شبکه های کامپیوتری ۱

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

لایه پیوند داده

Data Link Control Protocols

کنترل جریان

کنترل خطا

کنترل ارتباط داده سطح بالا (HDLC)

Data Link Control Protocols

بدلیل

احتمال خطای انتقال و

نیاز به تنظیم سرعت دریافت گیرنده

تکنیک های همگامی و اتصال کفایت نمی کندو نیاز به یک لایه کنترلی در هر دستگاه هست

لذا:

کنترل جریان، شناسایی خطا و کنترل خطا را فراهم سازد.

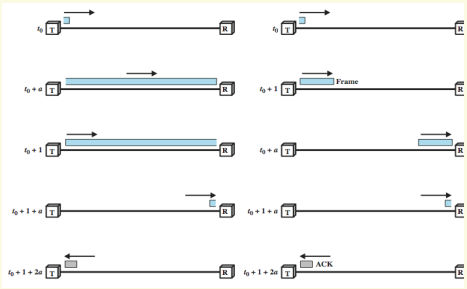
Data Link Control Protocols

- آنچه تا کنون گفته شد ارسال سیگنالها در یک خط بود. برای تبادل دیجیتال موثر نیاز به یک لایه بالاتر از لایه فیزیکی هست که تبادل دیتا را روی خط مدیریت کند.
  - frame synchronization
  - flow control
  - error control
  - addressing
  - control and data link management

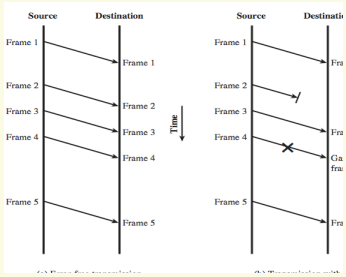
Flow Control

- کنترل جریان یعنی این که اطمینان حاصل کنیم که یک فرستنده ، گیرنده را از داده اشباع نمی کند.
  - جلو گیری از پر شدن بافر
- زمان انتقال
  - زمانی که فرستنده یک فریم را ارسال میکند.
- زمان انتشار
  - زمانی که یک بیت از مبدا به مقصد می رسد.

Stop and Wait Link Utilization



Model of Frame Transmission



بهره وری روش توقف و انتظار
(کانال بدون خطا)

B = R*D/V

B: طول ارتباط به بیت R:سرعت کانال D:فاصله به متر V: سرعت به متر

a = B/L L:طول فریم

a > 1 زمان انتشار (ناکارایی جدی داریم)

بزرگتر از زمان ارسال

a < 1 زمان انتشار کوچکتر از زمان ارسال

در سرعت های بالا و فواصل طولانی بهره برداری ناکافی از خط داریم.

25_stop and wait arq.swf

Stop and Wait

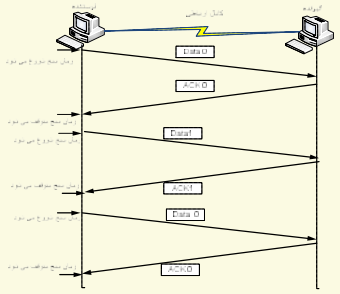
- مزایا:
  - سادگی پیاده‌سازی
- معایب
  - بهره‌وری کم

Stop and Wait

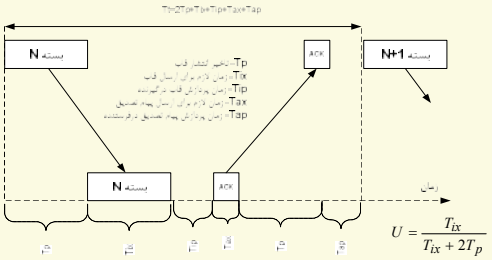
- فرستنده یک فریم را ارسال و برای ارسال فریم بعدی منتظر دریافت تایید گیرنده می ماند.
- در این حالت گیرنده بر اساس وضعیت خودش می تواند فرستنده را کنترل کند.
- این پروتکل برای فریم های بزرگ خوب کار می کند. ولی با این وجود به چند فریم کوچک شکسته می شود زیرا:
  - سایز بافر گیرنده ممکن است محدود باشد.
  - اگر در یک فریم بزرگ یک خطا باشد باید دوباره حجم زیادی را دوباره ارسال کند.

