زیرساخت شبکه "آقاخانی"

12 نمره نیمسال ترم

8 نمره میان ترم

2 نمره پروژه

- شبکه :

مجموعه ای از اشیا که با هم در ارتباط هستند و عمل انتقال بین آنها انجام می شود.

- شبکه های کامپیوتری:

مجموعه ای از کامپیوترهای مستقل و اجزای جانبی آن که با یکدیگر در ارتباط هستند و عمل انتقال داده بین آنها انجام می شود.

- کامپیوتر مستقل:

در خارج از شبکه هم کار می کند و اجزای خودش را دارد.

- host - workstation - nod:

پرسرعت افزاری است که بتوان IP روی آن set کرد.

(host) سرویس دهنده

(workstation) سیستم کامپیوتری ای که به شبکه وصل می شود.

- مزایای شبکه:

دسترسی زمانی آسان - به صرفه بودن هزینه - سرگرمی ها - انجام کارهای روزمره - قابلیت اطمینان -

- معایب شبکه :

پایین آمدن امنیت

دسته بندی های شبکه :

OS *

* محدودیت (محدوده ی تحت پوشش)

* توپولوژی

* کانال انتقال (نوع ارتباط)

• OS :

domain -

workgroup -

• محدوده تحت پوشش:

- PAN (گستردگی در حد چند متر)

(Personal area Network) مدیریت آن ساده است و از لحاظ هزینه ارزان و دارای امنیت بالا است قابلیت اطمینان آن به Backup خودمان دارد.

- LAN (گستردگی در حد یک ساختمان)

(Local Area Network) امنیت آن نسبت به PAN کم است و قابلیت اطمینان آن بالا است هزینه آن نسبت به PAN بیشتر است. مدیریت آن نسبت به PAN پیچیده تر است

- MAN (گستردگی در حد یک شهر یا کشور)

مدیریت آسان نسبت به LAN (Manipulation Area Network) امنیت بالاتر، هزینه بالاتر، قابلیت اطمینان بالاتر نسبت به (LAN)

- WAN (گستردگی در حد یک کشور یا چند کشور)

(wide Area Network) مدیریت پیچیده‌تر، قابلیت اطمینان بالاتر، امنیت پایین‌تر، هزینه بالاتر (نسبت به WAN)

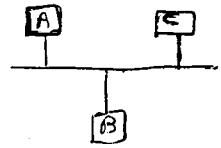
- GAN (گستردگی بین چند قاره)

(Global Area Network) امنیت پایین، هزینه بالا، مدیریت پیچیده، قابلیت اطمینان بالا (نسبت به WAN)

- توپولوژی:

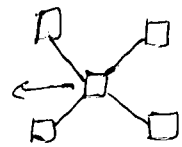
به چیدمان و ساختار شبکه workstation ها توپولوژی می‌گویند

- bus



راه‌اندازی ساده، مدیریت پیچیده، هزینه پایین، امنیت پایین، قابلیت اطمینان بالا.

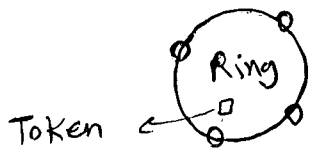
- star



computer یا server، switch، hub

امنیت بالا، قابلیت اطمینان بستگی به خطایی کدام سیستم دارد، مدیریت ساده، هزینه بالا.

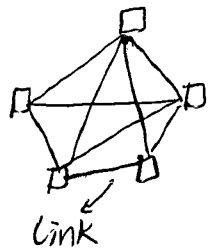
- حلقوی



هزینه پایین، مدیریت ساده (با استفاده از Token)، امنیت پایین

قابلیت اطمینان پایین

- Mesh (توری) (شبکه منظم)



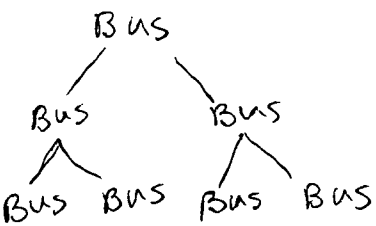
تعداد link = $\frac{n(n-1)}{2}$ n = تعداد node

قابلیت اطمینان بالا، امنیت بالا، هزینه بالا، مدیریت ساده

(هزینه بالا به دلیل زیاد بودن لینک)

اگر یکی از لینک های Mesh قطع شود، توپولوژی تا منظم نام می گیرد.

- درختی (Tree)

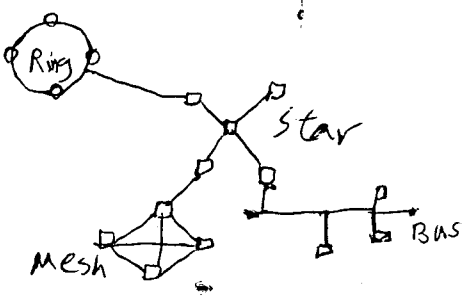


(یا یک توپولوژی دیگر)

امنیت پایین، هزینه پایین، قابلیت اطمینان پایین، مدیریت ساده

(شبکه ای به نوع توپولوژی کی (اصلی) آن دارد).

- ترکیبی



- پروتکل :

مجموعه قوانین و قواعدی است که برای انتقال داده در شبکه استفاده می شود.

- معماری شبکه :

ساختار و چیدمان شبکه کامپیوتری

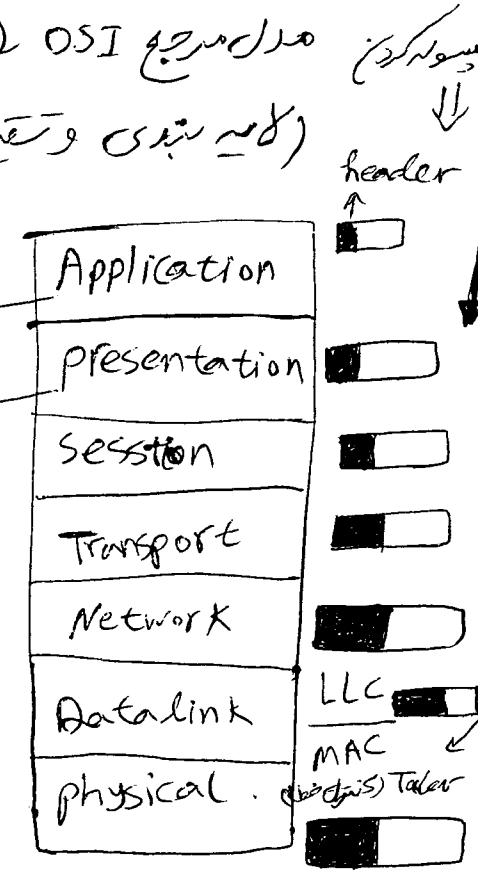
به مجموعه پروتکل ها و وظایفی که در هر لایه مشخص شده است.

- ISO (سازمان استاندارد سازی جهانی) :

مدل مرجع OSI را برای اصول نرم افزاری ارائه نمود.

(لایه بندی و تقسیم بندی وظایف در OSI) - مدیریت را ساده نمود.

خطایابی ساده تر - ایزوله کردن وظایف هر لایه (لایه ها روی هم تاثیر نمی گذارند)



- Application :

ارتباط مستقیم با کاربر دارد.

ارائه (فشرده سازی و برعکس) ، رمزنگاری و بازگشایی رمز ، مشخص کردن کدها ، مشخص کردن فرمت داده

(EBCDIC / ASSCI)

هر لایه با لایه ی بالاتر سرویس می دهد و لایه ی بالاتر سرویس می گیرد و خطای هر لایه به خودش مربوط است. (کپسوله سازی)

* به سه لایه ی اول ، message گفته می شود.
* به لایه ی چهارم ، segment می گویند.
* به لایه ی پنجم ، packet گفته شود.
* به لایه ی ششم ، frame گفته می شود.
* به لایه ی هفتم ، bit گفته می شود.

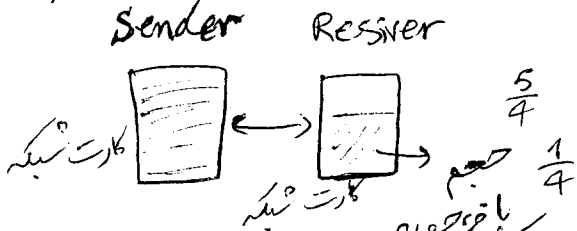
مجموعه ای از پروتکل ها که هر کدام از آنها با استفاده از نرم افزارهای خصوصی به خود به کاربران سرویس می دهند (http ، FTP ، SNTP ، telnet ، pop3 ، https)

- Session :

جلسه‌ای برای مشخص کردن اینکه کدام کامپیوتر، کدام اپلیکیشن با چه ارتباط برقرار کنند. مدیریت ارتباط در این لایه است. چون شناسی سیستم‌ها چیم می‌کند.

- Transport :

بسته‌ای ارتباطی را قطعه قطعه می‌کند و آنها را اسمبل می‌کند (اولویت و تحویل امن داده) کنترل خطا در ارسال بسته‌ها و کنترل جریان ارسال داده برای جلوگیری از بین رفتن اطلاعات. برقراری مدار مجازی (مداری) است که هم زمان، دو نفر هم می‌توانند از کانال ایجاد شده استفاده کنند.



ایجاد مدار و قطع و مدیریت

مدار او وظایف این لایه است.
پروتکل TCP در این لایه کار می‌کند.

- Network : (Connetion less) می‌شود

Router و Switch لایه 3 در این لایه کار می‌کند. آدرس‌یابی به صورت منطقی کنترل ازدحام و ترافیک. این لایه باعث برقراری شبکه، داده‌ها را ارسال می‌کند.

- Datalink :

مسیریابی (آدرس دهی) فیزیکی انجام می‌دهد. مدیریت لایه‌ی Physical را انجام می‌دهد. کارت شبکه، در لایه‌ی Datalink است.

MAC ← آدرس فیزیکی (24 بیتی)

LLC ← کنترل منطقی لینک

Logical link → Control

تحویل مرتب بسته‌ها با لایه‌ی بالایی (قطعه‌ها را شماره گذاری می‌کند $A_1, A_2, \ldots$) تا لایه‌ی Transport قطعه‌ها به ترتیب در کنار هم بچینند.

- Physical : نوع سیگنال (نوع ارتباط) را مشخص می‌کند. اطلاعات را به صورت 0 و 1 (در فیبر نوری) روی کانال قرار می‌دهد.

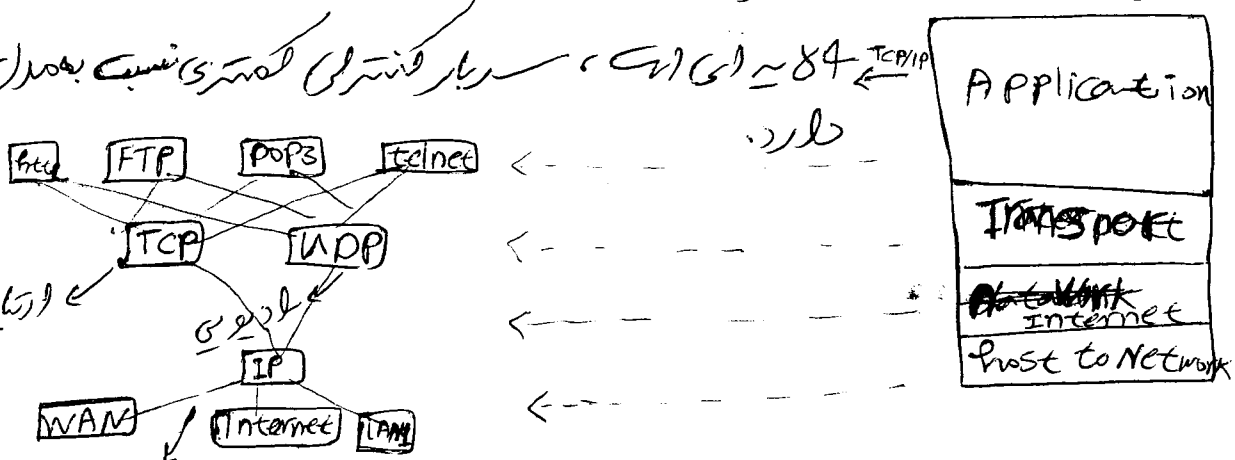
* ... سیستم مدل TCP/IP ...

