شبکه بوده است.

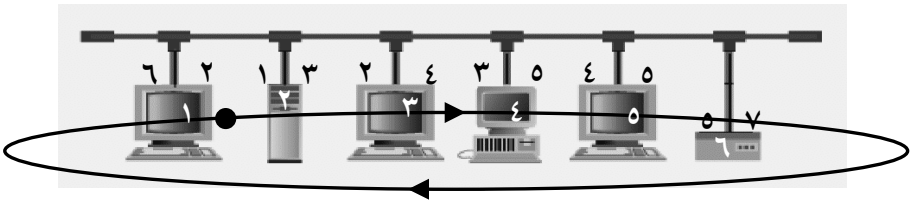
۲-۳) IEEE 802.4 : استاندارد شبکه‌های محلی توکن باس

در استاندارد IEEE 802.4 هدف اصلی ، پیاده‌سازی یک حلقهٔ مجازی بر روی یک شبکه با توپولوژی باس است به گونه‌ای که تصادم بر روی کانال بوجود نیاید و همهٔ ایستگاهها طبق یک روش سازمان‌یافته از کانال استفاده کرده و زمان تلف شده‌ای که صرف تصادم می‌شود حذف شود. در این استاندارد زمان انتظار برای استفاده از کانال و ارسال فریم قابل تخمین و تضمین شده می‌باشد ، زیرا اگر n ایستگاه در شبکه موجود و فعال باشد و هر ایستگاه فقط حق استفادهٔ حداکثر T ثانیه از کانال را داشته باشد ، در بالاترین حدّ ترافیک ، تاخیر حداکثر n.T ثانیه خواهد بود.

در این استاندارد کلیه ایستگاهها روی یک حلقهٔ مجازی فرض می‌شوند و نوبت ارسال ایستگاهها به ترتیبی است که روی حلقهٔ مجازی واقع شده‌اند؛ بنابراین هر ایستگاه موظف است: اولا آدرس ایستگاه چپ و راست خود را در حلقه حفظ نماید. ثانیاً هرگاه ایستگاهی ارسال فریم خود را به اتمام برساند ، باید یک فریم کنترلی تحت عنوان **توکن**[2] برای آدرس بعدی خود در حلقه بفرستد. در حقیقت **توکن** مجوز ارسال روی کانال محسوب می‌شود. اگر قاعده بر این باشد که فقط ایستگاهی که توکن را دریافت کرده حق ارسال داشته باشد ، هیچگاه تصادم رخ نمی‌دهد. شکل (۷-۲) یک شبکهٔ باس با حلقهٔ مجازی را نشان می‌دهد.

---

[1] Ethernet
[2] Token



شکل (۷-۲) حلقهٔ مجازی بر روی شبکهٔ باس

استاندارد IEEE 802.4 از لحاظ پیاده‌سازی بسیار پیچیده است و حداقل به ۱۰ زمان‌سنج سخت‌افزاری جهت کنترل و نظارت بر استاندارد محتاج است. برخی از مشخصات این استاندارد عبارت است از :

- نوع کانال : کابل کوآکس ۷۵ اهم تلویزیون
- در این استاندارد سطوح اولویت ۰ ، ۲ ، ٤ و ٦ وجود دارد که اولویت ٦ بالاترین سطح محسوب می‌شود. کلیهٔ ایستگاهها به سطوح اولویتی مجزا ، تقسیم می‌شوند. در سطح اولویت ٦ می‌توان برای انتقال بلادرنگ ، مثل ارسال صدا و تصویر از شبکه بهره برد. وجود اولویت یکی از نکات مثبتی است که شبکهٔ نوع CSMA/CD فاقد آن می‌باشد.
- قالب فریمهای داده در استاندارد IEEE 802.4 بصورت زیر است :

> 1 Byte	1 Byte	1 Byte	2 or 6 Byte	2 or 6 Byte	0~8182 Byte	4 Byte	1 Byte
Preamble	**Start of Frame Delimiter**	**Frame Control**	**Destination Address**	**Source Address**	**Data**	**CRC**	**End Delimiter**

- **Preamble** : همانند استاندارد 802.3 ، یک الگوی خاص از بیتها جهت سنکرون شدن گیرنده‌ها با فرستنده ، روی خط ارسال می‌شود و تعداد آن می‌تواند از یک تا چند بایت باشد.
- **Start Delimiter** : یک بایت جهت مشخص نمودن ابتدای فریم
- **End Delimiter** : یک بایت جهت مشخص انتهای فریم

کدینگ این دو بایت با کدینگ ارسال اطلاعات متفاوت است بدینگونه که روش عادی ارسال ، روش منچستر است ولی این دو بایت بروش NRZ-Half Binary-Unipolar ارسال می‌شوند تا ابتدا و انتهای فریم ، بصورت آنالوگ و سخت افزاری کشف شود و بهمین دلیل در این استاندارد ، به فیلد مشخص کنندهٔ طول داده (Data Length) نیازی نیست.

• **Frame Control** : در استاندارد IEEE 802.4 این فیلد انواع مختلف فریمهای کنترلی را برای عملیات نظارت بر حلقهٔ مجازی ، مشخص می‌نماید. اعداد این فیلد و معنای آن در زیر فهرست شده است:

♦ Claim Token (00H) : هر ایستگاه دارای یک زمان‌سنج (تایمر) است که بطور مرتب خط را بررسی می‌کند ، بنابراین روی خط باید یا توکن یا یک فریم داده ببیند؛ زیرا در این استاندارد بیکار بودن کانال معنا ندارد و اگر ایستگاهها ، فریم داده برای ارسال نداشته باشند ، بطور متوالی فریم توکن را برای یکدیگر ارسال می‌کنند. هر گاه اولین مدت زمان مجاز به سر برسد ولی ایستگاهی که نوبت ارسال اوست خط را بیکار ببیند ، تقاضای دریافت توکن می‌کند؛ یعنی یک فریم که در فیلد Frame Control آن کد 00 قرار دارد ، روی خط قرار می‌دهد تا ایستگاهی که توکن پیش اوست آنرا روی کانال بگذارد. اگر ایستگاهی که توکن را دریافت کرده ، بنحوی از خط خارج شده باشد ، ایستگاهها طبق الگوریتمی نظیر آنچه در استاندارد IEEE 802.3 گفته شد ، جهت رقابت و تصرف توکن مبارزه می‌کنند.

