CCSP.IR

Cisco Certified Security Professional

به نام خـــدا

CCSP.IR

Cisco Certified Security Professional

شبکه‌های کامپیوتری

مجموعهٔ مهندسی فناوری اطلاعات (IT)

دکتر ابوالفضل طرقی حقیقت

مؤسسهٔ آموزش عالی آزاد پارسه

ویرایش چهارم: بهار ۸۶ | تیراژ: ۱۰۰۰ نسخه |

شابک: ۳ - ۸۵ - ۸۷۱۹ - ۹۶۴ | ISBN: 964 – 8719 – 85 - 3

نشانی: بالاتر از میدان ولی‌عصر | کوچه دانش کیان | ساختمان پارسه | تلفن: ۸۸۸۴۹۲۱۱

مقدمه

در عصر فناوری اطلاعات، شبکه‌های کامپیوتری که به منظور انتقال داده‌ها، اشتراک منابع، توزیع داده‌ها و محاسبات از طریق اتصال کامپیوترهای مستقل به‌وجود آمده است از اهمیت ویژه‌ای برخوردار است. در این زمینه، ایجاد سیستم‌های باز که با رعایت استانداردهای بین‌المللی امکان اتصال کامپیوترهای مختلف و تجهیزات نامتجانس ساخت شرکت‌های گوناگون را فراهم آورده و یک محیط منسجم و یکپارچه را به‌وجود می‌آورند، مورد توجه جدی قرار گرفته است. یکی از مهم‌ترین استانداردهایی که در این زمینه بنا نهاده شده است، استاندارد هفت لایه‌ای OSI است که توسط موسسه ISO ارایه گردیده است. موضوع بحث درس انتقال داده‌ها بررسی دقیق کلیه مسائل مطرح در دو لایه پائینی این استاندارد، ISO، یعنی لایه فیزیکی و لایه پیوند داده می‌باشد. در درس شبکه‌های کامپیوتری ضمن بررسی لایه‌های فیزیکی و پیوند داده، مسائل مطرح در زیر لایه MAC شبکه‌های با سیم و بی‌سیم و نیز مسائل مطرح در لایه شبکه از جمله الگوریتم‌های مسیریابی و نیز استاندارد IP موردبحث قرار می‌گیرد. در بعضی از دانشگاه‌ها این دو درس تحت عنوان شبکه‌های کامپیوتری ۱ و ۲ مطرح می‌شود و تقریباً همه دانشجویان (حتی دانشجویان رشته مهندسی نرم‌افزار) هر دو درس را می‌گذرانند. بنابراین ضروری است دانشجویان گرامی برای شرکت در آزمون‌های کارشناسی ارشد، حداقل کلیه مسائل و جزییات مطرح در سه لایه پائین را بدانند. امید داریم که تلاش اساتید موسسه آموزش عالی پارسه بتواند به اعتلای دانشجویان و موفقیت دانشجویان و فارغ‌التحصیلان گرامی در آزمون‌های کارشناسی ارشد مثمرثمر واقع گردد.

در پایان از کلیه اساتید گرامی و دانشجویان عزیز خواهشمندم که کلیه پیشنهادات خود را در جهت بهبود این اثر برای استفاده بهتر دانشجویان و فارغ‌التحصیلان گرامی کتباً به آدرس انتشارات موسسه آموزش عالی پارسه ارسال فرمایند.

با امید توفیق

ابوالفضل طرقی حقیقت

فصل اول مفاهیم بنیادی انتقال داده‌ها و شبکه‌های کامپیوتری

فصل دوم آنالیز سیگنال‌ها و عوامل ایجاد خطا در سیستم‌های انتقال داده

فصل سوم استانداردهای واسط (interfacing Standard)

فصل چهارم Modulation Coding (کدگذاری و مدولاسیون)

فصل پنجم کنترل خطا

فصل ششم کنترل جریان

فصل هفتم زیرلایه کنترل دسترسی به رسانه انتقال (MAC Sulayer)

فصل هشتم لایه شبکه (Network Layer)

فصل نهم: پروتکل اینترنت (IP)

فصل اول

مقدمه‌ای بر انتقال داده‌ها و شبکه‌های کامپیوتری

در این فصل مفاهیم پایه و اصول اولیه شبکه های کامپیوتری و انتقال داده ها را مورد بررسی قرار می دهیم.

انتقال داده‌ها، شبکه‌های کامپیوتری و سیستم های توزیع شده

در دنیای امروز که می‌توان آن را عصر اطلاعات نامید، انتقال داده‌ها (Data Communication) و شبکه‌های کامپیوتری (Computer Networks) که حاصل پیوند دو صنعت کامپیوتر و مخابرات است، از اهمیت ویژه‌ای برخوردار می‌باشند. هدف از پیدایش شبکه‌های کامپیوتری، اتصال کامپیوترهای مستقل از طریق یک فناوری واحد و قوانین مشخص به منظور انتقال داده‌ها و اشتراک منابع است. منظور از انتقال داده‌ها ، ارسال و دریافت داده‌ها به صورت پیوسته آنالوگ یا گسسته دیجیتال بر روی رسانه‌های مختلف انتقال مانند زوج سیم به هم تابیده، فیبر نوری، هوا و غیره می‌باشد.

توجه کنید که اینترنت و وب، هیچکدام یک شبکه کامپیوتری نمی باشند. اینترنت (Internet)، شبکه شبکه‌ها است و از به هم پیوستن هزاران شبکه نا متجانس و گوناگون که هر کدام از آنها فناوری و قوانین مخصوص به خودش را دارد به وجود آمده است. اما وب گسترده جهانی (WWW: World Wide Web) نمونه ای از یک سیستم توزیع شده است. یک سیستم توزیع شده، مجموعه‌ای از چندین کامپیوتر مستقل است که از دید کاربر به صورت یک سیستم نامرئی (Transparent)، متمرکز (Centeralized) و متجانس به نظر می‌رسد و کاربر به جای نگرانی در مورد به خاطر سپردن آدرس ها (مثلا آدرس اینترنتی IP)، هر چیز را از طریق نام آن فراخوانی می نماید (مثلا در وب همه چیز به صورت سند یا صفحه وب است و از طریق نام URL قابل دستیابی است و این نام ها به صورت خودکار توسط خدمت‌گزارهای نام حوزه به آدرس IP تبدیل می شوند). همچنین دقت کنید که وب، میان افزار (Middleware) است و یک لایه نرم افزاری می‌باشد که در یک محیط ناهمگن بر روی سیستم عامل های متنوع مستقل قرار دارد، اما ایده سیستم‌های عامل توزیع شده، وظیفه ایجاد یک تصویر متمرکز از کامپیوتر های مستقل را بر عهده سیستم عامل واحد توزیع شده می سپارد.

کاربردهای شبکه

امروزه با گسترش اینترنت و جهانی شدن وب، کاربرد های شبکه های کامپیوتری از تنوع زیادی برخوردار است که برای نمونه، چند مورد از آنها عبارتند از: جستجو و تحقیق و دسترسی به اطلاعات به‌روز پراکنده در دنیا، تجارت الکترونیکی، خرید، فروش و حراج کالا، آموزش از راه دور و دانشگاه مجازی، دولت الکترونیکی، درمان از راه دور، کنفرانس صوتی و تصویری راه دور، کنترل، مدیریت و نظارت بر سیستم های صنعتی از راه دور، پست الکترونیکی، پیام رسانی فوری، گروه های خبری، گفتگو و گپ زدن، بازی و سرگرمی تعاملی، پخش فیلم های درخواستی، کمک به ایجاد واقعیت مجازی و ده‌ها کاربرد دیگر.

اجزای شبکه

شبکه‌های انتقال داده از سه بخش عمده تشکیل می‌شوند:

۱ـ کامپیوترهای میزبان (Host) که هدف اصلی ایجاد شبکه، اتصال کامپیوترهای میزبان به یکدیگر است.

۲ـ پردازنده‌های واسط مانند هاب‌ها (Hub)، تکرار کننده‌ها (Repeater)، پل‌ها (Bridge) ، سوئیچ‌ها (Switch) و مسیریاب‌های (Router) میانی که وظیفه مدیریت شبکه و هدایت ارسال داده‌ها از مبدا و مقصد را بر عهده دارند. مدل ریاضی شبکه‌های کامپیوتری یک گراف است که در آن، گره‌ها (Nodes) همان پردازنده‌های واسط هستند.

۳ـ لینک‌های ارتباطی (Link) که در واقع رسانه‌های انتقال داده هستند و با اتصال گره‌های شبکه به یکدیگر انتقال داده‌ها را بر عهده دارند.

پردازنده‌های واسط و لینک‌های ارتباطی زیر شبکه انتقال داده (Communication Subnet) را تشکیل می‌دهند.

۱-۱ طبقه بندی شبکه ها

شبکه‌های کامپیوتری از نظر اندازه و گستردگی جغرافیایی به ۵ دسته تقسیم می‌شوند:

۱- شبکه‌های شخصی(PAN : Personal Area Networks) که بر روی میز کار یا فاصله چندمتری یک شخص هستند. مانند ارتباط بی سیم اجزای کامپیوتر با کامپیوتر شخصی(PC) و دستیار دیجیتالی(PDA) و یا حتی کامپیوتر پوشیدنی (Wearable Computer) شخص.

۱ـ شبکه‌های محلی (LAN : Local Area Network) که دارای گستردگی در حد یک ساختمان یا یک کمپ کوچک می‌باشند.

۲ـ شبکه‌های شهری (MAN : Metropolitan Area Network) که دارای گستردگی در حد یک شهر می‌باشند.

۳ـ شبکه‌های گسترده (WAN : Wide Area Network) که دارای گستردگی بیش از حد یک شهر (در حد استان، کشور یا قاره) می‌باشند.

۵- شبکه‌های جهانی که همان شبکه شبکه‌ها یا اینترنت است.

انواع فناوری انتقال

به طور کلی دو نوع فناوری انتقال داده وجود دارد:

۱ـ نقطه به نقطه (Point to point) یا همتا به همتا (Peer to peer) یا تک پخشی (Unicast) که داده‌های ارتباطی از طریق لینک‌ها و گره‌های میانی به طور مستقیم بین دو ماشین مبدا و مقصد مبادله می‌شود (مانند شبکه‌های تلفنی)

۲ـ انتشاری (Broadcast) که به آن داده پراکن یا پخشی نیز می‌گویند و در آن همه ماشین‌ها به یک کانال مشترک متصل شده و داده‌ها بر روی کانال انتقال داده منتشر می‌شود و کلیه ماشین‌ها به داده‌ها روی کانال دسترسی دارند (مانند انتشار رادیویی). این ماشین‌ها با توجه به آدرس مقصد بسته‌ها آن‌ها را برداشته یا دور می‌اندازند.

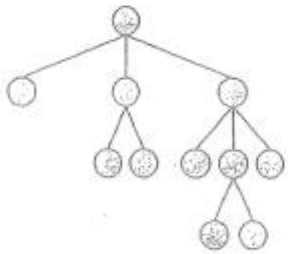
البته در بعضی از شبکه‌های انتشاری امکان ارسال داده‌ها از مبدا به گروهی از مقصدها وجود دارد که به آن پخش گروهی یا چند پخشی (Multicast) یا (Point to Multipoint) گویند.

همبندی (Topology)

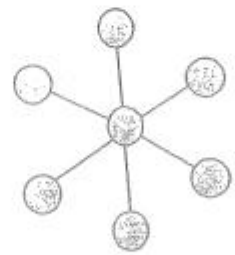
منظور از همبندی یا توپولوژی نحوه اتصال گره‌های تشکیل دهنده گراف شبکه از طریق لینک‌های ارتباطی است. ساختار و توپولوژی شبکه‌های کامپیوتری بر اساس ماهیت کانال‌های (Channel) انتقال داده و فناوری انتقال به دو دسته اصلی (نقطه به نقطه و انتشاری) تقسیم می‌شود.

انواع توپولوژی Point to point

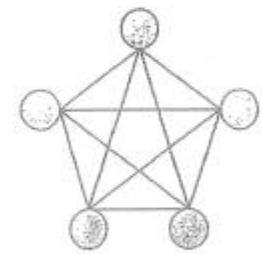
چندین نوع توپولوژی در شبکه‌های نقطه به نقطه مورد استفاده قرار می‌گیرد، مانند:



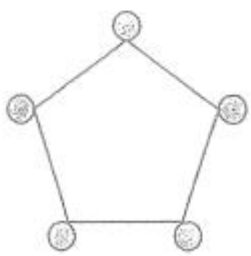
1) Tree (درختی)



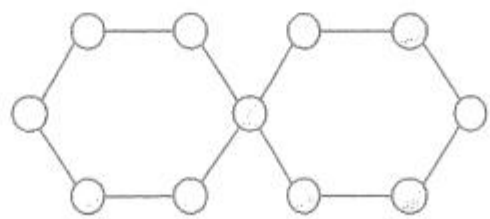
2) Star (ستاره)



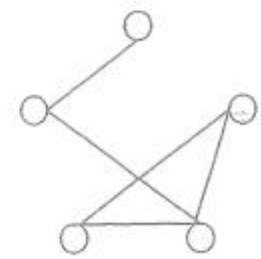
3) Mesh odr Complete



4) Ring (حلقه)



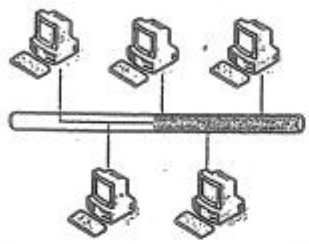
حلقه‌های متقاطع (5



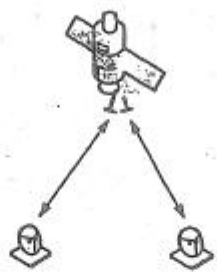
بی‌نظم (6

انواع توپولوژی Broadcast

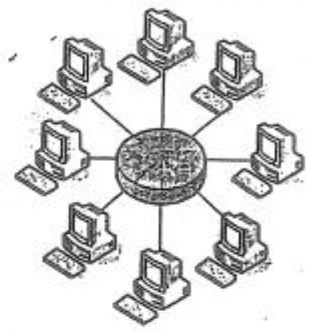
چندین نوع توپولوژی در شبکه‌های انتشاری مورد استفاده قرار می‌گیرد، مانند:



1) Bus (گذرگاه)



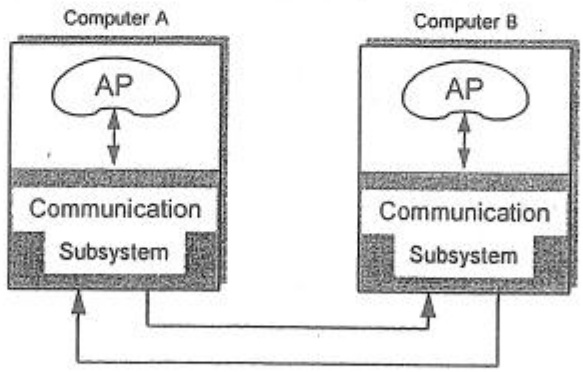
2) Satellite (ماهواره)



3) Shared Ring / LAN (حلقه مشترک)

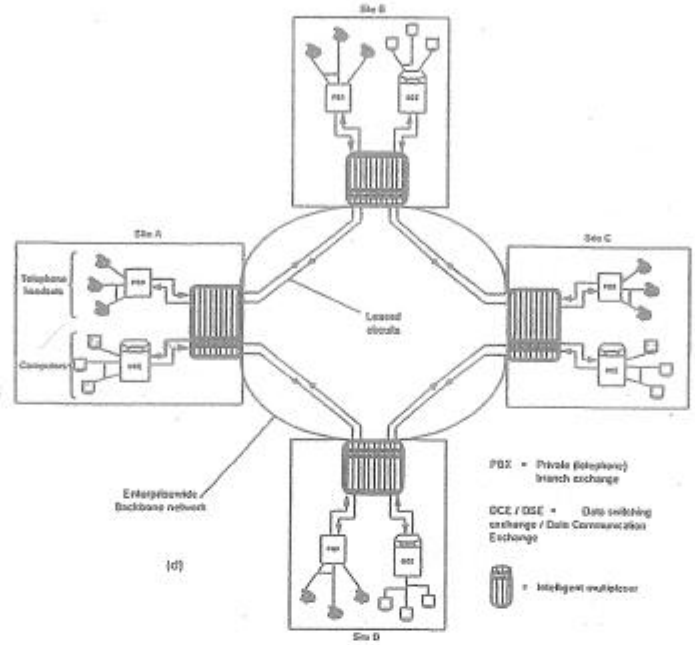
۲ـ۱ روند پیشرفت شبکه‌های کامپیوتری

در ابتدا طراحی شبکه‌های کامپیوتری به صورت موردی و خاص و با معماری‌های گوناگون و ناسازگار با یکدیگر انجام می‌شد و هر شرکت معماری و روش غیر استاندارد خودش را داشت. بنابراین قابلیت اتصال به کامپیوترهای شرکت‌های دیگر وجود نداشت و به همین دلیل به آن‌ها شبکه‌های بسته (Closed Network) گفته می‌شد. برای مثال شکل ۱ دو کامپیوتر را نشان می‌دهد که به طور مستقیم به یکدیگر متصل شده‌اند. این‌گونه شبکه‌ها از نوع شبکه‌های خصوصی با وسعت یک شرکت (Enterprise Network) بودند.



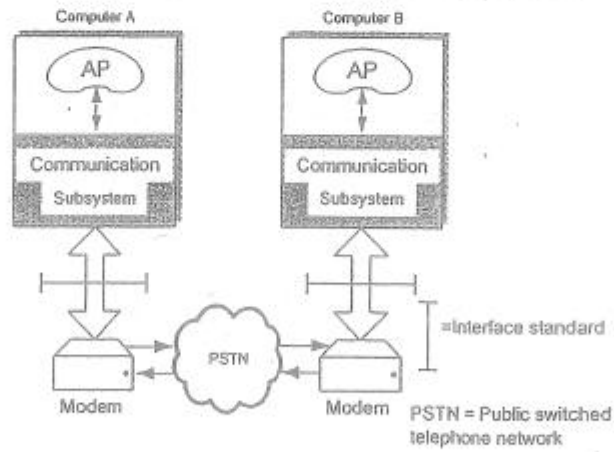
شکل ۱ . اتصال مستقیم دو کامپیوتر

نمونه دیگر شبکه‌های خصوصی استفاده از خطوط تلفن استیجاری (Leased Line) است که البته گران‌قیمت بوده و فقط شرکت‌ها یا سازمان‌های بزرگ از آن استفاده می‌کردند. شکل ۲ نمونه‌ای از این شبکه‌ها را نشان می‌دهد:



شکل ۲ . شبکه خصوصی Enterprise بر اساس Leased Line

در مقابل شبکه‌های خصوصی و Enterprise، شبکه‌های حامل عمومی (Public Carrier) وجود دارند که استفاده از آن‌ها اقتصادی است و نیاز به ایجاد بستر شبکه (برای مثال سیم‌کشی جدید) وجود ندارد. شبکه عمومی سوئیچ تلفنی (PSTN : Public Swiched Telephone Network) قدیمی‌ترین نوع این شبکه‌ها است. (به شکل ۳ توجه کنید):



شکل ۳. استفاده از شبکه عمومی سوئیچ تلفنی (PSTN) برای انتقال داده‌های دیجیتالی

از آن‌جا که PSTN برای ارسال سیگنال آنالوگ صدا طراحی شده است برای استفاده از این شبکه برای ارسال داده‌های دیجیتال از Modem (مودم) <Modulator / Demodulator> استفاده می‌شود.

در این شبکه‌ها کامپیوترها را DTE (Data Terminal Equipment) و مودم‌ها را DCE (Data Communication Equipment) یا (Data Circuit – terminating Equipment) می‌نامند.

در مقابل، روش انتقال بدون مدولاسیون داده‌های دیجیتال Binary را انتقال باند پایه (Base band) می‌نامند. ارسال داده‌های دیجیتال باند پایه بر دو نوع است:

۱ـ سریال : Bit – Serial mode

۲ـ موازی: Word – Parallel mode

برای تبدیل این دو مود به یکدیگر از Serial – to – parallel convertor و بالعکس استفاده می‌شود.

استاندارد سازی

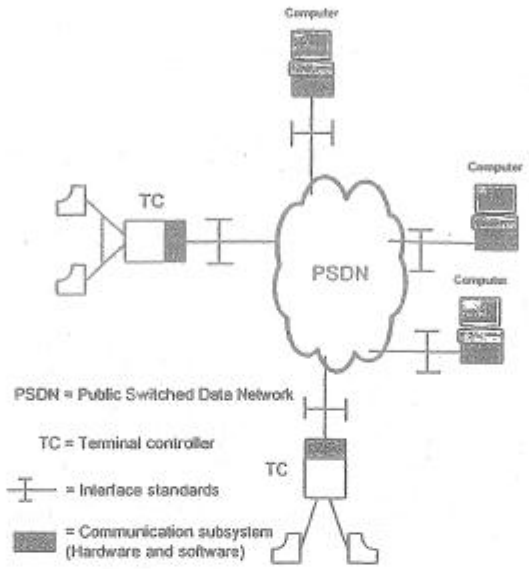
اولین استانداردها به علت علاقه صاحبان شبکه‌های عمومی (Public Carrier) به اتصال محصولات شرکت‌های مختلف به آن شبکه‌ها، توسط این موسسات شکل گرفت. این استانداردها، فقط در حد استانداردسازی ارتباط دستگاه‌ها به شبکه‌های عمومی است. برای مثال استانداردهای زیر توسط ITU-T شکل گرفته است:

V-Series	استانداردهای سری V برای اتصال تجهیزات و کامپیوترها (DTE) به مودم (DCE) متصل به PSTN
X-Series	استانداردهای سری X برای اتصال تجهیزات و کامپیوترها (DTE) به PSDN
I-Series	استانداردهای سری I برای اتصال تجهیزات و کامپیوترها (DTE) به ISDN

جدول زیر موسسات مهم استانداردکننده را در زمینه شبکه‌های کامپیوتری نشان می‌دهد:

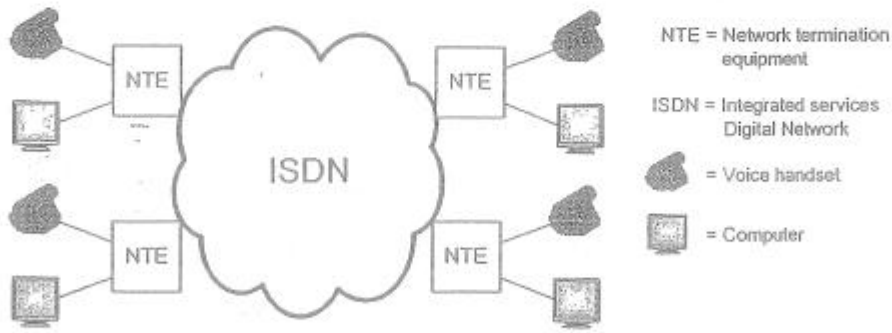
Abbreviation / Acronym	شرح	ملاحظات
ITU-T	International Telecommunication Union – Telecommunication Sector	
CCITT	International Telegraph & Telephone Consultative Committee	نام قدیم ITU-T
ISO	International Standard Organization	
ANSI	American National Standard Organization	شاخه امریکایی ISO
IEEE	Institute of Electrical & Electronics Engineers	LAN Standards
EIA	Electrical Industries Association	
ECMA	European Computer Manufactures Association	
CEPT	Conference European of Post & Telecommunications	

پس از شبکه‌های حامل عمومی سوئیچ تلفنی با گسترش نیاز به انتقال داده‌های دیجیتالی، شبکه‌های حامل عمومی مخصوص انتقال داده‌های دیجیتالی (Public Carrier Data Network) به وجود آمد. در شبکه‌های PSDN (Pubic Switched Data Network) مانند X.25 داده‌ها به صورت دیجیتال ارسال می‌شود. به شکل ۴ توجه نمایید.



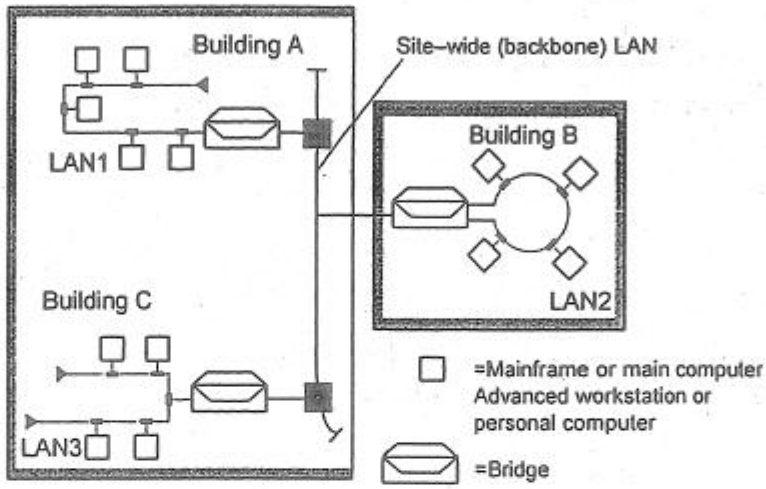
شکل ۴ استفاده از شبکه عمومی سوئیچ داده (PSDN) برای انتقال داده‌های دیجیتالی

ایده ISDN (Integrated Services Digital Networks) از ارتقا شبکه‌های PSTN برای پشتیبانی از ارسال داده‌های دیجیتال بدون نیاز به Modem سرچشمه گرفته است. این شبکه‌ها مثل ترکیب PSTN و PSDN عمل می‌کنند. به شکل ۵ نگاه کنید.



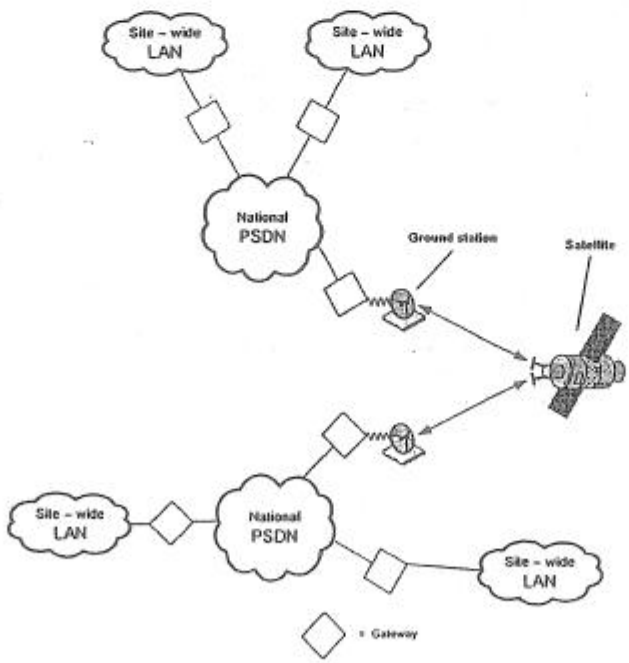
شکل ۵. استفاده از شبکه دیجیتال سرویس مجتمع (ISDN) برای انتقال داده‌های آنالوگ و دیجیتال در کنار یکدیگر

نرخ ارسال داده‌های دیجیتال در یک کانال انتقال داده با واحد بیت بر ثانیه (bps:bit per second) اندازه‌گیری می‌شود و واحدهای بزرگتر آن Kbps $(10^3 bps)$، Mbps $(10^6 bps)$ و Gbps $(10^9 bps)$ می‌باشد. هر چه ظرفیت یک کانال دیجیتال بیشتر باشد می‌توان داده‌ها را با نرخ بالاتر ارسال کرد و کانال دارای پهنای باند (Bandwidth) وسیع‌تر است. شکل ۶، سه شبکه LAN را نشان می‌دهد که با یک کانال دارای پهنای باند وسیع که به آن ستون فقرات (Backbone) شبکه گفته می‌شود به یکدیگر متصل شده‌اند.



شکل ۶. اتصال سه شبکه LAN با یک کانال دارای پهنای باند وسیع (Backbone)

شبکه‌های گسترده (WAN) از اتصال شبکه‌های LAN به یکدیگر ایجاد شده‌اند. اگرچه این شبکه‌ها دارای فن‌آوری‌ها، پروتکل‌ها (Protocol) < قوانین استاندارد حاکم بر شبکه > و استانداردهای متفاوتی هستند، اما پل‌ها (Bridge)، مسیریاب‌ها (Router) و دروازه‌ها (Gateway) اتصال شبکه‌های مختلف به یکدیگر را امکان‌پذیر ساخته است. به شکل ۷ توجه نمایید.



شکل ۷. اتصال شبکه‌های LAN و ایجاد شبکه‌های گسترده در مقیاس کشوری، قاره‌ای و جهانی

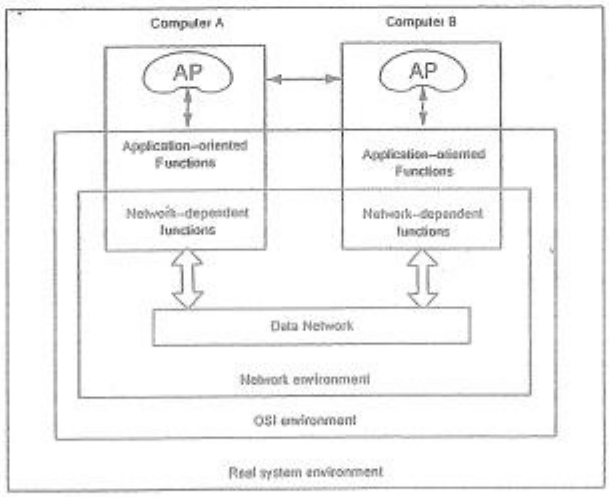
در همین راستا، گروه تحقیقاتی DARPA در وزارت دفاع آمریکا پروژه‌ای را برای اتصال ابر کامپیوترها به یکدیگر و ایجاد ارتباط بین شبکه‌ای (Internetworking) انجام داد که در نهایت منجر به پیدایش شبکه جهانی Internet گردید.

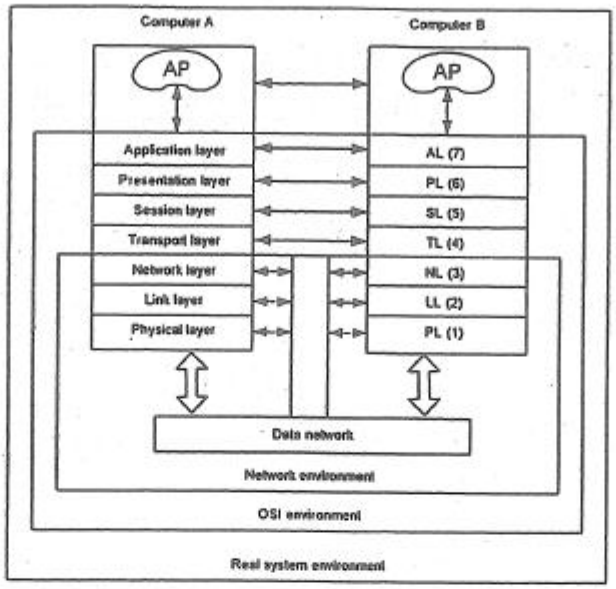
امروزه شبکه‌های استاندارد پیشرفته‌ای مانند ATM (Asynchronous Transfer Mode) وجود دارند که داده‌ها را با نرخ چند Gbps در مقیاس LAN و WAN انتقال می‌دهند. این شبکه‌ها علاوه بر سرعت بالا و پشتیبانی از سرویس‌های مختلف چند رسانه‌ای (Multimedia)، تضمین می‌نمایند که نیازهای مختلف QoS (Quality of Service) کاربران (معیارهایی نظیر تأخیر (Delay)، گذردهی (Throughput)، نسبت از دست دادن بسته‌ها (Packet Loss Ratio) و نوسان یا واریانس تأخیر (Jitter)) را تحقق بخشند. پس از ATM، فناوری پیشرفته MPLS (Multi Protocol Label Switching) در شبکه اینترنت، پشتیبانی از سرویس‌های مختلف چند رسانه‌ای و QoS را با پهنای باند بالا دنبال می‌کند.

۳ـ۱ سیستم‌های باز (Open System)

به تدریج با استفاده روز افزون شبکه‌ها و ارتباطات چند رسانه‌ای ، علاوه بر استانداردسازی واسط‌ها نیاز به استاندارد کردن لایه‌های بالاتر در ارتباط با فرمت، Syntax و کنترل تبادل داده موجب پیدایش استانداردهایی شد که تلاش دارد که محصولات همه شرکت‌ها بتوانند در لایه‌های مختلف ارتباطی به راحتی به یکدیگر متصل شوند و کار کنند. این استانداردها را اتصال سیستم باز (OSI: Open System Interconnection) گویند.

موسسه بین‌المللی استاندارد (ISO) یک استاندارد هفت‌لایه‌ای را در این ارتباط بوجود آورده است. در این استاندارد، هر لایه با لایه متناظر (Peer) خود صحبت می‌کند (بر اساس قوانینی به نام Protocol) و از سرویس لایه پایین‌تر استفاده می‌کند. به تفاوت بین مفهوم پروتکل و سرویس دقت نمایید. شکل ۸ و ۹ لایه‌های این استاندارد (ISO/OSI) را نشان می‌دهند.





شکل ۸. مدل استاندارد هفت‌لایه‌ای ISO/OSI

وظایف لایه‌های استاندارد OSI

۱ـ Physical Layer (لایه فیزیکی)

واحد داده‌های انتقالی : بیت (Bit)

هدف: تعریف واسط‌های الکتریکی و مکانیکی شبکه (این لایه یک خط دارای خطا را به لایه‌های بالاتر ارایه می‌کند)

وظایف: استانداردسازی موارد ذیل:

۱ـ شکل موج (پالسی ، سینوسی و غیره)

۲ـ مدولاسیون (PSK, FSK,ASK,FM,AM و غیره) و کدگذاری (NRZ-L، RZ، Manchester، HDB3 و غیره)

۳ـ دامنه (بر حسب ولت یا آمپر)

۴ـ عرض بیت (بر حسب µs)

۵ـ نحوه نمونه‌برداری(Sampling، Quantization و غیره با حداقل خطا)

۶ـ واسط‌های مکانیکی (Connectorها،Jackها ، Keystone ها و غیره)

۷ـ زمان‌بندی و سیگنالینگ (Timing، Handshake و غیره)

۸ـ مالتی پلکسینگ (TDM، FDM، WDM و غیره)

۲ـ Data Link Layer (لایه پیوند داده یا لایه پیوند)

واحد انتقال داده: فریم (Frame)

هدف: کنترل پیوند داده (این لایه می‌تواند یک خط بدون خطا و دارای کنترل جریان را به لایه‌های بالاتر ارایه دهد)

وظایف:

۱ـ Framing: شناسایی ابتدا و انتهای فریم

۲ـ Flow Control: تطبیق سرعت فرستنده و گیرنده

- ۱ـ مشکل عدم آمادگی CPU به علت پردازش وقفه قبلی
- ۲ـ مشکل عدم فضای کافی در بافر

۳ـ Error Control

- ۱ـ تشخیص خطا (Error Detection): مانند Parity، VRC، LRC، CRC و غیره
- ۲ـ تصحیح خطا (Error Correction): مانند Hamming، Acknowledge و غیره

۴ـ کنترل دسترسی به رسانه‌های مشترک انتشاری مثل پروتکل زیر لایه کنترل دسترسی به رسانه یا MAC (Medium Access Control) مانند: استانداردهای IEEE 802.x

۳ـ Network Layer (لایه شبکه)

واحد انتقال داده: بسته (Packet)

وظایف:

۱ـ مسیریابی در شبکه (Network Routing)

۲ـ جلو بردن (پیش‌بری) بسته‌ها در شبکه (Packet Forwarding)

۳ـ جلوگیری از ازدحام (Congestion Control)

۴ـ Addressing (مثل IP Address)

۵ـ برپایی و آزادسازی مکالمه Call Setup / Release در ارتباطات نوع Connection Oriented (اتصال گرا)

۶ـ تطبیق پروتکل‌ها در ارتباطات بین شبکه‌ای (Internetworking)

(به عبارت دیگر اتصال دو شبکه که ۳ لایه پایین آن‌ها متفاوت است به وسیله Router)

۷ـ Flow Control (کنترل جریان بین کامپیوتر و واسط شبکه)

۴ـ Transport Layer (لایه حمل)

واحد انتقال داده: پیغام (Message)

هدف: انتقال داده End – to – End پیغام‌ها

وظایف:

۱ـ Connection Management

۲ـ تقسیم پیغام به بسته‌ها و بالعکس (fragmentation / Defragmentation) و شماره‌گذاری بسته‌ها

۳ـ Error Control

۴ـ Flow Control (تطبیق سرعت میزبان‌های سریع و کند)

۵ـ QoS (Quality of Service) و پشتیبانی از چندین Class سرویس‌دهی

۶ـ تضمین دریافت صحیح داده‌ها با سرویس‌دهی مستقل از نوع شبکه برای ارسال پیغام‌های لایه پنجم به مقصد (فرض کنید بر روی یک لایه ۳ از نوع Connection less و نامطمئن قرار دارد)

۵ـ Session Layer (لایه جلسه یا نشست)

واحد انتقال داده: پیغام

هدف: کنترل ، سازماندهی، مدیریت و همگام‌سازی (Synchronization) جلسه بین مبدا و مقصد

وظیفه اصلی:

ـ Setup و Release جلسه از طریق یک کانال ارتباطی بین مبدا و مقصد برای کل زمان مکالمه

اقدامات خاص:

- برای ارتباط Half Duplex، همگام‌سازی و تعیین زمان شروع و پایان ارسال برای هر طرف
- برای مکالمات طولانی، تعیین نقاط شکست (Synchronization Point Transaction) برای همگام‌سازی (در صورت وقوع خطا، ارسال مجدد از آن نقاط انجام می‌شود (و نه از ابتدای مکالمه طولانی))
- گزارش خطاهای غیرقابل حل به لایه‌های بالاتر (Exception Reporting)

۶ـ Presentation Layer (لایه ارایه)

واحد انتقال داده: پیغام

هدف: مذاکره برای تعیین Syntax ها، نحوه بیان داده‌ها و غیره

وظایف: وظیفه این لایه ارسال و دریافت پیغام‌ها مستقل از نوع Syntax آن‌هاست که شامل موارد ذیل است:

۱ـ Data Representation (نحوه بیان داده‌ها و Syntax داده‌ها)

۲ـ فشرده‌سازی و باز کردن کدها (Compression / Decompression)

۳ـ رمز نگاری و رمزگشایی به منظور ایجاد امنیت و محرمانگی (Security و Encryption / Decryption)

۴ـ تبدیل کدینگ‌های مختلف به یکدیگر (مانند ASCII به ABCDIC)

۷ـ Application Layer (لایه کاربرد)

واحد انتقال داده: پیغام

هدف: ایجاد محیط مناسب جهت ارتباط برنامه‌های کاربردی کاربر انتهایی با سرویس‌های توزیع اطلاعات شبکه‌ای مانند Telnet, FTP و غیره از طریق Primitiveهای (عناصر بنیادی) سیستم عامل (فراخوان‌های سیستمی) به همراه پارامترهای مربوطه.

وظایف:

۱ـ File Transfer Access of Management: مدیریت ارسال فایل‌ها (مانند FTP)

۲ـ Document & Message Interchange : ارسال و دریافت پیغام‌ها و مدارک نظیر E.Mail (مانند SMTP)

۳ـ Job (process) Transfer & Manipulation: ارسال فرآیندها در شبکه و اجرای آن‌ها در ماشین‌های دور و به عبارت دیگر Remote login (مانند Telnet)

۴ـ تطبیق ترمینال‌های مختلف و متفاوت (Virtual Terminal)

۵ـ Direcoty Service: بانک‌های اطلاعاتی Name Server که برای شناسایی طرف مقابل به وسیله نام (به جای آدرس) به کار می‌روند (مانند DNS در اینترنت)

۶ـ تعیین این‌که آیا طرف مقابل ارتباط در حال حاضر در دسترس هست یا خیر

۷ـ واگذاری اختیارات (Authority) به طرف مقابل

۸ـ توافق بر سر مکانیزم‌های خصوصی‌سازی مثل رمزنگاری

۹ـ احراز هویت طرف مقابل (Authentication)

۱۰ـ توافق بر سر مسئولیت‌های ترمیم خطا

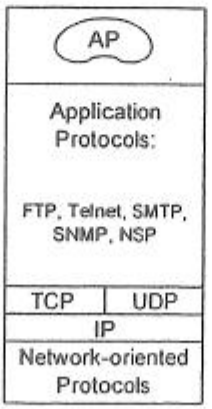
۱۱ـ شناسایی محدودیت‌ها بر روی Syntax های داده (ساختار داده، مجموعه کاراکترها و غیره)

۴ـ۱ ارتباطات بین شبکه‌ای (Internetworking)

برای اتصال شبکه‌های LAN و یا WAN به یکدیگر، ابتدا باید ببینیم که این شبکه‌ها از لایه یک تا چه لایه‌ای با یکدیگر متفاوت هستند. جدول زیر نشان می‌دهد که بسته به لایه‌های متفاوت دو شبکه از چه ابزارهایی برای اتصال آن‌ها استفاده می‌شود:

نام ابزار	تفاوت لایه‌های شبکه‌های متصل	شرح	مثال
Repeater (تکرارکننده)	–	دو شبکه کاملاً یکسان را به هم متصل می‌کنند و فقط به منظور تقویت سیگنال‌های الکتریکی به کار می‌روند	مانند اتصال دو قطعه (Segment) شبکه Ethernet (IEEE 802.3) به دلیل محدودیت طول کابل ناشی از پدیده تضعیف
Bridge (پل)	حداکثر تفاوت در لایه ۱ و ۲	۱) برای اتصال دو LAN متفاوت که تا زیر لایه MAC (از لایه ۲) با یکدیگر متفاوتند. ۲) برای تقسیم یک LAN بزرگ به چند LAN کوچک به منظور تقسیم بار و جلوگیری از ازدحام (Congestion) ۳) برای اتصال دو LAN از طریق شبکه‌های گسترده PSTN از پل راه دور (Remote Bridge) استفاده می‌شود.	مانند اتصال دو شبکه LAN از نوع Ethernet (IEEE 802.3) و Token Ring (IEEE 802.5)
Router (مسیریاب)	حداکثر تفاوت در لایه ۱ تا ۳	برای اتصال دو شبکه که در لایه‌های ۱ تا ۳ با یکدیگر متفاوتند به کار می‌روند تا مسیریابی و هدایت بسته بین دو شبکه و نیز تبدیل و تطبیق پروتکل های شبکه را انجام دهند.	مانند اتصال دو شبکه Ethernet و X.25
Gateway (دروازه)	تفاوت در بیش از ۳ لایه پایین	برای اتصال دو شبکه کاملاً متفاوت که حتی از نظر مدل لایه‌ای با یکدیگر متفاوتند. به آن‌ها مبدل پروتکل (Protocol Converter) نیز گفته می‌شود.	مانند اتصال یک شبکه با مدل لایه‌ای OSI به یک شبکه با مدل لایه‌ای TCP/IP

شکل ۹ مدل لایه‌ای TCP/IP را نشان می‌دهد که مدل شبکه اینترنت است و به وفور در شبکه‌ها مورد استفاده قرار می‌گیرد. نقطه قوت این استاندارد این است که لایه Network-oriented این شبکه‌ها، هر استانداردی می‌تواند باشد. برای مثال می‌توان TCP/IP را بر روی Ethernet ، X.25 و حتی ATM قرار داد.



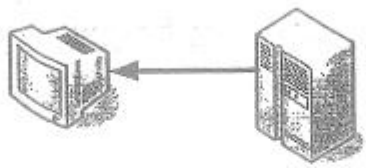
IP = Internet Protocol
TCP = Transmission Control Protocol
UDP = User Datagram Protocol
FTP = File Transfer Protocol
Telnet = Remote login
SMTP = Simple Mail Transfer Protocol
SNMP = Simple Network Management Protocol
NSP = Name Server Protocol

شکل ۹. مدل لایه‌ای TCP/IP

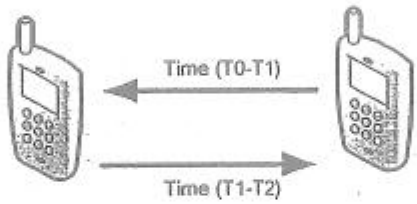
۵ـ۱ حالت‌های ارسال

درکانال‌های انتقال داده، سه حالت یا مود (Mode) ارسال وجود دارد که عبارتند از:

۱ـ ساده (Simple یا Simplex) یا یک طرفه که به آن SX نیز گفته می‌شود. این روش مخصوص ارسال یک سویه داده‌ها است که همواره یک طرف فرستنده و یک طرف گیرنده است. مانند ارتباط داده بین چاپگر، صفحه کلید یا ماوس با کامپیوتر (پردازنده).



۲ـ نیمه دوطرفه (Half Duplex) که به آن HDX نیز گفته می‌شود. در این روش می‌توان داده‌ها را بر روی کانال ارسال و دریافت کرد اما نه به طور همزمان (در هر لحظه ارتباط یک سویه است اما می‌توان جهت ارسال را تغییر داد. مانند: دستگاه بی‌سیم.



۳ـ کاملاً دو طرفه (Full Duplex) که به آن FDX نیز گفته می‌شود. در این روش همزمان می‌توان داده‌ها را بر روی کانال ارسال و دریافت کرد مانند: تلفن

۶ـ۱ رسانه‌های انتقال (Communication Media)

رسانه‌های انتقال دادهٔ متعددی وجود دارد که انتخاب آن‌ها به توپولوژی، پهنای باند یا نرخ بیت موردنیاز، محدوده فرکانسی امواج، فاصله فرستنده تا گیرنده، میزان تاثیر عوامل مخربی نظیر تضعیف، نویز، همشنوایی، تداخل و اعوجاج و نیز معیارهای QoS کاربران و نوع کاربرد بستگی دارد. به طور کلی رسانه‌های انتقال به دو دسته تقسیم می‌شوند:

۱ـ رسانه‌های هدایت شونده مانند زوج سیم به هم تابیده (به هم تافته)، کابل هم محور و فیبر نوری

۲ـ رسانه‌های غیر هدایت شونده مانند هوا، خلأ و آب با تکنیک‌هایی نظیر بی‌سیم، پخش رادیو، مایکروویو، ماهواره و مادون قرمز

۱ـ۶ـ۱ زوج سیم به هم تابیده (Twisted Pair)

یک زوج سیم مسی را به صورت منظم مارپیچی با الگوهای خاص محاسبه شده به هم می‌تابند تا اثر نویز و همشنوایی بر روی هر دو یکسان باشد و اختلاف پتانسیل اثر نویز بر روی آن‌ها صفر باشد. تعدادی زوج سیم به هم تابیده را در داخل یک کابل روکش دار قرار می‌دهند. برای مثال کابل‌های UTP (Unshielded Twisted Pair) در گونه‌ها یا دسته‌های مختلف (مانند Cat3 , Cat 5 و Cat6)

برای شبکه‌های Fast Ethernet با سرعت 100Mbps و Gigabit Ethernet با سرعت 1Gbps مورد استفاده قرار می‌گیرد. همچنین نوع STP (Shielded Twisted Pair) با حفاظ فلزی برای کاهش اثرات نویز خارجی با قیمت بیشتر عرضه می‌شود. به شکل ۱۰–b و ۱۰–c نگاه کنید.

ویژگی‌ها:

- نرخ انتقال داده: حدود 10Mbps تا 1Gbps
- پهنای باند آنالوگ (در محدوده 0 تا 1MHz)
- فاصله: کم (به علت پدیده تضعیف) برای مثال در Fast Ethernet حداکثر طول خط 100 متر است. برای فواصل بیشتر باید نرخ انتقال را کاهش داد و یا از تکرار کننده استفاده کرد.
- تضعیف: زیاد (وابسته به فرکانس)
- تاثیر نویز: زیاد به ویژه در UTP
- قیمت: رسانه قدیمی، متداول و ارزانتر از کابل هم محور و فیبر نوری
- نوع سیگنال: الکتریکی (آنالوگ یا دیجیتال)
- کاربرد: تلفن (فواصل نزدیک)، LAN و غیره

زوج سیم معمولی نیز برای فواصل نزدیک مانند اتصالات اجزای یک کامپیوتر به یکدیگر به کار می‌رود (شکل۱۰-a) برای مثال یک HDD توسط یک Flat ribbon به Main board متصل می‌شود.

۲ـ۶ـ۱ کابل هم محور (Coaxial Cable)

کابل هم محور شامل یک سیم مسی سخت با نام مغزی (Core) است که حول آن را یک ماده عایق فرا گرفته و دور ماده عایق یک هادی استوانه‌ای (هم‌محور با مغزی) وجود دارد که اغلب به شکل توری است و توسط یک پوشش محافظ پلاستیکی احاطه شده است. این ساختار کابل‌های هم محور باعث کاهش اثر عوامل مخربی مانند تضعیف (به علت اثر پوسته) و نویز و همشنوایی (به خاطر ساختار هندسی حفاظت شده آن) شده است. کابل‌های هم محور در گونه‌های مختلف (مانند ۵۰ اهم و ۷۵ اهم) مورد استفاده قرار می‌گیرد. نوع ۵۰ اهم آن را کابل هم محور باند پایه گویند که برای انتقال اطلاعات دیجیتال باند پایه و نوع ۷۵ اهم آن را کابل هم محور باند پهن گویند که برای انتقال اطلاعات آنالوگ در تلویزیون کابلی کاربرد دارد. به شکل ۱۰–d نگاه کنید.

ویژگی‌ها:

نرخ انتقال داده: حدود 10Mbps تا 100Mbps (برای کابل‌های ۵۰ اهم)

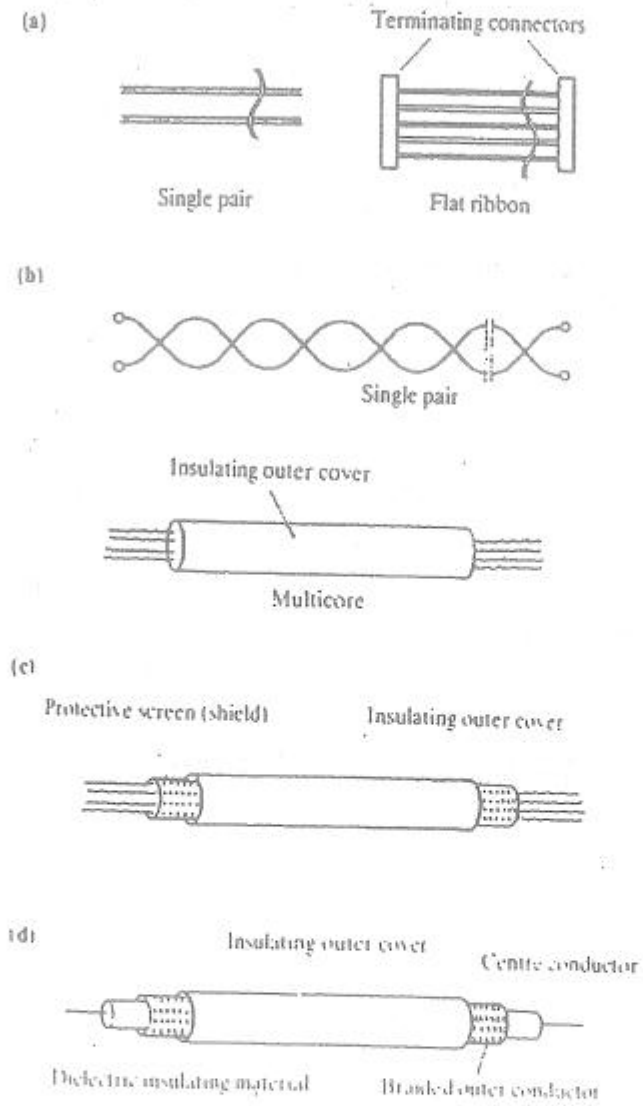
پهنای باند آنالوگ: در محدوده 0 تا 500MHz (برای کابل‌های ۷۵ اهم)

تضعیف: از زوج سیم به هم تابیده کمتر است. (وابسته به فرکانس)

تاثیر نویز: از نظر نویز خارجی مانند نویز ضربه‌ای همشنوایی و نیز تداخل از زوج سیم به هم تابیده بهتر است.

نوع سیگنال: الکتریکی (آنالوگ یا دیجیتال)

کاربرد: تلفن راه دور، تلویزیون کابلی ، LAN و غیره



شکل ۱۰ . a) زوج سیم b) زوج سیم به هم تابیده c) زوج سیم به هم تابیده حفاظ‌دار d) کابل هم محور

۳ـ۶ـ۱ فیبر نوری (Optical Fiber)

گسترش کاربرد چند رسانه‌ای و نیاز به نرخ انتقال داده بسیار بالا از یک طرف و رشد سریع فناوری اپتیک از طرف دیگر باعث پیدایش فیبر نوری و متداول شدن آن در سیستم های انتقال داده گردید. در فیبر نوری، سیگنال‌های دیجیتال به صورت قطع و وصل شدن (چشمک زدن) یک اشعه نوری ارسال می‌شود. وجود نور نشان‌دهنده منطق یک و قطع نور نشان‌دهنده منطق صفر می‌باشد. سیستم‌های انتقال داده نوری از سه قسمت تشکیل می‌شوند:

۱ـ منبع نوری (طرف فرستنده) که معمولاً یک دیود نوری ساده (LED) و در موارد خاص دیود لیزری (LD) است.

۲ـ آشکارساز نوری (طرف گیرنده) که معمولا یک فوتو دیود یا فوتو ترانزیستور است که با تابش نور یک پالس الکتریکی تولید می‌نماید.

۳ـ رسانه انتقال که همان فیبر نوری است.

یک فیبر نوری از سه قسمت اصلی تشکیل شده است (شکل a-۱۱) که عبارتند از:

۱ـ مغزی (Optical Core): یک ماده شفاف مانند شیشه ، پلاستیک و یا سیلیکون

۲ـ غلاف (Optical Cladding): یک ماده شفاف مانند شیشه با ضریب شکست متفاوت با مغزی که از موادی مانند شیشه، پلاستیک و یا سیلیکون ساخته می‌شود و این دو با هم یک تار فیبر نوری بسیار نازک و انعطاف‌پذیر را تشکیل می‌دهند.

۳ـ روکش پلاستیکی که یک یا چند تار در داخل آن قرار دارد.

انواع مختلفی از فیبر نوری وجود دارند (شکل b-۱۱) که عبارتند از:

۱ـ فیبر نوری چند حالته با ضریب شکست پله‌ای (Multimode Stepped Index)

۲ـ فیبر نوری چند حالته با ضریب شکست تدریجی (Multimode Graded Index)

۳ـ فیبر نوری تک حالته (Monomode یا Single Mode)

فیبر نوری چند حالته با ضریب شکست پله‌ای

اساس کار این فیبر نوری بر پایه اصل شکست نور در انتقال از محیط مغزی به محیط غلاف می‌باشد. میزان شکست به نسبت ضریب شکست دو محیط بستگی دارد. از آن‌جا که چگالی مغزی بیش از غلاف است ضریب شکست مغزی بیش از ضریب شکست غلاف است و بنابراین زاویه بازتابش از زاویه تابش بزرگتر است (می‌دانیم اگر θ_i زاویه تابش و θ_r زاویه بازتابش باشد و ضریب شکست مغزی را با I_{core} و ضریب شکست غلاف را با $I_{cladding}$ نامگذاری کنیم، آن‌گاه $\frac{\sin(\theta_i)}{\sin(\theta_r)} = \frac{I_{cladding}}{I_{core}}$ خواهد بود)

حال اگر زاویه تابش برابر زاویه حد (زاویه بحرانی) باشد زاویه بازتابش 90 درجه خواهد بود و اگر زاویه تابش بزرگتر از زاویه حد (زاویه بحرانی) باشد نور در برخورد به غلاف منعکس کننده دچار انعکاس کلی به داخل مغزی خواهد شد و این کار آنقدر تکرار می‌شود تا نور به مقصد برسد (شکل b(i)-۱۱)

فیبر نوری چند حالته با ضریب شکست تدریجی

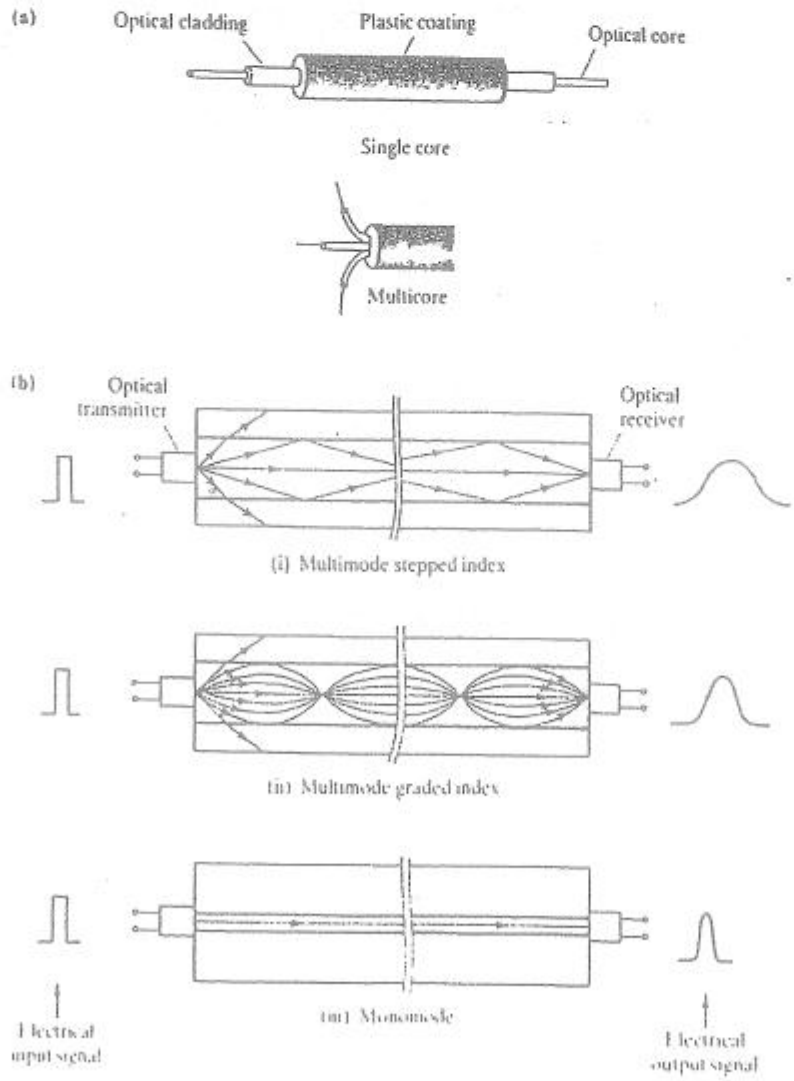
از آن‌جا که در فیبر نوری چند حالته با ضریب شکست پله‌ای شعاع‌های نوری که با زاویه تابش متفاوت دچار انعکاس می‌شوند همزمان به مقصد نمی‌رسند، عرض پالس در مقصد بیشتر شده و به دلیل تداخل پالس‌های مجاور نمی‌توان نرخ انتقال داده را از یک حد بالاتر برد. برای رفع این مشکل از فیبر نوری چند حالته با ضریب شکست تدریجی استفاده می‌شود که باعث می‌شود نور به تدریج و شبیه موج سینوسی بشکند. سرعت نور در هسته به دلیل چگالی بالاتر بیشتر است و لذا همه شعاع‌های نوری همزمان به مقصد می‌رسند. بنابراین به دلیل نزدیکتر شدن عرض پالس در گیرنده به عرض پالس در فرستنده، نرخ انتقال در آن‌ها بیشتر است. (شکل b(ii)-۱۱)

فیبر نوری تک حالته

قطر این فیبرهای نوری بسیار کوچک و در حد چند میکرون است و نور در داخل آن‌ها در خط مستقیم و بدون انعکاس منتشر می‌شود. فرستنده آن‌ها الزاما دیود لیزری (LD) است. تغییرات عرض پالس در آن‌ها ناچیز است و موجب تداخل پالس‌های نزدیک هم نمی‌شود و لذا بازده و نرخ بیت بسیار بالاتری (نسبت به دو روش قبلی) دارند وبه علت پایین بودن Diffraction برای فواصل دورتر نیز به کار می‌روند (شکل b(iii)-۱۱)

ویژگی‌ها:

- **نرخ انتقال داده:** با توجه به فرکانس بالای نور (10^{14} تا 10^{15} هرتز که محدوده مادون قرمز و طیف نور مرئی است) بسیار بالا است ؛ از چندین Gbps تا چندین Tbps با مالتی پلکسینگ WDM.
- **فاصله:** زیاد (از حدود 1 کیلومتر تا حدود 40 کیلومتر)
- **تضعیف:** بسیار کم
- **تاثیر نویز:** نویز الکتریکی مانند نویز ضربه‌ای، همشنوایی و نیز تداخل الکترومغناطیسی بر روی آن تاثیر نمی‌گذارد.
- **نوع سیگنال:** نوری (دیجیتال)
- **مزایا:** عمر طولانی، مقاومت در برابر دما و رطوبت و مواد شیمیایی، قابلیت اطمینان بالا، امنیت بالا در مقابل شنود، حجم و وزن پایین، مواد اولیه فراوان (سیلیکون در طبیعت فراوان‌تر از مس است)
- **کاربرد:** تلفن و مخابرات راه دور، شبکه‌های LAN و WAN سرعت بالا و غیره



شکل 11 . a) فیبر نوری b) اساس کار فیبرهای نوری، (i) فیبر نوری چند حالته با ضریب شکست پله‌ای (ii) فیبر نوری چند حالته با ضریب شکست تدریجی (iii) فیبر نوری تک حالته

۴ـ۶ـ۱ انتقال بی‌سیم (Wireless)

استفاده از فضای آزاد و رسانه‌های هدایت نشده به علت عدم نیاز به کابل‌کشی یک روش مهم در انتقال داده محسوب می‌شود. مشکل اصلی این روش‌ها احتمال تداخل امواج و پر بودن باندهای فرکانسی است.

امواج منتشر شده از طریق آنتن به دو دسته کلی تقسیم می‌شوند:

۱ـ همه جهته (Omni – directional): امواج فرکانس پایین که در همه جهت‌ها منتشر می‌شوند.

۲ـ مستقیم و جهت‌دار (Directional): امواج فرکانس بالای متمرکز که در یک جهت خاص منتشر می‌شوند و در این حالت باید آنتن فرستنده و گیرنده یکدیگر را در یک خط مستقیم و بدون مانع ببینند (خط دید).

حال به نکاتی درباره طیف امواج الکترومغناطیسی، انتشار آن‌ها و قوانین انتقال داده در رسانه‌های هدایت نشده می‌پردازیم.

نکته ۱: طول موج مسیری است که موج در یک پریود طی می‌کند (بر حسب m) و آن را با λ نشان می‌دهیم.

$$V = \lambda f$$

λ: طول موج (به m)

f: فرکانس موج (به Hz یا $\frac{1}{sec}$)

v: سرعت موج (به m/sec)

مثال: اگر ضریب انتشار هوا برابر 0.96 باشد، سرعت موج برابر 0.96c (c سرعت موج یا نور در خلأ است که برابر $3\times10^8\ m/sec$ است) خواهد بود و بنابراین:

$$V = 0.96c = \lambda f$$

این ضریب در کابل‌های فلزی کمتر از هوا می‌باشد.

نکته ۲: تلفات موج (تضعیف) به علت پراکندگی کروی موج در فضا از رابطه زیر بدست می‌آید:

$$\text{تلفات} = \frac{P_T}{P_R} = \left(\frac{4\pi d}{\lambda}\right)^2$$

$$\text{تلفات}(dB) = 10\log_{10}^{\left(\frac{P_T}{P_R}\right)}$$

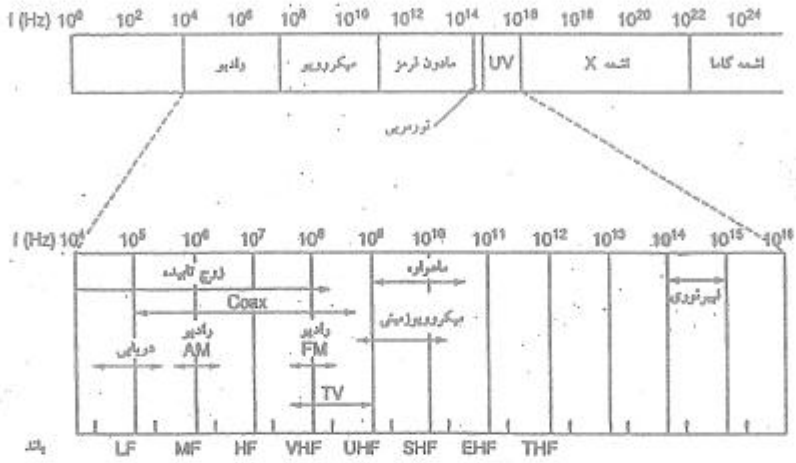
P_T: توان ارسالی (به W)

P_R: توان دریافتی (به W)

d: فاصله گیرنده با فرستنده (به m)

λ: طول موج (به m)

نکته ۳: شکل ۱۲ طیف امواج الکترو مغناطیسی و کاربردهای مخابراتی آن را به انضمام جدول باندهای ماهواره‌ای نشان می‌دهد.



طیف الکترومغناطیس و کاربردهای مخابراتی آن.

باند	دریافت از ماهواره	ارسال به ماهواره	پهنای باند	مشکلات
L	1.5 GHz	1.6 GHz	15 MHz	پهنای باند کم به شلوغ
S	1.9 GHz	2.2 GHz	70 MHz	پهنای باند کم به شلوغ
C	4.0 GHz	6.0 GHz	500 MHz	تداخل زمینی
Ku	11 GHz	14 GHz	500 MHz	باران
Ka	20 GHz	30 GHz	3500 MHz	باران با قیمت بالای تجهیزات

باندهای ماهواره‌ای.

شکل ۱۲. طیف امواج الکترو مغناطیسی و جدول باندهای ماهواره‌ای

به دلیل تفاوت در محدوده فرکانسی امواج الکترومغناطیسی و طبیعت هر کدام از آن‌ها ، ارتباطات بی‌سیم به چند دسته تقسیم می‌گردد:

۱ـ ارتباطات زمینی مایکروویو

۲ـ ارتباطات ماهواره‌ای مایکروویو

۳ـ پخش رادیویی

۴ـ امواج مادون قرمز

ارتباطات زمینی مایکروویو

محدوده فرکانسی: حدود 2GHz تا 40GHz (بخشی از UHF و SHF)

نرخ بیت: از حدود 10Mbps تا چند صد Mbps

نوع امواج: مستقیم و جهت‌دار (Directional) با یک اشعه باریک متمرکز در خط دید دیش آنتن گیرنده

نوع ارتباط: نقطه به نقطه

فاصله (d): وابسته به قطر دیش (h) می‌باشد ($d = 7.14\sqrt{kh}$ که ضریب k در محاسبات تقریبی در حدود 1.25 فرض می‌شود. h قطر دیش به متر و d فاصله فرستنده و گیرنده به km است. برای دیش 3 متری فاصله در حدود 15 کیلومتر می‌باشد. این رابطه تقریبی است و در فناوری جدید آنتن‌های پیشرفته به‌کار نمی‌رود.)

کاربرد: اتصال LANهای دور از هم، شبکه‌های تجاری، تلفن، تلویزیون

نقاط ضعف: تضعیف زیاد در باران به علت جذب انرژی و تبخیر قطرات باران (شبیه اجاق مایکروویو) تداخل فرکانسی در صورت عدم تخصیص پهنای باند و عدم وجود استانداردهای محلی.

ارتباطات ماهواره‌ای مایکروویو

محدوده فرکانسی: حدود 1GHz تا 10GHz

(در فرکانس‌های پایین‌تر از 1GHz تاثیر نویزهای ضربه‌ای، اتمسفری، خورشیدی و کهکشانی زیاد است و در فرکانس‌های بالاتر از 10GHz پدیده تضعیف به علت جذب انرژی سیگنال در اتمسفر بیشتر است)

نرخ بیت: از حدود 10Mbps تا چند صد Mbps

فاصله: اگر ماهواره به ارتفاع 36 هزار کیلومتر از استوا قرار گیرد دوره گردش 24 ساعت دارد و نسبت به زمین ثابت به نظر خواهد رسید.

نویز: تاثیر نویز و تداخل همشنوایی نسبت به فیبر نوری بیشتر است

کاربرد: اتصال LANهای دور از هم، شبکه‌های تجاری، تلفن، تلویزیون

پخش رادیویی

محدوده فرکانسی: حدود 30MHz تا 1GHz (VHF و بخشی از UHF)

نوع امواج: همه جهته (Omni – directional)

نوع ارتباط: انتشاری

تضعیف: بر خلاف مایکروویو حساسیت کمتری نسبت به تضعیف در باران وجود دارد.

مادون قرمز

محدوده فرکانسی: حدود 300GHz تا 200THz

نوع امواج: جهت دار (Directional)

فاصله: نزدیک (داخل اتاق)

نوع ارتباط: نقطه به نقطه

۷ـ ۱ مالتی پلکسینگ (Multiplexing)

معمولا ظرفیت یا پهنای باند یک رسانه انتقال داده از پهنای باند مورد نیاز یک فرستنده بیشتر است و باید بین کاربران مختلف به اشتراک گذاشته شود. تکنیک مالتی پلکسینگ (تسهیم) این امکان را به وجود می‌آورد که به طور همزمان (یا شبه همزمان) چند سیگنال مختلف را از یک خط عبور دهیم و از ظرفیت رسانه به صورت بهینه استفاده کنیم. عمل قرار دادن چند سیگنال بر روی یک خط در مبدا توسط دستگاهی به نام Multiplexer و عمل جداسازی آن‌ها در مقصد توسط دستگاهی به نام Demultiplexer انجام می‌شود.

انواع روش مالتی پلکسینگ به شرح زیر است:

۱ـ مالتی پلکسینگ تقسیم فرکانسی (FDM: Frequency Division Multiplexing)

۲ـ مالتی پلکسینگ تقسیم زمانی (TDM: Time Division Multiplexing) که بر دو نوع است:

۱ـ۲ـ TDM همگام (Synchronous TDM)

۲ـ۲ـ TDM ناهمگام (Asynchronous TDM) یا هوشمند که به آن مالتی پلکسینگ آماری (Statistical Multiplexing)نیز گفته می‌شود

۳ـ مالتی پلکسینگ تقسیم طول موج (WDM: Wave – length Division Multiplexing)

۴ـ مالتی پلکسینگ تقسیم کد (CDM: Code Division Multiple Access یا CDMA)

روش FDM

در روش FDM ابتدا باید سیگنال‌های دیجیتال را به وسیله مدولاسیون به سیگنال‌های آنالوگ تبدیل کرد. فرکانس حامل مدولاسیون سیگنال‌هایی که همزمان بر روی یک رسانه انتقال قرار می‌گیرند متفاوت است، به‌طوری که این سیگنال‌ها در حوزه فرکانس دربانده‌ای فرکانسی جدا از یکدیگر در کنار هم قرار می‌گیرند. (البته با یک فاصله فرکانسی (Guard Band) به منظور جلوگیری از تداخل امواج) این سیگنال‌ها در مقصد به وسیله عمل دی مدولاسیون (Demodulation) قابل جداسازی هستند (دقیقا همانند امواج رادیویی ایستگاه‌های مختلف که همگی در کنار یکدیگر در یک کانال (هوا) منتشر می‌شوند و بخش Tuner رادیو شما قادر است موج دلخواه شما را از سایر امواج جدا سازد.)

روش TDM همگام

در روش Synchronous TDM (گاهی برای سادگی به آن TDM گفته می‌شود) چون نرخ انتقال رسانه بیش از نرخ ترافیک هر یک از سیگنال‌های دیجیتال است، زمان را به برش‌های زمانی (Time Slice) کوچک تقسیم می‌کنیم و در هر برش زمانی بیت‌های مربوط به یکی از سیگنال‌های دیجیتال را بر روی خط قرار می‌دهیم. اگر در این روش یک فرستنده در برش زمانی خودش داده‌ای برای ارسال نداشته باشد، آن برش زمانی هدر می‌رود. دو روش FDM و Synchronous TDM در واقع یک رسانه انتقال را به چندین کانال مجزا تقسیم می‌نمایند.

روش TDM ناهمگام یا مالتی پلکسینگ آماری

در این روش که در شبکه‌های پیشرفته مانند ATM (Asynchronous Transfer Mode) به کار می‌رود، بر خلاف روش قبلی زمان را به برش‌های زمانی مساوی تقسیم نمی‌کنیم و پهنای باند ثابتی را برای هر کانال رزرو نمی‌نماییم؛ بلکه بسته‌ها یا سلول‌های داده ایجاد شده توسط کاربران مختلف را (که به صورت تصادفی ایجاد می‌شوند) بر روی خط قرار می‌دهیم. یعنی ظرفیت نرخ انتقال رسانه را به صورت پویا بین کاربران تقسیم می‌نماییم.

روش WDM

در این روش که در فیبرهای نوری مورد استفاده قرار می‌گیرد، چندین موج نوری با طول موج‌های (Wave – length) مختلف به طور همزمان در یک فیبر نوری منتشر می‌شود. واضح است که برای مثال جداسازی دو سیگنال نوری با طول موج‌های آبی و قرمز در مقصد به سادگی امکان‌پذیر خواهد بود. طول موج برابر است با نسبت سرعت موج به فرکانس موج: $\lambda = \frac{c}{f}$

روش CDM (CDMA)

در این روش که برای مثال در تکنیک طیف گسترده به کار رفته در شبکه‌های محلی بی‌سیم مورد استفاده قرار می‌گیرد، داده‌های مربوط به چند کانال به طور همزمان (بر خلاف TDM) و در یک باند فرکانسی (بر خلاف FDM) و بالطبع در یک طول موج (برخلاف WDM) در یک رسانه مشترک ارسال می‌شود! و برای جدا کردن داده‌ها از روش‌های خاص رمزگذاری و تئوری coding استفاده می‌شود و اطلاعات کانال‌های مجزا به صورت بردارهای متعامد ارسال می‌گردد، تا در گیرنده قابل جداسازی باشند.

۸ـ۱ تخصیص پهنای باند کانال (Bandwidth Allocation)

هنگامی که از یک کانال انتقال داده به طور اشتراکی برای ارسال چندین سیگنال جداگانه (مربوط به فرستنده‌های مختلف) استفاده می‌شود و از روش‌های مختلف مالتی پلکسینگ (روش‌های فوق) استفاده می‌شود، یک موضوع مهم میزان پهنای باند تخصیص یافته به هر یک از ارسال‌کننده‌ها می‌باشد. برای مثال در TDM می‌توان به یک فرستنده نسبت به دیگران برش زمانی بیشتری را تخصیص داد.
پهنای باند مورد نیاز هر فرستنده به نوع ترافیک بسته‌های ارسالی مربوط است که بر دو نوع است:

۱ـ نرخ بیت ثابت (CBR: Constant Bit Rate) : ترافیک‌هایی مانند پخش فیلم ویدیویی یا مکالمات صوتی

۲ـ نرخ بیت متغیر (VBR: Variable Bit Rate): ترافیک‌هایی مانند ارتباط با یک سایت وب یا ارسال E-mail یا Telnet

تخصیص پهنای باند کانال بر دو نوع است:

۱ـ تخصیص ایستا (Static Allocation): به هر فرستنده پهنای باند ثابتی را تخصیص می‌دهد. در ترافیک‌های VBR مناسب نیست، زیرا گاهی پهنای باند هدر می‌رود و گاهی دچار کمبود پهنای باند و کندی ارسال خواهیم شد. مانند روش Circuit Switching که در آن یک مدار خاص در ابتدای کار با پهنای باند ثابت رزرو می‌شود.

۲ـ تخصیص پویا (Dynamic Allocation): پهنای باند به صورت پویا و بر حسب نیاز هر فرستنده به آن تخصیص داده می‌شود. مانند روش Packet Switching (برای مثال در X.25) و نیز روش پیشرفته Virtual Circuit (که برای مثال در ATM به کار می‌رود و سلول‌های داده مانند Circuit Switching از یک مسیر یا مدار خاص که در ابتدای کار برپا شده است ارسال می‌شوند؛ اما همانند Packet Switching پهنای باند ثابتی را اشغال نمی‌کنند، یعنی از مزایای هر دو روش بهره می‌برد.)

کانال تبدیل ص ۲۹ ص ۱۰۲

فصل دوم

آنالیز سیگنال‌ها و عوامل ایجاد خطا در سیستم‌های انتقال داده

عوامل ایجاد اشکال (خطا) در سیستم‌های انتقال داده عبارتند از:

۱ـ تضعیف (Reduce ← Attenuation) : کاهش تدریجی سطح سیگنال در طی حرکت در کانال

۲ـ اعوجاج (Mis shape ← Distortion): تغییر شکل سیگنال در اثر عبور از کانال

← اعوجاج تضعیف <Attenuation Distortion> حاصل از تفاوت میزان تضعیف در فرکانس‌های مختلف

← اعوجاج تاخیر <Delay Distortion> حاصل از تفاوت میزان تاخیر در فرکانس‌های مختلف

← اعوجاج پهنای باند محدود <Bandwidth Distrotion> حاصل عدم توانایی عبور بعضی از مولفه‌های فرکانسی

۳ـ نویز (Noise) : تاثیرات نوسانات ناخواسته تصادفی بر سیگنال

← Crosstalk (همشنوایی) ← مهم‌ترین گونه آن NEXT (Near – End – Crosstalk) (همشنوایی نزدیک انتهای (خط))

← Impulse Noise (نویز ضربه‌ای)

← Thermal Noise (نویز حرارتی) یا White Noise (نویز سفید)

۱ـ۲ تضعیف

سینگالی که در یک کانال انتقال داده منتشر می‌شود هر چه از فرستنده دورتر می‌شود به‌تدریج دامنه آن به دلیل عواملی چون تشعشع (Radration)، اثر پوسته (Skin Effect)، مقاومت کانال و غیره کاهش می‌یابد (چون تلف توان داریم)

نکته ۱: هر چه فرکانس یک سیگنال سینوسی بیشتر باشد، تضعیف آن بیشتر خواهد بود (اثرات تشعشع، پوسته و غیره بیشتر است)

نکته ۲: تضعیف را بر حسب دسی بل (dB) از رابطه زیر بدست می‌آورند.

P_1 (P_T): توان سیگنال در فرستنده (بر حسب وات W). اگر به جای خط انتقال در مورد یک دستگاه صحبت کنیم آن را با P_{in} نمایش می‌دهیم.