- به خاطر سرعت بالا و هزینه کمتر به خاطر ترافیک بالا می‌رفت و سرعت ارسال بسته‌ها کمتر می‌آمد. (سرور کنترلی داده‌ها)، براساس Linux (opensource) و شرکت‌های دیگر برای سیستم عریض شرکت بر روی مدل TCP/IP سرعت گذاری کردند.

فلات دفاع آمریکا مدل TCP/IP چهارلایه‌ای را ارائه کرد تا با قطع در هر لایه، خللی در لایه‌های دیگر به وجود نیاید و بازدهی بسته‌ها توانست افزایش یابد.

در حال حاضر TCP/IP مدل استفاده می‌شود.

TCP/IP ← 4 لایه‌ای است، سرور کنترلی کمتری نسبت به مدل OSI دارد.



- شبکه براساس Client و Server کار می‌کند. (برای مثال Domain)

یک سرور برای مدیریت

- شبکه براساس peer to peer (نظیر به نظیر)

سرویس دهنده و سرویس گیرنده

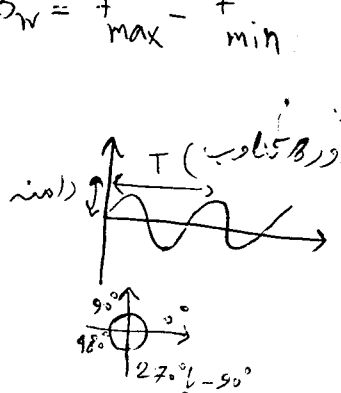
پروتکل R و RR در شبکه‌های workgroup کار می‌کند و یک بسته را به همه‌ی اعضا (سیستم‌ها) ارسال می‌کند و براساس آدرس MAC کار می‌کند.

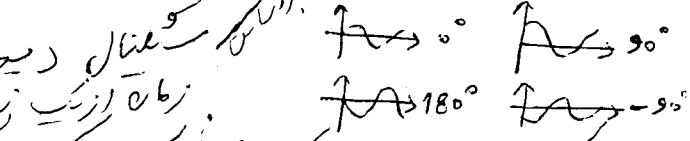
* انواع شبکه براساس چگونگی دسترسی به کانال
- point to point
- (Multipoint) Broadcast

- پهنای باند براساس سیگنال آنالوگ (حقیقی) و سیگنال دیجیتال

تفاوت پهنای باند سیگنال آنالوگ و دیجیتال: تعداد بیت‌هایی که در واحد زمان از یک نقطه به نقطه‌ی دیگر ارسال می‌شود.

$B_W = f_{max} - f_{min}$





(f) فرکانس: تعداد سیکل‌هایی کامل که سیگنال در یک ثانیه می‌زند. (Hz واحد آن)

$T = \frac{1}{f}$ فرکانس یا

فاز: زاویه‌ای که سیگنال با محور x ها می‌سازد.

* توان گذردهی کانال: ارتفاع، فاصله و ... روی آن تاثیر می‌گذارد (عملیاتی)
سرعت ارسال

محاسبه ظرفیت عملیاتی
- فرمول‌های ریاضی
- به صورت عملی استفاده می‌کنیم.

* توان عملیاتی اسمی:

* توان عملیاتی واقعی:

فاصله موثر است شرایط آب و هوایی در انتقال داده موثر است
نوع رسانه، Noise، سرویسی که ارائه سرویس می‌دهد و سرویس می‌گیرنده.
زمان، محتوای بیتی اطلاعات ارسالی.

(توان) ظرفیت محاسباتی (واقعی) کانال ← $C = 2B \log_2 m$ (فرمول نایکوئیست)

B: پهنای باند
m: تعداد سطوح سیگنال

مثال: اگر پهنای باند خط تلفن 4 کیلوهرتز باشد و فرستنده از 16 سیگنال مختلف برای ارسال داده استفاده کند، آنگاه پهنای باند یا توان عملیاتی (حداکثر تعداد بیت‌هایی که در واحد زمان) ارسال می‌شود را محاسبه کنید؟

$C = 2 \times 4 \times 10^3 \log_2 16$

$\rightarrow C = 2 \times 4 \times 10^3 \times \log_2 2^4$

$\rightarrow C = 2 \times 4 \times 10^3 \times 4 \times 10^2 \times \log_2 2$

$\rightarrow C = 32 \times 10^3$ bit/s

* قانون شانون: (قدرت سیگنال و Noise)
واحدکار برحسب W (وات) است

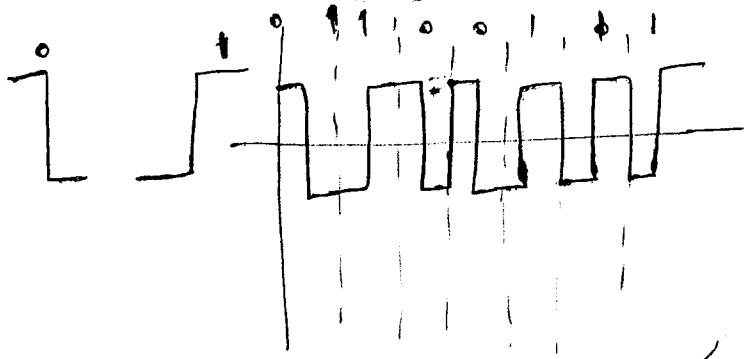
$C = B \log (1 + \frac{S}{N})$

Noise (برحسب وات W)

- تبدیل سیگنال آنالوگ به دیجیتال:
(مدالاسیون)

- تبدیل سیگنال دیجیتال به آنالوگ:
(مدالاسیون)

- داده دیجیتال ← سیگنال دیجیتال (منچستر) : رمزگذاری



در شبکه های کامپیوتر استفاده (رشته) می شود.

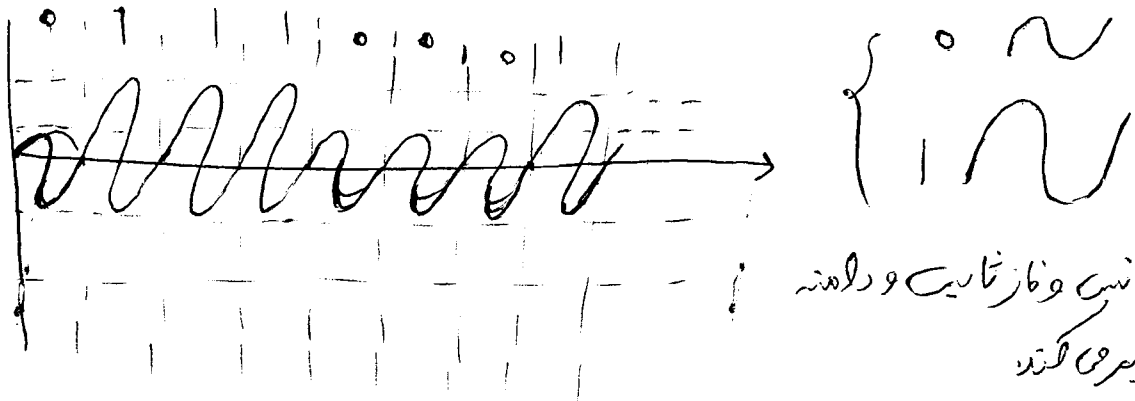
داده دیجیتال ← سیگنال آنالوگ

(دستگاه مودم این کار را انجام می دهد).

سیگنال { دامنه / فرکانس / فاز

* انواع روش های مدالاسیون:

1- تغییر دامنه (برای نمایش داده ای دیجیتال) : ASK



* فرکانس و فاز ثابت و دامنه تغییر می کند

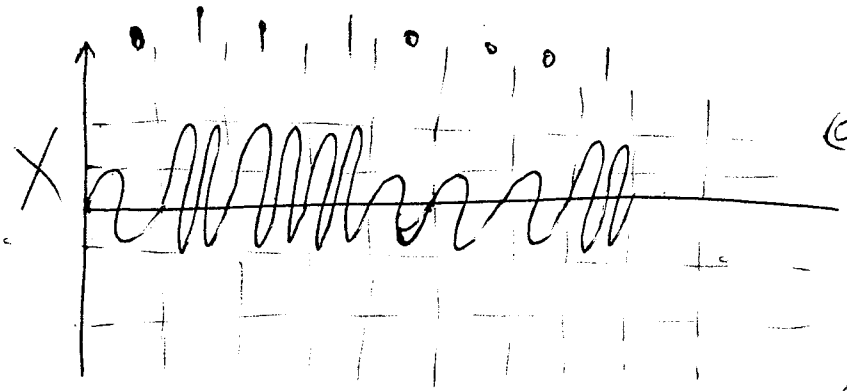
مثال: اگر پهنای باند خطوط تلفن ۴ کیلوهرتز باشد و قدرت Noise برابر با 1023 باشد آنگاه ظرفیت کانال (بهنای باند کانال) را بدست آورید.

$$C = 4\times10^3 \log(1+1023) \rightarrow C = 4\times10^3 \times 10 \log 2 \rightarrow C = 4\times10^4 \text{ (w)}$$

$1024 = 2^{10}$ ، $\log 2 = 1$ ، وات

2- تغییر فرکانس : FSK

(دامنه ثابت)

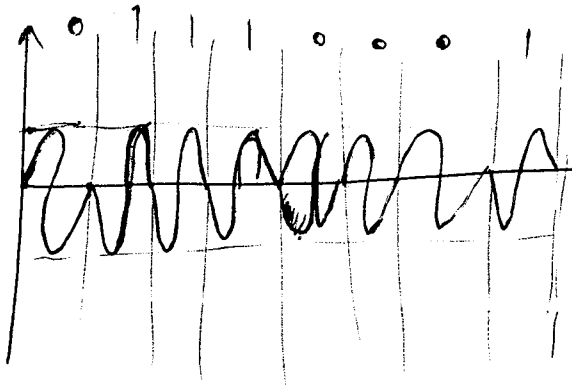


0 → 1Hz

1 → 2Hz

* دامنه و فاز ثابت و فرکانس تغییر می‌کند.

3- تغییر فاز PSK :



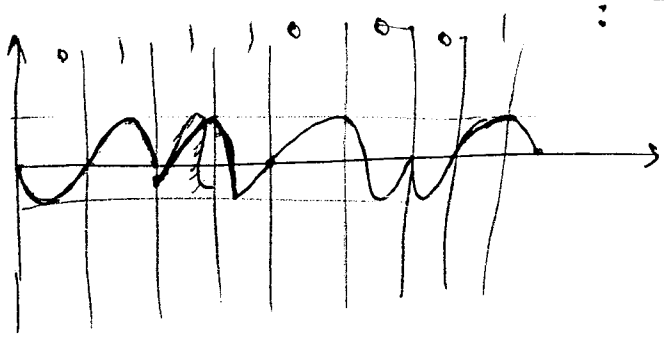
(1 بیت (داده)

0 → فاز 0°

1 → فاز 180°

فرکانس و دامنه ثابت و فاز تغییر می‌کند

4- 4PSK :



(تغییر فاز)

دامنه و فرکانس ثابت است.

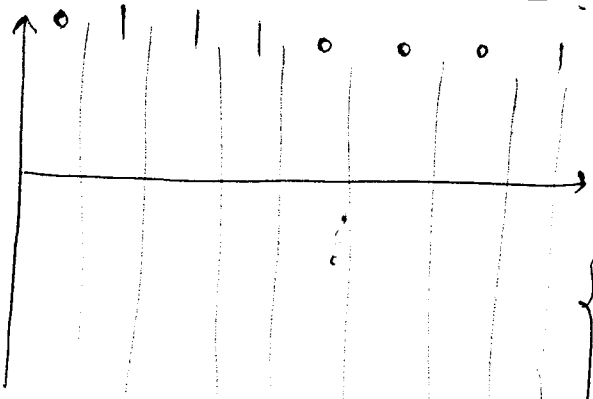
00 → فاز 0°

01 → فاز 180°

10 → فاز 90°

11 → فاز 270° = -90°

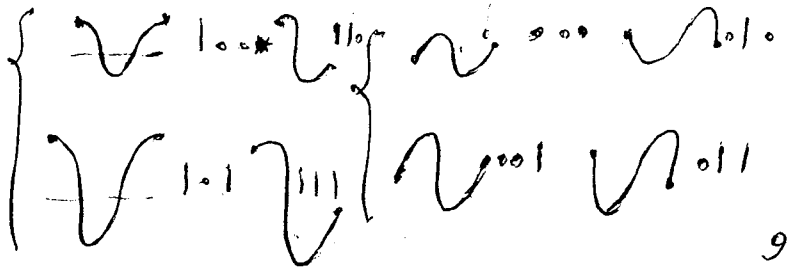
5- 8QAM : (2^3 3 بیت انتقال می‌یابد)



(در مودم کمپرس روش این گونه است)

(فرکانس ثابت)

دامنه و فاز تغییر می‌کند.