♦ Solicit-Succesor-1 (01H) : هر ایستگاه زمانسنجی دارد که بطور متناوب ایستگاههایی را که در حلقه نیستند و تقاضای ورود به شبکه را دارند ، دعوت می‌کند. طریقه دعوت آنها با ارسال فریمی است که در فیلد Frame Control آن ، کد 01 قرار دارد. ایستگاه ارسال کنندهٔ این فریم شماره خود و شماره‌هایی را که می‌توانند بعد از او وارد حلقه شوند ، معین می‌کند. در چنین زمانی ممکن است بین چند ایستگاه متقاضی ورود به شبکه تصادم رخ دهد ، بنابراین ایستگاه با قرار دادن فریم کنترلی 04H یا Resolve-Contention به رفع تصادم اقدام می‌نماید.

♦ گاهی اوقات توکن گم می‌شود مثلا ایستگاه شمارهٔ x ، توکن را برای آدرسی ارسال کرده است که اصلا روی حلقه وجود ندارد. در این حالت ایستگاهی که توکن را آزاد کند وجود ندارد؛ برای رفع این مشکل ، ایستگاه ارسال کنندهٔ توکن با تنظیم یک زمان‌سنج و بررسی خط ، پس از انقضای مهلتِ پاسخ دهی ، با ارسال فریم 03 یا Who-Follows ، آدرس ایستگاه بعد از خود را در حلقه سوال می‌کند. حال ایستگاهی که آدرس اعلام شده توسط این فریم را بعنوان آدرس ایستگاه قبل از خود می‌بیند با ارسال یک فریم کنترلی به نام Set-Successor به آن پاسخ می‌دهد و ایستگاه مربوط را از حلقه حذف کرده و حلقه اصلاح می‌شود. یعنی فرستندهٔ فریم Set-Successor جانشین ایستگاه خراب می‌شود.

♦ اگر ایستگاهی خراب یا از خط خارج شود و این اتفاق برای ایستگاه بعد از او هم بیفتد ، دیگر هیچ ایستگاهی به فریم Who-Follows پاسخ نمی‌دهد؛ در چنین حالتی با

ارسال فریم Solicit-Successor-2 همهٔ ایستگاه‌ها دعوت به بازسازی مجدد شماره‌های حلقه مجازی می‌شوند.

- 08H یا Token : فریمی است که هر ایستگاه با دریافت آن حق ارسال اطلاعات دارد.

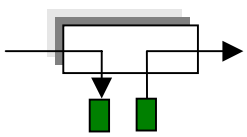
- بقیهٔ فیلدهایی که به آن اشاره نشد دقیقاً عملکردی شبیه به آنچه در استاندارد IEEE 802.3 توصیف شد ، دارند.

استاندارد IEEE 802.4 برای استفاده در محیطهای صنعتی و کاربردهای بلادرنگ ارائه شد و امروزه اهمیت خود را از دست داده است.[۱]

۳-۳) IEEE 802.5 : استاندارد شبکه‌های محلی حلقه

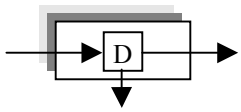
این استاندارد مختص توپولوژی حلقه است و اولین بار توسط IBM پیاده‌سازی شده است. در این استاندارد هر ایستگاه موظف است فریمهای داده را از ایستگاه قبلی دریافت و به ایستگاه بعدی در حلقه ارسال کند. ایستگاه حتی اگر اطلاعات برای او ارسال شده باشد ، موظف است ضمن برداشتن اطلاعات از روی خطّ مجدداً آنرا به ایستگاه بعدی ارسال کند. بنابراین اگر یک ایستگاه فریمی را روی کانال بگذارد ، نهایتاً خودش فریم خود را دریافت می‌کند. ایستگاههایی که اطلاعات برای آنها ارسال نشده است فقط وظیفه تقویت و انتقال آن را روی کانال برعهده دارند. هر ایستگاه در انتقال یک فریم حداقل یک بیت تاخیر ایجاد می‌کند. در شبکهٔ حلقه ، هر ایستگاه می‌تواند یکی از سه حالت زیر را داشته باشد:

- **حالت ارسال** : ایستگاه فقط زمانی مجوز ارسال دارد که یک فریم کنترلی خاصّ ۲٤ بیتی که توکن (نشانه) نام دارد ، دریافت کند. هرگاه یک ایستگاه توکن را دریافت کند ، اگر فریمی را برای ارسال آماده داشته باشد ، می‌تواند آنرا ارسال کرده و سپس توکن را آزاد کند. اگر ایستگاه فریمی جهت ارسال نداشته باشد ، توکن دریافتی را به ایستگاه بعدی در حلقه می‌فرستد. فرستنده پس از ارسال فریم خود و انتقال کامل آن در طول حلقه خودش آنرا دریافت کرده و از حلقه خارج می‌کند. ایستگاهِ در حال ارسال ، پس از دریافت آخرین بیتِ فریمِ خود ، توکن را آزاد می‌کند.

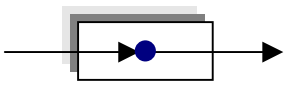


[۱] اولین بار این شبکه برای کاربردهای صنعتی در کمپانی جنرال موتورز (GMS) آمریکا پیاده‌سازی شد.

- **حالت شنود** : در این حالت ایستگاه فریم دریافتی را با یک بیت تاخیر برای ایستگاه بعدی در حلقه ارسال می‌کند.



- **حالت غیر فعال**[۱] : در این حالت ایستگاه از شبکه خارج شده و عملاً ورودی و خروجی ، اتصال کوتاهند.



در بار سبک (یعنی وقتی تقاضا برای ارسال کم است) ، توکن بسرعت و به ازای هر ایستگاه فقط با یک بیت تاخیر می‌چرخد و بنابراین هرگاه یک ایستگاه تقاضای ارسال داشته باشد ، پس از چند بیت تاخیر قادر به دریافت توکن و ارسال فریم خود خواهد بود.