P_2 (P_R): توان سیگنال در گیرنده (بر حسب وات W). اگر به جای خط انتقال در مورد یک دستگاه صحبت کنیم آن را با P_{out} نمایش می‌دهیم.

$$\text{تضعیف (به dB)} = 10\log_{10}^{\frac{P_1}{P_2}}$$

مثال ۱: اگر توان سیگنال در فرستنده 400mW و تضعیف کانال 10dB باشد توان سیگنال در گیرنده چقدر است؟

$$10 = 10\log_{10}^{\frac{400}{P_2}} \rightarrow \boxed{P_2 = 40mW}$$

مثال ۲: اگر توان سیگنال در فرستنده 400mW و تضعیف کانال 6dB باشد توان سیگنال در گیرنده چقدر است؟

$$6 = 10\log_{10}^{\frac{400}{P_2}} \rightarrow \boxed{P_2 = 100.475mW}$$

۱ـ۱ـ۲ آنالیز فوریه

برای تحلیل دقیق سیگنال‌ها می‌توان از آنالیز فوریه استفاده کرد. این آنالیز، سیگنال‌ها را از حوزه زمان (V نسبت به t) به حوزه فرکانس می برد و مولفه‌های مختلف فرکانسی یک سیگنال پریودیک (سری فوریه) و یا طیف فرکانسی یک سیگنال غیر پریودیک (تبدیل فوریه) را نشان می‌دهد.

سری فوریه (Fourier Series) یک سیگنال پریودیک V(t)

$T_0 \leftarrow$ پریود سیگنال (بر حسب sec)

$f_0 \leftarrow$ فرکانس سیگنال (بر حسب1/sec)

$\omega_0 \leftarrow$ فرکانس زاویه‌ای سیگنال (بر حسب رادیان بر ثانیه یا rad/sec)

$$\boxed{f_0 = \frac{1}{T_0}} \qquad \boxed{\omega_0 = 2\pi f_0}$$

سری فوریه این سیگنال پریودیک به شکل مقابل نوشته می‌شود:

$$\boxed{V(t) = \underset{\text{مولفه DC (ثابت)}}{a_0} + \sum_{n=1}^{\infty} a_n \cos n\omega_0 t + \sum_{n=1}^{\infty} b_n \sin n\omega_0 t}$$

f_0, ω_0 معرف فرکانس اصلی سیگنال (fundamental frequency) می‌باشند. ضرایب a_i و b_i از روابط زیر به دست می‌آیند:

$$\begin{cases} a_0 = \frac{1}{T_0}\int_0^{T_0} V(t)dt \\ a_n = \frac{2}{T_0}\int_0^{T_0} V(t)\text{Cos}n\omega_0 t\,dt \\ b_n = \frac{2}{T_0}\int_0^{T_0} V(t)\text{Sin}n\omega_0 t\,dt \end{cases}$$

تعبیر سری فوریه این است که یک سیگنال پریودیک از مجموع یک سری سیگنال سینوسی با دامنه‌های مختلف و با فرکانس‌های مختلف (که البته همگی مضارب فرکانس پایه سیگنال اصلی : f_0 ، $2f_0$ ، $3f_0$ ..... هستند) تشکیل می‌شود. این مولفه‌های فرکانسی را **هارمونیک** می‌گویند.

نکته ۱: منظور از پهنای باند یک سیگنال پریودیک، محدودهٔ فرکانسی مولفه‌های آن است. فرض کنید یک سیگنال فقط مولفه‌های a_0 ، a_1 ، a_3 و a_9 را دارد و بقیه ضرایب a_n و b_n صفرند:

$$Bandwidth = f_{High} - f_{Low} = 9f_0 - 0 = 9f_0$$

همین تعریف برای سیگنال‌های غیر پریودیک نیز (در مورد طیف فرکانسی آن‌ها) صادق است.

نکته ۲: منظور از پهنای باند محدود کانال چیست؟

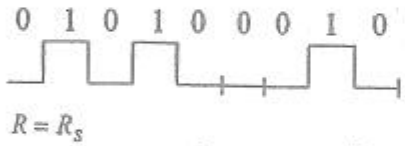
همان‌طور که بیان شد، هر چه فرکانس بالاتر می‌رود تضعیف بیشتر می‌شود. (البته فرکانس‌های پایین تضعیف ندارند) بنابراین کانال مثل یک فیلتر پایین‌گذر (Low Pass) عمل می‌کند. بالاترین فرکانسی که (f_c) بدون تضعیف از کانال عبور می‌کند را پهنای باند کانال می‌نامیم.

سیگنال‌های دیجیتال، نرخ بیت و نرخ سیگنال

R: نرخ بیت (Bit Rate) : تعداد بیت‌های ارسالی در واحد زمان بر حسب بیت بر ثانیه (bps)

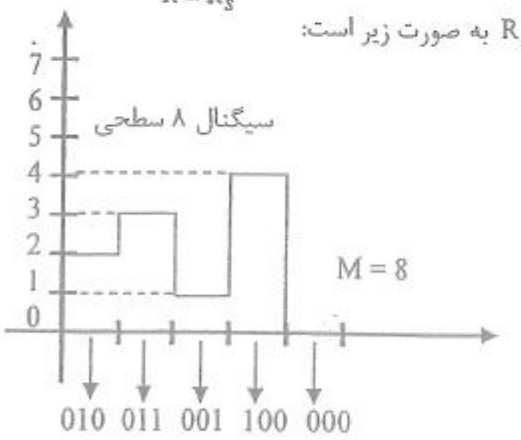
R_s : نرخ سیگنالینگ (Signaling Rate): حداکثر تعداد تغییرسطح سیگنال (چند سطحی) در واحد زمان بر حسب band. تعریف ساده‌تر نرخ سیگنالینگ یا نرخ باود تعداد سمبل (Symbol) های درون سیگنال در واحد زمان می‌باشد.

مثال ۱: برای سیگنال Binary دو سطحی شکل مقابل $R = R_S$ می‌باشد.



$R = R_S$

مثال ۲: برای سیگنال چند سطحی (مثلاً ۸ سطحی شکل زیر) رابطه بین R و R_s به صورت زیر است:



$R = R_s \log_2^M$ تعداد سطح سیگنال $\xrightarrow{\text{مثال ۲}} R = R_s \log_2^8 = 3R_s$

(در مثال ۱: $M = 2 \subset R = R_s \log_2^2 \subset R = R_s$)

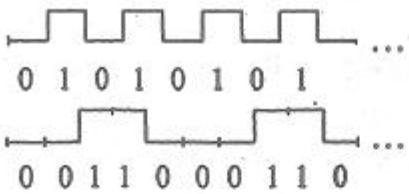
نکته ۱: حالت‌های خاصی وجود دارند که $R < R_s$ است . مثل سیگنالینگ مقابل که در آن

$R = \frac{1}{2}R_s$ می‌باشد:

نکته ۲: چگونه در یک سیگنال دیجیتال از آنالیز فوریه استفاده کنیم؟

پاسخ: یک روش رایج این است که سیگنال را پریودیک فرض کنیم و آن را تکرار یک سری الگو در نظر بگیریم.

مثال ۱: در شکل مقابل پریود سیگنال برابر زمان ارسال الگوی 01 است



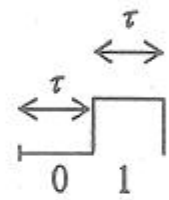
مثال ۲: در شکل مقابل پریود سیگنال برابر زمان ارسال الگوی 00110 است.

بنابراین اگر در مسئله یک الگوی خاص داده شود، سیگنال را تکرار آن الگو در نظر می‌گیریم حتی اگر پریودیک نباشد.

اما اگر الگوی خاصی داده نشود باید worst – case – sequence (ترتیب در بدترین حالت) را در نظر بگیریم. بدترین حالت (بالاترین فرکانس و بالاترین نرخ تغییر حالت‌ها را در ...010101010101 داریم.

لذا اگر یک کانال بتواند این سیگنال را عبور دهد، قطعاً سیگنال‌های دیجیتالی تصادفی را که نرخ تغییر حالت پایین‌تری دارند عبور خواهد داد (به خاطر بیاورید که کانال یک فیلتر پایین گذر است)

τ = عرض بیت (بر حسب Sec)



$$R = \frac{1}{\tau} \text{ bps}$$

$$T_0 = 2\tau \text{ (پریود)} \Rightarrow \boxed{f_0 = \frac{1}{T_0} = \frac{1}{2\tau} = \frac{R}{2}}$$

$\omega_0 = 2\pi f_0$ فرکانس هارمونیک اول worst - case

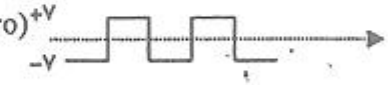
مثال: اگر نرخ سیگنال 500 bps باشد f_0 چقدر است؟

$$f_0 = \frac{R}{2} = \frac{500}{2} = 250\text{Hz}$$

سیگنال‌های Binary به دو روش ارسال می‌شوند.

1) Unipolar (تک قطبی) (Such as RZ:Return to Zero)

2) Polar (قطبی) و Bipolar (دو قطبی) (Such as NRZ: non return to zero)



نکته ۱: سری فوریه Binary دو سطحی worst – case - Sequence در دو حالت فوق به صورت زیر است:

$$\text{Unipolar (Such as RZ)} \rightarrow V(t) = \frac{V}{2} + \frac{2V}{\pi}\left(\cos\omega_0 t - \frac{1}{3}\cos 3\omega_0 t + \frac{1}{5}\cos 5\omega_0 t - .....\right)$$

$$\text{Polar \& Bipolar (Such as NRZ)} \rightarrow V(t) = \frac{4V}{\pi}\left(\cos\omega_0 t - \frac{1}{3}\cos 3\omega_0 t + \frac{1}{5}\cos 5\omega_0 t - ....\right)$$

هارمونیک ۵ هارمونیک ۳ هارمونیک ۱

نتیجه این‌که سیگنال دو سطحی worst case فقط هارمونیک‌های فرد $(f_0, 3f_0, 5f_0, ..)$ را دارد.

نکته ۲: به شکل موج‌های شکل ۱۳ نگاه کنید. فقط کافی است که هارمونیک اول سیگنال عبور کند تا در گیرنده بتوان تشخیص داد که سیگنال اصلی چه بوده است. زیرا از وسط هر بیت یک نمونه‌برداری صورت می‌گیرد و 0 یا 1 بودن آن از هارمونیک f_0 قابل تشخیص است.

نتیجه مهم: اگر حداقل پهنای باند کانال انتقال داده، f_0 باشد سیگنال دیجیتالی دو سطحی در بدترین حالت (Worst – Case - Sequence) قابل تشخیص (در گیرنده) خواهد بود و طبعاً یک سیگنال دیجیتال دو سطحی در حالت کلی نیز از این کانال عبور خواهد کرد.

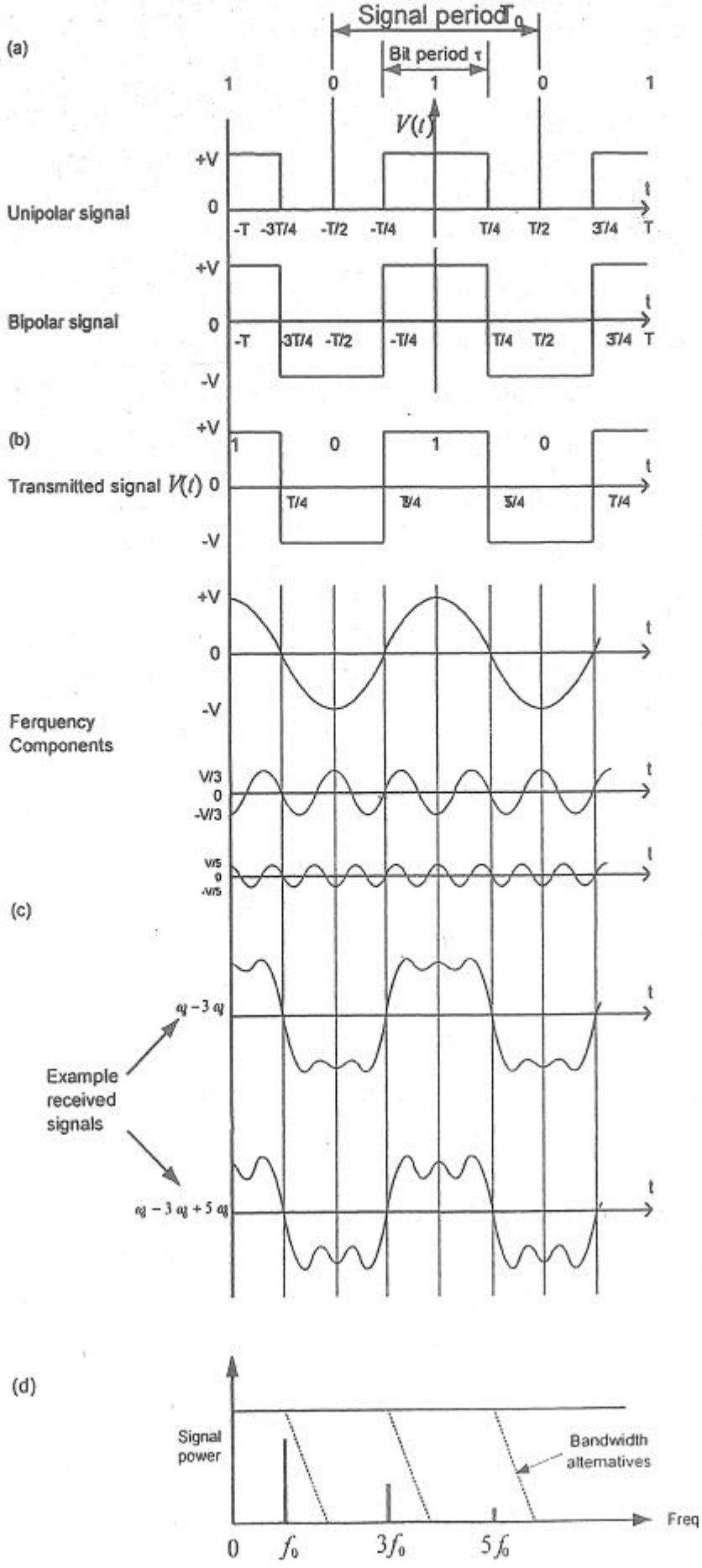
نکته مهم: کارآیی پهنای باند (Bandwidth Efficiency) عبارت است از نسبت نرخ بیت‌های ارسالی (Bit Rate) به پهنای باند کانال:

$$B=\frac{R}{W}$$

R نرخ بیت (بر حسب bps)

W: پهنای باند کانال (بر حسب Hz)

B: کارایی پهنای باند (بر حسب $bps\,Hz^{-1}$)



شکل ۱۳. سری فوریه و هارمونیک یک سیگنال مربعی و مفهوم پهنای باند (a) سه شکل موج بالایی، سیگنال‌های Binary تک قطبی و دو قطبی را نشان می‌دهند. (b) سه هارمونیک سیگنال مربعی فوق. (c) سیگنال دریافتی در اثر عبور تنها ۲ یا ۳ هارمونیک سیگنال ارسالی از کانال (d) پهنای باند کانال در سه حالت مختلف برای عبور هارمونیک (اول)، (اول و سوم) و (اول و سوم و پنجم)

۲ـ۲ اعوجاج

دومین عامل مخرب سیگنال‌ها در کانال‌ها و محیط‌های انتقال داده اعوجاج (Distortion) است که سه عامل اساسی موجب ایجاد آن می‌شود که به ترتیب به بررسی آن‌ها می‌پردازیم.

۱ـ۲ـ۲ اعوجاج پهنای باند

کانال مثل فیلتر پایین گذر عمل می‌کند. لذا مولفه‌های فرکانس بالای (هارمونیک بالای) سیگنال را عبور نمی‌دهد. به شکل ۱۳ نگاه کنید. اگر پهنای باند کانال f_0 باشد، در خروجی فقط مولفه اول را خواهیم داشت یا اگر پهنای باند مثلاً $5f_0$ باشد (دقیق‌تر: $5f_0 \le W < 7f_0$)

در خروجی هارمونیک‌های $5f_0$ و $3f_0$ و f_0 را خواهیم داشت. یعنی سیگنال خروجی مجموع این سه مولفه است که در شکل (c) ۱۳ به صورت $\omega_0 - 3\omega_0 + 5\omega_0$ نشان داده شده است.

نتیجه مهم: هر چه پهنای باند بیشتر باشد، شکل موج در گیرنده به فرستنده شبیه‌تر است و اعواج کمتری داریم.

۲ـ۲ـ۲ اعواج تاخیر

هر چه فرکانس بالاتر می‌رود تاخیر سیگنال بین فرستنده و گیرنده بیشتر می‌شود. $(f \uparrow \Rightarrow \text{delay} \uparrow)$ بنابراین مولفه‌های فرکانس بالا دیرتر می‌رسند. لذا اگر در جمع مولفه‌ها در مقصد برای مولفه‌های فرکانس بالاتر تاخیر اختلاف فاز را هم در نظر بگیری، در نتیجه شکل موج در گیرنده، تغییر می‌کند.

تاخیر زیاد مولفه‌های فرکانس بالا موجب مخلوط شدن آن‌ها با مولفه‌های فرکانسی بیت بعدی می‌شود و به این پدیده Inter symbol Interference (تداخل بین سمبل‌ها) نیز می‌گویند.

۳ـ۲ـ۲ اعواج تضعیف

میزان تضعیف فرکانس‌های بالا بیشتر است. $(f \uparrow \Rightarrow \text{Atenuation} \uparrow)$ این تفاوت تضعیف باعث می‌شود که دامنه مولفه‌های مختلف فرکانسی در اعداد مختلف ضرب شود و لذا شکل موج مجموع آن‌ها دچار اعواج می‌شود.

۳ـ۲ فرمول نایکوییست (Nyquist)

اگر کانال بدون نویز فرض شود، حداکثر نرخ انتقال داده یا ظرفیت (Capacity) کانال از رابطه زیر بدست می‌آید:

$$C = 2W\log_2^M$$

C: حداکثر نرخ انتقال داده (R_{max}) کانال بدون نویز (bps)

W: پهنای باند کانال (Hz)

M: تعداد سطح سیگنال

۴ـ۲ نویز (Noise)

یک کانال انتقال داده در حالت ایده‌آل هنگامی که سیگنالی وجود ندارد ولتاژ صفر دارد، اما در عمل یک سری نوسان تصادفی به نام نویز وجود دارد.

باید توجه نماییم که تضعیف (Attenuation) رفته رفته دامنه سیگنال را پایین می‌آورد و اگر این دامنه با سطح نویز زمینه خط (line noise level) قابل مقایسه شود، با خطر عدم تشخیص سیگنال در گیرنده < خطا -Error > روبرو می‌شویم. بنا بر این نسبت توان سیگنال به توان نویز (به dB) از اهمیت ویژه‌ای برخوردار است.

$$SNR = 10\log_{10}\left(\frac{S}{N}\right)$$

SNR: Signal to Noise Ratio (به dB)

S: توان متوسط سیگنال (به W)

N: توان تصادفی نویز (به W)

نکته ۱: همیشه وقتی نسبت دو مقدار بر حسب W به dB تبدیل می‌شود ضریب لگاریتم برابر 10 می‌باشد؛ اما اگر نسبت دامنه‌ها (مثلاً بر حسب ولت (V) یا mV) مطرح باشد، ضریب لگاریتم برابر 20 خواهد بود. $\left(20\log\frac{V_S}{V_N}\right)$ زیرا توان متناسب با مجذور دامنه سیگنال است.

نکته ۲: SNR بالاتر نشان دهنده کیفیت بالاتر است: $SNR \uparrow \Rightarrow Quality \uparrow$

نکته ۳: اگر به جای نسبت دو توان (که واحد ندارد)، بخواهیم یک پارامتر دیگر (برای مثال x) را به دسی بل بیان نماییم، $10\log_{10}^{x}$ را به دست می‌آوریم: دقت کنید که در این صورت، باید واحد x را نیز جلوی dB ذکر نماییم. مثلا اگر x بر حسب W باشد به dBW تبدیل می شود و اگر بر حسب mW (میلی وات) باشد به dBmW (یا به طور خلاصه dBm)تبدیل می شود. همچنین اگر x بر حسب V باشد به dBV تبدیل می شود و اگر بر حسب mV (میلی ولت) باشد به dBmV تبدیل می شود.

قانون (تئوری) شانون ـ هارتلی <Shanon – Hartley>

برای محاسبه حداکثر نرخ انتقال کانال در حضور نویز دیگر نمی‌توان از رابطه نایکوییست استفاده کرد. در این حالت از قانون شانون ـ هارتلی به شرح زیر استفاده می‌کنیم:

$$C = W\log_2\left(1+\frac{S}{N}\right)$$

S: توان متوسط سیگنال (به Watt)

N: توان تصادفی نویز (به Watt)

W: پهنای باند کانال (Hz)

C: حداکثر نرخ انتقال داده کانال نویزی (بیت در ثانیه bps)

نکته ۱: دقت کنید $\frac{S}{N}$ برابر نسبت توان‌هاست و بر حسب dB نیست. بنابراین اگر در مسئله SNR را بدهند؛ باید $\frac{S}{N}$ محاسبه شود.

نکته ۲: $\boxed{C \to 0} \Leftarrow \left(\frac{S}{N} \to 0\right)$

نکته ۳: $\boxed{C \to \infty} \Leftarrow \left(\frac{S}{N} \to \infty\right) \Leftarrow (N \to 0)$

از طرفی $(N = 0) \Leftarrow$ قانون نایکوییست : $\boxed{C = 2W \log_2^M}$

تعبیر: از نظر تئوری نایکوییست نیز می‌توان با افزایش تعداد سطح سیگنال (M) ظرفیت کانال را به میزان دلخواه افزایش داد.

$(M \to \infty) \Rightarrow \boxed{C \to \infty}$

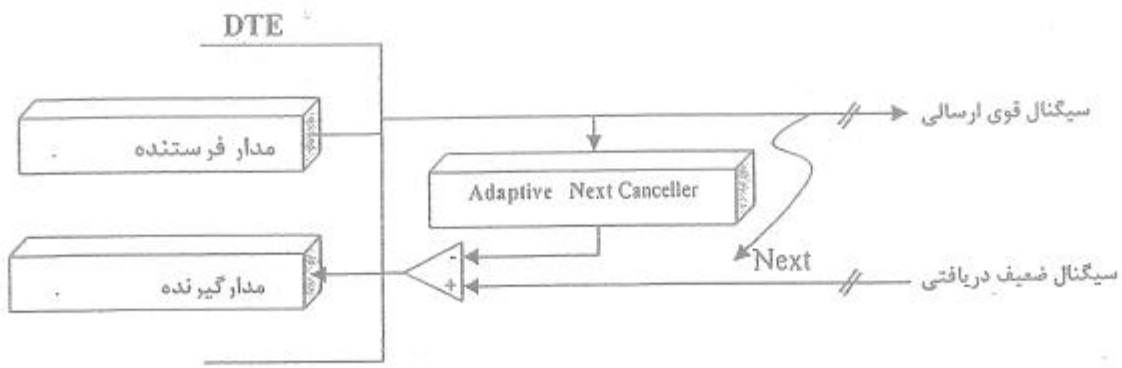
انواع نویز

- ← همشنوایی <Crosstalk> مانند Next (Near – End – Crosstalk)
- ← نویز ضربه‌ای <Impulse noise>
- ← نویز حرارتی <Thermal noise> ← نویز سفید <White noise>

Cross talk

کوپل الکتریکی ناخواسته بین خطوط همسایه (مثل خطوط تلفن PSTN) را همشنوایی گویند. مهم‌ترین نوع Crosstalk نوع Next یا همشنوایی نزدیک انتها (ی خط) <Near – End – Crosstalk> است. پدیده Next به علت تاثیر (کوپل) الکتریکی سیگنال قوی خروجی فرستنده <Transmitter> بر سیگنال ضعیف وارد شده به گیرنده <Receiver> در یک DTE است.

راه حل: استفاده از یک مدار مجتمع به نام Adaptive Next Canceller است که به صورت تطبیقی اثر همشنوایی را به کمک یک تفریق کننده از سیگنال دریافتی حذف می‌کند. به شکل ۱۴ نگاه کنید.



شکل ۱۴. مدار مجتمع Adaptive Next Canceller برای حذف همشنوایی Next

Thermal Noise

این نویز از حرکت تصادفی ذرات باردار (خصوصاً الکترون‌ها) در اثر انرژی جنبشی در دماهای بالاتر از صفر درجه کلوین بوجود می‌آید بنابراین در محیط‌های رسانا مانند خطوط انتقال و سایر دستگاه‌ها بدون حضور تاثیرات خارجی این نویز وجود دارد.

نکته : در این نویز همه فرکانس‌ها به صورت تصادفی با دامنه‌های مختلف تصادفی وجود دارد و به همین دلیل به آن نویز سفید گفته می‌شود.

تعریف: N_0 (چگالی توان نویز حرارتی) مقدار نویز حرارتی در پهنای باند 1Hz می‌باشد.

N_0: چگالی توان نویز (به $\frac{W}{Hz}$)
k: ثابت Boltzman برابر $1.3803\times10^{-23}\ {}^{J}/_{{}^{\circ}K}$
T: درجه حرارت کلوین (به $^{\circ}K$)

$$N_0 = kT$$

توان نویز حرارتی کانال:

N: توان نویز حرارتی (بر حسب W)
W: پهنای باند کانال ((بر حسب Hz))

$$N = N_0 W = kTW$$

پارامتر $\frac{E_b}{N_0}$

یک پارامتر دیگر (شبیه SNR) که نسبت انرژی سیگنال در هر بیت به چگالی توان نویز را نشان می‌دهد، $\frac{E_b}{N_0}$ می‌باشد.

E_b = انرژی یک بیت = توان سیگنال * پریود بیت $= S\tau = \frac{S}{R}$

S: توان سیگنال (بر حسب W)
R: نرخ انتقال داده (بر حسب bps)
k: ثابت Boltzman ($1.3803\times10^{-23}\ {}^{J}/_{{}^{\circ}K}$)
T: درجه حرارت (بر حسب $^{\circ}K$)
N: توان نویز : (بر حسب W)
W: پهنای باند کانال (بر حسب Hz)

$$\frac{E_b}{N_0} = \frac{\frac{S}{R}}{kT}$$

$$N_0 = \frac{N}{W} \rightarrow \frac{E_b}{N_0} = \frac{S}{N}\frac{W}{R}$$

رابطه فوق را بر حسب dB به صورت زیر می‌توان نوشت که کاربرد زیادی در حل مسائل دارد:

$$\frac{E_b}{N_0}(dB) = 10\log_{10}^{\left(\frac{S}{N}\right)} + 10\log_{10}^{W} - 10\log_{10}^{R} \Rightarrow \frac{E_b}{N_0}(dB) = SNR + 10\log_{10}^{\frac{W}{R}}$$

نکته ۱: نرخ خطای بیتی <BER:Bit Error Rate Ratio> که معرف نسبت (احتمال) خطا در هر بیت ارسالی است. با توجه به معیار $\frac{E_b}{N_0}$ تعیین می‌شود. برای مثال $BER = 10^{-4}$ به این معنی است که احتمالاً از هر 10000 بیت یکی خراب است

نکته ۲: BER علاوه بر $\frac{E_b}{N_0}$ به نوع مدولاسیون نیز بستگی دارد.

مثال : برای رسیدن به BER برابر 10^{-6}، $\frac{E_b}{N_0}$ در ASK و FSK باید 13 dB باشد در حالی که در PSK , 10dB کافی است.

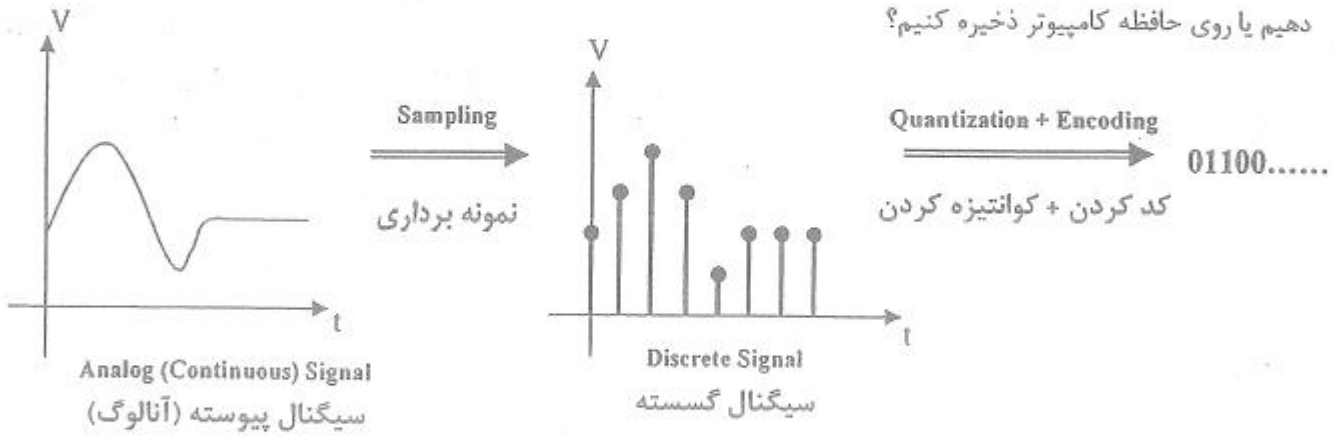
Impulse Noise

این نویز از تاثیر الکتریکی سیگنال‌های ناخواسته خارجی مثل رعد و برق، تجهیزات قوی مثل High Voltage ها و یا منابع تغذیه Switching که به صورت یک ضربه وارد می‌شوند سرچشمه می‌گیرند.

مثال : یک Impulse با عرض 0.5 ثانیه در یک کانال با نرخ ارسال 2400bps موجب خرابی 1200 بیت می‌شود.

۵ـ۲ تئوری نمونه‌برداری (Sampling)

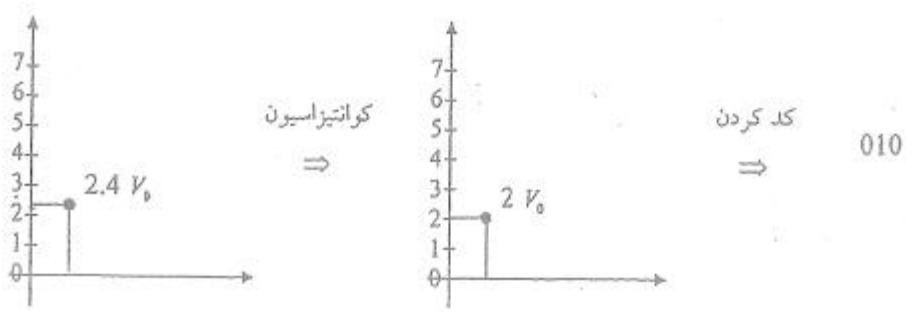
یک سیگنال آنالوگ مفروض است (مثلاً صدای دریافتی از میکروفن)؛ حال مسئله این است که چگونه آن را از یک خط دیجیتال عبور دهیم یا روی حافظه کامپیوتر ذخیره کنیم؟



شکل ۱۵. نمونه‌برداری و کوانتیزه کردن یک سیگنال آنالوگ

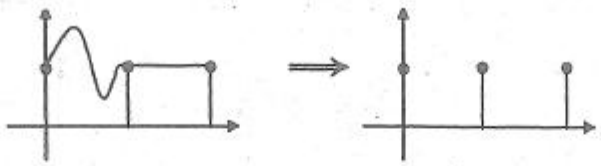
نمونه‌برداری: برداشتن نمونه‌هایی از سیگنال پیوسته در فواصل زمانی مساوی (پریودیک).

کوانتیزه کردن یا چندی کردن (Quantization): فرض کنید هر نمونه باید به ۳ بیت کد شود. بنابراین باید دامنه نمونه که یک عدد حقیقی است از مجموعه محدود (8 تایی) و گسسته‌ای از دامنه‌ها باشد و اگر نیست با تقریب (Round یا گرد کردن) به این مجموعه گسسته نگاشت شود. به شکل ۱۶ نگاه کنید.



شکل ۱۶. خطای گرد کردن دامنه‌ها در کوانتیزه کردن

نکته ۱: اگر فرکانس نمونه‌برداری پایین باشد، سیگنال اصلی از روی نمونه‌ها (در گیرنده) قابل بازسازی نیست.



مثل ولتاژ DC!

شکل ۱۷. فرکانس نمونه‌برداری پایین باعث شده است که نمونه‌ها مانند ولتاژ DC به نظر برسند

نکته ۲: کوانتیزه کردن نیز یک خطای (نویز) جدید به سیگنال اعمال می‌کند.

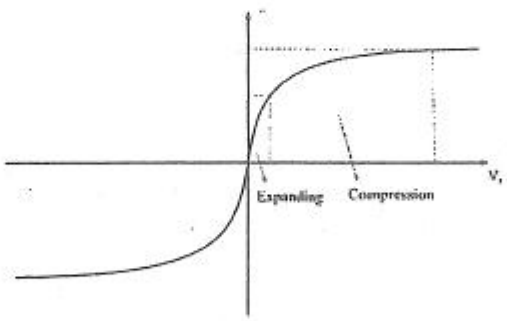
نکته ۳: واضح است که هر چه پهنای باند سیگنال پیوسته بیشتر باشد ($Band\ width = f_{High} - f_{Low}$) و به عبارت دیگر مولفه‌های فرکانس بالاتری داشته باشد (تغییرات سریعی داشته باشد) برای بازسازی باید نرخ نمونه‌برداری را بالا ببریم. البته معمولاً f_{Low} را صفر در نظر می‌گیرند و منظور از پهنای باند همان f_{High} است (بالاترین فرکانس سیگنال). در غیر این صورت f_{High} اهمیت دارد و f_{Low} را در نظر نمی‌گیریم. (در هر حالت پهنای باند را f_{High} در نظر بگیرید.)

نکته ۴: برای کاهش خطای کوانتیزاسیون دو راه حل اصلی وجود دارد:

۱) افزایش تعداد بیت به ازای هر نمونه

۲) Companding (Compress + Expanding) ← فشرده کردن ولتاژهای بالا + باز کردن ولتاژهای پایین

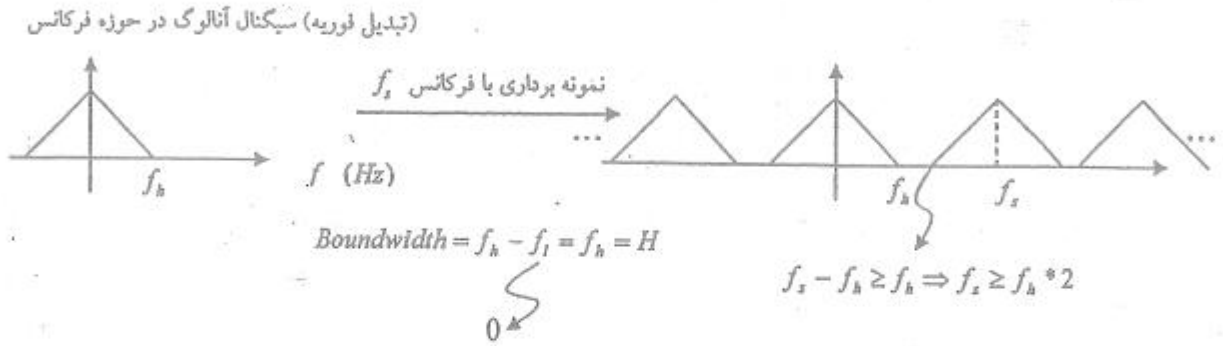
دلیل علمی: آمار نشان می‌دهد در سیگنال‌هایی مثل صدا، احتمال وجود ولتاژهای پایین بیشتر است. در نتیجه با این کار دقت در ولتاژهای پایین، بالا و در ولتاژهای بالا، پایین می‌آید. به شکل ۱۸ نگاه کنید.



شکل ۱۸. عمل Companding برای کاهش خطای کوانتیزه کردن

تئوری نایکوییست (Nyquist)

اگر پهنای باند سیگنال پیوسته برابر H باشد برای انتقال کلیه اطلاعات سیگنال و بازسازی کامل در گیرنده (اگر از خطای کوانیزاسیون نویز و اعوجاج صرف‌نظر کند) فرکانس نمونه‌برداری باید حداقل برابر 2H باشد. این فرکانس به نرخ نایکوییست معروف است. به شکل ۱۹ دقت کنید.



شکل ۱۹. تبدیل فوریه سیگنال آنالوگ اصلی و سیگنال نمونه‌برداری شده

نکته ۱: این نکته بسیار مهم است که با توجه به شکل ۱۸، منظور از پهنای باند H، حداکثر فرکانس سیگنال است و بنابراین اگر f_{Low} را صفر فرض کنیم؛ H همان پهنای باند است و در غیر این صورت به جای H باید حداکثر فرکانس سیگنال (f_{High}) در نظر گرفته شود.

نکته ۲: اگر فرکانس نمونه‌برداری کمتر از $2f_{High}$ باشد $(f_s < 2f_h)$ موجب روی هم افتادن مولفه‌های طیفی و اختلاط فرکانسی <Aliasing> می‌شود.

نکته ۳: اگر بخواهیم سیگنال گسسته نمونه‌برداری شده را به سیگنال اصلی (پیوسته) تبدیل کنیم، کافی است آن‌را از یک فیلتر پایین گذر با پهنای باند H عبور دهیم. در نتیجه اگر Aliasing رخ دهد، فرکانس‌های بالای سیگنال خراب می‌شود.

نکته ۴: اگر نمونه‌برداری با فرکانس بالاتر از f_s امکان‌پذیر نباشد (یا اقتصادی نباشد) و پهنای باند سیگنال آنالوگ (H) بیشتر از $\frac{f_s}{2}$ باشد Aliasing رخ می‌دهد، مگر این‌که قبل از نمونه‌برداری سیگنال آنالوگ را از فیلتر پایین گذر با پهنای باند $\frac{f_s}{2}$ عبور دهیم. به عبارت دیگر حذف فرکانس‌های بالا از اختلاط در فرکانس‌های بالا بهتر است.

نکته ۵: از نظر تئوری نایکوییست نمونه‌برداری با فرکانس‌های بالاتر از 2H هیچ برتری بر فرکانس 2H ندارد و بیهوده است. (مهم: پهنای باند سیگنال آنالوگ H است و یا تا H فیلتر شده است و فرکانس‌های بالاتر از H اصلا وجود ندارد.)

نکته ۶: اما در عمل چون فاصله نمونه‌ها دقیقاً یکسان نیست و کمی لرزش (Jitter) داریم؛ برای حذف این خطا می‌توان فرکانس نمونه‌برداری را افزایش داد (تا حداکثر 10 برابر). مثلاً صدا با پهنای باند 3KHz را به جای 6KHz با 8KHz نمونه‌برداری می‌نمایند.

تست‌های فصل اول و دوم

۱ ـ یک سیگنال باینری، دوسطحی، با نرخ انتقال داده 1000 bps از یک کانال با پهنای باند 3 KHz عبور می‌کند. کدام مولفه‌های سیگنال Worst – Case Sequence در گیرنده مشاهده می‌شود؟

۱) $f_0, 2f_0, 3f_0$ ۲) $f_0, 3f_0, 5f_0$ ۳) $f_0, 2f_0, 3f_0, 4f_0, 5f_0, 6f_0$ ۴) $f_0, 3f_0$

۲ ـ در تست فوق (۱) حداقل پهنای باند موردنیاز برای عبور هارمونیک $3f_0$ چقدر است؟

۱) 1500rad/sec ۲) 3000rad/sec ۳) $1500\pi \text{ rad/sec}$ ۴) $3000\pi \text{ rad/sec}$

۳ ـ یک سیگنال ۸ سطحی با نرخ سیگنالینگ 1000 band از یک کانال عبور می‌کند. حداقل پهنای باند موردنیاز برای آن چقدر است؟

۱) 500Hz ۲) 1000Hz ۳) 4000Hz ۴) 8000 Hz

۴ ـ در یک روش انتقال داده، ۸ سطح سیگنالینگ وجود دارد. اگر از یک کانال PSTN با پهنای باند 3000 Hz استفاده شود، حداکثرنرخ انتقال چقدر است؟ کانال را بدون نویز فرض کنید.

۱) 3 Kbps ۲) 6 Kbps ۳) 18 Kbps ۴) 24 Kbps

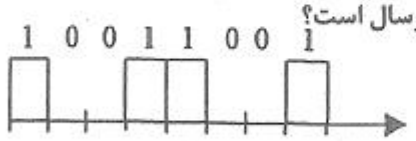
۵ ـ در تست فوق (۴) کارآیی پهنای باند (Bandwidth Efficiency) (یا کارآیی مدولاسیون) چقدر است؟

۱) 6 ۲) $\frac{1}{6}$ ۳) 0.5 ۴) 2

۶ ـ یک خط PSTN با پهنای باند 3KHz دارای نسبت سیگنال به نویز 20 dB است. از نظر تئوری حداکثر چه نرخ انتقال داده‌ای می‌توان از این کانال عبور داد؟ (به طور تقریبی)

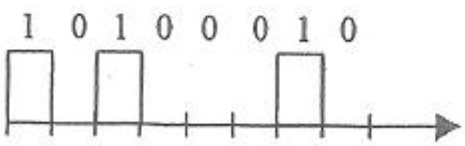
۱) 4.8 Kbps ۲) 9.6 Kbps ۳) 19.2 Kbps ۴) 36.4 Kbps

۷ ـ شکل مقابل نمایش یک سیگنال یک بایتی است که می‌بایستی از یک کانال با پهنای 8000 Hz ارسال گردد. پهنای هر پالس (بیت) 50 میکروثانیه است. حداکثر چند هارمونیک از این سیگنال با این کانال قابل ارسال است؟



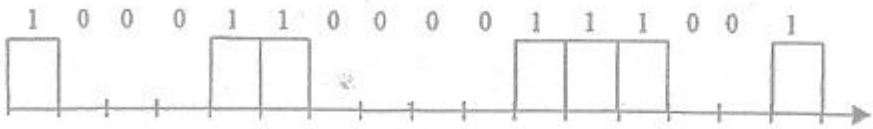
۱) 1 هارمونیک ۲) 2 هارمونیک
۳) 3 هارمونیک ۴) 4 هارمونیک

۸ ـ تست فوق را برای ارسال بایت مقابل حل کنید.



۱) 1 هارمونیک ۲) 2 هارمونیک
۳) 3 هارمونیک ۴) 4 هارمونیک

۹ ـ تست فوق (۷) را برای ارسال دو بایت شکل زیر حل کنید. (آزاد ـ ۸۱)



۱) 6 هارمونیک
۲) 8 هارمونیک
۳) 4 هارمونیک
۴) 2 هارمونیک

۱۰ ـ یک کانال ارتباطی با پهنای باند 1 MHz و نسبت سیگنال به نویز 100 dB حداکثر چه نرخ داده‌ای را می‌تواند ارسال کند؟ (آزاد ـ ۸۱)

۱) کمتر از 2 مگابیت در ثانیه
۲) بیشتر از 40 مگابیت در ثانیه ولی کمتر از 100 مگابیت در ثانیه
۳) بیشتر از 100 مگابیت در ثانیه
۴) بیشتر از 2 مگابیت در ثانیه ولی کمتر از 40 مگابیت در ثانیه

۱۱ ـ یک کانال تلویزیونی دیجیتالی دارای پهنای باند 6 مگاهرتز است. فرض کنید این کانال بدون نویز بوده و سیگنال‌های دیجیتال آن دارای 12 سطح می‌باشند چه نرخ داده‌ای بوسیله این کانال قابل ارسال است؟(آزاد ـ ۸۱)

۱) بیشتر از 12 مگابیت در ثانیه ولی کمتر از 36 مگابیت در ثانیه
۲) 6 مگابیت در ثانیه
۳) بیشتر از 36 مگابیت در ثانیه
۴) 12 مگابیت در ثانیه

۱۲ ـ در صورتی که پهنای باند کانال انتقال داده 4000 Hz و کانال مخابراتی بدون نویز باشد، حداکثر نرخ بیت قابل عبور از کانال چقدر است؟ (سراسری ـ ۸۱)

۱) 2000 بیت در ثانیه
۲) 8000 بیت در ثانیه
۳) 4000 بیت در ثانیه
۴) محدودیتی در نرخ بیت وجود ندارد

۱۳ ـ در سوال فوق (۱۲) حداکثر نرخ بیت قابل عبور از کانال برای یک سیگنال باینری دو سطحی چقدر است؟

۱) 2000 بیت در ثانیه
۲) 8000 بیت در ثانیه
۳) 4000 بیت در ثانیه
۴) محدودیتی در نرخ بیت وجود ندارد

۱۴ ـ یک کانال PSTN با پهنای باند 3000 Hz موجود است. اگر نویز بسیار بالا داشته باشیم $(SNR \cong 0dB)$ ظرفیت کانال چقدر است؟

۱) قابل محاسبه نیست
۲) بستگی به توان سیگنال دارد
۳) صفر (تقریباً صفر بیت در ثانیه)
۴) 3000 بیت در ثانیه

۱۵ ـ اگر یک سیگنال با SNR برابر 12 دسی بل از یک کانال با پهنای باند 3000 Hz عبور کند حداکثر نرخ انتقال داده با فرض $\frac{E_b}{N_0}$ برابر 13 دسی‌بل چقدر است؟

۱) 2382.32 bps
۲) بیش‌تر از 10 Kbps
۳) 4753.35 bps
۴) به نوع مدولاسیون بستگی دارد

۱۶ ـ یک سیگنال از کانال اول با تضعیف 3 dB عبور می‌کند. سپس با یک تقویت کننده با بهره 10 dB تقویت می‌شود. نهایتاً از یک کانال دوم با تضعیف 6 dB عبور می‌کند. نسبت توان خروجی به ورودی چقدر است؟

۱) 0.79 ۲) 1.25 ۳) 10 ۴) 1

۱۷ ـ در یک تقویت کننده که در دمای $500^{\circ}k$ کار می‌کند و پهنای باند 1MHz دارد، توان نویز حرارتی چقدر است؟

۱) -141.6 dBW ۲) -117.2 dBW ۳) -154.8 dBW ۴) -201.9 dBW

۱۸ ـ در تست شماره ۱۵، کارآیی پهنای باند چقدر است؟

۱) 0.79 ۲) 1.58 ۳) 0.75 ۴) 1.25

۱۹ ـ افت یک کانال 10 dB است. اگر سطح نویز خروجی 10 mW و توان سیگنال ورودی 10 W باشد، SNR خروجی چقدر است؟

۱) 10 dB ۲) 20dB ۳) 100 dB ۴) 200 dB

۲۰ ـ طول یک کابل با تضعیف $2^{dB/Km}$، 50 کیلومتر است، اگر دو تکرار کننده با بهره 45 dB در فواصل 20 و 40 کیلومتری قرار دهیم، توان سیگنال خروجی را با ورودی 2W محاسبه کنید.

۱) 2 mW ۲) 200 mW ۳) 20 mW ۴) 100 mW

۲۱ ـ می‌خواهیم تجهیزات یک سیستم قدیمی را با تجهیزات جدید ارتقا دهیم. اگر در این جایگزینی پهنای باند انتقال دو برابر و توان فرستنده نیز دو برابر شود، اما چگالی نویز کانال تغییر نکند، در این صورت ظرفیت انتقال اطلاعات دیجیتال در سیستم جدید نسبت به سیستم قدیمی: (آزاد – ۷۶)

۱) 4 برابر می‌شود ۲) دو برابر می‌شود

۳) $2\sqrt{2}$ برابر می‌شود ۴) بستگی به توان فرستنده دارد

۲۲ ـ تقویت کننده‌ای دارای توان 20 dB است، نسبت ولتاژهای بیانگر این بهره چیست؟

۱) 100 ۲) 1000 ۳) 10 ۴) 1

۲۳ ـ اگر در یک کوانتیزاسیون از 10 بیت استفاده شود، نسبت دامنه نویز کوانتیزه به حداکثر دامنه سیگنال چقدر است؟

۱) $\pm\frac{V_{max}}{128}$ ۲) $\pm\frac{V_{max}}{256}$ ۳) $\pm\frac{V_{max}}{2048}$ ۴) $\pm\frac{V_{max}}{1024}$

۲۴ ـ در تست فوق (۲۳) اگر محدوده دینامیک سیگنال 20 dB باشد، نسبت دامنه نویز کوانتیزه به حداقل دامنه سیگنال چقدر است؟

۱) $\pm\frac{V_{min}}{204.8}$ ۲) $\pm\frac{V_{min}}{2048}$ ۳) $\pm\frac{V_{min}}{10240}$ ۴) $\pm\frac{V_{min}}{102400}$

۲۵ ـ در صورتیکه پهنای باند یک سیگنال X(t) مقدار محدود B باشد، کدم اظهار نظر در مورد نرخ نمونه‌برداری، نادرست است؟ (سراسری-۸۱)

۱) هرچه از 2B بیشتر باشد سیگنال باز سازی شده دقیقتر است.

۲) در صورتیکه کمتر از 2 B باشد سیگنال X(t) از روی نمونه‌های آن قابل بازسازی نیست.

۳) در صورتیکه 2B یا بیشتر باشد و نمونه‌ها چندی (Quantise) شوند سیگنال X(t) فقط به طور تقریبی قابل بازیابی می‌باشد.

۴) در صورتیکه 2B یا بیشتر باشد و نمونه‌ها چندی (Quantise) شوند و نیز هرچه تعداد بیت‌های چندی کننده بیشتر باشد سیگنال X(t) با دقت بیشتری بازسازی می‌شود.

حل تشریحی تست‌های فصل اول و دوم

۱ـ گزینه ۲ صحیح می‌باشد.

حل :

$$f_0 = \frac{R}{2} = \frac{1000}{2} = 500\,Hz$$

چون فقط مولفه‌های فرد در Worst case sequence وجود دارد؛ پس گزینه ۲ صحیح می‌باشد.

۲ـ گزینه ۴ صحیح می‌باشد.

حل :

$$3f_0 = 3\times 500\ Hz = 1500Hz$$

$$3\omega_0 = 2\pi(3f_0) = 2\pi\times 1500 = 3000\pi\frac{rad}{sec}$$

۳ـ گزینه ۱ صحیح می‌باشد.

حل :

$$C = 2W\log_2^M = 2W\log_2^8 \Rightarrow W = \frac{C}{2\times 3} = \frac{3000bps}{2\times 3} = 500Hz$$

راه حل دوم :

$$W = \frac{C}{2\log_2^M} = \frac{R}{2\log_2^M} = \frac{R_s\log_2^M}{2\log_2^M} = \frac{R_s}{2} = \frac{1000}{2} = 500\,Hz$$

۴ـ گزینه ۳ صحیح می‌باشد.

حل :

$$C = 2W\log_2^M = 2\times 3000Hz\times\log_2^8 = 18Kbps$$

۵ـ گزینه ۱ صحیح می‌باشد.

حل :

$$B = \frac{R}{W} = \frac{18Kbps}{3KHz} = 6$$

۶ـ گزینه ۳ صحیح می‌باشد.

حل :

$$20 = 10\log\frac{S}{N}_{10}$$

$$\frac{S}{N} = 100$$

$$C = W\log_2^{\left(1+\frac{S}{N}\right)} = W\log_2^{1+100} \cong 19.2Kbps$$

۷ـ گزینه ۱ صحیح می‌باشد.

حل :

$$T_0 = 4\times 50\mu s = 200\mu s \rightarrow f_0 = \frac{1}{200\times 10^{-6}} = 5000Hz = 5KHz$$

فقط هارمونیک اول (f_0) عبور می‌کند.

۸ـ گزینه ۳ صحیح می‌باشد.

$$T_0 = 8\tau = 8\times 50\mu s = 400\mu s$$

$$f_0 = \frac{1}{T_0} = 2.5KHz$$

۳ هارمونیک $(3f_0, 2f_0, f_0)$

۹ـ گزینه ۱ صحیح می‌باشد.

$$T_0 = 16\times 50 = 800\mu s$$

$$f_0 = \frac{1}{T_0} = 1250Hz = 1.25KHz$$

$$6\times 1.25 = 7.5KHz$$

هارمونیک‌های $f_0, 2f_0, 3f_0, ..., 6f_0$ عبور می‌کنند.

۱۰ـ گزینه ۴ صحیح می‌باشد.

حل : با توجه به تئوری شانون هارتلی:

$$C = W\log_2^{\left(1+\frac{S}{N}\right)}$$

$$100dB = 10\log\frac{S}{N}_{10}$$

$$C = 10^6 \log_2^{(1+10^{30})} = 1M \times 33.2 = 33.2M$$

که به معنی صحت گزینهٔ ۴ می‌باشد.

اما اگر در سوال، سیگنال را دو سطحی فرض می نمود یا مثلا نوع آن را NRZ-L مشخص می کرد، با توجه به تئوری نایکوییست:

$$C = 2W \log_2^M = 2 \times 1M \times \log_2^M$$

لذا با فرض $M = 2$ ، $C = 2M$ خواهد بود. اما چون اندکی نویز داریم $C<2M$ می شود که در آن صورت گزینهٔ اول درست بود.

۱۱ـ گزینه ۳ صحیح می‌باشد.

حل :

$$C = 2W \log_2^M = 2 \times 6MHz \times \log_2^{12} = 2 \times 6 \times 3.85 = 42.96Mbps$$

۱۲ـ گزینه ۴ صحیح می‌باشد.

حل :

از نظر تئوری بستگی به M دارد.

$$C = 2W \log_2^M$$

$$M \to \infty \Rightarrow C \to \infty$$

۱۳ـ گزینه ۲ صحیح می‌باشد.

حل :

$$C = 2W \log_2^M = 2W \log_2^2 = 2W = 2 \times 4000 = 8000bps$$

۱۴ـ گزینه ۴ صحیح می‌باشد.

حل :

$$10 \log_{10}^{\frac{S}{N}} \to 0$$

$$\frac{S}{N} \to 1$$

$$C = W \log_2^{\left(1+\frac{S}{N}\right)} = 3000 \log_2^2 = 3000$$

۱۵ـ گزینه ۱ صحیح می‌باشد.

حل :

$$\frac{E_b}{N_0}(dB) = SNR(dB) + 10\log_{10}^{W} - 10\log_{10}^{R}$$

$$13 - 12 = 1 = 10\log_{10}^{3000} - \log_{10}^{R} \Rightarrow R = 2382.32bps$$

۱۶- گزینه ۲ صحیح می‌باشد.

حل :

$$\text{تضعیف} = 10\log_{10}\frac{P_T}{P_R} = 3 + 6 - 10 = -1$$

$$10\log_{10}\frac{P_R}{P_T} = 1 \Rightarrow \frac{P_R}{P_T} = 10^{0.1} = 1.25$$

۱۷- گزینه ۱ صحیح می‌باشد.

حل :

$$N = N_0 W = kTW = 1.3803 \times 10^{-23} \times 500 \times 10^{6}$$

$$10\log_{10}^{N} = 10\log_{10}^{6.9015 \times 10^{-15}} \cong -141.6\,dBW$$

۱۸- گزینه ۱ صحیح می‌باشد.

حل :

$$B = \frac{R}{W} = \frac{2382.32}{3000} \cong 0.79$$

۱۹- گزینه ۲ صحیح می‌باشد.

حل :

$$10 = 10\log_{10}^{\frac{P_T}{P_R}} = 10\log_{10}^{\frac{P_1}{P_2}} \rightarrow P_T = 10P_R$$

$$\Rightarrow P_R = \frac{1}{10}P_T = \frac{10}{10} = 1W$$

$$SNR = 10\log_{10}^{\frac{1000mw}{10mW}} = 20\,dB$$

۲۰- گزینه ۲ صحیح می‌باشد.

حل :

$$\text{تضعیف کابل} = 2\times 50 = 100\,\text{dB}$$

$$\text{تقویت تکرار کننده‌ها} = 2\times 45 = 90\,\text{dB}$$

$$\text{تضعیف کل} = 100-90 = 10\,\text{dB} = 10\log_{10}^{\frac{P_1}{P_2}} = 10\log_{10}^{\frac{2}{P_2}}$$

$$\frac{2}{P_2} = 10 \Rightarrow P_2 = 0.2\text{W} = 200\text{mW}$$

۲۱- گزینه ۲ صحیح می‌باشد.

حل :

$$\frac{C_2}{C_1} = \frac{W_2\log_2^{\left(1+\frac{S_2}{N_2}\right)}}{W_1\log_2^{\left(1+\frac{S_1}{N_1}\right)}} = \frac{2W_1\log_2^{\left(1+\frac{2S_1}{2N_0W_1}\right)}}{W_1\log_2^{\left(1+\frac{S_1}{N_0W_1}\right)}} = 2$$

۲۲- گزینه ۳ صحیح می‌باشد.

حل :

$$20\,\text{dB} = 20\log_{10}^{\frac{V_2}{V_1}} \Rightarrow \frac{V_2}{V_1} = 10$$

۲۳- گزینه ۳ صحیح می‌باشد.

حل :

$$2^{10} = 1024$$

$$\pm 0.5\times\frac{V_{max}}{1024} = \pm\frac{V_{max}}{2048}$$

۲۴- گزینه ۱ صحیح می‌باشد.

حل :

$$20 = 20\log_{10}^{\frac{V_{max}}{V_{min}}} \Rightarrow V_{max} = 10\,V_{min}$$

$$\text{دامنه نویز کوانتیزه} = \pm\frac{V_{max}}{2048} = \pm\boxed{\frac{V_{min}}{204.8}}$$

۲۵- گزینه ۱ صحیح می‌باشد.

فصل سوم

استانداردهای واسط (Interfacing Standards)

هنگامی که دو DTE نزدیک به هم بوده و با Rate پایین تبادل داده می‌نمایند می‌توان از دو سیم و واسط‌های ساده استفاده کرد؛ اما مثلاً فرض کنید که فاصله دو DTE بسیار زیاد و نرخ انتقال موردنیاز بالا باشد و بخواهیم از PSTN استفاده کنیم. در این صورت به تکنیک‌های مدولاسیون و ابزارهایی نظیر Modem (Modulation / Demodulation) و انواع مختلف سیگنال‌هایی که مناسب نرخ انتقال بالا و فواصل دور هستند نیاز داریم.

منظور از واسط (Interface)، مدارها و تجهیزات بین DTE و خط انتقال داده است که باید استاندارد شوند تا مثلاً مودم‌های کارخانجات مختلف بتوانند با هم کار کنند.

استانداردهای واسط برای استانداردسازی در لایه فیزیکی به کار می‌روند و دارای ابعاد ذیل می‌باشند:

- استانداردسازی ویژگی‌های مکانیکی (Mechanical): اتصالات فیزیکی، سیم‌ها، Connectorها، Plugها، Jack ها و غیره.
- استانداردسازی ویژگی‌های الکتریکی (Electrical): سطوح ولتاژ (یا جریان)، زمان‌بندی تغییرات ولتاژ، شکل سیگنال، نرخ انتقال و غیره.
- استانداردسازی ویژگی‌های عملیاتی (Functional): مشخص کردن وظیفه و عملکرد هر بخش از سیستم واسط.
- استانداردسازی ویژگی‌های رویه‌ای (Procedural): توالی زمانی گام به گام عملیات لازم برای انتقال داده.

۱ـ۳ حالت‌های ارسال داده‌های دیجیتال

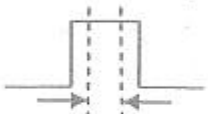
برای انتقال داده‌های دودویی به طور کلی دو حالت وجود دارد: حالت موازی و حالت سری.

در این‌جا یک طبقه‌بندی کامل از حالت‌های ارسال را مورد بررسی قرار می‌دهیم و در آن دو روش ارسال سری داده‌های دیجیتال را به طور دقیق شرح خواهیم داد.

ارسال داده
- موازی
- سری
  - Synchronous همزمان (همگام)
  - Asynchronous غیر همزمان (ناهمگام)

مفهوم همگام‌سازی فرستنده و گیرنده

فرض کنید که در هر عنصر سیگنال یک بیت ارسال می‌شود. در گیرنده در یک لحظه مناسب (معمولاً وسط پالس) برای آشکارسازی (تعیین صفر 0 یا یک (1) بودن) عنصر (بیت) ارسالی ، عمل نمونه برداری انجام می‌شود. حال اگر Clock فرستنده و گیرنده اختلاف داشته باشند، به تدریج زمان (لحظه) نمونه‌برداری از وسط پالس به سمت راست (یا چپ) جابجا می‌شود و اگر از پالس خارج شود خطای تشخیص رخ می‌دهد. برای درک بهتر این موضوع به شکل زیر نگاه کنید و تست شماره ۲۶ را حل نمائید.



زمان نمونه برداری

۱ـ۱ـ۳ انتقال Asynchronous (غیر همزمان ـ ناهمگام)

انتقال ناهمگام، مناسب سرعت‌های (نرخ بیت‌های) پایین است و در آن هیچ گونه ارتباط و هماهنگی بین پالس‌های ساعت فرستنده و گیرنده وجود ندارد. در این روش، داده‌های دیجیتال به صورت کاراکترهای مجزا در هر زمان که لازم باشد بدون نظم خاصی ارسال می‌گردند. در این روش برای تشخیص کاراکترها در گیرنده، 2 تا 3 بیت کنترلی به شرح زیر به هر کاراکتر اضافه می‌گردد:

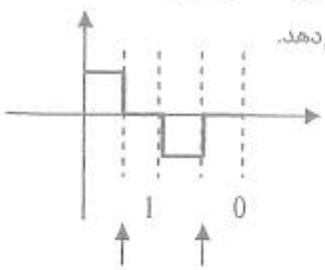
- یک بیت آغاز (Start Bit) به منظور تعیین مرز شروع کاراکتر ارسالی
- یک تا دو بیت پایان (توقف) (Stop bit) برای تعیین مرز پایان کاراکتر و جدا کردن آن از کاراکتر (احتمالی) بعدی (زیرا سطح ولتاژ بیت پایان مخالف سطح ولتاژ بیت آغاز است)

فرکانس ساعت فرستنده و گیرنده باید با هم برابر باشد، اما چون از یکدیگر جدا هستند، ممکن است کاملاً بر هم منطبق نباشند و لذا در ابتدای بیت آغاز عمل تطبیق صورت می‌گیرد.

این بیت‌های کنترلی، افزونگی ایجاد می‌کند و سربار (Overhead) حاصله، نقطه ضعف روش آسنکرون است. این روش دارای کاربردهای زیادی مانند اتصال پورت سریال DTE (مثلاً PC) به DCE (مثلا مودم) می‌باشد. دقت نمائید که بین ارسال کاراکترها، کانال می‌تواند در وضعیت بیکار (Idle) باشد.

نکته ۱: هیچ Clock از فرستنده به گیرنده ارسال نمی‌شود و Clock مشترکی وجود ندارد.

نکته ۲: سیگنال Clock در درون اطلاعات سیگنال نیز وجود ندارد. در این‌جا از کدهایی مانند تیپ NRZ استفاده می‌شود که اطلاعات مربوط به ساعت در خود سیگنال گنجانیده نمی‌شود. در مقابل در بعضی از روش‌های سنکرون از کدهای تیپ RZ استفاده می‌شود که اطلاعات مربوط به ساعت در خود سیگنال گنجانیده می‌شود. شکل ۲۰ این نکته را نشان می‌دهد.

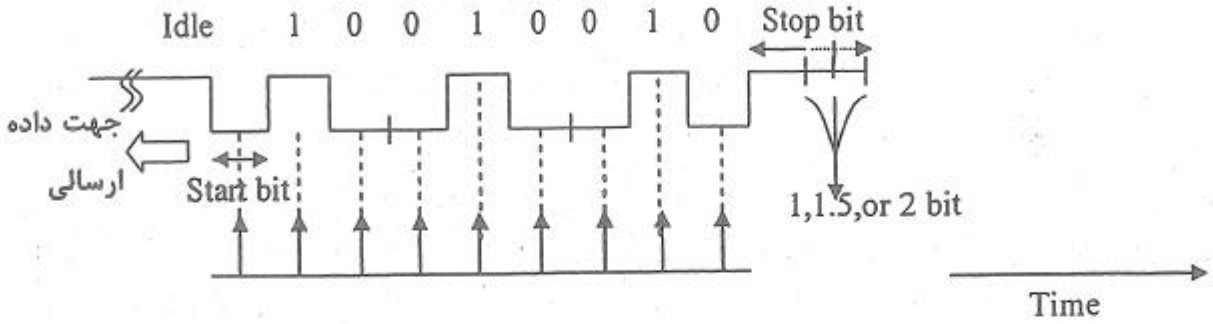


ارسال Clock به همراه Signal → Synchronous ...

شکل ۲۰. در کدگذاری RZ تغییر سطح سیگنال در وسط بیت نقش پالس‌های ساعت را دارد که با پیکان عمودی نشان داده شده است

نکته ۳: عمل همگام‌سازی، تنها در بیت‌های آغاز و پایان انجام می‌شود.

نکته ۴: بیت پایان تضمین می‌کند که اگر دو کاراکتر پشت سر هم ارسال شوند، ابتدای کاراکتر بعدی که منطق عکس (تغییر حالت سیگنال) دارد قابل تشخیص باشد (شکل ۲۱).



شکل ۲۱.پالس نمونه برداری در گیرنده خود را با بیت آغاز همگام می کند.

۲ـ۱ـ۳ انتقال Synchronous (همزمان، همگام)

در این روش که مناسب سرعت‌های بالاتر است ، استانداردها و روش‌های مختلفی وجود دارد. وجه اشتراک آن‌ها در این است که در همگی این روش‌ها فرستنده و گیرنده به طریقی با یکدیگر سنکرون می‌شوند. در زیر به سه روش انتقال سنکرون اشاره خواهیم کرد:

- می‌توان Clock فرستنده را از طریق یک کانال جداگانه به گیرنده ارسال کرد. (این روش بسیار پرهزینه است چون کانال جداگانه می‌خواهد.)
- می‌توان از کدهای تیپ RZ استفاده کرد و اطلاعات ساعت را همراه با خود سیگنال ارسال کرد (وجود تغییر حالت در هر بیت)
- یکی از متداول‌ترین روش‌ها این است که کل بیت‌های ارسالی را در یک Frame قرار دهیم و Frame ها را ارسال نمائیم. هر Frame با یک کاراکتر خاص شروع متن (STX) Start of Text شروع می‌شود. گیرنده در ابتدا به دنبال شکار (Hunt Mode)، این کاراکتر شروع است. همچنین یک فریم با یک کاراکتر خاص پایان متن (ETX) End of Text خاتمه می‌یابد. علاوه بر ا ین، معمولاً در Frameهای طولانی یک یا چند کاراکتر همزمانی در وسط کار نیز ارسال می‌شود تا گیرنده و فرستنده را همگام سازد. استانداردهای مختلفی از این روش استفاده می‌کنند؛ مانند استانداردهای HDLC ، SDLC، Bisync و غیره. (مثلا HDLC از بایت 01111110 به عنوان STX و ETX استفاده می نماید و برای پرهیز از این الگو در درون داده های اصلی فریم از تکنیک Bit Stuffing استفاده می‌نماید و بعد از هر رشته پنج تایی 1، یک صفر اضافی درج می شود)

نکته : در انتقال سنکرون، بیت‌های کنترلی اضافی ارسال نمی‌شود؛ در نتیجه مشکل کاهش حدود 25 درصدی در سرعت و کارایی که در روش آسنکرون به علت سربار بیت‌های کنترلی با آن روبرو بودیم، در این روش برطرف می‌شود. به عبارت دیگر به جای چند بیت در ازا هر بایت، فقط چند بایت برای یک فریم بزرگ ارسال می‌شود.

مثال ۱: یک پیغام شامل 500 کاراکتر 8 بیتی است. تعداد بیت اضافی ارسالی در انتقال آسنکرون (غیر همزمان) با یک بیت شروع، دو بیت پایان، بدون بیت توازن (Parity) چند است؟ (دو بایت اضافی نیز ارسال می‌شود تا شروع و پایان پیغام را نشان دهد)

راه‌حل:

$$[500*(1+2)]+[2*(8+2+1)]=1522bit$$

مثال ۲: در مثال فوق فرض کنید از روش همزمان با یک کاراکتر شروع frame، یک کاراکتر پایان frame و دو کاراکتر همزمانی در وسط frame استفاده می‌شود. پاسخ چند است؟

راه‌حل:

$$4*8=32bit$$

۲ـ۳ مهم‌ترین استانداردهای لایه فیزیکی

در ذیل چندین استاندارد مهم در ارتباط با ویژگی‌های الکتریکی، مدارهای واسط و اتصالات مکانیکی سیستم‌های انتقال داده مورد بحث قرار می‌گیرد.

۱ـ۲ـ۳ استاندارد EIA-232

نام اولیه : RS-232

آخرین نسخه تجدیدنظر شده: RS-232D (نسخهٔ D بعد از A و B و C)

هدف : تعریف ویژگی‌های مکانیکی، الکتریکی و عملیات واسط و استانداردسازی آن برای فواصل کوتاه و نرخ بیت پایین

کاربرد: اتصال DTE به DCE (چون مودم به کامپیوتر نزدیک است و خطوط PSTN سرعت پایینی دارند، با این استاندارد می‌توانند به کامپیوتر متصل شود) و نیز اتصال تجهیزات مختلف مانند ترمینال‌ها و دستگاه‌های جانبی به کامپیوترها

نکته ۱: ارتباط سری در IBM PC از این استاندارد استفاده می‌کند و واسط‌های USART و UART به همین دلیل توسط Intel ساخته شده است (UART ← آسنکرون، USART ← سنکرون و آسنکرون)

نکته ۲: در UART ارتباط Asynchronous قابل پیکره‌بندی است و بیت شروع، بیت پایان، بیت توازن و نرخ انتقال قابل تعریف است.

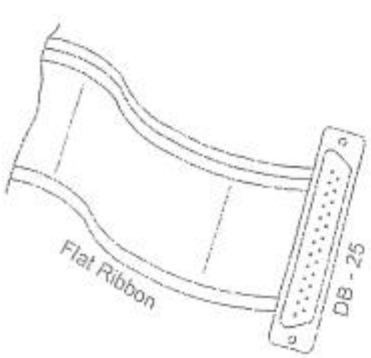
نکته ۳: استاندارد معادل EIA-232 که توسط ITU-T تعریف شده است V.24 نام دارد.

ویژگی‌های مکانیکی استاندارد لایه فیزیکی EIA-232/V.24:

- کابل 25 سیم معمولاً به صورت Flat Ribbon
- کانکتور DB-25 ، 25 پایه، 13 پایه ردیف بالا، 12 پایه ردیف پایین (مانند شکل ۲۲)
- حداکثر مسافت : 15 متر

ویژگی‌های الکتریکی:

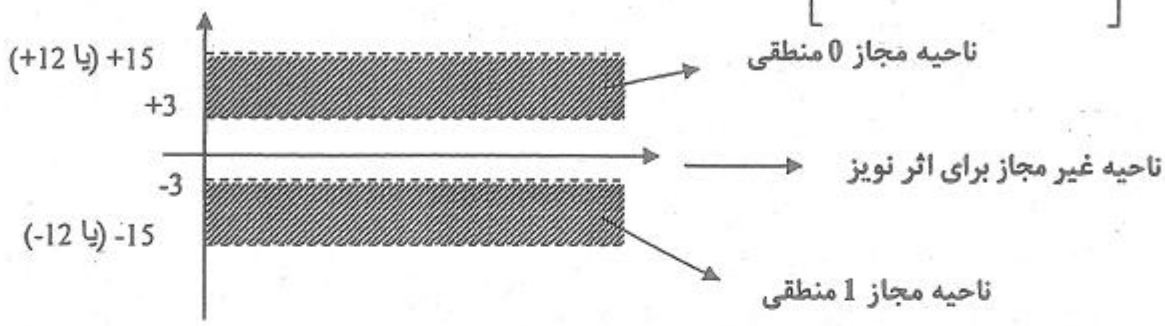
- هر عنصر معرف 0 یا 1 منطقی است.



شکل ۲۲. یک کانکتور DB-25 متصل به Flat Ribbon

- Coding مورد استفاده NRZ-L است.
- حداکثر نرخ انتقال : 20kbps
- استاندارد سطح سیگنال الکتریکی در ITU-T Recommendation دیگری به نام V.28 تعریف شده است (مطابق شکل ۲۳)

$$\left[3^V \le V \le 12 \quad or \quad 15^V\right]$$



شکل ۲۳. سطوح ولتاژ استاندارد V.28

شکل۲۴ جزئیات بیشتری از این استاندارد را نشان می‌دهد.

شکل (a)۲۴، جایگاه این استاندارد را در ارتباط دو DTE از طریق PSTN (به وسیله مودم) نشان می‌دهد.

شکل (b) ۲۴ یک کانکتور DB25 را نشان می‌دهد.

شکل (c) ۲۴، پین‌های کانکتور DB25 و تعریف هر یک ا ز سیگنال‌های آن را نشان می‌دهد.

خطوط TD(TxD) و RD(RxD) به ترتیب برای ارسال و دریافت داده در DTE استفاده می‌شود و بقیه خطوط برای تبادل سیگنال‌های زمان‌بندی و کنترل به کار می‌روند.

برخی از خطوط برای Setup و Clear کردن اتصال بین دو طرف به کار می‌روند. مثلاً RTS که از طرف DTE به DCE فرستاده می‌شود به معنای درخواست برای ارسال است.

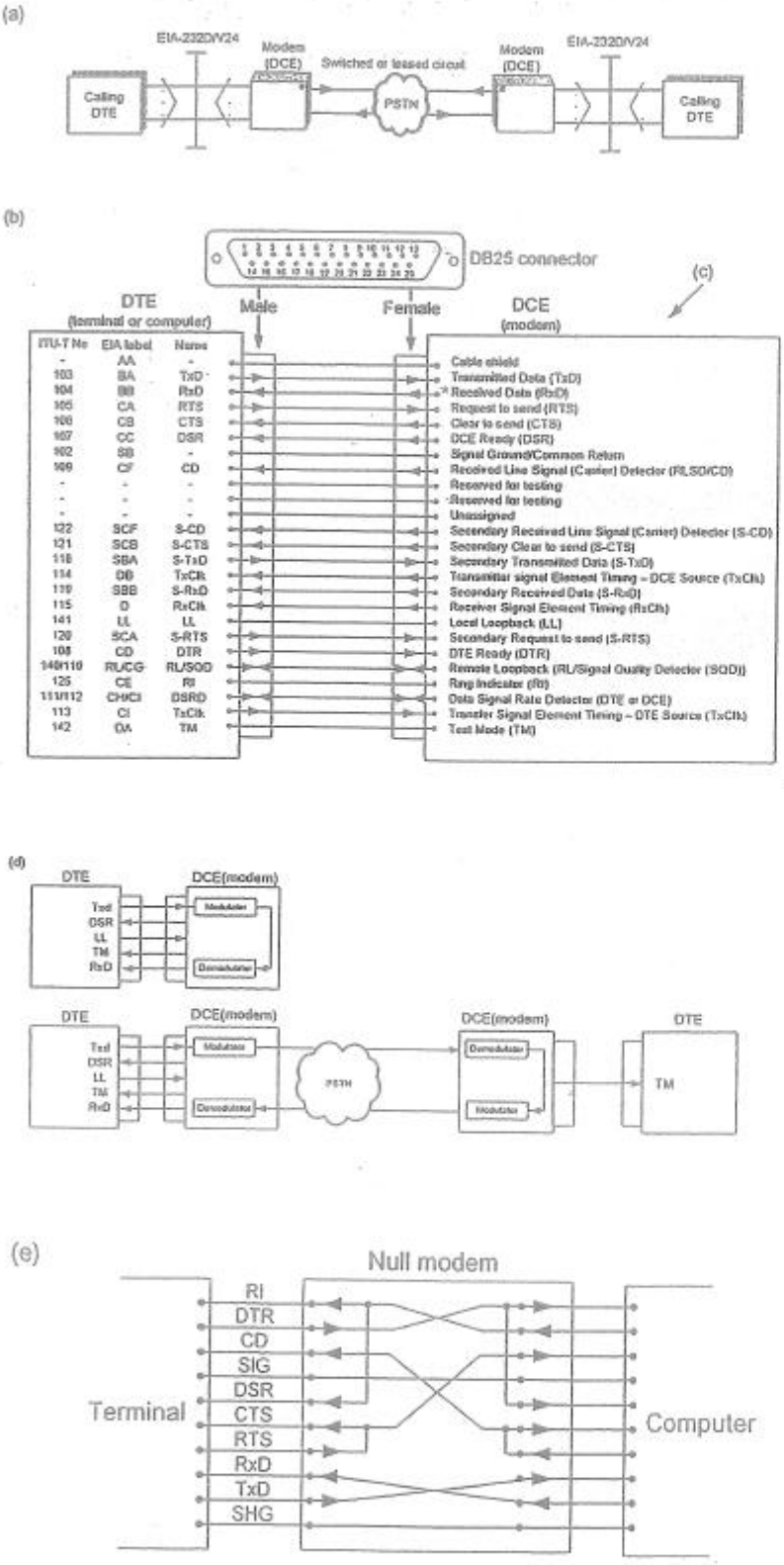
نکته ۱: ارتباط سنکرون / آسنکرون:

در ارتباط آسنکرون، پالس‌های ساعت که برای کنترل زمان‌بندی سیگنال ارسالی (پالس ساعت TxClk) و سیگنال دریافتی (پالس ساعت RxClk) به کار می‌روند، توسط مولدهای Clock جداگانه و مستقل تولید و به طور مستقیم به پین‌های مربوطه در DTE متصل می‌شوند. ولی در ارتباط سنکرون سیگنال‌های Clock توسط مودم‌ها تولید می‌شوند و ارسال و دریافت اطلاعات توسط DTE ها با پالس‌های ساعت تولید شده توسط مودم‌ها سنکرون می‌شود.

نکته ۲: شکل (c)، ۲۴ نحوه اتصال پین‌ها برای حالت Handshake کامل DTE و DCE را نشان می‌دهد.

نکته ۳: مودم پوچ (Null Modem):

اگر دو دستگاه نزدیک مثل دو DTE بخواهند از استاندارد RS-232D استفاده نمایند چون نیاز به خط تلفن، مدولاسیون و مودم وجود ندارد، از یک اتصال خاص ضربدری (Cross-Connection) که به مودم پوچ معروف است استفاده می‌شود. شکل (e)۲۴ ، یک مودم پوچ را نشان می‌دهد.