در LAN معمولا زمان زیادی برای ارسال بسته های بزرگ به طول نمی انجامد

مثالی از روش توقف و انتظار



محاسبه بهره وری کانال
(کانال بدون خطا)



$$U = \frac{T_{ix}}{T_{ix} + 2T_p}$$

بهره وری روش توقف و انتظار
(کانال بدون خطا)

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

- کانال های کوتاه
- برای کانال های نسبتا کوتاه که مقدار a کمتر از ۱ است ، بهـره وری کانـال بـا تقریبـا خوب براب با ۱۰۰٪ بوده و مستقل از نرخ داده است.
- پروتکل توقف و انتظار برای کانال های کوتاه و نرخ داده متوسط کافی است.
- مثال شبکه هایی مبتنی بر مودم و تلفن عمومی آنالوگ

بهره وری روش توقف و انتظار
(کانال بدون خطا)

- کانال های طولانی
- در خطوط طـولانی تـر زمینـی ، بهـره وری خـط بـرای نـرخ هـای داده پـایین (و ازاینرومقادیر کم a) بالا است اما بـا افـزایش نـرخ داده (واز اینـرو a) بطـور قابـل ملاحظه ای کاهش می یابد.
- بهره وری کانال برای خطوط ماهواره حتی با نرخ داده پایین ضعیف است.
- پروتکل توقف و انتظار برای این قبیل کاربردها و خطوط زمینی با سرعت بـالا مثـل شبکه های محلی و اکثر شبکه های گسترده عمومی مناسب نیست.

مشکل اتلاف ظرفیت کانال درروش توقف وانتظار

- مشکل روش توقف و انتظار:
  - چنانچه فاصله فرستنده و گیرنده از یکدیگر زیاد باشد، در این صورت طولانی بودن این فاصله باعث افزایش تأخیر بین ارسال قاب‌ها و کاهش بهره‌وری از کانال می‌شود.
- مثال :یک کانال ماهواره :
  - سرعت ارسال ۵۰ کیلوبیت بر ثانیه
  - تأخیر انتشار رفت و برگشت =۵۰۰ میلی ثانیه
  - طول قاب ۱۰۰۰ بیت

مشکل اتلاف ظرفیت کانال درروش توقف وانتظار

سرعت ارسال ۵۰ کیلوبیت بر ثانیه

تأخیر انتشار رفت و برگشت =۵۰۰ میلی ثانیه

طول قاب ۱۰۰۰ بیت

توجه به سرعت کانال ماهواره، ۲۰ میلی ثانیه بعد، ارسال قاب تمام شده است و ۲۷۰میلی ثانیه بعد قاب به‌طور کامل به گیرنده می‌رسد.

در صورتی که گیرنده همان لحظه پیام تصدیق ارسال دارد ۵۲۰ میلی ثانیه بعد فرستنده متوجه سالم رسیدن قاب ارسالی خود در گیرنده می‌شود.

فرستنده در حدود۹۶ (۵۲۰/۵۰۰) درصد از کانال را از دست داده است و فقط از ٤ درصد ظرفیت کانال استفاده می‌نماید.

راه حل : روش پنجره لغزان (ARQ پیوسته)

- فرستنده منتظر دریافت پیام گواهی نشده و پشت سرهم (تاتعداد محدود) قاب ارسال می دارد.
- طول پنجره = تعداد قاب هایی که می تواند فرستنده بدون دریافت پیام تصدیق به گیرنده ارسال دارد.
- شماره قاب : پیمانه N (ازشماره ۰ تا N-1)

راه حل : روش پنجره لغزان (ARQ پیوسته)

مثال چنانچه N=8 باشد، در این صورت قاب‌های ارسالی به‌صورت ۰،۱،۲،۳،۴،۵،۶،۷،۰،۱،۲،۳،۴،۵،۶،۷،۰،... شماره‌گذاری و ارسال می‌گردند

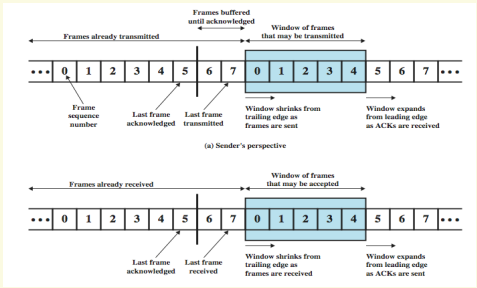
با دریافت پیام تصدیق یک قاب ارسالی، آن قاب از پنجره خارج شده و امکان ارسال قاب جدید فراهم می آید

با ارسال هرقاب، یک کپی از قاب دربافر فرستنده کپی شده و تایمر خاصی فعال می شود.

