مهندسی اینترنت و شبکه

ارائه دهنده
دکتر سید امین حسینی
E.mail: hosseini@um.ac.ir
Home page: http://hosseini.staffcms.um.ac.ir

مفاهیم مرتبط با لایه واسط

فهرست مطالب

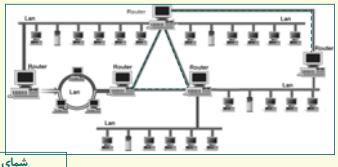
- لایه شبکه و مسائل خطوط انتقال داده
- استانداردهای انتقال روی خطوط نقطه به نقطه
  - پروتکل SLIP
  - پروتکل PPP
- استانداردهای انتقال در شبکه های با کانال مشترک
  - IEEE 802.3 CSMA/CD
  - IEEE 802.4 Token Bus
  - IEEE 802.5 Token Ring
  - IEEE 802.6 DQDB
  - IEEE 802.11 Wireless LAN

لایه واسط شبکه

1. تبدیل کانال دارای خطا به یک خط مطمئن و بدون خطا.
2. در راستای وظیفه فوق فریم بندی اطلاعات صورت می گیرد.
3. در استفاده از کانال مشترک، مدیریت کانال و جلوگیری از تصادم به عهده این لایه هست.

ارتباطات شبکه

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



شمای یک شبکه فرضی

مشخصه های کانالهای انتقال:

وظیفه سخت افزار انتقال در لایه واسط شبکه: انتقال بیتهای داده بر روی کانال فیزیکی بدون توجه به نوع و محتوای دادها

سخت افزار انتقال دارای قسمت است:

- گیرنده
- فرستنده
- کانال انتقال

در این قسمت صرفا به کانالهای انتقال خواهیم پرداخت

مشخصه های کانالهای انتقال:

پهنای باند: توانایی و ظرفیت آن در ارسال اطلاعات با نرخ **b** بیت در هر ثانیه. (با سرعت بیشتر از **b** بیت بر ثانیه نمی توان اطلاعات را سالم به مقصد رساند). در این رابطه داریم:
رابطه شانون:

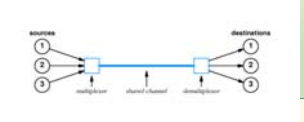
$$C=B.\log_2(1+S/N)$$

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

مشخصه های کانالهای انتقال:

نرخ خطای بیت: معیار خطا در کانال احتمال بروز یک بیت خطا روی کانال تعریف می شود. متوسط تعداد بیتهایی که در حین انتقال از طریق یک کانال دچار خطا می شوند نرخ خطای بیت یا **BER** گویند.

مالتی پلکسینگ: چون ظرفیت بعضی از کانالها زیاد است مثل فیبر نوری میتوان پهنای باند کانال را بین چند ایستگاه تقسیم کرد.



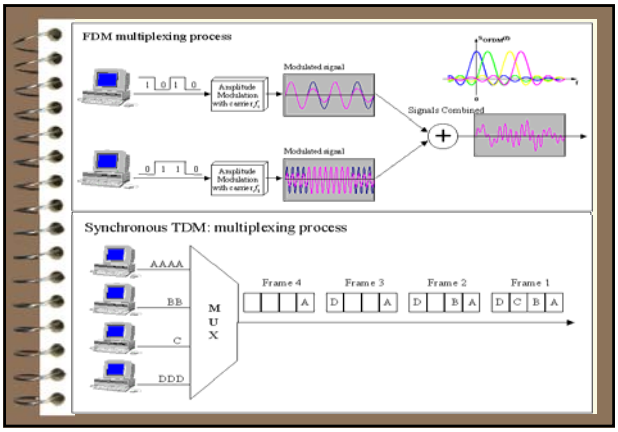
مشخصه های کانالهای انتقال:

مالتی پلکس یا تسهیم : تقسیم پهنای باند یک کانال بین چند ایستگاه

- تسهیم در میدان فرکانس یا **FDM** — **Frequency Division Multiplexing**
- تسهیم در میدان زمان یا **TDM** — **Time Division Multiplexing**

FDM: تقسیم پهنای باند فرکانسی به **N** باند مجزا (**N** تعداد ایستگاه موجود در شبکه) که هر باند به یک ایستگاه اختصاص داده می شود.