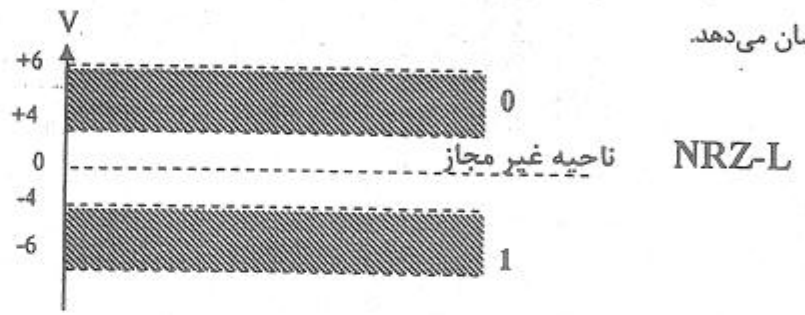
شکل ۲۴. استاندارد RS-232 و کاربردهای آن

۲ـ۲ـ۳ سیگنال 20 mA Current Loop (حلقه جریان 20 میلی آمپر)

به جای استاندارد EIA-232D/V.28 می‌توان از یک حلقه جریان 20 میلی‌آمپری (که البته هم برای ارسال و هم برای دریافت داده، هر کدام به دو خط نیاز دارد تا حلقه جریان بین فرستنده و گیرنده برقرار شود) استفاده کرد. این روش تاثیری بر Bit Rate ندارد و فقط برای جداسازی فیزیکی پتانسیل‌های فرستنده و گیرنده به کار می‌رود.

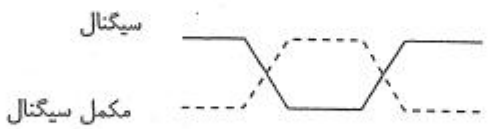
۳ـ۲ـ۳ استاندارد RS-422A/V.11

برای فواصل دورتر و برای نرخ انتقال داده بالاتر به‌جای RS-232 از RS-422 استفاده می‌شود. در این روش از یک زوج سیم به هم تابیده (twisted pair) به جای هر خط ارسال یا دریافت استفاده می‌شود. (2 برابر سیم مصرف می‌کند).شکل ۲۵ سطح ولتاژهای این استاندارد را نشان می‌دهد.



شکل ۲۵. سطوح ولتاژ استاندارد V.11

استفاده از دو سیم به این دلیل است که سیگنال (S) را از یک سیم و مکمل سیگنال (S-) را از سیم دیگر ارسال می‌کنند. (شکل ۲۶)



شکل ۲۶. یک سیگنال و مکمل آن

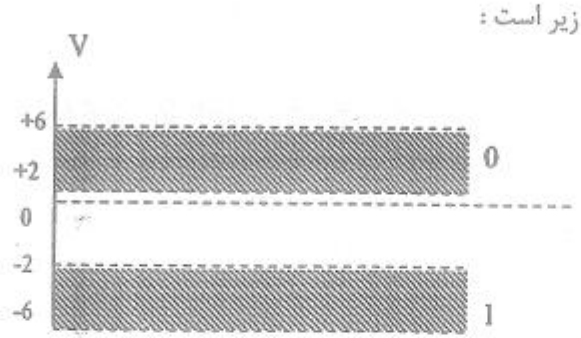
در گیرنده دو سیگنال فوق از یکدیگر تفریق می‌شود (روش Differential یا تفاضلی است). این روش به نام متوازن (Balanced) یا Double- Ended نیز معروف است. بنابراین مشخصات اصلی روش تفاضلی یا متوازن به شرح زیر است:

- سطح سیگنال تفاضلی دو برابر سطح سیگنال اصلی است.
- با تفاضل دو سیگنال نویز موثر بر دو سیم به هم تابیده از هم کسر و نویز کل برابر (تقریباً) صفر می‌شود.
- فاصله تا 10 متر ← نرخ انتقال 10Mbps
- فاصله تا 1000 متر ← نرخ انتقال 100kbps
- برای جلوگیری از انعکاس سیگنال (Echo) لازم است یک مقاومت برابر امپدانس خط در انتهای هر خط قرار داده شود.

۳ـ۲ـ۴ استاندارد RS-423 / V.10

از استاندارد RS-422 مشتق شده است. تفاوت اصلی آنها در این است که در این استاندارد می‌توان ولتاژهای Single-Ended (Unbalanced یا نامتوازن) خروجی RS-232 را در گیرنده تفاضلی دریافت کرد. شکل ۲۷ سطح ولتاژهای این استاندارد را نشان می‌دهد. سایر ویژگی‌های این استاندارد به شرح زیر است :

- نرخ انتقال : 100kbps
- فاصله: 1000 متر



شکل ۲۷. سطوح ولتاژ استاندارد V.10

۳ـ۲ـ۵ استاندارد EIA-449

هدف این استاندارد، رفع محدودیت‌های EIA-232 می‌باشد. در این استاندارد دو نوع کانکتور DB-9 (9 پینی) و DB-37 (37 پینی) تعریف شده است که ترکیب آن‌ها 46 پینی خواهد بود.

۳ـ۲ـ۶ استاندارد EIA- 530

این استاندارد دارای ویژگی‌های زیر است:

- همان مجموعه سیگنال‌های EIA-232D را تعریف کرده است.
- از سیگنال‌های الکتریکی تفاضلی (Balanced) استاندارد RS-422A/V.11 استفاده می‌کند.
- بنابراین یک کانکتور DB-37 می‌خواهد (2 سیم تابیده برای هر سیگنال دارد و تعداد پین‌ها بیشتر می‌شود) و به‌علاوه یک کانکتور DB-9 (9 پین) اضافی نیز لازم دارد. (البته به شرط این‌که مجموعه سیگنال‌های فرعی (Secondry or test lines) را نیز به کار ببریم).

۳ـ۲ـ۷ استاندارد V.35

هدف این استاندارد اتصال DTE به مودم‌های سنکرون آنالوگ باند پهن (48 – 168 Kbps) می‌باشد و ویژگی‌های آن به شرح زیر است:

- واسط مکانیکی: مانند EIA-232D به استثناء مجموعه سیگنال‌های فرعی (تست)
- ویژگی‌های الکتریکی : ترکیب RS-232 و RS-422 به شرح ذیل:
- Unbalanced RS-232/V.28: برای سیگنال‌های کنترلی
- Balanced RS-422/V.11 : برای سیگنال‌های داده و زمان‌بندی و Clock مربوطه

۸ـ۲ـ۳ استاندارد X.21

در این استاندارد سیگنال‌های کنترل و داده به صورت جریانی از بیت‌ها بر روی یک خط ارسال می‌شوند (نوع سنکرون یا همزمان). لذا DTE و DCE هر دو مدارات منطقی لازم برای ایجاد، دریافت و جدا کردن این سیگنال‌ها از یکدیگر را دارند. ویژگی‌های این استاندارد به شرح زیر است:

کاربرد:

- اتصال کامپیوتر دیجیتال (DTE) به مودم آنالوگ (DCE) سنکرون
- اتصال کامپیوتر دیجیتال به واسطهای دیجیتال (PSDN) مانند X.25

نرخ انتقال: 64kbps

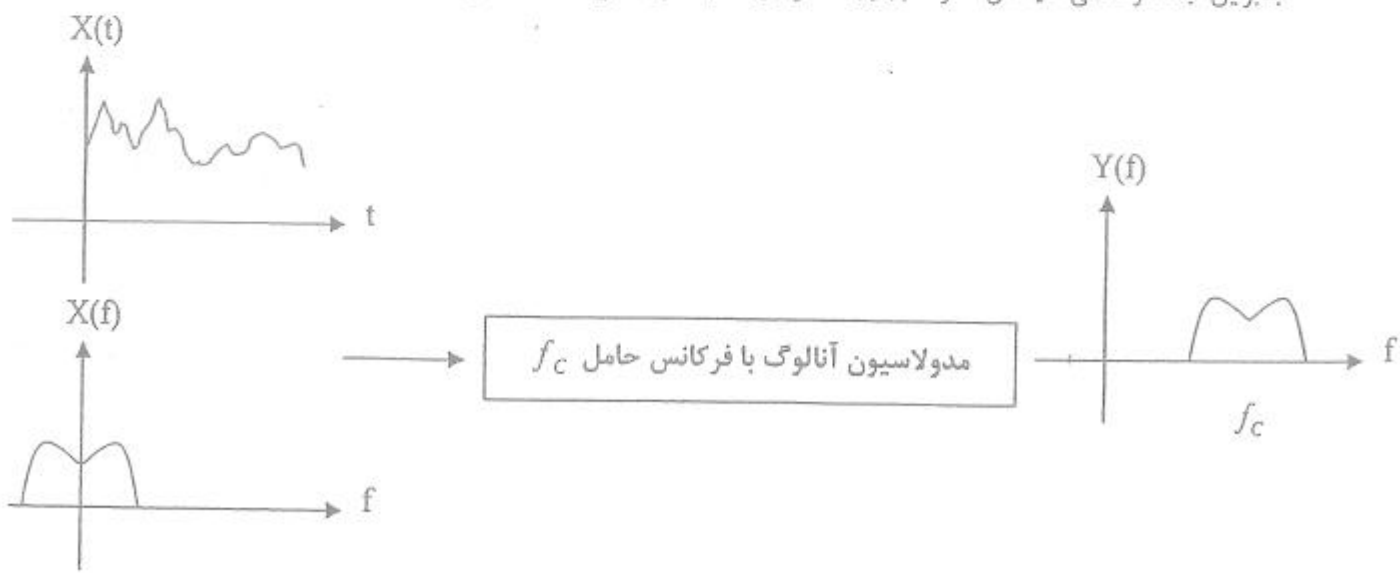
نوع مدرهای واسط و استاندارد الکتریکی: Balanced (متوازن) RS-422A/V.11

فصل چهارم

Coding و Modulation (کدگذاری و مدولاسیون)

معمولاً سیگنال x(t) (آنالوگ یا دیجیتال) قبل از ارسال به صورت یک سیگنال کدگذاری شده یا مدوله شده y(t) (آنالوگ یا دیجیتال) تبدیل می‌شود. دلایل استفاده از تجهیزاتی مانندCoder ، Decoder، Modulator و Demodulator به شرح زیر است:

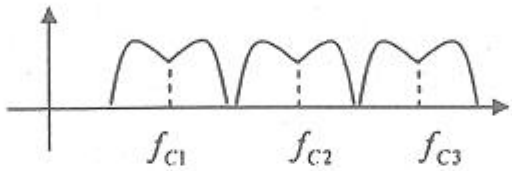
- کاهش تاثیر عوامل مخرب مانند تضعیف ، اعواج ، نویز و غیره (مینیمم کردن اثر نویز و اعواج و غیره)
- امکان ارسال با نرخ بیت یا سرعت بالاتر
- تغییر باند فرکانسی سیگنال x(t) در باند پایه (Base Band) قرار دارد و باید به فرکانس‌های باند محدود (Band Limit) یا باند گذر (Band Pass) منتقل شود. به کمک مدولاسیون سیگنال باند پایه را سوار بر موج حامل (Carrier) با فرکانس f_c می‌نمایند. بنابراین باند فرکانسی سیگنال مدوله y(t) به اندازه f_c شیفت پیدا می‌کند. به شکل ۲۸ نگاه کنید.



شکل ۲۸. شیفت فرکانسی حاصل از مدولاسیون آنالوگ

- می‌توان از یک رسانه مشترک مثل هوا یا فیبر نوری ، چند سیگنال را به‌طور همزمان با روش FDM (Frequency Division Multiplexing) ارسال کرد. به عبارت دیگر یک خط انتقال به چند کانال انتقال تقسیم می‌شود. بنابر این گاهی سیگنال آنالوگ صدا را به سیگنال آنالوگ باند گذر مدوله می‌کنند تا در باند گذر کانال انتقال داده قرار بگیرد و امکان ارسال همزمان چند سیگنال به روش FDM فراهم شود.

مثال : اگر $x_1(t)$ صدایی رادیوی شماره 1 باشد و به اندازه f_{c1} شیفت پیدا کند، $x_2(t)$ صدای رادیوی شماره 2 باشد و به اندازه f_{c2} شیفت پیدا کند و به همین ترتیب تا $x_n(t)$ (صدای رادیوی شماره n) به اندازهٔ f_{cn} شیفت پیدا نماید، شکل ۲۹ نشان می دهد که چگونه این سیگنال‌ها در حوزه فرکانس از یکدیگر قابل تفکیک هستند و به طور همزمان به روش FDM در یک رسانه مشترک مانند هوا ارسال می‌شوند.



شکل ۲۹. در FDM سیگنال‌های مدوله شده در باندهای فرکانسی مجزا در کنار یکدیگر چیده شده‌اند (با فاصله اطمینان)

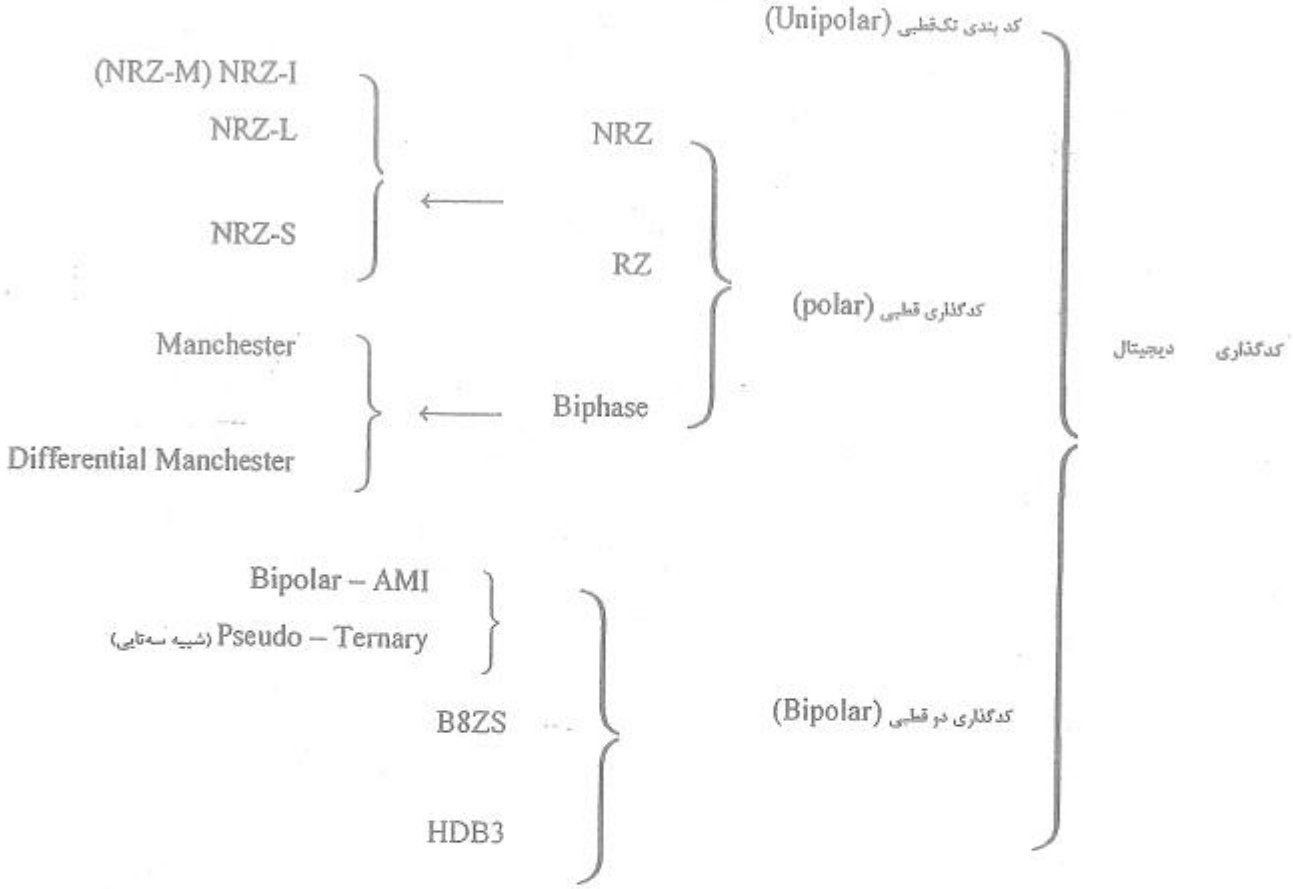
- گاهی سیگنال‌های دیجیتال نیز به آنالوگ تبدیل می‌شوند. زیرا بعضی از رسانه‌های انتقال مثل هوا فقط سیگنال‌های باند گذر را به‌خوبی عبور می‌دهند.
- مدولاسیون برای کاهش پهنای باند نیز به کار می‌رود.

۱ـ۴ انواع کدگذاری و مدولاسیون

چهار روش مختلف کدگذاری و مدولاسیون در علم ارتباطات مورد استفاده قرار می گیرند:

- آنالوگ به آنالوگ (مانند رادیو)
- آنالوگ به دیجیتال (مانند تلفن اینترنتی)
- دیجیتال به دیجیتال (مانند PSDN)
- دیجیتال به آنالوگ (مانند ارسال داده از طریق ماهواره)

۲ـ۴ کدگذاری دیجیتال (ارسال داده‌های دیجیتال با سیگنال‌های دیجیتال)



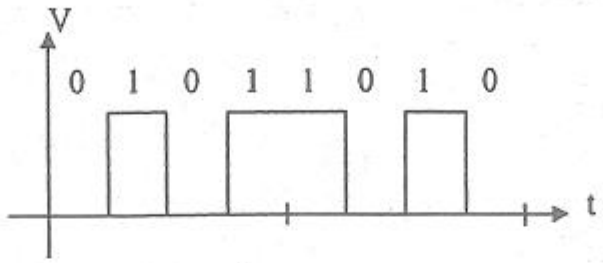
در عبارات اختصاری مربوط به روش NRZ، حرف I به معنی Inverse (معکوس)، حرف M به معنی Mark (یک)، حرف S به معنی Space (صفر) و حرف L به معنی Level (سطح) به کار رفته است.

پلاریته یک سیگنال به مثبت یا منفی بودن (و احتمالاً صفر بودن) ولتاژهای سیگنال ربط دارد. در حالت تک قطبی فقط یک پلاریته داریم (یا پالس‌های مثبت و یا پالس‌های منفی) اما در حالت‌های قطبی و دو قطبی هم از پالس‌های مثبت و هم از پالس‌های منفی استفاده می‌شود که تفاوت این دو را ذکر خواهیم کرد. یکی از مهم‌ترین نکات، مولفه DC این روش‌ها می‌باشد. مشخص است که در روش تک قطبی مولفه DC داریم. اما بعضی از کانال‌ها مولفه DC را عبور نمی‌دهند.

۱ـ۲ـ۴ کدگذاری تک قطبی (Unipolar)

فقط ولتاژ صفر و ولتاژ مثبت (یا منفی) داریم. ولتاژ صفر (یا خط Idle) برای نمایش سطح منطقی صفر و ولتاژ مثبت (یا منفی) برای نمایش سطح منطقی یک به کار می‌رود (و یا بالعکس).

مثال : در شکل ۳۰ ولتاژ مثبت برای نمایش سطح منطقی یک به کار رفته است.



شکل ۳۰. کدگذاری تک قطبی

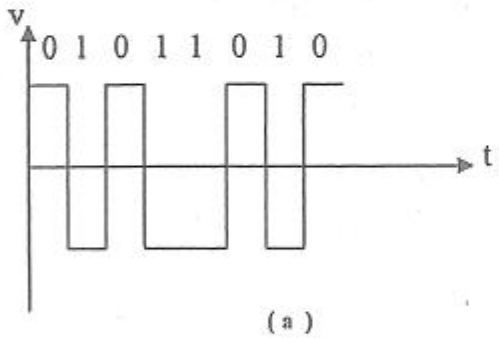
۲ـ۲ـ۴ کدگذاری قطبی (Polar)

در این روش هم ولتاژهای مثبت و هم ولتاژهای منفی وجود دارند و بنابراین مولفه DC سیگنال کاهش می‌یابد. یکی از روش‌هایی که مولفه DC را کاملاً حذف می‌کند، روش Biphase است که در هر بیت به‌صورت متقارن هر دو سطح ولتاژ وجود دارد. در ادامه سه روش کدگذاری قطبی مورد بررسی قرار خواهند گرفت.

۱ـ۲ـ۲ـ۴ کدگذاری قطبی به روش NRZ

این روش کدگذاری به سه صورت زیر پیاده سازی می‌شود:

- NRZ-L
- NRZ-I (NRZ-M)
- NRZ-S



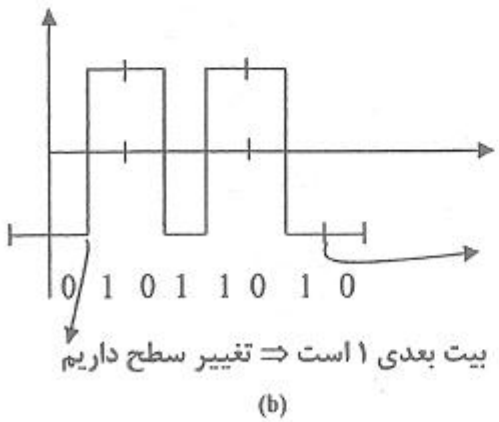
(a)

$NRZ-L^{Level} \Leftarrow$
- 0: سطح ولتاژ مثبت (یا بالعکس)
- 1: سطح ولتاژ منفی (یا بالعکس)

NRZ-I یا NRZ-M
- 0: عدم تغییر سطح در ابتدای فاصله زمانی بیت
- 1: تغییر سطح در ابتدای فاصله زمانی بیت

برای درک بهتر روش‌های کدگذاری NRZ-L و NRZ-M به شکل ۳۱ نگاه کنید.

NRZ-Sمنطق صفر و یک برعکس NRZ-M است.



(b)

شکل ۳۱. (a)کدگذاری NRZ-L (b)کدگذاری NRZ-M (NRZ-I)

نکته : روش‌های NRZ-I و NRZ-S روش‌های تفاضلی محسوب می‌شوند و بر اساس تغییر سطح در آغاز بیت عمل می‌کنند در حالیکه روش NRZ-L بر اساس سطح (Level) سیگنال عمل می‌کند و چون احتمال شناسایی گذار در حضور نویز بالا است، روش‌های تفاضلی در برابر نویز تاثیرپذیری کمتری دارند.

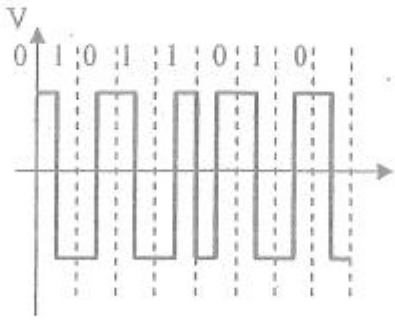
۲ـ۲ـ۲ـ۴ کدگذاری قطبی به روش RZ

عیب روش‌های NRZ این است که رشته طولانی مثلاً صفر (0...000) موجب می‌شود که سطح سیگنال ثابت بماند و در تشخیص با مشکل روبرو می‌شویم. البته برای همگام‌سازی می‌توان سیگنال Clock را جداگانه ارسال کرد که هزینه بالایی دارد. راه حل بهتر، سیگنال RZ است که Clock را درون خود اطلاعات گنجانیده است. به شکل ۳۲ نگاه کنید.

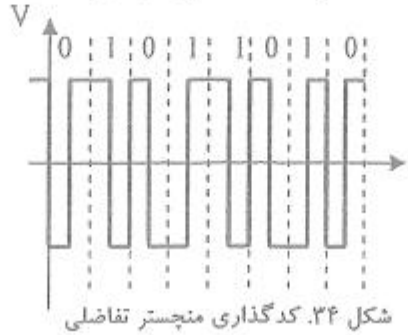
شکل ۳۲. کدگذاری RZ

۳ـ۲ـ۲ـ۴ کدگذاری قطبی به روش Biphase

در این روش همانند روش RZ، یک تغییر حالت در وسط هر بیت وجود دارد و بنابراین امکان استخراج Clock همزمانی در گیرنده وجود دارد. اما بر خلاف روش RZ، فقط تغییر حالت بین ولتاژ مثبت و منفی است (نه ولتاژ 0) و در نتیجه سطح DC سیگنال، صفر است. شکل های ۳۳ و ۳۴ دو روش Manchester (Biphase-L) و Differential Manchester را نشان می‌دهند. در روش منچستر سطح سیگنال، منطق صفر یا یک را مشخص می‌کند و در روش منچستر تفاضلی وجود یا عدم وجود تغییر سطح در شروع بیت، منطق صفر یا یک را نشان می‌دهد. کدگذاری منچستر در شبکه‌های Ethernet و کدگذاری منچستر تفاضلی در شبکه‌های Token Ring کاربرد دارد.



شکل ۳۳. کدگذاری منچستر



* وجود تغییر حالت در شروع بیت به معنای بیت 0 است.

شکل ۳۴. کدگذاری منچستر تفاضلی

۳ـ۲ـ۴ کدگذاری دو قطبی (Bipolar)

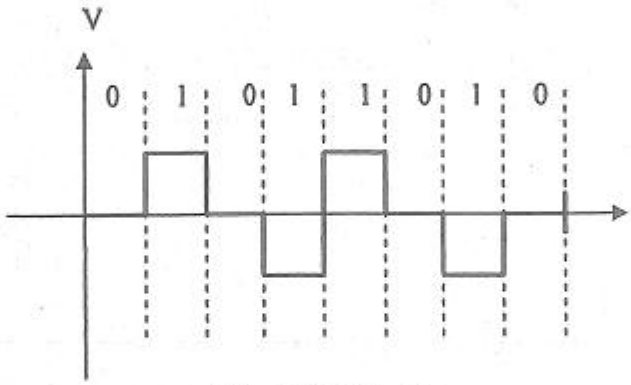
این کدگذاری مانند RZ، چند سطحی محسوب می‌شود چون هم سطح ولتاژ مثبت ، هم صفر و هم سطح ولتاژ منفی در آن دیده می‌شود. اما در این‌جا بر خلاف روش RZ، از سطح ولتاژ 0 نیز برای منطق 0 یا 1 استفاده می‌شود. در ادامه چهار روش مهم دو قطبی مورد بررسی قرار خواهد گرفت.

۱ـ۳ـ۲ـ۴ کدگذاری دوقطبی AMI (Alternate Mark Inversion)

در این روش کدگذاری، مطابق شکل ۳۵، صفرها و یک‌ها، یک در میان با سطح ولتاژ مثبت و منفی مشخص می‌شوند.

منطق 0 → 0 ولت

Mark ها (یک‌ها) یک در میان مثبت و منفی می‌شوند. ⇒ منطق 1 → (V- و V+)



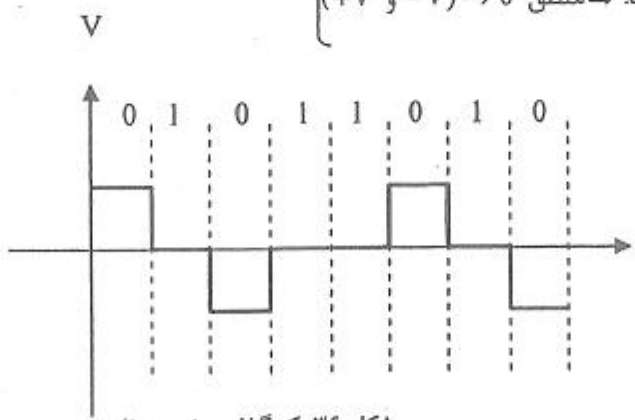
شکل ۳۵. کدگذاری AMI

۲ـ۳ـ۲ـ۴ کدگذاری دو قطبی شبه سه‌تایی (Pseudo – ternary)

این روش همانند AMI است؛ فقط با این تفاوت که منطق صفر و یک برعکس آن روش می‌باشد. (به شکل ۳۶ نگاه کنید)

منطق 1 → 0 ولت

Space ها یک در میان مثبت و منفی می‌شوند. ⇒منطق 0 → (V- و V+)

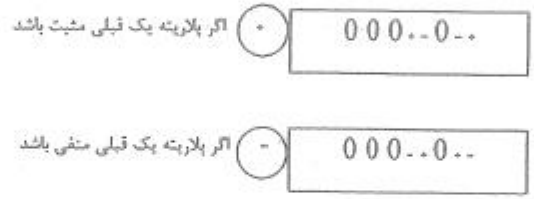


شکل ۳۶. کدگذاری شبه سه‌تایی

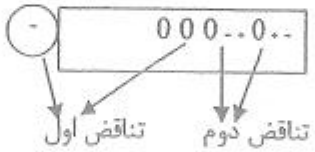
نکته ۱: در کدگذاری‌های نظیر AMI، مجدداً مشکل رشته طولانی صفر وجود دارد و عمل همزمانی دچال اشکال می‌شود.
نکته ۲: از طرف دیگر در کدگذاری‌های نظیر Manchester پهنای باند زیادی لازم داریم.
برای حل این مشکلات دو کدگذاری در آمریکای شمالی (B8ZS) و در اروپا و ژاپن (HDB3) طراحی شده است که در ادامه به تشریح آنها خواهیم پرداخت.

۴-۲-۳-۳ کدگذاری B8ZS (Bipolar – 8 Zero Substituation)

این روش اصولا همانند AMI است و اختلاف این دو روش در این است که هر گاه هشت صفر پشت سر هم پیدا شود کدگذاری B8ZS به جای 8 صفر یک الگو به شکل زیر را جایگزین می‌کند.
توجه کنید که در AMI یک‌ها، یک در میان + و - می‌شوند و بنابراین در الگوی فوق الذکر دو تناقض وجود دارد. (2 مثبت و 2 منفی متوالی)



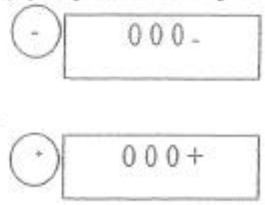
شکل زیر نشان می‌دهد که دو تناقض در الگوی جایگزین وجود دارد. به الگوی جایگزین، الگوی تناقض یا تخطی(Violation) نیز گفته می‌شود.



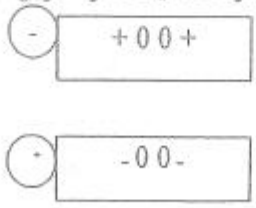
۴-۲-۳-۴ کدگذاری HDB3 (High Density Bipolar 3)

اساس این روش نیز AMI است با این تفاوت که این استاندارد چهار صفر پشت سر هم (بر خلاف عدد 3 درون نامش!) را با یک الگوی تناقض به شرح زیر جایگزین می‌کند. (دایره‌ها پلاریته یک قبلی را نشان می‌دهند.)

اگر تعداد یک‌ها از آخرین جایگزینی قبلی فرد باشد.



اگر تعداد یک‌ها از آخرین جایگزینی قبلی زوج باشد



۴-۲-۴ نکاتی در مورد روش‌های کدگذاری دیجیتال

نکته ۱: نرخ مدولاسیون همان نرخ سیگنالینگ (R_s) است. قبلاً دیدیم که در یک سیگنال 8 سطحی رابطه زیر برقرار است:

$$\text{Bit Rate}(\text{bps}) = R = 3R_s\,(\text{Band}) \quad \left(\log_2^M = \log_2^8 = 3\right)$$

اما واضح است که در کدگذاری RZ می‌توان از رابطه زیر استفاده کرد:

نرخ مدولاسیون = نرخ سیگنالینگ $R_s = 2R$

رابطه فوق در روش‌های کدگذاری منچستر و منچستر تفاضلی نیز صادق است؛ زیرا در این 3 روش کدگذاری، حداقل اندازه یک عنصر سیگنال پالسی است که به اندازه نصف عرض بیت است.

$$\text{عرض هر عنصر سیگنال} = \frac{1}{2}\tau_B = \frac{1}{2R}$$

با توجه به اینکه برای محاسبه Band Rate و پهنای باند لازم برای عبور سیگنال، بدترین حالت را در نظر می‌گیرند، می‌توان نوشت:

$$\Rightarrow \text{Max (نرخ مدولاسیون)} = \text{Max}(R_S) = 2R$$

از طرف دیگر در روش‌های کدگذاری NRZ مانند NRZ-L ، NRZ-S و NRZ-I می‌توان نوشت:

$$\text{نرخ مدولاسیون} = R_S = R$$

نکته ۲: برای محاسبه پهنای باند، لازم برای عبور سیگنال دیجیتال از کانال، سیگنال مربعی بدترین حالت (Worst Case) را در نظر بگیرید.

مثال ۱: در کدگذاری RZ، بدترین حالت یک‌های متوالی است که در آن حالت $R_S = 2R$ و بنابراین $f_0 = R$ خواهد بود (f_0 فرکانس پایه سیگنال است) و لذا پهنای باند لازم برای عبور سیگنال برابر R خواهد بود.

مثال ۲: در کدگذاری تک قطبی، بدترین حالت ..... 010101است که در آن حالت $R_S = R$ و بنابراین $f_0 = \frac{R}{2}$ خواهد بود و لذا پهنای باند لازم برای عبور سیگنال برابر $\frac{R}{2}$ می‌باشد.

مثال ۳: در منچستر تفاضلی، صفرهای متوالی بدترین حالت سیگنال را بوجود می‌آورند و پهنای باند لازم مانند مثال ۱ خواهد بود.

۳ـ۴ مدولاسیون دیجیتال به آنالوگ

مهم‌ترین کاربرد این نوع از مدولاسیون، ارسال داده‌های دیجیتال از طریق شبکه‌های عمومی مثل PSTN می‌باشد (مودم‌ها در این روش سیگنال‌ها را در محدوده فرکانسی صوت انسان تولید می‌کنند). یک کاربرد دیگر آن مودم‌های Microwave می‌باشند که با فرکانس‌های بالاتری کار می‌کنند. برای درک مفهوم مدولاسیون، یک موج سینوسی حامل را در نظر بگیرید. با تغییر در یک یا چند مشخصه از موج حامل می‌توان داده‌های دیجیتال را سوار بر این موج حامل نمود (مدولاسیون). این مشخصات موج حامل عبارتند از:

- مشخصه دامنه
- مشخصه فرکانس
- مشخصه فاز

مهم‌ترین روش‌های مدولاسیون دیجیتال به آنالوگ عبارتند از:

- ASK (Amplitude Shift Keying): شیفت گسسته دامنه ← در مدولاسیون آنالوگ به آنالوگ به AM (Amplitude modulation) مشهور است.
- FSK (Ferquency Shift Keying): شیفت گسسته فرکانس ← در مدولاسیون آنالوگ به آنالوگ به FM(Ferquency Modulation) مشهور است.
- PSK (Phase Shift Keying): شیفت گسسته فاز ← در آنالوگ به آنالوگ به PM (Phase Modulation) مشهور است.
- QPSK (Quadrature-PSK): شیفت گسسته فاز چهار گانه (تربیعی) ← به 4-PSK نیز مشهور است. (با توسعه آن 8-PSK ، 16-PSK و غیره خواهیم داشت)
- QAM (Quadrature Amplitude Modulation): مدولاسیون دامنه چهارگانه (تربیعی) (با توسعه آن 16-QAM و غیره خواهیم داشت)

نکته : به روش‌های QPSK ، QAM و مشتقات آن‌ها مدولاسیون‌های چند سطحی (Multilevel Modulation) می‌گویند.

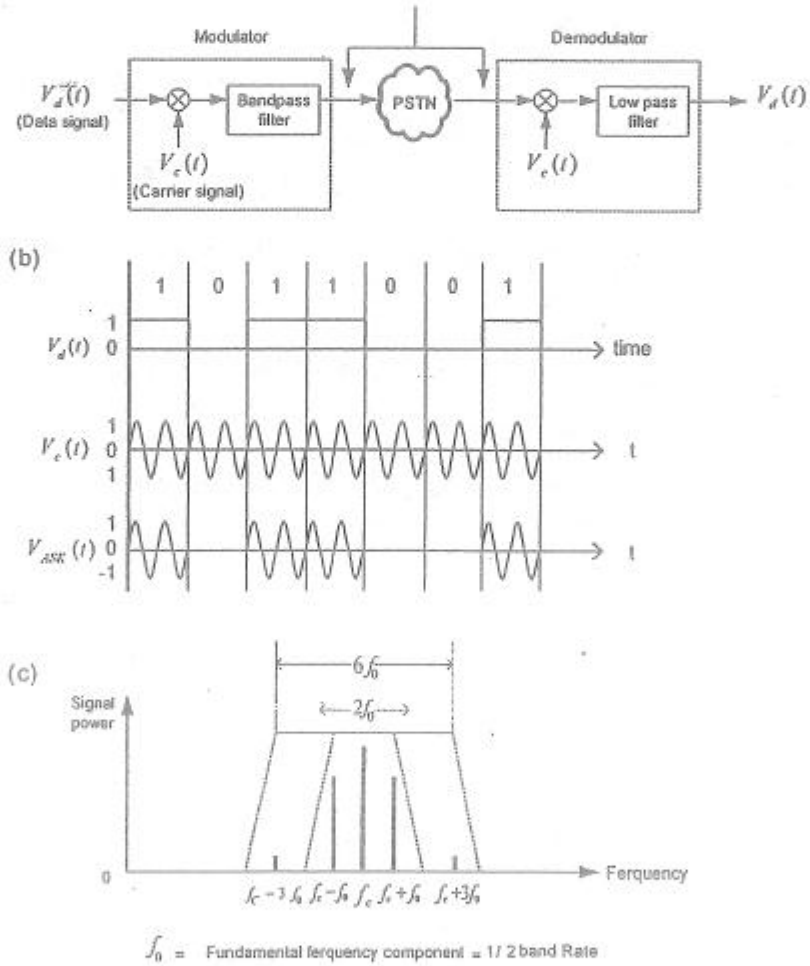
۱_۳_۴ ASK

فرض کنید که سیگنال حامل یک موج سینوسی با فرکانس f_c (فرکانس زاویه‌ای = $\omega_c = 2\pi f_c$) باشد: $V_c(t) = \text{Cos}\omega_c t$

شکل ۳۷ عملکرد ASK را نشان می‌دهد.

همان‌طور که قبلا دیدیم $V_d(t)$ (سیگنال باینری که باید ارسال شود) در حالت worst Case Sequence به‌صورت زیر است:

$$V_d(t) = \frac{1}{2} + \frac{2}{\pi}\left\{\cos\omega_0 t - \frac{1}{3}\cos 3\omega_0 t + \frac{1}{5}\cos 5\omega_0 t - \ldots\right\}$$



شکل ۳۷. مدولاسیون ASK

نکته ۱: با توجه به شکل (b) ۳۷، Band Rate سیگنال ASK برابر Bit Rate است و می‌توان نوشت:

$$f_0 = \frac{1}{2}R(\text{bps}) = \frac{1}{2}R_s(\text{band})$$

مطابق شکل (a) ۳۷، مدولاسیون ASK از ضرب سیگنال دیجیتال در موج سینوسی حامل و عبور آن از یک فیلتر باند گذر بدست می‌آید:

$$V_{ASK}(t) = V_C(t)V_d(t) \Rightarrow V_{ASK}(t) = \frac{1}{2}\cos\omega_c t + \frac{2}{\pi}\left\{\cos\omega_C t\cos\omega_0 t - \frac{1}{3}\cos\omega_C t\cos 3\omega_0 t + ...\right\}$$

توجه کنید که در مدولاسیون ASK ممکن است به جای دامنه‌های 0 و V دو سطح V_1 و V_2 را ارسال نمائیم

نکته ۲ (مهم): رابطه مثلثاتی زیر را در نظر بگیرید:

$$2\cos A\cos B = \cos(A-B) + \cos(A+B)$$

بنابراین می‌توان نوشت:

$$V_{ASK}(t) = \frac{1}{2}\cos\omega_C t + \frac{1}{\pi}\left\{\cos(\omega_c - \omega_0)t + \cos(\omega_c + \omega_0)t - \frac{1}{3}\cos(\omega_C - 3\omega_0)t - \frac{1}{3}\cos(\omega_c + 3\omega_0)t + ...\right\}$$

بنابراین نتیجه می‌گیریم که در سیگنال ASK (بدترین حالت) فرکانس‌های، f_c، f_c+f_0، f_c-f_0، f_c+3f_0، f_c-3f_0 و ... وجود دارند.

نکته ۳ (مهم): اگر پهنای باند فیلتر Bandpass را $2f_0$ فرض کنیم مولفه‌های f_c و $f_c \pm f_0$ عبور می‌کنند که برای تشخیص کافی است. بنابراین در مسائل اگر هیچ نکته خاص دیگری ذکر نگردد، پهنای باند سیگنال ASK را $\left[BW = 2f_0 = R(bps) = R_S(band)\right]$ در نظر می‌گیریم.

نکته ۴: اگر بخواهیم مولفه‌های هارمونیک سوم سیگنال اصلی نیز دریافت گردد، پهنای باند $6f_0$ لازم است.

نکته ۵: می‌توان یک فیلتر Bandpass با پهنای باند f_0 داشت. در نتیجه مولفه‌های f_c و $f_c + f_0$ عبور خواهند کرد و از آنجائیکه مولفه سیگنال اصلی وجود دارد، قابل تشخیص خواهد بود. به مولفه‌های $f_c \pm f_0$ و $f_c \pm 3f_0$ مولفه‌های Side Band می‌گویند. ما در اینجا Side Band پائین را حذف کرده‌ایم (حذف $f_c - f_0$). البته واضح است که در این صورت، مشکل دیگری پیش می‌آید، توان سیگنال اصلی نصف می‌شود و بنابراین SNR کاهش می‌یابد و BER افزایش می‌یابد. در هر حال، به این پهنای باند، پهنای باند نرخ نایکوییست می‌گویند.

مثال: اگر نرخ بیت سیگنال ...101010 برابر 1200bps باشد:

مولفه اصلی فرکانسی : $f_0 = 600Hz$

مولفه هارمونیک سوم: $3f_0 = 1800Hz$

پهنای باند (پهنای باند مولفه اصلی): $2f_0 = 1200Hz$

پهنای باند با مولفه سوم: $6f_0 = 3600Hz$

پهنای باند نایکوییست: $f_0 = 600Hz$

FSK ۴_۳_۲

در FSK به‌جای شیفت در دامنه، دامنه سیگنال مدوله را ثابت می‌گیرند و شیفت گسسته را در فرکانس ایجاد می‌نمایند.

فرض کنید که $V_d(t)$ سیگنال ارسالی (باینری) باشد؛ $V'_d(t)$ را به صورت مکمل $V_d(t)$ در نظر می‌گیریم $\left[V'_d(t) = 1 - V_d(t)\right]$. در نتیجه سیگنال FSK به صورت زیر تعریف می‌شود.

$$V_{FSK}(t) = \cos\omega_1 t V_d(t) + \cos\omega_2 t V'_d(t)$$

ω_1 و ω_2 معرف فرکانس‌های زاویه‌ای حامل می‌باشند. در حالت worst Case Sequence می‌توان نوشت:

$$V_{FSK}(t) = Cos\omega_1 t\left\{\frac{1}{2} + \frac{2}{\pi}\left(\cos\omega_0 t - \frac{1}{3}\cos 3\omega_0 t + ...\right)\right\} + \cos\omega_2 t\left\{\frac{1}{2} - \frac{2}{\pi}\left(\cos\omega_0 t - \frac{1}{3}\cos 3\omega_0 t + ...\right)\right\}$$

$$V_{FSK} = \frac{1}{2}\cos\omega_1 t + \frac{1}{\pi}\left\{\cos(\omega_1-\omega_0)t + \cos(\omega_1+\omega_0)t - \frac{1}{3}\cos(\omega_1-3\omega_0)t - \frac{1}{3}\cos(\omega_1+3\omega_0)t + \ldots.\right\}$$
$$+\frac{1}{2}\cos\omega_2 t + \frac{1}{\pi}\left\{\cos(\omega_2-\omega_0)t + \cos(\omega_2+\omega_0)t - \frac{1}{3}\cos(\omega_2-3\omega_0)t - \frac{1}{3}\cos(\omega_2+3\omega_0)t + \ldots.\right\}$$

نکته ۱: $f_s = f_2 - f_1$ را شیفت فرکانسی می‌نامند. (تفاوت بین دو فرکانس حامل)

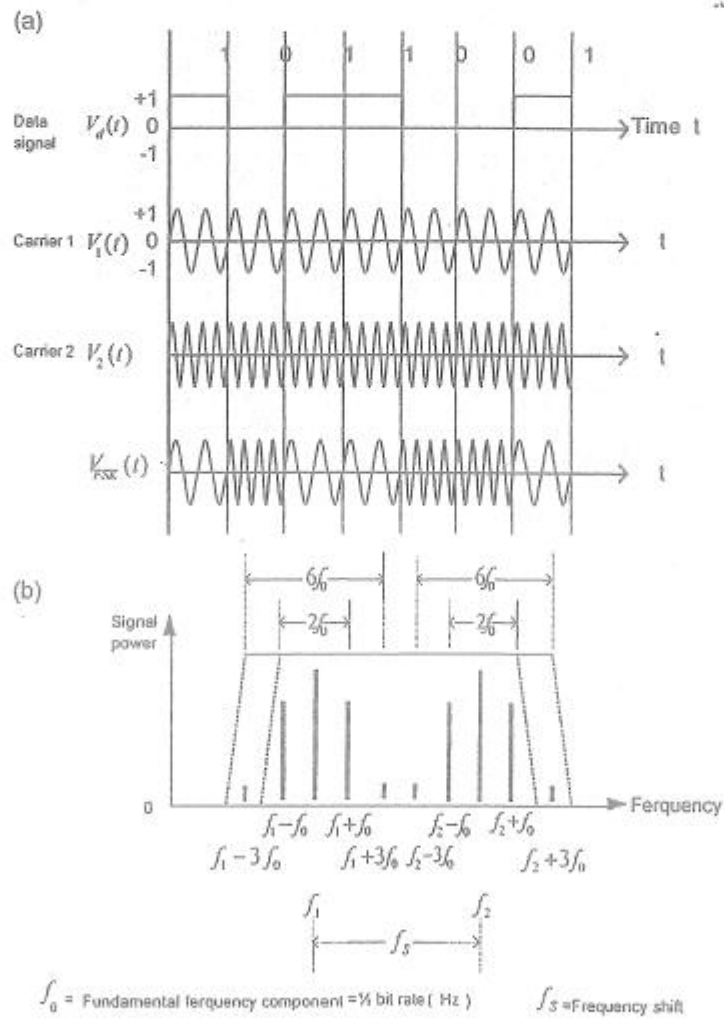
نکته ۲: همان‌طور که در شکل ۳۸(b) دیده می‌شود در سیگنال مدوله FSK فرکانس‌های f_1، $f_1 \pm f_0$، $f_1 \pm 3f_0$ و.... و نیز فرکانس‌های f_2، $f_2 \pm f_0$، $f_2 \pm 3f_0$ و .... دیده می‌شوند.

نکته ۳: پهنای باند لازم برای عبور کامل مولفه f_0 و شناسایی قابل قبول سیگنال در گیرنده از رابطه زیر استفاده می‌شود:

$$\boxed{BW = f_s + 2f_0}$$

نکته ۴: پهنای باند لازم برای عبور کامل مولفه $3f_0$ برابر $f_s + 6f_0$ است که البته در عمل همان $f_s + 2f_0$ کافی است.

نکته ۵: در این‌جا نیز مانند روش ASK ، Bit Rate با Band Rate برابر است و به عبارت دیگر در این روش‌ها هر عنصر سیگنال یک بیت را ارسال می‌کند.



شکل ۳۸. مدولاسیون FSK

PSK ۴_۳_۳

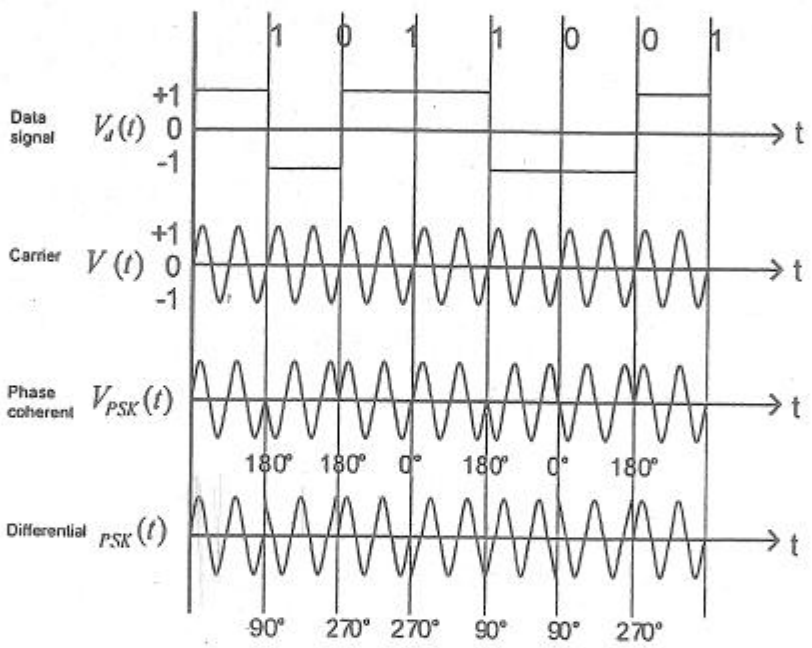
در این نوع مدولاسیون، دامنه و فرکانس ثابت است و 0 و 1 را با شیفت فاز نشان می‌دهند.

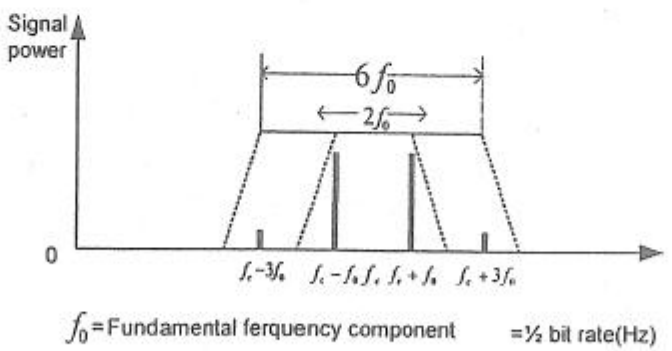
دو روش PSK وجود دارد.

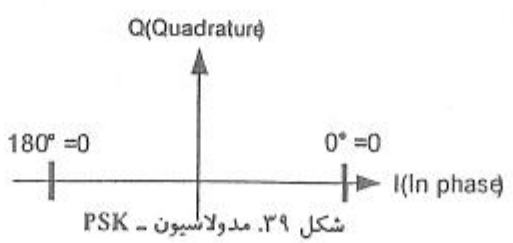
- Phase Coherent PSK
- Differential PSK

در روش اول، بین صفر و یک 180^0 اختلاف فاز وجود دارد. اشکال این روش این است که گیرنده برای تشخیص صفر و یک به سیگنال حامل مرجع نیاز دارد تا آن را با سیگنال دریافتی مقایسه کند.

اما در روش دوم ، یک شیفت 90^0 نسبت به سیگنال جاری معرف این است که بیت دودویی بعدی صفر است و یک شیفت 270^0 نسبت به سیگنال جاری معرف این است که بیت دودویی بعدی یک است.







شکل ۳۹. مدولاسیون ـ PSK

نکته ۱: اگر فرض کنید که مطابق شکل ۳۹ (برای روش اول) سیگنال باینری را به صورت زیر می‌توان نوشت (worst case):

$$V_d(t)=\frac{4}{\pi}\left\{\cos\omega_0 t-\frac{1}{3}\cos 3\omega_0 t+\frac{1}{5}\cos 5\omega_0 t-....\right\}$$

$$V_{PSK}=\frac{4}{\pi}\left\{\cos\omega_0 t\cos\omega_c t-\frac{1}{3}\cos 3\omega_0 t\cos\omega_c t+....\right\}$$

$$V_{PSK}=\frac{2}{\pi}\left\{\cos(\omega_c-\omega_0)t+\cos(\omega_c+\omega_0)t-\frac{1}{3}\cos(\omega_c-3\omega_0)t-\frac{1}{3}\cos(\omega_c+3\omega_0)t....\right\}$$

نکته ۲: در این روش، فقط مولفه‌های $f_c\pm f_0$ ، $f_c\pm 3f_0$ ، $f_c\pm 5f_0$ و ...وجود دارند.

نکته ۳: در این روش نیز Bit Rate با Band Rate برابر است و $f_0=\frac{1}{2}R=\frac{1}{2}R_S$.

نکته ۴: پهنای باند موردنیاز برای عبور کامل مولفه‌های (دو مولفه) f_0 برابر نرخ بیت است $[BW=2f_0=R=R_S]$.

نکته ۵: در این روش نیز اگر پهنای باند نرخ نایکوییست را بخواهیم، برابر f_0 یا $\frac{R}{2}$ خواهد بود که البته SNR را می‌کاهد.

نکته ۶ (مهم): باتوجه به اینکه در Modulator و Demodulator از فیلتر استفاده می شود و در عمل، فیلترها ایده‌ال نمی‌باشند (البه های آن تیز نبوده و انحنا دارد) یک ضریب حذف فیلتر ($0<r<1$) نیز در روابط پهنای باند ظاهر می شود و برای عبور کامل مولفه‌های (دو مولفه) f_0 در مدولاسیون‌های ASK ، FSK و PSK به صورت زیر است:

$$BW(ASK)=R_s(1+r)$$
$$BW(PSK)=R_s(1+r)$$
$$BW(FSK)=f_s+[R_s(1+r)]$$

۴ـ۳ـ۴ روش‌های مدولاسیون چند سطحی

همان‌گونه که قبلا اشاره شد هر عنصر از سیگنال می‌تواند به یکی از سه صورت زیر باشد:

- کمتر از یک بیت (مثل Manchester)
- یک بیت (مثل NRZ-L و FSK).
- بیشتر از یک بیت (مثل QPSK).

در روش‌های ذیل در هر عنصر سیگنال بیش از یک بیت ارسال می‌شود.

- روش QPSK (4-PSK) [Quadrature – PSK]

همانند شکل (a,b) ۴۰ ، چهار تغییر فاز مختلف °0، °90، °180 و °270 نشان‌دهنده 00 ، 01، 10 و 11 می‌باشند. در این روش می‌توان نوشت:

$$R=R_S\log_2^4=2R_S$$

نکته : برای دستیابی به نرخ بیت‌های بالاتر، 8 یا 16 تغییر فاز نیز امکان‌پذیر است. (16-PSK,8-PSK)

اشکال مهم: کاهش اختلاف فازها موجب می شود که حساسیت به نویز بیشتر شود . بنابراین کمتر از روش‌های 16-PSK و بالاتر استفاده می‌شود.

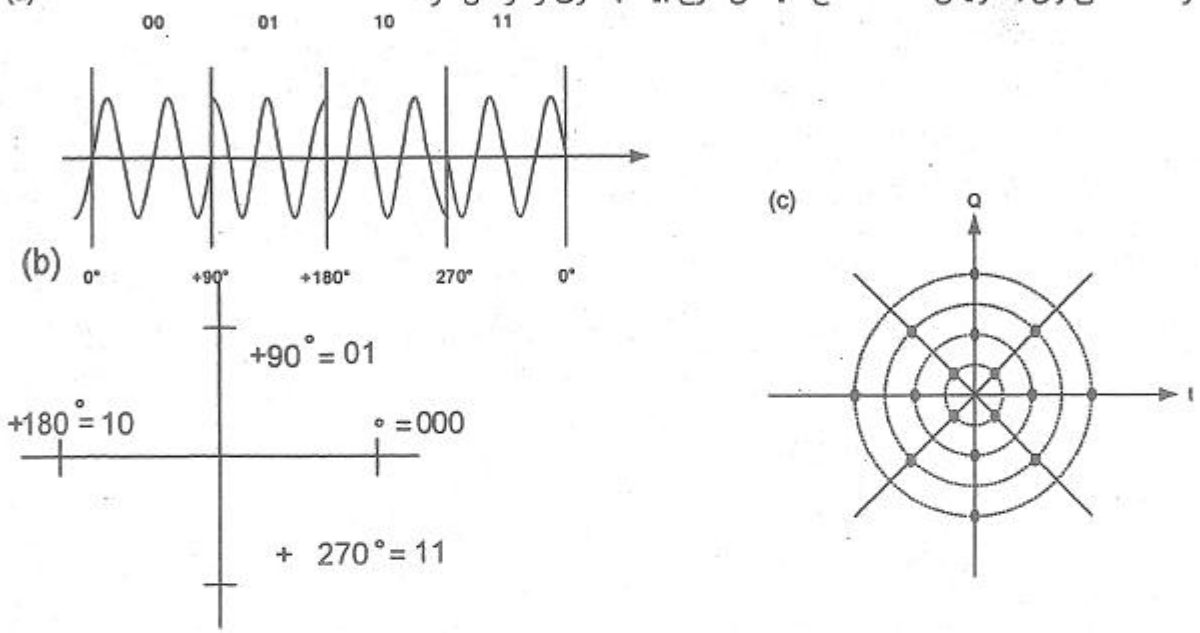
نکته مهم : برای افزایش نرخ بیت، پیشنهاد می‌شود که علاوه بر فاز ، دامنه سیگنال نیز تغییر نماید. این روش QAM نامیده می‌شود که در زیر شرح داده می‌شود.

- روش QAM (Quadrature Amplitude Modulation)

دیاگرام فضایی شکل (c) ۴۰، QAM را با 16 سطح سیگنال (هر band معرف 4 بیت) نشان می‌دهد.

$$16-QAM \Rightarrow R = R_s \log_2^{16} = 4R_s \quad (\text{Bit Rate} = 4 * \text{baud Rate})$$

نکته مهم: در این‌روش‌ها، f_0 (فرکانس پایه worst case) را برابر $\frac{R_s}{2}$ در نظر بگیرید. به عبارت دیگر، با پهنای باند محدود $2f_0$ در PSK و ASK می‌توان با افزایش تعداد سطح سیگنال، نرخ بیت بالاتری را ارسال کرد.



شکل ۴۰. مدولاسیون چند سطحی

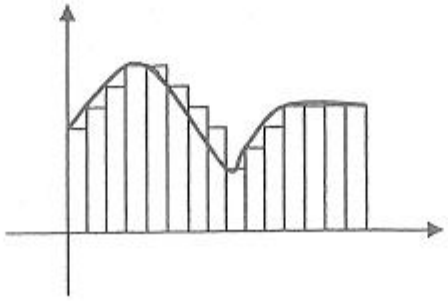
۴ـ۴ مدولاسیون آنالوگ به دیجیتال

در این مدولاسیون، داده‌های آنالوگ مثل صوت را به صورت دیجیتال در می‌آوریم. مهم‌ترین روش‌های آن عبارتند از:

- مدولاسیون PAM
- مدولاسیون PCM
- مدولاسیون DM

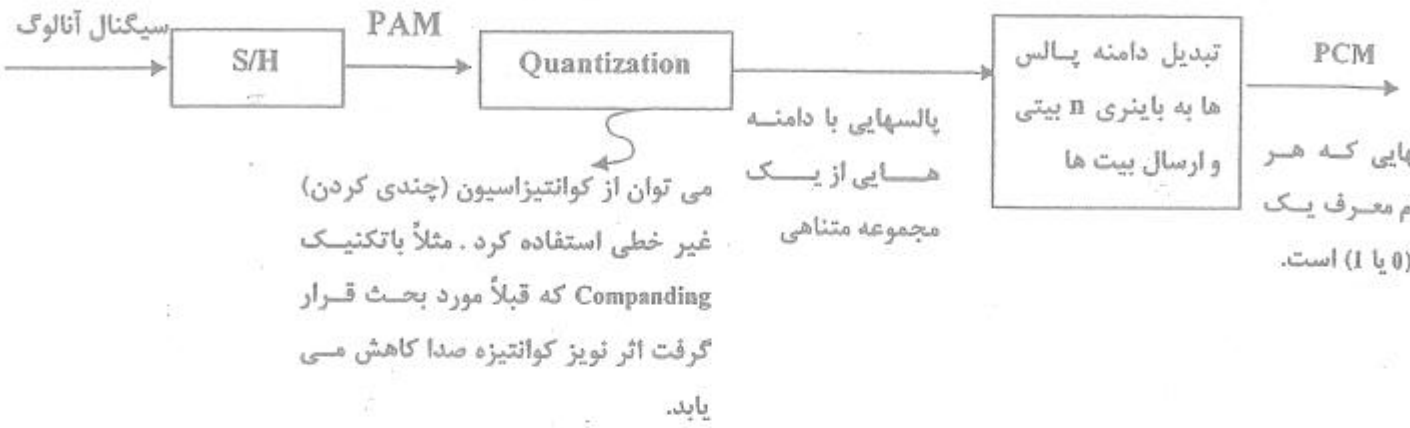
۴ـ۴ـ۱ PAM (Pulse Amplitude Modulation)

در این تکنیک، با یک فرکانس مخصوص بر اساس تئوری نایکوییست ($f_s \geq 2 * f_{max}$) از سیگنال آنالوگ نمونه‌برداری (Sampling) می‌کنیم و هر نمونه یک پالس با ارتفاع (دامنه) نمونه خواهد بود. در واقع یک قطار پالس از نمونه‌ها داریم که از یک S/H (Sample & Hold به معنی نمونه‌برداری و نگهداری) بدست می‌آید. به شکل ۴۱ توجه کنید.



شکل ۴۱ مدولاسیون PAM

۲-۴-۴ PCM (Plule Code Madulation)



شکل ۴۲. مدولاسیون PCM

مراحل ایجاد سیگنال PCM به شرح زیر است:

۱ـ ایجاد سیگنال PAM به کمک S/H

۲ـ Quantization

۳ـ Binary Encoding

۴ـ کدگذاری دیجیتال به دیجیتال [مثل NRZ-L (و ارسال پالس‌های دیجیتال)]

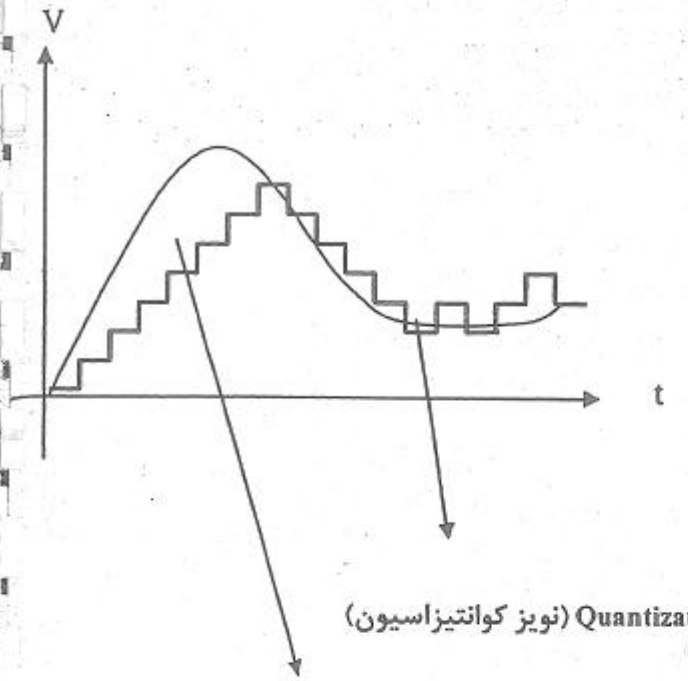
نکته : SNR کوانتیزاسیون خطی با n بیت از رابطه زیر بدست می‌آید.

$$SNR_{dB} = 20\log_{10}^{2^n} + 1.76 \approx \boxed{6.02n + 1.76}\,(dB)$$

۳ـ۴ـ۴ DM (Delta Modulation)

در این روش (مدولاسیون دلتا) پالس‌ها بر خلاف روش PAM دقیقاً از نمونه‌برداری بدست نمی‌آید، بلکه هر پالس با پالس قبلی حداکثر به اندازه یک سطح کوانتیزاسیون (δ) اختلاف دارد. اختلاف دامنه هر پالس با پالس قبلی یا δ+ و یا δ- است. اختلاف سطح صفر و نیز اختلاف سطح بیش از δ غیرمجاز است.

هدف اصلی این نوع مدولاسیون این است که به ازاء هر پالس فقط یک بیت نگهداری یا ارسال شود. به عبارت دیگر، حجم اطلاعات کم و فشرده است.



Quantization Noise (نویز کوانتیزاسیون)

نویز مدولاسیون دلتا یا Slop Overload Noise (نویز اضافه بار شیب)

شکل ۴۳. مدولاسیون DM

نکته ۱: شکل ۴۳، نشان می‌دهد که در این مدولاسیون ۲ نوع خطا (نویز) وجود دارد:

- نویز مدولاسیون دلتا: حاصل از اضافه بار شیب‌های تند.
- نویز کوانتیزاسیون: حاصل از پله‌ای بودن سیگنال مدوله شده.

نکته ۲: برای کاهش نویز اضافه بار شیب، باید δ افزایش یابد، از طرفی افزایش δ موجب افزایش نویز کوانتیزاسیون می‌شود.

تست‌های فصل سوم و چهارم

۱ ـ داده‌های دیجیتالی به روش NRZ-L با نرخ انتقال 100Kbps ارسال می‌شود. اگر Clock فرستنده و گیرنده، اختلاف نسبی 10^{-3} (0.1% اختلاف) داشته باشند، بعد از چند Clock اولین خطای تشخیص در اثر ناهمگامی Clock ها مشاهده خواهد شد؟ (هر چند Clock یک بار خطای تشخیص رخ می‌دهد؟)

۱) 1000 ۲) 500 ۳) 100000 ۴) 50000

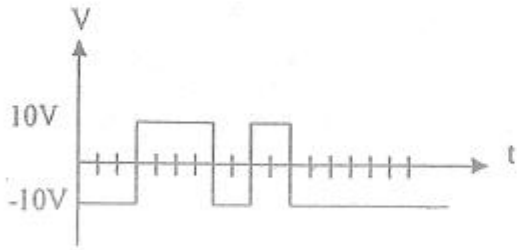
۲ ـ یک پیغام به طول 1000 کاراکتر 8 بیتی مفروض است. اگر از روش غیر همزمان در انتقال آن استفاده شود، زمان مورد نیاز برای انتقال این پیغام چقدر است؟ سرعت (نرخ) انتقال را 5000bps فرض نمائید. یک بیت شروع و یک بیت پایان داریم و بیت توازن وجود ندارد.

۱) تقریباً 1.6 ثانیه ۲) 2 ثانیه ۳) 16 ثانیه ۴) 20 ثانیه

۳ ـ در تست ۲، چند درصد زمان انتقال، سربار بیت‌های کنترلی است؟

۱) %20 ۲) %30 ۳) کمتر از %1 ۴) بیش از %1 و کمتر از %10

۴ ـ فرض کنید از یک خط RS-232D سیگنال زیر دریافت شده است. نرخ انتقال 10000band و هر تیک در شکل زیر 0.1ms فرض می‌شود. اگر کاراکترهای ارسالی 7 بیتی باشند و یک بیت توازن (parity) داشته باشیم (بیت توزان در موقعیت MSB است) کاراکتر ارسالی کدام است؟



۱) 0011000 ۲) 0001111 ۳) 1110000 ۴) 0001100

۵ ـ در تست ۴ اگر فرض کنیم، خطا در ارسال صورت نگرفته است، نوع parity کدام است و چند بیت خطا را آشکار می‌سازد؟

۱) توازن فرد (odd parity) و یک بیت خطا
۲) توازن زوج (even parity) و یک بیت خطا
۳) توازن فرد و دو بیت خطا
۴) توازن زوج و دو بیت خطا

۶ ـ در تست ۴، اگر نرخ انتقال 4800 باشد و هر تیک برابر 0.104mS باشد، کاراکتر ارسالی و بیت Parity را مشخص کنید.

۱) 0000110 و بیت توازن 0
۲) 1011111 و بیت توازن 0
۳) 1111001 و بیت توازن 1
۴) 1111010 و بیت توازن 1

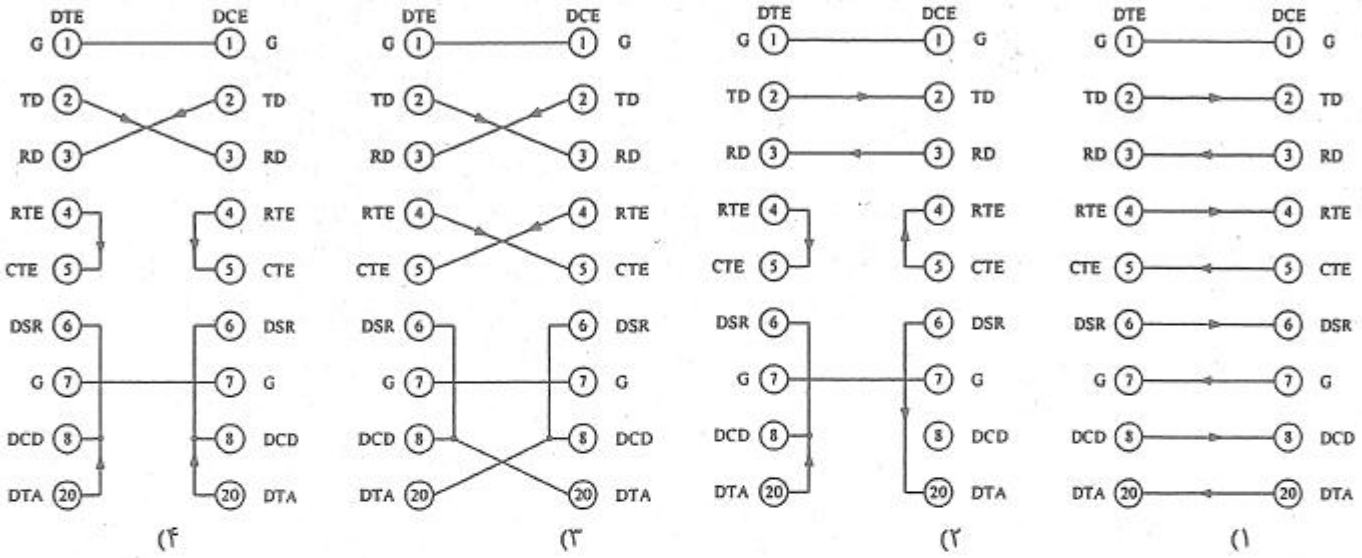
۷ ـ در تست ۲ اگر از روش انتقال سنکرون با طول فریم 1000 بیت استفاده شود و هر فریم یک کاراکتر شروع، یک کاراکتر پایان و 8 کاراکتر همزمانی داشته باشد (اضافه بر 1000 بیت اصلی داده)، زمان انتقال چقدر خواهد بود؟

۱) تقریباً 1.6 ثانیه ۲) 1.6 ثانیه ۳) 1.728 ثانیه ۴) تقریبا 2 ثانیه

۸ ـ اگر در انتقال غیرهمزمان، برای ارسال کاراکترهای 8 بیتی (شامل یک بیت توازن و 7 بیت داده) با یک بیت شروع و 2 بیت پایان استفاده شود، چند درصد نرخ انتقال (حداکثر) برای انتقال داده‌های اصلی صرف می‌شود؟

۱) %64 ۲) %67 ۳) %80 ۴) %85

۹ ـ کدام یک از اتصالات زیر برای Full Handshake در استاندارد RS-232 استفاده می‌شود.(سراسری ـ ۷۳)



۱) ۲) ۳) ۴)

۱۰ ـ در مقایسه با استاندارد RS-232 موارد زیر در مورد استانداردهای دیگری که بین DTE و DCE وجود دارند، می‌توان بیان کرد (سراسری ۷۲ و آزاد ۷۹)

۱) استاندارد X.21 دارای اتصالات کمتری نسبت به RS-232 است و هم برای انتقال سنکرون و هم آسنکرون به کار می‌رود، در حالی‌که RS-232 فقط برای انتقال آسنکرون مصرف می شود.

۲) RS-422 از روش نامتوازن (Unbalanced) استفاده می‌کند و مشخصه مسافت سرعت بهتری نسبت به RS-232 دارد.

۳) RS-423 از روش متوازن (Balanced) استفاده می‌کند و مشخصه مسافت سرعت بهتری نسبت به RS-232 دارد.

۴) RS-449 مشخصه مسافت سرعت بهتری نسبت به RS-232 داشته و این استاندارد باعث کنترل بیشتری روی مودم می‌شود.

۱۱ ـ یک منبع داده کاراکترهای ASCII هفت بیتی تولید و از طریق یک سیستم انتقال سنکرون با سرعت 300bps ارسال می‌کند. انتقال به صورت کاراکتری (Character – Oriented) بوده و هر قاب اطلاعات از 8 کاراکتر کنترل و 120 کاراکتر اطلاعات تشکیل شده است. چنانچه به همراه هر کاراکتر یک پریتی در سیستم انتقال به کاراکترها اضافه شود، Throughput (مقدار کاراکتر ارسالی در ثانیه) چقدر است؟(آزاد ۷۸)

۱) 30 کاراکتر در ثانیه ۲) 36 کاراکتر در ثانیه ۳) 24 کاراکتر در ثانیه ۴) 42 کاراکتر در ثانیه

۱۲ ـ برای انتقال غیر همزمان هر 8 بیت، یک بیت توازن و یک بیت شروع و 1.5 بیت پایان استفاده می‌شود. سرعت انتقال 2400bps است. یک پیام 1KB در چند ثانیه انتقال داده می‌شود؟

۱) 0.591 ثانیه ۲) 4.906 ثانیه ۳) 5.940 ثانیه ۴) 5.120 ثانیه

۱۳ ـ یک UART با نرخ 9600 بیت در ثانیه اطلاعات خود را ارسال می‌کند. اگر فرکانس ساعت ورودی به آن 153600 Hz باشد، حداکثر اعوجاج از مرکز بیت چقدر است؟

۱) %12.5 ۲) %6.25 ۳) %25 ۴) %5

۱۴ ـ در مورد انتقال داده‌ها به روش سنکرون، کدام یک از جملات زیر غلط است؟ (آزاد ـ ۷۸)

۱) برای همزمانی گیرنده و فرستنده می‌توان Clock فرستنده را توسط یک کانال مخابراتی به گیرنده منتقل کرد.

۲) در این روش انتقال داده‌ها، برای همزمانی کاراکترها بین فرستنده و گیرنده، نیاز به ارسال یک کاراکتر خاص به نام sync در ابتدای هر پیغام است

۳) این روش انتقال داده‌ها زمانی مناسب است که بین کاراکترها فاصله (Gap) نباشد و کاراکترها به صورت یک رشته پشت سر هم روی خط قرار گیرند.

۴) اگر از کدهایی که خاصیت همزمانی دارند (Self Clocking code) استفاده شود تا گیرنده و فرستنده همزمان شوند دیگر احتیاج به یک منبع Clock (مستقل از فرستنده) در گیرنده نمی‌باشد.

۱۵ ـ یک کامپیوتر و یک چاپگر توسط ارتباط RS-232 و مودم و خطوط تلفن به هم متصل شده‌اند. فرض کنید که در ضمن ارسال یک فایل کاغذ تمام شود. کامپیوتر چگونه عمل ارسال را تمام می‌کند؟ (آزاد ـ ۷۹)

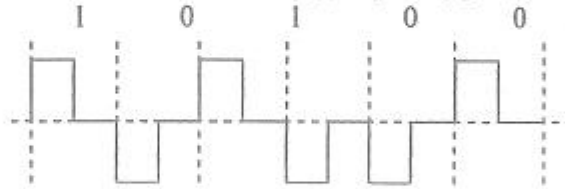
۱) نیاز به یک کانال رفت (کامپیوتر به چاپگر) و یک کانال برگشت (چاپگر به کامپیوتر) است که پهنای باند دو کانال برابر باشد.

۲) چاپگر نمی‌تواند کامپیوتر را متوقف کند، چون خط تلفنی این دو را به هم متصل می‌کند.

۳) برای این‌که چاپگر بتواند کامپیوتر را متوقف کند نیاز به دو خط تلفن می‌باشد.

۴) نیاز به یک کانال رفت و یک کانال برگشت می‌باشد که پهنای باند کانال برگشت بسیار کوچکتر است.

۱۶ ـ اطلاعات و سیگنال یک خط انتقال به شکل مقابل است:



از کدام روش جهت کد کردن این اطلاعات استفاده شده است؟ (سراسری ۷۲، آزاد ۷۹)

۱) RZ ۲) PCM ۳) NRZ ۴) Manchester

۱۷ ـ کدام یک از روش‌های زیر برای انتقال بیت (0 و 1) ما بین دو نقطه با اتصال فیزیکی به کار می‌رود؟ (آزاد ـ۷۹)

۱) پروتکل اینترنت (IP) ۲) کد منچستر

۳) پروتکل نقطه به نقطه (PPP) ۴) استاندارد X.25

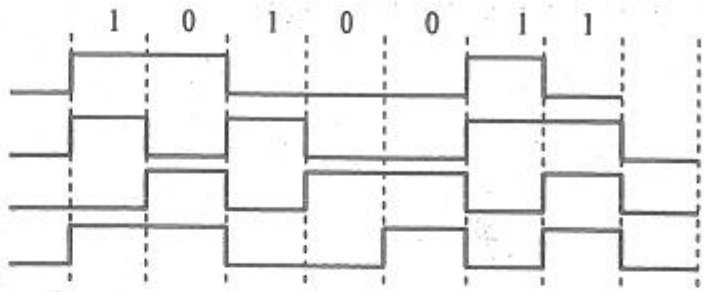
۱۸ ـ کدام یک از روش‌های کد گذاری زیر همزمانی را ایجاد نمی‌کند؟ (سراسری ـ ۸۱)

۱) HDB3 ۲) B8ZS ۳) Manchester ۴) NRZ-L

۱۹ ـ فرستنده‌ای اطلاعات دیجیتال را با نرخ 10Mbps ارسال می‌کند. به کمک یک دستگاه اسیلوسکپ موج خروجی را اندازه می‌گیریم و مشاهده می‌کنیم که یک موج مربعی پریودیک با فرکانس 5MHz است (مطابق شکل) با توجه به این‌که فرستنده از کدبندی منچستر تفاضلی استفاده می‌کند قطار بیت‌های ارسالی کدام یک از موارد زیر است؟

۱) ...00110011... ۲) ...01010101... ۳) ...00000000... ۴) ...11111111...