* 16 QAM

$2^{④}$ → تعداد بیت انتقالی

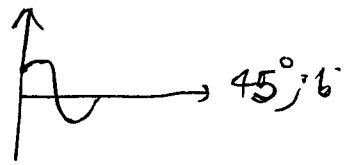
* 64 QAM

$2^{⑥}$ → تعداد بیت انتقالی

تعداد سطوح سیگنال ← ⓜ

* فرمول $\log_2^{M}$ = تعداد بیت‌هایی که هر سطح سیگنال می‌تواند انتقال دهد.

$\log_2^{64} = 6$



135° باز

225° باز

315° باز

$\log_y^{n} = p \rightarrow y^{p} = n$

نرخ Bond : تعداد سیگنال‌هایی که در واحد زمان ارسال می‌شود.

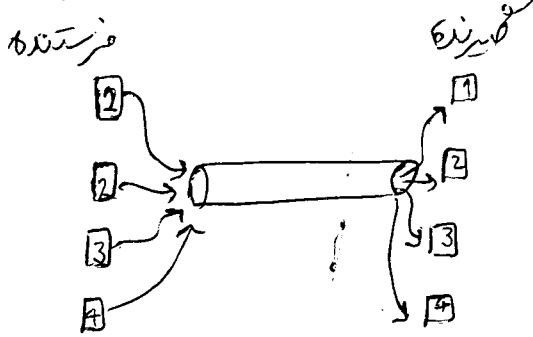
مثال- اگر از مدالاسیون 8QAM استفاده کنیم و نرخ بیتی ما برابر با 1200b/s باشد نرخ Bond را محاسبه کنید؟

$\log_2^{8} =$ ③ ← تعداد بیت‌ها

1200 bit $\Rightarrow \frac{1200}{3} = 400$ → تعداد بیت‌هایی که هر سیگنال می‌تواند انتقال دهد.

- Multiplexing :

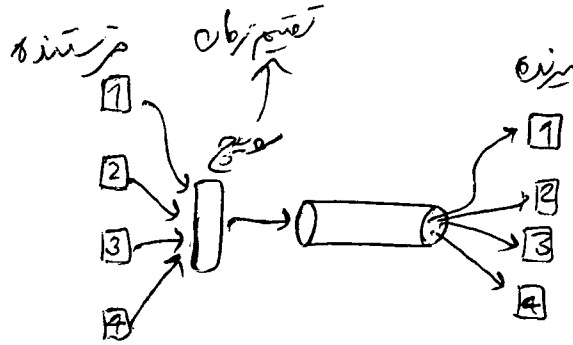
از یک کانال برای ارسال داده از بین چند منبع فرستنده استفاده می‌شود. (هم‌زمان یا غیر هم‌زمان)



* شبکه‌های TV از یک کانال با چندین فرکانس دریافت می‌شود.

: (Time Division Multiplexing) TDM -1

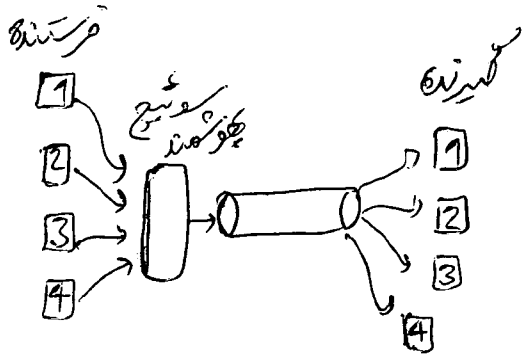
(برای ارسال داده)
تقسیم زمان



*عیب:
سوئیچ توانایی تشخیص نیاز زمانی فرستنده ها را ندارد بنابراین زمان را که به فرستنده‌ای بدون بیت

اختصاص می‌دهد حتی در صورتی که کانال به صورت بهینه استفاده نمی‌شود.

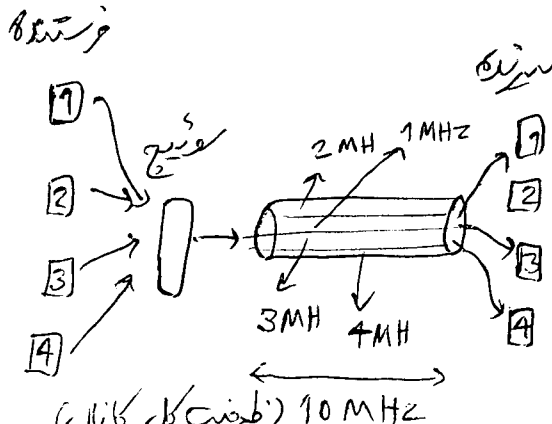
: (Satistical Time Division Multiplexing) STDM -2



از تقسیم زمانی هوشمند استفاده می‌کند.
یعنی از کانال به صورت بهینه استفاده می‌کند.

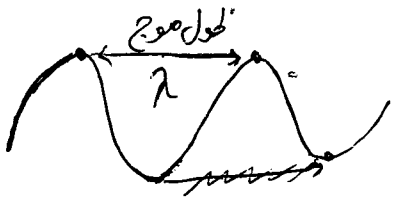
: (Fraquence Time Division Multiplexing) FTDM -3

تقسیم فرکانس قسمت‌های مختلف کانال



- طول موج: فاصله‌ی بین دو قله‌ی متوالی در یک سیگنال را می‌گویند.

4- WDM (Wave Division Multiplexing)



- هر فرستنده از یک طول موج خاصی استفاده می‌کند.
(فیبر نوری از نور روشن استفاده می‌کند)

* دوره تناوب: مدت زمانی که طول می‌کشد که طول موج یک سیکل کامل را بزند.

λ (طول موج) $= V \times T$
- V: سرعت
- T: زمان (دوره تناوب)

(یک سیکل کامل)

$$\Rightarrow \lambda = V * \frac{1}{f} \Rightarrow \lambda = \frac{V}{f} = \frac{3\times10^8}{f(Hz)}$$

سرعت نور

فرکانس 1 (در ثانیه) یک سیکل کامل زده است.

5- COM (Code Division Multiplexing)

* فرکانس صدای انسان 4 (KHz)

~~از یک فرکانس برای همه~~

از کدهای مختلف استفاده می‌شود که هر کدام به هر کدام قبلی عمود است که از بین نروند.

- انواع تکنولوژی کانال برای انتقال داده با توجه به جهت انتقال داده:

1- Simplex (مثل تلویزیون) کانال در یک زمان یا فقط فرستنده است یا گیرنده.

2- Halfduplex (مثل بیسیم) از کانال هم برای دریافت و هم برای ارسال استفاده می‌شود اما نه در یک زمان.

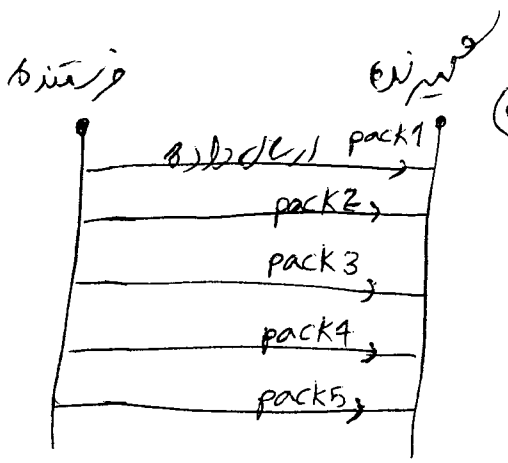
3- Full duplex (مثل موبایل) هم زمان از کانال برای دریافت و ارسال استفاده می‌شود.

وظایف لایه‌ی physical: مدالاسیون
نگهداشتن اطلاعات به صورت 0 و 1 روی کانال
مشخص کردن نوع سیگنال ارسالی (دیجیتال یا آنالوگ)

MAC (Media Access Control) (بالایی فیزیکی در ارتباطات) (مدیریت کانال را انجام می‌دهد).
LLC (Logical Link Control) (بالایه شبکه) (کنترل منطقی لینک در ارتباطات)

*وظایف:
1- کنترل جریان داده 2- کنترل دسترسی به رسانه
3- کنترل از دست رفتن داده 4- ارائه سرویس‌های ارتباطی به لایه شبکه

* سرویس‌های پیوند داده:



1- بدون اتصال بدون دریافت پاسخ (اینترنت یا رادیو)
2- با اتصال با پیغام پاسخ
3- بدون اتصال با دریافت پاسخ

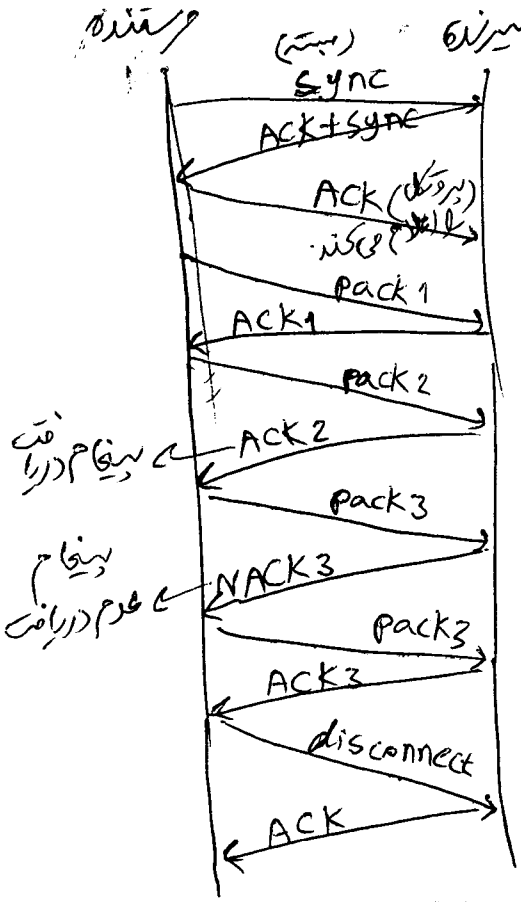
روش اول: قابلیت اطمینان کمی دارد ولی برای ارتباطات RealTime (online) مناسب است مثل رادیو، صفحات وب، تلویزیون و...
بهتر است در کانال‌های با قابلیت اطمینان بالا استفاده شود از جمله: کانال فیبر نوری. نرخ ارسال داده‌ی بالایی دارد. (مزیت)

روش دوم:

(مثل دستگاه فکس)

و تلفن.

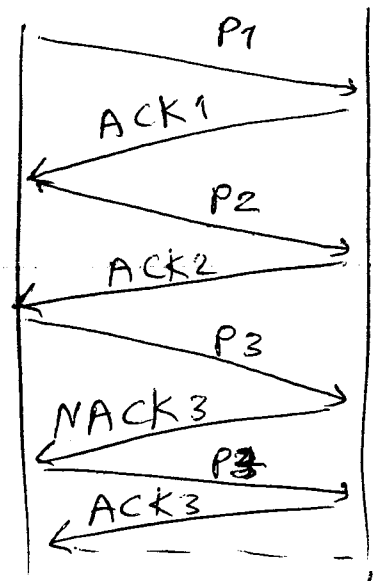
* قابلیت اطمینان بالاتر از روش سوم



روش سوم:

گیرنده

فرستنده



* قابلیت اطمینان بالاتر از روش اول

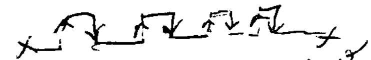
نرخ ارسال بالاتر از روش دوم

منبع: در شبکه‌های بی‌سیم قابل استفاده است.