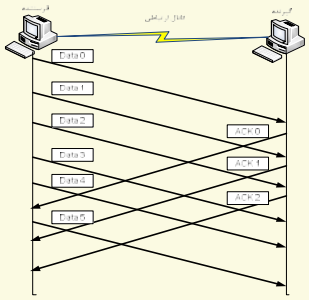
به تعداد N تایمر و N فضای بافر درفرستنده نیاز است

Sliding_Window

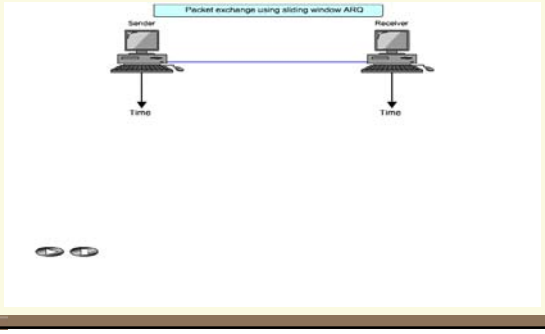
Sliding Window Diagram



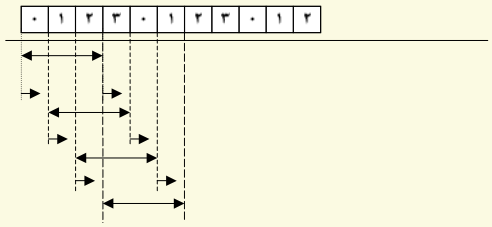
مثال : روش پنجره لغزان



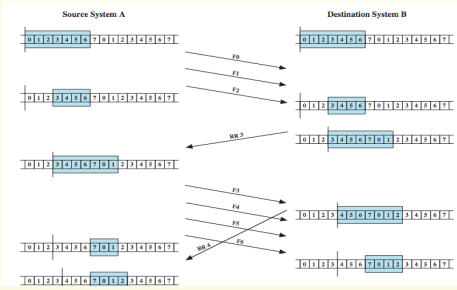
Sliding_Window_ARQ.swf



مثال پنجره لغزان با N=4



Sliding Window Example



باز یابی خطا درروش پنجره لغزان

- سه استراتژی مختلف درصورت مواجه به خطا:
  - روش بازگشت به عقب به اندازه N (Go Back N)
    - فرستنده مجددا از محل قاب خراب شده همه قاب ها را ارسال می دارد
    - بهره وری کم می شود
    - گیرنده فقط آخرین قابی که به ترتیب دریافت کرده است دربافر ذخیره می کند
    - نیاز به بافر کم درگیرنده
  - روش تکرار انتخابی(Selective Repeat)

Error Control

- شناسایی و اصلاح خطا
  - فریم گم شده
  - فریم آسیب دیده
- تکنیکهای بکارگیری
  - تشخیص خطا
  - دریافت تائیدیه مثبت
  - ارسال مجدد پس از انقضای مهلت
  - دریافت تائیدیه منفی

باز یابی خطا درروش پنجره لغزان

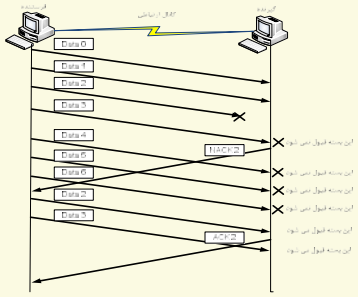
- ✓ فرستنده در صورت عدم دریافت پیام تصدیق به بطور ضمنی (با سرریز شدن تایمر) نتیجه می گیرد داده قبلی خراب شده است گیرنده نیاز به بافر طولانی برای ذخیره کردن قاب های دریافتی خارج از ترتیب دارد.
- ✓ گیرنده با تشخیص قاب خراب یک پیام عدم تصدیق می دهد

باز یابی خطا درروش پنجره لغزان

- ✓ فرستنده فقط قاب هایی که خراب شده اند را ارسال مجدد می کند
- ✓ بهره وری بیشتر می شود
- ✓ گیرنده نیاز به بافر طولانی برای ذخیره کردن قاب های دریافتی خارج از ترتیب دارد.
- ✓ بافر طولانی
- ✓ پیاده سازی مشکل تر است
- ✓ روش توقف و انتظار (stop& wait)
- ✓ گیرنده تنها برای دادهای صحیح پیام تصدیق می فرستد