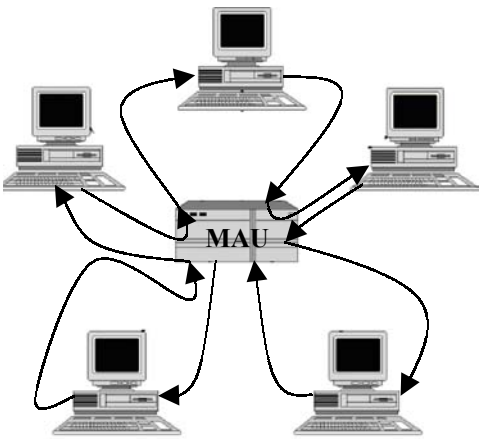
ایستگاهی که توکن را دریافت می‌کند ، مجاز است آنرا تا زمان محدودی ، برای ارسال فریمش نگه دارد. در استاندارد IEEE 802.5 ، "زمان مجاز در اختیار داشتن توکن"[۲] ، بطور پیش فرض ده میلی‌ثانیه در نظر گرفته شده است. چون هر ایستگاه موظف به ارسال فریم در زمان مجاز می‌باشد و پس از این زمان باید توکن را به ایستگاه بعدی تحویل بدهد لذا در بار سنگین همه در یک صف منظم سرویس‌دهی شده و از کانال استفادهٔ بهینه می‌شود. بنابراین می‌توان ادعا کرد در استاندارد IEEE 802.5 ، راندمان کانال در بار سنگین ، با تقریب خوبی نزدیک به ٪۱۰۰ است.

در شبکه‌های حلقه اگر یکی از ایستگاهها خراب شود کل شبکه مختل خواهد شد؛ بهمین دلیل باید تدبیری اتخاذ گردد تا یک ایستگاه به محض خرابی ، از حلقه خارج شود. در شبکهٔ حلقه ، از یک ابزار به نام MAU[۳] استفاده می‌شود تا به محض خروج یک ایستگاه از شبکه ، حلقه اصلاح شود. بزبان ساده تمام کابلهای شبکه از طریق MAU به هم وصل می‌شوند تا هنگام خرابی یک ایستگاه ، ورودی و خروجی آن ایستگاه را اتصال کوتاه کند و ایستگاه از حلقه خارج شود. شکل (۸-۲) یک شبکهٔ حلقه را با MAU ، نشان می‌دهد. هرچند در شبکهٔ

---

[۱] Idle
[۲] Token Holding Time
[۳] Multi Access Unit

حلقه وجود MAU ضروری نیست ولی شبکه را قابل اعتماد می‌کند. وجود یک MAU مرکـزی برای شبکه‌های با محدوده جغرافیایی وسیع مشکل‌آفرین است و در بعضی از مواقع می‌توان از چند MAU مجزا ، بصورت منطقه‌ای استفاده کرد.



شکل (۸-۲) شبکهٔ حلقه با MAU

در استاندارد IEEE 802.5 باید یک ایستگاه بعنوان ناظر[1] وظائف زیر را برعهده بگیرد: (هـر ایستگاه این قابلیت را دارد که نقش ناظر را بازی کند و نیازی به ایستگاه مجزا نیست.)

- **بررسی وجود توکن** : هر ایستگاه حداکثر ۱۰ میلی ثانیه می‌تواند توکن را در اختیار داشته باشد و ایستگاه ناظر باید با تنظیم یک زمان‌سنج ، از چرخش توکن مطمئن شود.
- **از بین بردن و پاک کردن فریمهای سرگردان و آشغال** (فریمهای سـرگـردان ، فریمـهای کوتاهی هستند که فرستندهٔ آنها ، پس از ارسال از حلقه خـارج شـده و آنـها روی حلقـه ، سرگردان می‌چرخند.)
- **ایجاد و تضمین حداقل ۲٤ بیت تاخیر در حلقه** : حداقل تأخیر در شبکهٔ حلقه مبتنـی بـر استاندارد IEEE 802.5 ، باید بقدری باشـد کـه توکـن بتوانـد یـک دور کـامل بزنـد؛ یعنـی ایستگاهی که توکن را ایجاد می‌کند نباید در حین تولیـد آنـرا دریـافت کنـد. پـس در ایـن استاندارد که توکن ، ۲٤ بیتی است ، حداقل باید ۲٤ بیت تاخیر وجود داشته باشـد و ایـن تاخیر برای عملکرد درست شبکه ضروری است. مساله بسـیار مـهم در طراحـی و تحلیـل

[1] Monitor

شبکهٔ حلقه آنست که طول فیزیکی یک بیت[۱] چقدر است؟ در یک کانال به طول L متر ، هرگاه یک پالس در ابتدای آن قرار گیرد ، مدت τ ثانیه طول خواهد کشید تا به انتهای کانال برسد. در شبکهٔ حلقه ، با نرخ ارسال " R مگابیت بر ثانیه" (روی کانال مسی با سرعت انتشار 200 m/μs) طول فیزیکی یک بیت 200/R تعریف می‌شود. (R برحسب مگابیت بر ثانیه است.) بعنوان مثال برای شبکه ای با طول ۱۰۰۰ متر و نرخ ۱ مگابیت بر ثانیه ، طول فیزیکی بیت برابر با ۲۰۰ متر است؛ یعنی تا زمانی که بیت بعدی روی کانال شود ، بیت اول ۲۰۰ متر طی از کانال را طی خواهد کرد. در نتیجه تا زمانی که بیت اول به انتهای کانال برسد ، فرستنده ۵ (۱۰۰۰/۲۰۰) بیت بعدی فریم را ارسال کرده است.
نسبت طول کانال به طول فیزیکی بیت ، "تاخیر انتشار کانال بر حسب بیت" خواهد بود.
در شبکهٔ حلقه با استاندارد IEEE 802.5 ، مجموع تعداد ایستگاههای فعال (که بصورت پیش‌فرض یک بیت تاخیر ایجاد می‌کنند) و تاخیر انتشار کانال بر حسب بیت ، نباید از ۲٤ کمتر شود؛ در غیر اینصورت ایستگاه ناظر موظف است تاخیر مصنوعی ایجاد کند.

روش کدینگ در این استاندارد ، منچستر تفاضلی[۲] با سطوح 3± ولت تا 4.5 ± ولت می‌باشد و نرخ ارسال ۱ تا ٤ مگابیت بر ثانیه است.