— وظیفه‌ی لایه‌ی پیوند داده؟

- فریم‌بندی: (مشخص کردن ابتدا و انتهای یک بسته * یا تعدادی از بیت‌ها)

← روش‌های فریم‌بندی:

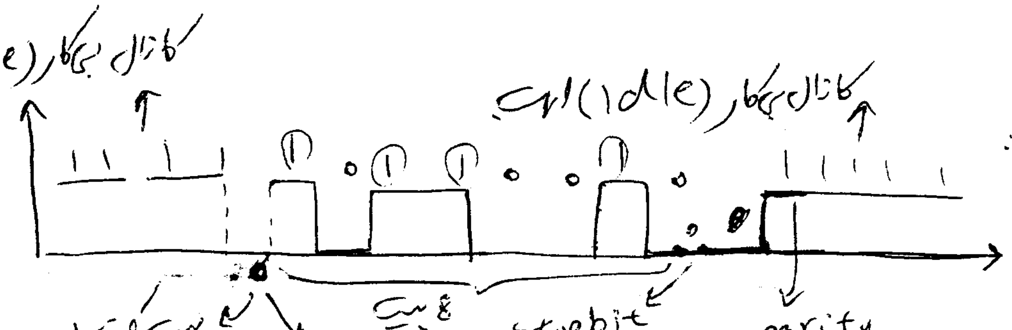


1- درج فاصله زمانی: گیرنده و فرستنده زمان ارسال و دریافت را مشخص می‌کنند. (مدت زمان ارسال)

2- استفاده از بیت‌های کنترلی (آسنکرون): هیچ چیزی برای ارسال و دریافت بین فرستنده و گیرنده قرار داده. هم‌زمان نیست.

3- استفاده از بایت‌های کنترلی ← آسنکرون / سنکرون

روش دوم:



سه بیت کنترلی (بعد از دریافت) بیت روی کانال، 8 بیت از روی کانال باید برداشته شود.

بیت parity = 0 چون قبل از آن (4) بیت یک داریم. زوج است، اگر فرد بود برابر با صفر می‌شد.

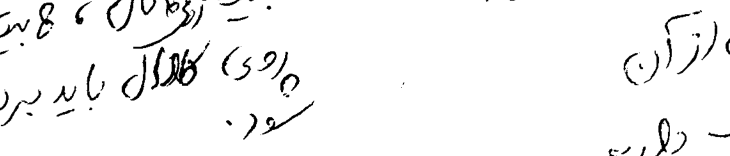
$$\text{بازدهی} = \frac{\text{تعداد بیت‌های مفید}}{\text{کل تعداد بیت‌ها}} \longrightarrow \text{بازدهی} = \frac{8}{11} \times 100 =$$

(درصد)

$$\text{سربار} = \frac{\text{بیت‌های کنترلی}}{\text{کل تعداد بیت‌ها}} = \frac{3}{11} \times 100$$

روش سوم:

— آسنکرون:



DLE ← فرستنده این بایت را قبل از بایت‌های داده‌ای که شبیه بایت کنترلی ETX است قرار می‌دهد تا نشان دهد

دهد که بعد بایت داده است فقط. و بعد آن DLE را حذف می‌کند و داده را ارسال می‌کند. و اگر بایتی شبیه DLE باشد قبل از آن DLE هم یک DLE قرار می‌دهد تا گیرنده بفهمد که منظور دهد که بعد DLE فقط داده است

نکته: در شبکه‌های اترنت، 1500 بایت می‌تواند ارسال کند روی کانال

- سنکرون:

استفاده از بایت‌های کنترلی سنکرون

در این روش از flag (پرچم) استفاده می‌شود. ارسال بیت می‌کند.

بیتی برای شروع و بیتی برای پایان ارسال داده.

بیت صفر

01111110	01111101	01111110

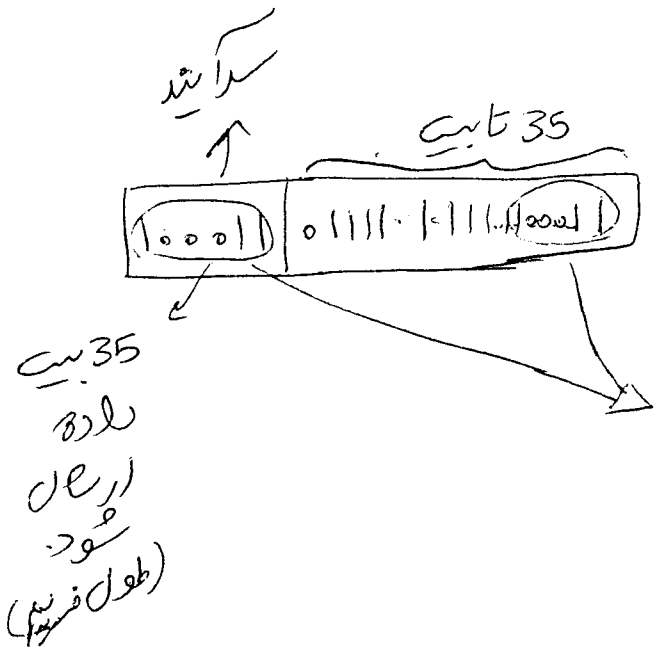
flag شروع — بیت‌های داده‌ای — flag پایانی

syn | STX | DLE | bitstuffing*

اگر بیت‌های داده‌ای شبیه flag باشد، قرار می‌دهیم که بعد از هر بیت یک صفر قرار داده و بعد از دیدن آن صفر را حذف کرده و بیت بعدی را داده به حساب بیاورد (بیت ششم برابر با صفر می‌شود).

نکته: اگر flag پایان داده‌ای (بیت صفر) در وسطش شود (یعنی خراب شود) از بیت syn، داده‌ی بعدی متوجه می‌شود که این flag اصلی نیست بایت داده‌ای و بعد گیرنده بفرستنده می‌گوید که فریم‌بندی را از اول انجام بدهد.

4- قرارداده طول فریم در سرآیند بسته:



اگر بیت‌های قرارداده شده در سرآیند شبیه قسمتی از بیت‌های داده‌ای ارسال شده شود فقط تا همان جا بیت منتقل می‌شود و مقداری از داده‌ها ارسال نمی‌شود.

5- ترکیبی از روش‌های قبل

* وظیفه‌ی دیگر لایه‌ی پیوند داده؟

← کنترل خطا:

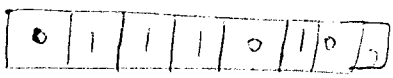
1- کشف خطا و تشخیص خطا

2- تصحیح خطا (چیزی که در لایه‌ی پیوند داده معمولاً انجام نمی‌گیرد)

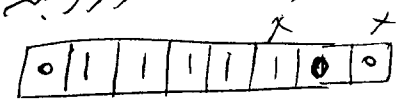
از کد hamming برای این منظور در کانال‌های ماهواره‌ای (که برای ارسال داده‌ها است) جهت تصحیح خطا استفاده می‌گیرد.

* parity bit → odd (تعداد یک‌ها فرد)

even (تعداد یک‌ها) بیت‌های یک ارسال شده زوج



دو بیت خطا دار در بسته ی ارسالی



۸ بیت یک

طبق بسته ی صفحه ی قبل در این بسته ی مقابل خطا صورت گرفته است چون تعداد بیت های یک فرستاده شده زوج نیست.

۶ بیت یک

خطا صورت گرفته است ولی قابل تشخیص در روش parity bit نمی باشد. در واقع خطاهای فرد را در این روش می توان تشخیص داد ولی خطاهای زوج را نمی توان تشخیص داد.

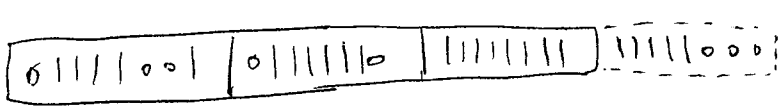
روش تشخیص خطای Check SUM :

از جمع مقابله ای استفاده می کند

بایستی با هم جمع می کند و نتیجه ی آن را در انتهای آن عبارت دهدو بعد

طبق زیر عمل می کنیم:

Check sum



(1) 0 1 1 1 1 0 0 1

(2) 0 1 1 1 1 1 1 0 +1

(3) 1 1 1 1 1 1 1 1

(+) نتیجه ی 1 1 1 1 0 0 0

1 ⊕ 0 = 1

0 ⊕ 1 = 1

1 ⊕ 1 = 0

0 ⊗ 0 = 0

XOR

1 ⊕ 2 ⊕ 3 ⊕ 4 XOR ⟹ نتیجه = 0 0 0 0 0 0 0 0 ⟹ چون خطا نداریم. نتیجه صفر شده است ✓

* نکته:
مراحل تشخیص خطا در کارت شبکه بصورت می گیرد.

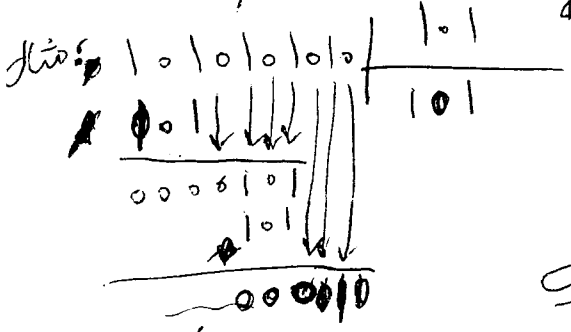
3- روش CRC برای تشخیص خطا:

از تقسیم شبکه ای استفاده می کند توافقی بین گیرنده و فرستنده با استفاده از بایت Generator.

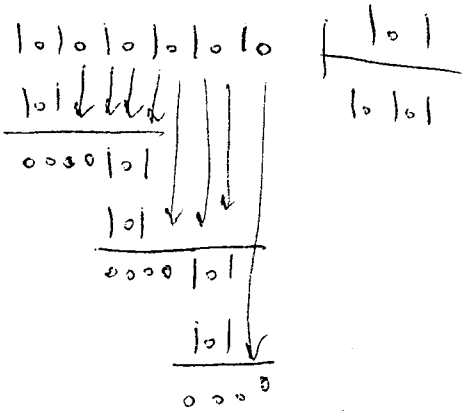
چند جمله ای مولد (Generator) ←

چند جمله ای داده

مثال:



خرستنده کد CRC (باقی مانده) ایجاد می کند که معمولاً یک بیت کمتر از بایت Generator است. اگر کد CRC + چند جمله ای داده شود و دوباره بر Generator بایت تقسیم شود و باقی مانده برابر با صفر شود متوجه می شویم که خطایی رخ نداده است.



نکته: ابتدا و انتهای بایت Generator نباید صفر باشد به همین دلیل کدهای خاصی تعبیه شده است

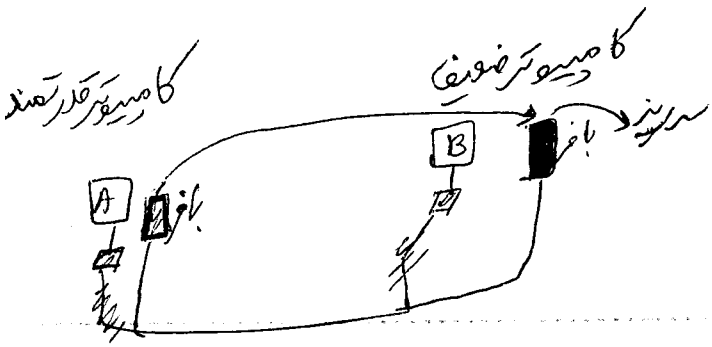
مثال برای آدرس گیرنده CRC:

1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1

- وظیفه ی دیگر لایه ی پیوند داده؟

- کنترل جریان داده :

اگر کامپیوتر گیرنده با بافری مشخص باشد در مرحله ی ارسال داده به یک گیرنده ممکن است سرریز صورت گیرد. در نتیجه فرستنده پیغامی مبنی بر توقف بودن بافر گیرنده ارسال می کند.