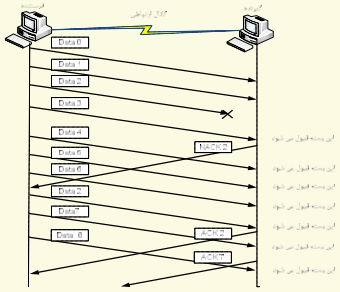
26_go back n arq.swf

مثال روش بازگشت به عقب به اندازه N



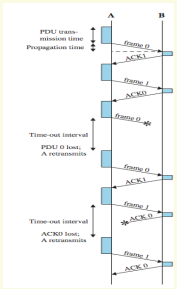
27_selectiverepeatarq-ARQ.swf

مثال روش تکرار انتخابی

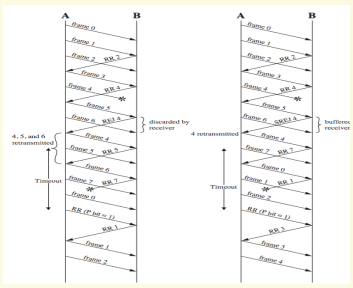


Stop and Wait

- see example with both types of errors



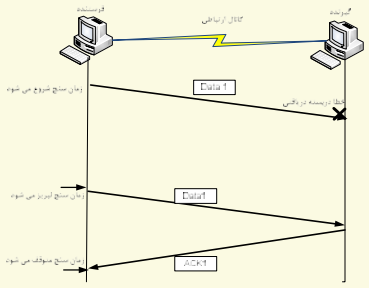
Go Back N vs Selective Reject



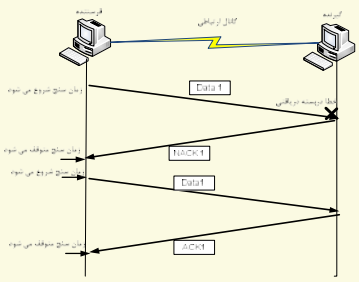
مواجه با خرابی درروش توقف و انتظار

- بازیابی خطا:
  - روش ارسال مجدد ضمنی (Implicit Retransmission)
    - گیرنده تنها برای دادهای صحیح پیام تصدیق می فرستد
    - فرستنده در صورت عدم دریافت پیام تصدیق به بطور ضمنی (با سرریز شـدن تایمر) نتیجه می گیرد داده قبلی خراب شده است
  - روش درخواست صریح (Explicit Request)
    - گیرنده با تشخیص قاب خراب یک پیام عدم تصدیق می دهد

بازیابی خطا: روش ارسال مجدد ضمنی



بازیابی خطا: روش درخواست صریح



Types of Error

- هنگامی خطا رخ می دهد که یک بیت بین فرستنده و گیرنده تغییر کند.
- انواع خطا
- single bit errors
  - فقط یک بیت تغییر می کند
  - بوسیله پارازیت سفید ایجاد می شود
- burst errors

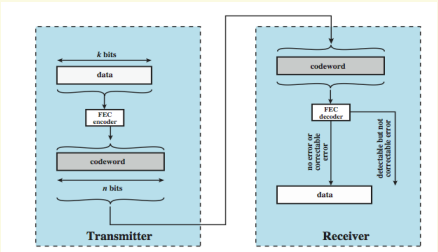
Types of Error

- دسته ای از بیت ها وجود دارد که که در آن خطایی رخ داده است (دو بیت متوالی خطا دار)
- بوسیله پارازیت ضربه ای و یا ضعیف و یا محو شدگی امواج در ارتباط بی سیم ایجاد می شود
- تاثیر این نوع در سرعت های بالا بیشتر می باشد

Error Detection

- خطا همیشه وجود دارد و بعث تغییر ۱ یا چند بیت می شود.
- تشخیص خطا با استفاده از اضافه کردن کد های تشخیص خطا انجام می شود
- کد های تشخیص خطا توسط فرستنده اضافه می شود
- گیرنده با محاسبه مجدد کد آن را با کد ارسالی مقاسیه می کند
- احتمال اینکه خطایی تشخیص داده نشود هم هست

Error Detection Process



Error Detection

- parity
  - parity bit set so character has even (even parity) or odd (odd parity) number of ones
  - even number of bit errors goes undetected

انواع خطا در شبکه‌های کامپیوتری

•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.

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.

۴۵

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

۴۸

روشهای کشف خطا

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

۴۷

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

۴۹

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

۵۰

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.

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

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

کدهای CRC

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.

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

Error Correction

➢ اصلاح خطا نیاز به ارسال مجدد داده دارد

➢ این روش برای کاربردهای بی سیم مناسب نیست

● در بیسیم میزان خطا زیاد است

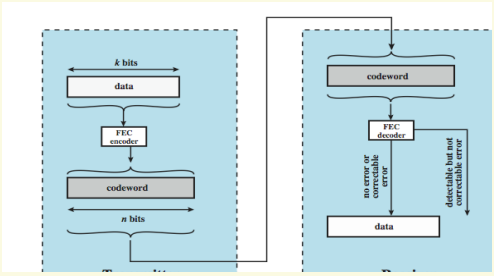
● در ارتباطات ماهواره ای تاخیر انتشار از فقط انتقال بیشتر است. ارسال مجدد معمولا از از فریم خطا دار شروع می شود(بعضی فریم ها چند بار ارسال می شوند) که کارایی را کم می کند.