۲۰ ـ شکل سیگنال حاصل از انتقال بیت‌های اطلاعات زیر به روش NRZ-I چگونه خواهد بود؟



۲۱ ـ اگر طیف فرکانسی یک سیگنال دارای پهنای باند 3000Hz با بیشترین فرکانس 4000Hz باشد نرخ نمونه‌برداری نایکوییست چقدر است؟

۱) 3000 نمونه در ثانیه ۲) 6000 نمونه در ثانیه ۳) 4000 نمونه در ثانیه ۴) 8000 نمونه در ثانیه

۲۲ ـ درکدام روش کدبندی همواره مولفه DC (میانگین دامنه) مخالف صفر است؟

۱) Unipolar ۲) Polar ۳) Bipolar ۴) هر سه مورد

۲۳ ـ کدبندی RZ و Bipolar چند سطح دامنه سیگنال دارند؟

۱) 2 ۲) 3

۳) 4 ۴) (RZ ، 2 سطح) و (Bipolar، 3 سطح)

۲۴ ـ مشکل همزمانی در رشته‌های طولانی 0 در کدام روش حاصل شده است؟

۱) B8ZS ۲) AMI ۳) HDB3 ۴) 1 و 3

۲۵ ـ کدام یک از روش‌های کدبندی روش تفاضلی دارند؟

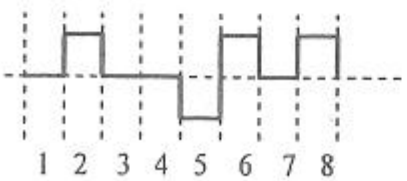
۱) Manchester ، RZ

۲) Manchester ، NRZ-I

۳) NRZ-L ، RZ

۴) AMI ، NRZ-I

۲۶ ـ اگر با روش کدبندی Bipolar AMI رشته زیر دریافت شود و فقط یک خطا رخ داده باشد، خطا در چه بیتی است؟



۱) 2 ۲) 8 یا 6 یا 7

۳) 8 ۴) 7

۲۷ ـ در روش HDB3 ، با فرض این‌که آخرین پلاریته قبل (-) باشد و رشته 01010000 بلافاصله بعد از آخرین جایگزینی Violation ارسال شود ، کدام گزینه برای ارسال این رشته صحیح است؟

۱) 0+0-+00+ ۲) 0+0--00- ۳) 0+0-000- ۴) 0-0+000+

۲۸ ـ اگر یک مودم اطلاعات دیجیتال را از خط تلفن با نرخ 19200bps انتقال دهد، کدام روش مدولاسیون زیر ممکن است به کار رفته باشد؟(آزاد ـ ۷۶)

۱) ASK ۲) FSK ۳) PSK ۴) QAM

۲۹ ـ پهنای باند یک سیگنال ASK برابر 10KHz است. Band Rate و Bit Rate به ترتیب برابر است:

۱) 5000 Band و 10000 bps

۲) 5000Band و 5000bps

۳) 10000Band و 5000bps

۴) 10000Band و 10000bps

۳۰ ـ یک خط نیمه دو طرفه (HDX) با پهنای باند 10KHz وجود دارد نرخ بیت سیگنال ASK ارسالی حداکثر چقدر است؟

۱) 5Kbps

۲) 10Kbps

۳) 15Kbps

۴) 20Kbps

۳۱ ـ یک خط تمام دو طرفه با فرکانس پائین 10KHz و فرکانس بالای 15KHz (پهنای باند 5KHz) وجود دارد. پهنای باند سیگنال ارسالی ASK (یا دریافتی) چقدر است؟ حداکثر نرخ بیت ارسالی چقدر است؟ (مدولاسیون ASK)

۱) 2.5KHz، 2.5Kbps ۲) 2.5KHz، 5000Kbps ۳) 5KHz ، 2.5Kbps ۴) 5KHz، 5Kbps

۳۲ ـ در تست ۳۱ فرکانس حامل (f_c) سیگنال ASK ارسالی و دریافتی چند است؟

۱) 11.25KHz، 13.75 KHz ۲) هر دو 12.5 KHz ۳) 10KHz، 15KHz ۴) 11KHz، 14KHz

۳۳ ـ یک سیگنال FSK با سرعت 4000bps در یک خط انتقال HDX ارسال می‌شود. اگر شیفت فرکانسی 5KHz باشد، پهنای باند لازم برای ارسال این سیگنال چقدر است؟ (شیفت فرکانسی = فاصله میان دو فرکانس حامل)

۱) 5KHz ۲) 7KHz ۳) 9KHz ۴) 13KHz

۳۴ ـ یک خط انتقال با پهنای باند 20KHz مفروض است در مدولاسیون FSK ، اگر مد انتقال FDX باشد، با فرض این‌که شیفت فرکانسی 6KHz است، حداکثر نرخ سیگنال ارسالی چند Band است؟ حداکثر نرخ بیت ارسالی چند است؟

۱) 4000Band، 8Kbps ۲) 4000Band، 4Kbps

۳) 14000Band، 7Kbps ۴) 14000Band، 14Kbps

۳۵ ـ یک سیگنال QPSK در مد انتقال HDX با سرعت 4Kbps ارسال می‌شود. حداقل پهنای باند کانال چقدر است؟

۱) 1000Hz ۲) 2000Hz ۳) 4000Hz ۴) 8000Hz

۳۶ ـ یک سیگنال 16-PSK، در مد انتقال FDX در یک کانال با پهنای باند 4000Hz ارسال می‌شود. حداکثر نرخ بیت ارسال چقدر است؟

۱) 2Kbps ۲) 4Kbps ۳) 8Kbps ۴) 16Kbps

۳۷ ـ یک سیگنال 16-PSK در مد انتقال HDX در یک کانال PSTN با پهنای باند 3 KHz ارسال می‌شود. حداکثر نرخ ارسال داده نایکوییست چقدر است؟ راندمان پهنای باند چقدر است؟

۱) 24Kbps ، $8\frac{bps}{Hz}$ ۲) 12Kbps ، $4\frac{bps}{Hz}$ ۳) 6Kbps ، $2\frac{bps}{Hz}$ ۴) هیچکدام

۳۸ ـ در روش نمودار کدبندی QAM، 16 نقطه بر روی دو دایره به زاویه‌های مساوی قرار گرفته‌اند. اگر نرخ ارسال 2000Band باشد حداکثر نرخ انتقال چقدر است؟

۱) 8000bps ۲) 2000bps ۳) 16000bps ۴) 4000bps

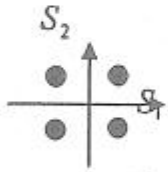
۳۹ ـ در روش QAM – 64، اگر band Rate برابر 10000 باشد، نرخ حداکثر انتقال بیت‌ها چقدر است؟

۱) 60Kbps ۲) 640Kbps ۳) 10Kbps ۴) 6.4Kbps

۴۰ ـ اگر نرخ باشد (Band Rate) در مدولاسیون 4-PSK برابر 800 باشد نرخ بیت چه اندازه است؟ (بر حسب بیت در ثانیه) (سراسری ـ ۸۱)

۱) 3200 ۲) 1600 ۳) 800 ۴) 200

۴۱ ـ یک کانال تلفن دارای پهنای باند قابل استفاده از 600 هرتزالی، 3400 هرتز است. فرکانس حامل 2000 هرتز است. فرکانس یک مودم QAM دارای دیاگرام سیگنالی زیر است. این مودم چه نرخ داده‌ای را می‌تواند ارسال نماید؟(آزاد ـ ۸۱)



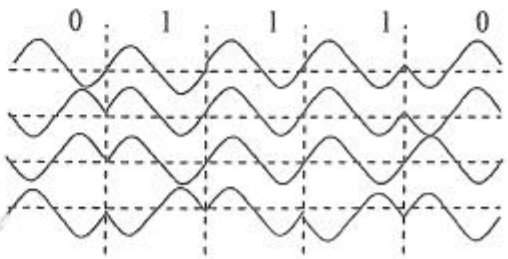
۱) بیشتر از 3000 بیت در ثانیه ولی کمتر از 5000 بیت در ثانیه

۲) بیشتر از 5000 بیت در ثانیه ولی کمتر از 7000 بیت در ثانیه

۳) کمتر از 3000 بیت درثانیه

۴) بیشتر از 7000 بیت در ثانیه

۴۲ ـ شکل سیگنال حاصل از مدولاسیون بیت‌های اطلاعات زیر به روش DPSK چگونه خواهد بود؟ (سراسری ـ ۷۲)

۱) 

۲)

۳)

۴)

۴۳ ـ در مدولاسیون QPSK، اگر SNR را 10dB فرض کنیم، نسبت $\frac{E_b}{N_0}$ تقریباً چقدر خواهد بود؟ (بر حسب dB)

۱) 7dB ۲) 13dB ۳) 10dB ۴) قابل محاسبه نیست و نیاز به داده‌های بیشتری دارد.

۴۴ ـ می‌خواهیم سیگنال زیر را در نرخ نایکوییست نمونه‌برداری کرده و به کمک 10 بیت PCM آن را ارسال کنیم، سرعت خط چقدر باید باشد؟ (سراسری ـ ۷۳)

$S(t) = 3Cos500t + 3Cos700t + 2Cos1000t$

۱) 20000bps ۲) 44000bps ۳) 3184bps ۴) 14012bps

۴۵ ـ تست فوق (۴۴) را برای سیگنال زیر حل کنید.

$S(t) = 12 + Cos^2 400\pi t + Sin20\pi t$

۱) 8Kbps ۲) 44000bps ۳) 4Kbps ۴) 88000bps

حل تشریحی تست‌های فصل سوم و چهارم

۱ـ گزینه ۲ صحیح می‌باشد.

حل :

$$500 * \frac{1}{1000} = 0.5_{Clock}$$

۲ـ گزینه ۲ صحیح می‌باشد

حل :

$$1000(8+2) = 10000bit \text{ و } \frac{10000bit}{5000bps} = 2sec$$

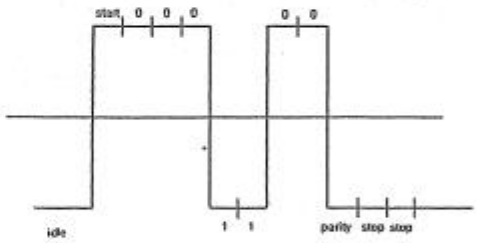
۳ـ گزینه ۱ صحیح می‌باشد

حل :

$$\frac{2000}{10000} \times 100\% = \%20$$

۴ـ گزینه ۱ صحیح می‌باشد

حل :



$\tau = \frac{1}{10000} = 0.1ms \Rightarrow$ هر تیک در شکل برابر عرض یک بیت است

۵ـ گزینه ۱ صحیح می‌باشد

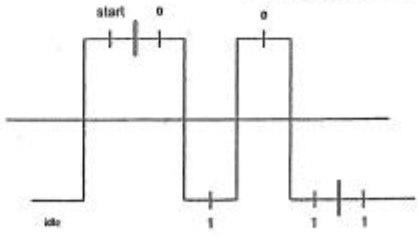
حل :

parity =1

(فرد است) 3= تعداد یک با احتساب بیت توازن

۶ـ گزینه ۴ صحیح می‌باشد

حل :



$\tau = \frac{1}{4800} = 0.204 = 2 \times 0.104 \Rightarrow$ در هر 2 تیک یک بیت ارسال می‌شود.

۷ـ گزینه ۳ صحیح می‌باشد.

حل :

$$1000\times 8 = 8000\text{bit} \quad و \quad \frac{8000\text{bit}}{1000} = 8\text{frame}\times(1+1+8) = 80\text{byte}$$

$$8000+640 = \frac{8640}{5000} = 1.728$$

۸ـ گزینه ۱ صحیح می‌باشد

حل :

$$\frac{7}{7+1+1+2} = \frac{7}{11} = 0.6363\times 100\% = \%63.7 = 64\%$$

۹ـ گزینه ۱ صحیح می‌باشد.

حل : دقت کنید مودم پوچ فقط برای اتصال مستقیم دو DTE استفاده می‌شود ولی در اینجا اتصال یک DTE به یک DCE خواسته شده است. لذا پین‌های همنام (و هم شماره) به هم متصل می‌شوند.

$PTE \rightarrow DCE$

هر دو DTE مودم برج شکل

۱۰ـ گزینه ۳ صحیح می‌باشد

حل :

گزینه اول نادرست است، زیرا استاندارد X.21 از روش سنکرون و استاندارد RS-232 از روش سنکرون و استاندارد RS-232 از روش سنکرون و آسنکرون استفاده می‌کند.

گزینه دوم نادرست است، زیرا استاندارد RS-422 از روش متوازن (Balanced) استفاده می‌کند.

گزینه چهارم نادرست است، مشخصه مسافت سرعت و RS-449 از RS-232 بهتر نمی‌باشد.

۱۱ـ گزینه ۲ صحیح می‌باشد

حل : جواب تقریبی بدست می‌آید:

$$1\,\text{frame} = 128\text{char} \Rightarrow \quad \frac{120}{128}\times 300 = 281.25\text{bps}$$

$$\frac{281.25\text{bps}}{8\text{bit}} = 35.17\,\text{char/sec}$$

۱۲ـ گزینه ۲ صحیح می‌باشد

حل :

$$(8+1+1+1.5) = 11.5\text{bit}$$

$$1\text{KB} = 1024\times 11.5\text{bit} = 11776\text{bit} \quad (\text{ارسالی}) \qquad \Rightarrow \quad \frac{11776}{2400} = 4.906_{\text{sec}}$$

۱۳ـ گزینه ۲ صحیح می‌باشد

حل :

حداکثر اعوجاج را به اندازه یک Clock در نظر بگیرید.

$\frac{153600}{9600} = 16\text{clock per bit}$

$\frac{1}{16} = \%6.25$ (حداکثر اعوجاج)

۱۴ـ گزینه ۲ صحیح می‌باشد

۱۵ـ گزینه ۴ صحیح می‌باشد

۱۶ـ گزینه ۱ صحیح می‌باشد

۱۷ـ گزینه ۲ صحیح می‌باشد

۱۸ـ گزینه ۴ صحیح می‌باشد

۱۹ـ گزینه ۴ صحیح می‌باشد

حل :

گزینه ۱ نادرست است، چون موج مربعی شکل نخواهیم.

گزینه ۲ نادرست است، چون موج مربعی شکل نخواهیم داشت.

گزینه ۳ نادرست است، چون اگر ...0000... باشد فرکانس 16MHz خواهد بود

گزینه ۴ صحیح است چون فرکانس 5MHz است.

۲۰ـ گزینه ۱ صحیح می‌باشد

حل :

فقط در گزینه ۱، در ابتدای بیت‌های یک، تغییر سطح سیگنال مشاهده می‌شود.

۲۱ـ گزینه ۴ صحیح می‌باشد

حل :

دقت کنید که f_{max} را در نظر می‌گیریم نه پهنای باند $\left(BW = f_{max} - f_{low}\right)$

$4000 * 2 = 8000$

۲۲ـ گزینه ۱ صحیح می‌باشد

۲۳ـ گزینه ۲ صحیح می‌باشد

۲۴ـ گزینه ۴ صحیح می‌باشد

۲۵ـ گزینه ۲ صحیح می‌باشد

۲۶ـ گزینه ۲ صحیح می‌باشد

۲۷ـ گزینه ۱ صحیح می‌باشد

حل :

از آخرین جایگزینی 2 تا یک داشتیم. لذا تعداد یک‌ها ا زآخرین جایگزینی زوج است.

۲۸ـ گزینه ۴ صحیح می‌باشد

حل :

گزینه‌های۱ تا ۳ نادست است، زیرا:

$ASK \rightarrow R = R_s = 19200 = 2f_0 = BW >> 4KHz$ (برای PSK هم همین‌طور است)

$FSK \rightarrow BW = 2f_0 + f_s\, 19200 + f_s >> 4KHz$

۲۹ـ گزینه ۴ صحیح می‌باشد

حل :

$B = 10\ KHz = R = R_s = 2f_0$

۳۰- گزینه ۲ صحیح می‌باشد.

حل : $R = R_s = BW = 10kbps$

۳۱ـ گزینه ۱ صحیح می‌باشد

حل :

$Full\ Duplex \rightarrow Channel\ \ BW = 5KHz/2 = 2.5KHz$

$R = R_S = BW = 2f_0 \rightarrow R = 2.5kbps$

۳۲ـ گزینه ۲ صحیح می‌باشد

حل : فاصله 10 تا 15 کیلو هرتز را به دو قسمت مساوی 2.5KHz تقسیم می‌کنیم و وسط هر فاصله را فرکانس حامل رفت و برگشت در نظر می‌گیریم، زیرا:

$f_0 = \frac{R}{2} = 1250\ Hz$

۳۳ـ گزینه ۳ صحیح می‌باشد

حل :

$BW = f_S + 2f_0 = f_S + R = 5KHz + 4KHz = 9KHz$

۳۴ـ گزینه ۲ صحیح می‌باشد

حل :

$\frac{20}{2} = 10KHz$ (پهنای باند کانال ارسال)

$10 = f_S + 2f_0 = 6 + 2f_0$

$2f_0 = R = 4KHz = R_S$

۳۵ـ گزینه ۲ صحیح می‌باشد.

$R = 4Kbps$ و $R = R_s \log_2^4 = 2R_s$

$R_s = 2000band$

$BW = R_s = 2000\ Hz$

نکته : اگر 16-PSK و 16-QAM بود، جواب 1000 بود.

۳۶ـ گزینه ۳صحیح می‌باشد.

(ارسال)

$BW = 4KHz$ و $BW \uparrow = \frac{4}{2} = 2KHz$ و $R_s = 2000band$

$R = R_S \log_2^{16} = 4R_s = 8Kbps$

۳۷ـ گزینه ۱صحیح می‌باشد.

حل :

$BW = f_0 = \frac{R_s}{2} \Rightarrow R_s = 2BW = 2 \times 3 = 6Kbps$ نایکوییست

$R = R_S \times \log_2^{16} = 6 \times 4 = 24Kbps \Rightarrow \quad B = \frac{R}{W} = \frac{24}{3} = 8$

۳۸ـ گزینه ۱صحیح می‌باشد.

حل :

$R_s = 2000\ band$ و $R = R_s \log_2^{16} = 4\ Rs = 8Kbps$

۳۹ـ گزینه ۱صحیح می‌باشد.

حل :

$R = R_s \times \log^{64}{}_2 = 6R_s = 60Kbps$

۴۰ـ گزینه ۲صحیح می‌باشد.

حل :

$R = R_S \log_2^4 = 800 \times 2 = 1600$

۴۱ـ گزینه ۲صحیح می‌باشد.

حل :

$BW = R_s = 2f_0 = 2800 \Rightarrow R_s = 2800\ band$

$R = 2800 \log_2^4 = 5600\ bps$

۴۲ـ گزینه ۴ صحیح می‌باشد.

۴۳ـ گزینه ۱صحیح می‌باشد.

$\frac{E_b}{N_0}(dB) = SNR + \log_{10}^{\frac{BW}{R}}$ و $R_s = BW \quad \Rightarrow R = 2R_s = 2BW$

$= 10 + 10 \log 0.5 = 10 - 3 = 7\ dB$

۴۴ـ گزینه ۳صحیح می‌باشد.

حل :

$$\omega_{max} = 1000 = 2\pi f_{max}$$

$$f_{max} = \frac{1000}{2\pi}$$

$$f_{sampling} = 2f_{max} = \frac{1000}{\pi} = 318.4$$ نمونه در ثانیه

از طرفی در 10 بیت PCM، در هر نمونه 10 بیت خواهیم داشت، لذا:

$$R = 318.4 \times 10 = 3184\,bps$$

۴۵ـ گزینه ۱صحیح می‌باشد.

حل :

$$\cos^2\alpha = \frac{1+\cos 2\alpha}{2}$$

$$\omega_{max} = \cos 2 \times 400\pi t$$

$$\omega_{max} = 2\pi f_{max}$$

$$\Rightarrow f_{max} = 400$$

$$f_{sampling} = 2f_{max} = 2 \times 400 = 800$$ نمونه در ثانیه

$$R = 800\frac{sample}{Sec} \times 10\frac{bit}{sample} = 8\,Kbps$$

فصل پنجم

کنترل خطا

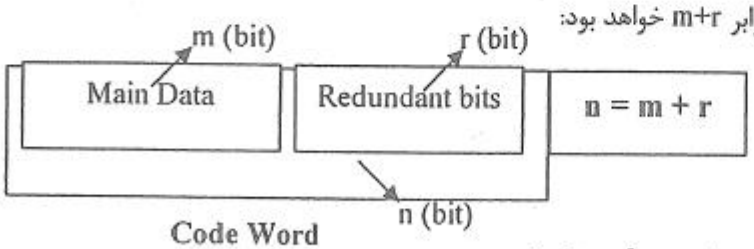
خطا در انتقال داده به مفهوم تشخیص نادرست بیت ارسالی در گیرنده است (برای مثال بیت صفر ارسال شده را در گیرنده یک تشخیص دهیم). در فصل گذشته عوامل ایجادکننده خطا مورد بحث و تحلیل قرار گرفت.

منظور از کنترل خطا، امور مربوط به شناسایی یا تشخیص خطا (کشف وجود خطا (Error Detection)) و تصحیح آن (کشف موقعیت بیت خطا (Error Correction)) می‌باشد.

به طور کلی دو روش برای کنترل خطا وجود دارد:

- پیش‌رو (Forward Error Correction :FEC) : در این روش داده‌های افزونه به همراه اطلاعات اصلی به گیرنده ارسال می‌شود. این افزونگی (Redundancy) برای تشخیص و تصحیح خطا در گیرنده به کار می‌رود.
- پس رو (Feedback (Backward) Error Correction) : در این روش افزونگی فقط می‌تواند به گیرنده در تشخیص وجود خطا کمک کند و اطلاعات دارای خطا باید دوباره ارسال شود.

فرض کنید یک داده (فریم یا کاراکتر) را باید ارسال نمائیم. اگر طول ناحیه داده اصلی برابر m بیت و اطلاعات افزونه (برای تشخیص و/یا تصحیح خطا) برابر r بیت باشد، طول کل فریم (کد) برابر m+r خواهد بود:



۵ـ۱ Hamming Distance

فاصله همینگ (D) بین دو کد C_1 و C_2 برابر تعداد بیت‌های متفاوت در آن دو کد است.

مثال : اگر C_1=1 0 0 1 0 0 و C_2= 1 0 1 0 1 0 باشد، فاصله همینگ C_1 و C_2 عبارت است از:

$$D(C_1, C_2) = 3$$

وزن (Weight) یک کد برابر تعداد یک‌های آن کد است:

$$W(C_1) = 2 \quad , \quad W(C_2) = 3$$

نکته ۱: فاصله همینگ مجموعه‌ای از کدها، برابر حداقل فاصله همینگ بین اعضا مجموعه می‌باشد.

مثال : برای مجموعه کدهای {1100 , 0001 , 0011}، فاصله همینگ را محاسبه کنید.

$C_2 = 0001$

$C_3 = 1100$

$D(C_1, C_2) = 1$

$D(C_1, C_3) = 4$

$D(C_2, C_3) = 3$

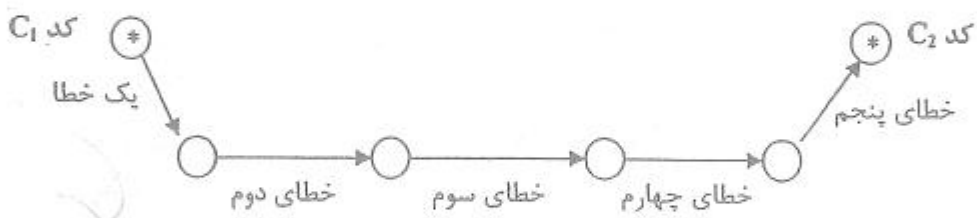
$D = \text{Min}\{1,3,4\} = 1$

نکته ۲: فاصله همینگ دو کد برابر وزن XOR آن دو کد است:

$$D(C_1, C_2) = W(C_1 \oplus C_2)$$

نکته ۳: اگر فاصله همینگ در یک مجموعه کد، برابر 5 باشد. چند بیت قابل تشخیص است؟

فرض کنید حداقل فاصله همینگ مربوط به دو کد C_1 و C_2 از این مجموعه باشد. بنابراین همانطور که در شکل ۴۴ دیده می‌شود، ممکن است با رخداد پنج خطا، کد C_1 به کد C_2 که هر دو مجاز هستند تبدیل شود و تشخیص غیر ممکن شود.



شکل ۴۴. اگر به اندازه فاصله همینگ (D) خطا رخ دهد از کد مجاز C_1 به کد مجاز C_2 می‌رسیم و خطا غیرقابل تشخیص است.

حداکثر تعداد خطاهای قابل تشخیص (d) در یک مجموعه کد با فاصله همینگ D از رابطه زیر بدست می‌آید:

$$\boxed{d = D - 1}$$

نکته ۴: در مثال فوق چند خطا قابل تصحیح است؟

اگر یک یا دو خطا رخ دهد، کد غیر مجازی بوجود می‌آید که به کد مجاز اولیه از سایر کدهای مجاز نزدیکتر (D_{min}) است و علاوه بر تشخیص خطا، تصحیح نیز صورت می‌گیرد و کد اولیه به عنوان کد صحیح انتخاب می‌شود. اما اگر سه خطا رخ دهد، فاصله همینگ کد حاصل با یک کد مجاز دیگر، کمتر از فاصله همینگ آن با کد صحیح اولیه است و لذا منجر به اشتباه در تصحیح خواهد شد. رابطه زیر، حداکثر تعداد خطاهای قابل تصحیح (c) در یک مجموعه کد با فاصله همینگ D را مشخص می‌کند:

$$\boxed{c = \left[\frac{D-1}{2}\right]}$$

مثال : اگر فاصله همینگ یک مجموعه کد برابر 4 باشد:

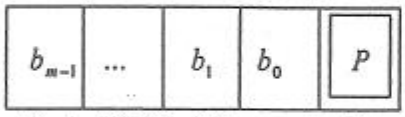
- تا سه خطا قابل تشخیص است: $d = D - 1 = 4 - 1 = 3$
- فقط یک خطا قابل تصحیح است: $c = \left[\frac{D-1}{2}\right] = \left[\frac{4-1}{2}\right] = 1$
- دو بیت خطا قابل تشخیص است، اما چون فاصله همینگ از دو طرف برابر است عمل تصحیح غیرممکن خواهد بود.

- سه خطا منجر به تصحیح نادرست می‌شود.

۵_۲ Parity Bit (بیت توازن)

روش بیت توازن یکی از پرکاربردترین روش‌های تشخیص خطا است که خصوصیات آن به شرح زیر است:

- یک بیت به داده‌ها اضافه می‌کند و افزونگی آن برابر یک است (r=1).
- تعداد کل یک‌های کد باید فرد (Odd parity) یا زوج (Even parity) باشد.
- فاصله همینگ: D=2
- امکان تشخیص خطا برای یک خطا (و خطاهای فرد: 3 خطا، 5 خطا، ...) وجود دارد.
  $d = D - 1 = 1$
- امکان تصحیح خطا وجود ندارد.
- اگر بیت‌های داده را b_0 ، b_1 ، ... و b_{m-1} بنامیم:



$P = b_0 \oplus b_1 \oplus ... \oplus b_{m-1}$ → Even parity → Odd parity

- اگر فریم به گیرنده نرسد ⇐ Ack ارسال نمی‌شود ⇐ Time Out (در فرستنده) ⇐ ارسال مجدد
- اگر فریم به طور صحیح به گیرنده برسد ⇐ Ack ارسال می‌شود
- اگر فریم با خطا به گیرنده برسد ⇐ Nack ارسال می‌شود ⇐ ارسال مجدد

۵_۳ Block Sum Check

برای افزایش قدرت تشخیص خطا، علاوه بر بیت‌های توازن (مثلاً فرد در مثال زیر) که به ازاء هر کاراکتر یک بیت توازن عرضی (سطری) [Transverse (Row) Parity Bits] ارسال می‌شود، یک مجموعه بیت توازن اضافی برای کل کاراکترهای فریم نیز ارسال می‌گردد. در شکل ۴۵ از بیت‌های توازن طولی (ستونی) [Longitudinal (Column) Parity Bits] زوج استفاده شده است

	P_R	b_6	b_5	b_4	b_3	b_2	b_1	b_0
	0	1	0	1	0	0	1	0
	1	0	(1)	0	0	(1)	0	0
	1	0	1	1	0	0	1	1
	0	1	(0)	0	1	(0)	0	1
	0	0	1	1	0	1	1	1
	0	0	1	1	1	0	1	1

بیت های توازن (فرد) عرضی(سطری)

بیت های توازن (زوج) طولی(ستونی) یاBCC نیز می‌گویند.

شکل ۴۵ .روش LRC (بیت‌های مشخص شده با دایره نشاندهنده خطاهای غیر قابل تشخیص می‌باشند.)

نکته ۱: از آن‌جا که بیت‌های توازن طولی (ستونی) مانند جمع modul-2 (مدول ۲) کل بیت‌ها عمل می‌کنند، به این مجموعه

بیت‌های توازن، BCC (Block (Sum) Check Character) گفته می‌شود.

نکته ۲: بیت‌های توازن عرضی (سطری) VRC (Vertical Redundancy Check) نیز نامیده می‌شود.

نکته ۳: اگر از BCC به همراه VRC استفاده شود (مانند شکل۴۵)، روش LRC (Longitudinal Redundancy Check) نامیده می‌شود.

نکته ۴: BCC می‌تواند انواع دیگری به غیر از جمع Modul-2 (توازن زوج) داشته باشد، برای مثال می‌توان از جمع 1's Complement استفاده کرد.

نکته۵: اگر از LRC استفاده شود، باز هم بعضی از خطاها قابل تشخیص نیست. به عنوان مثال به بیت‌هایی که در شکل ۴۵ با دایره مشخص شده‌اند دقت نمایید.

۴ـ۵ Hamming Code

کد همینگ برای تشخیص و تصحیح خطا به کار می‌رود. فرض کنید می‌خواهیم کدی با m بیت داده اصلی و r بیت افزونگی طرح کنیم که بتواند تمام خطاهای تک‌بیتی را تصحیح کند. حداقل r چقدر است؟

- هر کلمه کد دارای n بیت است (n=m+r).
- برای این منظور که بتوان یک خطا در هر کلمه را تشخیص و مکان وقوع خطا را تعیین کرد، لازم است تا هر پیام مجاز، n کد غیر مجاز (با فاصله 1) داشته باشد که هر یک از این کدها از یک بیت خطا در کد مجاز بوجود می‌آید.
- تعداد پیام‌های مجاز: 2^m
- هر پیام مجاز به n+1 کد (n کد غیر مجاز و یک کد مجاز) نیاز دارد.

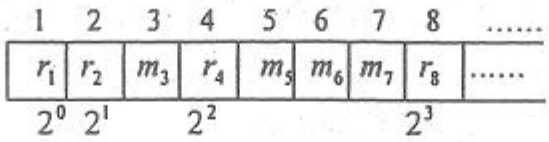
$\Rightarrow$ حداقل تعداد کل کدهای لازم $= 2^m(n+1)$

این کدها نباید همپوشانی داشته باشند تا قابل تشخیص و نیز قابل تصحیح باشند. از طرفی کدها n بیتی هستند و بنابراین کل ترکیبات ممکنه 2^n کلمه کد است. بنابراین می‌توان نوشت:

$$\begin{cases}(n+1)2^m \le 2^n \\ n = m+r\end{cases} \Rightarrow \boxed{m+r+1 \le 2^r}$$

نکته : این قانون به کد همینگ ربطی ندارد و در مورد همه کدهای تصحیح خطا صادق است.

همینگ در سال 1950 یک روش با حداقل افزونگی مشخص شده در رابطه فوق معرفی کرد که به Hamming Code معروف است. همانطور که در شکل ۴۶ دیده می‌شود، در این روش اگر بیت‌های کد را از چپ به راست شماره‌گذاری کنید، بیت‌هایی که توان‌هایی از 2 هستند (بیت‌های 1، 2، 4، 8 و ...) بیت‌های افزونه چک کننده هستند (r بیت) و بیت‌های دیگر (3، 5، 6، 7، 9 و...) بیت‌های داده اصلی می‌باشند (m بیت). هر بیت چک کننده، توازن مجموعه‌ای از بیت‌ها (از جمله خودش) را زوج (یا فرد) می‌کند. توجه نمایید که هر بیت می‌تواند در بیش از یک مجموعه توازن دخالت کند. در این‌جا این سوال مطرح می‌شود که کدام بیت‌های چک‌کننده در محاسبه توازن بیت داده موقعیت k (m_k) دخالت دارند؟ برای تعیین این بیت‌ها، k را به صورت مجموع توان‌های 2 بنویسید. بیت‌های افزونه با اندیس‌های بدست آمده در محاسبه توازن بیت داده m_k به کار می‌روند.



شکل ۴۶. شماره‌گذاری بیت‌های داده اصلی (m_i) و بیت‌های افزونه (r_j) در کد همینگ

مثال : برای k=13، ابتدا 13 را به صورت 13=8+4+1 در نظر می‌گیریم. بنابراین بیت‌های چک کننده r_1، r_4 و r_8 در محاسبه توازن بیت داده m_{13} دخالت دارند.

برای تشخیص و تصحیح خطاهای تک بیتی در گیرنده کلیه بیت‌های چک کننده را به طور جداگانه از نظر توازن چک می‌نمایند. مثلا اگر بیت‌های توازن 1، 4 و 8 از نظر توازن مشکل داشته باشد، خطا در بیت موقعیت 13 (8+4+1) رخ داده است.

همان‌طور که دیدیم کد همینگ برای تصحیح خطاهای تک بیتی به کار می‌رود. در این‌جا یک روش برای تصحیح خطاهای فورانی (Burst) ارائه می‌شود. در این روش اگر حداکثر k بیت پشت سر هم خراب شوند تصحیح آن‌ها امکان‌پذیر خواهد بود. برای رسیدن به این هدف، k کلمه کد m بیتی، زیر هم نوشته شده و با r بیت افزونگی (کد همینگ)، هر کد به صورت m+r بیتی ایجاد می‌شود. حال به جای ارسال سطر به سطر، داده‌ها به صورت ستون به ستون ارسال می‌شوند. در این صورت اگر حداکثر k خطای پشت سر هم رخ دهد، قابل تشخیص و تصحیح خواهد بود، زیرا حداکثر یک بیت در هر کلمه کد تغییر می‌کند. در واقع در این روش k*m بیت داده اصلی با k*r بیت افزونگی همینگ محافظت شده است.

توجه: اگر کد همینگ بخواهد قابلیت شناسایی و تصحیح t بیت خطا را داشته باشد، باید:

$$2^r \geq 1+\binom{n}{1}+\binom{n}{2}+\ldots+\binom{n}{t}$$

Cyclic Redundancy Check : CRC ۵ـ۵

بر خلاف کلیه روش‌های قبلی که به گونه‌ای از بیت توازن استفاده می‌کردند، اساس این روش متفاوت بوده و بر قوانین زیر استوار است:

- در آن از تقسیم مبنای 2 استفاده می‌شود.
- در تقسیم مبنای 2، جمع و تفریق‌ها به صورت Modul-2 انجام می‌شود (شبیه XOR عمل می‌کند).
- نام دیگر این کد Polynomial Code (کد چند جمله‌ای) است، زیرا در این روش فرض می‌شود که هر عدد مبنای دو متناظر با یک چند جمله‌ای است. برای مثال، چند جمله‌ای معادل 10101، x^4+x^2+1 می‌باشد. کم ارزش‌ترین بیت (LSB) را ضریب x^0 فرض کنید.
- فرستنده و گیرنده بر سر یک چند جمله‌ای مولد (Generator Polynomial) به نام G(x) توافق می‌کنند.
- با ارزش‌ترین (چپ‌ترین) و کم ارزش‌ترین (راست‌ترین) بیت‌های عدد دودویی متناظر با G(x) باید یک باشد.

۱ـ۵ـ۵ رویه تولید کلمه کد ارسالی در CRC

۱ـ ابتدا r بیت صفر به سمت راست داده اصلی اضافه کنید. (r یکی کمتر از تعداد بیت‌های G(x) است)

۲ـ داده جدید را بر G(x) تقسیم دودویی نمایید (با خصوصیت تفریق Modul-2)

۳ـ باقیمانده تقسیم همان CRC یا باقیمانده CRC نام دارد.

۴ـ CRC بدست آمده را به صورت (r بیتی) به سمت راست داده اصلی (m بیتی) اضافه و آن را ارسال کنید.

مثال ، فریم داده 1101011011 (که چند جمله‌ای متناظربا آن M(x) نامیده می‌شود) را با مولد $G(x)=x^4+x+1$ در نظر بگیرید. فریم ارسالی حاوی افزونگی CRC چه خواهد بود؟

ابتدا چهار بیت صفر ($r=4$) به سمت راست داده اصلی اضافه کرده و آن را بر عدد دودویی متناظر با G(x) (10011) تقسیم Modulo-2 می‌نمائیم:

$$\Rightarrow \begin{array}{l|l} 11010110110000 & 10011 \\ \hline 10011 & 1100001010 \\ \hline 010011 \\ \quad 10011 \\ \hline 0000010110 \\ \quad\quad 10011 \\ \hline 0010100 \\ \quad\quad 10011 \\ \hline 001110 \end{array}$$

تفریق Modul-2 مانند XOR

$\Rightarrow$ باقیمانده r بیتی $= 1110 \Rightarrow R(x)=x^3+x^2+x \Rightarrow$

1101011011	1110
M(x)	R(x)

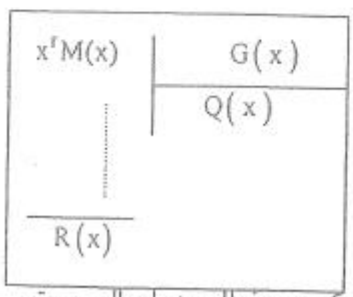
کد ارسالی=

نکته ۱: اگر در گیرنده کد ارسالی را بر G(x) تقسیم نمائیم باید باقیمانده تقسیم، صفر شود در غیر این صورت خطا داشته‌ایم.

نکته ۲: تقسیم فوق را می‌توان به صورت چند جمله‌ای نیز انجام داد. محاسبات زیر این مطلب را نشان می‌دهد:

$$\begin{array}{l|l} x^{13}+x^{12}+x^{10}+x^8+x^7+x^5+x^4 & x^4+x+1 \\ \hline x^{13}+x^{10}+x^9 & x^9+x^8+x^3+x \\ \hline x^{12}+x^9+x^8+x^7+x^5+x^4 \\ x^{12}+x^9+x^8 \\ \hline x^7+x^5+x^4 \\ x^7+x^4+x^3 \\ \hline x^5+x^3 \\ x^5+x^2+x \\ \hline x^3+x^2+x=R(x) \end{array}$$

بنابراین باز هم به همان R(x) یا همان CRC می‌رسیم.



$\Rightarrow$

M(x)	R(x)

کد ارسالی =

نکته ۳: کد ارسالی از تفریق Modul-2 یا XOR باقیمانده R(x) با $x^rM(x)$ بدست می‌آید

نکته ۴: اگر در گیرنده، کد دریافتی را بر G(x) تقسیم کنیم و باقیمانده صفر شود به معنای آن است که هیچ خطایی در ارسال صورت نگرفته است. اما اگر باقیمانده مخالف صفر شود، به معنای وجود خطا در کد دریافتی است.

نکته ۵: فرض کنید فریم ارسالی معادل چند جمله $T(x)$ باشد:

$T(x)=$ | $M(x)$ | $R(x)$ |

اگر در کانال خطایی به $T(x)$ اضافه شود، در گیرنده چه خواهیم داشت؟

$$T'(x)=T(x)+E(x)$$

اگر در گیرنده آن را تست کنیم، $\frac{T'(x)}{G(x)}$ یا $\frac{T(x)}{G(x)}+\frac{E(x)}{G(x)}$ را خواهیم داشت.

باقیمانده 0

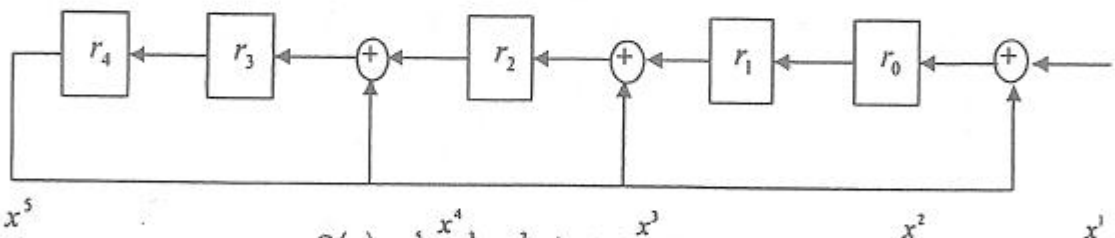
نکته ۶: فقط در صورتی خطا در گیرنده غیر قابل تشخیص خواهد بود که $E(x)$ بر $G(x)$ بخش‌پذیر باشد و در نتیجه $\frac{E(x)}{G(x)}$ باقیمانده صفر داشته باشد. (مثلاً $E(x)=G(x)$ باشد، یعنی همان بیت‌های متناظر با یک‌های $G(x)$ دچار خطا شده باشد.)

۵ـ۵ـ۲ پیاده‌سازی CRC با Shift Register

می‌توان مدار مولد کد CRC را مانند مثال زیر با Shift Register پیاده‌سازی کرد.

مثال: اگر $G(x)=x^5+x^3+x^2+1$ باشد، مولد کد CRC آن به صورت زیر بدست می‌آید:

- باقیمانده تقسیم بر $G(x)$ فوق، حداکثر 5 جمله دارد: $(r=5)$.
- شیفت رجیستر را 5 بیتی در نظر بگیرید.
- به ازای هر جمله $G(x)$ (به ازای هر یک در عدد دودویی متناظر با $G(x)$ یک XOR قبل از بیت متناظر با آن به کار ببرید (به غیر از جمله آخر؛ مانند x^5 در این مثال به شکل ۴۷ نگاه کنید.



شکل ۴۷. مولد کد CRC برای $G(x)=x^5+x^4+x^3+x^2+1$

- در ابتدا در رجیستر 0 قرار دارد. ورودی یا $M(x)$ از چپ به راست از ورودی وارد می‌شود. در انتها، $R(x)$ در رجیستر خواهد بود.

۵ـ۵ـ۳ خطاهای قابل شناسایی در روش CRC

فرض کنید خطای $E(x)$ به کد ارسالی اضافه شده است:

$$T'(x)=T(x)+E(x)$$

حال باید ببینیم که آیا $E(x)$ بر $G(x)$ بخش‌پذیر هست یا خیر؟ اگر بخش‌پذیر باشد خطا قابل تشخیص نمی‌باشد.

نکته ۱: کلیه خطاهای تک‌بیتی قابل شناسایی است:

در خطای تک بیتی، $E(x)=x^i$ (i شماره بیت (موقعیت) خطا است). بنابراین واضح است که چون در $G(x)$ جمله x^0 وجود دارد،

x^i بر G(x) بخش‌پذیر نمی‌باشد. لذا E(x) باید حداقل دو جمله داشته باشد تا قابل شناسایی نباشد.

نکته ۲: اگر G(x) بر x+1 بخش‌پذیر باشد، تمام خطاهای فرد (1 خطا، 3 خطا، 5 خطا دارد و ...) قابل شناسایی است.

می‌توان ثابت کرد که هیچ چند جمله‌ای با تعداد جملات فرد در Modul-2 بر x+1 بخش‌پذیر نیست و بنابراین اگر تعداد خطاها فرد باشد، E(x) یک چند جمله‌ای با تعداد جملات فرد است و بر x+1 بخش‌پذیر نیست.

اثبات (برهان خلف):

فرض کنید E(x) یک چند جمله‌ای با تعداد جملات فرد است که بر x+1 بخش‌پذیر است. می‌توان نوشت:

$$E(x)=(x+1)Q(x)$$
$$E(1)=\underbrace{(1+1)Q(1)}$$

$E(1)$: فرد — $(1+1)Q(1)$: زوج

در این صورت، طرف راست تساوی زوج و طرف چپ آن فرد است که یک تناقض آشکار است.

به همین ترتیب می‌توان نکات ذیل را اثبات کرد:

نکته ۳: اگر G(x) حداقل دارای سه جمله باشد، تمامی خطاهای 2 بیتی قابل تشخیص است.

نکته ۴: اگر باقیمانده r بیتی فرض شود، تمامی خطاهای فورانی با طول کوچکتر یا مساوی r قابل تشخیص است.

نکته ۵: اکثر خطاهای فورانی با طول بزرگتر از r نیز قابل تشخیص است.

نکته ۶: احتمال عدم تشخیص خطاهای فورانی به طول r+1 برابر $\frac{1}{2^{r-1}}$ است (طرح بیت خطا خود G(x) باشد).

نکته ۷: احتمال عدم تشخیص خطاهای فورانی به طول بیش‌تر از r+1 برابر $\frac{1}{2^r}$ است.

در هر صورت خطاهایی که طرح بیت آن‌ها دارای عامل G(x) باشد، غیرقابل شناسایی می‌باشند. برای مثال در نکته ۶، با توجه به این‌که می‌دانیم بیت اول و آخر یک است باید r-1 بیت وسط در E(x) معادل G(x) باشد.

۶ـ۵ روش‌های کنترل خطا

حال فرض کنید یک خطا رخ داده است، به طور کلی دو روش برای کنترل خطا و برطرف کردن مشکل وجود دارد:

- **Manual Error Control (کنترل دستی خطا):** مثلاً کاراکتر ارسالی از طرف صفحه کلید را کامپیوتر دریافت می‌کند و عیناً در مانیتور Echo می‌کند. حال اگر خطایی رخ داده باشد خود کاربر، آن را حذف کرده (Back Space) و کاراکتر را مجدداً تایپ می‌کند.
- **Automatic Repeat Request (ARQ):** خود سیستم خطا را تشخیص می‌دهد و درخواست ارسال مجدد می‌کند. دو روش برای این کار وجود دارد:
  - **Idle RQ (نوع ارتباط Half Duplex است):** در این روش فرستنده صبر می‌کند تا مطمئن شود frame یا کاراکتر قبلی رسیده است (به طور صحیح)یا خیر و نهایتاً یا داده بعدی را می‌فرستد و یا قبلی را دوباره ارسال می‌کند. دو راه برای پیاده‌سازی آن وجود دارد. یکی این‌که در صورت تشخیص خطا در گیرنده، به فرستنده Ack نمی‌دهیم تا Time out نماید (تایمر فرستنده به انتها برسد و مهلت در نظر گرفته شده منقضی شود) و داده‌ها را مجدداً ارسال نماید. دوم این‌که در صورت تشخیص خطا به وسیله ارسال Nack (تصدیق منفی یا Negative Acknowledgement) از فرستنده می‌خواهیم تا مجدداً داده را ارسال نماید. این

روش از کارایی و درجه توازی بسیار پائینی برخوردار است. روش زیر، کارایی را افزایش می‌دهد.

- **Continuous RQ (نوع ارتباط Full Duplex است)**: در این روش، k فریم بدون انتظار برای Ack، پشت سر هم ارسال می‌شود. فریم‌های ارسالی شماره ترتیب دارند. به موازات ارسال، Ackها با شماره ترتیب بر می‌گردند.دو روش برای پیاده‌سازی Continuous RQ وجود دارد:

- **بازگشت به N (Go-back-N)**: در این روش اگر گیرنده یک فریم خارج از ترتیب دریافت کند، یک Nack با شماره فریم دریافت نشده می‌فرستد (یا اینکه Ack نمی‌فرستد تا تایمر فرستنده به انتها برسد). با این تفاوت که بر خلاف روش Selective Reject فریم‌های بعدی را نمی‌گیرد و منتظر می‌شود تا فریم دارای خطا مجدداً ارسال شود. در این صورت مجدداً شروع به دریافت فریم‌ها با ترتیب درست می‌کند و برای هر کدام Ack شماره‌دار می‌فرستد. به عبارت دیگر، در این روش، لایه پیوند داده در گیرنده هیچ فریمی غیر از آن فریمی که باید به لایه شبکه تحویل دهد را قبول نمی‌کند. این رهیافت در کانال‌های دارای نرخ خطای بالا (مانند بی‌سیم) باعث اتلاف شدید پهنای باند می‌شود. این مشکل در رهیافت تکرار انتخابی حل می‌شود.
- **تکرار انتخابی (Selective Repeat) یا رد انتخابی (Selective Reject)** : در این روش، فریم خراب در گیرنده دور انداخته می‌شود؛ اما فریم‌های سالم بعدی بافر می‌شوند و Ack آن‌ها ارسال می‌شود. دو راه برای پیاده‌سازی آن وجود دارد:

- در روش اول گیرنده برای فریم‌هایی که به طور صحیح دریافت شده Ack شماره‌دار می‌فرستد و فرستنده از روی شماره ترتیب Ackها فریم دارای خطا را پیدا می‌کند (چون Ack آن دریافت نمی‌شود و تایمر فریم معیوب منقضی می‌شود) و فقط آن را مجدداً ارسال می‌کند. اگر این فریم سالم رسید، لایه پیوند داده آن را و سپس فریم‌های بافر شده بعدی را به ترتیب به لایه شبکه تحویل می‌دهد.
- در روش دوم، گیرنده یک Nack مخصوص شماره‌دار برای فریم دارای خطا می‌فرستد این رهیافت از روش قبلی کارایی بیشتری دارد، زیرا در فرستنده زمان برای انقضای تایمر تلف نمی‌شود.

Sequence Number ۵ـ۷

حتماً تا به حال این موضوع مهم پی برده‌اید که باید برای هر فریم شماره ترتیب (شماره شناسایی) در نظر گرفته شود، در این صورت مثلاً اگر در روش Idle RQ ، Ackگم شود (loss) و تایمر فرستنده به انتها برسد کند و frame دریافت شده قبلی را مجدداً ارسال کند، گیرنده از روی شماره ترتیب متوجه می‌شود که فریم تکراری است و آن را دور می‌اندازد. البته لازم نیست شماره ترتیب همواره اضافه شود و به‌طور نامحدود بزرگ شود. به عنوان مثال در IdleRQ، فقط کافی است که شماره‌ها یکی در میان 0 و 1 باشند.

فصل ششم

کنترل جریان

اگر به هر دلیل سرعت فرستنده و گیرنده یکسان نباشد و گیرنده کندتر باشد، بافر گیرنده پر می‌شود و فریم‌های بعدی را نمی‌توان دریافت کرد. (دور ریخته می‌شوند!) یکی از مهم‌ترین وظائف لایه ۲ (پیوند داده) برطرف کردن این مشکل با مکانیزم‌های کنترل جریان (Flow Control) بین فرستنده و گیرنده است.

به طور کلی کنترل جریان به دو صورت انجام می‌شود:

- سخت‌افزاری
- نرم‌افزاری

۱ـ۶ کنترل سخت‌افزاری جریان

در این روش یک خط جداگانه و سیگنال‌های سخت‌افزاری برای کنترل جریان مورد استفاده قرار می‌گیرد. برای مثال، سیگنال‌های سخت‌افزاری RTS (Request to Send) و CTS (Clear to Send) در استاندارد RS-232 به همین منظور مورد استفاده قرار می‌گیرند. اگر فرستنده بخواهد شروع به ارسال نماید درخواست خود را با سیگنال RTS به گیرنده اعلام می‌نماید (RTS را Set می‌کند). حال اگر گیرنده آماده باشد CTS را فعال می‌کند و اگر آماده نباشد (مثلا بافر پر باشد) آن‌را Reset می‌کند. خصوصیات این روش به شرح ذیل است:

- مزیت : سرعت بالا
- عیب: فقط مناسب ارتباطات نزدیک است؛ زیرا چند خط اضافی برای سیگنال‌های کنترلی استفاده می‌شود.

۲ـ۶ کنترل نرم‌افزاری جریان

روش‌های کلاسیک مختلفی برای کنترل جریان به صورت نرم‌افزاری وجود دارد. مهم‌ترین روش‌های کنترل نرم‌افزاری جریان به شرح زیر است:

- روش X-ON / X-OFF
- روش Stop & Wait (توقف و انتظار)
- روش Sliding Window (پنجره لغزنده یا پنجره لغزان)

۱ـ۲ـ۶ روش X-ON / X-OFF

در این روش، هر گاه گیرنده نتواند داده‌های بعدی را دریافت نماید، (مثلاً محتوای بافر به یک حد آستانه رسیده باشد) یک فریم یا کاراکتر (سیگنال) X-OFF به فرستنده می‌فرستد تا ارسال را متوقف نماید. این روش در ترمینال‌ها برای ارسال کلیدهای ارسالی از صفحه کلید به کامپیوتر مرکزی مورد استفاده قرار می‌گیرد. هر گاه گیرنده مجدداً آماده دریافت داده‌های [کاراکترهای / فریم‌های] بعدی بشود، با ارسال X- ON به فرستنده اعلام می‌نماید که آماده دریافت داده‌های جدید است و فرستنده می‌تواند شروع به ارسال داده‌ها نماید.

این روش کنترل جریان، یک روش in- band به حساب می‌آید و در مقابل، روش استفاده از خطوط کنترل Hand shake سخت‌افزاری مانندRTS / CTS، یک روش کنترل جریان Out-of-Band محسوب می‌شود.

۲ـ۲ـ۶ روش Stop & Wait (توقف و انتظار)

طرز کار این روش نرم‌افزاری، بسیار ساده است. فرستنده یک فریم را ارسال می‌کند و منتظر دریافت Ack گیرنده می‌شود و در صورت دریافت Ack می‌تواند فریم بعدی را ارسال کند. (تا وقتی که Ack ارسال نشده است، ارسال داده متوقف می‌شود.) این روش مناسب محیط‌های نویزی (با احتمال خطای بالا) نمی‌باشد. همچنین این روش وقتی موثر است که فریم‌ها بزرگ باشد.

راندمان (بهره) کانال بدون خطا در روش Stop & Wait

بهره کانال (Channel Utilization) که آن را با U نشان می‌دهیم در روش Stop & Wait از رابطه زیر بدست می‌آید:

$$U = \frac{\text{زمان مفید مصرف شده برای ارسال فریم داده در فرستنده}}{\text{زمان انتشار Ack + کل زمان لازم برای دریافت فریم از لحظه شروع ارسال}} = \frac{\text{زمان انتقال}}{\text{زمان انتشار} + \text{زمان انتقال} + \text{زمان انتشار}} = \frac{\text{زمان انتقال}}{(\text{زمان انتشار} \times 2) + \text{زمان انتقال}} = \boxed{\frac{1}{1+2\left(\frac{\text{زمان انتشار}}{\text{زمان انتقال}}\right)}}$$

توجه کنید در رابطه فوق، منظور از زمان انتقال فریم در صورت کسر، حاصلضرب اندازه فریم در نرخ انتقال داده می‌باشد، زیرا در کاراترین حالت اگر منتظر Ack می‌شدیم و فریم‌ها را پشت سر هم ارسال می‌کردیم برای انتقال یک فریم به همین اندازه زمان صرف می‌شد. اما در مخرج، کل زمان را در نظر می‌گیریم و اولاً زمان انتظار مربوط به تاخیر انتشار کانال را به آن اضافه می‌کنیم. ثانیاً باید زمان لازم برای انتقال و تاخیر انتشاری Ack را نیز به کل زمان اضافه کنیم، اما به علت کوچک بودن Ack از زمان انتقال آن (حاصلضرب اندازه Ack در نرخ ارسال) صرف‌نظر کرده و فقط زمان تاخیر انتشاری مربوط به Ack را به مخرج اضافه می‌کنیم. رابطه فوق را به شکل ساده زیر می‌نویسیم:

$$\boxed{U = \frac{1}{1+2a}}$$

اگر Ack نداشتیم $U = \frac{\text{زمان انتقال}}{\text{زمان انتقال} + \text{زمان انتشار}} = \frac{1}{1+0} = 1$

در رابطه فوق a به صورت زیر محاسبه می‌شود (در پرانتزها، واحد سنجش هر پارامتر نوشته شده است):

$$a = \frac{\text{تاخیر انتشاری کانال}}{\text{زمان انتقال یک فریم}} = \frac{\frac{D(m)}{V(m/s)}}{\frac{L(bit)}{R(bps)}}$$

D : طول کانال (فاصله بین فرستنده و گیرنده)

V : سرعت انتشار سیگنال در کانال (مضربی از سرعت نور)

L : طول فریم

R : نرخ ارسال بیت‌ها

راندمان (بهره) کانال با وجود خطا در روش Stop & Wait

در این روش، اگر خطا رخ دهد از روش Backward Error Control یا ARQ (Automatic Repeat Request) [از نوع Idle RQ] استفاده می‌شود (گیرنده به جای Ack ، Nack ارسال می‌کند) و فریم معیوب یا گم شده مجدداً ارسال می‌شود.

فرض کنید احتمال خطا در هر بیت ارسالی را با P_{bit} و احتمال خطا در فریم به طول L را با P_f نشان دهیم. راندمان کانال با وجود خطا از رابطه زیر بدست می‌آید:

$$U = \frac{1-P_f}{1+2a} \quad ; \quad P_f \text{ (تقریبی)} = L * P_{bit}$$

$$P_f \text{ (دقیق)} = 1-(1-P_{bit})^L$$

نکته : عیب اساسی روش توقف و انتظار کارآیی و بهره پایین آن است.

۳ـ۲ـ۶ روش Sliding Window (پنجره لغزان)

هدف اصلی این روش برطرف کردن مشکل پائین بودن بهره و کارآیی روش توقف و انتظار می‌باشد. به این منظور، فرستنده می‌تواند تعداد W فریم را بدون دریافت Ack ارسال نماید. (فرض بر این است که بافر گیرنده گنجایش W فریم را دارد). پیغام‌هایی که هنوز Ack آن‌ها دریافت نشده است در بافر فرستنده نگهداری می‌شوند (ممکن است نیاز به ارسال مجدد داشته باشند (بروز خطا)). در هر حال، اگر تعداد W فریم ارسال شود و Ack هیچ‌کدام دریافت نشود فرستنده باید ارسال را متوقف کند. بدین‌ترتیب گیرنده می‌تواند با عدم ارسال Ack، جریان داده را کنترل نماید (در صورتی که نتواند فریم‌های بعدی [بیش از W تا] را دریافت نماید).

نکته ۱: اگر اندازه پنجره (W) در فرستنده را برابر یک بگیریم به روش Stop & Wait و ARQ می‌رسیم.

نکته ۲: فریم‌ها باید شماره‌گذاری شوند، زیرا باید مشخص شود که کدام فریم درست رسیده است و هر Ack مربوط به کدام فریم است.

نکته ۳: به مفهوم پنجره گیرنده و پنجره فرستنده و تفاوت آن‌ها دقت نمائید:

- پنجره گیرنده (پنجره دریافت) : فریم‌های دریافت شده که Ack آن‌ها ارسال نشده، پنجره گیرنده را مشخص می‌کند.
- پنجره فرستنده (پنجره ارسال) : فریم‌هایی که ارسال شده‌اند، بدون دریافت Ack از گیرنده، پنجره فرستنده را مشخص می‌کنند.

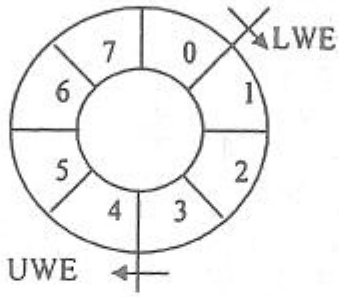
نکته ۴: فاکتورهای اندازه فریم، تاخیر انتشار خط، نرخ بیت ارسالی و اندازه بافرها، حداکثر اندازه پنجره ارسال (W) را تعیین می‌کنند.

به شکل ۴۸ نگاه کنید و در آن به نکات ذیل دقت نمائید:

- UWE (Upper Window Edge : لبه بالایی پنجره ارسال): با ارسال هر فریم این لبه یک واحد جلو می‌رود (در جهت عقربه‌های ساعت)
- LWE (Lower Window Edge: لبه پایینی پنجره ارسال): با دریافت هر Ack، این لبه نیز یک واحد جلو می‌رود (در جهت عقربه‌های ساعت)

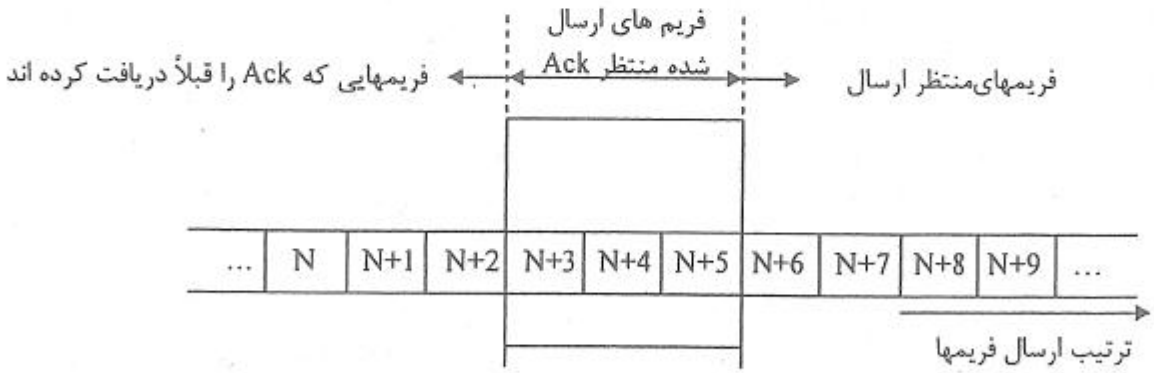
هر دو لبه در ابتدای کار در مبدا (ابتدای فریم صفر) قرار دارند و اگر اختلاف UWE و LWE به W (حداکثر اندازه پنجره) برسد فرایند ارسال باید متوقف شود.

دقت کنید تعداد شماره ترتیب‌ها W+1 است (از 0 تا W) که دلیل آن ذکرخواهد شد. البته واضح است که UWE نمی‌تواند آن‌قدر جلو برود که بر روی LWE قرار بگیرد چون پنجره ارسال برابر W+1 خواهد شد که از حد مجاز (W) بزرگتر خواهد بود.



شکل ۴۸. پنجره ارسال با اندازه W در پروتکل Go-Back-N

شکل ۴۹ نیز همین موضوع را برای پنجره‌ای به اندازه W=3 نشان می‌دهد. تفاوت این شکل با شکل ۴۸ در این است که شماره فریم‌ها افزایشی است (در عمل چنین نیست و تعداد شماره ترتیب‌ها مشخص است و حالت تکراری دارد) یعنی در شکل زیر، اگر Ack فریم شماره N+3 دریافت شود، فرستنده می‌تواند فریم N+6 را ارسال کند و پنجره را به سمت جلو بلغزاند. اگر خط بدون خطا باشد پنجره با طول W=3 روی فریم‌ها می‌لغزد (پنجره لغزان).



شکل ۴۹. مفهوم پنجره لغزان

شماره ترتیب (Sequence Number) فریم‌ها

در کلیه روش‌های کنترل خطا و کنترل جریان شماره ترتیب فریم‌ها، لازم نیست نامحدود باشد. اما حداقل تعداد شماره ترتیب‌های لازم بستگی به روش‌های کنترل جریان و کنترل خطا دارد. در ادامه، حداقل تعداد شماره ترتیب لازم در روش کنترل جریان پنجره لغزان، برای سه روش متفاوت کنترل خطا مورد بحث قرار می‌گیرند:

- **Go-Back-N**

در روش Go-Back-N اگر اندازه پنجره فرستنده W باشد، حداقل تعداد شماره‌های شناسایی باید W+1 (0 , 1 , ... , W-1 , W) باشد؛ زیرا اگر W فریم از شماره 0 تا W-1 ارسال شود و Ack هر W فریم نیز از گیرنده ارسال شود و در راه خراب شوند (هر W تا Ack نرسد) و تایمر فرستنده منقضی شود، همه فریم‌ها را دوباره ارسال می‌نماید. گیرنده که منتظر دریافت فریم شماره W است، به محض دریافت مجدد فریم شماره صفر، یک Nack (W) ارسال می‌کند. اما اگر شماره‌ها از صفر تا W-1 باشد، مشخص نمی‌شود که فریم شماره صفر قبلی دوباره ارسال شده است یا این‌که فرستنده همه Ack ها را دریافت کرده و یک فریم شماره صفر مربوط به دور جدید را ارسال نموده است.

- **Selective Repeat**

در روش Selective Repeat تعداد شماره های ترتیب نباید کمتر از 2W باشد. (W اندازه پنجره فرستنده است). فرض کنید W فریم ارسال شده و به طور صحیح در گیرنده دریافت شده است و هر W تا Ack در راه خراب شده‌اند، گیرنده باید بفهمد که مجموعه جدید شامل W فریم ارسال مجدد است و یا مربوط به پنجره بعدی است.

جدول زیر اندازه پنجره‌گیرنده، پنجره فرستنده و تعداد شماره ترتیب لازم در روش پنجره لغزان را برای سه روش کنترل خطای متفاوت نشان می‌دهد. توجه نمائید که پنجره لغزان با کنترل خطا به روش Idle-RQ دقیقاً مانند روش Stop & Wait عمل می‌کند.

پروتکل کنترل خطا	اندازه پنجره فرستنده	اندازه پنجره گیرنده	تعداد شماره ترتیب لازم
Idle-RQ	1	1	2
Selective-Repeat (Selective-Reject)	W	W	2W
Go-back-N	W	1	W+1

راندمان روش پنجره لغزنده

• بهره یا راندمان پنجره لغزان در حالت بدون خطا از رابطه زیر بدست می‌آید:

$$U = \frac{W}{1+2a} \; ; \; W < 1+2a$$

نکته : اگر $W \geq 1+2a \Leftarrow U = 1$ (راندمان بزرگتر از یک بی‌معنی است)

• بهره یا راندمان پنجره لغزان در کانال دارای خطا با روش کنترل خطای Selective Repeat (تکرار انتخابی یا رد انتخابی) از روابط زیر به دست می‌آید:

P_f: احتمال خطا در فریم

W: اندازه پنجره فرستنده (و گیرنده)

a : نسبت زمان انتشار به زمان انتقال فریم

$$\begin{cases} U = \dfrac{W(1-P_f)}{1+2a} & ; W < 1+2a \\ U = 1-P_f & ; W \geq 1+2a \end{cases}$$

• بهره یا راندمان پنجره لغزان در کانال دارای خطا با روش کنترل خطای Go-back-N از روابط زیر به دست می‌آید:

$$\begin{cases} U = \dfrac{1-P_f}{1+2aP_f} & ; W \geq 1+2a \\ U = \dfrac{W(1-P_f)}{(1+2a)(1-P_f+W*P_f)} & ; W < 1+2a \end{cases}$$

تست‌های فصل پنجم و ششم

۱ ـ در یک سیگنال PCM با کوانتیزاسیون خطی 10 بیتی، SNR چقدر است؟ (نسبت سیگنال به نویز کوانتیزاسیون)

۱) 62.7 dB ۲) 61.96dB ۳) 65.91dB ۴) 721dB

۲ ـ نرخ خطا در یک کانال، 1 در 10^6 است (10^{-6}) و خطاها غیر فورانی هستند. اگر اندازه هر بلوک داده 1000 بیت باشد و هر بلوک یک کد همینگ (افزونگی) 10 بیتی داشته باشد و یک مگابیت (1Mb) داده ارسال شود، هزینه کشف و تصحیح یک بیت خطا نسبت به روش بیت توازن چقدر است؟

۱) 10000 ۲) 10000/1001 ۳) 10000/1000 ۴) 10000/2001

۳ ـ در یک سیستم انتقال اطلاعات از روش کدهای خطی با استفاده از ترکیب عملیات XOR روی داده‌ها برای کنترل خطا استفاده می‌شود. سه نمونه از کدهای این سیستم عبارتند از: 0011110 , 1001011 , 0101101 که در هر یک از این کدها سه بیت MSB داده می‌باشند (به عنوان مثال 001) و چهار بیت LSB توازن هستند (به عنوان مثال 1110). کد توازن جهت داده 110 چه خواهد بود ؟ (سراسری ـ ۷۵)

۱) 1000 ۲) 0110 ۳) 1111 ۴) 1110

۴ ـ برای ارسال یک متن انگلیسی از کد اسکی (7 بیت داده + توازن) استفاده کرده‌ایم و در انتهای پیام یک بایت توازن عمودی اضافه می‌کنیم تا توانایی تشخیص خطا را بهتر کنیم. کدام یک از اظهارات زیر نادرست است؟ (سراسری ـ ۷۴)

۱) دو بیت خطا در هر صورت در گیرنده قابل تشخیص است.

۲) سه بیت خطا در هر صورت در گیرنده قابل تشخیص است.

۳) چهار بیت خطا در هر صورت در گیرنده قابل تشخیص است.

۴) پنج بیت خطا در هر صورت در گیرنده قابل تشخیص است.

۵ ـ فرض کنید احتمال این‌که یک کاراکتر در ارسال دچار خطا شود P باشد احتمال این‌که یک پیغام n کاراکتری دچار خطا شود چقدر است؟ (سراسری ـ ۷۳)

۱) P^n ۲) P ۳) $1-(1-P)^n$ ۴) هیچ‌کدام

۶ ـ اگر چند جمله‌ای مولد برابر $G(x)=x^2+1$ باشد کلمه کد چرخه‌ای حاصل برای بلوک دیتای 1 0 1 1 0 چگونه خواهد بود؟ کلمه کد شامل بلوک دیتا و کد CRC می‌باشد. (سراسری ـ ۷۲)

۱) 1011010 ۲) 1011001 ۳) 1010110 ۴) 0110110

۷ ـ فرض کنید اطلاعاتی را می‌خواهیم ارسال کنیم که تنها از چهار کاراکتر تشکیل شده‌اند. کدهای باینری زیر را برای آن‌ها انتخاب کرده‌ایم: 1111 1111، 0000 1111، 1111 0000 و 0000 0000 چند بیت خطا را می‌توان در گیرنده تصحیح کرد؟ (آزاد ـ ۷۸)

۱) 5 بیت ۲) 4 بیت ۳) 2 بیت ۴) 3 بیت

۸ ـ فرستنده‌ای پیام‌هایی را به کمک کد CRC با مولد $G(x)=x^3+x^2+1$ کد می‌کند. و پیام‌های زیر توسط گیرنده دریافت می‌شود. کدام یک دارای خطای بیت است؟ (آزاد ـ ۷۶)

۱) 11011101 ۲) 01001011 ۳) 00110110 ۴) 10110101

۹ ـ یک کد همینگ در اختیار داریم که می‌تواند حداقل 5 خطا را در هر بلوک تشخیص دهد. این کد چند خطا را می‌تواند تصحیح کند؟ (آزاد ـ ۷۶)

۱) یک ۲) سه ۳) چهار ۴) دو

۱۰ ـ به یک کاراکتر 7 بیتی اسکی در هنگام ارسال، دو بیت پریتی اضافه می‌کنیم یک بیت پریتی برای بیت‌های زوج و یک بیت پریتی برای بیت‌های فرد؛ کدام یک از جملات زیر صحیح است؟ (آزاد ـ ۷۸،۷۹)

۱) فاصله همینگ این کد برابر با حالتی است که فقط یک بیت پریتی به هر کاراکتر اضافه کرده باشیم

۲) فاصله همینگ این کد برابر با 3 می‌باشد

۳) فاصله همینگ این کد بستگی به این دارد که بیت‌های پریتی هر کدام از نوع زوج یا فرد انتخاب شود

۴) این کد قادر است 2 بیت خطا را در هر صورت تشخیص دهد

۱۱ ـ احتمال این‌که در یک سیستم هفت بیتی کد همینگ که به منظور کشف خطای یک بیتی طراحی شده است خطا وجود داشته باشد چقدر است؟ (به شرط این‌که احتمال وجود خطا در یک بیت برابر P باشد) (آزاد ـ ۷۹)

۱) $\frac{7!}{4!\ 3!}P^3(1-P)^4$ ۲) $\frac{7!}{5!\ 2!}P^2(1-P)^5$ ۳) $P(1-P)^7$ ۴) $P^7(1-P)$

۱۲ ـ در محاسبه CRC چند جمله‌ای مولد را $G(x)=x^3+x+1$ در نظر بگیرید. اطلاعات به صورت 1001 می‌باشد. کلمه کد حاصل با خطا در اولین بیت (از سمت چپ) به گیرنده می‌رسد. کلمه کد ارسالی و باقیمانده بدست آمده در گیرنده چیست؟ (سراسری ـ ۸۱)

۱) 1001110 و 101 ۲) 1001000 و 000 ۳) 1001101 و 110 ۴) 1001111 و 100

۱۳ ـ فرض کنید یک کانال ارتباطی با نرخ 3Mbps (مگابیت در ثانیه) فعالیت می‌کند و نرخ خطای آن 10^{-3} است. خطاهای بیت تصادفی هستند و مستقل از یکدیگرند. فرض کنید برای ارسال 1 از کد 111 و برای ارسال 0 از کد 000 استفاده شود. گیرنده با الگوریتم رای اکثریت تشخیص صفر یا یک می‌دهد. احتمال خطای بیت در گیرنده چقدر است؟ (سراسری ـ ۸۱)

۱) 10^{-9} ۲) 10^{-3} ۳) 3×10^{-6} ۴) 3×10^{-3}

۱۴ ـ اگر سرعت دستیابی به حافظه در یک PBX (سوییچ کوچک) که به روش تقسیم زمانی سوییچ می‌کند 50 ns باشد، حداکثر تعداد پورت این PBX چقدر می‌تواند باشد، در صورتی که هر پورت 8000 بار در ثانیه نمونه‌برداری شود؟ (آزاد ـ ۷۸)

۱) 2500 پورت ۲) 2000 پورت ۳) 5000 پورت ۴) 1250 پورت

۱۵ ـ یک مالتی پلکسر ترمینال دارای 6 خط ورودی با سرعت 1200 بیت در ثانیه و N خط ورودی با سرعت 300 بیت در ثانیه است. سرعت خط خروجی 9600 بیت در ثانیه می‌باشد.اگر خطوط ورودی و خروجی همگی آسنکرون باشند، حداکثر مقدار N چقدر می‌تواند باشد؟ (آزاد ـ ۷۸)

۱) 10 ۲) 8 ۳) 12 ۴) 15

۱۶ ـ در روش کنترل جریان ایست و انتظار (Stop & Wait) بهره‌وری کانال (Line Utilization) چه اندازه است؟ (فرض کنید طول فریم هزار بیت، سرعت ارسال ده هزار بیت بر ثانیه و تاخیر انتشار 200 میلی ثانیه است) (سراسری ـ ۸۱)

۱) کمتر از 10% ۲) 20% ۳) 33.3% ۴) 100%

۱۷ ـ یک سری فریم 1000 بیتی با استفاده از قرارداد RQ پیوسته ارسال می‌شوند. سرعت انتشار $2\times10^8\ m/s$ و نرخ خطا قابل چشم‌پوشی است. طول مسیر برابر 1Km و سرعت انتقال 1Mbps و تعداد پنجره ارسالی 2 است. بهره خط چیست؟ (سراسری ـ ۷۴)

۱) 0.5 ۲) 0.9 ۳) 0.8 ۴) 1

۱۸ ـ کدام یک از اظهارات زیر در مورد پروتکل‌های Go-back-N و یا Selective Reject غلط است؟(سراسری ـ ۷۵)

۱) جهت یک پروتکل Selective Reject در صورتی که ماکزیمم اندازه پنجره فرستنده و گیرنده 7 باشد پیغام‌ها را می‌توان با 3 بیت شماره‌گذاری کرد.

۲) جهت یک پروتکل Selective Reject در صورتی که ماکزیمم اندازه پنجره فرستنده و گیرنده 7 باشد پیغام‌ها را می‌توان با 4 بیت شماره‌گذاری کرد.

۳) جهت یک پروتکل Go-back-N می‌توان پیغام‌ها را با سه بیت شماره‌گذاری کرد.

۴) جهت یک پروتکل Go-back-N می‌توان پیغام‌ها را با چهار بیت شماره‌گذاری کرد.

۱۹ ـ می‌خواهیم به کمک یک پروتکل که از روش Stop & Wait کار می‌کند یک فایل بزرگ را از شهر A به B با فاصله 50 کیلومتر انتقال دهیم. اگر بخواهیم از یک ارتباط ماهواره‌ای با نرخ 20Kbps بهره جوییم طول هر بلوک اطلاعات تقریباً چقدر باشد تا نرخ واقعی ارسال اطلاعات حداقل معادل نرخ ارسال از طریق یک خط تلفن با سرعت 10Kbps باشد؟ فاصله ماهواره تا زمین 30000Km است. (آزاد ـ ۷۶)

۱) 8000 ۲) 4000 ۳) 12000 ۴) 16000

۲۰ ـ نرخ ارسال یک کانال در روش Stop & Wait، 6000 بیت بر ثانیه است. اگر تاخیر انتشار 20 میلی ثانیه باشد، اندازه فریم در چه محدوده‌ای باشد تا بهره‌وری کانال حداقل 50% شود؟

۱) بزرگتر یا مساوی 120 بیت ۲) بزرگتر یا مساوی 60 بیت

۳) بزرگتر یا مساوی 240 بیت ۴) بزرگتر یا مساوی 80 بیت

سوالات ۲۱ تا ۲۴، سوالات انتقال داده سراسری ۸۲ است و مربوط به کل فصول قبل است:

۲۱ ـ ماکزیمم بهره‌وری کانال (Channel Utilization) در یک انتقال ATM روی یک مسیر 30Km از فیبر نوری با مشخصات زیر کدام است؟

(سرعت نور در فیبر $3\times10^8\ m/s$، فریم‌ها 53 بایتی (8×53) و نرخ ارسال 155 مگابیت بر ثانیه و کنترل جریان (Flow control) به صورت‌های:

I) Stop & Wait II) Sliding window با طول پنجره 127

۱) $I(II,\frac{1}{74})$ ۲) $\frac{127}{74}(II,\frac{1}{74})$ ۳) $I(II,\frac{1}{10})$ ۴) هیچ‌کدام

۲۲ ـ یک دنباله بیت‌ها، کد شده با NRZ – L از فیلتری با r=0.5 عبور داده شده و سپس با یک حامل مدوله شده است. اگر نرخ بیت 4800 بیت بر ثانیه باشد، پهنای باند برای مدولاسیون‌های I) ASK II) FSK III) QPSK چیست؟ (در حالت FSK حامل فرکانس‌های 50KHz و 55KHz را دارد.)

۱) I(4800 , II(14800 , III(2400 ۲) I(7200 , II(17200 , III(3600

۳) I(7200 , II(12200 , III(3600 ۴) I(4800 , II(9800 , III(2400

۲۳ ـ کدام گزینه در مورد نویزهای کانال انتقال نادرست است؟

۱) توان نویز حرارتی متناسب با پهنای باند کانال انتقال است.

۲) منشا نویز Inter modulation کانال، منابع نویز خارجی هستند.

۳) منشا نویز Cross talk می‌تواند القای کانال‌های مجاور باشد.

۴) نویز ضربه‌ای (Impulse) در ارسال دیجیتال نسبت به ارسال آنالوگ مشکل بیشتری ایجاد می‌کند.

۲۴ ـ در صورتی‌که تابع تبدیل یک کانال انتقال در حوزه فرکانس برای تمام فرکانس‌ها مقدار ثابت یک باشد ولی فاز آن مقادیر دلخواهی باشد می‌توان گفت:

۱) سیگنال خروجی کانال تضعیف شده سیگنال ورودی است.