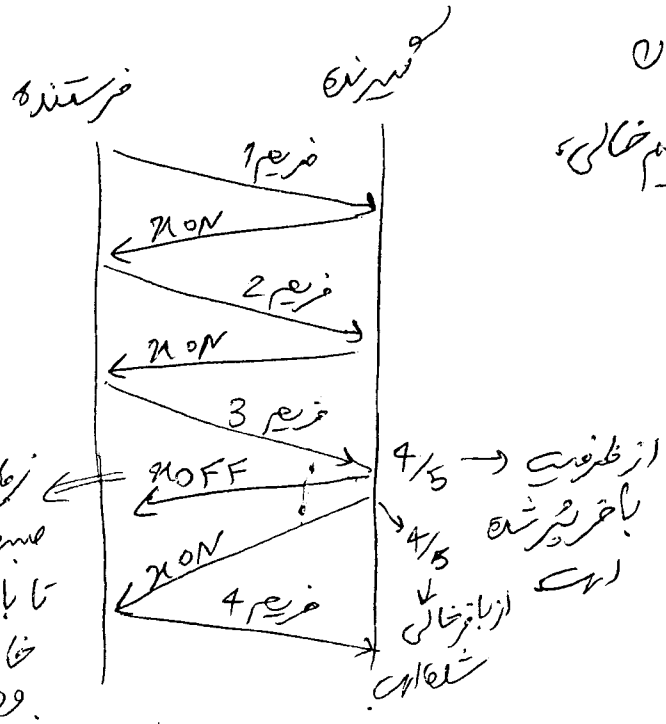


① کنترل جریان نرم افزاری:

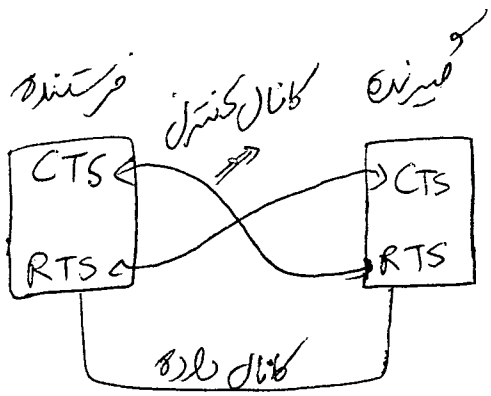
با استفاده از سگنال هایی که در کانال رد و بدل می شود تا از ارسال بیش از ظرفیت بافر گیرنده، جلوگیری کند. داده بفرست ← XON

داده نفرست ← XOFF

فرستنده XOFF شده کانال، کانال بی کار نمی ماند هم چنان فریم ارسال می کند ولی فریم خالی، ارسال می کند.



② کنترل جریان سخت افزاری:



داده ارسال شده ↑ و باقر دریافت می‌کند RTS=1 CTS=1

| RTS=1 | → باقر 4/5 پر شده است.
| CTS=0 |

RTS=0	RTS=0
CTS=1	CTS=0 ↘

← باقر خالی است ولی داده‌ای برای ارسال نیست

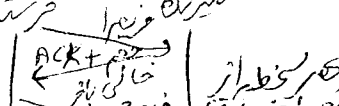
نه داده‌ای برای ارسال است و نه باقر ظرفیتی برای دریافت داده دارد.

* نکته: اصلی روش (کنترل جریان سخت افزاری) هزینه بر است و سرعت پایین‌تری نسبت به روش کنترل جریان نرم افزاری دارد.

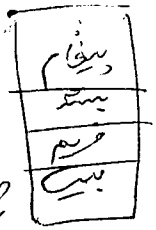
در ضمن در این روش، پیغام‌های کنترلی هم دست فرستنده است و هم دست گیرنده ولی در روش کنترل جریان نرم افزاری پیغام‌های کنترلی فقط گیرنده صادر می‌کند.

* نکته ③: روش "slow start" در گام‌های انتقال صورت می‌گیرد در صورتی که بیتی drop شده باشد به عقب برگشته و دوباره ارسال می‌کند.

نکته ④: در روش کنترل جریان نرم افزاری علاوه بر ارسال فریم (اندازه‌ی حجم خالی فریم ارسال می‌کند.



* مزیت: فرستنده در هر گام بیش از حجم خالی فریم داده ارسال نمی‌کند.



* کنترل جریان نرم افزاری در لایه‌ی انتقال:

- مدیریت کانال:

مدیریت دسترسی فرستنده‌ها به کانال در شبکه‌های Broadcast و نقطه به نقطه

کنترل جریان و ازدحام باید صورت پذیرد.

نوع اول: نقطه به نقطه:

نوع دوم: همه‌پخشی:

توضیح نوع اول (نقطه به نقطه):

روش اول ← Stop & wait (IQELARQ)

روش دوم ← Go back N

روش سوم ← Selective Reject

فرستنده گیرنده

فرستنده بسته ۱ به گیرنده می‌فرستد و زمانی که گیرنده پاسخ دریافت بسته ۱ به فرستنده را داد، فرستنده بسته ۲ را ارسال می‌کند.

فرستنده گیرنده

فرستنده بسته‌ها را ارسال می‌کند و گیرنده هم‌زمان پیغام ACK یا NACK را به فرستنده می‌دهد و در صورت دریافت پیغام NACK، فرستنده بسته را ارسال می‌کند.

22 دقیقه

فرستنده گیرنده

فرستنده بسته‌ها را ارسال انجام می‌دهد و گیرنده هم ACK می‌دهد و هرزمان که NACK یا خطا در بسته‌ها فرستنده به همان بسته‌ی NACK داده شده بازگشته و ارسال را دوباره از آن جا شروع می‌کند.

برای شبکه‌هایی با خطای زیاد مناسب نیست.

دوباره فرستنده، ارسال انجام می‌دهد و اگر پاسخی دریافت نکند، بسته را دوباره ارسال می‌کند.

برای شبکه‌ای که بیم آن قابلیت اطمینان پائینی دارد مناسب است و کارایی آن پایین است.

مقایسه ی سه روش مدیریت کانال:

روش اول کارایی پائینی دارد نسبت به روش دوم و روش سوم کارایی بالاتری نسبت به هر دو روش دارد. روش اول از کانال half duplex ، روش دوم و روش سوم از کانال full duplex استفاده می کند. باقر فرستنده در روش سوم نسبت به دو روش قبل باید ظرفیت بالاتری داشته باشد تا بتواند ترتیب بسته ها در ارسال را حفظ نماید. 1. در هر سه روش قابلیت اطمینان بالا است چون هر سه روش کنترل خطا را انجام می دهند. 2. این سه روش از لحاظ کارایی به ترتیب روش سوم بالاتر، روش دوم و روش دوم بالاتر از روش اول است. 3. در روش اول به دلیل اینکه کانال برای ارسال فریم مدت زمانی را صبر می کند تا تصدیق (ACK) بسته قبلی را دریافت کند کانال به صورت بهینه استفاده نمی شود. در روش دوم نیز به دلیل اینکه

* کانال ها از لحاظ جهت استفاده به 3 دسته تقسیم می شوند:

1- Simplex (کانال یک جهته است یا فقط ارسال داده می کند یا فقط دریافت داده می کند). شبکه ی TV

2- half duplex (کانال هم می تواند فرستنده باشد هم گیرنده ولی نه در یک زمان) شبکه ی بیسیم

3- full duplex (کانال در هر لحظه هم گیرنده است و هم فرستنده) شبکه ی تلفن

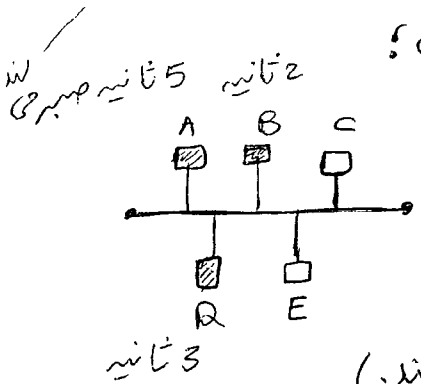
با خراب بودن یک بسته، تمام بسته های ارسال شده بعد از آن، مجدداً ارسال خواهند شد کارایی اگر از روش سوم پائین تر است یعنی اینکه مقداری از ظرفیت کانال صرف ارسال بسته های تکراری می شود.

4. روش اول از کانال half duplex و دو روش دیگر از کانال full duplex استفاده می کنند. 5. اندازه ی Buffer در فرستنده ی روش اول و دوم می تواند به اندازه ی یک باقر باشد. اما در روش سوم اندازه ی باقر فرستنده، دو در نظر گرفته می شود.

زیرا در دو روش اول و دوم، ترتیب ارسال فریم ها و دریافت فریم ها حفظ می شود ولی در روش سوم، اگر یک فریم خطا دار باشد، آن گاه گیرنده از فرستنده درخواست ارسال مجدد آن را می نماید به همین دلیل تا دریافت صحیح بسته، گیرنده بایستی دیگر بسته های دریافتی را در بافر به صورت صحیح ذخیره کند زیرا این بسته ها دیگر، ارسال مجدد نخواهند شد پس از اینکه همه بسته ها به ترتیب دریافت (دریافت شدند لایه ی پروتکل داده ی گیرنده، تمام بسته هایی دریافت شده را به صورت مرتب به لایه بالاتر (لایه شبکه) تحویل می دهد.

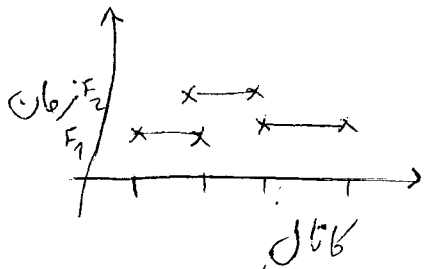
* روش های دسترسی به کانال به صورت پخش همه:

1- CSMA:



(همه ی فرستنده و گیرنده ها در این کانال باید به صورت یکسان به کانال دسترسی داشته باشند.)

همان طور که قبلاً بیان شد یکی از روش های دسترسی به کانال پخش همگانی است. در این روش از یک کانال اشتراکی برای ارسال داده بین چند فرستنده و چند گیرنده استفاده می شود. از آنجایی که باید کانال به صورت عادلانه بین فرستندگان



* الوهای زمان دسترسی به کانال در هر زمان را مشخص می کنند.

برای ارسال تقسیم شود، مدیریت این نوع کانال پیچیده است چرا که همه‌ی همه‌ی گامپیوترها، از یک کانال برای ارسال استفاده می‌کنند و این باعث می‌شود که تصادم (برخورد) در کانال زیاد باشد و در نتیجه کارایی کانال پائین می‌آید. یکی از روش‌ها برای مدیریت این نوع کانال، "مدیریت به صورت آشتا" می‌باشد. که این روش از همان تکنیک Multi plexing استفاده می‌کند یعنی برای هر کانال یک سیگنال الکترومغناطیسی از تقسیم کانال و برای کانال‌ها مانند فیبر نوری که از نور استفاده می‌کند از تقسیم طول موج WQM → wave → Multiplexing ↓ Division یا کدهای عمود برهم CDM → Multiplexing ↓ code ↓ Division استفاده می‌شود.

"مدیریت به روش نوبتی": در این روش، زمان در اختیار گرفتن کانال برای فرستنده‌ها به صورت متغیر است به عبارت دیگر فرستنده‌ها برای استفاده از کانال با یکدیگر رقابت می‌کنند. در این روش اگر دو فرستنده هم زمان به کانال دسترسی پیدا کنند اطلاعات شما با یکدیگر تداخل پیدا کرده و در نتیجه از بین می‌رود به همین دلیل برای اینکه بتوانند ارسال داده انجام دهند دوباره باید برای دسترسی به کانال با یکدیگر رقابت کنند (مدت زمان تصادفی‌ای صبر می‌کنند تا کانال خالی شود).

البته اگر از تکنولوژی Token استفاده شود در این صورت زمان استفاده از کانال بدون به وجود آمدن تصادم بین فرستنده ها تقسیم می شود.

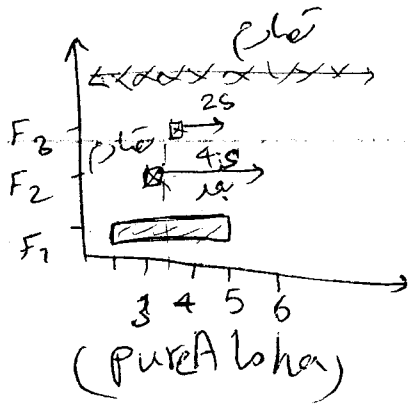
نکته: در تمام این روش ها فرستنده فقط یکی است ولی گیرنده می تواند چندتا باشد.

دسترسی کانال به صورت

- تعدادی از روشهای پخش همگانی به صورت زیر است:

Aloha-1

* تصادم در کل طول کانال رخ دهد

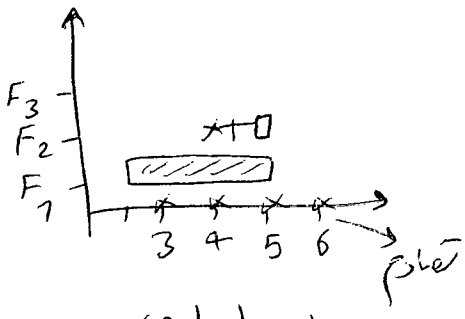


(pureAloha)

در هر لحظه که تصادم رخ می دهد فرستنده مدتی صبر می کند و بعد ارسال را انجام می دهد.

pureAloha-2 :

تصادم ممکن است در طول کانال رخ دهد. و کانال بخش بندی شده است تا کمتر تصادمی رخ دهد.