TDM: تقسیم زمان به بازه‌های کوچک (ارسال اطلاعات بر روی کانال توسط هر ایستگاه فقط در بازه زمانی مشخص)



مشخصه های کانالهای انتقال:

روشهای **FDM** و **TDM** زمانی کارآمد هستند که:

- تعداد ایستگاهها ثابت و محدود
- ارسال حجم ثابت و دائمی داده توسط هر ایستگاه بر روی کانال

لذا برای شبکه های که تعداد ایستگاهای آنها نامشخص ویا از ترافیک انفجاری (در یک زمان حجم زیادی داده برای ارسال دارند و در زمان دیگر چیزی ارسال نمی کنند) باید به سمت روشهای پویا برای استفاده اشتراکی رفت.

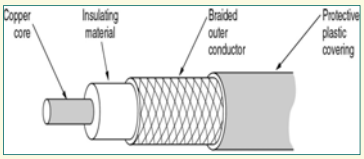
وظیفه سخت افزار انتقال در لایه واسط شبکه: انتقال بیتهای داده بر روی کانال فیزیکی بدون توجه به نوع و محتوای دادها

کانالهای انتقال

- خطوط تلفن
- فیبرهای نوری
- سیمهای به هم‌بافته‌شدهٔ زوجی
- کابلهای هم‌محور (کواکسیال)
- کانالهای ماهواره‌ای
- کانالهای رادیویی
- امواج طیف نوری

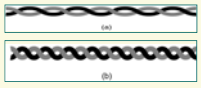
کانالهای انتقال

کابلهای هم‌محور (کواکسیال):
در انواع مختلف مانند:
کابل کواکس ۵۰ اهم ضخیم Tick Coaxial Cable
کابل کواکس ۵۰ اهم نازک Thin Coaxial Cable
کابل کوآکس ۷۵ اهم معمولی)



کانالهای انتقال

سیمهای به هم بافته شده زوجی:
• UTP : یک زوج سیم معمولی به هم بافته شده
• STP : یک زوج سیم معمولی به هم بافته شده به همراه یک پوشش آلومینیمی بر روی آنها جهت کاهش اثر نویزهای محیطی بر روی سیم



(a) Category 3 UTP.
(b) Category 5 UTP.

انواع UTP:	کاربرد	حد اکثر سرعت	پهنای باند
Cat 1 :	مدم های معمولی و فاکس ،	، 144 kbps	100KHz
Cat 2 :	مناسب برای ISDN	۲ Mbps	1M kz
Cat 3 :	مدم های معمولی و فاکس ،	، 10 Mbps	16MHz
Cat 4 :	token ring ،	، 16 Mbps	20MHz
Cat 5 :	اترنت ،	، 100 Mbps	100MHz
Cat 6 :	شبکه گیگا ،	، 1 Gbps	250MHz
Cat 7 :	شبکه گیگا ،	، 10Gbps	600MHz

کانالهای انتقال

کانالهای ماهواره‌ای : در باندهای فرکانسی مختلف مانند :
باند C (5.9-6.4GHz) ارسال و (3.7-4.2GHz) دریافت،
باندKu (14-14.5 GHz) ارسال و (11.7-12.2GHz) دریافت
باند Ka (27-30GHz) ارسال و (17.7-21.7GHz) دریافت

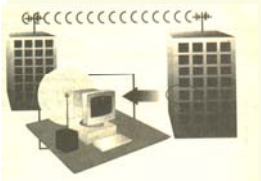
کانالهای رادیویی : شامل باندهای فرکانسی مختلف مثل UHF ، VHF