۲) توان متوسط خروجی کانال می‌تواند متفاوت از توان ورودی آن باشد.

۳) شکل موج خروجی کانال انتقال با شکل موج ورودی آن یکسان است.

۴) امکان بوجود آمدن تداخل بین سمبل‌ها (ISI) در کانال وجود دارد.

۲۵ ـ اگر در یک کانال ماهواره با سرعت 1 Mbps از فریم‌های 1000 بیتی استفاده شود و تاخیر انتشار 250ms باشد برای روش کنترل جریان پیوسته با اندازه پنجره 8 حداکثر راندمان چقدر است؟ (روش پنجره لغزنده)

۱) 0.014 ۲) 0.14 ۳) 0.016 ۴) 1

۲۶ ـ در تست ۲۵، اگر از روش Stop & Wait استفاده کنیم، حداکثر بهره‌وری چقدر است؟

۱) تقریبا 0.002 ۲) تقریبا 0.004 ۳) 0.02 ۴) 0.04

۲۷ ـ تست ۲۵ را برای کانالی که احتمال خطای بیت در آن 10^{-4} است و از روش Selective – Repeat استفاده می‌شود، حل کنید:

۱) 0.0183 ۲) 0.0133 ۳) 0.0144 ۴) 0.0126

۲۸ ـ تست ۲۶ را برای کانالی که احتمال خطای فریم در آن 0.1 است حل کنید. (تقریبی)

۱) 18×10^{-4} ۲) 36×10^{-4} ۳) 2×10^{-3} ۴) 0.02

۲۹ ـ در روش کنترل جریان پنجره لغزنده با روش کنترل خطای بازگشت به N(Go-back-N) اگر اندازه پنجره فرستنده، 10 باشد شماره ترتیب فریم‌ها در چه بازه‌ای است؟

۱) 0 تا 10 ۲) 0 تا 11 ۳) 0 تا 20 ۴) 1 تا 20

۳۰ ـ در کدام یک از روش‌های کنترل خطا، علیرغم این‌که یک فریم خراب می‌شود ممکن است چند فریم مجدداً ارسال شود؟

۱) Idle-RQ ۲) Selective Repeat (Selective Reject)

۳) Go-back-N ۴) هیچ‌کدام

حل تشریحی تست‌های فصل پنجم و ششم

۱ـ گزینه ۲ صحیح می‌باشد

حل :

$$n=10 \Rightarrow SNR = 6.02*n+1.76 = 60.2+1.76 = 61.96dB$$

۲ـ گزینه ۴ صحیح می‌باشد

حل :

$$Parity \Rightarrow \frac{1000000\,bit}{1000\,bit/Block} = 1000\ \ Block \quad \Rightarrow \quad 1000\times 1bit\,(Parity) = 1000\ bit\,(Redundancy\ of\ parity\ bits)$$

$$1000\,(Parity\ bits) + 1000^{-6} * 1000^{6} * (1000+1) = 1000+1001 = 2001 = \text{افزونگی ارسال مجدد فریم معیوب + افزونگی بیت‌های توازن = افزونگی کل}$$

$$Hamming \rightarrow 1000\,Block * 10bit = 10000\,(Redundancy) \Rightarrow \ \text{نسبت} = \frac{10000}{2001}$$

۳ـ گزینه ۲ صحیح می‌باشد

حل :

دقت کنید که تعداد کل یک‌ها زوج است. پس گزینه ۲ یا ۳ صحیح می‌باشد. آیا می‌توان با توجه به این‌که تعداد کل یک‌ها برابر ۴ است، چنین نتیجه گرفت که گزینه ۲ صحیح است؟!

در هر حال؛ راه حل کامل آن به صورت زیر است که در ابتدا آنرا اثبات می‌کنیم:

فرض کنید هر بیت توازن حاصل XOR دو بیت داده باشد (قابل تعمیم به n بیت):

$$m_1m_2m_3r_1r_2r_3r_4 \rightarrow r_i = m_p \oplus m_K$$

$$m_1'm_2'm_3'r_1'r_2'r_3'r_4' \rightarrow r_i' = m_p' \oplus m_K'$$

اگر عبارت‌های بالا و پایین را XOR نمائیم: $r_i \oplus r_i' = (m_p \oplus m_p') \oplus (m_k \oplus m_k')$ (یعنی اگر بخش داده در دو کد XOR شوند بخش افزونگی نیز XOR می‌شوند)

$$110 = 100 \oplus 010$$

$$\Rightarrow R = 1101 \oplus 1011 = 0110$$

۴ـ گزینه ۳ صحیح می‌باشد

حل :

چهار بیت خطا که رئوس یک مربع را تشکیل می‌دهند، قابل تشخیص نمی‌باشد.

۵ـ گزینه ۳ صحیح می‌باشد

حل :

احتمال عدم خطا در یک کاراکتر: $1-P$

احتمال عدم خطا در n کاراکتر: $(1-P)^n$

احتمال خطا در n کاراکتر: $1-(1-P)^n$

۶ ـ گزینه ۱ صحیح می‌باشد.

حل :

$$10110 \rightarrow 1011000 \qquad x^6+x^4+x^3 \;\big|\; x^2+1$$

$$\underline{x^6+x^4} \qquad\qquad x^4+x$$

$$x^3$$

$$\underline{x^3+x}$$

$$x \rightarrow R(x)=\boxed{10}$$

$$M(x)\,R(x)$$

$$\boxed{10110}\boxed{10}$$

۷ ـ هیچ گزینه‌ای صحیح نمی‌باشد.

حل :

$$D=4 \quad \Rightarrow \quad c=\left[\frac{4-1}{2}\right]=\left[\frac{3}{2}\right]=1$$

این تست نادرست است و گزینه صحیح ندارد.

۸ ـ گزینه ۳ صحیح می‌باشد

حل :

باید همه گزینه‌ها را آزمایش کنیم! برای گزینه ۳، باقیمانده مخالف صفر است.

$$x^5+x^4+x^2+x \qquad \big|\, x^3+x^2+1$$

$$\underline{x^5+x^4+x^2} \qquad\qquad x^2$$

$$x$$

۹ ـ گزینه ۴ صحیح می‌باشد

حل :

$$d=5$$

$$D=d+1=6$$

$$c=\left[\frac{6-1}{2}\right]=2$$

۱۰ ـ گزینه ۱ صحیح می‌باشد

حل :

مثلاً اگر دو بیت زوج خراب شوند قابل تشخیص نمی‌باشد.

۱۱ ـ گزینه ۲ صحیح می‌باشد

حل :

$$\text{احتمال ۲ بیت خطا} = \binom{7}{2} P^2 (1-P)^{7-2}$$

۱۲ ـ گزینه ۱ صحیح می‌باشد

حل :

$$1001000 = x^6 + x^3 \quad \left| \frac{x^3+x+1}{x^3+x} \right.$$

$$\frac{x^6+x^4+x^3}{x^4}$$

$$\frac{x^4+x^2+x}{x^2+x} \rightarrow R(x) = 110$$

خطا

$$1001110 \rightarrow \overset{x^3x^2x}{0001110} \quad \left| \frac{x^3+x+1}{1} \right.$$

$$\frac{x^3+x+1}{x^2+1} \rightarrow R(x) = 101$$

۱۳ ـ گزینه ۳ صحیح می‌باشد

حل :

$$10^{-9} + \binom{3}{2} \times 10^{-3} \times 10^{-3} = \frac{3!}{1!\,2!} * 10^{-6} + 10^{-9} = 3 \times 10^{-6}$$

۱۴ ـ گزینه ۴ صحیح می‌باشد

حل :

در رابطه $2 \times x$ قرار داده‌ایم که عمل نوشتن در حافظه و خواندن مجدد از حافظه سوییچ را در نظر گرفته باشیم:

زمان نمونه‌برداری $\geq 50ns$

$$\text{Min}\left(\frac{1}{\text{نرخ نمونه‌برداری}}\right) = 50 \times 10^{-9}$$

$$\frac{1}{2 \times x \times 8000} = 50 \times 10^{-9}$$

$$2 \times x \times 50 \times 10^{-9} \times 8 \times 10^{3} = 1$$

$$2 \times x = \frac{1}{0.400 \times 10^{-3}} = 2500 \Rightarrow x = 1250$$

۱۵ ـ گزینه ۲ صحیح می‌باشد

حل :

$$6 \times 1200 + 300N \leq 9600$$

۱۶ ـ گزینه ۲ صحیح می‌باشد

حل :

$$a = \frac{200ms}{\frac{1000b}{10000\frac{b}{s}}} = \frac{200ms}{100ms} = 2 \Rightarrow U = \frac{1}{1+2a} = \frac{1}{5}$$

۱۷ ـ گزینه ۴ صحیح می‌باشد

حل :

$$a = \frac{\frac{1000}{2 \times 10^{8}}}{\frac{1000}{10^{6}}} = \frac{10^{9}}{2 \times 10^{11}} = \frac{1}{200}$$

$W = 2 > 1 + 2a \Rightarrow U = 1$

۱۸ ـ گزینه ۴ صحیح می‌باشد

حل :

Selective Reject $\rightarrow W = 7 \rightarrow$ تعداد شماره $= 2W = 2 \times 7 = 14 \rightarrow$ (سه بیت (0 تا 7) غلط است)

۱۹ ـ گزینه ۲ صحیح می‌باشد

حل :

$$\frac{1}{1+2a} \times 20 = \frac{1}{1+2a'} \times 10$$

$$\frac{1+2a}{1+2a'} = 2$$

$$2a = 1 + 4a'$$

$$2 \times \frac{2000}{L} = 1 + 4 \times \frac{5 \times 10^{-8}}{3 \times 10^{-8} L} = 1 + \frac{20}{3L}$$

$$\frac{4000}{L} = 1 + \frac{20}{3L}$$

$$4000 = L + \frac{20}{3} \rightarrow L = 4000$$

$$\frac{1}{1 + 2 \times \frac{2000}{L}} = \frac{1}{2} \Rightarrow L \approx 4000$$

راه‌تستی کوتاه:

۲۰ ـ گزینه ۳ صحیح می‌باشد

حل :

$$\frac{1}{1+2a} \geq \frac{1}{2}$$

$$a = \frac{20 \times 10^{-3}}{\frac{L}{6000}} = \frac{120}{L}$$

$$\frac{1}{1 + \frac{240}{L}} \geq \frac{1}{2} \Rightarrow L \geq 240$$

سوالات ۲۱ تا ۲۴ کل سوالات انتقال داده سراسری ۸۲ است و مربوط به کل فصول قبل است:

۲۱ ـ گزینه ۱ صحیح می‌باشد

حل :

$$U = \frac{1}{1+2a} = \frac{1}{1 + 2 \times \frac{\frac{30000}{3 \times 10^8}}{\frac{53 \times 8}{155 \times 10^6}}} = \frac{1}{1+73} = \frac{1}{74}$$

II) $W > 1 + 2a \Rightarrow U = 1$

۲۲ ـ گزینه ۳ صحیح می‌باشد

حل :

$$ASK \rightarrow BW = 2f_0(1+r) = R(1+r) = 4800 \times 1.5 = 7200$$

$$FSK = f_s + 2f_0(1+r) = (f_2 - f_1) + R(1+r) = 5KHz + 4800 \times 1.5 = 5000 + 7200 = 12200$$

$$BW(PSK) \overset{\text{همانند}}{=} BW(ASK) \rightarrow BW = 7200$$

$$BW(QPSK) = \frac{BW(PSK)}{\log_2^M} = \frac{BW(PSK)}{\log_2^4} = \frac{7200}{2} = 3600$$

۲۳ ـ

حل : گزینه ۲ صحیح می‌باشد

۲۴ ـ

حل : گزینه ۴ صحیح می‌باشد

۲۵ ـ گزینه ۳ صحیح می‌باشد

حل :

$$U = \frac{W}{1+2a} = \frac{8}{1+2*\frac{250\times10^{-3}}{\frac{1000}{1000000}}} = \frac{8}{1+500} \simeq 0.016$$

۲۶ ـ گزینه ۱ صحیح می‌باشد

حل :

$$U = \frac{1}{1+2a} = \frac{1}{1+500} = 0.002$$

۲۷ ـ گزینه ۳ صحیح می‌باشد

حل :

$$P_f = 1000 \times 10^{-4} = 10^{-1}$$

$$U = \frac{W(1-P_f)}{1+2a} = 0.9 \times \frac{W}{1+2a} = \frac{0.9\times8}{501}$$

۲۸ ـ گزینه ۱ صحیح می‌باشد

حل :

$$U = \frac{(1-P_f)}{1+2a} = \frac{0.9}{501} \approx \frac{18\times10^{-1}}{10^3} = 18\times10^{-4}$$

۲۹ ـ گزینه ۱ صحیح می‌باشد

۳۰ ـ گزینه ۳ صحیح می‌باشد

فصل هفتم

زیر لایه کنترل دسترسی به رسانه انتقال (MAC Sublayer)

برخی از شبکه‌های کامپیوتری دارای فناوری انتقال انتشاری (Broadcast) بوده (عموماً شبکه‌های محلی LAN و شخصی PAN و به ندرت شبکه‌های WAN) و مبتنی بر روش دسترسی چندگانه (Multiple Access) به رسانه انتقال (Media) می‌باشند. بدین معنی که کلیه عناصر شبکه به‌طور همزمان به کانال انتقال داده که از نوع کانال با دسترسی تصادفی (Random Access Channel) می‌باشد دسترسی دارند و می‌توانند فریم‌های ارسالی خود را بر روی آن قرار داده و ارسال نمایند.

مشکل اصلی در این شبکه‌ها، کنترل دستیابی به رسانه انتقال (MAC : Medium Access Control) می‌باشد. هدف از این کنترل جلوگیری از تصادم (Collision) فریم‌های داده میزبان‌های مختلف است.

نکته : MAC و LLC دو زیر لایه از لایه دوم (پیوند داده) محسوب می‌شوند که البته LLC بر روی MAC قرار گرفته است و ارتباط آن را با لایه شبکه برقرار می‌کند.

LLC	Data link Layer
MAC	

MAC : Medium Access Control

LLC : Logical Link Control

۱ ـ ۷ انواع شبکه‌های دسترسی چندگانه

شبکه‌های دارای دسترسی چند گانه به چند دسته تقسیم می‌شوند.

- LAN
- (Ethernet) IEEE 802.3
- (Token bus) IEEE 802.4
- (Token ring) IEEE 802.5
- FDDI Token ring
- (Wireless LAN) IEEE 802.11

- PAN (Personal Area Network)
- IEEE 802.15 (Blue tooth) شبکه‌های بی‌سیم با برد کوتاه که برای اتصال تجهیزات جانبی به یک کامپیوتر شخصی به کار می‌روند حوزه آن در حدود 10 چند متر است.
- WAN (اکثراً از نوع Point to point اند اما چند نمونه Broadcast هم به شرح زیر دارند.)
- شبکه‌های ماهواره‌ای (Sattelite Networks)
- Mobile Radio Networks یا شبکه‌های سیار رادیویی (از نسل سوم تلفن‌های همراه به بعد، این فناوری ارتباط دیجیتال و ارسال همزمان صدا و داده را پشتیبانی می‌کند.)

بحث MAC ابتدا در شبکه‌های LAN مطرح شده و در آن‌جا از سیم‌های مسی یا فیبر نوری به عنوان رسانه دسترسی چندگانه و تصادفی استفاده می‌شود. حال به مرور اجمالی چند شبکه LAN می‌پردازیم.

۱ـ۱ـ۷ اترنت (Ethernet) یا DIX

اولین شبکه محلی در سال ۱۹۷۶ توسط شرکت Xerox طراحی و پیاده‌سازی شد و به یاد ماده خیالی به‌نام Ether که تا مدت‌ها تصور می‌شد محیط انتشار امواج الکترومغناطیسی است Ethernert نامگذاری شد.

در اولین نسل آن از کابل هم محور یا (Coaxial) ضخیم (Thick) استفاده می‌شد و به همین دلیل Thick Ethernert نام‌گذاری شد. (این شبکه‌ها دارای طول حداکثر 2500 متر و حداکثر 4 تکرار کننده در فواصل 500 متری بودند. حداکثر 256 کامپیوتری می‌توانستند به کابل اترنت با نرخ انتقال 2.94 مگابیت در ثانیه متصل شوند. روش کنترل دستیابی به محیط انتقال بدین صورت است که هر زمان که یک کامپیوتر بخواهد داده‌های خود را ارسال کند در صورتی‌که مطمئن شود کامپیوتر دیگری در آن لحظه در حال استفاده از کانال نیست داده‌های خود را ارسال می‌کند. جزئیات این روش را بعداً مورد بررسی خواهیم داد.

در اینجا هیچ‌گونه نوبتی برای دسترسی نداریم و دسترسی از نوع تصادفی است. این شبکه توسط IEEE با عنوان IEEE 802.3 استاندارد شد. وظیفه پیاده‌سازی پروتکل رایک کارت واسط شبکه یا NIC : Network Interface Card بر عهده دارد.

۲ـ۱ـ۷ خط توکن یا (Token Bus)

این روش تقریباً همزمان با اترنت در شرکت General Motors برای خط تولید اتومبیل طراحی و پیاده‌سازی شد و سپس توسط IEEE استاندارد شد و IEEE 802.4 نام گرفت.

توپولوژی آن یک Bus است اما پروتکل کنترل دستیابی به رسانه انتقال در آن کاملاً با اترنت متفاوت است و روش آن نوبت گردشی است؛ بدین طریق که نوبت ارسال کامپیوترها به کمک یک بسته خاص به نام نشانه (Token) که بین کامپیوترها دست به دست می‌چرخد تعیین می‌گردد. هر کامپیوتر که Token را در اختیار داشته باشد در صورت نیاز به ارسال، داده خود را ارسال می‌کند و در غیر این‌صورت Token را به کامپیوتر بعدی تحویل می‌دهد. General Motors اصرار داشت که برای خط تولید اتومبیل حتماً از این روش استفاده شود و روش مبتنی بر تصادم و تصادفی Ethernet قابل اعتماد نیست.

۳ـ۱ـ۷ حلقه توکن یا Token Ring

این روش توسط IBM ابداع شد و دقیقاً مانند Token Bus عمل می‌کرد با این تفاوت کوچک که در حلقه Token، کابل شبکه یک مسیر بسته (Ring) را تشکیل می‌داد. استاندارد IEEE 802.5 برای همین منظور بنا نهاده شد.

امروزه اثری از Token Bus وجود ندارد (بر خلاف ادعای General Motors) و به ندرت از Token Ring استفاده می‌شود. نوع خاصی از Token Ring به نام FDDI که با فیبر نوری کار می‌کردگاهی به عنوان Backbone یا ستون فقرات شبکه‌های محلی استفاده می‌شد اما به علت گرانی تجهیزات هرگز به عنوان شبکه کامپیوترهای Desktop مورد استفاده قرار نگرفت.

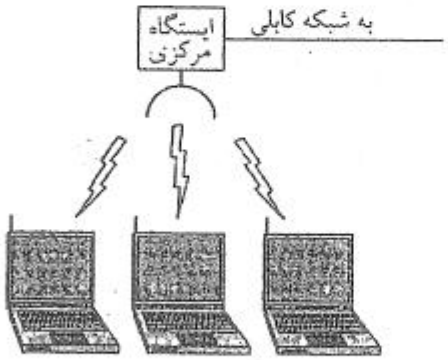
اگرچه امروزه تلاش‌هایی در جهت توسعه Token Ring سریع گیگابیتی انجام می‌شود و استاندارد IEEE 802.5v برای آن پایه گذاری شده است اما بعید به نظر می‌رسد بتواند با نسخه‌های جدید اترنت (Gigabit Ethernet , Fast Ethernet و 10 Gigabit Ethernet) رقابت نماید. بنابراین نتیجه می‌گیریم که در مهندسی هر چه ساده و ارزان طراحی کنیم بهتر است. به این دلیل به اترنت DIX می‌گوییم چون سه شرکت DEC-Intel-Xerox در ایجاد آن دخالت داشتند.

تفاوت‌های جزئی بین DIX و IEEE 802.3 وجود دارد که مورد بررسی قرار خواهند گرفت.

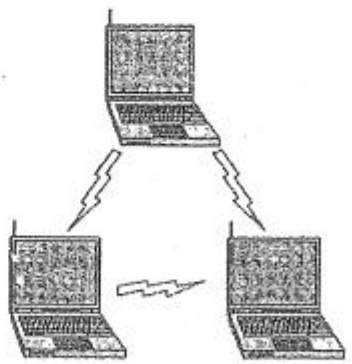
۴ـ۱ـ۷ شبکه‌های محلی بی‌سیم یا Wireless LAN

با رشد کامپیوترهای کتابی، نیاز به شبکه‌های محلی بی‌سیم با ارتباط رادیویی برد کوتاه روز به روز بیشتر احساس می‌شد و شبکه‌های متنوعی در این راستا طراحی شد. IEEE برای جلوگیری از هرج و مرج، یک استاندارد بنام 802.11 بنا نهاد که در میان مردم بنام WiFi مشهور است. این استاندارد در دو حالت کار می‌کند:

- وجود یک ایستگاه مرکزی به‌نام نقطه دسترسی (Access Point) که همه کامپیوترها از طریق آن با یکدیگر ارتباط برقرار می‌کنند. به شکل الف نگاه کنید.
- عدم وجود یک ایستگاه مرکزی و ارتباط مستقیم کامپیوترها با یکدیگر. به شکل (ب) نگاه کنید.



(الف)


(ب)

مهم‌ترین مسائل مطرح در این استاندارد عبارتند از:

۱) انتخاب باند فرکانسی مناسب

۲) محدود بودن برد امواج رادیویی

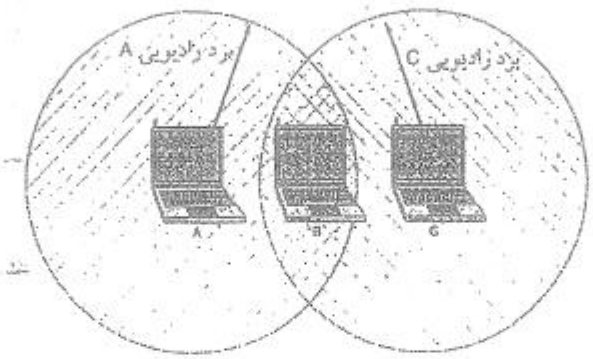
۳) مسائل بهداشتی و تاثیر امواج الکترومغناطیسی بر سلامت انسان

۴) سیار بودن کامپیوترها و جابجایی آن‌ها و ورود به محیط‌های جدید.

۵) سازگاری با اترنت از نظر ایجاد واسط یکسان به‌منظور ارائه سرویس به لایه بالاتر (مانند IP)

مهم‌ترین مشکلات طراحی شبکه‌های بی‌سیم

۱) گوش دادن به رسانه انتقال (شنود کانال) و تشخیص خالی بودن آن پیچیده‌تر از اترنت است. برای مثال فرض کنید کامپیوترهای A و C هر دو در برد رادیویی کامپیوتر B هستند اما کامپیوتر A در برد رادیویی کامپیوتر C نیست. اگر A بخواهد با B ارتباط برقرار کنند چگونه می‌تواند اطمینان حاصل کند که C در حال ارسال اطلاعات به B نمی‌باشد؟



۲) انعکاس یا Echo امواج رادیویی توسط اجسام سخت و تداخل امواج باعث می‌شود که امواج از چندین مسیر مختلف و در زمان‌های مختلف به گیرنده رسیده و تداخل نمایند. این مشکل را محو شدگی چند مسیره (Multipath Fading) می‌گویند.

۳) ناسازگاری برخی نرم‌افزارها با جابجایی کامپیوترها و ورود به محیط‌های جدید با دستگاه‌های جانبی جدیدا

۴) خروج یک کامپیوتر از یک سلول (محدودهٔ برد یک ایستگاه مرکزی) و ورود به یک سلول دیگر. البته یک راه‌حل این مشکل این است که ایستگاه‌های مرکزی را با اترنت به هم وصل نمائیم.

تعریف : نقطه اتصال شبکه محلی بی‌سیم به دنیای خارج (مثلاً یک Gateway) را درگاه (Portal) می‌نامند.

نرخ انتقال در استاندارد 802.11 یک تا دو مگابیت در ثانیه بود. در نتیجه IEEE دو کمیته را برای ایجاد استانداردهای جدید با سرعت بیشتر مامور کرد و نتیجه کار آن‌ها استانداردهای 802.11a و 802.11b بود.

نکته ۱: استاندارد 802.11a با نرخ انتقال 54 Mbps از باند فرکانسی وسیع‌تری استفاده می‌کرد.

نکته ۲: استاندارد 802.11b با نرخ انتقال 11 Mbps با همان باند فرکانسی قبلی اما با مودولاسیون‌های خاص جدید کار می‌کرد.

نکته ۳: استاندارد 802.11g در باند فرکانسی 802.11b ولی با مدولاسیون 802.11a کار می‌کند تا تنوع استانداردها بیشتر شود.

۲ـ۷ آنالیز کنترل دسترسی به کانال در پروتکل‌های مختلف MAC

نکته اصلی کنترل دستیابی به رسانه‌این است که تخصیص کانال را پویا در نظر بگیریم یا از روش‌های ایستا استفاده کنیم؟ تحلیل زیر نشان می‌دهد که روش‌های ایستا راندمان یا بهره کانال را به شدت کاهش داده و قابل استفاده نیستند.

از آن‌جا که در MAC، فریم‌ها در زمان‌های تصادفی و با اندازه‌های تصادفی تولید می‌شود لذا تحلیل آن‌ها پیچیده است و نیاز به آشنایی با تئوری صف (Queuing Theory) دارد. ما در این‌جا از نتایج تحلیل تئوری صف استفاده می‌کنیم.

قضیه: در تئوری صف اثبات می‌شود که اگر در یک صف ورود نهادها تصادفی و با توزیع پواسون (Poisson) با میانگین λ باشد و مدت زمان سرویس‌دهی به نهادها تصادفی و با توزیع نمایی و میانگین $\frac{1}{\mu}$ (نرخ سرویس μ) باشد آن‌گاه میانگین زمان انتظار در صف (تاخیر صف) از رابطه زیر بدست می‌آید:

$$T = \frac{1}{\mu - \lambda}$$

مثال : فرض کنید یک شبکه در لایه MAC خود از FDM استفاده کند. می‌خواهیم ببینم چرا راندمان پایین است؟ برای پاسخ به این پرسش نرخ ارسال را R فرض کنید و فرض کنید که N کامپیوتر جمعاً (روی هم) فریم‌ها را با نرخ متوسط λ فریم در ثانیه ارسال می‌کنند. اگر طول هر فریم، تصادفی و با توزیع نمایی و میانگین $\frac{1}{\mu}$ فرض شود تاخیر انتظار را در دو روش تخصیص ایستا و پویا با هم مقایسه کنید؟

الف) تخصیص پویا

λ = نرخ ورود بسته‌ها

Poisson : تابع توزیع ورود بسته‌ها

$= \frac{1}{\mu}$ میانگین اندازه فریم

$= \frac{1}{R}$ میانگین زمان ارسال یک بیت

$= \frac{1}{\mu} \times \frac{1}{R}$ میانگین زمان ارسال فریم‌ها = میانگین یا متوسط زمان سرویس

$= \mu R$ میانگین نرخ سرویس

$\boxed{= T_{Dynamic} = \frac{1}{\mu R - \lambda}}$ میانگین زمان انتظار یک فریم در صف

ب) تخصیص ایستا

در این حالت ما نرخ انتقال را بین N کامپیوتر تقسیم می‌کنیم (FDM)

$= \frac{\lambda}{N}$ متوسط نرخ ورود بسته از هر کامپیوتر

$= \frac{R}{N}$ متوسط نرخ ارسال برای هر کامپیوتر

$= \mu \frac{R}{N}$ میانگین نرخ سرویس

$$T_{Static} = \frac{1}{\frac{\mu R}{N} - \frac{\lambda}{N}} = \frac{N}{\mu R - \lambda} \Rightarrow T_{Static} = N.T_{Dynamic}$$

تاخیر در تخصیص ایستا N برابر بیشتر از تخصیص پویا می‌شود، لذا Bus را به صورت ایستا تقسیم نمی‌کنیم. به عبارت دیگر، در MAC نباید پهنای باند را تقسیم کنیم و همه باید از یک باند به‌طور مشترک و پویا استفاده کنند. این نتیجه برای TDM هم صادق است.

مثال : اگر R=100Mbps (برای کل کانال) و متوسط طول فریم‌ها $\left(\frac{1}{\mu}\right)$ برابر 10000 bit و متوسط نرخ تولید فریم‌ها $5000 \frac{frame}{s}$ باشد متوسط تاخیر صف، متوسط تاخیر انتقال و تاخیر انتشار یک فریم را در یک کانال به طول 2Km برای حالت‌های زیر بدست آورید؟

الف) تخصیص پویا ب) روش تخصیص ایستا با 10 کامپیوتر

- تخصیص پویا :

$$= T_Q = \frac{1}{10^{-4} \times 10^8 - 5 \times 10^3} = 200\mu S \quad \text{متوسط تاخیر انتظار در صف}$$

$$\frac{L \text{ (اندازه فریم)}}{R} \quad = \frac{\frac{1}{\mu}}{R} = \frac{10^4}{10^8} = 10^{-4} \sec = 100\mu S \quad \text{= متوسط تاخیر انتقال (برای فرستادن روی خط)}$$

تاخیر انتشار (برای رسیدن به مقصد) (حداکثر) $= \frac{D}{V} = \frac{2\times10^3}{3\times10^8} = \frac{2}{3}\times10^{-5} = 6.66\mu S$

- تخصیص ایستا:

$T_Q = 10\times200\mu S = 2m\sec$

متوسط تاخیر انتقال $= \frac{\frac{1}{\mu}}{\frac{R}{N}} = \frac{10^4}{\frac{10^8}{10}} = 10^{-3}\sec = 1000\mu S = 1ms$

حداکثر تاخیر انتشار = $6.66\mu S$

۱ـ۲ـ۷ تخصیص پویای کانال

مفروضات ما برای تحلیل حالت پویا به شرح زیر است:

الف) N ایستگاه داریم که روی هم فریم‌ها را با توزیع پواسون و میانگین λ ارسال می‌کنند. احتمال این‌که در بازه کوچک Δt یک فریم ارسال شود $\lambda\Delta t$ خواهد بود.

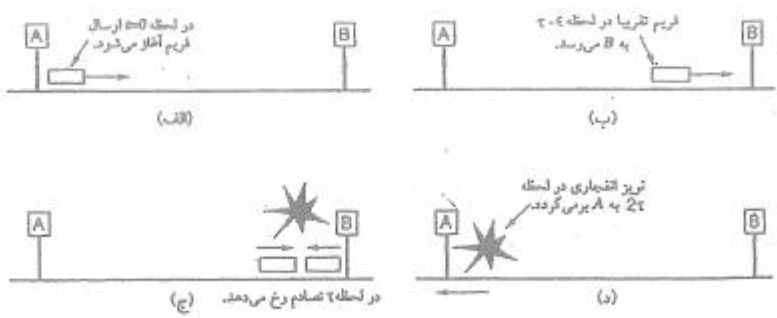
ب) یک کانال منفرد داریم که به طور اشتراکی استفاده می‌کنیم.

ج) احتمال وقوع تصادم (Collision) وجود دارد. به دو دلیل زیر تصادم پیش می‌آید:

۱) دو ایستگاه همزمان به خط گوش می‌دهند و هر دو آن را آزاد می‌یابند و با هم فریم خود را روی خط قرار می‌دهند.

نکته : اگر حتی همزمان این اتفاق نیفتد، باز هم احتمال تصادم وجود دارد. به شکل زیر دقت کنید.

فرض کنید تاخیر انتشار در کل کانال برابر $\tau = \frac{D}{V}$ باشد و ایستگاه A در یک سر کانال و B در سر دیگر آن باشد. اگر ایستگاه A در لحظه صفر کانال را آزاد ببیند و فریم خود را بر روی خط بگذارد و ایستگاه B در لحظه $\tau-\varepsilon$ به خط گوش دهد خط را آزاد می‌بیند و اطلاعات خود را روی خط می‌گذارد حال سوال این است که ایستگاه A در چه لحظه‌ای متوجه تصادم می‌شود؟ پاسخ 2τ است. بنابراین بازه تشخیص تصادم 2τ می‌باشد. این زمان را (Round Trip Time) یا RTT می‌نامند و در واقع زمان رفت و برگشت سیگنال بر روی خط است.



۲) فرض کنید که دو ایستگاه همزمان کانال (حامل) را شنود نمایند (Carreir Sense) و آن را مشغول یابند. اگر هر دو در ادامهٔ شنود برای ارسال اصرار ورزند (Persistant)، هر گاه خط آزاد شود مطمئناً دو ایستگاه همزمان فریم خود را بر روی خط گذاشته و تصادم رخ می‌دهد.

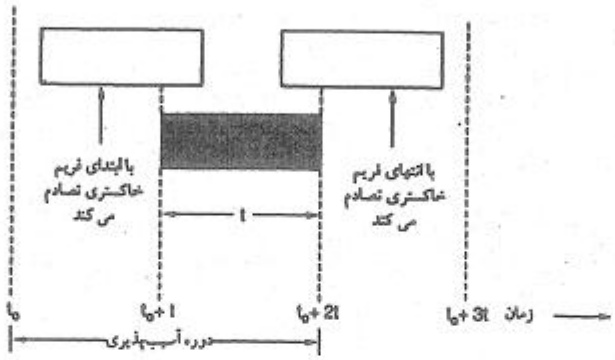
د) دو مدل زمانی برای ارسال فریم‌ها وجود دارد.

۱) مدل زمان پیوسته (Continuous Time) : در این مدل هر وقت که فرستنده اراده کند می‌تواند ارسال را آغاز نماید.

۲) مدل زمان گسسته (Discrete Time) : در این روش برشهای زمانی داریم و فقط می‌توان در شروع Time Slot شروع به ارسال فریم نمود.

نکته : روش دوم بهتر است زیرا احتمال تصادم نصف می‌شود.

در روش اول بسته ممکن است با دو بسته دیگر تصادم داشته باشد اما در روش دوم تنها با بسته‌هایی که در همان فضای یک برابر برش زمانی خودش آغاز می‌شوند، تصادم پیدا می‌کند. به شکل زیر نگاه کنید.



هـ) دو روش برای ارسال فریم وجود دارد:

۱) شنود خط و ارسال در صورت آزاد بودن خط (Carreir Sense)

۲) عدم شنود به خط و ارسال تصادفی (No Carreir Sense)

نکته : نتیجه این‌که بهترین و کاراترین روش، شنود کانال و کشف تصادم و استفاده از روش Slotted و نیز عدم اصرار بر گوش دادن به کانال مشغول می‌باشد و در مقابل بدترین روش، ارسال تصادفی بدون شنود کانال و عدم کشف تصادم و اصرار بر ارسال مجدد می‌باشد (مانند شبکه Pure ALOHA که جد همه روش‌های MAC است.)

۲ـ۲ـ۷ انواع پروتکل‌های MAC

دراین بخش، انواع مختلف پروتکل‌های به‌کار رفته در زیر لایهٔ MAC را مورد بررسی قرار می‌دهیم.

ALOHA ۷ـ ۲ـ۲ـ۱

قدیمی‌ترین پروتکل MAC مربوط به سال 1970 می‌شود که نورمن آبرانسون در دانشگاه هاوایی شبکه‌ای به نام ALOHA طراحی و پیاده‌سازی کرد که مبتنی بر پخش امواج رادیویی زمینی بود. در این روش فرستنده در هر زمان که بخواهد فریم خود را ارسال می‌کند و با توجه به این‌که شنود امواج الکترومغناطیسی مشکلات خاص خود را دارد (مثلاً در ارتباط ماهواره‌ای 270 ms طول می‌کشد که متوجه تصادم شویم که البته در این مدت چندین فریم را می‌توان ارسال کرد.) باید فریم را به صورت تصادفی ارسال کرد و برای اطمینان از صحت ارسال به Acknowledge توجه داشت و منتظر رسیدن آن شد. این روش به دلیل عدم شنود خط و اصرار بر ارسال مجدد، راندمان بسیار پائینی دارد.

تحلیل آماری نشان می‌دهد که احتمال ارسال K فریم در بازه زمانی t (زمان ارسال یک فریم دیگر) از توزیع پواسون پیروی می‌کند:

$$P_r[K]=\frac{G^k e^{-G}}{K!}$$

G متوسط تولید فریم جدید در واحد زمان (همان بازهٔ زمانی t) می‌باشد. (هم فریم‌های اصلی و هم فریم‌های ارسال مجدد در اثر تصادم در نظر گرفته می‌شود).

بازده کانال که برابر با حاصل‌ضرب میزان بار (G) در احتمال موفقیت در ارسال (عدم تصادم) می‌باشد که این احتمال از رابطه زیر بدست می‌آید:

احتمال موفقیت در ارسال $= P_r[0] = e^{-G}$

البته این در روش Slotted ALOHA صادق است. اما در Pure ALOHA احتمال موفقیت در ارسال که احتمال عدم تصادم در بازهٔ زمانی 2t است، از رابطه زیر بدست می‌آید:

احتمال موفقیت در ارسال $= e^{-2G}$

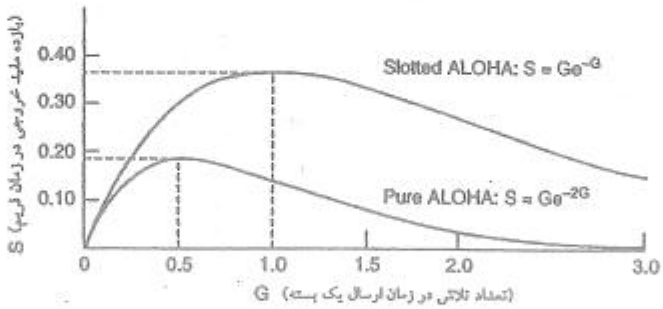
بنابراین بازده (راندمان) کانال در روش ALOHA از رابطه زیر بدست می‌آید:

$$U_{ALOHA} = Ge^{-2G}$$

همیشه راندمان کانال در Slotted ALOHA به صورت زیر خواهد بود:

$$U_{Slotted\ ALOHA} = Ge^{-G}$$

شکل زیر نشان می‌دهد که در Pure ALOHA بهترین حالت مربوط به G= 0.5 می‌باشد که نشان می‌دهد حداکثر راندمان ALOHA برابر $\frac{1}{2e}$ (تقریباً برابر 0.18) است و در Slotted ALOHA بهترین حالت مربوط به G=1 است و حداکثر راندمان آن برابر با $\frac{1}{e}$ (تقریباً برابر 0.36) می‌باشد.



دسته دیگری از پروتکل‌هایی MAC وجود دارند که بر اساس شنود کانال عمل می‌کنند و در ادامه مورد بحث قرار می‌گیرند.

۲-۲-۲-۷ CSMA (Carreir Sense Multiple Access)

مشکل اصلی ALOHA راندمان پایین آن بود. تفاوت پروتکل CSMA با ALOHA در این است که به خط گوش می‌دهد تا چنانچه خط مشغول است فریم خود را ارسال نکند. این عمل راندمان کانال را به صورت موثر افزایش می‌دهد.

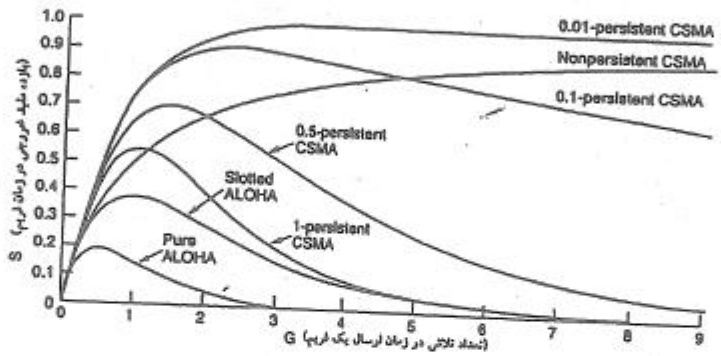
سه نوع پروتکل CSMA وجود دارد.

۱) 1- Persistant CSMA : یعنی به خط گوش می‌دهیم و چنانچه آزاد باشد بدون قید و شرط (صد درصد و با احتمال 1) فریم خود را ارسال می‌کنیم.

۲) Nonpersistant CSMA : در این روش به خط گوش می‌دهیم، چنانچه مشغول باشد خط را رها کرده و به یک مدت تصادفی کنار می‌کشیم و پس از طی آن دوره زمانی مجدداً به خط گوش می‌دهیم.

بدین ترتیب احتمال تصادم کاهش یافته و راندمان بسیار بهتر از 1- Persistant می‌شود.

۳) p – Persistant CSMA : این پروتکل CSMA به صورت Slotted Time عمل می‌کند. در این روش، قبل از فاز ارسال، یک فاز رقابتی داریم که در آن ایستگاه‌های کاری برای ارسال با یکدیگر به رقابت می‌پردازند. این فاز رقابتی از چندین برش زمانی (پنجرهٔ زمانی) تشکیل می‌شود. اگر یک ایستگاه کاری بخواهد یک فریم را ارسال نماید، در شروع هر پنجرهٔ زمانی عمل شنود کانال را انجام می‌دهد و چنانچه کانال را آزاد بیابد، با احتمال p اقدام به ارسال می‌کند و با احتمال q = 1 – p ارسال نمی‌کند و کنار می‌کشد و تا شروع پنجره زمانی بعدی صبر می‌کند و مجدداً کانال را شنود می‌کند. این فرآیند آن‌قدر تکرار می‌شود تا این‌که فریم ارسال شود یا ایستگاه دیگری ارسال خود را آغاز نماید. چنانچه هنگام شنود کانال در فاز رقابتی، کانال را مشغول بیابد، ایستگاه ناموفق، مانند حالتی که تصادم رخ داده عمل می‌کند و به اندازه یک مدت زمان تصادفی صبر می‌کند و دوباره شروع می‌کند. شکل زیر بازده یا بهره کانال را برای پروتکل‌های مختلف بر حسب بار نشان می‌دهد.



۳_۲_۲_۷ CSMA / CD (Carreir Sense Multiple Access with Collision Detection)

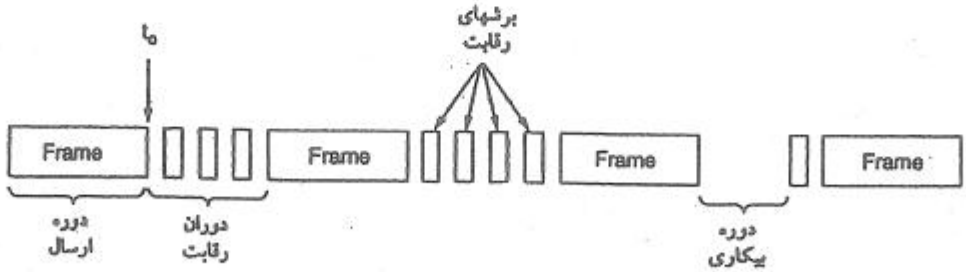
بهبود دیگر در CSMA این است که پس از این‌که خط را آزاد دیدیم و فریم خود را بر روی خط گذاشتیم به شنود ادامه دهیم تا مطمئن شویم تصادم رخ نداده است. در صورت وقوع تصادم بلافاصله کنار بکشیم و یک مدت تصادفی (که الگوریتم آن را مطالعه خواهیم کرد) صبر کنیم و مجدداً به خط گوش دهیم.

در این پروتکل سیستم‌ها در یکی از سه وضعیت زیر قرار دارند (به شکل زیر نگاه کنید):

۱) فاز رقابتی

۲) فاز ارسال

۳) فاز بیکاری ← هیچ کس علاقه به ارسال ندارد.



نکته ۱: یک ایستگاه کاری پس از قرار دادن فریم خود بر روی خط تا چه مدت موظف به شنود خط است تا مطمئن شود تصادفی رخ نداده است؟

جواب : $RTT = 2\tau$

نکته ۲: کشف تصادم در CSMA / CD بر عهده کدام مرجع است؟ بر عهده یک مدار الکترونیکی آنالوگ به نام Tranciever است که به‌خط گوش می‌دهد و از روی افزایش توان متوجه تصادم می‌شود. البته روش کدینگ خاصی بنام منچستر با ولتاژهای مثبت و منفی 0.85± ولت در اترنت استفاده می‌شود که به کشف تصادم کمک می‌نماید.

نکته ۳: پروتکل CSMA / CD هیچ کمکی به کشف و کنترل خطا نمی‌کند. اگرچه Collision ها کشف می‌شود اما بدون وقوع Collision هم به دلایلی چون نویز، تضعیف و اعوجاج و غیره امکان وقوع خطا وجود دارد. به عبارت دیگر ارسال ACK از وظایف زیر لایه MAC نیست. (LLC کنترل خطا را بر عهده دارد.)

نکته ۴: کنترل خطا و مهم‌تر از آن تطبیق پروتکل‌های مختلف MAC با لایه شبکه و یکسان جلوه دادن پروتکل‌هایی نظیر Wireless LAN و Ethernet به لایه شبکه (مثلاً IP) از وظایف زیر لایه LLC است که بر روی MAC قرار دارد.

۳ـ۷ اترنت (Ethernet)

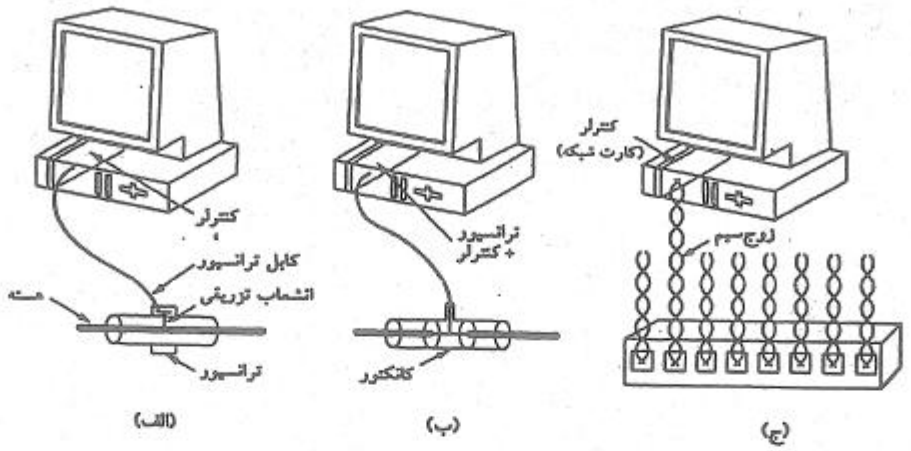
در این‌جا می‌خواهیم اترنت را با جزئیات کامل مورد بررسی قرار دهیم. در ابتدا ذکر این نکته ضروری است که پروتکل اولیه اترنت که نام سه شرکت DEC – Intel – Xerox (DIX) بر روی آن نهاده شده است دو تفاوت جزئی با استاندارد IEEE 802.3 دارد که البته IEEE در سال 1997 با این موضوع کنار آمد و DIX را هم پذیرفت.

۱ـ۳ـ۷ کابل‌کشی اترنت

اترنت اولیه که با سرعت 2.94Mbps کار می‌کرد خیلی زود منسوخ شد و در استاندارد DIX به سرعت 10Mbps ارتقاء یافت. جدول زیر چهار نوع کابل‌کشی را در استاندارد DIX نشان می‌دهد.

مزایا	تعداد گره در هر قطعه	حداکثر طول کابل در یک قطعه	نوع کابل	نوع اتصال	نام کابل
کابل اصلی و اولیه (منسوخ شده)	100	500 m	Thick coax	انشعاب تزریقی (پیچیده)	10Base 5
عدم نیاز به Hub	30	185 m	Thin coax	کانکتور T شکل و BNC (ساده و ارزان)	10Base 2
ارزان (و به Hub یا Switch نیاز داریم.)	1024	100 m	Twisted pair	اتصال مستقیم ایستگاه‌ها به پورت Hub یا Switch	10Base-T
امنیت ـ اطمینان ـ فاصله دور (در این‌جا هم نیاز به Hub یا Switch داریم)	1024	2000m	Fiber optics	اتصال مستقیم ایستگاه‌ها به پورت‌های Hub یا Switch	10Base-F

در نام‌گذاری روش‌های کابل‌کشی DIX، عدد 10 نشان‌دهنده سرعت شبکه (10Mbps)، کلمه Base به معنی استفاده از سیگنالینگ باند پایه (Baseband) است. اعداد 2 و 5 حداکثر تقریبی طول قطعه را بر حسب 100 متر نشان می‌دهند و حروف T و F به‌ترتیب معرف Twisted Pair و Fiber Optics می‌باشند.



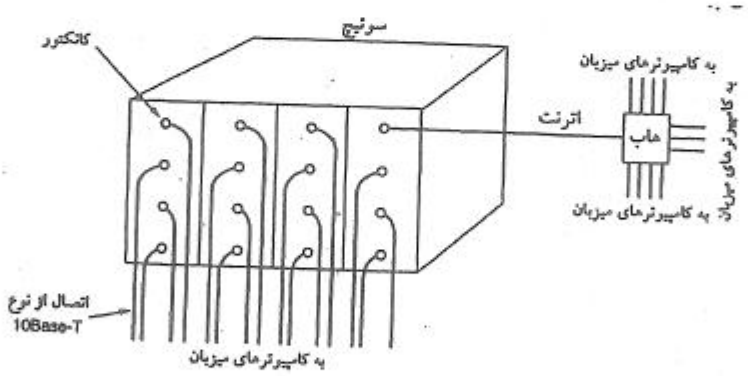
نکته : تفاوت Hub و Switch در چیست؟

تنها وظیفه Hub، اتصال الکتریکی ایستگاه‌های متصل به پورت‌های Hub است. به عبارت دیگر Hub فقط نقش یک Bus را بازی می‌کند و یک حوزه تصادم (Collision Domain) است.

اما سوییچ‌ها دو ویژگی خاص دارند:

۱) برای افزایش Scalability یا قابلیت توسعه شبکه محدودیت تعداد ایستگاه‌ها را از بین می‌برند. بدین طریق که در درون یک سوییچ یک یا چند Backplane وجود دارد که با تکنولوژی خاصی (که ربطی به اترنت ندارد) کار می‌کند و پورت‌های ورودی سوییچ را با سرعت چند گیگابیت در ثانیه به هم متصل می‌کنند. در سوییچ‌ها عمل Forwarding داریم.

۲) سوییچ‌ها قابلیت بافر کردن فریم‌ها را در حافظه درون سوییچ دارند. بدین ترتیب در درون سوییچ تصادم رخ نمی‌دهد، لذا سوییچ حوزه تصادم نیست.



مثال : کدام یک از گزینه‌های زیر صحیح است؟

۱) حوزه تصادم در Hub، خود Hub و در سوییچ Backplaen است.

۲) حوزه تصادم در Hub و سوییچ Backplane است.

۳) حوزه تصادم در Hub، خود Hub و در سوییچ، پورت است.

۴) حوزه تصادم در Hub و سوییچ، پورت است.

پاسخ صحیح، گزینه ۳ می‌باشد.

نکته : مسائل مربوط به کدبندی، سطوح ولتاژ، مسائل الکتریکی، کانکتورها، پورتها، کابلها و غیره، لایه فیزیکی DIX یا اترنت را تشکیل می‌دهند که موردبحث قرار گرفت. اما مسائلی همچون فریمینگ و فیلدهای تشکیل دهنده فریم‌ها و پروتکل CSMA/CD، زیر لایه MAC از لایه پیوند داده را تشکیل می‌دهند که می‌خواهیم مسائل مربوط به آن را دقیقاً بررسی کنیم.

۲ـ۳ـ۷ پروتکل زیر لایه MAC در اترنت

در این بخش می‌خواهیم، مسائل مربوط به لایه فیزیکی و حوزه مهندسی الکترونیک را کنار گذاشته و مسائل مربوط به لایه پیوند داده در حوزه مهندسی کامپیوتر را مورد بررسی قرار دهیم.

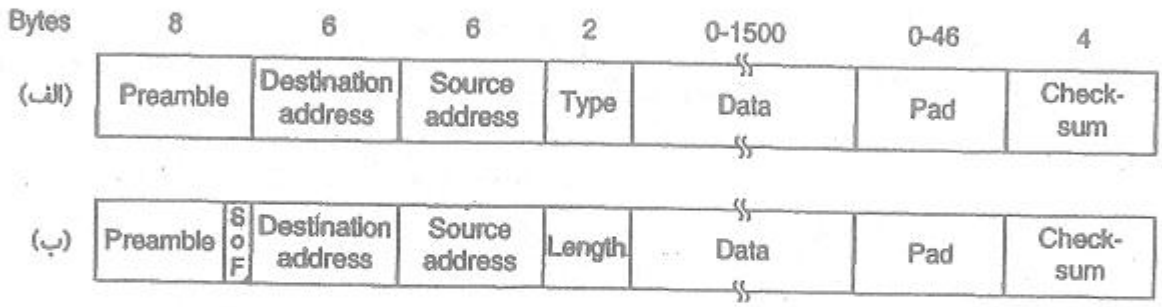
۱ـ ۲ـ۳ـ۷ قالب (Format) فریم در اترنت

شکل زیر قالب یک فریم اترنت را در DIX و IEEE 802.3 نشان می‌دهد.

نکته : همان‌طور که در شکل دیده می‌شود استاندارد IEEE فقط دو تفاوت کوچک با DIX دارد:

۱) یک بایت آخر Preamble برای همگام سازی در شروع فریم است.

۲) به جای Type از Length یا طول بخش داده فریم استفاده شده است. در این صورت پیشنهاد شده است که نوع فریم به عنوان دو بایت اول بخش داده منظور گردد.



معرفی فیلدها:

۱) Preamble : مقدمه یا دیباچه : 8 بایت یا 64 بیت با الگوی .....101010 در ابتدای فریم که با کدبندی منچستر ارسال می‌شود و به مدت 6.4 میکروثانیه یک موج مربعی با فرکانس 5MHz تولید می‌کند (با توجه به نرخ 10 Mbps اترنت اولیه) که برای همگام سازی ساعت (Clock) فرستنده و گیرنده به کار می‌رود.

۲) آدرس مبدأ و مقصد: در استاندارد اولیه پیشنهاد شده است که این آدرس 2 یا 6 بایت باشد ولی بعداً مقرر گردید که فقط آدرس‌های 6 بایتی (48 بیتی) مورد استفاده قرار گیرد. سه نوع آدرس در اترنت مورد استفاده قرار می‌گیرد:

الف) آدرس نقطه به نقطه یا تک پخشی: اگر بیت با ارزش (MSB) صفر باشد آن آدرس آدرس، یک کارت شبکه (NIC) خاص و منحصر به فرد در دنیا می‌باشد. این آدرس توسط کارخانه سازنده به صورت سخت‌افزاری گذاشته می‌شود. اسم این آدرس MAC Address است.

ب) آدرس چندپخشی یا Multicast : اگر بیت با ارزش یا (MSB) یک باشد 64 بیت باقیمانده یک آدرس گروهی را مشخص می‌کند و فریم ارسالی توسط یک گروه از ایستگاه‌های کاری برداشته می‌شود.

نکته : اترنت از Multicasting پشتیبانی می‌کند.

ج) آدرس انتشاری یا Broadcast : اگر همه بیت‌های آدرس مقصد یک باشد، به معنای آن است که این فریم باید توسط همه کارت‌های شبکه برداشته شود و به لایه بالاتر تحویل داده شود.

نکته : بیت مجاور MSB یا بیت 46 ام، سراسری یا محلی بودن آدرس‌ها را مشخص می کند. آدرس محلی، آدرسی است که در درون LAN توسط Supervisor مشخص می‌شود ولی آدرس سراسری در دنیا منحصر به‌فرد است. 64 بیت باقیمانده (به‌غیر از بیت باارزش و بیت مجاور آن) فضایی معادل 2^{64} (حدود 7×10^{13}) آدرس سراسری را ایجاد می‌کنند.

نکته : دو نوع آدرس به کارت شبکه می‌توان داد :

- آدرس جهانی که به‌صورت سخت‌افزاری قرار داده شده و ثابت است.
- آدرس محلی که به صورت نرم‌افزاری داده می‌شود و قابل تغییر است.

۳) فیلد **Type** : نوع فریم را مشخص می‌کند. از آن‌جا که در هسته سیستم عامل ممکن است چندین پروتکل لایه شبکه اجرا شود و همچنین فرآیندهای مختلفی در حال اجرا باشند، در این فیلد مشخص می‌شود که فریم دریافتی باید به کدام فرآیند تحویل داده شود.

۴) فیلد **Data** : محتوای اصلی داده‌های درون فریم در این‌جا قرار می‌گیرد. (داده‌هایی که از لایه شبکه دریافت شده است.)

داده می‌تواند از 0 تا 1500 بایت باشد. (وقتی صفر است که بخواهیم یک سیگنال کنترلی بفرستیم و داده‌ای در کار نیست.)

نکته ۱ : طول یک فریم مقصد حداقل 64 بایت باید باشد. چرا؟

$$\text{حداقل طول فریم} = L = 64\times8 = 512\text{bit} \Rightarrow \text{حداقل زمان انتقال فریم} = \frac{L}{R} = \frac{512}{10^7} = 51.2\mu S$$

از طرف دیگر طول حداکثر کابل در اترنت 2500 متر است و زمان انتشار رفت و برگشت یک فریم برابر است با:

$$\tau = \frac{2500}{3\times10^8} = 8\mu s \qquad \Rightarrow RTT = 2\tau = 16\mu s$$

زمان انتقال فریم باید بزرگتر از حداکثر زمان رفت و برگشت فریم (شامل حداکثر تاخیر انتشار رفت و برگشت به‌علاوه تاخیر حداکثر چهار تکرار کننده در دو جهت) باشد؛ زیرا در غیر این صورت بعد از تمام ارسال فریم، دیگر کارت شبکه متوجه تصادم نخواهد شد.

$$\text{حداکثر زمان رفت و برگشت} = 16\mu s + 8x = 50$$

(x زمان تاخیر تکرار کننده‌ها می‌باشد)

با توجه به این‌که سرعت انتقال 10Mbps است در $50\mu s$، 500 بیت ارسال می‌شود. استاندارد برای اطمینان بیشتر 512 بیت معادل 64 بایت را به‌عنوان حداقل تعداد بایت در یک فریم در نظر گرفته است. لذا طول قسمت داده حداقل باید 64 بایت باشد (فیلد Preamble در محاسبات شرکت نمی‌کند و مابقی فیلدها 18 بایت می‌شود)

۵) فیلد **Pad** : اگر فیلد داده شما از 64 بیت کمتر باشد، باید آن‌قدر بایت زائد در Pad اضافه ارسال شود تا طول کل فریم 64 بایت شود. (بدون احتساب Preamble که برای سنکرون کردن است و جز فریم محسوب نمی‌شود.)

۶) فیلد **Checksum** : در اترنت Checksum از نوع CRC در نظر گرفته شده است که قادر به تشخیص خطا است (و نه تصحیح آن). البته در عمل، اترنت مساله تصحیح خطا به کمک Acknowledge را پشتیبانی نمی‌کند و این موضوع به LLC مربوط است. به عبارت دیگر، فریمی که MAC به LLC می‌دهد حتی در صورت عدم بروز تصادم ممکن است حاوی خطا باشد.

IEEE در سال 1997 استاندارد DIX را پذیرفت و اعلام کرد اگر در فیلد Length عددی کوچکتر یا مساوی 1500 قرار داشته باشد به معنای طول فریم است و در غیر این صورت به معنای نوع فریم می‌باشد.

نکته : محاسبات فوق مربوط به اترنت 10 Mbps بود حال فرض کنید اگر در اترنت 1Gbps بخواهیم طول کابل را 2500 متر نگه داریم، حداقل اندازه فریم چقدر می‌شود؟ 6400 byte ! یعنی اگر بخواهیم یک بایت داده بفرستیم باید مقدار بسیار زیادی داده اضافی بیهوده ارسال کنیم.

۲ـ ۲ـ ۳ـ ۷ الگوریتم Binary Exponential Backoff (الگوریتم عقبگرد نمایی دودویی)

۱) فرستنده به خط گوش می‌دهد، دو حالت زیر ممکن است پیش بیاید:

- اگر خط مشغول بود عقبگرد می‌کند و یک مدت تصادفی که مضربی از برش زمانی به طول 2τ می‌باشد صبر می‌کند و مجدداً برگشته و به خط گوش می‌دهد. این مدت تصادفی طبق الگوریتم عقبگرد نمایی دودویی محاسبه می‌شود.
- در غیر این صورت، یعنی اگر خط آزاد است، داده خود را ارسال می‌کند و البته موظف است تا یک برش زمانی (2τ) همزمان با ارسال به خط گوش دهد تا تصادم را تشخیص دهیم (Collision Detect / CD)

نکته : هر گاه یک ایستگاه تصادم را تشخیص دهد وظیفه دارد، یک نویز با توان بالا به مدت 48 بیت بر روی کانال قرار دهد تا همه ایستگاه‌ها متوجه تصادم شوند.

الگوریتم عقبگرد نمایی دودویی به شرح زیر است: (زمان عقبگرد چه در حالت شلوغی خط و چه در صورت تصادم با این الگوریتم محاسبه می‌شود.)

۱) اگر اولین بار باشد که تصادم رخ داده است، یک عدد تصادفی (0 یا 1) تولید می‌کند (50% احتمال دارد 0 و 50% احتمال دارد 1 تولید شود.) و به اندازه $0\times 2\tau$ یا $1\times 2\tau$ صبر می‌کند و بر می‌گردد. و دوباره به خط گوش می‌دهد.

۲) اگر دوباره تصادم رخ داد، یک عدد تصادفی (بین 0 , 1 , 2 , 3) تولید می‌کند و بین 0τ تا 6τ صبر می‌کند.

۳) در سومین تصادم متوالی، عدد تصادفی (بین 0 تا 7) و مدت انتظار 0τ تا 14τ خواهد بود.

نکته : این‌کار تا 10 تصادم متوالی ادامه می‌یابد. در تصادم 10 ام عدد تصادفی بین 0 تا 1023 خواهد بود، یعنی بین 0τ تا 2046τ صبر می‌کند.

نکته ۱: زمان عقبگرد به صورت نمایی افزایش می‌یابد. (0، 2، 4، 8 و غیره)

نکته ۲: اگر باز هم تصادم رخ دهد، تا 6 مرتبه دیگر اما با همین زمان (0 تا 1023) صبر می‌کند. اما 16 تصادم پیاپی به معنای مشکل اساسی یا جدی (Fatal Error) تلقی شده و الگوریتم Crash می‌کند و به لایه بالاتر اعلام می‌شود که شبکه خراب است.

۳ـ۲ـ۳ـ۷ بازده یا بهره اترنت

اگر در مرحله رقابت با احتمال P اقدام به ارسال فریم نماییم و با احتمال (1-P) عقبگرد نماییم (از همین بدو شروع مشخص است در مدلسازی تحلیلی تقریب بسیار زیادی به دلیل پیچیدگی الگوریتم عقبگرد نمایی دودویی صورت گرفته است.) احتمال این‌که یک ایستگاه در همان برش زمانی موفق به ارسال شود، (فرض کنید که تعداد ایستگاه‌های کاری برابر K باشد.) از رابطه زیر به‌دست می‌آید:

$$A = \text{احتمال عدم تصادم} = K\,\overbrace{P}^{\text{یک ایستگاه موفق شود}}\underbrace{(1-P)^{K-1}}_{\text{بقیه موفق نشوند}}$$

نکته ۱: A زمانی حداکثر می‌شود که $P=\frac{1}{K}$ باشد و چنانچه K به سمت بی‌نهایت میل کند، $A=\frac{1}{e}$ خواهد بود:

$$\lim_{\substack{k\to\infty \\ p=\frac{1}{k}}} A = \frac{1}{e}$$

نکته ۲، میانگین تعداد دفعات تلاش تا موفقیت در ارسال از رابطه زیر بدست می‌آید:

$$\sum_{J=0}^{\infty} JA(1-A)^{J-1} = \frac{1}{A}$$

در واقع یک آزمایش برنولی با احتمال موفقیت A و احتمال شکست $A - 1$ داریم و تعداد دفعات تکرار آزمایش تا رسیدن به اولین پیروزی یک سری هندسی است که تابع چگالی احتمالی آن $f(J)=(1-A)^{J-1}A$ است و میانگین آن $\frac{1}{A}$ می‌باشد.

با فرض این‌که تعداد ایستگاه‌های کاری به سمت ∞ میل می‌کند کارایی کانال از رابطه زیر بدست می‌آید.

$$\text{کارآیی کانال یا بهره کانال} = U = \frac{T_f}{T_f + \frac{2\tau}{A}}$$

که T_f زمان ارسال فریم و $\frac{2\tau}{A}$ میانگین زمان رقابت با فرض برش زمانی برابر 2τ (RTT) خواهد بود. اگر به‌جای τ معادل آن $\frac{D}{V}$ و به جای T_f معادل آن $\frac{L}{R}$ را قرار دهیم و A را با $\frac{1}{e}$ تقریب بزنیم، راندمان از رابطه زیر به‌دست می‌آید:

$$\text{راندمان} = U = \frac{1}{1+2ae} \quad ; \quad a = \frac{RD}{VL}$$

۳_۳_۷ Fast Ethernet یا اترنت سریع

IEEE در سال 1995 یک استاندارد جدید برای اترنت بنا نهاد و آن را IEEE 802.3u نامید (حرف u معرف ultra است) اما مهندسین معمولاً به آن Fast Ethernet می‌گویند.

سرعت انتقال (نرخ انتقال) در اترنت سریع 100 Mbps است و در آن یک بیت به جای 100ns در 10ns ارسال می‌شود. با توجه به این‌که در این‌استاندارد، برای ایجاد امکان کشف تصادم، اگر نخواهیم طول حداقل فریم را از 64 بایت به 640 بایت برسانیم، (تا راندمان کاهش نیابد) باید طول حداکثر کابل کاهش یابد. به‌همین منظور، پیشنهاد شد در اترنت سریع فقط از Hub یا سوییچ استفاده شود و کابل‌ها از نوع UTP، STP و یا فیبر نوری خواهد بود. با تغییر نرخ انتقال از 10 به 100 مگابیت در ثانیه اگر از منچستر استفاده کنیم Band Rate برابر $200M\frac{band}{s}$ خواهد بود و بنابراین فاصله حداکثر ایستگاه‌ها با Hub یا سوییچ را 100m در نظر گرفتند. جدول زیر انواع استاندارد کابل‌کشی در اترنت سریع را نشان می‌دهد:

نام کابل	نوع کابل	حداکثر طول هر قطعه	مزایا	رده کابل برای Twisted pair
100Base -T4	Twisted pair	100 m	استفاده از کابل‌های معمولی تلفن (4 زوج UTP Cat3)، ارزان	UTP Cat3
100Base -TX	Twisted pair	100 m	ارسال دو طرفه همزمان (Full Duplex) با نرخ 100Mps	UTP Cat5
100Base -FX	Fiber optics	2000 m	فاصله طولانی، ارسال دو طرفه، قیمت بالا	-

محاسبات مربوط به حداکثر طول کابل نشان می‌دهد که روش کدینگ منچستر باید کنار گذاشته شود. به همین دلیل، IEEE روش کدینگ turnary را برای این استاندارد پیش‌بینی کرده است.

نکته : در مورد فیبر نوری به طول 2000m موضوع بسیار پیچیده تر خواهد شد چون 2τ زمان بسیار طولانی خواهد بود. بنابراین IEEE پیشنهاد کرد که فیبر نوری در این استاندارد فقط باید به سوییچ متصل شود و هر ایستگاه مستقیماً با یک فیبر به سوییچ متصل شود. (تا روی پورت تصادم نداشته باشیم)؛ یعنی اصلاً قضیه تصادم منتفی خواهد بود.

۳ـ۴ـ۷ Gigabit Ethernet

در سال 1998، IEEE دوباره سرعت اترنت را 10 برابر افزایش داد و آن را به 1000 Mbps یعنی به 1Gbps رساند و ازآن‌جا که فکر می‌کرد کار به انتها رسیده است آخرین حرف الفبا را روی آن نهاد (IEEE 802.3z).

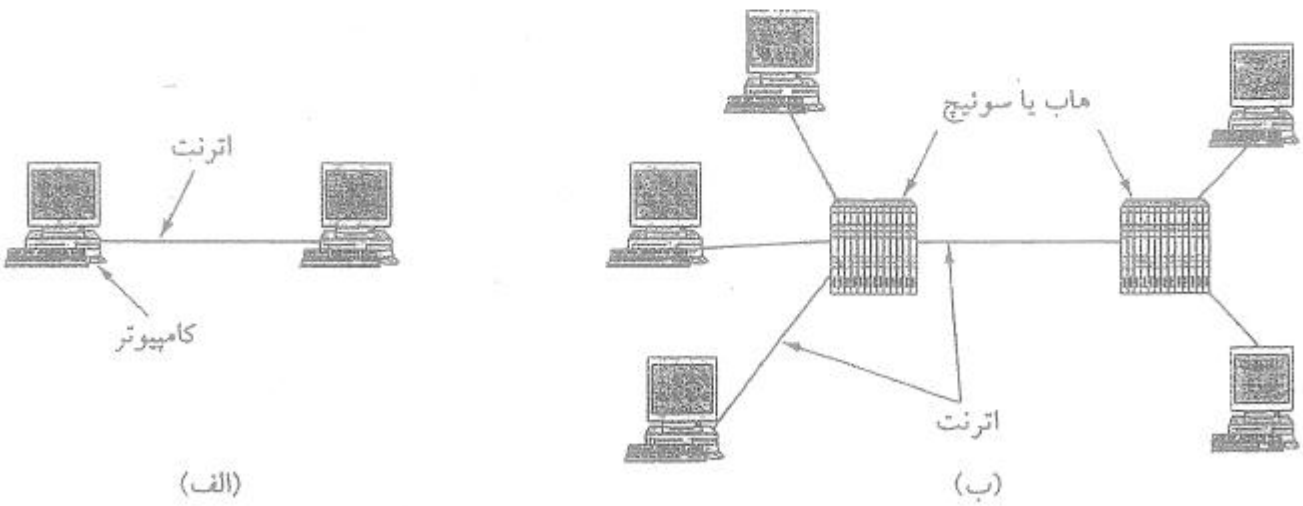
نکات مربوط به Gigabit Ethernet

اترنت گیگابیت نیز انتقال فریم‌ها را به صورت دیتاگرام بدون تصدیق (یا Connection less که بدون Acknowledge است) به صورت تک‌پخشی، چند پخشی و انتشاری انجام می‌دهد و از همان MAC Address های 48 بیتی و همان قالب فریم DIX با طول حداقل و حداکثر استاندارد DIX استفاده می‌کند.

نکته : اترنت گیگابیت دیگر ساختار کلاسیک Bus را پشتیبانی نمی‌کند (در اترنت سریع، Hub در واقع همان Bus است) یعنی به‌جای آن‌که همه ایستگاه‌ها به یک کابل مشترک متصل باشند هر ایستگاه به‌طور مستقیم به یک پورت سوییچ متصل می‌شود. اگرچه IEEE این استاندارد را به دو گونه پیاده‌سازی کرده است تا هم Hub و هم Switch پشتیبانی شوند اما در عمل هیچ شرکتی کارت‌های گران قیمت اترنت گیگابیت را با Hub های ارزان هدر نمی‌دهد.

نکته : اترنت گیگابیت هم به صورت Full Duplex و هم Half Duplex عمل می‌کند اما پیش فرض Full Duplex است.

شکل زیر دو نوع همبندی یا Topology را در اترنت گیگابیت نشان می‌دهد.



شکل (الف) اتصال مستقیم کامپیوترها از طریق کارتهای شبکه بدون نیاز به Hub یا Switch (نقطه به نقطه) شکل (ب) کامپیوترها مستقیماً به پورت‌های Switch متصل می‌شوند و سوییچ‌ها به هم متصل می‌شوند. در این‌جا هیچ حوزه تصادمی وجود ندارد مگر این‌که به جای Switch از Hub استفاده شود که اقتصادی نخواهد بود.

نکته : در سوییچ‌ها از بافر و Backplane های بسیار سریع استفاده شده است. بنابراین، فرستنده و گیرنده نیاز به شنود کانال ندارند و می‌توانند همزمان (Full Duplex) اطلاعات را ارسال و دریافت نمایند زیرا کانال رفت و برگشت از یکدیگر جدا هستند.

نکته : اگر به‌خاطر قیمت کسی بخواهد از Hub استفاده کند IEEE دو تکنیک جدید به‌نام Carrier Extention و Frame Bursting را برای حل مشکل طول کابل پیشنهاد کرده است.

- Carrier Extention طول Pad یا داده‌های زائد را اضافه می‌کند.
- در frame Bursting کارت شبکه آن‌قدر می‌ایستد تا چند فریم جمع شده و بعد آن‌ها را می‌فرستد.

جدول زیر انواع کابل‌کشی استاندارد در اترنت گیگابیت را نشان می‌دهد.

نام کابل	نوع کابل	حداکثر طول هر قطعه	مزایا
1000Base- SX	Fiber optics	550 m	از فیبرهای چند مد با تکنولوژی 50 و 62.5 میکرون استفاده شده و لذا ارزان است.
1000Base- LX	Fiber optics	5000 m	از فیبرهای تک مد به قطر 10 میکرون با لیزر 1.3 میکرون استفاده می‌شود. (در طول حداکثر)
1000Base -CX	2 Pairs of STP	25 m	از کابل‌های زره‌دار STP استفاده می‌شود.
1000Base-T	4 pairs of UTP	100 m	از کابل‌های UTP نوع Cat 5 استفاده می‌شود.

نکته : روش کدینگ اطلاعات در اترنت گیگابیت نه منچستر است و نه turnary بلکه روش جدیدی به نام 8B/10B برای آن ابداع شده است.

نکته بسیار مهم: سرعت 1Gbps بسیار بالا است و اگر مثلاً فقط 1ms مشغول پردازش باشید 1953 فریم در بافر شما جمع شده است. بنابراین نیاز به کنترل جریان داریم. در روش کنترل جریان پیشنهادی IEEE، هر وقت گیرنده می‌خواهد فرستنده را متوقف کند یک فریم به نام PAUSE ارسال می‌کند برای ارسال فریم PAUSE با قرار دادن عدد 0x8808 در فیلد Type فریم، آن‌را از نوع کنترلی مشخص می‌کنیم و مدت زمان توقف را بر مبنای طول حداقل فریم به‌عنوان پارامتر آن مشخص می‌کنیم.

۴-۷- LLC (IEEE 802.2) یا Logical Link Control

وظائف این زیر لایه عبارتند از:

- کنترل خطا به کمک CRC و سیگنال تصدیق یا Acknowledge
- تطبیق پروتکل‌های مختلف MAC و ایجاد یک واسط یکسان و یکنواخت بین لایه شبکه LLC و زیر لایه‌های MAC

متفاوت سه LLC رده از خدمات را پشتیبانی می‌کند:

۱) ارسال نامطمئن دیتاگرام

۲) خدمات دیتاگرام با Acknowledge

۳) ارسال اتصال‌گرای مطمئن (Reliable Connection Oriented)

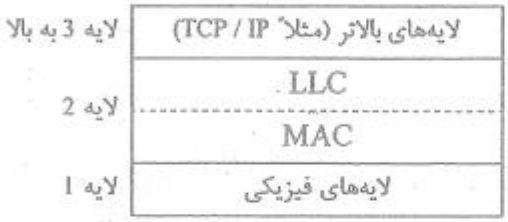
نکته مهم: IP در اینترنت نیازی به لایه پیوند داده مطمئن ندارد و صرف تلاش در جهت ارسال بسته IP کافی است و به پیغام اعلام وصول فریم در سطح LLC نیازی نیست.

۵ـ۷ شبکه‌های محلی بی‌سیم (Wireless LAN)

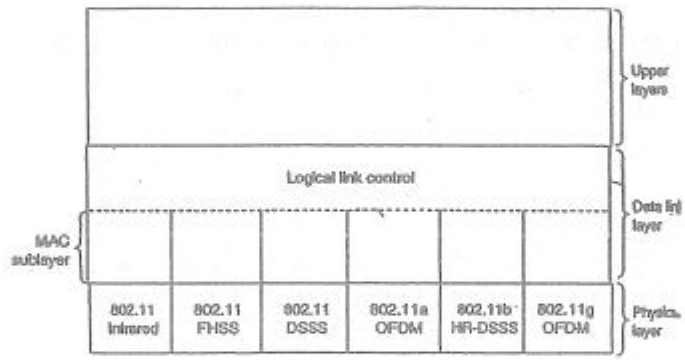
در سال 1997، IEEE شبکه‌های محلی بی‌سیم را به دو صورت زیر استاندارد کرد و آن استاندارد را 802.11 نامید:

- یک ایستگاه ثابت به عنوان Access Point یا نقطه دسترسی
- بدون نقطه دسترسی یا Access Point

پشته پروتکل (Protocal Stack) در این‌جا نیز مانند اترنت به صورت زیر است



IEEE 802.11 لایه فیزیکی و MAC را استاندارد کرده است که در زیر بررسی این دو می‌پردازیم.



۱ـ۵ـ۷ لایه فیزیکی شبکه‌های محلی بی‌سیم

۱) IEEE 802.11 با فن‌آوری مادون قرمز (InfraRed)

۲) IEEE 802.11 با امواج رادیویی و تکنیک FHSS

۳) IEEE 802.11 با امواج رادیویی و تکنیک DSSS

۴) IEEE 802.11a با امواج رادیویی و تکنیک OFDM

۵) IEEE 802.11b با امواج رادیویی و تکنیک HR – DSSS

۶) IEEE 802.11g با امواج رادیویی و تکنیک OFDM جدید

سه استاندارد اول همگی در سال 1997 تحت عنوان 802.11 عرضه شد. دو استاندارد 802.11a و 802.11b در سال 1999 معرفی شدند تا نرخ ارسال را افزایش دهند. در سال 2001 گونه جدیدی از مدولاسیون OFDM تحت عنوان 802.11g معرفی شد که در باند فرکانسی متفاوتی کار می‌کرد.

۱ـ ۱ـ ۵ـ ۷ 802.11 با امواج مادون قرمز

این روش، مبتنی بر امواج مادون قرمز می‌باشد. این امواج دارای برد کوتاه بوده و کاربردهای دیگری نظیر کنترل راه دور تلویزیون دارد. در این تکنیک از امواج پخشی با طول موج 0.85 یا 0.95 میکرون استفاده می‌شود. نرخ انتقال 2 Mbps یا 1 است. معایب این روش عبارتند از:

- عدم عبور از موانع
- نرخ ارسال پایین
- محو شدن سیگنال در نور خورشید

به همین دلیل کمتر کسی از این روش استفاده کرد و این روش منسوخ شد.