(Aloha)

توضیح Pure Aloha (TDM) :

① هر ایستگاه، هر وقت نیاز به ارسال داده داشته باشد، همان لحظه بدون اینکه کانال را بررسی کند، ارسال داده را انجام می دهد در صورتی که بیش از یک فرستنده در یک زمان تصمیم به ارسال داده داشته باشند تصادم رخ می دهد در غیر اینصورت فرستنده، داده‌ی خود را بروی کانال انتقال می دهد.

② - پس از اتمام ارسال، فرستنده دوباره به کانال گوش می دهد و در صورت کشف برخورد، یک مدت زمان تصادفی برای ارسال داده صبر می کند. کانالی را که در مرحله‌ی دوم گوش می دهد کانالی است به جز کانال ارسال داده و در واقع کانالی است که feed back ارسال داده را (تصادم داده) مشخص می کند.

③ - فرستنده، مراحل ① و ② را آنقدر انجام می دهد تا موفق به ارسال داده شود.

+ در این روش از کانال به صورت بهینه استفاده نمی شود چون اتلاف زمانی داریم. (در این روش با توجه به اینکه برخورد اطلاعات یا برخورد فریم های ارسالی زیاد می باشد کارایی کانال کاهش می یابد).

+ مزیت - (TDM) همانند است.

- توضیح sloted Aloha : (STDM)

در این روش کانال به اسلایدهای زمانی تقسیم می‌شود و شروع این اسلایدهای زمانی به همه‌ی فرستنده‌ها (سیستم‌ها) ارسال می‌شود، هم‌چنین حداکثر مدت زمانی که یک فرستنده می‌تواند از کانال استفاده کند یک اسلاید زمانی است. مراحل به شرح زیر است:

① هر فرستنده، هر زمان نیاز به ارسال اطلاعات داشته باشد، صبر می‌کند تا به شروع یک اسلاید زمانی برسد بدون اینکه کانال را بررسی کند

② اگر پیش از ارسال با گوش دادن به کانال feedback، تداخل را کشف کرد یک مدت زمان تصادفی صبر می‌کند.

③ مراحل ① و ② آن‌قدر تکرار می‌شود تا داده‌ی فرستنده ارسال شود.

+ مزایا: این روش همانند روش (STDM) و یا (STDM) این روش عمل می‌کند. این روش در ماهواره‌ها و ایستگاه‌های زمینی استفاده می‌شود. در واقع ایستگاه زمینی برای ارسال اطلاعات یک اسلاید زمانی را صبر می‌کند و در شروع اسلاید، اقدام به ارسال اطلاعات می‌کند و اگر دو ایستگاه به صورت هم‌زمان اقدام به ارسال کنند، تصادم رخ می‌دهد.

- مقایسه‌ی روش Slotted Aloha و pure Aloha:

SAloha نیاز به هم‌زمان‌سازی سراسری برای تمام ایستگاه‌ها دارد.

اما PAloha نیازی به این کار ندارد به همین دلیل در روش SAloha، تصادم کمتر رخ می‌دهد. زیرا که تصادم در SAloha فقط در شروع اسلات‌های زمانی رخ می‌دهد درحالی‌که در روش PAloha در هر لحظه امکان دارد، تصادم رخ دهد، پس می‌توان گفت کارایی SAloha بالاتر است.

* ادامه‌ی روش‌های دسترسی به کانال (چند دهنده)

- CSMA/CD (Carrier sense Multi Access / Collision Detect) (در شبکه‌های اترنت)

در این روش مراحل ارسال فریم از طرف فرستنده به گیرنده به شکل زیر است:

1- ابتدا فرستنده به کانال گوش می‌دهد یا به عبارت دیگر ابتدا کانال را بررسی می‌کند و در صورت اشغال نبودن کانال، فریم را بر روی کانال قرار می‌دهد.

2- در هنگام ارسال (یا هنگام sense کردن) اگر تداخل به وجود آید فرستنده یک مدت زمان تصادفی صبر کرده و سپس مجددا مرحله 1 را انجام می‌دهد.

3- مراحل بالا آنقدر تکرار می‌شود تا داده به مقصد برسد. این پروتکل (الگوریتم) در صورت اشغال بودن کانال به صورت مصر عمل می‌کند.

Carrier Sense Multi Access / Collision Avoidance) CSMA / CA

(در شبکه‌های بی سیم یا وایرلس)

(RTS) فرستنده به گیرنده می دهد و CTS گیرنده به فرستنده می دهد. RTS شامل مدت زمان اشغال بودن کانال و کد CRC می باشد و CTS شامل مدت زمان اشغال بودن کانال و بیتی در پاسخ می باشد.) کامپیوترهای در شبکه‌های بی سیم برای دسترسی به کانال با یکدیگر و جلوگیری از تصادم با یکدیگر رقابت می کنند. برای کاهش احتمال برخورد در شبکه‌های بی سیم (802.11) به صورت زیر عمل می شود:

1- ابتدا فرستنده قبل از ارسال فریم به کانال گوش می دهد، سپس اگر کانال مشغول باشد، یک مدت زمان تصادفی صبر می کند.*

2- در صورتی که کانال خالی باشد فرستنده، یک پیام کنترلی RTS (Ready To Send) را که شامل آدرس مبدأ، آدرس مقصد، مدت زمان استفاده از کانال و الگوریتم کنترل خطا (مکانیزم کشف خطا) می باشد به گیرنده ارسال می کند.

3- ایستگاه گیرنده در صورتی که کانال خالی باشد و اینکه تصادفی صورت نگرفته باشد (یعنی فریم RTS بدون خطا دریافت کرده باشد) توسط ارسال فریم کنترلی CTS آمادگی دریافت خود را اعلام می کند. این فریم کنترل CTS شامل اطلاعاتی نظیر: آدرس مقصد، مکانیزم کشف خط

مدت زمان اشغال بودن کانال می باشد.

4- باقی مانده ی گیرنده ایستگاه ها با دریافت پیام RTS و CTS، جدول NAV (Network Allocation Table) خود را به مدت زمان مشخص شده در RTS، CTS تنظیم یا مقداردهی کرده و در این مدت زمان هیچ یک نمی توانند به کانال دسترسی داشته باشند چون که می دانند کانال اشغال است.

5- فرستنده با دریافت CTS مطمئن می شود که در این مدت زمان، کسی به کانال دسترسی ندارد و می تواند داده ی خود را بدون رخ دادن Collision ارسال دهد اما در صورت عدم دریافت CTS یا کشف برخورد در هنگام بررسی کانال یک مدت زمان تصادفی صبر خواهد کرد.

6- گیرنده با دریافت صحیح فریم داده پیام ACK یا تصدیق و در صورت دریافت فریم داده ی خطا دار پیام NAC را به فرستنده ارسال می کند.

فرمت RTS:

2 byte	2	2	4	6
Frame control	DA	SA	Duration	CRC

فرمت CTS:

2	2	4	6
Frame control	DA	Duration	CRC

فرمت ACK:

2	2	4	6
Frame control	DA	Duration	CRC

نکته: تصادم در روش جانمط در هنگام گوش دادن به کانال رخ می دهد. و اینجا از کانال Full استفاده می کنیم. (CSMA/CA)

در هنگام ارسال داده برخورد (ها) رخ می شود و از برخورد اجتناب می شود چون که با استفاده از پیام های کنترل RTS و CTS مدت زمان اشغال بودن

کانال را مشخص کرده و دیگر کامپیوترها با مشخص شدن مدت زمان اشغال بودن کانال منتظر بوده و دیگر فریمی را ارسال نخواهند کرد اما در هنگام ارسال RTS و CTS و هنگام بررسی کانال، ممکن است تصادم رخ دهد یعنی تصادم برای فریم‌های کنترلی رخ می‌دهد در هنگام گوش دادن به کانال اگر کانال خالی باشد، تصادم رخ نمی‌دهد اما اگر کانال اشغال باشد، تصادم رخ خواهد داد و گیرنده با دریافت پیام خطا از RTS دیگر CTS را به فرستنده ارسال نخواهد کرد و گیرنده و فرستنده با توجه به عدم دریافت CTS یا ACK متوجه برخورد شده و یک مدت زمان تصادفی را صبر می‌کند. 2- در این روش از دو کانال full Duplex استفاده می‌شود تا امکان ارسال و دریافت به صورت هم زمان امکان پذیر باشد.

* الگوریتم محاسبه‌ی زمان تصادفی:

همان طور که قبلاً مشاهده کردید در صورت وقوع برخورد در هنگام ارسال داده به بردی کانال یا در هنگام بررسی کانال، یک مدت زمان تصادفی صبر می‌کرد. الگوریتم محاسبه‌ی مدت زمان تصادفی به شکل زیر است. اگر n امین مدت زمان تصادفی در نظر بگیریم، آن گاه:

1) برخورد اول $0 < n < 1 * |ST|$

2- برخورد دوم $0 < n < 3 * |ST|$

3- برخورد سوم $0 < n < 2^i - 1 * |ST|$

4- برخورد پانزدهم تا پانزدهم $0 < n < 2^{10} - 1$

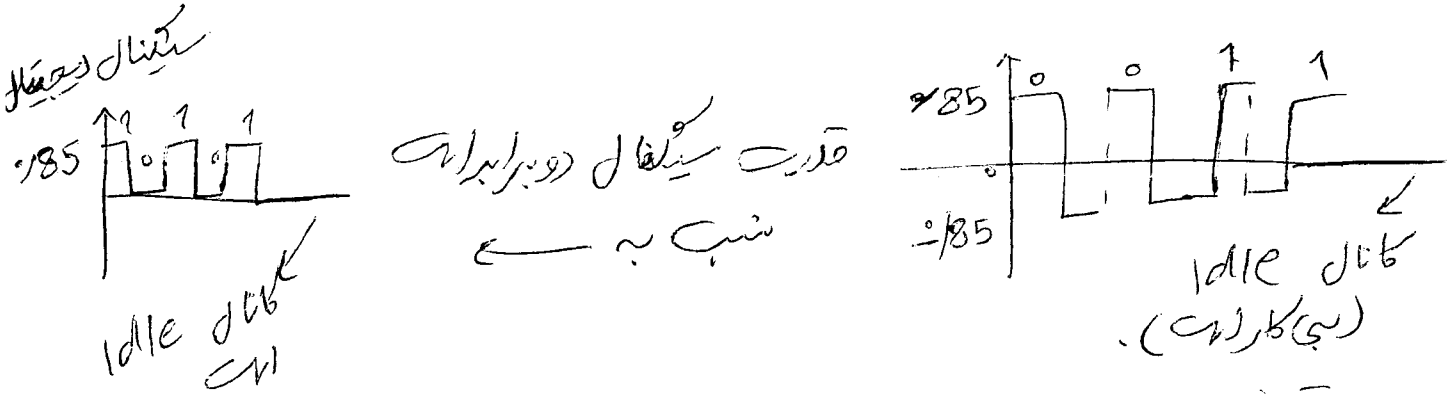
5 - برخورد شانزدهم: صرف نظر از ارسال فریم و ارسال پیغام خطا به لایه بالاتر

استانداردهای مؤسسه IEEE: (استانداردهای شبکه).

1- اترنت 802.3

کابل Coaxial ضخیم 50 اهمی - پروتکل CSMA/CD - کدگذاری منچستر

1: ⌐¬ 0: ¬⌐ (منچستر همواره زمان سازی می کند)



* توضیح:

مؤسسه IEEE برای شبکه های مختلف استانداردهای متفاوتی را انجام داده اند که به صورت (فرمت) IEEE 802.x مشخص می شود که اسم استانداردها نیز بدین گونه از آن ها اشاره می کنیم:

1- 802.3 اسم استاندارد به شکل زیر است:

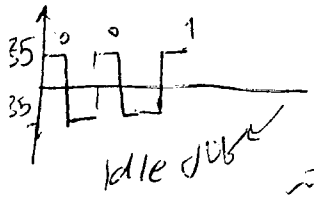
1- توپولوژی BUS (در گذشته به این شکل بوده است امروزه به شکل ستاره ای می باشد) 2- استفاده از کانال کابل Coaxial ضخیم 50 اهمی (یا نازک) (برای شبکه T2) 3- دسترسی به کانال CSMA/CD

CS، بررسی کانال توسط فرستنده ، MA دسترسی چندکانال به طور همزمان به یک کانال و CD (Collision Detect) تشخیص برخورد در صورت اشغال بودن کانال ؛ نوع ایثرنت بدین شکل به صورت کابلی می باشد. نرخ انتقال 10 مگابیت بر ثانیه است و الگوریتم مورد استفاده برای رمزگذاری روش منچستر می باشد.