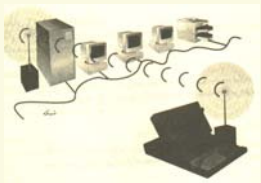
امواج طیف نوری: شامل نور مادون قرمز

فیبرهای نوری : در انواع مختلف مثل فیبر تک‌موده و چندموده

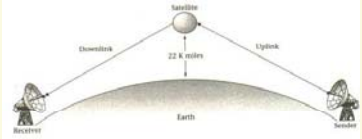
۱۵

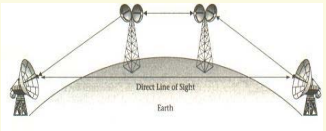
کانالهای انتقال





کانالهای انتقال

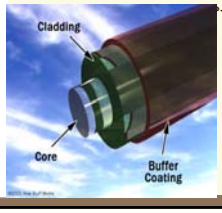




فیبرنوری

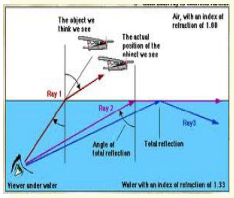
♦ فیبرهای نوری رشته های بلند و نازکی از شیشه بسیار خالصند که ضخامتی در حدود قطر موی انسان دارند. آنها در بسته هایی بنام کابلهای نوری کنار هم قرار داده میشوند و برای انتقال سیگنالهای نوری در فواصل دور مورد استفاده قرار میگیرند.

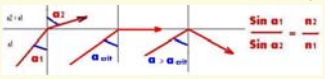
♦ هسته: هسته بخش مرکزی فیبر است که از شیشه ساخته شده و نور در این قسمت سیر میکند.
♦ لایه روکش: واسطه شفافی که هسته مرکزی فیبر نوری را احاطه میکند وباعث انعکاس نور به داخل هسته میشود.
♦ روکش محافظ: روکشی پلاستیکی که فیبر نوری در برابر رطوبت و آسیب دیدن محافظت میکند.



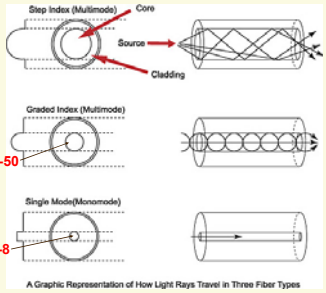
فیزیک نور

- شکست نور یک پدیده اپتیکی است که در آن نور رسیده از یک منبع نورانی به خاطر تغییر سرعتی که برای آن در دو محیط با ضریب شکست متفاوت رخ می‌دهد دچار تغییر مسیر می‌شود





انواع فیبرنوری



ویژگی های فیبرنوری

- پهنای باند فوق العاده بالا
- ایمنی فوق العاده بالا در مقابل نویز
- امنیت اطلاعات
- وزن،حجم و قیمت پائین
- تضعیف ناچیز
- ایمنی محیط (جرقه، برق گرفتگی)

مقایسه مشخصات برخی از کانالهای انتقال

نوع کانال	پهنای باند	خطا	پیاده سازی	قیمت	توضیح
خطوط تلفن معمولی	کم (حدود KHz۴)	زیاد	ساده	ارزان	از قبل وجود دارد
زوج سیم	متوسط (حدود چند ده تا صد مگاهرتز)	متوسط	ساده	ارزان	برای فواصل دوتاه مناسب است
کواکس	حدود چند صد مگاهرتز	کم	متوسط	متوسط	
فیبرهای نوری	حدود چند گیگا هرتز	بسیار کم	پیچیده	متوسط	بهترین کارایی
کانالهای ماهواره	حدود چند صد مگا هرتز	متوسط	بسیار پیچیده	گران	در همه جا تحت پوشش
کانالهای رادیویی	حدود چند مگا هرتز	زیاد	نسبتا پیچیده	نسبتا گران	در جایی که کابل کشی عقلایی نیست مناسب می باشد.

انواع خطا در شبکه‌های کامپیوتری

• نویز حرارتی

•این نویز به دلیل حرکت اتفاقی الکترونها بوجود میآید و با افزایش دما ، شدت این نویز هم به صورت خطی تقویت میشود. 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.

• 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.