قالب فریمهای داده در استاندارد IEEE 802.5 بصورت زیر است. بدلیل مفصل بودن عملکرد برخی از فیلدها ، فقط به معرفی آنها بسنده کرده‌ایم.

1 Byte	1 Byte	1 Byte	2 or 6 Byte	2 or 6 Byte	No Limit	4 Byte	1 Byte	1 Byte
Start of Frame Delimiter	**Access Control**	**Frame Control**	**Destination Address**	**Source Address**	**Data**	**CRC**	**End Delimiter**	**Frame Status**

- **Start Delimiter** : یک بایت جهت مشخص نمودن ابتدای فریم
- **End Delimiter** : یک بایت جهت مشخص کردن انتهای فریم

کدینگ این دو بایت با کدینگ ارسال اطلاعات متفاوت است تا ابتدا و انتهای فریم ، بصورت آنالوگ و سخت افزاری کشف شود.

- **Access Control** : این فیلد هشت بیتی دارای چهار قسمت است:

---

[۱] Physical Length
[۲] Differential Manchester

- بیت توکن : این بیت مشخص کنندهٔ آن است که فریم جاری ، یک فریم داده نیست بلکه فریم توکن است و به ایستگاه مجوز ارسال می‌دهد. اگر این بیت فعال (۱) باشد ، ساختار فریم به صورت زیر خواهد بود:

- بیت مانیتور : این بیت را ایستگاه ناظر ، ۱ می‌کند تا یک فریم داده ، بیش از یکبار در حلقه نچرخد.
- بیتهای رزرو توکن و بیتهای اولویت : در این استاندارد سطوح اولویت وجود دارد و کلیهٔ ایستگاهها ، فریمهای ارسالی خود را به سطوح اولویتی مجزا تقسیم می‌کنند. توکن ابتدا با سطح اولویت بالا می‌چرخد و ایستگاههایی که یک فریم با اولویتِ مطابق با اولویت تعیین شده در توکن آمادهٔ ارسال دارند ، حق دارند آنرا ارسال نمایند. در غیر این صورت در بیتهای رزرو توکن ، اولویت فریم خود را رزرو می‌کند.

- **Access Control** : این فیلد هشت بیتی ، انواع مختلف فریم را برای نظارت بر عملکرد صحیح حلقه ، تعریف می‌کند. در جدول زیر برخی از انواع این فریمها و کاربرد آنها ، به اختصار فهرست شده است:

شماره	نام فریم	عملکرد کنترلی فریم
00000000	Duplicate Address Test	زمانی که دو ایستگاه شمارهٔ یکسان داشته باشند ، از این فریم استفاده می‌شود.
00000010	Beacon	از این فریم برای کشف محل پارگی کانال ، استفاده می‌شود.
00000011	Claim Token	با این فریم یک ایستگاه تلاش می‌کند تا خود را نامزد "ایستگاه ناظر" نموده و بر شبکه نظارت کند.
00000100	Purge	با این فریم از تمام ایستگاهها تقاضا می‌شود تا حلقه را از نو بازسازی کنند.
00000101	Active Monitor Present	ایستگاه ناظر به طور متناوب این فریم را ارسال می‌کند تا بقیه را از حضور خود مطمئن کند.
00000110	Standby Monitor Present	در این استاندارد برای ایستگاه ناظر یک ایستگاه پشتیبان در نظر گرفته می‌شود تا در مواقع اضطراری جایگزین ایستگاه ناظر شود. ایستگاه پشتیبان به طور متناوب این فریم را ارسال می‌کند تا بقیه را از حضور خود مطمئن کند.

• **Frame Status** : در این فیلد که در آخر فریم قرار گرفته ، فقـط دو بیـت بـا ارزش A و C تعریف شده است. این دو بیت که در ابتدا صفر است باید توسط ایستگاه مقصـدِ فریـم تنظیـم شود. پس از چرخش فریم روی حلقه و بـازگشـت بـه ایسـتگاه تولیـد کننـدهٔ آن ، از حـالات مختلف این دو بیت می‌توان اطلاعات زیر را استنتاج کرد:

ایستگاه مقصد ، در شبکه نیست و فریم دریافت نشده است.	**A=0 , C=0**
ایستگاه مقصد ، در شبکه وجود دارد ولی فریم پذیرفته نشد.	**A=1 , C=0**
فریم توسط ایستگاه مقصد ، سالم دریافت شده است.	**A=1 , C=1**

شبکه‌های مبتنی بر استاندارد IEEE 802.5 ، بدلیل راندمان بسیار خوب کانال ، مـورد توجـه قرار گرفتند ، به گونه‌ای که IBM آنرا به عنوان شبکهٔ داخلـی خـود بـرگزیـد و بـر اسـاس آن شبکه‌های بین شهری با سرعت بالا (مثل شبکهٔ بین‌شهری FDDI) پیاده‌سازی شدند.

۴-۳) مقایسهٔ سه استاندارد معرفی شده برای شبکه‌های محلی

برای تعیین یک طرح اولیه برای نصب و پیاده‌سازی شبکه ، باید شرایط حـاکم و همچنیـن الزاماتی که در محیط وجود دارد ، در نظر گرفته شود و بالطبع یک استاندارد هیچ رجحانی بـر دیگری ندارد مگر در قیاس با شرایطِ حاکم بر محیطی که قرار است در آنجا شبکه نصب شود. در زیر مشخصات کلیدی استانداردهای معرفی شده را فهرست می‌کنیم:

IEEE 802.3 - CSMA/CD

- دسترسی به کانال قطعیت و روال منظم ندارد.[1]
- در بار پایین ، تاخیر چندانی وجود ندارد و راندمان کانال مناسب است.
- در بار بالا به دلیل افزایش تصادم ، این استاندارد راندمان خوبی ندارد.
- در سرعت بالا و کاهش طول فریم ، راندمان کانال کاهش می‌یابد.
- فریمها سطوح اولویت ندارند و ارسال صوت و تصویر در آن گنجانده نشده است.

[1] Nondeterministic Channel Allocation

- با تمام کاستیها ، هزینهٔ نصب و راه‌اندازی این نوع شبکه کم است.