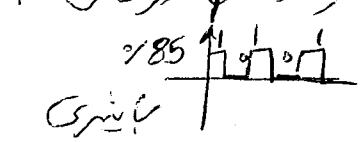
← کدگذاری منچستر: در این روش، از سه سطح مختلف ولتاژ استفاده می شود. داده ی دیجیتال باینری به صورت دو سیگنال مختلف ارسال می شود. ~~سیگنال به دو سیگنال تقسیم می شود و همین~~

← مزایای منچستر: در روش منچستر از پالس زمانی بین گیرنده و فرستنده استفاده می شود یعنی به همراه ارسال داده ، پالس هم زمانی بین فرستنده و گیرنده نیز ارسال می شود. زیرا در هنگام ارسال داده، هر بیت از داده یک پالس ساعت نیز وجود دارد. ۲- در روش منچستر عدم ارسال اطلاعی یا خالی بودن کانال با استفاده از ولتاژ صفر به راحتی قابل تشخیص است. چرا که اگر فرستنده ای داده ای برای ارسال نداشته باشد به راحتی می تواند با سطح ولتاژ صفر خالی بودن کانال را تشخیص داد.

← معایب منچستر: سطح ولتاژ (فرکانس ارسال فرستنده) باینری دوبرابر فرکانس در هنگام ارسال به صورت باینری باشد.



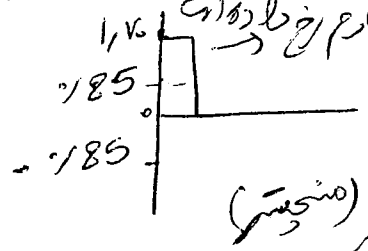
منچستر (سیگنال دیجیتال)



باینری

نکته: منظور از زمان تاخیر برگشتی: مدت زمانی است که طول می کشد تا گیرنده، دریافت کند و دوباره روی کانال ارسال دهد.

اگر دو فرستنده، هم زمان فریمی را روی کانال ارسال کنند سطح ولتاژ داده ای ارسالی دو برابر شده و چون شناخته نشده اند متوجه ایجاد تصادم می شویم. (در منچستر فقط سه سطح ولتاژ 85+، 85-، و ۰ داریم)



* فرمت فریم بندی ارسالی روی یک کانال: (حداکثر 1518 بایت)
(حداقل 64 بایت)

preamble and STX	Distination Address	Sourc Address	lenght	Rata	PAD	CRC
8 bytes	6 bytes	6 bytes	2 byte	46 byte		4 bytes

PAD : همان طور که می دانید اگر دو سیستم (مرسنده و) به طور هم زمان به کانال دسترسی داشته باشند تداخل پیش می آید و معمولاً تا زمانی که سیستم ها بفهمند که در هنگام ارسال داده بر روی کانال تداخل رخ داده است حداکثر 63 بایت داده بر روی کانال ارسال می کند. پس می توان گفت بسته ای کمتر از 64 بایت به عنوان بسته ی تداخلی در نظر گرفته می شوند که node ها میانی این بسته های تداخلی را حذف می کنند و از خود عبور نمی دهند.

حال فرض کنید که کاربری می خواهد داده ای با طول 20B را بر روی کانال بفرستد از آن جایی که 18 بایت نیز به عنوان سرآیند و دنباله در نظر گرفته می شوند مجموع داده ی ارسالی و سرآیند و دنباله برابر با 38 بایت می شود حال برای اینکه بسته ارسالی در شبکه به 64 بایت برسد و به عنوان بسته ی تداخلی در نظر گرفته نشود از فیلد به عنوان PAD استفاده می شود که اندازه ی این فیلد 46 بایت است.

Data + PAD + سرآیند و دنباله = 64

20 + 46 + 18 = 64

پس حداقل اندازه ی بسته ی ارسالی برابر با 64 بایت است و حداکثر بسته ی ارسالی 1518 بایت است.

- شبکه های 802.11 (300-400 گیگ هرتز)

این استاندارد یک شبکه ی بی سیم است که دارای ویژگی های زیر است:

أ- از آن جایی که دستگاه ها در این نوع شبکه ها دائما در حال حرکت اند، توپولوژی خاصی برای این نوع شبکه ها در نظر گرفته نمی شود.

ب- روش رمزگذاری مجموعاً از دو روش رمزگذاری (منظور از رمزگذاری گذاشتن

داده بروی کانال (ها) به دو روش زیر است:

روش اول: مادون قرمز یا IR یا infrared: در این روش برای انتقال داده از فرکانس 300-400 گیگا هرتز برای انتقال داده استفاده می شود. این تکنولوژی در ریموت های تلویزیون و موس و کیبورد های بی سیم مورد استفاده قرار می گیرند. از آنجایی که فرکانس بالایی دارند از موانع سخت عبور نمی کنند و مزیت آن فضای باند بالایی است که دارند.

روش دوم: Spread Spectrum: در این روش پهنای باند به بخش های متفاوتی تقسیم می شوند که هر کدام از یک محدوده فرکانسی خاصی برای ارسال داده استفاده می کنند. مجموعه ظیف فرکانسی که در این روش استفاده می شود، نیازی به کسب مجوز از جایی را ندارد (Free ligence) این روش به دو صورت پیاده سازی می شود: FHSS و DSSS. روش DSSS با استفاده از تکنولوژی multiplexing CDM پیاده سازی می شود که قبلاً توضیح داده شد است روش FHss نیز از تقسیم فرکانس استفاده می کند. در واقع این روش با استفاده از تکنولوژی FSK در طیف فرکانسی 2.4 گیگا هرتز پیاده سازی می شود به طوری که هر فرستنده داده اش را در شیفت های فرکانسی متفاوت ارسال می نماید

تکنولوژی مورد استفاده در رابع روش FDM می باشد.

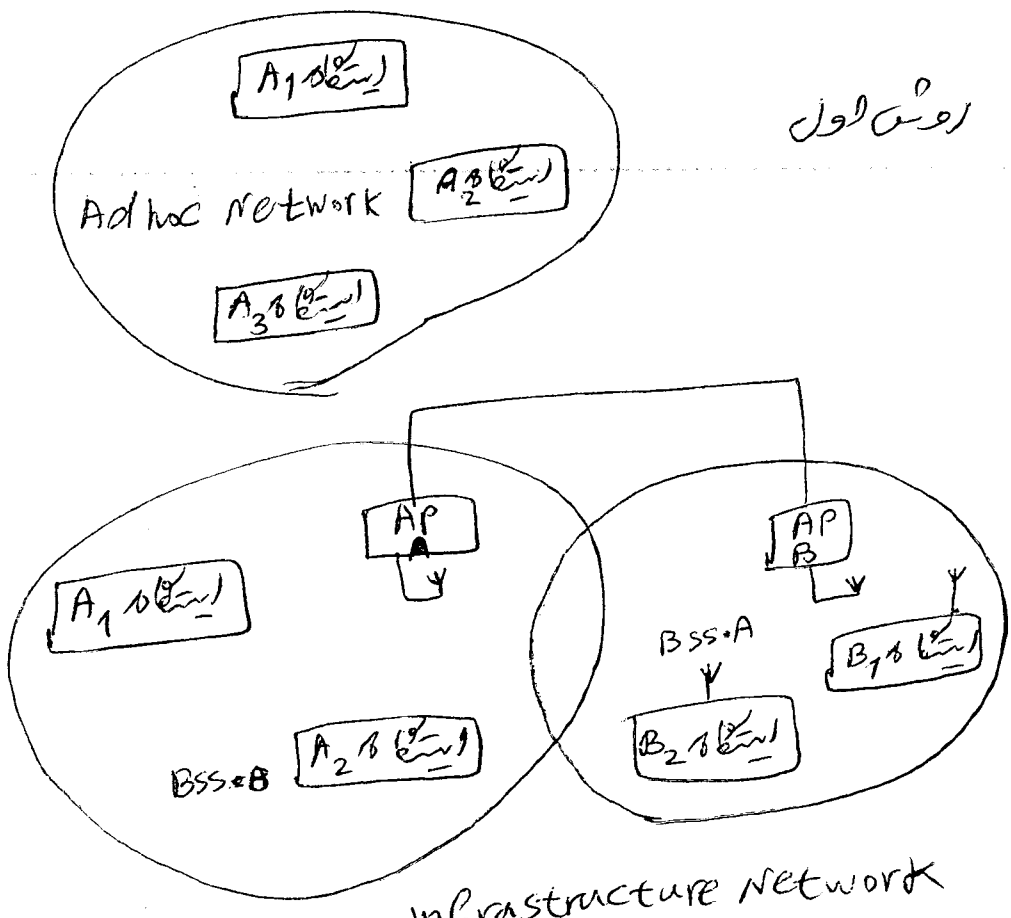
پیاده سازی شبکه استاندارد:

1- Ad hoc: در این حالت از پیاده سازی سیستم به صورت بی سیم با یکدیگر ارتباط برقرار می کنند در واقع در این روش کامپیوتر ها یا سیستم ها به صورت point to point با یکدیگر ارتباط برقرار می کنند یعنی شبکه ی Mesh در ارتباط

به شرط آن که فاصله 2 سیستم در یک فاصله ی معین باشد.

Infrastructure: در این روش از پدیده سازی برای ارسال کامپیوتر به یکدیگر از یک نقطه ی مرکزی به نام AP یا Access Point استفاده می شود. در واقع AC سگنال ها را دریافت می کند و آن ها را برای کامپیوتر دیگر تقویت می کند.

شکل این دو روش پدیده سازی به صورت زیر است:



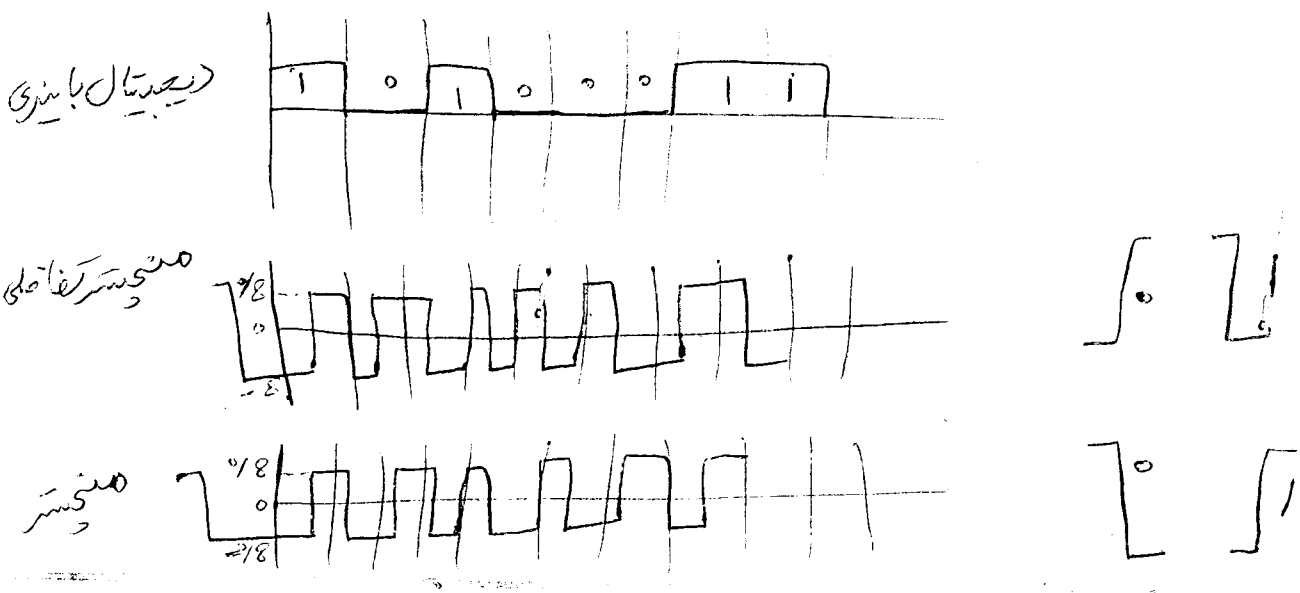
شبکه های 802.5 (TokenRing):

این نوع از شبکه ها دارای مشخصات زیر است:

1- توپولوژی مورد استفاده در این شبکه ها Ring است. در واقع توپولوژی این شبکه Ring می باشد اما ساختار سیم بندی آن به شکل Star است.