۲ـ ۱ـ ۵ـ ۷ 802.11 با تکنیک FHSS (Frequency Hopping Spread Spectrum)

در این روش از 79 کانال مستقل استفاده می‌شود که پهنای باند هر کدام 1MHz است و از پایین‌ترین فرکانس باند ISM (2.4 GHz) که سازمان FCC در ایالات متحده در گذشته فقط این باند را بدون نیاز به اخذ مجوز دولتی مجاز به استفاده می‌دانست) شروع می‌شود. البته دقت کنید به دلیل این‌که کاربردهای گوناگونی نظیر قفل‌های کنترل از راه دور درب گاراژ، اجاق مایکروویو، تلفن بی‌سیم و غیره همگی در این فرکانس قرار دارند. رقیب‌های شما در این باند فرکانسی زیادند. به همین دلیل سیگنال‌ها در این باند فرکانسی توان بسیار کمی دارند تا از تداخل آن‌ها جلوگیری شود.

در این روش فرستنده و گیرنده با هم سنکرون می‌شوند و به کمک یک مولد تصادفی مشخص(Seed معلوم و رابطه معلوم) اعداد تصادفی تولید می‌کنند و پس از گذشت اسلات‌های زمانی به طول مشخص توافق شده (کمتر از 400 میلی ثانیه) که به آن زمان دوئل (Dwell Time)گویند به صورت تصادفی باید فرکانس خود را در این 79 کانال جابجا کنند.

Hacker ها فقط در صورتی می‌توانند این سیگنال را شنود نمایند که زمان دوئل، Seed و مولد تصادفی را بدانند. همچنین به دلیل جابجایی سریع باند فرکانسی مشکل محو شدگی چند مسیره (Multipath Fading) حل می‌شود. زیرا قبل از این‌که سیگنال‌های مزاحم که از انعکاس سیگنال اصلی نشات گرفته‌اند به گیرنده برسند، گیرنده باند فرکانسی خود را عوض کرده است.

با همه این مزایا، مشکل اصلی این تکنیک، پهنای باند فرکانسی کم آن و نرخ پایین ارسال (1Mbps) می‌باشد.

۳ـ ۱ـ ۵ـ ۷ 802.11 با تکنیک DSSS (Direct Sequence Spread Spectrum)

این تکنیک نیز با نرخ 2 Mbps یا 1 کار می‌کند اما تکنیک استفاده از باند فرکانسی ISM (2.4GHz) در آن کمی عجیب به نظر می‌رسد در این تکنیک چندین ایستگاه می‌توانند همزمان در یک باند فرکانسی به ارسال داده بپردازند.

نکته در این‌جاست که چگونه اطلاعات آن‌ها دچار تداخل نمی‌شود. در فصول قبل دیدیم که می‌توان با سه تکنیک مالتی پلکسینگ TDM ، FDM و WDM از تداخل داده‌ها جلوگیری کرد، اما در این‌جا همزمان (بر خلاف TDM) در یک باند فرکانسی و یک طول موج (بر خلاف FDM و WDM) به ارسال داده می‌پردازیم. این تکنیک را CDMA (Code Division Multiple Access) می‌نامند. در این تکنیک برای جدا کردن داده‌ها از روش‌های خاص رمزگذاری و تئوری Coding استفاده می‌کنند. به این شکل که اطلاعات به صورت بردارهای متعامد (Ortogonal) ارسال می‌شوند. (فرض کنید در یک سالن همزمان چهار نفر به زبان‌های فارسی، روسی، فرانسوی و انگلیسی صحبت کنند. انسان می‌تواند سیگنال صحبت موردنظر خود را به‌طور مفهومی به دلیل عمود بودن این زبان‌ها بر هم و تفاوت آشکار در گرامر و لغات آن‌ها از سایر سیگنال‌ها استخراج کند.)

به تکنیک‌هایی از این دست که همزمان از کل باند فرکانسی برای ارتباط بین هر یک از زوج دستگاه‌های در حال مکالمه استفاده می‌نمایند، طیف گسترده (Spread Spectrum) می‌گویند.

۷ـ۵ـ۱ـ۴ 802.11a با تکنیک OFDM (Ortogonal Frequency Division Multiplexing)

هنگامی که سازمان FCC قانون منع استفاده از باندهای فرکانسی بالاتر از ISM (2.4 GHz) را لغو کرد IEEE از این فرصت استفاده کرد و در استاندارد 802.11a با بهره‌گیری از مدولاسیون OFDM (Ortogonal Frequency Division Multiplexing) در باند فرکانسی 5GHz به نرخ انتقال 54 Mbps دست یافت. در این تکنیک 52 زیر کانال فرکانسی استفاده می‌شود که 48 مورد از آن‌ها برای انتقال داده و 4 تای دیگر برای همگام سازی است و از این نظر شبیه ADSL عمل می‌کند.

از آن‌جا که در این روش نیز به‌طور همزمان بر روی فرکانس‌های متفاوت به ارسال داده می‌پردازیم این روش نیز نوعی تکنیک Spread Spectrum یا طیف گسترده محسوب می‌شود .

در این روش از سیستم کدینگ پیچیده‌ای که مبتنی بر مدولاسیون تغییر فاز برای نرخ ارسال کمتر از 18Mbps و QAM برای سرعت‌های بالاتر می‌باشد استفاده می‌شود

نکته: تقسیم سیگنال به تعداد بسیار زیادی باند باریک در مقایسه با استفاده از یک باند واحد عریض، مزایای متعددی دارد که از جمله می‌توان به ایمنی بیشتر در مقابل تداخل و امکان استفاده از باندهای غیرمجاور اشاره کرد.

۷ـ۵ـ۱ـ۶ 802.11b با تکنیک HR – DSSS (High Rate DSSS)

این روش از همان تکنیک DSSS با نرخ بالاتر داده استفاده می‌کند و به سرعت 1 , 2 , 5.5 , 11 Mbps دست می‌یابد. در این تکنیک از مدولاسیون تغییرفاز و کدینگ‌های ویژه استفاده شده است. (برای بالا بردن سرعت)

۷ـ۵ـ۱ـ۶ـ۵ 802.11 g با تکنیک OFDM جدید

در نوامبر 2001 بالاخره IEEE از بین تکنیک‌های متنوع، مدولاسیون OFDM (مانند 802.11a) را انتخاب کرد با این تفاوت که مانند 802.11b در باند 2.4GHz کار می‌کند و استاندارد IEEE 802.11g را به عنوان آخرین استاندارد ارائه داد. سرعت این شبکه 54Mbps است.

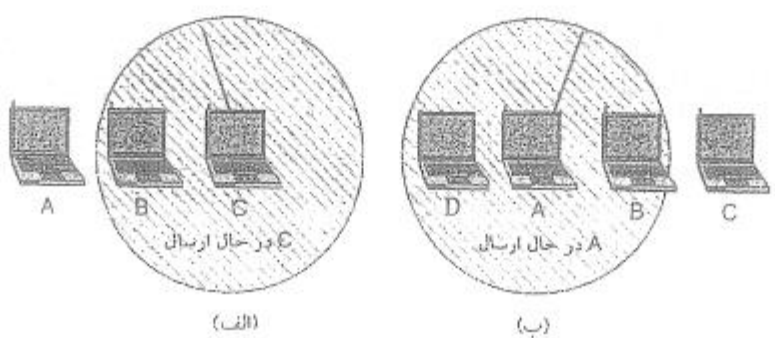
۷ـ۵ـ۲ زیر لایه MAC در شبکه‌های محلی بی‌سیم

در اترنت و CSMA / CD اگر در خلال 64 بایت اول یک فریم افزایش توان و یا یک سیگنال پرتوان نویز مشاهده نشود، دلیل بر آن است که تصادفی رخ نداده است اما در شبکه‌های بی‌سیم چنین وضعیتی وجود ندارد و مساله به این سادگی نیست و به عبارت دیگر پروتکل CSMA/CD قابل استفاده نخواهد بود. دو دلیل عمده برای عدم امکان استفاده از این پروتکل به شرح زیر است:

۱) در هنگام ارسال در شبکه‌های بی‌سیم، فرستنده نمی‌تواند همزمان به کانال گوش دهد و تصادم را کشف کند

۲) مشکل گره مخفی یا ایستگاه مخفی که قبلاً شرح داده شد نیز دلیل دیگری برای این موضوع می‌باشد.

برای مثال به شکل زیر نگاه کنید.



در شکل (الف) ایستگاه A می‌خواهد با ایستگاه B تماس برقرار کند و در همان زمان ایستگاه C مشغول ارسال اطلاعات به ایستگاه B است. A با شنود کانال متوجه این ارتباط نخواهد شد و فکر می‌کند خط آزاد است.
در شکل (ب) ایستگاه B می‌خواهد با ایستگاه C ارتباط برقرار کند اما در همان لحظه A مشغول ارتباط با ایستگاه D است. B به اشتباه فکر می‌کند که کانال مشغول است در صورتی‌که می‌تواند بدون تداخل در همان لحظه اطلاعات خود را به C ارسال کند.

نکته : ارسال همزمان از A به D هیچ تاثیری برای اطلاعات ارسال B به C ندارد زیرا D در برد B نیست و C در برد A قرار ندارد.

نکته : نتیجه این‌که در این‌جا گوش دادن به خط کمکی به تشخیص تصادم نمی‌کند.

نکته : برای کاهش هزینه‌ها در 802.11 نوع ارتباط Half Duplex می‌باشد.

انواع روش‌های ارتباطی در لایه MAC استاندارد 802.11

- DCF (Distributed Coordination) ← پشتیبانی اجباری
- PCF (Point Coordination Function) ← پشتیبانی اختیاری (منظور از Point در این‌جا همان Access Point است)

روش DCF :

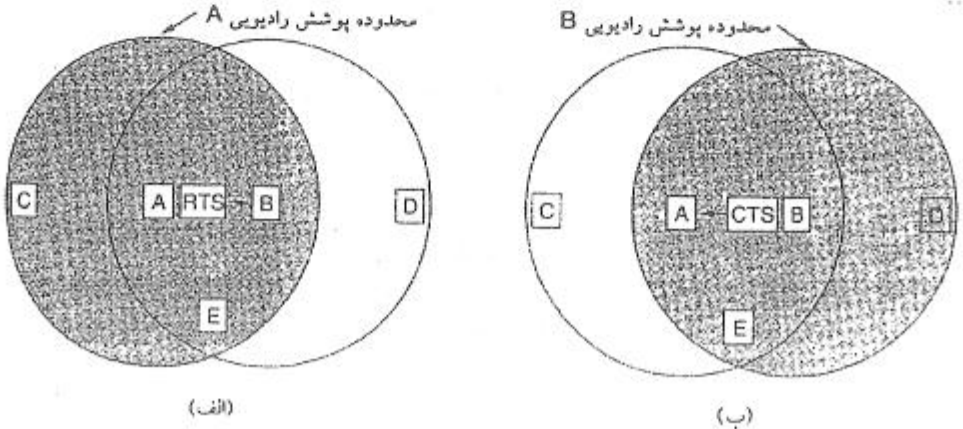
پروتکل مورد استفاده در DCF پروتکل CSMA / CA (Carrier Sense Multiple Access with Collision Avoidance) با امکان اجتناب از تصادم می‌باشد. این پروتکل که در آن هم کانال فیزیکی و هم کانال مجازی شنود می شوند، از دو بخش عمده تشکیل می‌شود:

۱) به خط گوش می‌دهیم اگر کانال آزاد بود ارسال می‌کنیم. در هنگام ارسال به کانال گوش نمی‌دهیم و تا انتهای فریم ادامه می‌دهیم. اما اگر کانال مشغول باشد کنار می‌کشیم و یک مدت تصادفی (بر اساس الگوریتم عقبگرد نمایی دودویی) منتظر مانده و مجدداً تلاش می‌کنیم.

۲) به کمک مکانیزمی بنام MACAW به کانال مجازی گوش می‌دهیم تا از تصادم اجتناب کنیم.

قبل از ادامه بحث پروتکل MACA را مورد بررسی قرار می‌دهیم:

در پروتکل MACA (Multiple Access with Collision Avoidance) که به معنی پروتکل دسترسی چند گانه با اجتناب از تصادم است، در واقع فرستنده و گیرنده هر دو در ابتدای مکالمه دو فریم کوچک RTS (Request to Send) از طرف فرستنده به گیرنده و پس از آن CTS (Clear to Send) از طرف گیرنده به فرستنده به‌ترتیب به نشانه درخواست ارسال و آمادگی دریافت ردوبدل می‌شود. کاربرد مهم این دو فریم کوچک حل مشکل ایستگاه مخفی است. به شکل زیر دقت کنید:



(الف) (ب)

در این شکل، ابتدا فرستنده، (ایستگاه A) یک فریم کوتاه 30 بایتی بنام RTS که حاوی طول فریم داده اصلی است به گیرنده (B) ارسال می‌کند. B، Cو E این سیگنال را دریافت می‌کنند اما D دریافت نمی‌کند. سپس گیرنده، (ایستگاه B) سیگنال CTS (فریم 30 بایتی که آن هم حاوی طول فریم است) را به فرستنده یا A بر می‌گرداند. دقت کنید D و E همانند A سیگنال CTS را دریافت می‌کنند اما C آن را نمی‌شنود. در نتیجه علاوه بر طرفین ارتباط (A و B):

۱) C فقط RTS را دریافت می‌کند.

۲) D فقط CTS را دریافت می‌کند.

۳) E هم RTS و هم CTS را دریافت می‌کند.

اما هر سه ایستگاه فوق قادرند با توجه به طول فریم و استفاده از تایمرهای داخلی و متغیرهای درونی، پایان این مکالمه را محاسبه نموده و بدون این‌که نیاز باشد تا انتهای مکالمه به گوش دادن ادامه دهند از این مکالمه و زمان پایان کاملاً مطلع باشند. به این روش، شنود کانال مجازی می‌گویند. بنابراین اگر سه ایستگاه C، D و E تا پایان مکالمه اقدام به ارسال ننمایند از تصادم اجتناب (Avoidance) خواهد شد. در سال 1994 یک گروه تحقیقاتی این پروتکل (MACA) را توسعه داد و آن را MACAW (Multiple Access with Collision Avoidance for Wireless LAN) نامید. پیشنهادات آن‌ها برای توسعه MACA عبارت است از:

الف) استفاده از فریم ACK به منظور اعلام وصول فریم داده از گیرنده به فرستنده؛ زیرا اگر این کار در لایه پیوند داده انجام نشود به لایه انتقال یا حمل موکول می‌شود که سیستم را بسیار کند می‌کند. بنابراین از آن جا که این پروتکل در CSMA / CA به کار می‌رود، در واقع استاندارد 802.11 در لایه پیوند داده از کنترل خطا به روش Backward برخوردار است. در صورتی‌که لایه MAC در اترنت این‌کار را نمی‌کرد.

ب) برای کاهش احتمال تصادم در اثر ارسال همزمان دو RTS، از دو ایستگاه مختلف به یک ایستگاه واحد عمل گوش دادن به خط یا شنود کانال نیز به پروتکل اضافه شده است.

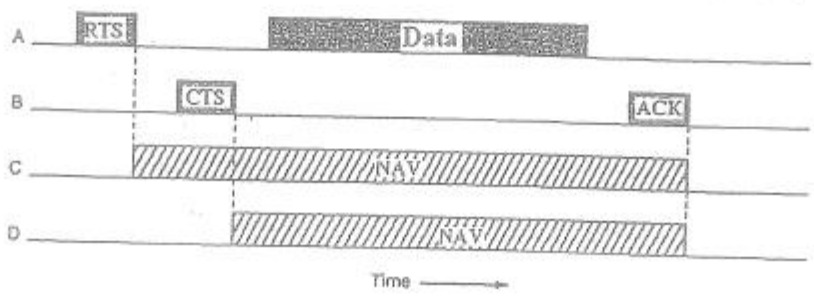
ج) پیشنهاد شده است که الگوریتم عقبگرد نمایی به جای این‌که بر روی یک ایستگاه اعمال شود بر روی یک جریان داده خاص اعمال شود که منظور از جریان داده تعدادی فریم است که در یک مکالمه مشخص با زمان مشخص بین مبدا و مقصد برقرار است.

د) مکانیزم‌هایی برای کنترل ازدحام و ردوبدل کردن اطلاعاتی بین ایستگاه‌ها به منظور گزارش وضعیت ترافیک شبکه پیشنهاد شده است که تمامی این پیشنهادها موجب افزایش کارایی شبکه خواهد شد.

حال به قسمت دوم از پروتکل CSMA/CA بر می‌گردیم. در این پروتکل با توجه به توضیحات فوق پس از ارسال هر فریم داده یک تایمر به نام ACK-Timer تنظیم (Set) و روشن می‌شود. اگر پیش از دریافت ACK این زمان‌سنج منقضی شود نشان دهنده بروز تصادم و یا وجود خطا است و نیاز به ارسال مجدد می‌باشد.

نکته : یکی از دلایل بروز تصادم، اقدام همزمان به ارسال RTS به یک ایستگاه واحد است.

شکل زیر کاربرد کانال مجازی را در روش CSMA / CA نشان می‌دهد.



NAV : Network Allocation Vector

C و D به کانال مجازی گوش می‌دهند در حالی‌که E نیاز به این کار ندارد و به کانال فیزیکی گوش می‌دهد.

چند نکته در مورد پروتکل CSMA / CA وجود دارد:

نکته ۱: احتمال خطا در شبکه‌های بی‌سیم باند ISM بالاست. لذا اگر طول فریم بزرگ شود احتمال خطای فریم بسیار بالا خواهد بود.

P = احتمال خطای یک بیت

$1 - P$ = احتمال عدم خطای بیت

$(1-P)^L$ = احتمال عدم خطا در یک فریم به طول L

$1-(1-P)^L$ = احتمال خطا در فریم به طول L

یعنی هر چه طول فریم افزایش یابد، احتمال خطا بیشتر می‌شود.

مثال: اگر فریم اترنت طولش 12144 بیت باشد با احتمال خطای بیت 10^{-4} احتمال خطای فریم بیش از 0.70 خواهد بود.

نتیجه: در این پروتکل فریم‌ها به قطعات کوچک تقسیم و شماره‌گذاری شده و با پروتکل Stop & Wait ارسال می‌شوند. ارسال پشت سر هم این دنباله قطعه‌های (فریم‌های) کوچک را فوران تکه‌ها (Fragment Burst) می‌گویند. علت استفاده از فوران تکه‌ها کمک به سیستم کنترل خطا است.

نکته ۲: تاکنون روش DCF مورد بررسی قرار گرفت. در این‌جا لازم است کمی در مورد روش PCF تعریف کنیم. در این روش از یک ایستگاه ثابت یا Access Point برای کنترل دسترسی به کانال استفاده می‌شود. از آن‌جا که یک ایستگاه مرکزی وجود دارد پروتکل بسیار ساده است. مکانیزم ارتباطی مورد استفاده در این‌جا Polling (سرکشی) است. یعنی این‌که ایستگاه مرکزی به یکایک ایستگاه‌ها سرکشی می‌کند و سوال می‌کند که آیا نیاز به ارسال دارد یا خیر؟

واضح است مکانیزم سرکشی تصادم ندارد.

در روش سرکشی یک فریم خاص به نام فانوس دریایی (Beacon Frame) به طور متناوب در بازه‌های 10 تا 100 میلی ثانیه منتشر می‌شود و حاوی اطلاعاتی در مورد ترتیب پرش فرکانسی (Hopping Sequence) و زمان دوئل در مدولاسیون FHSS و نیز پارامتر سنکرون‌سازی ساعت و مواردی از این قبیل می‌باشد. همچنین در این فریم از ایستگاه‌های جدید دعوت می‌شود تا به‌منظور سرکشی شدن ثبت‌نام نمایند. در این استاندارد کیفیت سرویس (QOS) موردنیاز در فاز آغاز مکالمه درخواست و توسط شبکه رعایت آن تضمین می‌شود. هر ایستگاه جدید که وارد سیستم می‌شود باید خود را در ایستگاه ثابت مرکزی ثبت‌نام نماید.

۶ـ۷ IEEE 802.16 (بی‌سیم باند گسترده یا Broadband Wireless Network)

این شبکه‌ها که گاهی تحت عنوان شبکه‌های بی‌سیم شهری باند گسترده نامیده می‌شوند برای ارتباطات بی‌سیم درون شهری با پهنای باند و سرعت بالاتر از شبکه‌های محلی بی‌سیم طراحی شده است.

واضح است که استفاده از آنتن‌های بلند بر روی تپه‌ها یا نقاط مرتفع شهر و نیز نصب آنتن‌هایی بر روی پشت بام‌های ساختمان‌های شهر (رو به آنتن‌های بلند) بسیار ارزان‌تر از حفاری زمین و کشیدن فیبرنوری یا کابل‌های UTP و STP تا درب منزل صدها هزار شهروند است.

توجه به طراحی شبکه‌های بی‌سیم شهری چند گیگابیتی و تنوع محصولات، IEEE را بر آن داشت تا در اوایل 2002 استاندارد IEEE 802.16 را با نام واسط هوایی برای سیستم‌های بی‌سیم ثابت با پهنای باند وسیع (Air Interface for Fixed Broadband Wireless Access System) معرفی کرد.

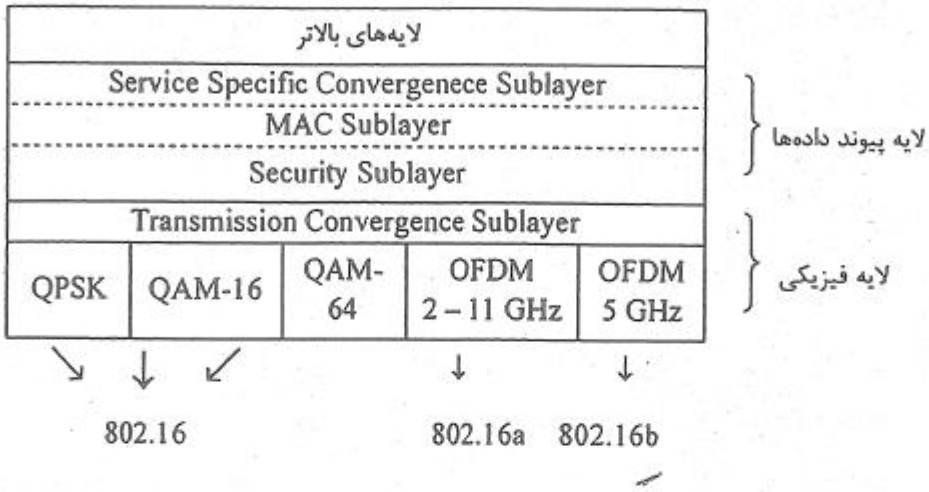
در زیر شبکه‌های محلی بی‌سیم با شبکه‌های شهری بی‌سیم از جوانب مختلف مقایسه شده است.

مورد مقایسه	(محلی بی‌سیم) IEEE 802.11	(شهری بی‌سیم) IEEE 802.16
حرکت	کامپیوترهای کیفی متحرکند.	ساختمان‌ها ثابت‌اند.
شارژ و هزینه	هزینه کمتری می‌دهند.	صاحبان ساختمان‌ها پول بیشتری می‌دهند.
حالت ارتباطی	Half Duplex	(بدلیل هزینه بیشتری که می‌پردازند) Full Duplex
فاصله	داخل طبقات ساختمان و محل‌های کوچک	2.5 کیلومتر ـ در شهرهای بزرگ مثل تهران نیاز به تعداد زیادی آنتن بلند دارد.
SNR	فاصله‌ها نزدیک است و SNR بالاست و خوب است.	در فواصل زیاد تاثیر Noise بیشتر می‌شود زیرا سیگنال تضعیف و SNR کم می‌شود لذا از چندین روش مدولاسیون استفاده می‌شود.
نیاز به پهنای باند	کمتر پیش می‌اید در یک LAN 50 نفر همزمان فیلم تماشا کنند و شبکه را از کار بیاندازند.	ممکن است همزمان صدها نفر به تماشای فیلم‌ها بپردازند. (پهنای باند موردنیاز زیاد است.)
باند فرکانسی	2.4 , 5 GHz	10-66 GHz بدترین فرکانس‌های ته مانده با مشکل جذب امواج میلی‌متری در باران، برف، مه، برگ درخت، و غیره
پشتیبانی از QOS	اگرچه تا حدی از QOS برای سرویس‌های بلادرنگ پشتیبانی می‌کنند اما در واقع برای چنین ترافیک‌هایی طراحی نشده‌اند.	پشتیبانی قوی از کیفیت خدمات به علت نیاز به ارتباطات چند رسانه‌ای (Multimedia). مانند پخش فیلم و غیره

نکته : شبکه‌های باند گسترده بی‌سیم شهری چه تفاوتی با شبکه‌های تلفن همراه (شبکه‌های تلفن سلولی) دارند؟

از آن‌جا که شبکه‌های تلفن برای ارتباط صوتی با باند باریک و توان مصرفی پایین طرح شده است، مناسب شبکه‌های بی‌سیم شهری با باند گسترده نیست.

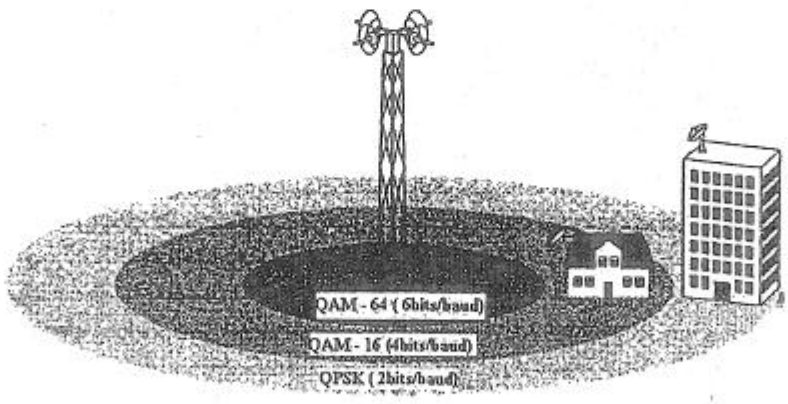
۱ـ۶ـ۷ پشته پروتکل IEEE 802.16



در پشته پروتکل استاندارد IEEE 802.16 (شکل زیر) جمعاً پنج زیر لایه در دو لایه فیزیکی و پیوند داده دیده می‌شود.

زیر لایه مدولاسیون در لایه فیزیکی

همان‌طور که قبلاً گفته شد این شبکه از آنتن‌های بلند تشکیل شده است و از آن‌جا که امواج میلی‌متری در باند 66GHZ – 10 که نزدیک امواج مادون قرمز است، تک جهته است و به صورت یک اشعه در راستای خاص حرکت می‌کند (بر خلاف تلفن‌های سلولی که همه جهته هستند.) لذا بر روی این آنتن بلند چندین دیش در جهات مختلف برای پوشش دادن قطاع‌های مختلف نصب می‌شود. به شکل زیر نگاه کنید.



$\begin{cases} R = \log_2^{64} \times R_s \leftarrow QAM-64 \\ R = 6R_s \end{cases}$ حساسیت به نویز بالا است و برای فواصل نزدیک باید استفاده شود.

$R = 4R_s \leftarrow QAM-16 \leftarrow$ برای فواصل متوسط

$R = 2R_s \leftarrow Q-PSK \leftarrow$ حساسیت به نویز کمتر است و برای فواصل دورتر استفاده می‌شود.

نکته : در این استاندارد از دو روش استاندارد FDD (Frequency Devision Duplexing) و TDD (Time Devision Duplexing) برای ایجاد ارتباط Full Duplex استفاده می‌شود. در این دو روش یا زمان (در TDD) و یا فرکانس، بین ارتباطات در دو جهت (Upstream از مشتری به آنتن مرکزی و Downstream از آنتن مرکزی یا ایستگاه مرکزی به مشتری‌ها) تقسیم می‌شود.

پروتکل زیر لایه MAC در 802.16

یک نکته مهم در این استاندارد این است که خود لایه فیزیکی که بحث آن مطرح گردید با استفاده از کد همینگ و مکانیزم کنترل خطای FEC (Forward Error Correction) به طور خودکار خطاها را کشف و تصحیح می‌کند و شبکه بی‌سیم راه دور پر از خطا را به صورت یک شبکه کم خطا به لایه‌های بالاتر نشان می‌دهد. لذا امکان بروز خطا و نیاز به ارسال مجدد در صورت عدم دریافت ACK (مربوط به پشت CRC) بسیار پایین خواهد بود.

نکته : تنها شبکه‌ای که در لایه فیزیکی آن با کد همینگ عمل FEC انجام می‌شود 802.16 است.

در پروتکل MAC شبکه‌های بی‌سیم شهری برای ایجاد امنیت زیر لایه‌ای تخصیص یافته است و با کمک روش‌های پیشرفته رمزنگاری (Encryption) فقط بخش Header داده‌ها را از استراق سمع مصون نگه می‌دارند این زیر لایه از 4 رده خدمات استفاده می‌کند.

۱) CBR (Constant Bit Rate) نرخ ثابت

۲) Real-time VBR (Variable Bit Rate) نرخ متغیر بلادرنگ

۳) Non Real-time VBR نرخ متغیر غیر بلادرنگ

۴) Best Effort بهترین تلاش

۷ـ۷ دندان آبی یا (Bluetooth)

این شبکه بی‌سیم برای کامپیوترهای شخصی و ارتباط آن با دستگاه‌های جانبی برای فواصل چندمتری (حداکثر 10 متری) در داخل اتاق طراحی شده است.

کنسرسیوم متشکل از شرکت‌هایEricson، IBM، Intel، Toshiba و Nokia در سال 98 این استاندارد را به یاد دندان آبی یکی از پادشاهان قدیمی وایکینگ که نروژ و دانمارک را متحد کرد Bluetooth نامیده شد.

IEEE شبکه دندان آبی را در سال 1999 تحت عنوان IEEE 802.15 استاندارد کرد.

تست: برای اتصال هر یک از شبکه‌های 802.11، 802.16، 802.15، 802.3، 802.4 و 802.5 (به‌طور کلی MAC ها) با فرض این‌که لایه 3 و 4 در همه آن‌ها یکسان است (مثلاً TCP / IP) چه دستگاهی لازم است؟

۱) Repeater (تکرارکننده)

۲) Bridge (پل) ← چون در لایه 1 و 2 با هم اختلاف دارند، پاسخ صحیح پل است.

۳) Router (مسیریاب)

۴) Gateway (دروازه)

نکته : اگر دوتا 802.11 را بخواهیم به هم متصل کنیم از تکرارکننده استفاده می‌کنیم.

فصل هشتم

لایه شبکه (Network layer)

همانطور که در فصل اول ذکر شد وظایف لایه شبکه عبارتند از :

- وظیفه اصلی لایه شبکه، رساندن بسته‌ها از مبدا به مقصد است. (ایجاد یک ارتباط end to end)

لایه شبکه پایین‌ترین لایه‌ای است که ارتباط end to end بین مبدا و مقصد برقرار می‌کند.

- در اینجا بحث Addressing هم مطرح می‌شود، یعنی آدرس‌ها باید واحد، یکتا و جامع باشند.
- وظیفه دیگر این لایه Forwarding است یعنی وقتی بسته‌ای وارد مسیریاب (Router) می‌شود باید یک گام (Hop) به سمت مقصد به پیش رانده شود. از روی جداول درون مسیریاب تشخیص داده می‌شود که هر بسته ورودی از کدام درگاه خروجی خارج شود. این تصمیم‌گیری یا براساس آدرس مقصد و یا شماره ارتباط انجام می‌شود.
- Routing که پیدا کردن بهترین یا مناسبترین مسیر بین مبدا و مقصد است از دیگر وظایف این لایه است. این کار یا به ازای هر بسته تکرار می‌شود و یا یک بار در ابتدای مکالمه در فاز برقراری اتصال (Connection Setup) انجام می‌شود. نتیجه عملیات مسیریابی، به روز رسانی جداول درون مسیریاب‌ها است.

نکته : مسیریاب‌ها هم وظیفه Routing و هم Forwarding را بر عهده دارند.

- وظیفه دیگر این لایه، کنترل ازدحام (Congestion Control) است.

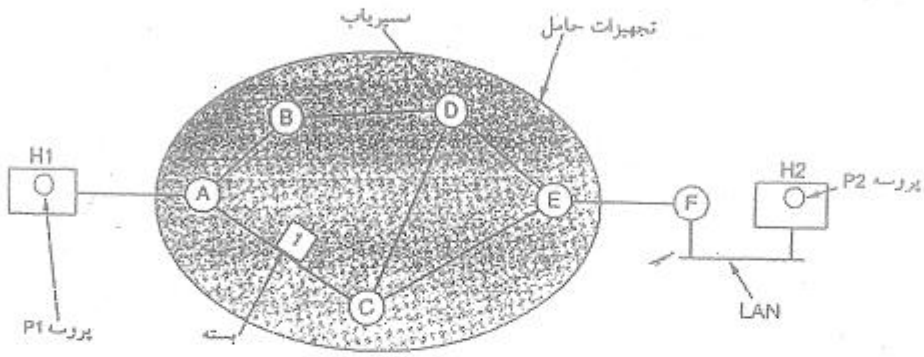
باید از اعمال بار بیش از حد بر زیر شبکه ارتباطی (Communication Subnet) جلوگیری شود. زیرا چنانچه بار شبکه از یک حد مشخص بیشتر شود کارایی شبکه روند نزولی را طی خواهد کرد.

- از دیگر وظایف مهم این لایه، تطبیق پروتکل‌ها است (Protocol Matching)

لینک‌های ورودی و خروجی مسیریاب‌ها ممکن است دارای پروتکل‌ها و استانداردهای متفاوت و متعلق به شبکه‌های مختلف باشند. وظیفه دیگر مسیریاب‌ها، تطبیق پروتکل و یا نگاشت (تبدیل) بسته‌های اطلاعاتی از یک پروتکل به پروتکل دیگر می‌باشد. (حذف Header مربوط به پروتکل قبلی و افزودن Header مربوط به پروتکل جدید و به‌طور کلی ایجاد فرمت جدید)

ذخیره و هدایت بسته‌ها (Store & Forward)

شکل زیر نشان می‌دهد که در یک شبکه تجهیزات حامل (Carrier Equipment) در کنار تجهیزات مشتریان (Costomer Equipment) قرار گرفته‌اند. در این شکل تجهیزات حامل در درون بیضی نشان داده شده است. دقت کنید مسیریاب F مربوط به مشتری است اما عملکرد آن از نظر ساختار داده و الگوریتم هیچ تفاوتی با سایر مسیریاب‌های حامل ندارد.



ذخیره و هدایت بسته‌ها یعنی این‌که باید بسته به‌طور کامل دریافت و ذخیره شود و بعداز این‌که اطمینان حاصل شد که بسته درست است یک گام به سمت مقصد Forward شود.

خدمات لایه شبکه به لایه انتقال

این خدمات باید به‌صورت سرویس به لایه انتقال داده شود. این سرویسها می‌توانند از طریق فراخوانی توابع بنیادی (مثل send packet یا receive packet) انجام گیرند. این خدمات خصوصیات زیر را باید داشته باشند.

۱ـ مستقل از تکنولوژی باشند.

۲ـ مستقل از توپولوژی باشند.

۳ـ یک مکانیزم آدرس‌دهی استاندارد و متحدالشکل داشته باشند.

سرویس‌هایی که لایه شبکه به لایه انتقال می‌دهد بر دو نوع است.

۱ـ Connection less یا بدون اتصال :

وظیفه یک مسیریاب در این شبکه هدایت (Forward) بسته‌ها است و نه چیز دیگر. این شبکه‌ها ذاتاً غیرقابل اعتمادند و کنترل خطا و کنترل جریان را به لایه انتقال می‌سپارند. در این شبکه‌ها ممکن است با تغییر پویای جداول مسیریابی درون مسیریاب ها (با توجه به شرایط جدید شبکه) بسته‌های مربوط به یک مکالمه از مسیرهای متفاوتی و با ترتیب متفاوت به مقصد برسند و یا حتی غلط برسند. اینترنت با یک تجربه ۳۰ ساله از این روش استفاده می‌کند و حتی اگر لایه‌های زیرین IP، کنترل خطا و جریان را انجام دهند فقط دوباره‌کاری کرده‌اند زیرا TCP در لایه چهارم این امر را برعهده دارد. نام دیگر این روش ارسال دیتاگرام (Datagram) است. هرگاه حجم اطلاعات رد و بدل شده در یک مکالمه کم باشد این روش مقرون به صرفه است زیرا سربار فاز برقراری اتصال اولیه را ندارد.

۲ـ Connection Oriented یا اتصال‌گرا :

شبکه‌های سوییچ تلفنی با تجربه بیش از یک قرن از این مکانیزم استفاده می‌کنند. در این روش در فاز برقراری اتصال یک مسیر مشخص بین مبدا و مقصد ایجاد می‌شود و جداول مسیریابی به روز در می‌آیند. این مسیر را در شبکه‌های سوییچ تلفنی Circuit

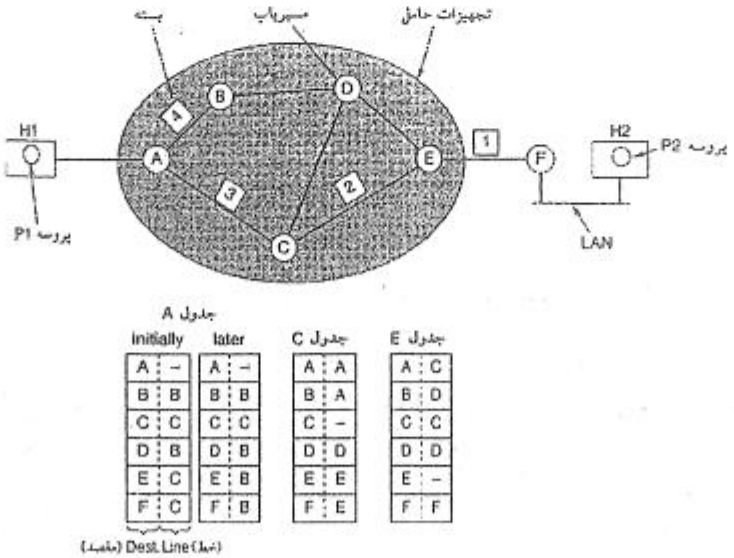
(مدار) می‌گویند و به روش سوییچینگ آن هم Circuit Switching می‌گویند اما در شبکه‌های مدرن به آن Virtual Circuit یا مدار مجازی می‌گویند. در فاز برقراری اتصال، منابع شبکه (Resources) مانند پهنای باند link ها، فضای بافر در حافظه مسیریاب‌ها، زمان CPU برای پردازش در گره‌های میانی و غیره باید رزرو شوند تا مطمئن شویم بار اضافه بر زیر شبکه ارتباطی تحمیل نخواهد شد. این کار برای جلوگیری از ازدحام و نیز تضمین تحقق معیارهای کیفیت سرویس (QOS) شامل حداکثر تاخیر، حداقل پهنای باند، حداقل گذردهی (Throughput)، حداکثر نسبت از دست رفتن بسته‌ها PLR (Packet Loss Ratio)، حداکثر لرزش تاخیر (Delay Jitter)، قابلیت اطمینان (Reliability) و امنیت (Security) انجام می‌گیرد.

در شبکه‌های مدرن پروتکل Resource ReserVation Protocol (RSVP) برای رزرو منابع بکار می‌رود. ارتباطات اتصال‌گرا مطمئن بوده و از کنترل جریان و خطا بهره‌مندند و با توجه به تضمین کیفیت سرویس برای ارتباطات چندرسانه‌ای نظیر کنفرانس تصویری راه دور و پخش فیلم بکار می‌روند. ATM یکی از مهم‌ترین شبکه‌هایی است که از خدمات اتصال‌گرا استفاده می‌کند. اینترنت نیز برای اینکه از این غافله عقب نماند در IPv6 گامهای بزرگی در جهت تحقق ملزومات QOS برداشته است.

پیاده‌سازی خدمات بدون اتصال :

فرض کنید فرآیند P_1 در میزبان H_1 در شکل زیر یک پیغام بزرگ برای فرآیند P_2 در میزبان H_2 می‌فرستد. لایه شبکه این پیغام را برای مثال به چهار بسته (Packet) می‌شکند و هر یک از این بسته‌ها را به‌صورت یک دیتاگرام مجزا با استفاده از یک پروتکل لایه پیوند داده مانند HDLC یا PPP به مسیریاب A ارسال می‌کند. فرض کنید عواملی مانند افزودن یک link جدید، خرابی یک مسیریاب، افزایش یا کاهش پهنای باند و یا تغییر در وضعیت ترافیکی شبکه باعث تغییر در مسیرها و به روزرسانی جداول درون مسیریاب‌ها می‌شود. بنابراین جدول مسیریابی A در مسیریاب A تغییر می‌کند و گام بعدی برای رسیدن به مقصد F به جای C مسیریاب B تعیین می‌شود. به روزرسانی جداول مسیریابی توسط الگوریتمی ویژه بنام Routing Algorithm انجام می‌شود.

شکل زیر جداول مسیریابی مسیریاب‌های A، C و E را نشان می‌دهد. در مسیریاب A، از جدول اولیه برای هدایت بسته‌های 1 و 2 و 3 و از جدول جدید برای هدایت بسته 4 استفاده شده است.

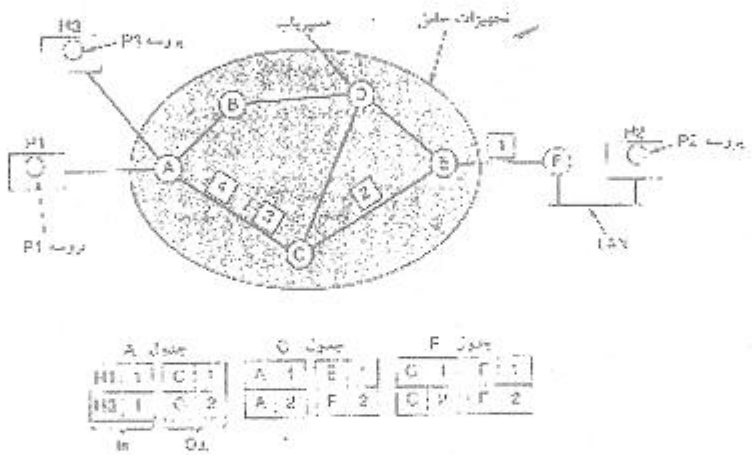


مسیریابی به روش دیتاگرام انجام می‌شود. واضح است که در این شکل مسیریابی براساس آدرس مقصد در جداول مسیریابی انجام می‌شود.

پیاده‌سازی خدمات اتصال‌گرا:

در این روش عمل هدایت بسته‌ها (Forwarding) از طریق آدرس مقصد صورت نمی‌گیرد بلکه برای هر مدار مجازی یک شماره (VCID یا Virtual Circuit ID) تخصیص داده می‌شود و مسیریاب از در بسته دریافت شده شماره مدار مجازی را استخراج و با توجه به جداول مسیریابی بسته را به سمت مقصد هدایت می‌کند.

نکته: دقت کنید که ممکن است همانطور که در شکل زیر دیده می‌شود فرآیند P_3 نیز بخواهد یک ارتباط با P_2 همزمان با P_1 داشته باشد. از آنجا که میزبانهای H_1 و H_3 از یکدیگر خبر ندارند و ممکن است شماره VC خود را یکسان (در اینجا شماره 1) انتخاب کرده باشند، مسیریاب باید یک شماره VC جدید برای H_3 انتخاب کند تا بسته‌های ارسالی P_1 و P_3 مخلوط نشوند.



در مسیریاب A بسته‌ای که از H_1 با شماره مجازی 1 می‌آید باید با همان شماره مجازی 1 به C برود اما بسته‌ای که از H_3 با شماره مجازی 1 آمده است باز هم به C اما با شماره مجازی 2 می‌رود.

مقایسه زیر شبکه‌های مدار مجازی و دیتاگرام

مورد مقایسه	دیتاگرام	مدارمجازی
تنظیم مدار (Circuit Setup)	مسیریاب نیاز به نگهداری اطلاعات در خصوص وضعیت هر اتصال ندارد.	به ازای هر مدار مجازی تمامی مسیریاب‌ها باید اطلاعاتی در خصوص وضعیت آن را نگه دارند (برای تضمین QOS)
آدرس‌دهی	براساس آدرس‌های مبدا و مقصد است.	بسته‌ها براساس یک شماره ID مخصوص به VC آدرس‌دهی می‌شوند.
مسیریابی (Routing)	به‌صورت پویا برای هر بسته مستقلاً انجام می‌شود.	فقط یکبار و آن هم در فاز برقرار اتصال و برپایه‌ازی مدار مجازی انجام شده و همه بسته‌های آن اتصال از آن مسیر هدایت می‌شوند.
تاثیر خرابی مسیریاب	فقط بسته‌هایی خراب می‌شوند که در حافظه مسیریاب خراب در آن در لحظه بار شده بودند.	همه مدارهای مجازی که از مسیریاب خراب عبور می‌کرده‌اند قطع می‌شوند.
تضمین QOS (کیفیت سرویس)	بسیار دشوار است. (مطالب اضافه‌تر در سایت IETF موجود می‌باشد)	در فاز برقراری مدار مجازی یک مذاکره بین کاربر و شبکه انجام می‌شود و کاربر ملزومات QOS خود را اعلام می‌کند و چنانچه شبکه قادر باشد بدون ایجاد مشکلاتی مثل ازدحام آن معیارها را تحقق بخشد و تحقق آن‌ها را تضمین نماید پس از رزرو منابع مورد نیاز، مدار مجازی را برقرار می‌کند و در غیراین صورت مکالمه را نمی‌پذیرد مگر اینکه کاربر توقع خود را کاهش دهد. به این فاز مذاکره CAC (Call Admission Control) می‌گویند.
کنترل ازدحام	بسیار دشوار است اما با مسیریابی پویا امکانپذیر است.	با تخصیص منابع شبکه در فاز CAC از ازدحام جلوگیری می‌شود.

۱ـ ۸ الگوریتم‌های مسیریابی

هر یک از الگوریتم‌های مسیریابی به‌طور کلی 6 ویژگی داشته باشند.

۱) صحت عملکرد (Correctness) : الگوریتم باید صحیح عمل کند

۲) سادگی (Simplicity) :

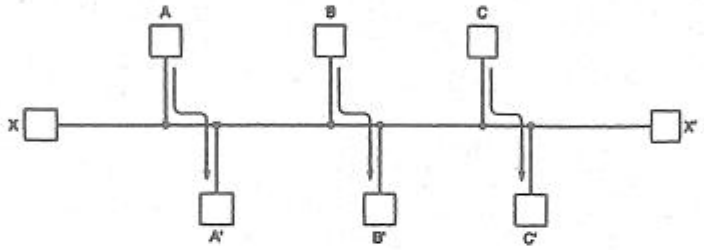
۳) قابلیت تحمل (Robustness) : خرابی سخت‌افزار و نرم‌افزار تاثیری بر عملکرد شبکه نگذارد. (شبکه را از کار نیاندازد)

۴) پایداری(Stability) : الگوریتم همگرا باشد زیرا اگر چنین شرطی وجود نداشته باشد در حلقه ابدی گرفتار خواهد شد.

۵) عدالت و مساوات (Fairness) : منابع به صورت عادلانه تقسیم شوند.

۶) بهینه بودن (Optimality)

برخی از این معیارها متاسفانه با هم در تضاد هستند مثلاً مساوات با بهینگی تضاد دارد و باید موازنه برقرار شود. در شکل زیر برای بهینگی باید ارتباط بین x با x′ قطع باشد تا 3 ارتباط دیگر برقرار شود ولی این با مساوات در تضاد است.



الگوریتم‌های مسیریابی به دو دسته تقسیم می‌شوند:

۱) وفقی (Adaptive) یا پویا ۲) غیروفقی(non Adaptive) یا ایستا

انتخاب مسیر در الگوریتم‌های وفقی بر اساس شرایط فعلی شبکه عوض می‌شود.

از طرف دیگر ا لگوریتم‌های مسیریابی را می‌توان به سه دسته تقسیم کرد:

۱) Centeralized (متمرکز)

۲) Distributed (توزیع شده)

۳) Hierarchical (سلسله مراتبی)

در الگوریتم‌های متمرکز اطلاعات وضعیت شبکه مانند توپولوژی و میزان ترافیک جاری در نقاط مختلف شبکه همگی در یک جا در درون هر مسیریاب متمرکز می‌شوند و هر مسیریاب کل اطلاعات شبکه را در اختیار دارد و تصمیم‌گیری به صورت محلی یا متمرکز انجام می‌شود.

اما در الگوریتم‌های مسیریابی توزیع شده تصمیم‌گیری به صورت توزیع شده است و اطلاعات وضعیت شبکه بر روی مسیریاب‌های مختلف توزیع شده است و تصمیم‌گیری (اجرای الگوریتم) نیز به صورت غیر متمرکز انجام می‌شود.

در روش سلسله مراتبی برای جلوگیری از بزرگ شدن بیش از حد جداول مسیریابی کل یک شبکه بسیار بزرگ را به تعدادی ناحیه(Region) تقسیم می‌کنیم. هر مسیریاب فقط اطلاعات مسیریابی مربوط به ناحیه خود را دارد ولی چیزی در خصوص جزئیات و ساختار داخلی دیگر نواحی ندارد. البته در شبکه‌های عظیم سلسله مراتب از دو سطح هم بیشتر است. در این شبکه‌ها هر ناحیه به تعدادی خوشه (Cluster) و هر Cluster به تعدادی Zone و هر Zone به تعدادی گروه (Group) تقسیم می‌شوند.

مسیریابی سلسله مراتبی : تعداد سطوح در درخت شبکه‌ای با N مسیریاب = معادل $\ln(N)$ ها است و هر مسیریاب به جهت $\ln(N)$ عدد در جدول نیاز خواهد داشت ← بهترین حالت تعداد سلسله مراتب طراحی کتاب کتن ۴۰

الگوریتم غیروفقی یا ایستا

۱ـ ۱ـ ۸ الگوریتم مسیریابی ابتدا کوتاه‌ترین مسیر Shortest Path

الگوریتم کوتاه‌ترین مسیر یک الگوریتم متمرکز است که در روی گراف شبکه برای رسیدن از یک گره (مسیریاب) به یک گره دیگر کوتاه‌ترین مسیر را انتخاب می‌کند. در این گراف به هر کمان یا Arc (linkها یا کانال‌های ارتباطی) یک وزن یا Weight تخصیص یافته است. منظور از کوتاه‌ترین مسیر مسیری است که مجموع وزن‌های کمان‌های درون آن حداقل باشد.

نکته : وزن‌ها معرف چه پارامترهایی از لینک‌های ارتباطی هستند؟

وزن‌ها می‌توانند معرف فاصله، تعداد گام(Hop)، پهنای باند، میانگین ترافیک، هزینه ارتباط، طول متوسط صف انتظار بسته‌ها در مسیریاب‌ها، تاخیر، گذردهی، نسبت از دست رفتن بسته‌ها، نوسان یا لرزش تاخیر و یا حتی ترکیبی از این پارامترها باشد؛ اما بیش از یک عدد نمی‌تواند به عنوان وزن هرلینک انتخاب شود.

الگوریتم‌های زیادی برای حل این مسئله (انتخاب کوتاه‌ترین مسیر) ارائه شده است. مشهورترین الگوریتم در سال 1959 توسط Dijkstra ارائه شد. در این الگوریتم هر گره دارای یک برچسب دو قسمتی است که حاوی فاصله آن با گره مبدا و نام گره‌ایست که آن گره را به گره مبدا متصل می‌کند. (با فاصله مذکور)

همچنین هر گره در طی پیشرفت الگوریتم یکی از دو وضعیت زیر را دارد:

- T یا Tentative یا موقتی
- P یا Permanent یا دایمی

گره دایمی گره‌ایست که برچسب آن مطمئناً کوتاه‌ترین مسیر تا مبدأ را نشان می‌دهد.

الگوریتم:

۱) برچسب همه گره‌ها تا مبدا را (∞,-) قرار دهید (یعنی فاصله آن تا مبدا ∞ و از طریق گره نامشخص)

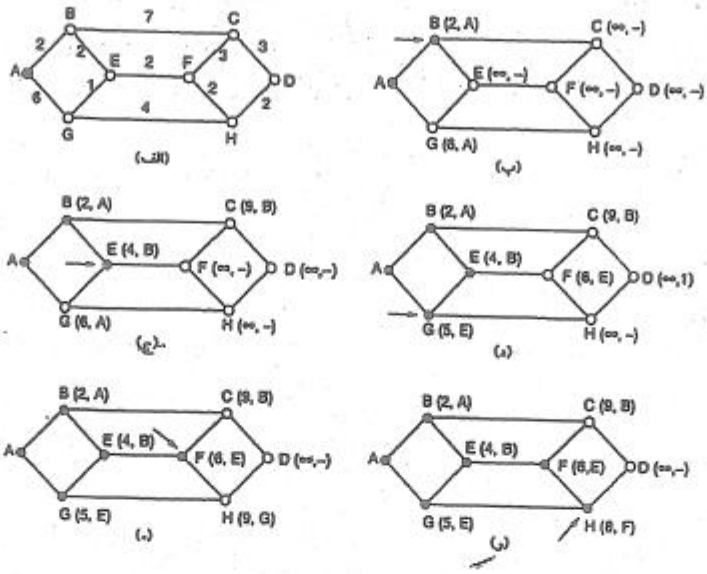
۲) از گره مبدا شروع می‌کنیم (فرقی کند؛ از مقصد هم می‌توانستیم شروع کرده و تا مبدا ادامه دهیم) آن را دایمی علامت بزنید. این گره را گره کار در نظر می‌گیریم.

۳) برای کلید همسایگان گره کار در صورتی که مجموع برچسب گره کار و فاصله گره کار تا آن گره از برچسب آن گره کوچکتر باشد، فاصله هر کدام با گره کار را (وزن link متصل را) با فاصله گره کار تا گره مبدا جمع کنید و به همراه نام گره کار به عنوان برچسب گره همسایه قرار دهید.

۴) به کلیه گره‌های موقتی نگاه کنید. کوچکترین آن‌ها را پیدا کنید و به عنوان گره کار در نظر بگیرید و آن را به صورت دایمی علامت بزنید.

۵) اگر همه گره‌ها دایمی نشده‌اند به قسمت ۳ مراجعه کنید.

اگر مثلاً 720 مسیریاب، اگر سلسله‌مراتب وجود نداشته باشد هر مسیریاب در جدول مسیریابی خود 720 درایه نیاز خواهد داشت. اگر از شبکه 24 منطقه و 30 مسیریاب در هر منطقه، هر مسیریاب به 30 درایه برای مسیریاب‌های که خود و (24-1) 23 درایه برای مناطق خارجی نیاز دارد. اگر سلسله‌مراتب سه سطحی انتخاب شود، چهار 8 دسته cluster، هر دسته شامل 9 ناحیه و در هر ناحیه 10 مسیریاب، چهار (1-9)+10+(1-8) = 25 درایه نیاز داریم



۲ـ ۱ـ ۸ الگوریتم مسیریابی بردار فاصله یا DVR (Distance Vector Routing)

الگوریتم DVR که نام‌های دیگر آن Bellman-Ford یا Ford-Fulkerson می‌باشد و برای اولین بار در شبکه ARPANET مورد استفاده قرار گرفت و سپس در اینترنت با نام RIP (Routing Information Protocol) به کار گرفته شد.

این الگوریتم به صورت زیر عمل می‌کند:

هر مسیریاب یک جدول مسیریابی دارد که به ازای هر مسیریاب موجود در زیر شبکه یک سطر در آن وجود دارد (مراجعه به جدول به کمک اندیس صورت می‌گیرد) در هر سطر دو فیلد زیر وجود دارد:

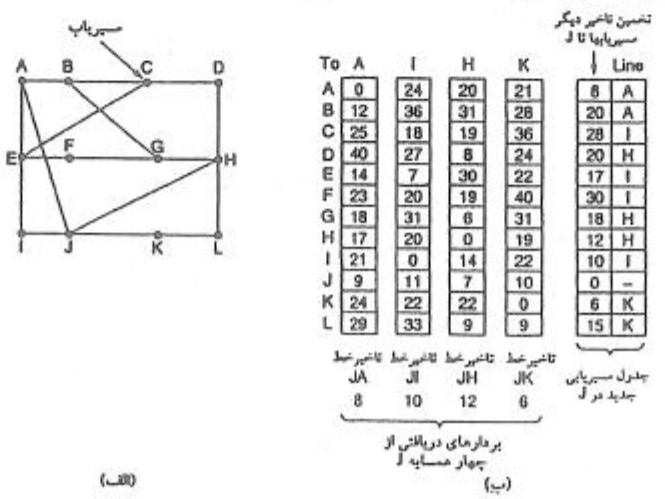
۱) link خروجی مناسب برای رسیدن به مقصد موردنظر

۲) تخمینی از زمان یا فاصله رسیدن به آن مقصد (این هزینه می‌تواند تعداد گام، تاخیر و یا هر پارامتر دیگر شبکه باشد.)

نحوه محاسبه یا تخمین هزینه

اگر هزینه، نشان‌دهنده تعداد گام باشد، فاصله هر گره با همسایگانش برابر یک در نظر گرفته می‌شود. اگر معیار، طول صف یا تاخیر صف باشد مسیریاب از صف‌های درون خود به سادگی مطلع است و اگر معیار، تاخیر کل، تاخیر انتشار یا صف باشد یک بسته خاص به نام Echo به سمت هر گره همسایه ارسال می‌شود همسایه موظف است فوراً آن را باز گرداند. می‌توان تاخیر کل را فاصله زمانی بین ارسال و دریافت تقسیم بر 2 در نظر گرفت. (با فرض این‌که شبکه متقارن است و زمان رفت و برگشت یکسان است.)

شکل زیر نحوه عملکرد این الگوریتم را نشان می‌دهد.



در این شکل می‌بینیم که گره J ابتدا بردار فاصله چهار همسایه خود را (A, I, H, K) را دریافت می‌کند و بر اساس این چهار بردار و فاصله خود از این چهار گره بردار فاصله خود را به روز در می‌آورد.

نکته : این الگوریتم مشکلات اساسی دارد که باعث منسوخ شدن آن شده است. اگرچه از نظر تئوری الگوریتم درست عمل می‌کند اما دو مشکل اساسی زیر دارد:

۱) کندی همگرا شدن

۲) این الگوریتم خبرهای خوب را به سرعت منتقل می‌کند اما در انتقال خبرهای بد واگرا می‌شود و گاهی هرگز همگرا نمی‌شود. خبر خوب یعنی یک نود یا link اضافه شد، ترافیک فلان جا کمتر شد، طول فلان صف کوتاه‌تر شد (برعکس این‌ها خبرهای بدی هستند) به طور کلی این الگوریتم Stable نیست و در برخی شرایط می‌تواند واگرا باشد.

مثال : در این شکل هزینه را تعداد گام می‌گذاریم.

	A	B	C	D	E
در بدو شروع Initially	•	•	•	•	•
پس از اولین مبادله جدول	1	•	•	•	•
پس از دومین مبادله جدول	1	2	•	•	•
پس از سومین مبادله جدول	1	2	3	•	•
پس از چهارمین مبادله جدول	1	2	3	4	•

(الف)

	A	B	C	D	E
در بدو شروع Initially	1	2	3	4	•
پس از اولین مبادله جدول	3	2	3	4	•
پس از دومین مبادله جدول	3	4	3	4	•
سومین مبادله جدول	5	4	5	4	•
چهارمین مبادله جدول	5	6	5	6	•
پنجمین مبادله جدول	7	6	7	6	•
ششمین مبادله جدول	7	8	7	8	•
	•	•	•	•	•

(ب)

از این‌جا به بعد A حذف شده و خبر بد حذف A باید منتقل شود.

برای حل این مشکل پیشنهاد شده است که حداکثر فاصله را معین کنیم.

۳ـ ۱ـ ۸ مسیریابی حالت پیوند یا LS (Link State)

مشکل شمارش تا بی‌نهایت (∞ Count to Infinity Problem) که در بالا شرح داده شد و الگوریتم RIP یا همان DVR را واگرا می‌کرد و موجب ناپایداری آن می‌شد باعث شد که در سال 1979 الگوریتم دیگری بنام LS جایگزین آن شود. الگوریتم LS مزیت دیگری نیز نسبت به DVR دارد و آن این است که علاوه بر طول صف پهنای باند را نیز در محاسبه تاخیر در نظر می‌گیرد. این الگوریتم در ۵ مرحله زیر عمل می‌کند.

۱) همه همسایگان خود را شناسایی کن و آدرس یکتای هر یک را بدست بیاور.

۲) تاخیر یا هزینه (فاصله) هر یک از همسایگان خود را با خود اندازه‌گیری کن. (تخمین بزن)

۳) بسته‌ای (Packet) بساز و اطلاعاتی که از همسایگان خود کسب کرده‌ای در آن جاسازی کن.

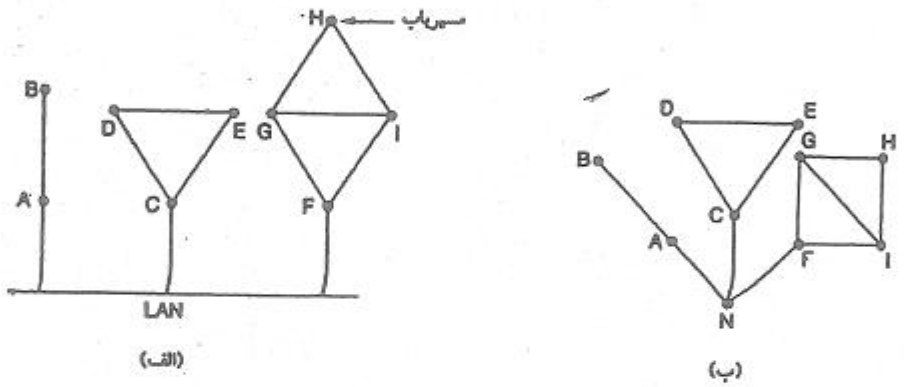
۴) این بسته را برای تمامی مسیریاب‌ها بفرست.

۵) با استفاده از الگوریتم کوتاه‌ترین مسیر Dijkstra کوتاه‌ترین مسیر رسیدن به هر یک از مسیریاب های شبکه را محاسبه کن.

مرحله ۱) شناسایی همسایه‌ها

هر گاه یک مسیریاب، boot شده و آغاز به کار می‌کند بر روی هر یک از پورت‌های خود بسته‌ای خاص بنام Hello packet را ارسال می‌کند و منتظر می‌نشیند تا پاسخ‌های سلام خود را بشنود. انتظار می‌رود مسیریاب های همسایه در پاسخ سلام آدرس خود را ارسال نمایند.

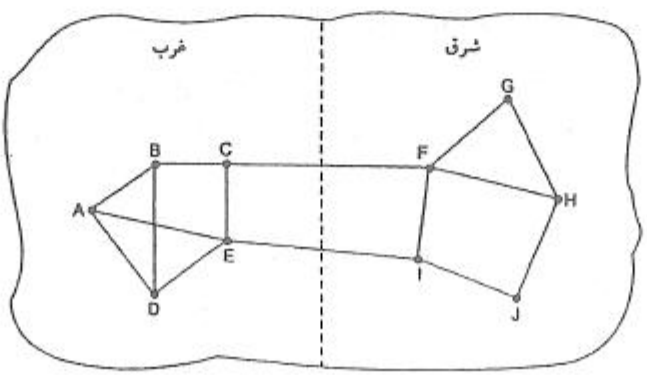
نکته : در شکل (الف) گره‌های A تا مسیریاب هستند. اما به یک شبکه LAN متصلند این توپولوژی را چگونه باید مدل کرد؟ برای مدل کردن آن می‌توان LAN را به صورت یک گره مصنوعی یا مسیریاب مصنوعی بنام N مدلسازی نمود. شکل (ب) این نکته را نشان می‌دهد.



مرحله ۲) اندازه‌گیری یا تخمین هزینه (تاخیر)

می‌خواهیم ببینیم وضعیت link بین ما با هر یک از همسایگانمان چگونه است و یک تخمین قابل قبول از تاخیر link ها بدست می‌آوریم. برای این کار یک بسته به نام Echo ارسال می‌کنیم و پس از بازگشت بسته Round Trip Time (RTT) را بر 2 تقسیم می‌کنیم. با فرض تقارن شبکه و تکرار این عمل و میانگین‌گیری تقریب خوبی از تاخیر بدست می‌آید.

نکته : چگونه می‌توان با توجه به حجم بار ترافیکی، بسته‌ها را از مسیر خلوت‌تر ارسال کرد؟به شکل زیر دقت کنید. خط چین عمودی شرق و غرب شبکه را از هم جدا می‌کند. تنها راه‌های ارتباطی غرب به شرق مسیر بالایی (BE) و مسیر پایین (DH) می‌باشد اگر اطلاعات وضعیت link ها نشان می‌دهد که خط پایین شلوغ است و اعلام کنیم که همه مسیر بالا را انتخاب کنند مسیر بالا دچار ازدحام خواهد شد و مجدداً اعلام می‌کنیم مسیر بالا شلوغ است و همه ترافیک را به مسیر پایین هدایت می‌کنیم این کار به جز این‌که باعث می‌شود جداول مسیریابی به طور متناوب نوسان کند و ترافیک سنگین به طور متناوب جابجا شود فایده دیگری ندارد.



نتیجه،راه‌حل معقول Load Balancing یا توازن بار می‌باشد باید شبکه مدیریت ترافیک و مهندسی ترافیک داشته باشد (Traffic Engineering) و بار ترافیکی که باید بر روی هر link قرار گیرد از قبل (با توجه به پهنای باند link) تعیین گردد.

مرحله ۳) ساخت بسته‌های وضعیت LINK (Link State Packet)

بسته وضعیت link حاوی فیلدهای زیر است:

۱) آدرس فرستنده

۲) شماره ترتیب (اولین بسته از صفر شماره‌گذاری می‌شود)

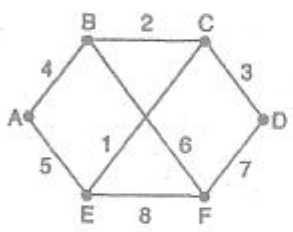
۳) Age یا TTL (Time To Live) کد یک شمارنده است و از مقدار معینی شروع می‌شود و هر دفعه (با عبور از هر مسیریاب یا گذشت یک ثانیه) یک واحد از آن کم می‌شود و هر وقت به صفر رسید این بسته از بین می‌رود.

۴) فهرست همسایه‌ها و وضعیت (تاخیر link بین ما و هر همسایه)

نکته : این بسته‌ها چه زمانی ارسال می‌شود؟ دو راه داریم

الف) پریودیک (در زمان‌های خاص)

ب) هر وقت تغییر ذاتی در توپولوژی شبکه یا وضعیت Link ها (میزان تاخیر و غیره) مشاهده شود.



(الف)

بسته‌های حالت لینک (Link State Packets)

نام مسیریاب	A	B	C	D	E	F
شماره ترتیب	Seq.	Seq.	Seq.	Seq.	Seq.	Seq.
طول عمر	Age	Age	Age	Age	Age	Age
	B 4	A 4	B 2	C 3	A 5	B 6
	E 5	C 2	D 3	F 7	C 1	D 7
		F 6	E 1		F 8	E 8

(ب)

مرحله ۴) توزیع بسته‌های Link state

مهم‌ترین نکته در توزیع این بسته‌های LS همگام‌سازی مسیریاب های دریافت کننده این بسته‌ها است زیرا اگر بعضی از router ها زودتر این بسته‌ها را دریافت کنند و جداول مسیریابی خود را به روز درآورند ولی هنوز این بسته‌ها توسط مسیریاب های دیگر دریافت نشده باشد اختلاف بین این جداول مشکلاتی از قبیل پیدایش حلقه بی‌نهایت و جدا شدن بعضی از مسیریاب‌ها را در توپولوژی شبکه ایجاد می‌کند.

یک راه‌حل برای این مشکل الگوریتم مسیریابی سیل‌آسا (Flooding) است. که موردبحث قرار خواهد گرفت.

نکته : دقت شود که برای این‌که جداول نگهدارنده این بسته‌ها بیش از حد بزرگ و پردازش آن‌ها پیچیده نشود و اطلاعات زائد در آن نباشد باید آخرین بسته ارسالی از هر مسیریاب را جایگزین قبلی نماییم اما طبق الگوریتم سیل‌آسا ممکن است بسته قدیمی بعد از بسته جدید از راه برسد و در نتیجه اعتبار اطلاعات از بین می‌رود. (چون جایگزین اطلاعات جدید می‌شود) راه‌حل این مشکل استفاده از شماره ترتیب است. بنابراین در صورتی بسته دریافتی جایگزین می‌شود که شماره ترتیب آن بزرگتر از قبلی باشد.

نکته : اگر محدودهٔ شماره کوچک باشد مثلاً 4 بیتی بعد از 16 بسته دوباره reset شده و طبق الگوریتم فوق بسته‌های دیگر در نظر گرفته نمی‌شوند. راه‌حل این است که محدوده شماره را 32 بیتی و بزرگ در نظر بگیریم.

همچنین با گذشت زمان طبق فیلد Age بسته Expired یا منقضی می‌شود.

مرحله ۵) محاسبه مسیرهای جدید

این کار توسط الگوریتم کوتاه‌ترین مسیر Dijkstra به راحتی انجام می‌شود.

پروتکل OSPF (Open Shortest Path First)

الگوریتم باز ابتدا کوتاه‌ترین مسیر (OSPF) یکی از رایج‌ترین الگوریتم‌های مسیریابی شبکه اینترنت است. این پروتکل توسعه یافته الگوریتم LS محسوب می‌شود.

پروتکل IS – IS (Intermediate System Intermrdiate System)

این پروتکل نیز مبتنی بر اطلاعات وضعیت link بوده و توسط شرکت Dec Net با توسعه LS بوجود آمده است. این پروتکل برای لایه شبکه CLNP که در محصولات این شرکت به کار می‌رفت طراحی شد. اما این پروتکل ویژگی بسیار جالبی دارد و قادر است همزمان با چندین پروتکل شبکه کار کند. Novel Netware نیز از این پروتکل برای هدایت بسته‌های IPX در لایه شبکه خود استفاده می‌کرد. به عبارت دیگر همزمان می‌توان چندین استاندارد آدرس‌دهی شبکه مانند Apple talk، CLNP، IP و IPX را با این پروتکل پشتیبانی کرد.

این ویژگی مهم در OSPF دیده نمی‌شود. IS – IS در ستون فقرات بخش‌های مهمی از شبکه اینترنت به کار رفته است .

۴ـ ۱ـ ۸ الگوریتم سیل‌آسا (Flooding)

در این الگوریتم سیلی از بسته‌ها از مسیرهای مختلف در آن واحد به سمت مقصد (در واقع در همه جهات) ارسال می‌شود. هر مسیریاب موظف است با دریافت آن بسته یک نسخه از آن را به تمام پورت‌های خروجی ارسال کند. واضح است که در این الگوریتم بسته‌های تکراری از مسیرهای مختلف به کلیه گره‌ها خواهد رسید و تولید بسته‌های تکراری موجب ازدحام و اشباع شبکه خواهد شد. برای حل این مشکل پیشنهاداتی ارائه شده است:

۱) یک شمارنده گام (Hop counter) داشته باشیم و در Header بسته قرار دهیم و در هر گام یک واحد از آن کم کنیم و پس از صفر شدن آن، بسته را دور بریزیم.

۲) فهرست بسته‌های سیل‌آسای ارسالی از هر گره مبدا را از طریق شماره ترتیب آن نگهداری نمائید و از ارسال مجدد بسته‌های تکراری جلوگیری کنیم.

۳) برای اجتناب از طولانی شدن این لیست فقط کافی است آخرین بسته (بزرگترین شماره ترتیب) مربوط به هر گره مبدا را لیست کنیم.

کاربردهای الگوریتم سیل‌آسا

۱) سیستم‌های نظامی

۲) پایگاه‌های داده توزیع شده

۳) شبکه‌های بی‌سیم

۴) شاخص برای مقایسه و ارزیابی سایر الگوریتم‌ها (نکته در این‌جاست که این الگوریتم بسته را در سریع‌ترین زمان ممکن خواهد رساند چون بهترین مسیر حتماً در بین مسیرها وجود دارد.) البته از سربار این الگوریتم چشم پوشی کرده‌ایم.

۵ـ ۱ـ ۸ مسیریابی انتشاری یا (Broadcast Routing)

برای انتشار بسته‌ها در لایه شبکه در شبکه‌ای مانند اینترنت چه باید کرد؟ هر یک از الگوریتم‌های زیر را می‌توان برای انتشار بسته‌ها از یک مبدا به همه میزبان‌های درون شبکه پیشنهاد کرد. البته هر روش مزایا و معایب خود را دارد.

روش ۱) یک لیست از آدرس همه مقاصد داشته باشیم و در یک حلقه به صورت نقطه به نقطه بسته را به یکایک ماشین‌ها ارسال کنیم. مشکلات این روش عبارتند از اتلاف پهنای باند، کندبودن الگوریتم و نیاز به نگهداری فهرست طولانی از آدرس‌ها

روش ۲) استفاده از الگوریتم مسیریابی سیل‌آسا

روش ۳) مسیریابی چندمقصدی (Multi-Destination Routing) : در این روش در آدرس بسته یک نگاشت بیتی وجود دارد (Bitmap) که هر بیت آن یکی از گره‌های شبکه را نشان می‌دهد. حال فرض کنید یک بسته انتشاری به یک گره می‌رسد بیت مربوط به خود را reset می‌کند و بسته را در صورتی به سمت link های خروجی می‌فرستد که بیت مربوط به گره متصل به آن link یک باشد (reset نشده باشد.)

روش ۴) استفاده از درخت پوشا (Spaning Tree): درخت پوشا درختی است (بدون حلقه) که شامل همه‌گره‌های شبکه می‌شود. اگر بهینه باشد به آن Sink Tree می‌گویند.

نکته : Spaning Tree واحد نیست. کافی است مسیریاب‌ها، اطلاعات یکی از درخت‌های پوشا را داشته باشند و بسته را از طریق این درخت یا شاخه‌های این درخت به همه گره‌ها برسند. مسیریاب با استفاده از اطلاعات وضعیت link ها می‌تواند این درخت را پیدا کند.

روش ۵) Reverse Path Forwarding (هدایت بر روی مسیر معکوس)

هر گره فقط بسته‌های پخشی را در صورتی می‌پذیرد که از مسیری دریافت شده باشد که برای ارسال یک بسته معمولی، آن بسته از طریق آن مسیر به سمت گره مبدا بسته‌های پخشی ارسال می‌شود. به عبارت دیگر بسته‌هایی که از سایر link ها دریافت می‌شود دور ریخته می‌شود تا از تکرار بسته‌های اضافی جلوگیری شود. بسته‌ای که از مسیر معکوس دریافت می‌شود به سمت هر یک از گره‌های مجاور ارسال می‌شود.

۶ـ ۱ـ ۸ مسیریابی چندپخشی یا (Muticast Routing)

در این‌جا، بحث گروه‌های کاری پیش می‌آید و یک بسته را باید به تعدادی گره (اعضای گروه) ارسال نمائیم.

۷ـ ۱ـ ۸ مسیریابی در شبکه‌های بی‌سیم متحرک

پیچیدگی این شبکه‌ها بسیار زیاد است زیرا ماشین‌ها حرکت می‌کنند و از یک حوزه وارد حوزه‌های دیگر می‌شوند. مثلا در شبکه تلفنی سلولی از یک سلول وارد سلول‌های دیگر می‌شوند.

در این شبکه‌ها چند مفهوم جدید تعریف می‌شود.

۱) ماشین متحرک یک محل استقرار دایمی دارد. اگرچه ممکن است در آن‌جا نباشد (مثل یک تلفن همراه که اگرچه شماره تهران (محل استقرار دایمی) است اما ممکن است اکنون در تبریز باشد.)

۲) یک عامل خانگی (Home Agent) که یک برنامه است در محل استقرار دایمی وجود دارد. (برای مثال ما در تهران)

۳) در هر ناحیه خارجی (شبکه از نظر جغرافیایی به چند ناحیه تقسیم می‌شود) یک عامل خارجی (Foreign Agent) وجود دارد وقتی ماشین متحرک واحد ناحیه خارجی می‌شود صبر می‌کند تا یک پیغام از عامل خارجی دریافت کند. این پیغام مبنی بر این است

که آیا ماشین متحرک خارجی در این ناحیه وجود دارد؟ اگر ماشین متحرک منتظر شود و این پیغام را دریافت نکند خودش یک پیغام منتشر می‌کند که آیا یک عامل خارجی در این‌جا وجود دارد؟

خلاصه در صورتی‌که عامل خارجی ماشین خارجی را پیدا کند ماشین متحرک در آن عامل خارجی ثبت‌نام می‌کند. عامل خارجی یک پیغام به عامل خانگی می‌فرستد (در مثال ما از تبریز به تهران) تا از این پس بسته‌های به مقصد ماشین متحرک به حوزه خارجی مربوط مسیریابی شود.

۲ـ۸ کیفیت خدمات (Quality of Services)

در تمامی شبکه‌های کامپیوتری پیشرفته تکنیک‌هایی متعدد وجود دارد که تمرکز ویژه‌ای بر روی تضمین کیفیت خدمات (QoS) متناسب با نیازهای برنامه‌های کاربردی دارند. این نیازها با چهار پارامتر " قابلیت اطمینان "، " تاخیر"، " لرزش"، و " پهنای باند" مشخص می‌شوند. راهکارهای مختلف دستیابی به کیفیت خوبِ خدمات به شرح زیر می‌باشد:

کنترل ازدحام (Conjestion Control) و شکل‌دهی ترافیک

سیاست‌های مختلفی در لایه‌های مختلف شبکه برای کنترل و پیش‌گیری از ازدحام پیشنهاد شده است. در هر حال دقت کنید که سیاست‌های گوناگونی بر پدیده ازدحام تاثیر مثبت یا منفی می‌گذارند. برای مثال در لایه پیونده داده سیاست ارسال مجدد، سیاست کنترل جریان، سیاست ارسال ACK و سیاست ذخیره بسته‌های خارج از ترتیب بر ازدحام تاثیر می‌گذارند.

همچنین در لایه شبکه سیاست‌هایی از جمله مسیریابی، طول عمر بسته‌ها، روش‌های مدار مجازی و رزرو منابع، مکانیزم‌های صف‌بندی و حذف بسته‌های اضافی بر کاهش ازدحام موثر خواهند بود.

همچنین در لایه انتقال سیاست‌هایی نظیر ارسال مجدد، ACK ذخیره بسته‌های خارج از ترتیب، کنترل جریان و زمان انقضای تایمرها بر ازدحام موثرند.