IEEE 802.4 – Token Bus

- دسترسی به کانال دارای روال باقطعیت و منظم‌تری نسبت به استاندارد قبلی است.
- این استاندارد برای فریمها اولویت قائل است و میتوان در اولویت بالا ارسال همزمان و بلادرنگ صوت و تصویر را ارائه کرد .
- استاندارد بسیار پیچیده است و قسمتی از سخت افزار آنالوگ می‌باشد .
- استفاده از کانال در بار بالا صحیحتر و با راندمان بهتری صورت می‌گیرد .
- برای فریمهای با طول کوتاه راندمان پائین می‌آید .
- برای سیستمهای بلادرنگ[1] قابل استفاده می‌باشد .

IEEE 802.5 – Token Ring

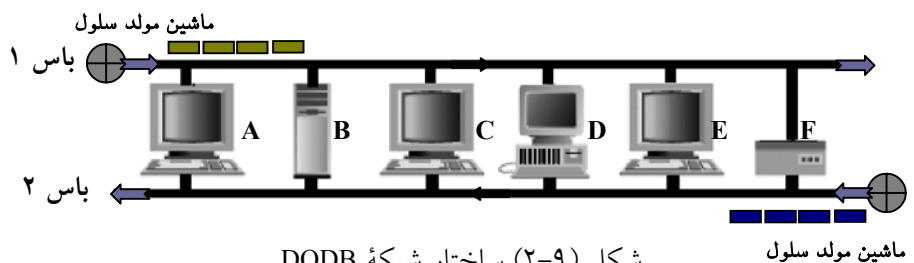
- سخت افزار کاملاً دیجیتال است و تصادم معنا ندارد.
- کابلهای زوج سیم تا فیبر نوری قابل استفاده می‌باشد.
- این استاندارد برای فریمها اولویت قائل است و می‌توان در اولویت بالا ارسال همزمان و بلادرنگ صوت و تصویر را ارائه کرد.
- فریمهای کوتاه قابل ارسالند بدون آنکه راندمان کانال بصورت بحرانی کم شود.
- راندمان در بار بالا بسیار عالی است. (نزدیک ۱۰۰٪)
- وجود ایستگاه ناظر درسیستم حساسیت حلقه را به آن ایستگاه افزایش می‌دهد. عملکرد بدِ[2] ایستگاه ناظر روی کل شبکه تاثیر می‌گذارد.
- در بار پایین مقداری تاخیر وجود خواهد داشت. (حداقل معادل زمان ۲٤ بیت)

[1] Real Time Systems
[2] Malfunctioning

۴) IEEE 802.6 - DQDB : استاندارد شبکهٔ بین‌شهری

هیچیک از استانداردهای IEEE که در بخشهای قبل معرفی شدند ، کارآیی لازم را برای بکارگیری در شبکه‌های بین‌شهری نداشتند. مسئلهٔ زیاد بودن طول کانال و تعداد بسیار زیاد ایستگاهها در شبکهٔ MAN ، تاثیر مخربی بر روی راندمان کانال دارد و باید برای چنین شبکه‌هایی ، استاندارد ویژه‌ای طراحی می‌شد.

با توجه به آنکه بهترین کانال انتقال برای شبکهٔ بین‌شهری فیبر نوری است ، لذا IEEE استانداردی به نام DQDB[1] که مبتنی بر دو رشته فیبر نوری است ، ارائه کرد. شبکهٔ مبتنی بر این استاندارد قادر است ناحیه‌ای به وسعت ۱۶۰ کیلومتر را با نرخ ارسال 44.736Mbps پوشش بدهد. در شکل (۹-۲) ساختار این شبکه به تصویر کشیده شده است. به گونه‌ای که دیده می‌شود دو رشتهٔ فیبر نوری که به هر کدام "باس" گفته می‌شود با طول بسیار زیاد ، ارتباط بین ایستگاهها را برقرار می‌کند. مسیر و جهت ارسال اطلاعات در هریک از این باسها یکطرفه است. در انتهای هر یک از باسها یک ماشین ویژه وجود دارد که بطور دائم ، سلولهای مشخص و ثابت ۵۳ بایتی تولید می‌کند. این ماشینهای تولید سلول ، در دو سمت مخالف به انتهای رشتهٔ فیبر متصل می‌شوند و برای هر فیبر فقط یک ماشین وجود دارد. تولید سلولها توسط یک ماشین خاص ، باعث می‌شود که علیرغم طول بسیار زیاد کانال و تاخیر انتشار ، ایستگاهها قادر باشند خود را با این سلولها سنکرون کرده و از لحاظ روال دسترسی به کانال مشکلی ایجاد نشود. سلولها در هنگام تولید ، خالی هستند و قادرند ٤٤ بایت داده را حمل نمایند. هر ایستگاه ضمن دریافت بیتهای سلول ، "بدون هیچ تاخیری" آنرا روی قطعهٔ بعدی فیبر تقویت و ارسال می‌نماید.



شکل (۹-۲) ساختار شبکهٔ DQDB

[1] Distributsed Queue Dual Bus

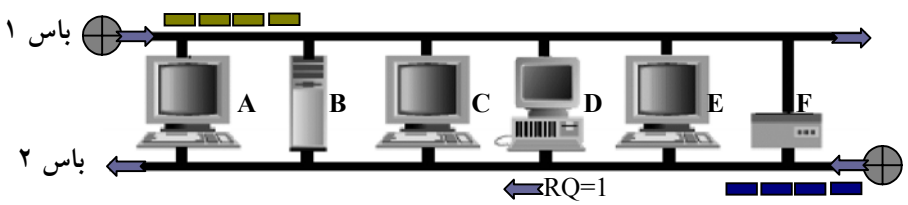
در هر سلول ، ۹ بایت ابتدایی سرآیند سلول هستند. در سرآیند هر سلول دو بیت کنترلی ویژه تعریف شده است که نام و عملکردشان به شرح زیر است:

- بیت اشغال **-Busy–** : در صورتی که این بیت ۱ باشد ، مشخص کنندهٔ آنست که سلول خالی نیست و محتوی داده می‌باشد. بدین معنا که سلول توسط ایستگاه دیگری که به ماشین تولید سلول نزدیکتر بوده پر شده است.
- **بیت تقاضا -Request–** : هرگاه ایستگاهی تقاضای ارسال داشته باشد ، با ۱ کردن این بیت ، تقاضای خود را اعلام می‌کند.