عبارت دیگر این نوع شبکه ترکیبی از تکنولوژی Star و Ring است که از یک واحد مرکزی به نام MAU (Multi Access Station Unit) برای مدیریت ایستگاه ها و افزایش قابلیت اطمینان شبکه استفاده می شود. با استفاده از MAU اگر یکی از ایستگاه ها کاری خراب شود کل شبکه از کار نمی افتد و MAU باعث برقراری ارتباط می شود اما اگر MAU از کار بیفتد کل شبکه از کار می افتد

محیط انتقال کابل زوج سیم به هم تابیده است. نرخ ارسال داده 4-16 مگابیت در ثانیه است روش رمزگذاری منچستر تفاضلی است در این روش نیز همانند روش منچستر از 3 سطح ولتاژ استفاده می شود. یعنی گذر ولتاژ از پایین به بالا برای صفر باینری و گذر ولتاژ از بالا به پایین برای یک باینری و عدم ارسال به صورت ولتاژ صفر است. (روش منچستر) اما در روش منچستر تفاضلی برای ارسال صفر عمل تعویض انجام می شود و برای یک باینری عمل تعویض انجام نمی شود. همان مقداریت به صورت منچستر تکرار می شود. عمل از ارسال داده فرستنده و گیرنده برروی سگنال ارسالی با مقدار یک توافق دارد.



- مراحل اجرای پروتکل Token:

الف) یک Token در حال گردش در حلقه است. با دریافت Token توسط هر ایستگاه، مجوزی برای ارسال فریم است. ج) هر ایستگاهی، Token را دریافت نمود:

1- یا اطلاعاتی برای ارسال ندارد، اولویت گذاری می کند و یا اطلاعاتی با اولویت کمتر از اولویت Token دارد که Token را برای ایستگاه بعدی ارسال می کند.

2- اطلاعاتی برای ارسال دارد (اولویتی بالاتر از اولویت Token) (یا برابر) بنابراین ایستگاه، Token را تصاحب می کند (با تغییر یکی از بیت های Token) Token آن، Token تبدیل به شروع یک فریم داده می شود و سپس فریم داده را به داده اضافه کرده و به ایستگاه بعدی ارسال می کند. ایستگاه بعدی اگر مقصد باشد، فریم را دریافت می کند و در غیر اینصورت، آن را برای ایستگاه بعدی ارسال می کند تا به مقصد برسد.

*تذکر: زمانی که بیت های فریم داده در شبکه در حال انتقال است، هیچ گاه دیگر فریم Token ای وجود ندارد. تنها فرستنده فریم Token را آزاد کند. د) هر ایستگاه، فریم داده را بدون تغییر

ه) هر ایستگاه بعد از اینکه فریم داده را از خود انتقال دادند (دوباره به فرستنده رسید) آن گاه فرستنده ابتدا فریم داده را از حلقه حذف می کند (یک بیت فریم داده را تغییر می دهد تا آن به Token تبدیل شود).

و Token به ایستگاه بعدی ارسال می‌شود تا اگر داده‌ای برای ارسال وجود دارد عملیات بالا مجدداً اجرا شود.

بیت‌های برای تشخیص گرفتن یا نگرفتن داده از Token:

Access = 1 (NACK)	Access = 0	Access = 1
copy = 0	copy = 0	copy = 1
	(NACK)	(ACK)

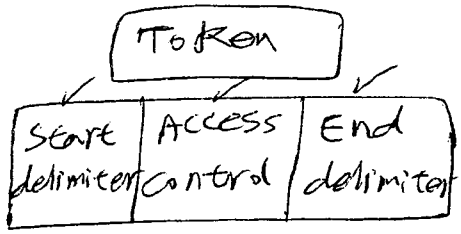
کار نکته: در شبکه‌ی اترنت برای اینکه فرستنده مطمئن شود گیرنده داده را دریافت کرده یا نکرده از یک فریم کنترلی به نام ACK استفاده می‌کند یعنی اینکه اگر از طرف گیرنده ACK دریافت کرد به این مفهوم است که گیرنده فریم داده را به صورت صحیح دریافت کرده است. اما اگر NACK دریافت کند نشان دهنده‌ی این است که گیرنده یا فریم داده را دریافت نکرده و یا اینکه فریم داده را خطادار دریافت کرده است. اما در شبکه‌های Token Ring برای اینکه فرستنده بداند آیا گیرنده فریم داده را دریافت کرده است یا خیر؛ از دو بیت کنترلی A و C استفاده می‌کند (Access و copy) بدین صورت که اگر داده به دست گیرنده رسید، گیرنده دو بیت A و C را ~~خاموش~~ می‌کند و در غیر این صورت هر دوی آنها یا یکی از آنها را تغییر نمی‌دهد و سپس مجدداً فریم داده را در حلقه به سمت فرستنده ارسال می‌کند. حال فرستنده با دریافت فریم داده، دو بیت A و C را کنترل می‌کند. اگر:

(الف) A و C هر دو صفر باشند یعنی گیرنده به فریم داده دسترسی نداشته است یا گیرنده خاموش بوده است.

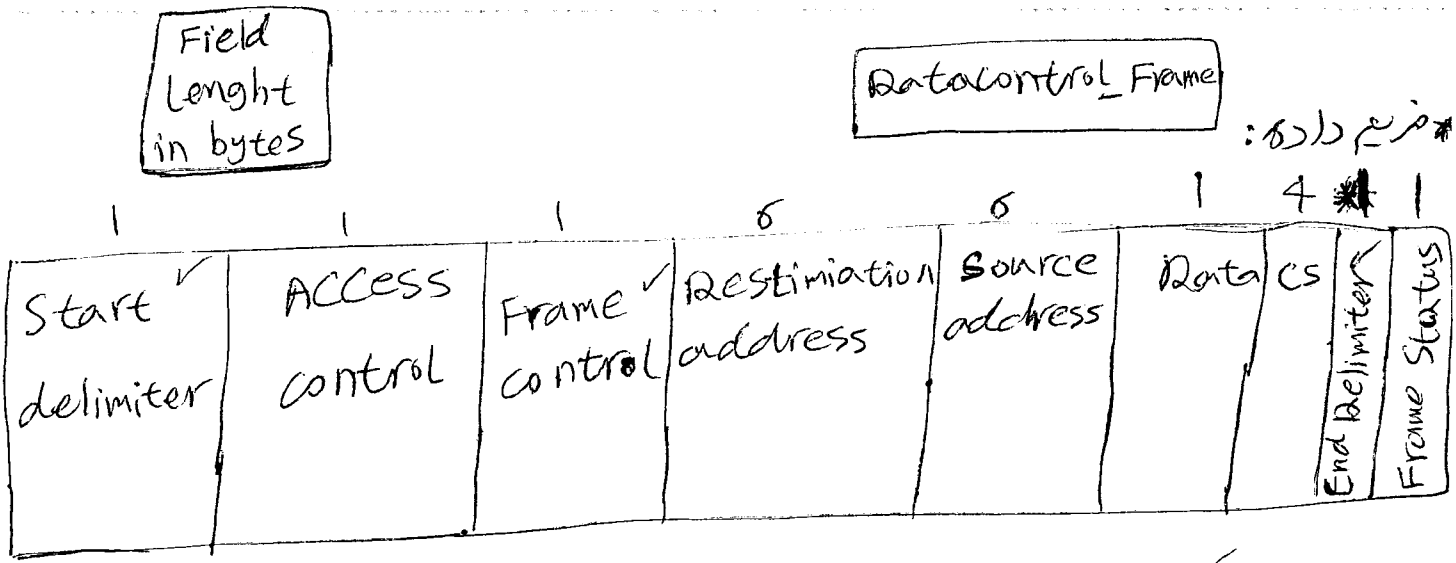
ب) اگر A=1 و C=0 باشد یعنی گیرنده روشن بوده است و به فریم دسترسی داشته است اما نتوانسته است آن را در بافر خود کپی نماید (یا بافر پر بوده است یا آدرس مقصد اشتباه بوده است یا محتوای داده، خطا دار بوده است).

ج) اگر A=1 و C=1 باشد گره گیرنده مشخص شده متوجه می شود کپی گیرنده به داده دسترسی داشته و فریم را داده و نیز در بافر خود کپی کرده است.

* فریم TokenRing :



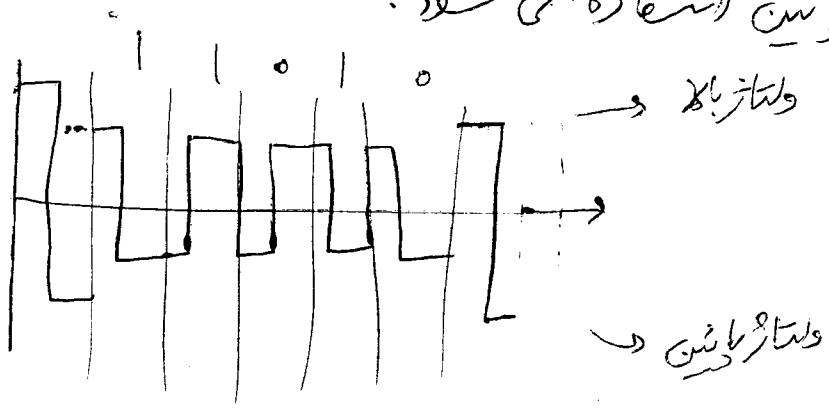
* فریم داده:



همان طور که در شکل بالا (فریم داده) می بینید: فریم داده ی Token Ring شامل فیلد ی 1- Start delimiter & End delimiter : این فیلد ها مشابه با همان دو فیلد ~~Start~~ STX و ETX

فریم داده است که بیان کننده ی ابتدا و انتها ی فریم می باشد. مجموعه ای برای تمایز این بایت ها کنترلی با دیگر بایت های کنترلی ارسالی از محیط نامعتبر در پروتکل مشخص تفاوتی استفاده می شود

منظور این است که به جای ارسال دو نیم سیکل برای بیت های داده از یک سیکل کامل ولتاژ بالا یا پائین استفاده می شود.



2- AccessControl: این فیلد 8 بیتی (1 بایتی) است که 3 بیت آن برای اولویت گذاری Token، 3 بیت دیگر برای رزرو اولویت و یک بیت برای مانیتورینگ و بیت دیگر آخری به عنوان بیت Token شناخته می شود که بیت Token برای تمایز فریم Token از فریم داده است و بیت مانیتورینگ برای جلوگیری از چرخش یک باربیت تر فریم داده در حلقه ی TokenRing است سه بیت اولویت گذاری نیز برای مشخص کردن اولویت دسترسی (ایستگاه های فرستنده) یا ایستگاه ها به Token است.

3- فریم control: این فیلد برای تمایز فریم کنترلی از فریم داده است و برای تعیین نوع فریم داده در لایه ی پیوند داده است. (نوع شبکه را مشخص می کند)

4- Restination & Source Address: فریم های آدرس مبدأ و مقصد می باشند که چون آدرس در لایه ی پیوند داده 48 بیتی است هر فریم، 6 بایت (از نظر گرفته شده) فیلد داده را مشخص کننده ی اندازه ی داده است که منحصر در TokenRing و ARC (این فیلد)

داده وابسته به مدت زمانی است که ایستگاه فرستنده می تواند Token را در اختیار داشته باشد.

5- CS : این فیلد برای کنترل خطا است.

6- End delimiter (گفته شده است.)

7- FramStatus : این فیلد برای تشخیص وضعیت فریم داده ای. بدین معنا که درون این فیلد برای فرستنده با استفاده از دو بیت A و C (Access) و C (copy) مشخص می شود که فریم داده برای گیرنده NACK یا ACK شده است.