روشهای کشف خطا

- اضافه کردن بیت توازن به داده‌ها
- روش Checksum
- کدهای کشف خطای CRC

بیت توازن

- ساده‌ترین روش کشف خطا
- اضافه نمودن یک بیت توازن به ازای هر بایت از اطلاعات
- انتخاب بیت توازن به گونه‌ای که مجموع تعداد بیتهای ۱ همیشه زوج یا فرد باشد
- این روش در صورتی موثر است که تعداد خطاهای رخ داده زوج نباشد

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

25

روش Checksum

- در این روش تمام بایتهای یک فریم ارسالی توسط فرستنده جمع (XOR) شده و ایجاد بایت Checksum می کند.
- این روش در صورتی قادر به کشف خطا است که تعداد خطاهای رخ داده در بیتهای هم ارزش زوج نباشد

۲۶

کدهای کشف خطای CRC

- محاسبه تعدادی بیت کنترلی به نام CRC (Cyclic Redundancy Check) به ازای مجموعه‌ای از بیتها و اضافه کردن آن به انتهای فریم
- مبنای کار : تقسیم چند جمله‌ای

۲۷

کدهای CRC

- 11100101: دادهٔ اصلی
- 7 6 5 4 3 2 1 0 موقعیت توانی
- 1 1 1 0 0 1 0 1 رشته اصلی
- ابتدا از روی دادهٔ اصلی یک چندجمله ای تولید میشود.

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

$D(x)= x^7 + x^6 + x^5 + x^2 + 1$

- برای تولید کد CRC چند جمله ای $D(X)$ را بر "چندجمله ای مولد" که بین گیرنده و فرستنده توافق میشود و اختیاری است ، تقسیم می گردد.

استانداردهای انتقال روی خطوط نقطه به نقطه

۱) پروتکل SLIP : Serial Line IP

۲) پروتکل PPP : Point to Point

30

کدهای CRC

- اگر چندجمله ای مولد $G(x)=x^2 + 1$ باشد برای تولید CRC تابع بدست آمده را در بزرگترین توان مولد ضرب و سپس حاصل را بر تابع مولد تقسیم می کنیم

$D(x) * x^2 = x^9 + x^8 + x^7 + x^4 + x^2$

- باقیمانده تقسیم با مقسوم جمع و به عنوان داده جدید ارسال می کنیم

- $x^9 + x^8 + x^7 + x^4 + x^2 \mod G(x) = 1$
- $x^9 + x^8 + x^7 + x^4 + x^2 + 1 \rightarrow 11100101\underline{01}$

CRC

پروتکل SLIP

مبادله اطلاعات بر روی اینترنت با استفاده از پروتکل TCP/IPانجام می شود . با این که پروتکل فوق یک راه حل مناسب در شبکه های محلی و جهانی را ارائه می نماید ، ولی به منظور ارتباطات از نوع Dial-up طراحی نشده است .

ارتباط Dail-up، یک لینک نقطه به نقطه (Point-To-Point)با استفاده از تلفن است . در چنین مواردی یک روتر و یا سرویس دهنده، نقطه ارتباطی شما به شبکه با استفاده از یک مودم خواهد بود. سرویس دهنده دستیابی راه دور موجود در مراکز ISP، مسئولیت ایجاد یک ارتباط نقطه به نقطه با سرپس گیرندگان Dial-upرا برعهده دارد .

SLIP و PPP پروتکل هائی می باشند که امکان استفاده از TCP/IPبر روی کابل های سریال نظیر خطوط تلفن را فراهم می نمایند.

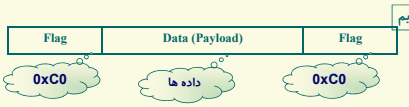
با استفاده از پروتکل های فوق ، کاربران می توانند توسط یک کامپیوتر و مودم به اینترنت متصل شوند .

پروتکل SLIP

روش کار:

1. ارسال علامت مشخصه یک بایتی 0xC0 روی خط توسط ایستگاه
2. انتقال داده بر روی خط
3. ارسال مجدد علامت مشخصه 0xC0 جهت مشخص نمودن انتهای فریم

قالب هر فریم



0xC0 | داده ها | 0xC0

جا نشانی کاراکتر Character Stuffing

اگر در درون قسمت داده ها ، کاراکتر 0XC0 جود داشته باشد ، چه تمهیدی برای جلوگیری از اشتباه در انتهای فریم اندیشیده شده است؟