هر ایستگاه که تقاضای ارسال یک سلول دارد ، باید تشخیص بدهد که گیرندهٔ سلول (ایستگاه مقصد) در سمت چپ او واقع شده یا در سمت راست او قرار دارد؛ چراکه مسیر ارسال یکطرفه است و برای ارسال سلول به سمت چپ باید از یک باس و برای سمت راست از باس دیگر استفاده کرد. در شکل (۹–۲) اگر ایستگاه B برای D ارسال داشته باشد باید از باس ۱ استفاده کند در حالیکه برای ارسال از B به A باید از باس ۲ استفاده شود.

در این استاندارد روش ارسال یک سلول بر روی کانال ، زمانبندی FIFO[1] است و هر ایستگاه موظف است خودش را طبق الگوریتم زیر نوبت‌بندی کند:

- هر ایستگاه دارای دو عدد شمارندهٔ سخت‌افزاری است که در ابتدای کار صفر است. این دو شمارنده ، RC[2] و CD نام دارند. شمارندهٔ RC بر اساس ۱ بودن "بیت تقاضا" در سرآیند سلول افزایش می‌یابد یعنی هرگاه یک ایستگاه سلولی را انتقال بدهد که "بیت تقاضا" در آن یک باشد یک واحد به RC اضافه می‌کند ، بدین معنی که یک ایستگاه "بالادست"[3] تمایل دارد روی باس مخالف ، ارسال داشته باشد. به شکل (۱۰–۲) نگاه کنید. ایستگاه D با ۱ کردن بیت تقاضا در یک سلول که روی باس ۲ جریان دارد ، به A ، B و C اعلام می‌کند که تمایل دارد روی باس ۱ ، سلولی را ارسال کند. (مثلاً برای E یا F)



شکل (۱۰–۲) اعلام تقاضا به ایستگاه‌های بالادست

---

[1] First In First Out
[2] Request Counter
[3] Upstream

این کار برای آنست که ایستگاههای بالادست که به ماشین تولید سلول نزدیکترند ، سلولهای خالی را قبضه نکنند و به ماشینهای پایین‌دست نیز اجازه بدهند تا ارسال داشته باشند. دقت کنید که هر ایستگاه فقط می‌تواند تقاضای ارسال یک سلول را داشته باشد. وقتی شمارندهٔ RC در یک ایستگاه مقدار غیر صفر دارد ، به معنای آنست که ایستگاههایی تقاضای ارسال دارند. با ارسال هر سلول یک واحد از RC کم می‌شود چراکه قطعاً یکی از متقاضیان آنرا پر کرده و از صف خارج شده است.

ایستگاهی که تقاضای ارسال ندارد ، با کم و زیاد کردن شمارندهٔ RC جریان سلولها و تقاضاهای ارسال را تعقیب می‌کند.

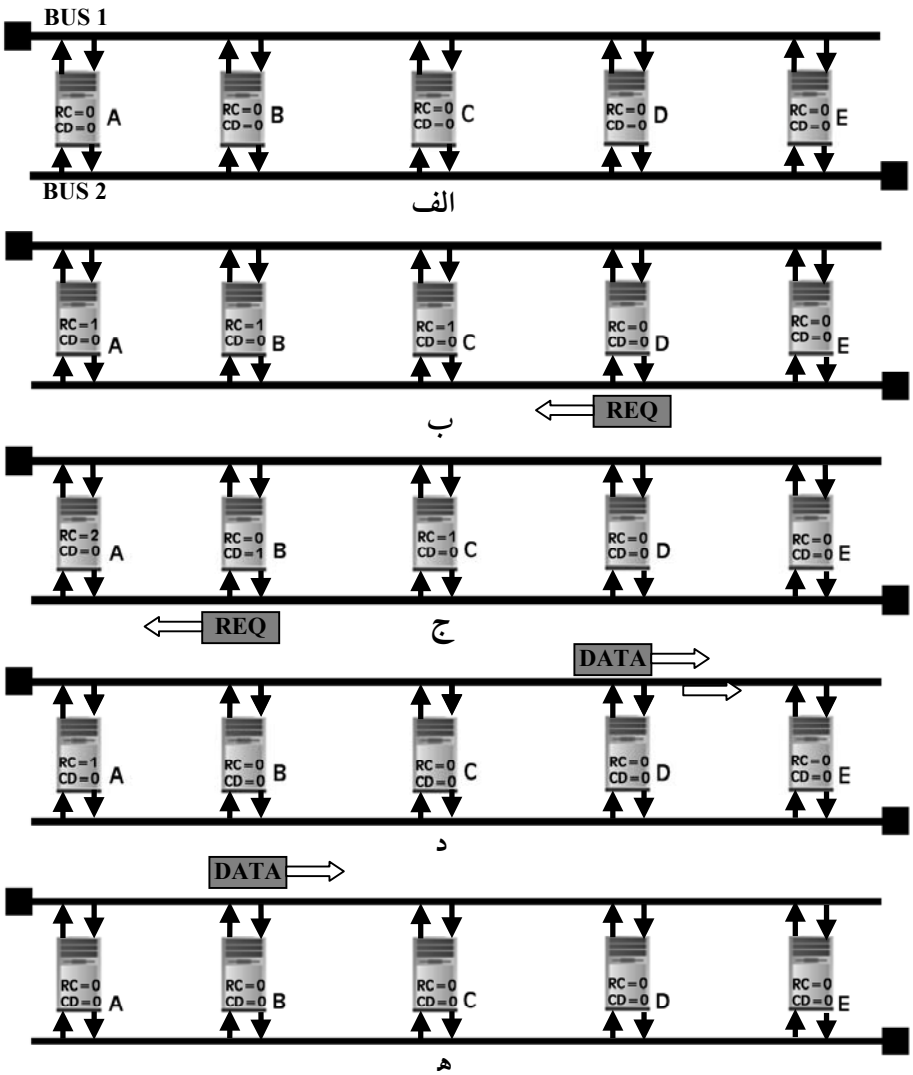
- به محض آنکه ایستگاهی تقاضای ارسال روی یکی از باسها داشته باشد و سلولی را روی باس مخالف دریافت کند که بیت تقاضا در آن صفر باشد ، آنرا ۱ کرده و با اعلام آن ، شمارندهٔ RC را در شمارندهٔ CD کپی کرده و RC را صفر می‌کند. این کار برای آنست که ایستگاه بداند در زمانی که او تقاضای ارسال را اعلام کرده ، چند ایستگاه قبل از او تقاضا داده‌اند و حق دارند زودتر ارسال کنند. پس از صفر شدن RC ، مقدار جدیدِ RC تقاضاهائی است که بعد از تقاضای ایستگاه ، اعلام شده است. با ارسال هر سلول روی باس یک واحد از CD کم می‌شود تا به صفر برسد. به محض صفر شدن CD ، نوبت ارسال ایستگاه فرا می‌رسد و با دریافت سلول خالی آنرا پر کرده و ارسال می‌نماید. به عنوان مثال اگر در لحظه‌ای مقدار CD=4 و RC=3 باشد به این معناست که در لحظهٔ اعلام تقاضا ٤ ایستگاه قبل از او تقاضای ارسال داده‌اند و ۳ ایستگاه نیز پس از او در صف هستند؛ بنابراین موظف است به اندازهٔ زمان ٤ سلول صبر کند تا نوبتش فرا برسد.