نکته ۱: یکی از بهترین مکانیزم‌ها برای جلوگیری از ازدحام ایجاد مدار مجازی و رزرو منابع، توسط پروتکل‌هایی نظیر RSVP است

نکته ۲: چگونه می‌توان در روش‌هایی مانند دیتاگرام از ازدحام اجتناب کرد؟

برای کنترل ازدحام در این شبکه‌ها مکانیزم‌های مختلفی پیشنهاد شده است که چند مورد از آن‌ها عبارتند از:

۱) Set کردن بیت هشدار در بسته‌ها در مواقعی که حجم ترافیک از یک حد آستانه بالاتر می‌رود.

۲) ارسال بسته‌های خاص دعوت به آرامش (Chock) در شرایطی که حجم ترافیک سنگین شده است.

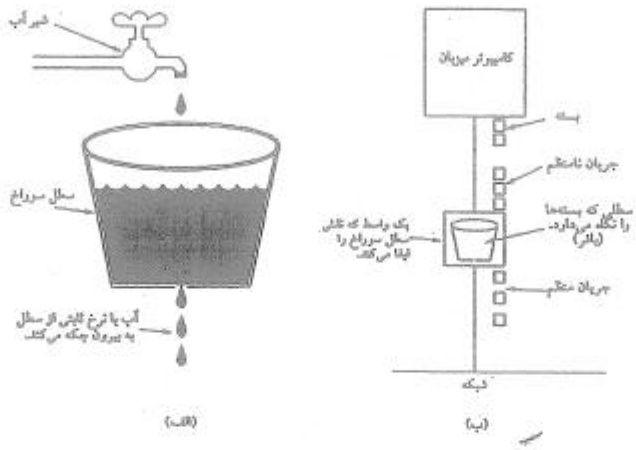
۳) دور ریختن بار اضافی مشتریان در صورتی‌که مشتری‌ها از تعهدات مندرج در مذاکره اولیه تخطی کرده‌اند.

نکته ۳: برای کنترل Jitter چه باید کرد؟

این کار به راحتی انجام می‌شود. بسته‌هایی‌که با نرخ متغیر و فواصل زمانی متفاوت دریافت می‌شوند در یک بافر ذخیره کرده و از یک طرف بسته‌ها را با نرخ ثابت از بافر خارج می‌کنیم.

نکته ۴: الگوریتم سطل سوراخ‌دار (Leaky Bucket) یکی از الگوریتم‌هایی است که در جهت افزایش QOS و کاهش ازدحام و جلوگیری از تحمیل بار اضافی توسط مشتری‌ها یا میزبان‌ها بر شبکه طراحی شده است. فرض کنید ترافیک نامنظمی را که یک کاربر ارسال می‌کند با قطره‌های نامنظم و تصادفی که به یک سطل سوراخ وارد می‌شوند مدل کنیم. همچنین فرض کنید که بافر اولین مسیریاب سر راه این بسته‌ها را تقسیم کنیم و یک فضای خاص با حجم معین به آن مشتری اختصاص دهیم (مدل این بخش از بافر، سطلی است که ظرفیت مشخصی دارد و در صورت پر شدن سرریز شده و بار اضافی ورودی دور ریخته

می‌شود.) از آن‌جا که اندازه سوراخ زیر سطل ثابت است قطرات از خروجی سیستم به‌طور منظم و با نرخ ثابت از بافر سطل خارج می‌شوند.



رزرو منابع (Resource Reservation)

توانایی شکل‌دهی و تنظیم ترافیک ارسالی، تمهید خوبی برای تضمین « کیفیت خدمات » (QoS) محسوب می‌شود ولیکن استفاده از این روش‌ها زمانی کارآمد خواهد بود که تمامی بسته‌ها از مسیر یکسانی عبور کنند. پراکندگی تصادفی بسته‌ها بر روی مسیرهای متفاوت، تضمین هر چیزی را بسیار دشوار می‌کند. بنابراین برای تامین کیفیت خدمات باید بین مبدا و مقصد چیزی شبیه به یک مدار مجازی ایجاد و تنظیم شود و تمام بسته‌های یک « جریان » از این مسیر حرکت کنند.

هر گاه برای جریان داده‌ها، مسیر ویژه داشته باشیم می‌توان منابع لازم را در طول این میسر، رزرو کرده و موجود بودن ظرفیت موردنیاز را تضمین کرد. سه نوع متفاوت از منابع را می‌توان از قبل رزرو کرد:

۱ـ پهنای باند

۲ـ فضای بافر

۳ـ سیکلهای CPU [ظرفیت پردازش موردنیاز]

کنترل پذیرش (Admission Control)

حال در مرحله‌ای هستیم که ترافیک ورودی از یک « جریان » (Flow) خاص به خوبی شکل و نظم داده شده و بسته‌ها از یک مسیر واحد حرکت می‌کنند و پیشاپیش ظرفیت موردنیاز در طول مسیر، پیش‌بینی و رزرو شده است. با چنین فرضی، هر گاه جریانی از بسته‌ها به یک مسیریاب تسلیم شود بر اساس ظرفیت موجود خود و سطح تعهداتی که در خصوص دیگر جریان‌ها پذیرفته، باید در خصوص قبول یا رد آن تصمیم بگیرد.

چونکه برای رسیدن به توافق نهایی در خصوص تامین نیازهای یک « جریان » باید مولفه‌های متعددی در مذاکرات شرکت داشته باشند (اعم از فرستنده، گیرنده و تمام مسیریاب‌های واقع بر روی مسیر)، لذا هر « جریان » باید بر حسب پارامترهای مشخصی به‌دقت توصیف شود تا بتوان بر روی این پارامترها مذاکره و توافق کرد. مجموعهٔ چنین پارامترهایی اصطلاحاً « مشخصات توصیفی جریان » (Flow Specification) نامیده می‌شود. بدین‌ترتیب یک فرستنده (مثل سرویس‌دهنده ویدیو) مشخصات توصیفی جریان را به صورت پارامترهای پیشنهادی و موردنظر خود تعریف می‌نماید. این پارامترهای پیشنهادی در طول مسیر منتشر می‌شود و هر مسیریاب واقع بر مسیر آن‌ها را بررسی کرده و درصورت نیاز در آن‌ها تغییراتی ایجاد می‌کند. این تغییرات فقط کاهشی است نه افزایشی (یعنی مثلاً نرخ موردنظر ارسال داده‌ها را کاهش می‌دهد نه افزایش). وقتی این پارامترها به طرف مقابل برسد، به اجرا گذاشته می‌شوند.

زمان‌بندی بسته‌ها

هرگاه یک مسیریاب هدایت چندین « جریان » را بر عهده داشته باشد این خطر وجود داردکه یک «جریان» از حدود و ظرفیت مجاز خود تجاوز نماید و در نتیجه جریان‌های دیگر را با کمبود منابع (Starvation) مواجه سازد. اگر پردازش بسته‌ها به ترتیب ورودشان انجام گیرد باعث می‌شود که یک فرستنده متجاوز بتواند بیشتر ظرفیت مسیریاب‌هایی را که بر روی خط سیر بسته‌های او هستند اشغال کرده و کیفیت خدمات دیگران کاهش یابد. برای خنثی کردن چنین تلاشی، الگوریتم‌هایی جهت زمان‌بندی بسته‌ها پیشنهاد شده است.

یکی از اولین روش‌ها، الگوریتم « صف‌بندی بی‌طرفانه» (Fair Queuing) است. جوهره این الگوریتم آن است که مسیریاب‌ها باید برای هر خط خروجی و به ازای هر « جریان » که از آن خط خروجی می‌گذرد، صف‌های جداگانه‌ای تشکیل بدهند. هر گاه خطی بیکار شود، مسیریاب‌ها صف‌ها را به ترتیب پویش کرده و از سر هر صف یکی را بر می‌دارد. بدین‌ترتیب، در شرایطی که n ماشین میزبان برای یک خط خروجی رقابت می‌کنند، از هر n بسته ارسالی بر روی خط یک بسته به هر ماشین میزبان تعلق می‌گیرد. افزایش نرخ ارسال بسته‌ها، در نسبت سهم هر ماشین تغییری ایجاد نخواهد کرد.

یک اشکال این الگوریتم آن است که به تمام ماشین‌های میزبان، اولویت یکسانی می‌دهد. در بسیاری از محیط‌ها مطلوب‌تر آن است که به سرویس‌دهنده‌های ویدیو (Video Server) اولویت بیشتری نسبت به یک سرویس‌دهنده معمولی فایل داده شود و در هر تیک ساعت، سهم آن دو یا چند بایت باشد. این الگوریتم اصلاح شده به نام الگوریتم صف‌بندی بی‌طرفانهٔ وزن‌دار» Weighted Fair) (Queuing مشهور است و کاربرد گسترده‌ای دارد.

۱ ـ ۲ ـ ۸ خدمات مجتمع (Integrated Services)

در خلال سال‌های 1995 تا 1997، تلاش IETF بر آن بود که برای انتقال داده‌های مالتی مدیا (Multimedia Streaming) معماری مناسبی ابداع کند. این پروژه با نام کلی « الگوریتم‌های مبتنی بر جریان» (Flow – based algorithms) یا « خدمات مجتمع » (Integrated Services) شناخته می‌شود و کاربردهای چند پخشی (Multicast) و تک پخشی (Unicast) را در بر می‌گیرد.

به عنوان مثالی از کاربردهای چندپخشی، ایستگاه‌های پخش تلویزیون دیجیتال را در نظر بگیرید که برنامه‌های خود را در قالب جریانی از بسته‌های IP به گیرندگان بی‌شمار و پراکندهٔ خود ارسال می‌دارند.

RSVP [1]: پروتکل رزرومنابع

اصلی‌ترین پروتکل پیشنهاد شده توسط IETF برای ارائه خدمات مجتمع، RSVP نامیده می‌شود و برای رزرو کردن پهنای باند به‌کار می‌آید.

RSVP اجازه می‌دهد که چندین فرستنده بتوانند برای چندین گروه از گیرندگان خود داده بفرستند و همچنین امکان آن را فراهم کرده که گیرندگان بتوانند کانال موردنظر خود را آزادانه عوض کنند. در عین حال پروتکل RSVP، استفاده از پهنای باند را بهینه‌سازی کرده و از بروز ازدحام جلوگیری می‌کند.

در ساده‌ترین حالت این پروتکل از روش « مسیریابی چندپخشی مبتنی بر درخت پوشا» بهره می‌گیرد. به هر گروه یک آدرس یکتا انتساب داده می‌شود و برای ارسال یک بسته به گروه خاص، آدرس آن گروه در بسته قرار می‌گیرد. سپس توسط الگوریتم استاندارد مسیریابی چند پخشی، یک درخت پوشا که تمام اعضای آن گروه را در بر می‌گیرد، ایجاد می‌گردد.

---

[1] Resource Reservation Protocol

۲ـ۲ـ۸ خدمات متمایز (Differentiated Services)

«الگوریتم‌های مبتنی بر جریان» قابلیت عرضه کیفیت خوب خدمات به یک یا چند جریان را دارند زیرا در طول مسیر هر منبعی را که نیاز است از قبل رزرو می‌کنند. ولی این روش‌ها یک اشکال دارند: در این الگوریتم‌ها نیاز است که برای هر جریان (Flow) پیشاپیش تنظیمات لازم انجام شود در حالی که در مقیاس کلان یعنی وقتی که هزاران یا میلیون‌ها « جریان » وجود دارد قابلیت اجرایی خود را از دست می‌دهند. از طرفی در هر مسیریاب « وضعیت » هر جریان به‌طور جداگانه نگهداری می‌شود و عملکرد این الگوریتم‌ها در مقابل خرابی یک مسیریاب آسیب‌پذیر خواهد بود. نهایتاً آن‌که برای تنظیم و ایجاد « جریان » باید تبادل اطلاعات پیچیده‌ای بین مسیریاب‌ها انجام گیرد. در نتیجه RSVP یا الگوریتم‌های مشابه آن بسیار کم پیاده‌سازی عملی شده‌اند.

به همین دلایل، IETF راهکارهای ساده‌تر برای تامین کیفیت خدمات (QoS) ابداع کرد؛ روشی که بدون نیاز به هیچ تنظیمات قبلی یا تعیین کل مسیر می‌تواند به صورت محلی و مجزا در هر مسیریاب پیاده‌سازی شود. این راهکار اصطلاحاً « روش مبتنی بر کلاس » (Class – Based) برای تضمین کیفیت خدمات نامیده می‌شود (در مقابل روش‌های مبتنی بر جریان). IETF یک معماری مناسب به نام «خدمات متمایز » برای آن طراحی و استانداردسازی کرده است.

« خدمات متمایز » (که به اختصار DS گفته می‌شود) می‌تواند توسط مجموعه‌ای از مسیریاب‌ها که در یک «حوزهٔ مدیریتی واحد» (Administrative Domain) قرار می‌گیرند (مثلاً یک ISP یا شرکت مخابرات)، عرضه شود. مدیریت مسئول شبکه، مجموعه‌ای از کلاس‌های متفاوت خدمات و متناظر با آن، قواعد هدایت بسته‌ها (Forwarding Rules) را تعریف می‌کند.

اگر یک مشتری برای دریافت خدمات نوع DS تقاضای ورود به شبکه را بدهد، بسته‌های ارسالی او در ورود به حوزه، فیلد « نوع خدمات » (Type of Service) را با خود حمل می‌کنند تا به برخی از آن‌ها خدمات بهتری (مثل خدمات ویژه) ارائه شود. ممکن است لازم باشد ترافیک تعریف شده در هر کلاس از شکل خاصی پیروی نماید (مثلاً باید از الگوریتم سطح سوراخ با نرخ خروجی مشخص تبعیت کند). متصدی شبکه با گرایشات اقتصادی و تجاری ممکن است برای انتقال « بسته‌های ویژه » (Premium Packets) هزینه اضافی بگیرد یا مثلاً به ازای بهای اشتراک ثابت و ماهانه، تعداد N بسته ویژه از کاربر پذیرفته و هدایت شود. دقت کنید که این الگو نیاز به تنظیمات قبلی، رزروسازی منبع و نیازی به اتلاف وقت برای مذاکره بین طرفین نهایی در هر « جریان » ندارد. به همین دلیل پیاده‌سازی خدمات DS بسیار آسان است.

برای بسته‌های حاوی اطلاعات، کلاس‌های متفاوت خدمات بر حسب میزان« تاخیر »، «لرزش» (Jitter)، احتمال حذف بسته در صورت بروز ازدحام و امکاناتی نظیر همین‌ها تعیین می‌شود.

برای آن‌که تفاوت بین « کیفیت خدمات مبتنی بر جریان » و « کیفیت خدمات مبتنی بر کلاس » روشنتر شود نمونه‌ای مثل « تلفن اینترنتی» را مدنظر قرار بدهید. در روش مبتنی بر جریان، هر تماس تلفنی منابع خاص خود و تضمین‌های لازم را از شبکه اخذ می‌کند. در روش مبتنی بر کلاس تمام تماس‌های تلفنی همگی از منابع رزرو شده‌ای که برای « کلاس تلفنی » تهیه دیده شده، استفاده می‌کنند. این منابع در اختیار بسته‌هایی که در کلاس انتقال فایل یا کلاس‌های دیگر هستند، قرار نمی‌گیرد و صرفاً برای « کلاس تلفنی » پیش‌بینی شده است ولی این‌گونه هم نیست که برای هر تماس تلفنی منابع اختصاصی و مجزا در نظر گرفته شود.

۳ـ۲ـ۸ سوییچ برچسب و MPLS [1]

در ابتدای هر بسته یک «برچسب» (Label) اضافه شود و به‌جای آن‌که مسیریابی و هدایت بسته‌ها مبتنی بر آدرس مقصد باشد براساس این «برچسب» انجام شود. با استفاده از این «برچسب» به عنوان یک اندیس در جدول داخلی هر مسیریاب، خط خروجی

---

[1] Multi Protocol Label Switching

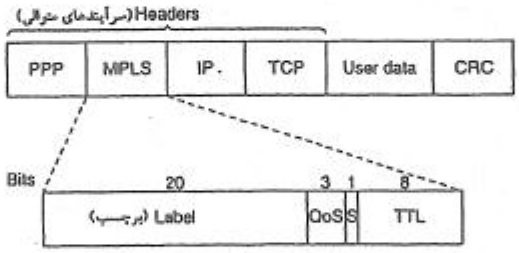
صحیح و مناسب برای هر بسته پیدا می‌شود. به کمک این روش، مسیریابی بسته‌ها به سرعت انجام شده و منابع موردنیاز در طول مسیر رزرو خواهد شد.

البته برچسب‌گذاری بر روی هر «جریان» شباهت عجیبی به مدارهای مجازی پیدا می‌کند. در شبکه‌های ATM، X.25 و Frame Relay یا هر زیر شبکه مدار مجازی دیگر نیز یک « برچسب» (یا به عبارتی یک شناسهٔ مدار مجازی) در هر بسته قرار داده می‌شود و با استفاده از آن به عنوان یک اندیس برای درایه‌های جدول، مسیر مناسب به‌دست می‌آید.

ایدهٔ جدید سوییچینگ با نام‌های متنوعی مثل «سوییچینگ برچسب»[1] یا « سوییچینگ علامت»[2] شناخته می‌شود. در نهایت IETF آن را تحت نام MPLS استاندارد کرد.

مضاف بر این، برخی افراد بین «مسیریابی » و « سوییچینگ » فرق می‌گذارند. مسیریابی فرآیند جستجو در جدول مسیریابی به دنبال آدرس مقصد هر بسته و پیدا کردن خط مناسب برای آن است. برعکس در فرآیند سوییچینگ از برچسب هر بسته به عنوان یک اندیس در جدول مسیریابی استفاده می‌شود و با استفاده از این اندیس بلافاصله خط خروجی پیدا می‌شود، بدون آن که نیازی به جستجو باشد. البته این تعاریف و تعابیر جهان شمول و همگانی نیستند.

اولین مسئله آن است که این برچسب در کجا قرار داده شود. از آنجایی که بسته‌های IP برای شبکه‌های مدار مجازی طراحی نشده بودند، طبعاً هیچ فیلدی در سرآیند بستهٔ IP برای درج شماره‌های مدار مجازی وجود ندارد به همین دلیل سرآیند جدید MPLS، باید در جلوی سرآیند هر بسته IP قرار بگیرد. در خطوط مستقیم بین هر دو مسیریاب که مبتنی بر « فریمینگ PPP » کار می‌کنند ترتیب سرآیندها طبق شکل زیر عبارتند از: سرآیند PPP، سرآیند MPLS، سرآیند IP و نهایتاً سرآیند TCP. در واقع باید MPLS را در لایه 2.5 فرض کرد!!!



ارسال یک قطعه TCP (TCP Segment) با استفاده از IP , MPLS، و PPP.

سرآیند عمومی MPLS (MPLS Header) چهار فیلد دارد که مهم‌ترین آن‌ها فیلد Label (فیلد برچسب) است که در آن یک اندیس درج می‌شود. فیلد QoS، کلاس خدمات را مشخص می‌کند. فیلد S بدان منظور تعریف شده که در شبکه‌های سلسله مراتبی چندین سرآیند MPLS متوالیاً به بسته اضافه گردد. فیلد TTL زمان حیات بسته را مشخص می‌کند و به ازای هر گام یک واحد از آن کم می‌گردد؛ هر گاه مقدار این فیلد به صفر برسد، بسته حذف می‌شود. این ویژگی بدان منظور مفید است که از حلقهٔ بی‌نهایت که در اثر ناپایداری (عدم همگرایی) جدول مسیریابی بروز می‌کند، اجتناب شود.

از آنجایی که سرآیند MPLS بخشی از بسته لایه شبکه یا فریم لایه پیوند داده‌ها محسوب نمی‌شود لذا MPLS تا حد زیادی مستقل از هر دو لایه است. از بین تمام محاسن دیگر، دستاورد ویژگی « استقلال از دیگر لایه‌ها » آن است که می‌توان سوییچ‌های MPLS را به گونه‌ای ساخت که بتواند هم بسته‌های IP و هم سلول‌های ATM را برحسب مورد، هدایت کند. این ویژگی همانی است که براساس

---

[1] Label Switching

[2] Tag Switching

آن کلمه Multiprotocol در ابتدای نام MPLS ظاهر شده است.

وقتی یک بسته یا سول غنی‌شده با سرآیند MPLS در یک مسیریاب MPLS دریافت می‌شود از برچسب آن به عنوان اندیسی در جدول داخلی مسیریاب استفاده شده و خط خروجی متناسب با آن تعیین می‌شود و قبل از خروج بسته از آن خط، برچسب جدیدی در فیلد مربوطه درج می‌گردد. تغییر در برچسب‌ها در تمام زیر شبکه‌های مدار مجازی معمول و متعارف است چرا که برچسب‌ها در هر مسیریاب معنای محلی دارند و دو مسیریاب متفاوت ممکن است بسته‌های نامربوط را با برچسبی یکسان برای مسیریاب دیگر بفرستند چرا که این بسته‌ها همگی در بخشی از مسیر مشترک‌اند. به همین دلیل در هر گام برچسب‌های بسته قبل از انتقال بر روی خط خروجی به برچسب جدید و معتبر در مسیریاب بعدی نگاشته می‌شود.

فصل نهم

پروتکل اینترنت (IP)[1]

جوهرهٔ اینترنت به گونه‌ای شکل گرفته است که مجموعه ای از شبکه‌های خودمختار[2] را به همدیگر وصل می‌نماید. هیچگونه ساختار حقیقی و ثابتی نمی‌توان برای اینترنت متصوّر شد. این نکته را بایستی یادآور شویم که در قسمت "زیرشبکه" از شبکهٔ اینترنت، تعدادی از خطوط ارتباطی با پهنای باند (نرخ ارسال) بسیار بالا و مسیریاب‌های بسیار سریع و هوشمند، برای پیکرهٔ شبکهٔ جهانی اینترنت یک "ستون فقرات"[3] را تشکیل داده است. شبکه‌های منطقه ای و محلّی پیرامون این ستون فقرات شکل گرفته و ترافیک دادهٔ آن‌ها به نحوی از این ستون فقرات خواهد گذشت. ستون فقرات در شبکهٔ اینترنت که با سرمایه گذاری عظیمی در آمریکا، اروپا و قسمت‌هایی از اقیانوسیه و آسیا ایجاد شده است حجم بسیار وسیعی از بسته‌های اطلاعاتی را در هر ثانیه حمل می‌کنند و اکثر شبکه‌های منطقه‌ای و محلی یا ارایه دهندگان سرویس‌های اینترنت[4] به نحوی با یکی از گره‌های این ستون فقرات در ارتباطند. در شکل ۱ سیمای کلّی و ساده از مفهوم ستون فقرات را می‌بینید.

قراردادی که حمل و تردد بسته‌های اطلاعاتی و همچنین مسیریابی صحیح آن‌ها را از مبدأ به مقصد، مدیریّت و سازماندهی می‌نماید پروتکلIP[5] نام دارد. درحقیقت، پروتکل IP که روی تمامی ماشین‌های شبکه اینترنت وجود دارد، بسته‌های اطلاعاتی را (بسته‌های IP) از مبداء تا مقصد هدایت می‌نماید، فارغ از آنکه آیا ماشین‌های مبدأ و مقصد روی یک شبکه هستند یا چندین شبکهٔ دیگر بین آن‌ها واقع شده است.

ساده ترین تعریف برای پروتکل IP روی شبکهٔ اینترنت به‌صورت زیر خلاصه می‌شود :

لایهٔ IP، یک واحد از داده‌ها را از لایهٔ بالاتر تحویل می‌گیرد؛ به این واحد اطلاعات معمولاً یک "دیتاگرام" گفته می‌شود[6]. امکان دارد طول این دیتاگرام بزرگ باشد، در چنین موردی لایهٔ IP آنرا به واحدهای کوچکتری که هر کدام "قطعه"[7] نام دارد شکسته و با تشکیل

---

[1] بخشهایی از فصول هفتم و هشتم و تمامی فصل نهم، از کتاب های مهندسی اینترنت (تالیف آقای مهندس احسان ملکیان) و شبکه های کامپیوتری (تالیف تنباوم؛ ترجمه آقایان دکتر پدرام، مهندس ملکیان و مهندس زارع پور)، هر دو از انتشارات نص، استخراج شده است. لذا بدینوسیله از زحمات دوست عزیزم جناب آقای مهندس ملکیان تشکر می نمایم.

[2] Autonomous

[3] Backbone

[4] Internet Service Provider (ISP)

[5] Internet protocol

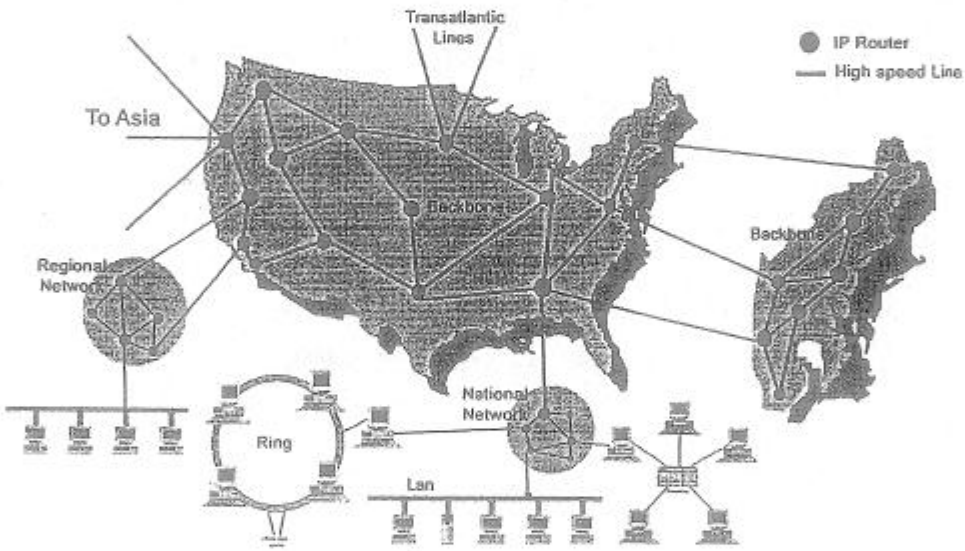
[6] اصطلاح دیتاگرام در ادبیّات شبکه‌های کامپیوتری به معانی متفاوت و در موارد متعدّد استفاده شده است. لذا به مورد استفادهٔ آن دقّت داشته باشید.

[7] Fragment

یک بستهٔ IP به ازای هر قطعه، اطلاعات لازم برای طی مسیر در شبکه را به آن‌ها اضافه میکند و سپس آن‌ها را روی شبکه به جریان می‌اندازد؛ هر مسیریاب با بررسی و پردازش بسته‌ها، آن‌ها را تا مقصد هدایت می‌کند. هر چند طول یک بسته IP می‌تواند حداکثر 64Kbyte باشد و لیکن در عمل عموماً طول بسته‌ها حدود ۱۵۰۰ بایت است. (این قضیه به دلیل آنست که اکثر شبکه‌های محلی دنیا اعمّ از Bus، حلقه، ستاره، ... طول فریمی نزدیک به یک تا چند کیلو بایت دارند.) پروتکل IP مجبور است هنگام قطعه قطعه کردن یک دیتاگرام، برای کلّ آن یک شمارهٔ مشخصه و برای هر قطعه یک شمارهٔ ترتیب در نظر بگیرد تا آن دیتاگرام بتواند در مقصد برای تحویل به لایهٔ بالاتر یعنی لایهٔ انتقال بازسازی شود .

(مجدداً تأکید می‌کنیم که در این مبحث، دیتاگرام یک واحد اطلاعات است که به صورت یکجا از لایهٔ IP به لایهٔ انتقال تحویل داده می‌شود یا بالعکس لایه انتقال آنرا جهت ارسال روی شبکه به لایهٔ IP تحویل داده و ممکن است شکسته شود)

در کنار پروتکل IP چندین پروتکل دیگر مثل ICMP، ARP، RARP، RIP و غیره تعریف شده که پروتکل IP را در عملکرد بهتر، مسیریابی صحیح، مدیریت خطاهای احتمالی یا کشف آدرس‌های ناشناخته کمک می‌کنند.



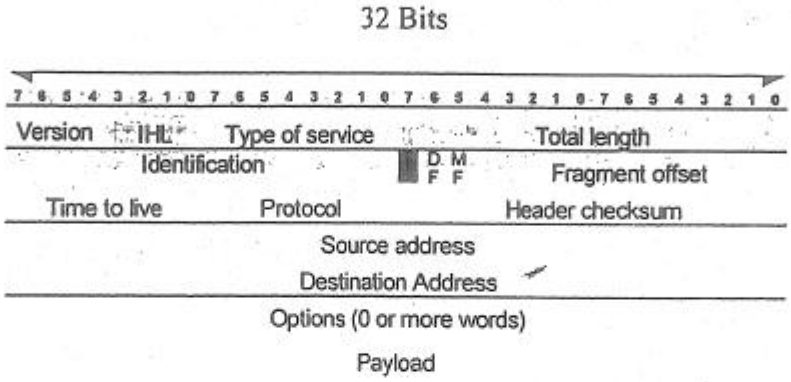
شکل ۱. سیمای کلّی و تجسّمی ستون فقرات در شبکهٔ اینترنت

تواناییهایی که پروتکل IP و پروتکلهای جانبی آن عرضه می‌کنند این امکان را فراهم آورده است که تمامی شبکه‌ها و ابزارهای شبکه‌ای (مثل ماشین‌های میزبان، مسیریاب‌ها، پلها، و...) فارغ از نوع ماشین و نوع سخت افزار و حتی با وجود تفاوت در سیستم عامل مورد استفادهٔ آن‌ها، بتوانند بسته‌های IP را با یکدیگر مبادله کنند. پروتکل IP ساختاری استاندارد دارد و به هیچ سخت افزار یا سیستم عامل خاصّ وابسته نیست.

به عنوان اولین گام در شناخت پروتکل IP لازم است قالب یک بستهٔ IP را کالبد شکافی کرده و در گامهای بعدی چگونگی آدرس دهی ماشین‌ها و انواع کلاس‌های آدرس در شبکهٔ اینترنت را معرفی نموده و نهایتاً به روش‌های مسیریابی و همچنین تعریف پروتکلهای وابسته به IP بپردازیم.

۱ـ۹ـ قالب یک بستهٔ IP

شکل ۲، قالب یک بسته IP را به تصویر کشیده است. یک بستهٔ IP از دو قسمت سرآیند و قسمت حمل داده تشکیل شده است. مجموعهٔ اطلاعاتی که در سرآیند بستهٔ IP درج می‌شود توسط مسیریاب‌ها مورد استفاده و پردازش قرار می‌گیرد.



شکل ۲. قالب یک بستهٔ IP

فیلد Version : اولین فیلد در سرآیند یک بستهٔ IP که چهار بیت است، نسخهٔ پروتکلِ IP که این بسته بر اساس آن سازماندهی و ارسال شده است را تعیین می‌کند. در حال حاضر تمامی شبکه‌ها و مسیریاب‌ها از نسخهٔ شماره ۴ پروتکل IP پشتیبانی می‌کنند. امروزه نسخهٔ شمارهٔ ۶ پروتکل IP به نامهای IPng یا IPv6 معرفی و در حال بررسی و نصب است. عددی که در حال حاضر در این فیلد قرار می‌گیرد ۴ یا $_{B}(0100)$ است.

فیلد IHL[1] : این فیلد هم چهاربیتی است و طول کل سرآیند بسته را بر مبنای کلمات ۳۲ بیتی مشخص می‌نماید. به عنوان مثال اگر در این فیلد عدد ۱۰ قرار گرفته باشد بدین معناست که کل سرآیند ۳۲۰ بیت معادل چهل بایت خواهد بود. اگر به ساختار یک بستهٔ IP دقّت شود به غیر از فیلد Options که اختیاری است، وجود تمامی فیلدهای سرآیند الزامی می‌باشد. طول قسمت اجباری سرآیند ۲۰ بایت است و به‌همین دلیل حداقل عددی که در فیلد IHL قرار می‌گیرد ۵ یا $_{2}(0101)$ خواهد بود و هر مقدار کمتر از ۵ به عنوان خطا تلقّی شده و منجر به حذف بسته خواهد شد. با توجه به طول ۴ بیتی این فیلد، بدیهی است که حداکثر مقدار آن ۱۵ یا $_{2}(1111)$ خواهد بود که در این صورت طول قسمت سرآیند ۶۰ بایت (۴×۱۵) و طول قسمت اختیاری ۴۰ بایت می‌باشد. قسمت اختیاری در سرآیند برای اضافه کردن اطلاعاتی مثل آدرس مسیرهای پیموده شده، "مهر زمان" و برخی دیگر از گزینه‌هاست که در ادامه توضیح داده خواهد شد.

فیلد Type Of Service : این فیلد هشت بیتی است و توسط آن ماشین میزبان (یعنی ماشین تولید کنندهٔ بستهٔ IP) از مجموعهٔ زیرشبکه (یعنی مجموعهٔ مسیریاب‌های بین راه) تقاضای سرویس ویژه‌ای برای ارسال یک دیتاگرام می‌نماید. به عنوان مثال ممکن است یک ماشین میزبان بخواهد دیتاگرامِ صدا یا تصویر برای ماشین مقصد ارسال نماید؛ در چنین شرایطی از زیرشبکه تقاضای ارسال سریع و به موقع اطلاعات را دارد نه قابلیت اطمینان صد در صد، چرا که اگر یک یا چند بیت از داده‌های ارسالی در مسیر دچار خرابی شود تاثیر چندانی در کیفیت کار نخواهد گذاشت ولی اگر بسته‌های حاوی اطلاعات صدا یا تصویر به سرعت و سر موقع تحویل نشود اشکال عمده بوجود خواهد آمد. در چنین مواقعی ماشین میزبان از زیرشبکه تقاضای سرویس سریع (و لاجرم غیر قابل اطمینان) می‌نماید. در

[1] IP Header Length

برخی از محیطهای دیگر مثل ارسال نامهٔ الکترونیکی یا مبادلهٔ فایل انتظارِ اطمینان[1] صد درصد از زیر شبکه وجود دارد و سرعت تاثیر چندانی بر کیفیّت کار ندارد.

از طریق این فیلد نوع سرویس درخواستی مشخص می‌شود، این فیلد خودش به چند بخش تقسیم شده است :

P2	P1	P0	D	T	R	
تقدم بسته			تأخیر	توان خروجی	قابلیّت اطمینان	بلا استفاده

الف) سه بیت سمت چپ : اولویت بستهٔ IP را تعیین می‌کند. اگر در این سه بیت صفر قرار گرفته باشد، بسته اطلاعاتی از نوع معمولی تلقی می‌شود، یعنی دارای پایین ترین مقدار اولویت است و اگر مقدار ۷ یعنی $_2(111)$ در این سه بیت قرار گرفته باشد، بالاترین اولویت برای بسته درنظر گرفته می‌شود. مسیریاب در بین بسته‌های IP که از کانالهای مختلف وارد شده‌اند، بسته‌هایی را زودتر پردازش و مسیریابی می‌کند که دارای حقّ تقدمِ و اولویت بالاتری باشند. بسته‌های با حقّ تقدم بالا برای عملیاتی نظیر ارسال بسته‌های اطلاعاتی به منظور تنظیم و پیکربندی پارامترهای زیرشبکه مورد استفاده قرار میگیرد. (مثلاً برای گزارش یک خرابی در زیر شبکه یا مبادلهٔ جداول مسیریابی)

ب) بیت‌های R , T , D : بیت D به معنای تأخیر[2]، بیت R به معنای قابلیت اطمینان و بیت T به معنای توان خروجی خط[3] است و ماشین میزبان با قرار دادن ۱ در این بیتها انتظارش را از زیرشبکه بیان می‌کند. مسیریاب‌ها با بررسی این سه بیت می‌توانند در مورد انتخاب مسیر مناسب تصمیم بگیرند. به عنوان مثال یک کانال ماهواره‌ای دارای توان خروجی بسیار بالا (از لحاظ نرخ ارسال) ولیکن تاخیر نامناسب است، در صورتی که یک خط اجاره‌ای می‌تواند دارای تاخیر کمتر و همچنین توان خروجی کمتر باشد. اگر در ارسال یک بستهٔ IP ، تاخیر پذیرفتنی نباشد با یک کردن بیتِ D مسیریاب را وادار می‌کند که حتی الامکان از خطوط پرتاخیر مثل خط ماهواره‌ای استفاده نکند؛ با یک کردن بیت R مسیریاب موظف خواهد بود تا از بین خطوط خروجی، امن ترین و کم خطاترین آن‌ها را انتخاب کند. (البته در صورت امکان)

اکثر مسیریاب‌های تجاری فیلد Type of Service را نادیده می‌گیرند و اهمیتی به محتوای آن نمی‌دهند.

فیلد Total Length : در این فیلدِ ۱۶ بیتی عددی قرار می‌گیرد که طول کل بستهٔ IP را که شامل مجموع اندازهٔ سرآیند و ناحیه داده است، تعیین می‌کند. مبنای طول برحسب بایت است و بنابراین حداکثر طول کل بستهٔ IP می‌تواند ۶۵۵۳۵ بایت باشد.

فیلد Identification : همانگونه که قبلاً اشاره شد برخی از مواقع مسیریاب‌ها یا ماشین‌های میزبان مجبورند یک دیتاگرام را به قطعات کوچکتر بشکنند و ماشین مقصد مجبور است آن‌ها را بازسازی کند، بنابراین وقتی یک دیتاگرامِ واحد شکسته می‌شود باید مشخصه‌ای داشته باشد تا در هنگام بازسازیِ آن در مقصد بتوان قطعه‌های آن دیتاگرام را از بقیه جدا کرد. در این فیلدِ ۱۶ بیتی عددی قرار می‌گیرد که شمارهٔ یک دیتاگرام واحد را مشخص می‌کند. کلیه بسته‌های IP که با این شماره وارد می‌شوند قطعه‌های مربوط به یک دیتاگرام بوده و باید پس از گردآوری قطعه‌ها، آن را مجدداً بازسازی کرد. به عنوان مثال، اگر در این فیلد عدد ۱۶۵۲ قرار بگیرد تمامی بسته‌های IP که مشخصهٔ ۱۶۵۲ دارند قطعه‌های مربوط به یک دیتاگرام هستند و پس از دریافت کل قطعه‌ها باید بازسازی شوند. البته برای حفظ ترتیب، هر قطعه گذشته از یک شمارهٔ مشخصه بایستی دارای شمارهٔ ترتیب نیز باشد تا بتوان آن‌ها را طبق این شماره مرتب و بازسازی کرد.

---

۱ Reliability
۲ Delay
۳ Throughput

فیلد **Fragment offset** : این فیلد در سه بخش سازماندهی شده است :

الف) بیت DF[1]: با یک شدن این بیت در یک بستهٔ IP هیچ مسیریابی حق ندارد آن را قطعه قطعه کند، چرا که مقصد قادر به بازسازی دیتاگرام‌های تکه تکه شده نیست. به عنوان مثال وقتی که یک کامپیوتر بدون دیسک از طریق ROM بوت می‌شود، اطلاعات هسته اصلی سیستم عامل باید در قالب یک دیتاگرام واحد برای آن کامپیوتر ارسال شود چرا که آن کامپیوتر در حال حاضر نرم افزار لازم برای بازسازی بسته‌های قطعه قطعه شده را ندارد. اگر این بیت به ۱ تنظیم شده باشد و مسیریابی نتواند آنرا به دلیل بزرگی اندازهٔ آن، انتقال بدهد لاجرم آنرا حذف خواهد کرد.

ب) بیت MF[2]: این بیت مشخص می‌کند که آیا بستهٔ IP آخرین قطعه از یک دیتاگرام محسوب می‌شود یا باز هم قطعه‌های بعدی وجود دارد. در آخرین قطعه از یک دیتاگرام بیت MF صفر خواهد بود و در بقیه الزاماً ۱ است.

ج) Fragment offset : این قسمت که سیزده بیتی است در حقیقت شماره ترتیب هر قطعه در یک دیتاگرام شکسته شده محسوب می‌شود. با توجه به سیزده بیتی بودن این فیلد، یک دیتاگرام حداکثر می‌تواند به ۸۱۹۲ تکه تقسیم شود.

نکته بسیار مهم در مورد این فیلد آن است که اندازهٔ هر قطعه باید ضریبی از ۸ باشد. یعنی به استثنای قطعهٔ آخر، اندازه بقیهٔ قطعه‌ها بایستی بگونه‌ای انتخاب شود که ضریبی از ۸ بایت باشد؛ مثلاً اگر در فیلد آفست مقدار ۷ قرار بگیرد نشان می‌دهد که محل قرار گرفتن قطعهٔ جاری در دیتاگرام بازسازی شده در موقعیت بایت پنجاه وششم (۵۶=۸×۷) خواهد بود. به عنوان مثالی دیگر، فرض کنید مسیریابی مجبور است یک دیتاگرام به طول ۵۰۰۰ بایت را قطعه قطعه کند به گونه‌ای که اندازهٔ هر قطعه زیر ۱۵۰۰ بایت باشد. در چنین موردی نمیتواند اندازهٔ هر قطعه را ۱۲۵۰ بایت در نظر بگیرد چرا که ضریبی از ۸ نیست ولی اندازهٔ ۱۲۸۰ مناسب است. در این حالت مسیریاب، دیتاگرام را به سه بستهٔ ۱۲۸۰ بایتی و یک بستهٔ ۱۱۶۰ بایتی می‌شکند. در این مثال فرض کنید مسیریاب شمارهٔ ۲۳۲۲ را به عنوان مشخصهٔ دیتاگرام انتخاب کرده است؛ بنابراین برای هر یک از چهار قطعهٔ دیتاگرام، فیلد آفست و مشخصه به صورت زیر خواهد بود:

شمارهٔ قطعه	Identification	Fragment Offset	بیت MF	آدرس محل قرار گرفتن قطعه در دیتاگرام	طول هر قطعه
قطعهٔ شماره ۱	2322	0	1	8*0=0	۱۲۸۰
قطعهٔ شماره ۲	2322	160	1	8*160=1280	۱۲۸۰
قطعهٔ شماره ۳	2322	320	1	8*320=2560	۱۲۸۰
آخرین قطعه	2322	480	0	8*480=3840	۱۱۶۰

(بیت اول، یعنی بیت سمت چپ از این فیلد که در شکل ۲ به رنگ سیاه علامت گذاری شده، مورد استفاده ندارد.)

ممکن است یک دیتاگرامِ واحد از یک ماشین میزبان روی زیر شبکه تزریق شود و در طول مسیر به مسیریابی برسد که به دلیلی مجبور به شکستن آن به قطعات کوچکتر شود. در چنین حالتی باز هم وظیفهٔ بازسازی قطعات به عهده ماشین مقصد می‌باشد. به عبارت ساده تر عمل شکستن یک دیتاگرام در هر جای زیر شبکه ممکن است اتفاق بیفتد ولیکن عمل باز سازی فقط در ماشین مقصد انجام می‌شود.

---

[1] Don't Fragment

[2] More Fragment

فیلد **Time To Live** : این فیلد هشت بیتی در نقش یک شمارنده، طول عمر بسته را مشخص می‌کند. طول عمر یک بسته بطور ضمنی به زمانی اشاره می‌کند که یک بسته IP می‌تواند بر روی شبکه سرگردان باشد. حداکثر طول عمر یک بسته، ۲۵۵ خواهد بود که به ازای عبور از هر مسیریاب[۱] از مقدار این فیلد یک واحد کم می‌شود. هر گاه یک بستهٔ IP به دلیل بافر شدن در حافظهٔ یک مسیریاب زمانی را معطّل بماند، به ازای هر ثانیه یک واحد از این فیلد کم خواهد شد. به محض آنکه مقدار این فیلد به صفر برسد بستهٔ IP در هر نقطه از مسیر باشد حذف شده و از ادامهٔ سیرِ آن به سمت مقصد جلوگیری خواهد شد. (البته معمولاً یک پیام هشدار به ماشینی که آن بسته را تولید کرده باز پس فرستاده خواهد شد.)

اگرچه بزرگترین عددی که در فیلد طول عمر بسته قرار می‌گیرد ۲۵۵ است ولی در عمل مقداری که سیستمهای عامل در این فیلد قرار می‌دهند چیزی حدود ۳۰ است. (البته می‌توان مقدار پیش فرض آن را عوض کرد.)

این فیلد برای پاکسازی زیر شبکه از بسته‌های IP که به هر دلیل در یک مسیرِ بسته می‌چرخند بسیار حیاتی است وگرنه پس از مدتی کلّ زیر شبکه از بسته‌های آشغال پر خواهد شد. بسته‌های سرگردان گاهاً به این دلیل بوجود می‌آیند که جداول مسیریابی در بعضی از مسیریاب‌ها آلوده به اطلاعات نادرست[۲] شده‌اند. سرگردانی یک بسته در زیرشبکه مسئلهٔ غیر ممکنی نیست و گاهی اتفاق می‌افتد.

فیلد **Protocol** : دیتاگرامی که در فیلد داده از یک بستهٔ IP حمل می‌شود با ساختمان دادهٔ خاصّ از لایهٔ بالاتر تحویلِ پروتکل IP شده تا روی شبکه ارسال شود. به عنوان مثال ممکن است این داده‌ها را پروتکل TCP در لایه بالاتر ارسال کرده باشد و یا ممکن است این کار توسط پروتکل UDP انجام شده باشد. بنابراین مقدار این فیلد شمارهٔ پروتکلی است که در لایه بالاتر تقاضای ارسال یک دیتاگرام کرده است؛ بسته‌ها پس از دریافت در مقصد باید به پروتکل تعیین شده تحویل داده شود. فیلد پروتکل ۸ بیتی است و پروتکلهای لایهٔ بالاتر دارای یک شمارهٔ هشت بیتیِ منحصر بفرد و استاندارد هستند که درصورت نیاز به دانستن شمارهٔ آن‌ها می‌توانید به انتهای این فصل مراجعه کنید.

فیلد **Header Checksum** : این فیلد که شانزده بیتی است به منظور کشف خطاهای احتمالی در سرآیند هر بستهٔ IP استفاده می‌شود. برای محاسبهٔ کد کشف خطا، کلّ سرآیند به‌صورت دو بایت، دوبایت با یکدیگر جمع می‌شود. نهایتاً حاصل جمع به روش "مکمل یک"[۳] منفی می‌شود و این عدد منفی در این فیلد از سرآیند قرار می‌گیرد.

در هر مسیریاب قبل از پردازش و مسیریابی ابتدا صحتِ اطلاعات درون سرآیند بررسی می‌شود. روش بررسی بدینصورت است که اگر تمامی سرآیند به‌صورت دو بایت، دوبایت در مبنای مکمل یک با یکدیگر جمع شود باید حاصل جمع، صفر بدست آید؛ در غیر این صورت بستهٔ IP فاقد اعتبار بوده و حذف خواهد شد.

دقت کنید که فیلد Checksum در هر مسیریاب باید از نو محاسبه و مقداردهی شود زیرا وقتی یک بستهٔ IP وارد یک مسیریاب می‌شود حداقل فیلد TTL از آن بسته عوض خواهد شد.

فیلد Checksum برای کشف خطاهای احتمالی درون داده‌های فیلد Payload استفاده نمی‌شود چرا که اینگونه خطاها در لایه پایینتر یعنی لایه فیزیکی معمولاً توسط کدهای CRC نظارت می‌شود؛ در ضمن لایه‌های بالاتر نیز مسئلهٔ خطا را بررسی می‌کنند.

در حقیقت این فیلد برای کشف خطاهایی است که یک مسیریاب در تنظیم سرآیند یک بستهٔ IP مرتکب شده است.

فیلد **Source Address** : هر ماشین میزبان در شبکهٔ اینترنت یک آدرس جهانی و یکتای ۳۲ بیتی دارد. بنابراین هر ماشین میزبان در هنگام تولید یک بستهٔ IP باید آدرس خودش را در این فیلد قرار بدهد.

---

[۱] در ادبیات شبکه به عبور بسته از یک مسیریاب یک جهش یا Hop گفته می‌شود.

[۲] Corrupt

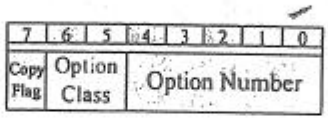
[۳] One's Compelement

بحث آدرس‌ها در اینترنت یکی از مسائل بسیار مهمی است که در فصلی مجزا به آن خواهیم پرداخت. (به این آدرس از این بعد، "آدرسِ IP" می‌گوئیم.)

فیلد Destination Address : در این فیلد آدرس ۳۲ بیتیِ مربوط به ماشین مقصد که باید بسته IP تحویل آن بشود، قرار می‌گیرد.

فیلد اختیاری Options : در این فیلدِ اختیاری می‌توان تا حداکثر ۴۰ بایت قرار داد و محتوی اطلاعاتی است که می‌تواند به مسیریاب‌ها در مورد یافتن مسیر مناسب کمک کند. البته به گونه‌ای که اشاره شد حداکثر فضای این فیلد ۴۰ بایت است که بسیار کم به نظر می‌رسد.

از آنجایی که در فضای ۴۰ بایتی این فیلد چندین گزینه می‌تواند قرار بگیرد و هر گزینه نیز اندازهٔ متفاوتی دارد (بر حسب بایت) لذا هر گزینه با یک کد یک بایتی مشخص می‌شود:



بیت Copy Flag : ۱ بودن این بیت مشخص میکند که اگر مسیریابی مجبور به شکستن بستهٔ فعلی شود، این گزینه در یکایک قطعات بسته تکرار شود. صفر بودن این بیت به معنای آنست که در هنگام شکسته شدن بسته این گزینه فقط در اولین قطعه وجود داشته باشد.

دو بیت Option Class : این دو بیت نوع عملکرد گزینه را تعیین میکند:

00 : عملکرد گزینه

10 : عملکرد گزینه برای اشکال‌زدایی و مدیریت شبکه می‌باشد.

01 و 11 : تعریف نشده است.

پنج بیت Option Number : این پنج بیت نوع و معنای گزینه را مشخص می‌کند. تاکنون پنج گزینهٔ متفاوت در این فیلد تعریف شده است:

Option Class	Option Number	Name Of Options	شرح
00	0	End of Options List	۱-تعیین پایان لیست گزینه‌ها
00	1	Null Option	۲-گزینهٔ پوچ (فقط برای پر کردن فضا)
00	2	Security	۳-گزینهٔ امنیت
00	3	Loose Source Routing	۴-گزینهٔ تعیین مسیر به‌صورت ناقص
00	7	Record Route	۵-گزینهٔ ثبت مسیر
00	9	Strict Source Routing	۶-گزینهٔ تعیین مسیر به‌صورت دقیق و صریح
10	4	Timestamp	۷-گزینهٔ ثبت مسیر و زمان

گزینهٔ اوّل : با این گزینه پایان مجموعهٔ گزینه‌ها مشخص می‌شود.

گزینهٔ دوم : این گزینه هیچ ارزش اجرایی ندارد و فقط برای آنست که فضای فیلد Options به گونه‌ای پر شود تا ضریبی از ۴ باقی بماند.

گزینهٔ سوم : مشخص می‌کند که بسته IP تا چه حد محرمانه است و در این شرایط مسیریاب خواهد دانست که این بسته را از طریق چه مسیرهایی به سمت مقصد هدایت نماید تا امنیت بسته تامین شود و از چه مسیرهایی باید احتراز نماید. اکثر مسیریاب‌های تجاری از این گزینه چشم‌پوشی می‌نمایند.

گزینه چهارم: با این گزینه می‌توان مسیری را برای عبور بسته (به‌صورت ناقص) مشخص کرد و بسته باید قطعاً از مسیریاب‌های مشخص شده عبور نماید ولی از آن جائی که این گزینه مسیر کامل را مشخص نکرده است بقیه مسیر توسط مسیریاب تعیین می‌شود. برای مثال فرض کنید بخواهید بسته ای را که باید از لندن به سیدنی طی مسیر کند، بجای عبور از شرق به غرب از مسیرهای نیویورک، لس آنجلس و هانولولو به سمت سیدنی ارسال شود. کافی است فقط آدرس مسیرهای ابتدائی را با این گزینه مشخص کرده و بقیه مسیر بعهده مسیریاب‌ها گذاشته شود.

گزینه پنجم: با درج این گزینه در بستهٔ IP از تمامی مسیریاب‌ها خواسته می‌شود که قبل از ارسالِ بسته به مسیریاب بعدی آدرس خودشان را در فیلد Option ثبت نمایند. با بررسی مسیرهایی که یک بسته از مبداء به سمت مقصد پیموده است می‌توان به اشکالات احتمالی در الگوریتمهای مسیریابی هر مسیریاب پی برد. دقّت کنید که پروتکل IP زمانی وضع شده است که فضای ۴۰ بایتی فیلد Options برای تمامی شبکه‌ها کافی بود؛ چرا که این پروتکل برای اولین بار در ARPANET پیاده شد که حداکثر تعداد مسیریاب‌ها در طولانی‌ترین مسیر، ۹ عدد بود. بنابراین فضای چهل بایتی برای امروزه که هزاران مسیریاب در جهان نصب و راه‌اندازی شده است بسیار ناکافی به نظر می‌رسد.

گزینه ششم : با این گزینه می‌توان مسیر از پیش تعیین شده ای را برای بستهٔ IP تعیین کرد و مسیریاب‌ها نیز موظفند از مسیر تعیین شده تبعیت نمایند. با توجه به آنکه در زیرشبکه، مسیریابی به روش‌های پویا انجام می‌شود، استفاده از این گزینه چندان منطقی و مناسب به نظر نمی‌رسد بلکه فقط به عنوان یک ابزار برای مدیران سیستم جهت آزمایش و بررسی شرایط یک مسیر و تخمین جداول مسیریابی (به‌صورت دستی) مفید خواهد بود.

گزینه هفتم: این گزینه از تمامی مسیریاب‌ها می‌خواهد که زمان دریافت بسته را در فیلد Options درج کنند. این گزینه برای اشکال زدائی از الگوریتمهای مسیریابی مناسب است.

فیلد Payload : در این فیلد داده‌های دریافتی از لایهٔ بالاتر قرار می‌گیرد.

پس از شناسائی ساختار یک بسته IP، بایستی به مبحث آدرس‌ها در پروتکل IP بپردازیم. مفاهیم آدرس‌های IP شما را در درک واقعیت چگونگی مسیریابی بهتر کمک می‌کند. سپس به پروتکلهائی خواهیم پرداخت که به پروتکلIP در لایه شبکه کمک می‌کنند تا یک مسیریابی صحیح امکان پذیر باشد.

۲ ـ ۹ ـ مبحث آدرس‌ها در اینترنت و اینترانت

همانگونه که در مباحث قبلی بدان اشاره کردیم، پروتکل اینترنت در ارتباطات بین شبکه ای[1] از آدرس‌های منحصر به فرد و یکتای ۳۲ بیتی بهره می‌برد. (هر چند که در نسل بعدیِ پروتکل اینترنت که تا سال ۲۰۰۵ همه گیر خواهد شد این آدرس‌ها ۱۲۸ بیتی می‌شوند.) هر ابزار شبکه اعم از ماشین‌های میزبان، مسیریاب‌ها و چاپگرهای شبکه در اینترنت با یک آدرس IP شناسائی می‌شوند.

در ادامهٔ این فصل باید موارد زیر را بررسی و مطالعه کنیم:

قالب هر آدرس IP چگونه سازماندهی می‌شود؟

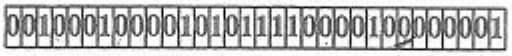
---

[1] Internetworking

کلاس‌های مختلف آدرس‌های IP به چه منظور و چگونه سازماندهی می‌شوند؟
چگونه آدرس‌های IP به آدرس‌های سخت افزاری لایه فیزیکی تبدیل خواهد شد و قراردادهای نمایش آدرس‌های IP چگونه هستند؟
یک مسیریاب چگونه می‌تواند از یک آدرس چهاربایتی، محل دقیق یک ماشین را بین دهها میلیون ماشین متصل به شبکه پیدا نماید؟
آدرس‌های IP درون یک عدد دودویی ۳۲ بیتی درج می‌شوند ولیکن برای سادگی نمایش به چهار قسمت هشت بیتی[۱] تقسیم و به‌صورت چهار عدد دهدهی که با نقطه از هم جدا شده‌اند، نوشته می‌شود؛ یعنی معادل دهدهی هر یک از بایتهای آدرس به‌صورت مجزا نوشته شده و هر عدد با یک علامتِ از دیگری تفکیک می‌شود. به عنوان مثال آدرس زیر یک آدرس IP معتبر می‌باشد که در قالب چهار قسمت دهدهی نوشته شده است:

34.21.225.1

این آدرس به‌صورت زیر در فیلد آدرس از یک بستهٔ IP تنظیم می‌شود:



پرارزش‌ترین بایت یعنی اولین بایتِ سمت چپ از آدرس IP، کلاس آدرس را مشخص می‌کند و از این رو دارای اهمیت ویژه است. ولی قبل از آنکه کلاس‌های آدرس را تشریح نماییم بازهم روی این نکته تکیه می‌کنیم که وقتی یک ماشین میزبان به شبکه اینترنت متصل می‌شود بایستی آدرس IP آن منحصر به فرد و یکتا[۲] باشد. در حقیقت هر ماشین روی شبکه با یک آدرس یکتا هویت پیدا میکند. برای اطمینان از یکتا بودن آدرس‌های IP برای ارتباطات عمومی، مرکز InterNIC[3] کنترل و نظارت بر روی آدرس‌های IP را بر عهده گرفته است.
IANA[۴] قدرت اجرائی برای اختصاص آدرس‌های IP منحصر به فرد را فراهم کرده است. هر چند شبکه‌های خصوصی که به اینترنت وصل نیستند می‌توانند از آدرس‌های IP دلخواه استفاده کنند ولی اگر این شبکه‌ها زمانی بخواهند به اینترنت وصل شوند دوگانگی آدرس‌های غیر یکتا و نهایتاً تناقض و اشکال در مسیریابی[۵] رخ خواهد داد؛ به همین دلیل پیشنهاد شده است که حتی شبکه‌های خصوصی نیز برای اختصاص آدرس به ماشین‌های میزبان از مرکز InterNIC مجوز بگیرند و از آدرس‌های معتبر و اختصاصی استفاده کنند.

۱ ـ ۲ ـ ۹ ـ کلاس‌های آدرسِ IP

از آنجا که TCP/IP برای شبکه‌های با مقیاس بزرگ طراحی شده است لذا نمی‌توان انتظار داشت که فضای ۳۲ بیتی آدرس که حدود چهار میلیارد و سیصد میلیون (4,294,967,295) آدرس را در اختیار می‌گذارد، بدون هیچ نظم و سیاق خاص به ماشین‌های شبکه اختصاص داده شود. این کار همانند آن خواهد بود که تمامی آپارتمانها و منازل در کل جهان با شماره‌های ده رقمی مشخص شود بدون آنکه هیچ ضابطه ای در شماره گذاری آن‌ها رعایت شده باشد. آنگاه منزلی با شماره ۱۰۶۵۴۳۲۳۹۰ چگونه پیدا می‌شود؟
آدرس‌های پستی ساختاری سلسله مراتبی به صورت زیر دارند، به گونه‌ای که هر منزل در هر کجای دنیا قابل آدرس‌دهی است و به راحتی پیدا می‌شود:

---

۱ Octet
۲ Unique
۳ Internet Network Information Center
۴ Internet Assigned Number Authority
۵ Conflict

شماره/کوچه/خیابان/ناحیه/شهر/کشور

فلسفهٔ کلاس‌های آدرس IP به همین منظور است :

آدرس ماشین/آدرس زیرشبکه/آدرس شبکه

با توجه به آنکه اینترنت مجموعه‌ای از شبکه‌های متصل شده به هم می‌باشد، برای آدرس دادن به ماشین‌های میزبان بهتر است ۳۲ بیت آدرس IP به قسمت‌های زیر تقسیم شود:

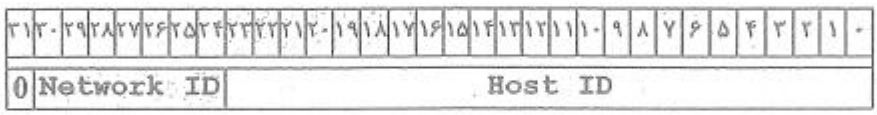
الف) آدرس شبکه

ب) آدرس زیر شبکه (درصورت لزوم)

ج) آدرس ماشین میزبان

آدرس‌های IP درپنج کلاس E,D,C,B,A معرفی شده‌اند که شما بایستی آن‌ها را بدقت بشناسید و تحلیل کنید. در زیر قالب کلاس‌های پنج گانهٔ آدرس IP مشخص شده است:

آدرس‌های کلاس A : قالب ۳۲ بیتیِ آدرس در کلاس A به صورت زیر است:



در کلاس A، پرارزش‌ترین بیت از آدرس، مقدار صفر دارد و این بیت، کلاس A را از دیگر کلاسها متمایز می‌کند؛ ۷ بیت بعدی "مشخصهٔ آدرس شبکه" و سه بایت باقیمانده، آدرس ماشین میزبان را تعیین می‌کند. بنابراین در کلاس A بایت پرارزش در محدوده صفر تا ۱۲۷ تغییر می‌کند. چون با ۲۴ بیت می‌توان حدود هفده میلیون ماشین میزبان را آدرس دهی کرد، می‌توان به این نتیجه رسید که آدرس‌های کلاس A بایستی برای آژانس‌های ستون فقرات اینترنت یا شبکه‌ها بسیار عظیم مثل NSFNet یا ARPANet اختصاص داده شده باشد. مشخصهٔ شبکه در این کلاس بهیچوجه نمی‌تواند اعداد صفر یا ۱۲۷ انتخاب شود چرا که این دو عدد در شبکه معنای دیگری خواهند داشت و بعداً به آن اشاره خواهیم کرد. بنابراین تعداد شبکه‌هایی که در جهان می‌توانند از کلاس A استفاده کنند، ۱۲۶ تا خواهد شد که بسیار کم است. امروزه اختصاص آدرس‌های کلاس A غیر ممکن است چرا که همهٔ آن‌ها توسط پیشگامان شبکه سالها قبل تملیک شده‌اند.

وقتی به یک آدرس IP که در قالب دهدهی نوشته شده است نگاه می‌کنید، براحتی می‌توانید کلاس آنرا تشخیص بدهید. اگر عدد سمت چپ آدرس، بین صفر تا ۱۲۷ باشد، آن آدرس از کلاس A خواهد بود:

74. 103 .14 .138

Net ID Host ID

آدرس IP معادل با (127.0.0.0) در پروتکل IP، یک شبکه را تعیین نمی‌کند بلکه به‌صورت قراردادی به عنوان آدرس "حلقه بازگشت"[1] جهت اهداف اشکال زدایی استفاده شده است چرا که این آدرس عملاً معادل آدرس خود ماشین محلی است.

آدرس‌های کلاس B : قالب ۳۲ بیتیِ آدرس در کلاس B به صورت زیر است:

[1] Loopback

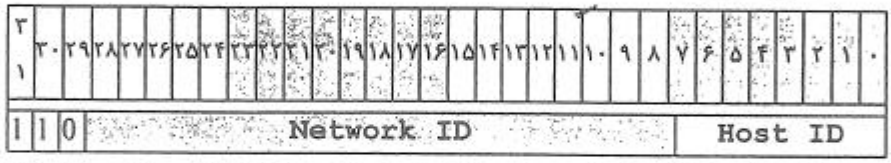
هر گاه دو بیت پرارزش از آدرس IP مقدار 10 داشته باشند، آن آدرس از کلاس B خواهد بود. ۱۴ بیت باقیمانده از ۲ بایت سمت چپ، آدرس شبکه را تعیین می‌کند و دو بایت اول از سمت راست (۱۶ بیت) آدرس ماشین میزبان خواهد بود.

در آدرس‌های کلاس B، تعداد ۱۶۳۸۲ (2^{14}-2) شبکهٔ گوناگون قابل تعریف خواهد بود و هر شبکه می‌تواند ۶۵۵۳۴ (2^{16}-2) ماشین میزبان تعریف نماید. اختصاص آدرس‌های کلاس B برای شبکه‌های بسیار عظیم مناسب است. هر چند تعداد این شبکه در جهان می‌تواند تا حدود شانزده هزار عدد باشد ولیکن امروزه عملاً نمی‌توان آدرس کلاس B گرفت چرا که تقریباً همهٔ آن‌ها آن تخصیص داده شده‌اند.

اگر آدرس IP به صورت دهدهی نوشته شود و عدد سمت چپ آن بین ۱۲۸ تا ۱۹۱ باشد، آن آدرس، کلاس B خواهد بود:

(134) 64. 143. 24
Net ID Host ID

آدرس کلاس C : قالب ۳۲ بیتیِ آدرس در کلاس C به صورت زیر است:



کلاس C، مناسب ترین و پرکاربردترین کلاس از آدرس‌های IP است. همانگونه که از شکل مشخص است در این کلاس، سه بیت پرارزش دارای مقدار 110 است و ۲۱ بیت بعدی از سه بایت سمت چپ برای تعیین آدرس شبکهٔ مورد نظر بکار رفته است. بنابراین در این کلاس می‌توان حدود دو میلیون شبکه را در جهان آدرس دهی کرد و هر شبکه می‌تواند تا ۲۵۴ عدد ماشین میزبان تعریف نماید.

برای تشخیص آدرس‌های کلاس C به عدد سمت چپ از آدرس IP که به صورت دهدهی نوشته شده است نگاه کنید. اگر عدد بین ۱۹۲ تا ۲۲۳ بود آن آدرس از کلاس C خواهد بود:

(199) 164. 78 .132
Net ID Host ID

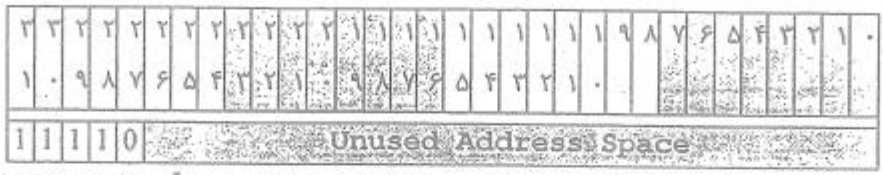
آدرس کلاس D : قالب ۳۲ بیتیِ آدرس در کلاس D به صورت زیر است:

در این کلاس، چهار بیت پرارزش دارای مقدار 1110 است و ۲۸ بیت باقیمانده از کلّ آدرس برای تعیین آدرس‌های "چند مقصده"[1] (آدرس‌های گروهی) است .

از این آدرس‌ها برای ارسال یک دیتاگرام به طور همزمان برای چندین ماشین میزبان کاربرد دارد و به‌منظور عملیات رسانه‌ای و چند پخشی بکار می‌رود. توضیح بیشتر در مورد این کلاس در بخشی مجزا ارایه خواهد شد .

[1] Multicast

آدرس کلاس E : قالب ۳۲ بیتی آدرس در کلاس E به صورت زیر است:



فعلاً این دسته از آدرس‌ها که پنج بیت پرارزش آن‌ها در سمت چپ 11110 است کاربرد خاصّی ندارند و برای استفاده در آینده بدون استفاده رها شده‌اند. البته گاهی به‌صورت آزمایشی از این آدرس‌ها استفاده شد ولی تاکنون جهانی نشده‌اند.

۲ ـ ۲ ـ ۹ ـ آدرس‌های خاص

در بین تمامی کلاس‌های آدرسIP پنج گروه از آدرس‌ها، معنای ویژه ای دارند و با آن‌ها نمی‌توان یک شبکهٔ خاص را تعریف و آدرس دهی کرد. این پنج گروه آدرس عبارتند از:

الف) آدرس 0.0.0.0 : هر ماشین میزبان که از آدرس IP خودش مطلع نیست، این آدرس را به عنوان آدرس خودش فرض می‌کند. البته از این آدرس فقط به عنوان آدرس مبدا و برای ارسال یک بسته می‌توان استفاده کرد و گیرندهٔ بسته نمی‌تواند پاسخی به مبدا بسته برگرداند.[1]

ب) آدرس 0.HostID : این آدرس زمانی به کار می‌رود که ماشین میزبان، آدرس مشخصهٔ شبکه‌ای که بدان متعلق است را نداند. در این حالت در قسمت NetID مقدار صفر و در قسمت HostID شمارهٔ مشخصهٔ ماشین خود را قرار می‌دهد.

ج) آدرس 255.255.255.255 : برای ارسال پیام‌های فراگیر برای تمامی ماشین‌های میزبان بر روی شبکهٔ محلی که ماشین ارسال کننده به آن متعلق است.

د) آدرس NetID.255 : برای ارسال پیام‌های فراگیر برای تمامی ماشین‌های یک شبکهٔ راه دور که ماشین میزبان فعلی متعلق به آن نیست. آدرس شبکهٔ مورد نظر در قسمت NetID تعیین شده و تمامی بیت‌های قسمت مشخصهٔ ماشین میزبان ۱ قرار داده می‌شود. البته بسیاری از مسیریاب‌ها برای مصون ماندن شبکه از مزاحمت‌های بیرونی، چنین بسته‌هایی را حذف می‌کنند.

ه) آدرس 127.xx.yy.zz : این آدرس به عنوان "آدرس بازگشت" شناخته می‌شود و آدرس بسیار مفیدی برای اشکال‌زدایی از نرم افزار می‌باشد. به عنوان مثال اگر بسته‌ای به آدرس 127.0.0.1 ارسال شود، بسته برای ماشین تولیدکنندهٔ آن بر خواهد گشت[2]؛ در این حالت اگر نرم افزارهای TCP/IP درست و بدون اشکال نصب شده باشد، فرستندهٔ بسته باید آنرا مجدداً دریافت کند. همچنین از این آدرس می‌توان برای آزمایش برنامه‌های تحت شبکه، قبل از نصب آن‌ها بر روی ماشین‌های میزبان استفاده کرد.

۳ ـ ۲ ـ ۹ ـ آدرس‌های زیرشبکه

در ادامهٔ بحث بایستی مسئله زیر شبکه را در خصوص آدرس دهی‌ها مطرح نمائیم. مبحث را با یک مثال آغاز می‌نمائیم:

فرض کنید دانشگاه شما یک کلاس C با قابلیت تعریف ۲۵۴ ماشین میزبان ثبت می‌نماید (مثلاً 211.11.121.0) ؛ یعنی شبکهٔ دانشگاه توانایی آدرس دهی ۲۵۵ ایستگاه را در شبکه دارد. در نظر بگیرید که دانشگاه دارای یک شبکهٔ محلی واحد و یکپارچه برای کل دانشگاه نیست بلکه دارای هشت شبکهٔ محلی مجزا است که برای هر دانشکده تهیه دیده شده است؛ (همانند ساختاری که در

---

[1] استفاده از این آدرس مانند آنست که در آدرس فرستندهٔ یک بستهٔ پستی نوشته شود : "خودم". بسته می‌تواند به مقصد برسد ولی پاسخی نخواهد داشت.

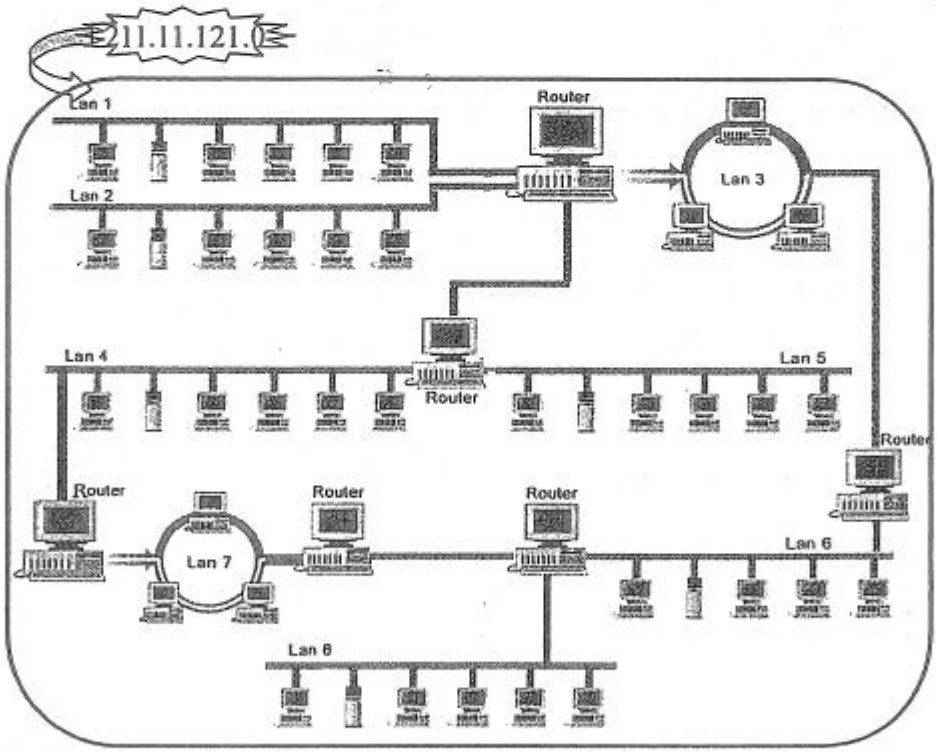
[2] این آدرس همانند آنست که فرستندهٔ یک بستهٔ پستی آدرس دقیق خودش را به عنوان گیرندهٔ آن درج نماید. بنابراین با آدرس 0.0.0.0 تفاوت ذاتی دارد.

شکل۳ ترسیم شده است). هر کدام از این شبکه‌ها که می‌تواند توپولوژی متفاوتی داشته باشد، از طریق مسیریاب به هم متصل شده‌اند و طبعاً برای ارتباط بین شبکه‌های هر دانشکده باید مسیریابی صورت گیرد. از دیدگاه بیرونی کلّ مجموعهٔ شبکه‌های محلی دانشگاه با یک آدرس مشخصه یعنی 211.11.121.0 شناخته می‌شود و مسیریاب‌های بیرونی هیچ شناختی از ساختار شبکه بندی داخلی دانشگاه ندارند. (هر یک از شبکه‌های محلی داخل دانشگاه یک زیرشبکه نامیده می‌شود.) بنابراین باید روشی وجود داشته باشد تا از طریق آدرس‌های کلاس C (یا هر کلاس دیگر) بتوان زیر شبکه‌ها را نیز مشخص کرد تا مسیریاب‌های داخلی نیز قادر باشند زیر شبکه‌های مختلف را شناسایی و تفکیک کنند.

این مسئله برای آدرس‌های کلاس B و A بسیار ضروری و اجتناب ناپذیر می‌نماید، چرا که نمی‌توان انتظار داشت که یک موسسه که آدرس کلاس B با قابلیت تعریف حدود ۶۶ هزار ماشین میزبان ثبت کرده است فقط یک شبکهٔ یکپارچه داشته باشد بلکه چنین مؤسسه‌ای ممکن است دارای صدها زیر شبکهٔ کوچک و بزرگ باشد.

برای آنکه بتوان زیرشبکه‌ها[1] را تفکیک کرد جدای از قسمت آدرس شبکه که کل شبکهٔ دانشگاه شما را مشخص می‌کند بایستی در قسمت مشخصهٔ ماشین میزبان نیز به گونه‌ای زیر شبکه‌ها مشخص شوند. این کار از طریق مفهومی به نام "**الگوی زیرشبکه**"[2] انجام می‌شود.

شما با نگاه اول به اولین عدد سمت چپ متوجه خواهید شد که این آدرس از چه کلاسی است ولی هنوز موارد مبهمی وجود دارد : آیا شبکه ای که آدرس آنرا پیش رو دارید فقط یک شبکه است یا خودش زیر شبکه بندی شده است؟ یعنی از چند شبکهٔ محلی متصل بهم تشکیل شده است؟



شکل۳. یک شبکهٔ خود مختار که کلاً با یک آدرس مشخصهٔ شبکه شناسایی می‌شود.

این اطلاعات برای شبکه‌های مبتنی بر TCP/IP که قابلیت مسیریابی دارند بسیار مهم است، چرا که هر ماشینِ میزبان بایستی قادر به درک این مطلب باشد که آیا یک ماشین مقصد با آدرس خاصّ و مشخص، بر روی شبکهٔ محلی خودش واقع است یا آنکه آن آدرس متعلق به زیر شبکه دیگری است. بر اساس این اطلاعات ماشین میزبان تصمیم می‌گیرد که آیا انتقال اطلاعات باید مستقیماً بر روی شبکهٔ محلی انجام شود یا آنکه باید از طریق یک مسیریاب روی شبکه ای دیگر ارسال شود.

تمامی ماشین‌های میزبان برای تشخیص محل مقصد یک بستهٔ IP در شبکه احتیاج به یک مشخصهٔ دیگر دارند و آن "الگوی زیرشبکه" نامیده می‌شود.

الگوی زیرشبکه یک عدد ۳۲ بیتی دودویی است که برای ماشین میزبان نقش یک مقایسه‌گر را بازی می‌کند تا با استفاده از آن بتواند تشخیص دهد که آیا مقصد روی همین شبکه محلی است که خودش به آن تعلق دارد یا روی شبکه دیگری است.