معایب پروتکل SLIP

- عدم وجود کد کشف خطا در این پروتکل
- قرار گرفتن فقط بسته‌های IP درون فیلد داده فریم
- عدم پشتیبانی بسیاری از سیستم‌عاملها از این پروتکل
- لزوم داشتن آدرسهای IP ثابت و شناخته شده برای هر دو ایستگاه برقرارکننده ارتباط
- عدم تأیید و احراز هویت کاربر برقرارکننده ارتباط در این پروتکل

پروتکلی بسیار سریع به دلیل نداشتن فیلدهای سرآیند اضافی

پروتکل PPP

فاز مذاکره
Negotiation

مراحل برقراری ارتباط از طریق خط سریال نقطه به نقطه:

- شماره‌گیری به کمک مودم
- اتصال تلفن توسط مودم طرف مقابل
- تبادل بسته‌های اطلاعاتی کنترلی LCP (Link Control Packet) بین طرفین
  - فریم‌های LCP حاوی اطلاعات پارامترهای پروتکل PPP
- تبادل بسته‌های NCP (Network Control Packet) جهت تنظیم پارامترهای لایه بالاتر
- آغاز مبادله فریمها
- در نهایت برای ختم اتصال دو باره بسته NCPجهت توافق بر سر خاتمه کار ارسال می شود.

۲) قالب فریم پروتکل PPP

Bytes	1	1	1	1 or 2	Variable	2 or 4	1
	Flag 01111110	Address 11111111	Control 00000011	Protocol	Payload	Checksum	Flag 01111110

ابتدا و انتهای فریم با علامت هشت بیتی ۰۱۱۱۱۱۱۰ (x7E) تعیین میشود و بالطبع چنین الگویی نباید در درون اطلاعات وجود داشته باشد.

Address Field

- مقدار فیلد تماماً ۱
- آدرس فراگیر
- عملا زاید است (فقط برای سازگاری با پروتکل پدرش آورده شده)

Character Stuffing جا نشانی کاراکتر

اگر در درون قسمت داده ها ، رشته بیتی 01111110 (0X7E) جود داشته باشد ، ویا از کارکترهای کنترلی ascii استفاده شده باشد، چه تمهیدی برای جلوگیری از اشتباه اندیشیده شده است؟

بجای کاراکتر با کد 0x7E ، زوج کاراکتر 0x7D-0x5E قرار می گیرد.
بجای کاراکتر با کد 0x7D ، زوج کاراکتر 0x7D-0x9D قرار می گیرد.
بجای کاراکتر با کدهای زیر ۳۲ اشدا بیت ششم از آن کاراکتر معکوس شده و سپس کاراکتر 0x7D قبل از آن اضافه می‌شود. مثلاً کاراکتر با کد 0x0A بصورت 0x7D-0x2A تبدیل و ارسال می‌شود.

۳۷

Control Field

• مقدار این فیلد در مورد فریمهای عادی = 00000011
• نشان دهنده آن است که این فریم شماره‌گذاری‌شده نیست و نیازی به ارسال پیغام ACK توسط طرفین برای فریمها نمی‌باشد

وقتی که یک فریم PPP در حالت عادی بسته‌های IP را حمل می‌کند هر دو فیلد "آدرس" و "کنترل" ثابت و عملاً زائد هستند

38

Payload

• سایز پیش فرض این فیلد = ۱۵۰۰ بایت
•محدودیتی در طول ندارد ولی باید اول توافق شود
• بسته مربوط به لایه بالاتر در این فیلد قرار می‌گیرد
•بخاطر امکان پیکر بندی در ابتدا توسط لایه شبکه انعطاف پذیر است که در شبکه های گوناگون بکار رود

Protocol

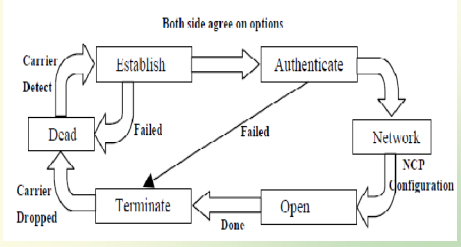
مشخص کننده آنکه بسته درون فیلد داده مربوط به چه پروتکلی در لایه بالاتر است.