دقت کنید که ارسال روی یک باس فقط به مقصد ایستگاههای "پایین‌دست"[۱] مقدور است چرا که جریان سلولها بصورت فیزیکی یکطرفه است. چون تقاضا باید به اطلاع ایستگاههای بالادست برسد تا ایستگاه را در صف وارد کنند ، لذا باید روی باس مخالف اعلام شود.

مراحل فوق را با مثال شکل (۱۱-۲) بررسی می‌کنیم. در شکل (الف) همهٔ ایستگاه‌ها آزاد هستند و چون هیچیک از آنها تقاضای ارسال ندارند ، لذا تمام شمارنده‌ها صفر است. در شکل (ب) ایستگاه D روی باس مخالف به ایستگاههای بالادست خود ، اعلام تقاضا کرده است. ایستگاههای A ، B و C با دیدن این تقاضا ، شمارندهٔ RC خود را یک واحد افزایش داده و متوجه می‌شوند که ایستگاهی قبل از آنها تقاضا داده است. در شکل (ج) فرض شده که B نیز تقاضای ارسال داده و مقدار RC در ایستگاه A باز هم افزایش یافته است.

---

[۱] Downstream



شکل (۱۱-۲) نوبت‌بندی FIFO در استاندارد DQDB

در شکل (د) یک سلول خالی تولید شده و چون D زودتر تقاضا داده و شمارندهٔ CD صفر است ، بنابراین مجاز به ارسال می‌باشد. پس از ارسال تمام شمارنده‌های غیر صفر یک واحد کاهش می‌یابد. در شکل (ه) یک سلول خالی دیگر تولید شده و B مجاز به ارسال می‌باشد.

در این روش هیچ ایستگاهی قبل از آنکه شمارندهٔ CD صفر نشود ، حق ارسال ندارد و با این روال یک "صف توزیع شده"[۱] پیاده‌سازی می‌شود.

در استاندارد IEEE 802.6-DQDB روال تولید سلولها بسیار سریع است و در فواصل ۲۳ نانوثانیه‌ای یک سلول جدید تولید خواهد شد و چون تصادم در این روش معنا ندارد ، ایستگاهها با تاخیر نامعقول مواجه نخواهند شد. تنها ایرادی که می‌توان بر این استاندارد وارد کرد سرآیند ۹ بایتی هر سلول است که تقریباً ۱۷ درصد از پهنای باند مفید کانال را هدر می‌دهد.

شبکه‌های مبتنی بر این استاندارد در کشورهای زیادی مورد استقبال قرار گرفت و به عنوان شبکه بین‌شهری نصب و پیاده‌سازی شد.

۵) IEEE 802.11 – Wireless Lan : استاندارد شبکه‌های بی‌سیم

با پیشرفت تکنولوژی و همه‌گیر شدن کامپیوترهای شخصی و ظهور کامپیوترهای قابل حمل و نقل ، نیاز به یک ارتباط بی‌سیم احساس می‌شد؛ بهمین دلیل در دههٔ نود تحقیقاتی در این زمینه انجام شد و شبکه‌های محلی بی‌سیم با پیکربندی[۲] زیر توسعه یافتند:

- ایستگاههای متحرک (همانند کامپیوترهای کیفی[۳]) باید بتوانند در بُرد محدود (در حدّ چند ده متر) روی باند UHF ، داده‌ها را انتقال بدهند.
- در محدودهٔ پیاده‌سازی چنین شبکه‌ای ، باید تعدادی ایستگاه ثابت[۴] وجود داشته باشد. (ارتباط آنها نیز با ایستگاههای متحرک بی‌سیم است.)
- پهنای باند کانال بین یک تا دومگابیت بر ثانیه ، مطلوب خواهد بود.
- ایستگاههای متحرک دارای توان انتقال ثابت و محدودی هستند. (یعنی بُرد سیگنال تمام ایستگاهها یکسان است)

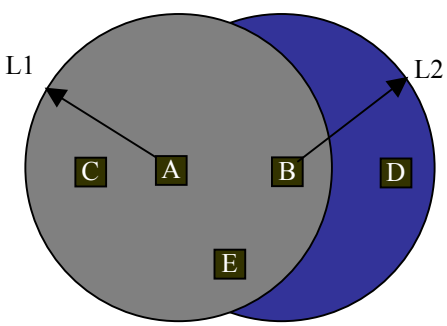
---

۱ Distributed Queue
۲ Configuration
۳ Notebook
۴ Base Station

- به دلیل پراکندگی تصادفی ایستگاهها ، فقط تعداد محدودی از ایستگاههای متحرک در محدودهٔ برد یکدیگر هستند.

هیچیک از استانداردهای IEEE مثل CSMA/CD یا Token Ring برای مدیریت کانال در چنین شبکه‌ای جوابگو نیست ، زیرا:
اولاً اکثر ایستگاهها متحرکند و مبادلهٔ توکن بین ایستگاههایی که زمانی در شبکه هستند و زمانی از شبکه خارج می‌شوند ، معقول نخواهد بود.
ثانیاً پراکندگی تصادفی و برد محدود ایستگاهها باعث می‌شود که نتوان از روشهای مبتنی بر گوش دادن به کانال استفاده کرد ، چراکه بسیاری از ایستگاهها بدلیل بعد مسافت ، سیگنال یکدیگر را نمی‌شنوند.