➢ مطلوب است اگر گیرنده براساس اطلاعات خطا ها را اصلاح کند

How Error Correction Works

- با افزودن اطلاعاتی به پیام ارسالی این امکان ایجاد می شود که گیرنده حتی در صورت وجود مقدار معینی خطا پیام اصلی را درک کند.
- eg. block error correction code
  - الگوریتم FEC به عنوان ورودی یک بلوک kبیتی را در نظر می گیرد و n-kبیت به عنوان تست یا وارسی به ان اضافه می کند.
  - از فاصله همینگ d(v1,v2) بین ۲ رشته دو دویی استفاده می شود که عبارت است از تعداد بیت های نابرابر v1,v2 . مثلا
  - v1=011011 v2=110001 d(v1,v2)=3

Error Correction Process



block error correction code technique

- برای k=2 و n=5 میتوان تخصیص های زیر را داشت.

کلمه کد	بلوک داده
۰۰۰۰۰	۰۰
۰۰۱۱۱	۰۱
۱۱۰۰۱	۱۰
۱۱۱۱۰	۱۱

- فرض کنید الگوی ۰۰۱۰۰ دریافت شده که بر اساس
- جدول این کد کلمه معتبر نیست لذا گیرندخ خطایی را
- شناسایی کرده است.

- d(00000,00100)=1 d(00111,00100)=2
- d(11001,00100)=4 d(11110,00100)=3
- 00000 کمترین فاصله را دارد و می توان آن را جایگزین ورودی کرد.
- اگر کلمه کد نامعتبری دریافت شد آنگاه کلمه کد معتبر کدی است که به آن نزدیکتر است.

استانداردهای انتقال روی خطوط نقطه به نقطه

۱) پروتکل SLIP : Serial Line IP

۲) پروتکل PPP : Point to Point

پروتکل SLIP

SLIP و PPP پروتکل هائی می باشند که امکان استفاده از TCP/IP بر 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

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-upطراحی 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 سریس گیرندگان Dial-upرا برعهده دارد .

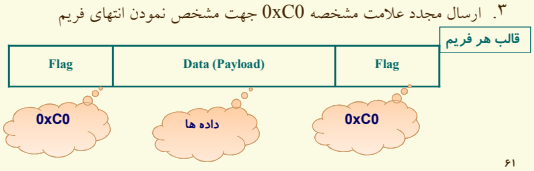
پروتکل SLIP

روش کار:

۱. ارسال علامت مشخصه یک بایتی 0xC0 روی خط توسط ایستگاه

۲. انتقال داده بر روی خط

۳. ارسال مجدد علامت مشخصه 0xC0 جهت مشخص نمودن انتهای فریم



۶۱

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؟

۶۲

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

۶۳

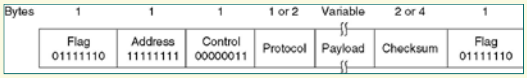
پروتکل PPP

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 NCP جهت توافق بر سر خاتمه کار ارسال می شود.

۶۴

۲) قالب فریم پروتکل PPP



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)

۶۵

جا نشانی کاراکتر Character Stuffing

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؟

جای کاراکتر با کد 0x7E ، زوج کاراکتر 0x7D-0x5E قرار می‌گیرد.
جای کاراکتر با کد 0x7D ، زوج کاراکتر 0x7D-0x9D قرار می‌گیرد.
جای کاراکتر با کدهای زیر ۳۲ ابتدا 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.

۶۶

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 عملا زائد هستند.

۶۷

Control Field

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 ٤ بایت می توانند توافق کنند.

• جهت کشف خطاهای احتمالی در فریم

۶۸

Payload

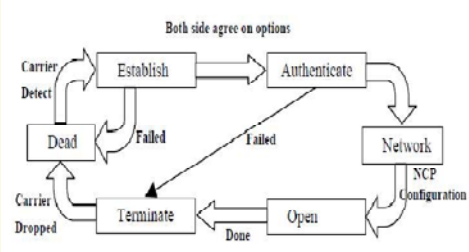
• سایز پیش فرض این فیلد = ۱۵۰۰ بایت

•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

مراحل برقراری و ختم یک ارتباط در پروتکل PPP



۷۰

برخی از بسته های 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 پاراشترها و گزینه‌ها پذیرفته نشد.
Configure Reject	I◀—R	برخی از پاراشترها 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 آي دي)

•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

احراز هویت به کمک بسته LCP

- 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 با 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.