Checksum

• به طور پیش فرض ۲ بایتی ولی در مرحله مذاکره روی ۴ بایت می توانند توافق کنند.
• جهت کشف خطاهای احتمالی در فریم

39

مراحل برقراری و ختم یک ارتباط در پروتکل PPP



41

برخی از بسته‌های LCP

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 بسته Echo Request)
Discard Request	I ⟶ R	لطفاً این بسته را نادیده بگیرید. (حذف کنید.)
Protocol Reject	I ⟵ R	پروتکلی را تعیین کرده‌اید که تشخیص داده نمی‌شود.

احراز هویت به کمک بسته LCP

• در PPP دو روش برای احراز هویت وجود دارد :

• PAP (Password Authentication protocol)

- LCP Authentication Request (ارسال رمز و آی دی)

•CHAP (Challenge & Handshake Authentication protocol)

- (one side) Send random challenge number
- (other side) Code the challenge number with DES algorithm and send it to sender
- Check the received code and send the LCP Success or LCP Failure.

•احراز هویت در PAP فقط یک بار انجام می شود ولی در CHAP می تواند به صورت متناوب هر از چند گاهی صورت گیرد.

فشرده سازی در PPP

• در PPP طرفین می توانند داده های خود را توسط الگوریتمی که اول توافق می کنند مانند دلف لیت یا کدهای هافمن فشرده و ارسال کنند.

•کوچک شدن فریمها و افزایش سرعت از مزایای آن است.

پروتکل MLPPP

• پروتکلی مبتنی بر PPP است که ار موازی سازی چند لینک فیزیکی در قالب یک لینک منطقی واحد پشتیبانی می کند.

•پس از مداکره و توافق MLPPP بسته های دریافتی از لایه های بالاتر را تیکه تیکه کرده و آنها را از لینکهای مختلف ارسال می کند.

استانداردهای انتقال اطلاعات بر روی کانال مشترک و مدیریت کانال

استانداردهای سری IEEE 802.X

IEEE 802.1

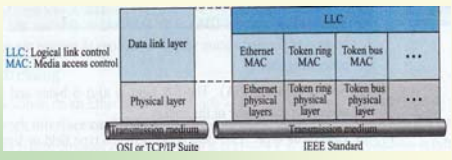
IEEE 802.1 یک پروتکل شبکه نیست بلکه استانداردی شامل یکسری تعاریف ، تشریح برخی از روشها و مقدمهای در مورد مجموعهٔ استانداردها است. همچنین طریقهٔ دسترسی به سرویسهای تعریف شده در هر استاندارد و نکات فنی در مورد پروتکلهایی که IEEE برای شبکه ها ارائه کرده ، در این استاندارد تشریح شده است.

IEEE 802.2

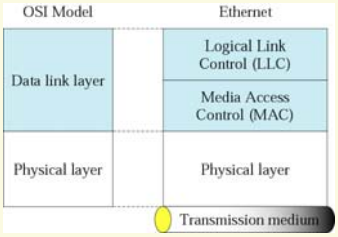
IEEE 802.2 یک زیرلایه به نام LLC تعریف کرده است تا

اولاً جزئیات سخت افزاری و توپولوژی شبکه را پنهان کند؛ (یعنی با استفاده از این زیرلایه ، شبکه های محلی با توپولوژیهای متفاوت همگی از لحاظ سرویسهایی که به لایهٔ بالاتر ارائه میدهند ، یکسان سازی خواهند شد.)

ثانیاً با استفاده از این زیرلایه سرویس انتقال فریمها مطمئن خواهد شد ، به گونه ای که ضمن شماره گذاری فریمها ، برای آنها پیغام تصدیق مبادله شده و بر روی جریان فریمها نظارت میشود.