در استاندارد IEEE 802.11 ایستگاهها قبل از ارسال روی کانال ، باید عملیات "دست‌تکانی"[1] انجام بدهند. عملیات دست‌تکانی به منظور اطلاع دادن به ایستگاههای متحرکی است که در محدودهٔ برد یکدیگر هستند و می‌توانند عامل بروز تصادم باشند. مراحل عملیات دست‌تکانی با یک مثال تشریح می‌شود. به شکل (۱۲-۲) دقت کنید. در این مثال پراکندگی اتفاقی ایستگاهها نشان داده شده است. دایره‌های L1 و L2 ، محدودهٔ برد سیگنال منتشره از ایستگاههای A و B را مشخص کرده‌اند. در این مثال ایستگاه C بدلیل بُعد مسافت در محدودهٔ سیگنال ایستگاه B نیست؛ D هم در محدودهٔ ایستگاه A نمی‌باشد. حال فرض کنید ایستگاه A تمایل دارد برای ایستگاه B فریمی را ارسال کند. عملیات دست‌تکانی به شرح زیر است:



شکل (۱۲-۲) پراکندگی اتفاقی ایستگاهها در شبکهٔ بی‌سیم

[1] Handshaking

- قبل از ارسال ، A موظف است فریمی کوتاه (۳۰ بایتی) به نام RTS[1] را در محدودهٔ برد سیگنال خود ارسال نماید. درون این فریم ۳۰ بایتی ، آدرس گیرنده ، آدرس فرستنده و طول فریمی که قرار است ارسال شود ، مشخص می‌شود.

- در صورتی که B آماده برای دریافت باشد در پاسخ ، فریم کوتاه CTS[2] را منتشر می‌کند. هنگامی که A این فریم را دریافت کند ، اجازه دارد فریمش را ارسال نماید.

- اصل بر این است که هر ایستگاهی که سیگنال RTS را احساس می‌کند (یعنی قادر است سیگنال منتشره از A را بشنود) ، قاعدتاً به A نزدیک است و باید به مدت کافی صبر کند تا CTS بدون تصادم به A برگردد. (این زمان پس از اتمام ارسال فریم RTS ، تقریباً به اندازهٔ زمان لازم برای ارسال ۳۰ بایت است.)

- هر ایستگاهی که CTS را می‌شنود به B نزدیک است و باید به اندازهٔ مدت انتقال فریم داده صبر کند تا انتقال فریم تمام شود. (طول فریم در RTS و CTS به همهٔ ایستگاهها اعلام می‌شود و همه می‌توانند تخمینی از زمان انتقال فریم داشته باشند.)

در شکل (۱۲-۲) ایستگاه A فریمی را برای B آمادهٔ ارسال دارد ، بنابراین فریم RTS را ارسال می‌کند. چون C در حوزهٔ شنوایی سیگنال A قرار دارد ، RTS را می‌شنود ولی چون در حوزهٔ شنوایی B قرار ندارد ، CTS را نمی‌شنود و پس از تاخیری معادل ۳۰ بایت آزاد است برای ایستگاههای دیگر ارسال داشته باشد ، زیرا ارسال C به دلیل دور بودن از B منجر به تصادم نخواهد شد. ایستگاه D هر چند در حوزهٔ شنوایی A نیست و RTS را نمی‌شنود ولی قادر است CTS را بشنود. بنابراین حق ندارد تا ارسال کامل فریم توسط A ، ارسال داشته باشد چراکه ارسال از طرف D منجر به تصادم در ایستگاه B خواهد شد.

در این پروتکل وقوع تصادم فقط در حین ارسال فریمهای RTS و CTS محتمل است. هرگاه در هنگام ارسال این دو فریم تصادم رخ بدهد ، الگوریتم **"عقب‌گرد توانی"** که در استاندارد IEEE 802.3 معرفی شد ، اجرا می‌شود.

در استاندارد IEEE 802.11 اولاً توپولوژی شبکه ثابت نیست و با زمان تغییر می‌کند و بهمین دلیل ایستگاهها موظفند بطور متناوب اطلاعاتی را از وضعیت شبکه بدست آورده و در جدولی ذخیره کنند. ثانیاً برای برقراری ارتباط بین ایستگاههایی که در بُرد یکدیگر نیستند باید مسیریابی انجام شود.

---

[1] Request To Send
[2] Clear To Send

۶) مراجع این فصل

مجموعهٔ مراجع زیر می‌توانند برای دست آوردن جزییات دقیق و تحقیق جامع در مورد مفاهیم معرفی شده در این فصل مفید واقع شوند.

"Computer Networks" , Andrew S.Tanenbaum, Third Edition, Prentice-Hall, 1996.	
IEEE, "IEEE Standards for Local Area Networks: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications", IEEE, New York, New York, 1985.	
IEEE, "IEEE Standards for Local Area Networks: Token-Passing Bus Access Method and Physical Layer Specification", IEEE, New York, New York, 1985.	
IEEE, "IEEE Standards for Local Area Networks: Token Ring Access Method and Physical Layer Specifications", IEEE, New York, New York, 1985.	
IEEE, "IEEE Standards for Local Area Networks: Logical Link Control", IEEE, New York, New York, 1985.	
IEEE 802.3/ISO 8802-3 Information processing systems - Local area networks - Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications, 1993.	
RFC1661	The Point-to-Point Protocol (PPP). W. Simpson, Editor. July 1994.
RFC1663	PPP Reliable Transmission. D. Rand. July 1994.
RFC1717	The PPP Multilink Protocol (MP). K. Sklower, B. Lloyd, G. McGregor, D. Carr. November 1994.
RFC1042	Standard for the transmission of IP datagrams over IEEE 802 networks. J. Postel, J.K. Reynolds. Feb-01-1988.
RFC1230	IEEE 802.4 Token Bus MIB. K. McCloghrie, R. Fox. May-01-1991.
RFC1231	IEEE 802.5 Token Ring MIB. K. McCloghrie, R. Fox, E. Decker.
RFC1055	Nonstandard for transmission of IP datagrams over serial lines: SLIP. J.L. Romkey. Jun-01-1988.