لایه های Ethernet



استانداردهای واسط شبکه‌های محلی با کانال اشتراکی

IEEE 802.3 : استاندارد شبکه‌های محلی باس

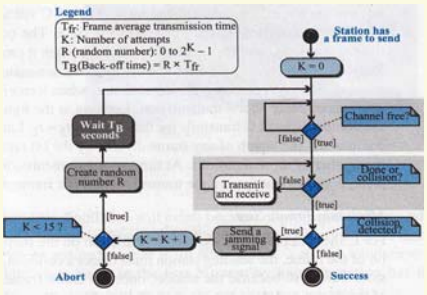
- تعریف این استاندارد برای شبکه‌های کانال مشترک با توپولوژی باس
- مدیریت کانال به روش CSMA/CD : Carrier Sense Multiple Access / Collision Detection

IEEE 802.3 : استاندارد شبکه‌های محلی باس

روش CSMA/CD:

- گوش دادن ایستگاه متقاضی ارسال فریم به کانال
- در صورت آزاد بودن کانال آغاز ارسال فریم
- اشغال بودن کانال توسط ایستگاه دیگر نتیجتا منتظر شدن تا اتمام ارسال و در صورت آزاد شدن کانال شروع ارسال فریم نتیجتا احتمال تصادم سیگنال به دلیل منتظر بودن ایستگاههای دیگر جهت ارسال فریم
- جهت کشف سریع تصادم : گوش دادن به کانال هنگام ارسال فریم تا در صورت بروز تصادم ارسال فریم متوقف گردد
- مواجه‌شدن ایستگاه آغازکننده ارسال با تصادم نتیجتا تولید عدد تصادفی توسط ایستگاه و توقف ارسال فریم به مدت عدد تصادفی و گوش دادن به خط
- تولید سیگنال نویز روی کانال هنگام آگاهی هر ایستگاه از تصادم جهت اطلاع ایستگاههای دیگر

IEEE 802.3 : استاندارد شبکه‌های محلی باس

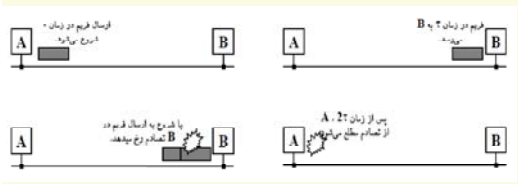


روش CSMA/CD

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[۲] سیگنال بستگی دارد.[۳] 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.

روش CSMA/CD



روش CSMA/CD

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.

روش CSMA/CD

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.

- سرعت انتشار امواج الکترو مغناطیس در سیم مسی 200000000 متر برثانیه است و به ازای هر 1000 متر 5 میکرو ثانیه تاخیر انتشار دارد

راندمان کانال در استاندارد IEEE 802.3

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

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

- کاهش طول فریم ← کاهش راندمان کانال
- افزایش طول کانال ← کاهش راندمان کانال
- افزایش نرخ ارسال ← کاهش راندمان کانال

۵۷

مشخصات فیزیکی استاندارد IEEE 802.3 بطور خلاصه عبارت است از :

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

قالب فریمهای داده در استاندارد IEEE 802.3

7 Byte	1 Byte	2 or 6 Byte	2 or 6 Byte	2 Byte	0–1500 Byte	0–45	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**"[3] را با الگوی 10101011 ، روی خط می‌گذارد. این بایت نقطهٔ شروع فریم را مشخص می‌کند.
- **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.

قالب فریمهای داده در استاندارد IEEE 802.3

- **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.

قالب فریمهای داده در استاندارد IEEE 802.3

شرکت‌های DEC ، Xerox و Intel یک پیاده‌سازی عملی از این استانداردها 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

آدرس در اترنت

- هر کارت شبکه دارای یک آدرس منحصر به فرد دارد که به آن آدرس MAC گفته می شود.
- این آدرس ۴۸ بیت است.
  - ۲۴(۲۳-۰) بیت اول شماره سریال،
  - ۲۲(۴۵-۲۴) بیت بعدی شماره شناسایی تولید کننده
  - ۲(۴۷-۴۶) بیت آخری مربوط به نوع است.
    - بیت ۴۶ = ۰ ادرس توسط مدیر شبکه ست شده و خارج شبکه ارزشی ندارد
    - بیت ۴۶ = ۱ ادرس توسط IEEE ست شده و اعتبار جهانی دارد

انواع آدرس

- Unicast Address گیرنده فقط یک کامپیوتر است $A_{47}=0$
- Multicast Address گیرنده گروهی از کامپیوترها هستند است $A_{47}=1$ و سایر بیتها شماره گروه را مشخص می کنند.
- Broadcast Address گیرنده تمام کامپیوترهای متصل به کانال است $A_{47}=1$ سایر بیتها نیز ۱ است.