فرآیند استفاده از "الگوی زیرشبکه" را با استفاده از مثال قبل ولی با آدرس کلاس B آموزش می‌دهیم:

فرض کنید شما کاربری روی یک ایستگاه در شبکه دانشگاه خودتان هستید و آدرس IP متعلق به دستگاه شما به‌صورت زیر اختصاص داده شده است :

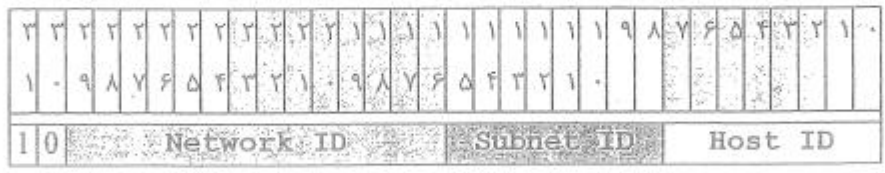
131.55.213.73

با یک نگاه متوجه می‌شوید که آدرس از کلاس B است که مشخصهٔ شبکهٔ آن معادل 131.55.0.0 و مشخصهٔ ماشین شما 0.0.213.73 است؛ ولی هنوز نمی‌دانید شبکه ای که مشخصهٔ آن معادل 131.55 است آیا زیر شبکه دارد یا خیر؟

فرض کنید که دانشگاه شما با آدرس شبکه 131.55.0.0، می‌خواهد حداکثر دارای ۲۵۴ زیر شبکه باشد، به‌همین دلیل فرض کرده است که در فیلد مشخصهٔ ماشین میزبان (Host ID) که در کلاس B دو بایت سمت راست را شامل می‌شود، بایت دوم آن به عنوان مشخصهٔ مربوط به زیر شبکه تعریف شود. یعنی فیلد دوبایتی مربوط به مشخصهٔ ماشین میزبان به دو بخش تقسیم شده است:

الف) مشخصهٔ زیرشبکه

ب) مشخصهٔ ماشین میزبان



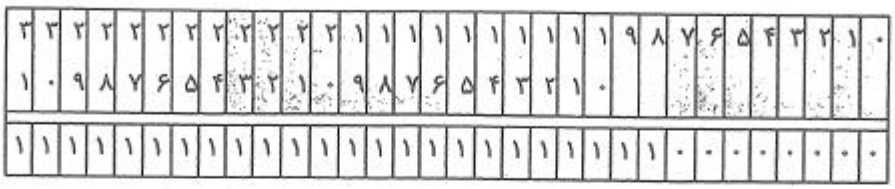
ماشین شما تصمیم دارد بسته ای را برای یک ماشین میزبان با آدرس IP معادل 131.55.108.75 بفرستد؛ ماشین از کجا می‌تواند بفهمد که مقصد روی همین شبکه محلی که شما بدان متعلق هستید واقع است یا آنکه به شبکهٔ محلی در یک دانشکدهٔ دیگر متعلق است. دانستن این موضوع بسیار با اهمیت خواهد بود چرا که اگر ماشین میزبان مورد نظر روی شبکهٔ دیگری باشد بسته باید با آدرس فیزیکی "مسیریاب پیش فرض"[1] روی کانال ارسال شود. بنابراین تمام ماشین‌های روی شبکه بایستی از وضعیت زیر شبکه‌ها مطلع باشند.

با توجه به آنچه که در بالا اشاره شد دومین بایت از سمت راست به عنوان مشخصهٔ زیر شبکه اختصاص داده شده است و به‌همین دلیل هر ماشین برای دانستن آنکه آیا ماشین مقصد در شبکه محلی خودش واقع است یا در خارج از شبکه قرار دارد باید قسمت "مشخصهٔ شبکه" و "مشخصهٔ زیرشبکه" از آدرس IP خودش را با همین مشخصه‌ها از آدرس مقصد مقایسه نماید.

---

[1] Default Gateway

اینجاست که یک الگوی ۳۲ بیتی تعریف می‌شود که یک عدد ۳۲ بیتی و در این مثال به‌صورت 255.255.255.0 است:



هر گاه ماشین بخواهدیک آدرس IP را تحلیل کند. الگوی فوق را با آدرس IP خودش AND می‌کند. (با اینکار در حقیقت Host ID خودش را صفر می‌نماید) سپس مجدداً الگو را با آدرس IP مقصد AND می‌کند (مشخصهٔ ماشین مقصد هم صفر می‌شود) حال نتیجه دو مرحله را با هم مقایسه می‌نماید. اگر نتیجه دو مرحله یکسان بود، هم مشخصهٔ شبکه و هم مشخصهٔ زیرشبکه از آدرس‌های مبدأ و مقصد یکی است و هر دو روی یک شبکهٔ محلی قرار دارند. در صورت عدم تساوی، ماشین مبدأ به این نتیجه می‌رسد که مقصد مورد نظر روی شبکه محلی خودش نیست و آن بسته‌بایستی به آدرس فیزیکی مسیریابِ پیش فرض ارسال شود.

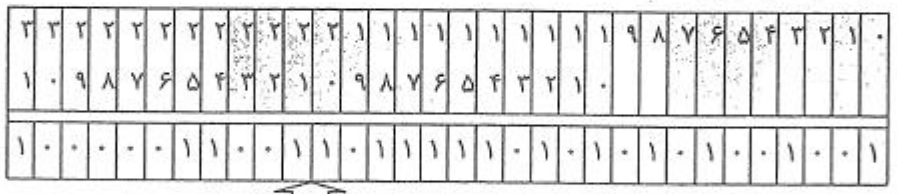
فرض کنید بسته ای با آدرس‌های مشخص زیر بخواهد ارسال شود:

آدرس ماشین مبدأ: 131.55.213.73

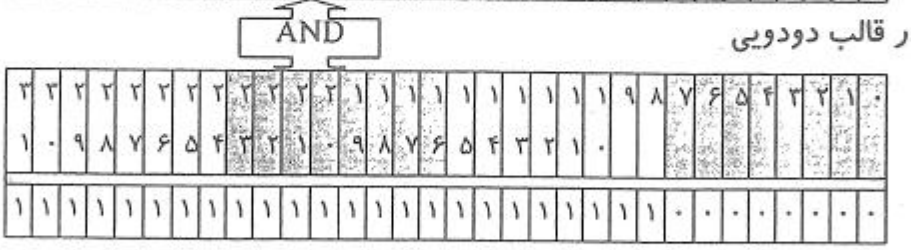
آدرس ماشین مقصد: 131.55.108.75

الگوی زیرشبکه: 255.255.255.0

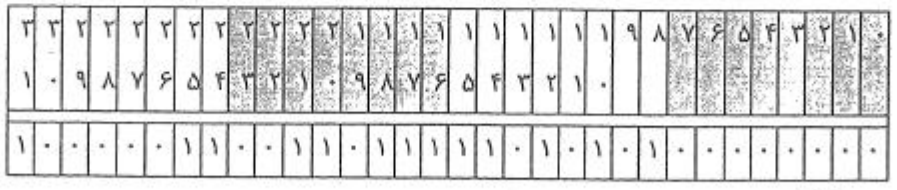
آدرس ماشین مبدا در قالب دودویی



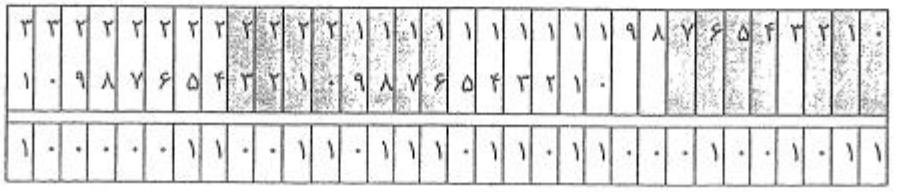
الگوی زیرشبکه در قالب دودویی



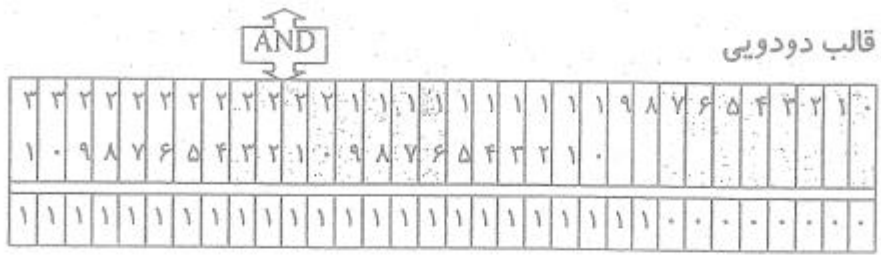
حاصل مرحلهٔ ۱ :



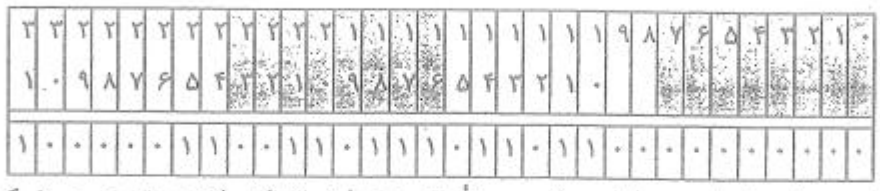
آدرس ماشین مقصد در قالب دودویی



الگوی زیرشبکه در قالب دودویی



حاصل مرحلهٔ ۲ :

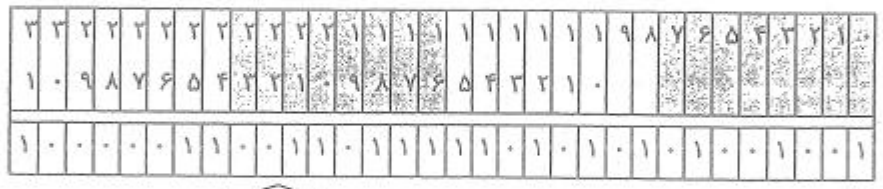


حاصل مراحل ۱ و ۲ با هم مساوی نیستند و بنابراین ماشین مبدأ متوجه خواهد شد که ماشین مقصد روی شبکه محلی خودش نیست و بسته اطلاعاتی را بایستی به آدرس فیزیکی مسیریاب پیش فرض ارسال نماید.

به عنوان مثالی دیگر فرض کنید ماشین شما می‌خواهد برای ماشینی با آدرس IP زیر بسته ای را ارسال نماید:

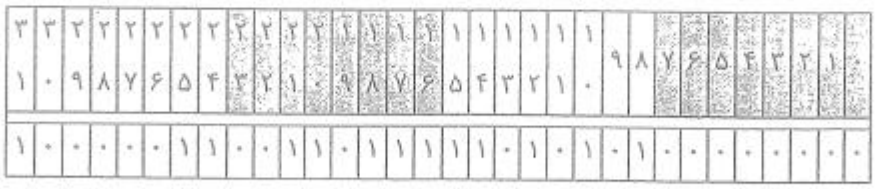
131.55.213.84

آدرس ماشین مبدأ در قالب دودویی

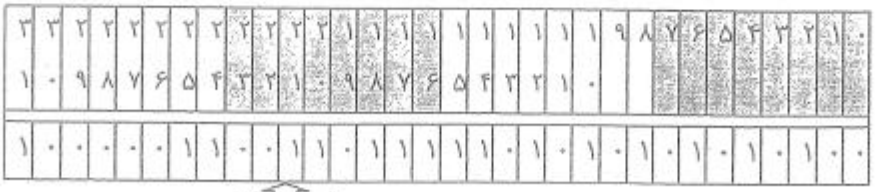


الگوی زیرشبکه در قالب دودویی

حاصل مرحلهٔ ۱ :



آدرس ماشین مقصد در قالب دودویی



الگوی زیرشبکه در قالب دودویی

حاصل مرحلهٔ ۲ :

۳۱	۳۰	۲۹	۲۸	۲۷	۲۶	۲۵	۲۴	۲۳	۲۲	۲۱	۲۰	۱۹	۱۸	۱۷	۱۶	۱۵	۱۴	۱۳	۱۲	۱۱	۱۰	۹	۸	۷	۶	۵	۴	۳	۲	۱	۰
۱	۰	۰	۰	۰	۰	۰	۱	۱	۰	۰	۱	۱	۰	۱	۱	۱	۱	۱	۰	۱	۰	۱	۰	۱	۰	۰	۰	۰	۰	۰	۰

همانگونه که مشاهده می‌شود حاصل مراحل ۱ و ۲ مساوی هستند و بالطبع مبدأ و مقصد روی یک شبکه محلی واقعند و هیچ لزومی ندارد که ارسال بسته به آدرس فیزیکی مسیریاب پیش فرض انجام شود، بلکه باید مستقیماً از آدرس فیزیکی ایستگاه مقصد استفاده شود .

ذکر این نکته ضروری است که الگوی زیرشبکه باید به عنوان یکی از پارامترهای پیکربندی TCP/IP تنظیم شود و فقط برای تشخیص محل شبکهٔ مقصد کاربرد دارد.

الگوی زیرشبکه در مثالهای بالا ساده‌ترین حالت بود که به آن‌ها "الگوی زیرشبکهٔ استاندارد"[1] گفته می‌شود چرا که الگوها دقیقاً مبتنی بر تقسیمات هشت‌بیتی هستند.

۳ـ۹ ـ زیر شبکه‌های غیر استاندارد

الگوهای زیرشبکه برای تقسیم فضای آدرس‌دهی در شبکه‌های کلاس A، B و C به تعدادی زیرشبکه، تعریف می‌شوند. در مثالهایی که بررسی کردیم الگوی شبکه به‌صورت زیر تعریف شده بود:

255.255.255.0

حال الگوی زیر را در نظر بگیرید:

255.255.240.0

عدد ۲۴۰ در الگوی زیرشبکه چه چیزی را تعریف می‌کند؟ به فرم دودویی الگوی بالا دقت کنید:

۳۱	۳۰	۲۹	۲۸	۲۷	۲۶	۲۵	۲۴	۲۳	۲۲	۲۱	۲۰	۱۹	۱۸	۱۷	۱۶	۱۵	۱۴	۱۳	۱۲	۱۱	۱۰	۹	۸	۷	۶	۵	۴	۳	۲	۱	۰
۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰

بفرض اگر الگوی بالا برای زیر شبکه بندی آدرس کلاس B به کار رفته باشد، نشان دهنده آن است که چهار بیت پرارزش از بایت دوم برای تعیین شماره زیر شبکه به کار رفته است و ۱۲ بیت باقیمانده به عنوان "مشخصهٔ ماشین میزبان" استفاده شده است؛ بدین معنا که با این الگو می‌توان ۱۴ زیر شبکه (2^4-2) تعریف کرد بگونه‌ای که در هر زیرشبکه ۴۰۹۴، ($2^{12}-2$) ماشینِ میزبان قابل آدرس دهی خواهد بود.

فراموش نکنید که همیشه تعداد زیرشبکه‌ها و ماشین‌های میزبان از کلّ تعداد قابل تعریف، دوتا کمتر است؛ چراکه زیرشبکه یا ماشینی که تمام بیت‌های آن صفر یا تماماً یک باشد قابل تعریف نیست.

کلاً برای آنکه با تنظیم الگوهای زیر شبکه آشنا شوید الگوریتم آنرا در زیر تشریح می‌کنیم:

الف) با دقت و دوراندیشی کافی تعیین کنید چه تعداد زیر شبکه و چه تعداد ماشین میزبان روی هر زیرشبکه خواهید داشت؟ به تعداد زیرشبکه‌ها و ماشین‌ها عدد ۲ را اضافه کرده و سپس تعیین کنید هر کدام از این اعداد به حداقل چند بیت نیاز دارند.

---

[1] Standard Subnet Mask

ب) الگوی ۳۲ بیتی زیرشبکه را بگونه‌ای تنظیم کنید که در سمت راست آن به تعداد بیتی که برای آدرس دهی ماشین‌های میزبان نیاز است صفر قرار بگیرد. بیت‌های باقیمانده را هم تماماً ۱ قرار بدهید.

ج) الگوی دودویی را بفرم دهدهی نقطه دار تبدیل کنید.

د) زیرشبکه‌ها و ماشین‌های میزبان روی هر زیرشبکه را تعریف نمایید.

حال با مثالی این روند را بهتر بررسی می‌کنیم:

فرض کنید یک شرکت بزرگ دارای حداکثر ۲۵ شبکه محلی است که هر شبکه محلی حداکثر تا ۱۰۰۰ میزبان را حمایت می‌نماید. الگوی زیر شبکه را تنظیم نمایید.

الف) برای آدرس دهیِ ۲۵ زیرشبکهٔ محلی ۵ بیت کفایت می‌نماید. (با ۵ بیت می‌توان سی زیرشبکه (2-32) را تعریف کرد.).

ب) آدرس از کلاس B است پس قسمت ۱۶ بیتی از مشخصهٔ ماشین میزبان، پس از کسر ۵ بیت که به عنوان زیر شبکه استفاده شد، مقدار ۱۱ بیت خواهد بود. حداکثر تعداد ماشین میزبان قابل تعریف به‌صورت زیر حساب می‌شود:

$$2^{11}-2=2046$$

تعداد ماشین قابل تعریف از تعدادی که نیاز داشتیم خیلی بیشتر است که اجازه می‌دهد زیرشبکه در آینده گسترش یابد. پس الگوی زیرشبکه برای شبکهٔ این شرکت به صورت زیر تنظیم می‌شود:

۳۱	۳۰	۲۹	۲۸	۲۷	۲۶	۲۵	۲۴	۲۳	۲۲	۲۱	۲۰	۱۹	۱۸	۱۷	۱۶	۱۵	۱۴	۱۳	۱۲	۱۱	۱۰	۹	۸	۷	۶	۵	۴	۳	۲	۱	۰
۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰

الگوی زیرشبکه 255.255.248.0

دقت کنید که اگر دور اندیشی کافی نداشته باشید و نیاز باشد که زمانی ساختار زیر شبکه را توسعه بدهید، برای تغییر یک الگوی زیر شبکه به الگوی دیگر، باید پیکربندی[1] تمام ماشین‌های شبکه به‌صورت دستی تنظیم شود که دردسر زیادی دارد. لذا از میزان رشد آدرس‌های زیرشبکهٔ خود اطمینان حاصل کنید و طرح را مطابق با نیازتان بریزید. هرگونه اشتباه در تنظیم الگوی زیرشبکه منجر به عدم کارکرد صحیح شبکه خواهد شد.

بگونه‌ای که اشاره شد وقتی تعداد زیر شبکه‌ها را حساب می‌نمایید نهایتاً عدد ۲ را با آن جمع کنید و سپس تعداد بیت‌های مورد نیاز را برای عدد بدست آمده محاسبه نمایید. مثلاً فرض کنید که کل شبکه دقیقاً چهار زیرشبکه داشته باشد؛ پس برای الگوی زیرشبکه باید سه بیت اختصاص بدهید.

۴ ـ ۹ ـ CIDR[2]: مسیریابی بر اساس آدرس‌های بدون کلاس

چندین دهه است که از پروتکل IP استفاده گسترده‌ای می‌شود. عملکرد این پروتکل بسیار عالی بوده و همان‌گونه که اشاره کردیم به رشد نمایی شبکه اینترنت کمک کرده است. متأسفانهIP در حال قربانی شدن در پای محبوبیت خود است چرا که با کمبود فضای آدرس مواجه شده است. از زمانی که افق این مشکل پدیدار شد، بحث‌ها و مناقشات بسیار گسترده‌ای را در جامعه اینترنت دامن زد که چه کاری می‌توان برای آن انجام داد. در بخش جاری، این مشکل و راه‌حل‌های پیشنهادی را تشریح می‌نماییم.

---

[1] Configuration

[2] CIDR: Classless InterDomain Routing

ب) الگوی ۳۲ بیتی زیرشبکه را بگونه‌ای تنظیم کنید که در سمت راست آن به تعداد بیتی که برای آدرس دهی ماشین‌های میزبان نیاز است صفر قرار بگیرد. بیت‌های باقیمانده را هم تماماً ۱ قرار بدهید.

ج) الگوی دودویی را بفرم دهدهی نقطه دار تبدیل کنید.

د) زیرشبکه‌ها و ماشین‌های میزبان روی هر زیرشبکه را تعریف نمایید.

حال با مثالی این روند را بهتر بررسی می‌کنیم:

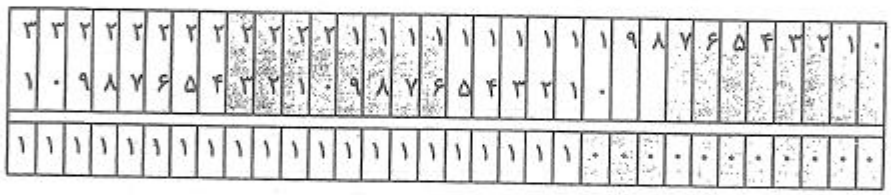
فرض کنید یک شرکت بزرگ دارای حداکثر ۲۵ شبکه محلی است که هر شبکه محلی حداکثر تا ۱۰۰۰ میزبان را حمایت می‌نماید. الگوی زیر شبکه را تنظیم نمایید.

الف) برای آدرس دهیِ ۲۵ زیرشبکهٔ محلی ۵ بیت کفایت می‌نماید. (با ۵ بیت می‌توان سی زیرشبکه (2-32) را تعریف کرد.)

ب) آدرس از کلاس B است پس قسمت ۱۶ بیتی از مشخصهٔ ماشین میزبان، پس از کسر ۵ بیت که به عنوان زیر شبکه استفاده شد، مقدار ۱۱ بیت خواهد بود. حداکثر تعداد ماشین میزبان قابل تعریف به‌صورت زیر حساب می‌شود:

$$2^{11}-2=2046$$

تعداد ماشین قابل تعریف از تعدادی که نیاز داشتیم خیلی بیشتر است که اجازه می‌دهد زیرشبکه در آینده گسترش یابد. پس الگوی زیرشبکه برای شبکهٔ این شرکت به صورت زیر تنظیم می‌شود:



الگوی زیرشبکه 255.255.248.0

دقت کنید که اگر دور اندیشی کافی نداشته باشید و نیاز باشد که زمانی ساختار زیر شبکه را توسعه بدهید، برای تغییر یک الگوی زیر شبکه به الگوی دیگر، باید پیکربندی[1] تمام ماشین‌های شبکه به‌صورت دستی تنظیم شود که دردسر زیادی دارد. لذا از میزان رشد آدرس‌های زیرشبکهٔ خود اطمینان حاصل کنید و طرح را مطابق با نیازتان بریزید. هرگونه اشتباه در تنظیم الگوی زیرشبکه منجر به عدم کارکرد صحیح شبکه خواهد شد.

بگونه‌ای که اشاره شد وقتی تعداد زیر شبکه‌ها را حساب می‌نمایید نهایتاً عدد ۲ را با آن جمع کنید و سپس تعداد بیت‌های مورد نیاز را برای عدد بدست آمده محاسبه نمایید. مثلاً فرض کنید که کل شبکه دقیقاً چهار زیرشبکه داشته باشد؛ پس برای الگوی زیرشبکه باید سه بیت اختصاص بدهید.

۴ـ۹ـ CIDR[2]: مسیریابی بر اساس آدرس‌های بدون کلاس

چندین دهه است که از پروتکل IP استفاده گسترده‌ای می‌شود. عملکرد این پروتکل بسیار عالی بوده و همان‌گونه که اشاره کردیم به رشد نمایی شبکه اینترنت کمک کرده است. متأسفانهIP در حال قربانی شدن در پای محبوبیت خود است چرا که با کمبود فضای آدرس مواجه شده است. از زمانی که افق این مشکل پدیدار شد، بحث‌ها و مناقشات بسیار گسترده‌ای را در جامعه اینترنت دامن زد که چه کاری می‌توان برای آن انجام داد. در بخش جاری، این مشکل و راه‌حل‌های پیشنهادی را تشریح می‌نماییم.

---

[1] Configuration

[2] CIDR: Classless InterDomain Routing

تا سال ۱۹۷۸ افراد دوراندیشی که حدس می‌زدند در روزگاری تعداد شبکه‌های متصل به اینترنت به مرز ۱۰۰۰۰۰ برسد، انگشت‌شمار بودند و حتی اغلب متخصصین این فن نیز چنین ایده‌ای را به مسخره می‌گرفتند، ولی صدهزارمین شبکه در دنیا در سال ۱۹۹۶ به اینترنت پیوست و به نحوی که در بالا اشاره شد اینترنت در حال مواجه شدن با کمبود آدرس‌های IP است. در اصل بیش از دو میلیارد آدرس IP وجود دارد ولی در عمل به دلیل تقسیم‌بندی نامناسب فضای آدرس در قالب چند کلاس، میلیون‌ها آدرس IP به هدر رفته است. بالاخص، بیشترین محدودیت در کلاس B است. برای بسیاری از موسسات یک شبکه کلاس A با شانزده میلیون آدرس، بسیار بزرگ و بی‌مصرف و کلاس C با 256 آدرس بسیار کوچک و ناکافی است؛ فقط شبکه کلاس B با 65536 آدرس مناسب است. این مشکل در فرهنگ رایج اینترنت به نام مشکل « سه خرس » مشهور شده است. (برگرفته از داستان موطلایی و سه خرس)

حقیقت آن‌است که حتی کلاس B هم برای بسیاری از سازمان‌ها و موسسات، بسیار بزرگ است. بررسی‌ها نشان داده که بیش از نیمی از شبکه‌های کلاس B، کمتر از 50 ماشین دارند! برای چنین شبکه‌هایی استفاده از کلاس C کفایت می‌کند ولی بی‌تردید تمام موسساتی که متقاضی کلاس B بوده‌اند بدان می‌اندیشیده‌اند که روزی فیلد هشت بیتی کلاس C برای شبکه آن ها کافی نخواهد بود. نگاهی به گذشته نشان می‌دهد که بهتر آن بوده در کلاس C فیلد شماره شبکه به جای هشت بیت، ده بیت می‌بود تا در هر شبکه 1022 ماشین میزبان قابل آدرس‌دهی باشد. اگر چنین حالتی را می‌داشتیم شاید بسیاری از موسسات و سازمان‌ها به کلاس C اکتفا می‌کردند و در عین حال نیم میلیون از چنین شبکه‌هایی قابل تعریف بود. (برخلاف کلاس B که فقط 16384 شبکه قابل تعریف است).

نمی‌توان تقصیر را به گردن طراحان اینترنت انداخت که چرا تعداد کلاس‌های B را بیشتر (و با فضای آدرس کوچکتر) در نظر نگرفتند. در روزگاری که تصمیم گرفته شد فقط سه کلاس وجود داشته باشد، اینترنت شبکه‌ای تحقیقاتی بود که فقط مراکز پژوهشی و دانشگاهی مهم ایالات متحده را به هم متصل می‌کرد. (البته به اضافه معدودشرکت‌ها و سایت‌های نظامی که آن‌ها نیز در کار پژوهش بودند) هیچ‌کس نمی‌توانست پیش‌بینی کند که اینترنت روزی بتواند در حد وسیع و به عنوان سیستمی ارتباطی حتی با شبکه‌های تلفن رقابت نماید! در آن زمان هیچ کس در این ادعا شکی نداشت که اگر تمام 2000 کالج و دانشگاه ایالات متحده و حتی اکثر دانشگاه‌های جهان به اینترنت بپیوندند باز هم 16000 تا نمی‌شود چرا که این تعداد دانشگاه در کل دنیا وجود نداشت. به علاوه در آن زمان برای آن‌که پردازش بسته‌ها سریع‌تر انجام بشود بهتر بود فیلد شماره ماشین در آدرس IP، تعداد صحیحی از بایت باشد.

[به دلیل سرعت پایین پردازنده‌ها در آن زمان، پردازش بیتی فیلدهای آدرس، از سرعت مسیریابی می‌کاست.]

ولیکن در طرف مقابل اگر مثلا برای فیلد شماره شبکه در کلاس B بیست بیت کنار گذاشته می‌شد مشکل دیگری بروز می‌کرد: « مشکل رشد انفجاری جداول مسیریابی». از دید مسیریاب‌ها فضای آدرس‌های IP، سلسله مراتب دو سطحی شامل شماره شبکه و شماره ماشین‌ها است. مسیریاب‌ها مجبور به دانستن شماره ماشین‌های میزبان نیستند ولی باید شماره شبکه‌ها را بدانند. اگر حتی نیمی از شبکه‌های کلاس C به‌کار گرفته شده باشند هر مسیریاب در کل اینترنت نیاز به جدولی با نیم میلیون درایه (Entry) دارد تا بتواند خط خروجی مناسب برای رسیدن به هر شبکه را مشخص نماید. (گذشته از اطلاعات دیگری که به ازای هر شبکه باید در جدول مسیریابی درج شود).

شاید تهیه فضای فیزیکی لازم برای ذخیره نیم میلیون درایه (Entry) در جدول مسیریابی، امکان‌پذیر باشد هر چند برای مسیریاب‌هایی که جداول مسیریابی را در حافظهٔ نوع ایستا (Static RAM) ذخیره می‌کنند، چنین فضایی بسیار گران تمام می‌شود. مشکل اساسی در پیچیدگی الگوریتم‌های مدیریت و پردازش چنین جدولی است.

پیچیدگی زمانی این الگوریتم‌ها غیرخطی است.[1] از این بدتر آن‌که نرم‌افزار یا سخت‌افزار طراحی شده برای مسیریاب‌های موجود، زمانی طراحی شده که به اینترنت بیش از هزار شبکه متصل نبود و به نظر می‌رسید که یک دهه طول می‌کشد تا این تعداد به 10000 برسد. امروزه این‌گونه طراحی‌ها بهینه نیستند.

مضاف بر این، در الگوریتم‌های مختلف مسیریابی نیاز است که جداول مسیریابی به‌طور متناوب ارسال و مبادله شود. (مثل الگوریتم بردار فاصله) هر چه جداول مسیریابی بزرگتر باشد احتمال آن‌که بخشی از آن در حین مبادله از دست برود بیشتر خواهد شد و به نقص داده‌های جدول مسیریابی و احتمالاً ناپایداری فرآیند هدایت بسته‌ها خواهد انجامید.

مشکل جداول مسیریابی را می‌توان با افزایش «سطوح سلسله مراتب» حل کرد. مثلاً می‌توان آدرس‌های IP را بدین نحو تعریف کرد که شامل فیلدهای کشور، ایالت/ استان، شهر، شبکه و شماره ماشین میزبان باشد. بدین ترتیب، مسیریاب‌های ستون فقرات باید در خصوص مسیرهای رسیدن به هر کشور آگاهی داشته باشند، مسیریاب‌های درون کشور در خصوص مسیرهای رسیدن به هر ایالت یا استان، مسیریاب‌های ایالت یا استان در مورد مسیرهای رسیدن به هر شهر و مسیریاب‌های هر شهر فقط باید راه رسیدن به هر شبکه را بدانند. متأسفانه چنین راه‌حلی نیازمند فضایی بزرگتر از 32 بیت برای آدرس IP است و طبعاً از فضای آدرس استفاده بهینه نخواهد شد. (چرا که مثلاً در این الگو کشور لیختن اشتاین به همان تعداد بیت در آدرس IP دارد که کشور ایالات متحده!)

کوتاه سخن آن‌که هر یک از راه‌حل‌های ارایه شده مشکلی را حل و مشکل جدیدی را ایجاد می‌کردند. راه‌حل نهایی و پیاده شده در اینترنت که توانست به اینترنت اجازه نفس کشیدن بدهد، روش CIDR (مسیریابی بر اساس آدرس‌های بدون کلاس) بود. ایدهٔ اصلی در CIDR که در سند RFC 1519 تشریح شده آن است که آدرس‌های IP بدون در نظر گرفتن کلاس و به صورت بلوک‌هایی با طول متغیر تخصیص یابد. مثلاً اگر یک سایت نیاز به 2000 آدرس داشته باشد یک بلوک آدرس 2048 تایی به او داده می‌شود.

حذف کلاس‌های آدرس، فرآیند هدایت بسته‌ها را پیچیده‌تر می‌کند. در سیستم مبتنی بر کلاس، فرآیند هدایت بدین نحو بود که وقتی بسته‌ای به یک مسیریاب می‌رسید، یک کپی از آدرس IP به اندازه 28 بیت به راست شیفت داده می‌شد تا فقط چهار بیت سمت چپ آدرس (که کلاس آدرس را مشخص می‌کند) باقی بماند. بر اساس این چهار بیت (16 حالت مختلف) بسته‌ها در یکی از کلاس‌های A و B و C (و D در صورت پشتیبانی از آن) مرتب می‌شدند. (از این 16 حالت مختلف، هشت حالت برای کلاس A است ـ 0xxx ـ چهار حالت برای کلاس B ـ 10xx ـ دو حالت برای کلاس C ـ 110x ـ و دو حالت برای کلاس‌های D و E است.) پس از تشخیص کلاس آدرس، برای به‌دست آوردن شماره شبکه، آدرس IP با یکی از الگوهای -8، -16، -24 به صورت بولی AND و بخش شماره ماشین حذف می‌شد. سپس شماره شبکه در هر یک از جدول مربوط به آدرس‌های کلاس A , B و C جستجو می‌شد. جداول مسیریابی برای کلاس‌های A و B بر حسب شماره شبکه ایندکس شده بودند.[2] درعوض جداول مسیریابی برای کلاس C مبتنی بر روش جداول Hash (Hash Table) پیاده شده بود. پس از آن‌که درایه متناظر با آدرس شبکه در یکی از این جداول پیدا می‌شد خط خروجی متناسب با آن شبکه مشخص شده و بسته بر روی آن خط هدایت می‌گردید.

در CIDR این الگوریتم ساده، کار نخواهد کرد. درعوض به هر یک از درایه‌های جدول مسیریابی یک فیلد 32 بیتی جدید افزوده شده که الگوی آن را [از طریق یک MASK سی و دو بیتی] مشخص می‌کند. بدین‌ترتیب برای تمام شبکه‌ها فقط یک جدول مسیریابی یکتا وجود دارد که در حقیقت یک آرایه ستونی متشکل از آدرس IP، الگوی زیرشبکه (Subnet Mask) و خط خروجی است. وقتی بسته‌ای وارد می‌شود ابتدا آدرس IP آن استخراج می‌شود. سپس جدول مسیریابی درایه به درایه (Entry by Entry) جستجو و آدرس مقصد بسته پس از AND شدن با الگوی زیر شبکه از هر درایه با آدرس IP از آن درایه مقایسه می‌شود. این فرآیند آن‌قدر تکرار

---

[1] پیچیدگی غیرخطی این الگوریتم‌ها عموما $O(n^2)$ و $O(n.\log n)$ است. - م

[1] به عبارت ساده به دلیل کم بودن تعداد شبکه‌ها جداول مسیریابی برای کلاس‌های A و B در ساختمان داده‌ای شبیه به آرایه ذخیره می‌شد. - م

می‌گردد تا به موارد مطابقت برسد. این امکان وجود دارد که چندین درایه با یک آدرس IP مطابقت داشته باشد (به دلیل طول متفاوت ا لگوهای زیر شبکه). در این حالت درایه‌ای که طول الگوی زیر شبکه آن از همه بزرگتر است از بین آن‌ها انتخاب می‌شود. به عبارتی اگر دو مورد مطابق با طول الگوی 255.255.240.0)/20) و الگوی 24 / (255.255.255.0) پیدا شود، درایه دوم انتخاب می‌شود.

برای سرعت بخشیدن به فرآیند جستجو و مطابقت، الگوریتم‌های پیچیده‌ای ابداع شده است. (Ruiz – Sanchesetal .2001) مسیریاب‌های تجاری در بازار امروز از تراشه‌های VLSI خاصی بهره گرفته اند که الگوریتم مذکور را به صورت یک «سخت‌افزار درون‌کار» (Embedded Hardware) پیاده‌سازی کرده‌اند.

برای آن‌که فهم فرآیند هدایت بسته‌ها در CIDR را ساده‌ترکنیم مثالی را مدنظر قرار بدهید که در آن میلیون‌ها آدرس تعریف شده است و آدرس شروع 194.24.0.0 است. فرض کنید که دانشگاه کمبریج به 2048 آدرس نیاز دارد و آدرس‌های 194.24.0.0 تا 194.24.7.255 به آن اختصاص داده شده است. (الگوی زیر شبکه نیز 255.255.248.0 است). بعداً دانشگاه آکسفورد تقاضای 4096 آدرس IP می‌دهد. از آنجایی که بلوک‌های آدرس 4096 تایی باید در مرز 4096 بایتی قرار بگیرد نمی‌توان آدرس‌هایی که از 194.24.8.0 شروع می‌شود را به آن اختصاص داد. درعوض آدرس اختصاص داده شده به او در محدودهٔ 194.24.16.0 تا 194.24.31.255 و با الگوی 255.255.240.0 خواهد بود. در این‌جا دانشگاه ادینبورو تقاضای 1024 آدرس داده و فضای 194.24.8.0 تا 194.24.11.255 با الگوی 255.255.252.0 به او تعلق می‌گیرد. این انتساب‌ها در جدول زیر خلاصه شده‌اند.

دانشگاه	اولین آدرس	آخرین آدرس	تعداد آدرس	الگوی نمایش
Cambridge	194.24.0.0	194.24.7.	2048	194.24.0.0/21
Edinburgh	194.24.8.0	194.24.11.255	1024	194.24.8.0/22
در دسترس و آزاد	194.24.12.0	194.24.15.255	1024	194.24.12/22
Oxford	194.24.16.0	194.24.31.255	4096	194.24.16.0/20

انتساب آدرس‌های IP

حال جداول مسیریابی در تمام مسیریاب‌های واقع بر ستون فقرات اینترنت در جهان باید با این سه درایه جدید به هنگام شود. هر درایه یک آدرس مبنا و یک الگوی زیر شبکه است. این درایه‌ها در مبنای دو عبارتند از:

	آدرس				الگوی زیر شبکه (Subnet Mask)			
C:	11000010	00011000	00000000	00000000	11111111	11111111	11111000	00000000
E:	11000010	00011000	00001000	00000000	11111111	11111111	11111100	00000000
O:	11000010	00011000	00010000	00000000	11111111	11111111	11110000	00000000

حال ببینیم وقتی که بسته‌ای با آدرس 194.24.17.4. وارد یک مسیریاب می‌شود چه اتفاقی می‌افتد. این آدرس به صورت دودویی عبارت است از:

11000010 00011000 00010001 00000100

ابتدا این آدرس با الگوی زیر شبکه کمبریج، AND می‌شود و نتیجه زیر به‌دست می‌آید:

11000010 00011000 00010000 00000000

این مقدار با آدرس مبنای دانشگاه کمبریج مطابقت ندارد. حال مجدداً آدرس اصلی با الگوی زیر شبکه دانشگاه ادینبورو AND شده و نتیجه زیر به‌دست می‌آید:

11000010 00011000 00010000 00000000

این مقدار نیز با آدرس مبنای دانشگاه ادینبورو تطابق ندارد و همین کار برای دانشگاه آکسفور تکرار شده مقدار زیر به‌دست می‌آید:

11000010 00011000 00010000 00000000

این مقدار با آدرس مبنای دانشگاه آکسفورد مطابقت دارد. اگر هیچ مورد تطبیق دیگری در جدول یافت نشد بسته بر روی خطی ارسال می‌شود که در درایه متناظر با شبکه دانشگاه آکسفورد درج شده است.

حال اجازه بدهید، آدرس این سه دانشگاه را از دید یک مسیریاب در نبراسکای اوهاما بررسی کنیم. این مسیریاب چهار خط به مینیاپولیس، نیویورک، دالاس و دنور دارد. وقتی نرم‌افزار مسیریاب اوهاما، این سه درایه جدید را جهت درج در جدول مسیریابی خود دریافت می‌دارد، متوجه می‌شود که قادر است هر سه تای آن‌ها را در یک «درایه واحد و تجمیع شده» (Aggregate Entry) به صورت 194.24.0.0/19 ادغام نماید.[1] آدرس و الگوی زیر شبکه در مبنای دو به صورت زیر است:

11000010 00000000 00000000 00000000 11111111 11111111 11100000 00000000

طبق این درایه، تمام بسته‌هایی که به مقصد یکی از این سه دانشگاه روانه شده‌اند به سوی نیویورک هدایت می‌شوند. با تجمیع این سه درایه، مسیریاب اوهاما توانسته به میزان دو درایه حجم جدول خود را کاهش بدهد.

به همین ترتیب اگر مسیریاب نیویورک برای تمام ترافیک منتهی به انگلستان فقط یک خط به لندن داشته باشد او نیز سه درایه فوق را در یک درایه ادغام می‌کند ولیکن اگر برای لندن و ادینبورو دو خط مجزا داشته باشد باید هر سه تای آن‌ها را به‌طور مجزا در جدول ذخیره کند. عمل تجمیع (Aggregation) در اینترنت به‌طور گسترده‌ای مورد استفاده قرار گرفته تا حجم جداول مسیریابی کاهش یابد.

آخرین نکته در این مثال آن است که بر طبق درایه ادغام شده در جدول مسیریابی مسیریاب واقع در اوهاما حتی بسته‌هایی که به آدرس اختصاص داده نشده روانه هستند [یعنی آدرس‌های بین 194.24.12.0 تا 194.24.15.255] نیز به سوی نیویورک هدایت می‌شوند. مادامی که این آدرس‌ها به کسی اختصاص داده نشده، هیچ مشکلی به وجود نمی‌آید چرا که بنا نیست بسته‌هایی با این آدرس‌ها تولید شوند. ولی اگر این بلوک آدرس، به شرکتی در کالیفرنیا داده شود باید درایه‌ای جدید به شکل 194.24.12.0/22 در جدول مسیریابی تمام مسیریاب‌ها درج شود تا بسته‌هایی به مقصد این شبکه نیز به درستی مسیریابی شوند.

۵ ـ ۹ ـ پروتکل ICMP[2]

پروتکل IP، پروتکلی "بدون اتصال"[3] و "غیر قابل اعتماد"[4] است؛ بدون اتصال بدین معنا که مسیریاب هر بسته را بدون هیچگونه هماهنگی با مقصد بسته یا مسیریاب بعدی ارسال می‌نماید، بدون آنکه بتواند اطلاعی از وجود یا عدم وجود مقصد داشته باشد. در ضمن هر مسیریاب پس از ارسال یک بسته آنرا فراموش می‌کند و منتظر "پیام دریافت بسته"[5] از گیرندهٔ آن نخواهد ماند. اگر یک بستهٔ IP با خطا به مقصد برسد و یا اصلا به مقصد نرسد این پروتکل هیچ اطلاعی در مورد سرنوشت آن به فرستندهٔ بسته نمی‌دهد.

دلایل مختلفی برای نرسیدن یک بسته به مقصد وجود دارد: ممکن است "زمان حیات"[6] بسته قبل از رسیدن به مقصد منقضی شود؛ ممکن است مسیر یاب بسته را به مسیری اشتباه هدایت کند؛ ممکن است در هنگام قطعه قطعه کردن بسته و ارسال آن‌ها، یکی از قطعات دچار خطا شود یا به هر دلیلی به مقصد نرسد بنابراین کل دیتاگرام قابل بازسازی نخواهد بود؛ ممکن است مقصد بسته آمادگی

---

[1] از آن جهت امکان تجمیع این سه آدرس وجود داشته که بسته‌هایی که مقصدشان هر یک از این سه دانشگاه است باید بر روی خط خروجی یکسان بروند. ـ م

[2] Internet Control Message Protocol

[3] Connectionless

[4] Unreliable

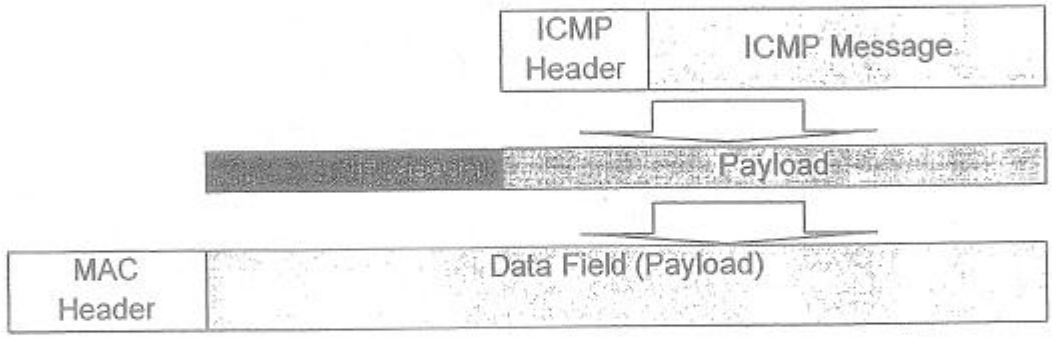
[5] Acknowledgement Message

[6] Time To Live

دریافت بسته را نداشته باشد یا اصلاً وجود خارجی نداشته باشد. در هنگام بروز هرگونه خطا، پروتکل IP به فرستندهٔ بسته هیچ اطلاعی در مورد سرنوشت آن نخواهد داد.

عدم گزارشِ خطا به تولید کنندهٔ یک بسته منجر به تکرار خطا و حمل بیهوده و زائد بسته‌هایی می‌شود که محکوم به فنا و حذف در شبکه هستند. به عنوان مثال عدم گزارش در مورد آماده نبودن مقصد برای دریافت بسته باعث خواهد شد که فرستندهٔ آن اقدام به ارسال بسته‌های دیگر کند در حالی که این کار بی ثمر خواهد بود و فقط بار ترافیک شبکه را افزایش می‌دهد و حتی می‌تواند منجر به بروز "ازدحام"[1] شود.

پروتکلICMP در کنار پروتکل IP، برای بررسی انواع خطا و ارسال پیام برای مبدأ بسته در هنگام بروز اشکالات ناخواسته استفاده می‌شود. در حقیقت ICMP یک سیستم گزارش خطا است که بر روی پروتکلIP نصب می‌شود تا در صورت بروز هرگونه خطا به فرستندهٔ بسته پیام مناسب را بدهد تا آن خطا تکرار نشود. در واقع ICMP وظیفه ای در قبال وقوع خطا ندارد بلکه فقط پیامی که بیانگر بروز خطا و نوع آن است به فرستنده برمیگرداند. این پروتکل اشکالات موجود را در قالب یکسری پیام گزارش می‌کند که این پیام خود در یک بسته IP قرار می‌گیرد که از جانب یک مسیریاب یا ماشین مقصد به آدرس فرستنده باز می‌گردد. در شکل ۴ چگونگی قرار گرفتن یک پیام ICMP درون یک بستهٔ IP تصویر شده است.

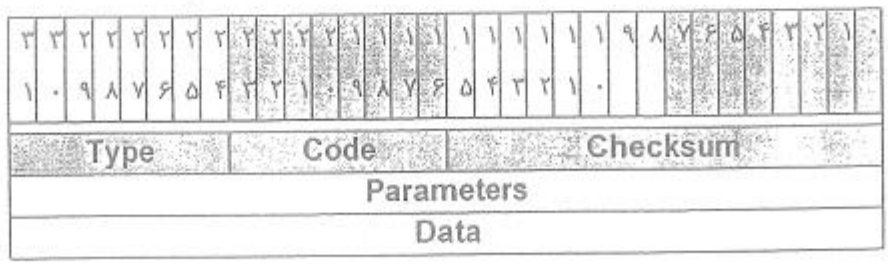


شکل ۴. چگونگی قرار گرفتن یک پیام ICMP درون یک بستهٔ IP

با توجه به آنکه پیام ICMP خود درون یک بسته IP جاسازی می‌شود بنابراین فیلدProtocol در سرآیند بستهٔ IP باید با شمارهٔ مشخصهٔ پروتکل ICMP (یعنی ۱) تنظیم شود.

دقّت کنید که خود بسته‌های ICMP نیز ممکن است دچار خطا شوند که برای این گونه خطا پیامی ارسال نخواهد شد .

شکل کلّی و قالب پیام ICMP در زیر مشخص شده است:



فیلد Type : در این فیلد عددی قرار می‌گیرد که بیانگر نوع پیام می‌باشد و ساختار فیلدهای Parameters و Data بسته به عددی که در این فیلد قرار می‌گیرد متفاوت خواهد بود.

فیلد Code : گاهی خود نوع پیام به چند زیر نوع دیگر تقسیم می‌شود که کد زیر نوع در این فیلد قرار می‌گیرد.

---

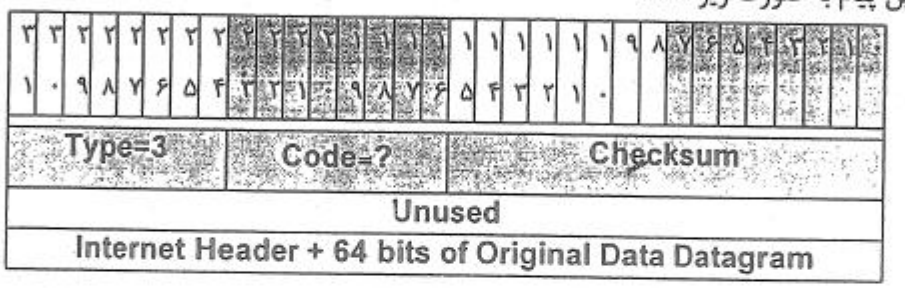
[1] Congestion

فیلد Checksum : محتوای این فیلد برای سنجش اعتبار و سلامت بستهٔ ICMP مورد استفاده قرار می‌گیرد. تمامی بستهٔ ICMP به‌صورت دوبایت دوبایت جمع شده و نهایتاً از مکمل ۱ حاصل جمع، عددی ۱۶ بیتی بدست می‌آید که درون این فیلد قرار می‌گیرد.

در ادامه نوع و ساختار پیام‌های ICMP را توضیح می‌دهیم:

پیام Destination Unreachable : این پیام زمانی صادر می‌شود که زیر شبکه یا یک مسیریاب نتواند آدرس مقصد را تشخیص بدهد یا به هر دلیلی بسته توسط ماشین میزبان تحویل گرفته نشود. (مثلاً بدلیل بزرگ بودن اندازهٔ بسته‌ها و عدم اجازه به مسیریاب برای شکستن آن.)

ساختار بستهٔ حامل این پیام به صورت زیر است:



معنای شماره‌های مختلف در فیلد Code به شرح زیر است:

0 : شبکهٔ مورد نظر در دسترس نمی‌باشد.

1 : ماشین میزبان مورد نظر در دسترس نمی‌باشد.

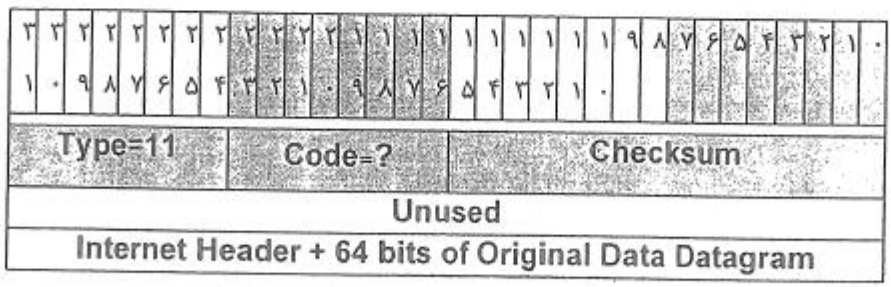
2 : پروتکل مورد نظر تعریف نشده است.

3 : شمارهٔ پورت مورد نظر وجود ندارد.

4 : اندازهٔ بسته بزرگ است و نیاز به شکستن دارد در حالی که اجازه داده نشده است.

پیام Time Exceeded : این پیام زمانی صادر می‌شود که مهلت قانونی یک بسته منقضی شده باشد و یک مسیریاب مجبور شود آنرا حذف کند؛ در چنین حالتی این پیام به آدرس فرستنده بسته IP برای آگاهی ارسال خواهد شد.

ساختار بستهٔ حامل این پیام به صورت زیر است:



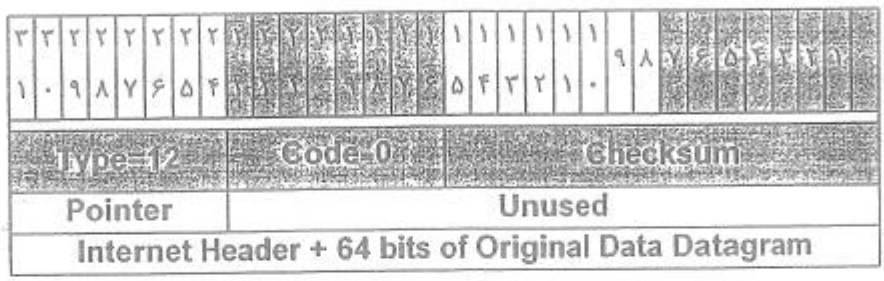
معنای شماره‌های مختلف در فیلد Code به شرح زیر است:

0 : زمان حیات بسته منقضی شده است. (این پیام معمولاً توسط مسیریاب صادر می‌شود.)

1 : زمان بازسازی قطعات یک دیتاگرام منقضی شده است. (این پیام توسط ماشین میزبان صادر می‌شود.)

پیام Parameter Problem : این پیام زمانی صادر خواهد شد که مقداری نامعتبر در یکی از فیلدهای سرآیند در بسته IP قرار گرفته باشد و مسیریاب قادر به تشخیص و تفسیر سرآیند آن بسته IP نباشد. به عنوان مثال در فیلد Version از بسته IP عدد ۵ قرار گرفته باشد و یا Checksum با سرآیند تناقض داشته باشد.

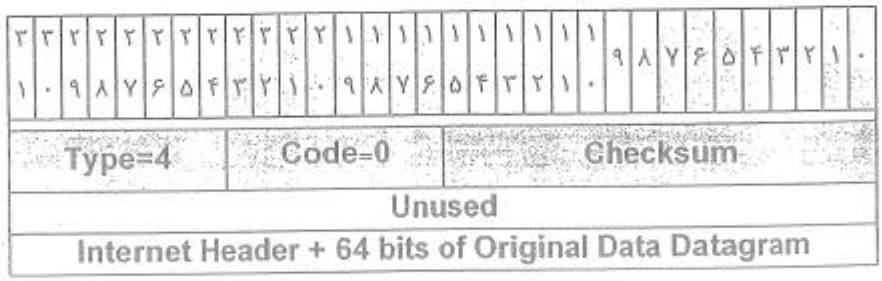
ساختار بستهٔ حامل این پیام به صورت زیر است:



فیلد Pointer محل بایتی را در بسته مشخص می‌کند که خطا در آن ناحیه بوده است.

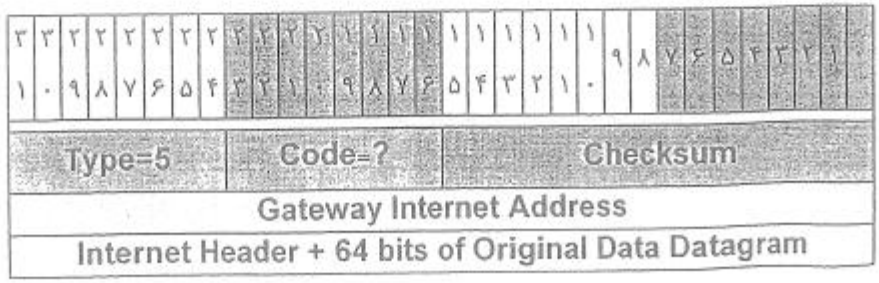
پیام Source Quench : این بسته زمانی برای یک ماشین میزبان ارسال می‌شود که از آن خواسته شود حجم ارسال بسته‌هایش را کاهش بدهد چرا که در غیر این‌صورت ازدحام پیش خواهد آمد. در مجموع هر گاه ازیک ماشین میزبان تقاضای کاهش نرخ تولید و ارسال بسته‌های IP را داشته باشد این پیام را صادر می‌نماید. اگر ماشین میزبان پس از طی مدت مشخصی این پیام را دریافت نکرد می‌تواند سرعت تولید بسته‌ها را به حالت اول برگرداند.

ساختار بستهٔ حامل این پیام به صورت زیر است:



پیام Redirect : این پیام زمانی صادر می‌شود که یک مسیریاب احساس کند بسته یا بسته‌هایی که برای او ارسال شده است در مسیر صحیح نیستند و احتمالاً اشکالی در مسیریابی وجود دارد. این پیام می‌تواند برای هشدار خطاهای احتمالی موثر باشد.

ساختار بستهٔ حامل این پیام به صورت زیر است:



معنای شماره‌های مختلف در فیلد Code به شرح زیر است:

0 : باید تغییر مسیر به شبکه ای که آدرس آن مشخص شده است انجام شود.

1 : باید تغییر مسیر به ماشینی که آدرس آن مشخص شده است انجام شود.

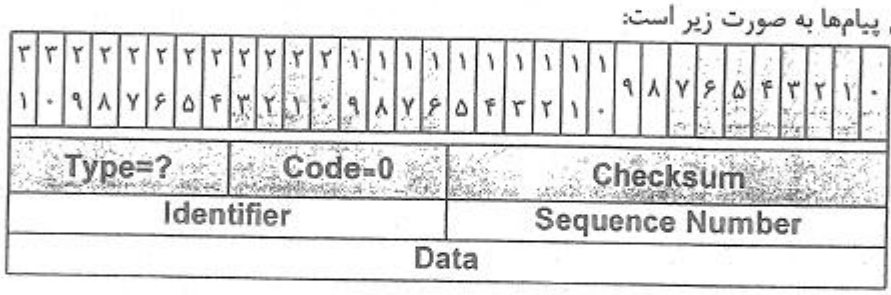
2 : برای برآورده شدن سرویس ویژهٔ درخواستی که در فیلد Type of service مشخص شده، باید تغییر مسیر به شبکه ای که آدرس آن مشخص شده است انجام شود.

3 : برای برآورده شدن سرویس ویژهٔ درخواستی که در فیلد Type of service مشخص شده، باید تغییر مسیر به ماشینی که آدرس آن مشخص شده است انجام شود.

فرض کنید به مسیریاب R1 بسته ای ارسال شده و او با بررسی جدول مسیریابی آنرا به مسیریاب R2 فرستاده تا او آنرا به مقصد X برساند .حال اگر R2 با مقایسهٔ الگوی زیرشبکه به این نتیجه رسید که خود او و فرستنده آن بسته در یک شبکه واقعند با ارسال این پیام به فرستنده اعلام میکند اگر از این به بعد بسته‌هایش به جای اینکه به R1 ارسال شود به R2 داده شود، زودتر به مقصد خواهد رسید؛ ضمناً آدرس IP خودش را نیز در فیلد Gateway Internet Address قرار می‌دهد .

پیام‌های Echo Request , Echo Reply : پیام Echo Request وقتی صادر می‌شود که یک مسیریاب بخواهد بداند آیا یک ماشین خاصّ شبکه قابل دسترس و موجود است یا خیر. در پاسخ به دریافت Echo Request، مقصد با ارسال پیام Echo Reply به آن پاسخ می‌دهد. با این پرسش و پاسخ، یک ماشین می‌تواند از قابل دسترس بودن یک مسیریاب یا ماشین میزبان در شبکه مطلع شود.

ساختار بستهٔ حامل این پیام‌ها به صورت زیر است:



معنای شماره‌های مختلف در فیلد Type به شرح زیر است:

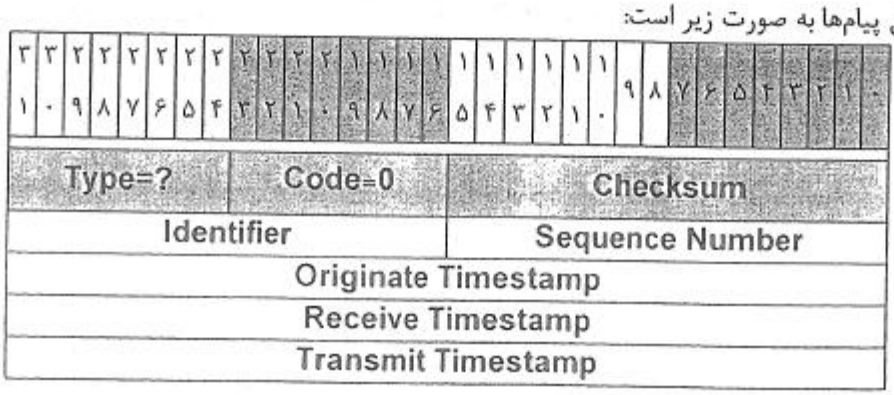
8 : برای مشخص کردن پیام Echo Request

0 : برای مشخص کردن پیام Echo Reply

ابتدا پیام Echo Request به سمت ماشین مقصد ارسال می‌شود و ماشینی که آنرا دریافت کند، آدرس‌های مبدا و مقصد را عوض کرده و شمارهٔ نوع آنرا از ۸ به صفر تغییر داده، پس از محاسبهٔ مجدد کد کشف خطا، آنرا برمیگرداند. فیلدهای Identifier و Sequence number برای پیشگیری از اشتباه در همخوانی و تطابق پیام‌های رفت و برگشتی است تا مبدأ بداند یک پاسخ مربوط به کدام تقاضای اوست.

پیام‌های Timestamp Reply وTimestamp Request : این دو پیام دقیقاً شبیه دو پیام تعریف شده در قبل هستند با این تفاوت که دریافت کنندهٔ آن، زمان دریافت و زمان ارسال بسته را نیز در پاسخ به آن اضافه خواهد کرد. بنابراین ارسال کننده پیام Timestamp Request پس از دریافت پاسخ نه تنها از قابل دسترس بودن مقصد باخبر می‌شود بلکه زمان رفت و برگشت یک بسته را نیز می‌تواند تخمین بزند و به کمک آن جداول مسیریابی و همچنین کارائی شبکه را اندازه گیری نماید.

ساختار بستهٔ حامل این پیام‌ها به صورت زیر است:



معنای شماره‌های مختلف در فیلد Type به شرح زیر است:

13 : برای مشخص کردن پیام Timestamp Request

14 : برای مشخص کردن پیام Timestamp Reply

Identifier & Sequence Number همانند پیام‌های قبلی برای پیشگیری از اشتباه در همخوانی و تطابق پیام‌های رفت و برگشتی است. Originate Timestamp زمانی است که مبدأ آن پیام را ارسال کرده است (زمان بر حسب میلی ثانیه گذشته از نیمه شب و بر اساس زمان جهانی گرینویچ است). Receive Timestamp زمانی است که گیرنده آن را دریافت کرده است و Transmit Timestamp زمان ارسال پاسخ بسته از طرف مقابل است. اگر زمان بر حسب میلی ثانیه آماده نبود بیت پرارزش از فیلد زمان یک می‌شود تا معلوم شود که آن فیلد معتبر نیست.

در پروتکل ICMP چهار پیام دیگر نیز وجود دارد، که با استفاده از آن‌ها یک ماشین میزبان می‌تواند آدرس IP شبکه محلی خود را در هنگامیکه چندین شبکه محلی از آدرس‌های IP مشترک استفاده می‌کند پیدا نماید.

۶-۹- پروتکل ARP[1]

نکته ظریفی که در مورد شبکه اینترنت وجود دارد آن است که اگر چه تمامی ماشین‌های میزبان و ابزارهای شبکه ای از آدرس IP که آدرس منحصر به فرد و یکتا است استفاده می‌کنند ولیکن یک بسته IP فقط در لایه شبکه قابل شناسائی و تحلیل است. یک بسته IP قبل از ارسال روی کانال از لایه اول یعنی لایهٔ فیزیکی عبور می‌کند و ضمن اضافه شدن اطلاعات لازم و تشکیل یک فریم، روی کانال فیزیکی ارسال می‌شود. بعبارت روشنتر بسته IP قبل از ارسال درون فیلد داده از فریمی قرار می‌گیرد که بعداً در لایهٔ اول تشکیل می‌شود؛ لایه و اول وظیفه ای در قبال مسیریابی و کارهایی از این قبیل ندارد و فقط با آدرس‌های فیزیکی کار می‌کند. به عنوان مثال اگر ماشین شما بخواهد بسته ای را برای ماشینی که روی شبکه محلی خودتان واقع است بفرستد، در لایه اول الزاماً بایستی آدرس فیزیکی ماشین شما (مبداء) و آدرس فیزیکی ماشین طرف مقابل (مقصد) معین باشد. (این آدرس‌ها به‌صورت سخت افزاری در کارت شبکه درج شده است) عدم دانستن آدرس‌های فیزیکی عملاً مساوی عدم توانایی برای ارتباط خواهد بود چرا که روی کانال انتقال آدرس‌های IP بی معنا هستند.

حال فرض کنید ماشین شما می‌خواهد بسته ای را برای ماشین دیگر ارسال کند که روی شبکه فعلی شما نیست، در این حالت هم لایه اول یک فریم برای ارسال روی کانال فیزیکی تشکیل می‌دهد و نیاز به آدرس MAC از مقصد دارد؛ آدرس فیزیکی مقصد چیست؟ در لایه اول هر گاه بسته ای قرار است به خارج از شبکه ارسال شود آدرس فیزیکی مقصد، آدرس مسیریاب پیش فرض شما خواهد بود. بنابراین آدرس‌های MAC مقوله ای جدا هستند و آدرس‌های IP مقوله ای دیگر.

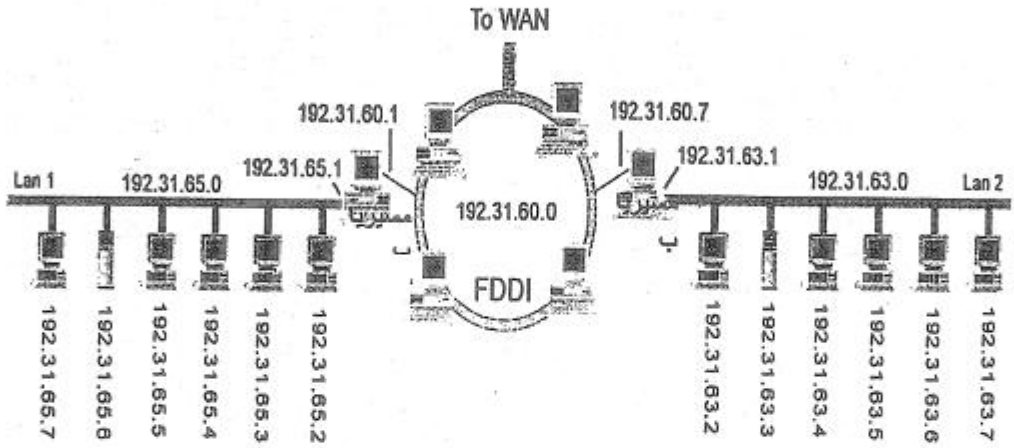
با مقدمه فوق به این نتیجه خواهیم رسید که هر ماشینی روی اینترنت گذشته از آن که بایستی آدرس‌های IP خودش و مقصدش را بشناسد و بداند، نیازمند به دانستن آدرس‌های فیزیکی ماشین‌هائی که مستقیماً با او در ارتباطند، می‌باشد. به عنوان مثال شبکه اترنت که در تمام دنیا شناخته شده است از آدرس‌هائی استفاده می‌کند که منحصر به فرد و ۴۸ بیتی (۶ بایتی) است. بنابراین کامپیوتری که به یک کارت اترنت مجهز است گذشته از آن که بایستی یک آدرس IP منحصر به فرد داشته باشد یقیناً دارای یک آدرس ۴۸ بیتی یکتاست که این آدرس یکتا در کارخانه سازندهٔ آن، تنظیم شده است. بنابراین وقتی پروتکل IP می‌خواهد یک بسته اطلاعاتی را روی شبکه بفرستد، باید به نحوی آدرس فیزیکی اولین ماشینی که با آن بایستی ارتباط برقرار کند را بداند؛ این ماشین می‌تواند مسیریاب پیش فرض او باشد یا می‌تواند آدرس فیزیکی مقصد روی همین شبکه محلی باشد.

---

[1] Address Resolution Protocol

حال فرض کنید ایستگاهی آدرس IP ماشینی را که میخواهد با آن ارتباط برقرار کند، می‌داند ولی آدرس فیزیکی او را نمی‌داند. چه کاری می‌تواند انجام بدهد؟ باید از پروتکل ARP بهره ببرد! در این پروتکل فرض بر آن است که تمامی ماشین‌های روی یک شبکه محلی آدرس IP خود را می‌دانند.

برای روشن شدن وظیفهٔ پروتکل ARP به شکل ۵ نگاه کنید. در مثال شکل ۵ فرض کنید سه شبکه در دانشگاه شما نصب شده است. شبکهٔ محلی اول در دانشکدهٔ کامپیوتر با آدرس کلاس C به شماره 192.31.65.0 و شبکهٔ دوم در دانشکده برق با آدرس کلاس C به شمارهٔ 192.31.63.0 نصب شده است. (هر دو شبکه از نوع اترنت هستند)



شکل ۵. شبکه بندی و آدرس دهی آن‌ها در یک دانشکده

این دو شبکه از طریق یک شبکه فیبر نوری با استاندارد FDDI و با آدرس IP شماره 192.31.60.0 به همدیگر متصل شده‌اند. هر ماشین در شبکهٔ اترنت یک آدرس ۴۸ بیتی یکتا دارد. مسیریاب‌ها در شکل مشخص شده‌اند و ارتباط دو شبکه اترنت را با FDDI برقرار می‌کنند. شبکهٔ FDDI از طریق یک خط اختصاصی به شبکهٔ جهانی اینترنت متصل شده است. هر مسیریاب به دو شبکهٔ متفاوت متصل شده و به عنوان عضوی از هر دو شبکه دارای دو آدرس IP مجزا می‌باشد، که هر یک از آن‌ها در یکی از شبکه‌های محلی تعریف شده است.

حال فرض کنید که ماشینی مایل است به آدرس خاصی مثلاً 192.31.65.5 بستهٔ IP بفرستد. در لایهٔ شبکه یک بستهٔ IP با مشخصات لازم ساخته می‌شود و در قسمت آدرس مقصد مقدار 192.31.65.5 قرار می‌گیرد. از دیدگاه لایه شبکه پس از تشکیل بستهٔ IP، کار تمام است و لیکن از دیدگاه لایه اول که بایستی آن بسته را روی کانال ارسال کند دانستن آدرس فیزیکی (آدرس MAC) ماشین مقصدی که آدرس IP آن 192.31.65.5 است، حیاتی است.

وظیفه پروتکل ARP در اینجا آن است که یک "بسته فراگیر"[1] روی کل شبکه محلی منتشر کند که این بسته در حقیقت سوال می‌کند:

" کسی که آدرس IP او 192.31.65.5 است، آدرس فیزیکی او چیست؟"

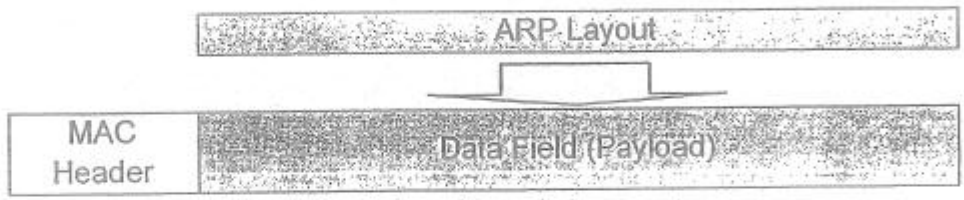
با توجه به آنکه بسته‌های فراگیر توسط تمامی ماشین‌های روی شبکهٔ محلی دریافت می‌شود، ماشینی که آدرس IP خودش را درون این بسته می‌بیند، بدان پاسخ می‌دهد و آدرس فیزیکی خود را برای ارسال کنندهٔ آن بسته می‌فرستد. پس از آنکه آدرس فیزیکیِ مقصد بدست آمد، یک فریم اترنت ساخته شده بر روی کانال منتقل می‌شود.

---

[1] Broadcast

به این نکته توجه داشته باشید که هر ماشین بر روی شبکهٔ محلی از پروتکل ARP حمایت می‌کند و این پروتکل عملیات پرسش و پاسخ را برای هر ماشین که تقاضای ارسال بستهٔ IP دارد، انجام می‌دهد.

بر خلاف پروتکل ICMP که روی پروتکل IP قرار می‌گیرد، پروتکل ARP مستقیماً بر روی پروتکل لایهٔ فیزیکی عمل میکند؛ یعنی یک بستهٔ ARP ساخته شده و درون فیلد داده از فریم لایهٔ فیزیکی قرار گرفته و روی کانال ارسال می‌شود. در شکل ۶ چگونگی ساخته شدن یک پیام ARP به تصویر کشیده شده است. در شکل ۷ ساختار درونی بستهٔ ARP تشریح شده است.



شکل ۶. چگونگی قرار گرفتن یک پیام ARP درون فریم لایهٔ فیزیکی

Hardware Type	
Protocol Type	
Hardware Address Length	Protocol Address Length
Operation Code	
Source Hardware Address	
Source IP Address	
Destination Hardware Address	
Destination IP Address	

شکل ۷. ساختار پیام‌های ARP

Hardware Type : شمارهٔ مشخصهٔ نوع سخت افزار کارت شبکه که در لایهٔ اول وظیفهٔ انتقال اطلاعات روی کانال فیزیکی را بر عهده دارد. این شماره‌ها در جدول ۱ مشخص شده‌اند.

Protocol Type : نوع پروتکلی که در لایهٔ دوم از آن استفاده می‌شود. برای شبکه‌های مبتنی بر TCP/IP این شماره ۲۰۴۸ است.

Hardware Address Length : با توجه به آنکه طول آدرس‌های فیزیکی در شبکه‌ها، متفاوت است در این فیلد طول آدرس (بر حسب بایت) مشخص می‌شود.

Protocol Address Length : طول آدرس‌های IP که در پروتکل TCP/IP مقدار ۴ است.

Operation Code (Opcode) : ۱ برای ARP request

۲ برای ARP reply

Source Hardware Address : آدرس فیزیکی مبدأ

Source IP Address : آدرس IP ماشین مبدأ

Destination Hardware Address : آدرس فیزیکی ماشین مقصد

Destination IP Address : آدرس IP ماشین مقصد

برای بالا بردن سرعت پروتکل ARP ، وقتی برای یکبار آدرس فیزیکی متناظر با آدرس IP از یک ایستگاه بدست آمد، پروتکل ARP این دو آدرس را در جدولی درون حافظهٔ اصلی که ARP Cache نامیده می‌شود ذخیره می‌کند تا اگر مجدداً به این آدرس نیاز شد به سرعت در اختیار قرار بگیرد. ساختار هر رکورد از این جدول به‌صورت زیر است:

IF Index	Physical Address	IP Address	Type

شماره نوع	عنوان سخت افزار کارت شبکه
1	Ethernet
2	Experimental Ethernet
3	X.25
4	Proteon ProNET (Token Ring)
5	Chaos
6	IEEE 802.X
7	ARCnet

جدول ۱. تعریف استاندارد سخت افزار کارت شبکه

IF Index : شماره پورت سخت افزاری متناظر با آن کارت شبکه

Physical Address : آدرس سخت افزاری کارت شبکه

IP Address : آدرس IP متناظر با آدرس سخت افزاری

Type : مقداری که در این فیلد قرار می‌گیرد وضعیت هر رکورد را در این جدول مشخص می‌کند: مقدار ۱ : یعنی این رکورد باید بطور متناوب به هنگام شود. دقت کنید که ARP Cache هر دقیقه یکبار "بهنگام سازی"[1] می‌شود. مقدار ۴: بدین معناست که این رکورد ثابت و بدون تغییر است و نباید بهنگام شود. مقدار ۱: یعنی رکورد چون بهنگام نشده از اعتبار ساقط است.

مسئله دیگری که ممکن است در هنگام بکارگیری پروتکل ARP رخ بدهد آن است که وقتی آدرس IP مربوط به ایستگاهی روی شبکه محلی سوال می‌شود، ممکن است آن ایستگاه روی شبکه محلی دیگری باشد و بالطبع پاسخی نمی‌رسد. در چنین حالتی دو راه حل وجود دارد:

الف : وقتی مسیریابی که به آن شبکه متصل است می‌بیند آدرس مقصدی که توسط ARP سوال شده روی یک شبکه محلی دیگر واقع است در پاسخ به آن، آدرس فیزیکی خودش را به ایستگاه سوال کننده ارسال می‌دارد؛ به این روش **Proxy ARP** گفته می‌شود.

ب: ایستگاهها خودشان موظفند به روشی که در مبحث "الگوی زیرشبکه" اشاره شد، مستقلاً محلی بودن یا خارجی بودن ماشین مقصد را تشخیص داده و در صورت خارجی بودن، آدرس فیزیکی یک مسیریاب مناسب را انتخاب نمایند.

نکته آخری که در مورد پروتکل ARP بایستی توضیح بدهیم آن است که در مسیریاب‌ها نیز برای شناسائی آدرس ایستگاه‌های یک شبکهٔ محلی متصل به آن‌ها به‌همین روش عمل می‌شود. برای جزئیات دقیقتر پروتکل ARP به REC-826 مراجعه کنید.

[1] Update

۷ـ۹ـ پروتکل RARP[1]

پروتکل ARP برای یافتن آدرس‌های فیزیکی ایستگاههایی است که آدرس IP خود را می‌دانند. پروتکل RARP دقیقاً عکس پروتکل ARP عمل می‌کند. گاهاً اتفاق می‌افتد که ایستگاه آدرس فیزیکی مورد نظرش را میداند ولیکن آدرس IP آنرا نمی‌داند؛ این قضیه برای ایستگاههائی که بدون دیسکند و از طریق سرویس دهنده بوت می‌شوند صادق است.

در این پروتکل برای شناسایی آدرس IP متناظر با یک آدرس فیزیکی یک بسته فراگیر روی خط ارسال می‌شود که در آن آدرس فیزیکی یک ایستگاه قرار دارد. تمامی‌ایستگاه‌هایی که از پروتکل RARP حمایت می‌کنند و بسته‌های مربوطه را تشخیص می‌دهند، در صورتی که آدرس فیزیکی خودشان را درون بسته ببینند در پاسخ به آن، آدرس IP خود را در قالب یک بستهٔ RARP Reply برمی‌گردانند. به عنوان مثال فرض کنید ایستگاهی با قرار دادن بستهٔ RARP و آدرس ۶ بایتی اترنت 14-04-D5-C8-01-25 روی خط، آدرس IP آنرا طلب می‌کند. هر ماشین که آدرس IP متناظر با آن را می‌داند به این بسته RARP پاسخ می‌دهد.

دقت کنید که بسته‌های RARP, ARP از نوع "فراگیر محلی"[2] هستند و بالطبع توسط مسیریاب‌ها منتقل نمی‌شوند و فقط در محدوده شبکه محلی عمل می‌کنند. (کلاً بسته‌هایی که درون فریم لایهٔ فیزیکی قرار می‌گیرند -کپسوله می‌شوند-، فقط قادرند در محدودهٔ شبکهٔ محلی به‌صورت فراگیر و همگانی ارسال شوند و این بسته‌ها توسط مسیریاب هدایت نخواهد شد.)

۸ـ۹ـ پروتکل BootP

با توجه به آنچه که در مورد RARP گفته شد بسته‌های سوال کننده آدرس IP از نوع محلی هستند و بالطبع این گونه بسته‌ها از مسیریاب‌ها به خارج از شبکه منتقل نخواهد شد.

گاهی نیاز است که یک آدرس IP روی چند شبکه محلی جستجو شود که در این حالت RARP جوابگو نیست. (این نیاز برای ایستگاه‌های بدون دیسک بوجود می‌آید چرا که پس از روشن شدن بایستی از طریق سرویس دهندهٔ شبکه[3] بوت شوند.)

پروتکل BOOTP در چنین محیطهایی کاربرد دارد و از دیتاگرام‌های نوع UDP که در آینده به آن‌ها خواهیم پرداخت، استفاده می‌کند و مسیریاب‌ها موظف به انتقال آن‌ها هستند. در این پروتکل نکته جالبی وجود دارد و آن هم آنست که در پاسخ به چنین بسته‌هائی به غیر از آدرس IP ایستگاه مورد نظر، اطلاعات لازم جهت بوت شدن سیستم و همچنین "الگوی زیرشبکه" برای ایستگاه تقاضا کننده که احتمالاً یک ایستگاه بدون دیسک است در قالب یک بستهٔ UDP ارسال خواهد شد.

---

[1] Reverse Address Resolution Protocol

[2] Local Broadcast

[3] Network Server

I) کل سوالات انتقال داده (گرایش معماری) سراسری ۸۳:

۱ ـ یک بسته داده از لایه بالاتر از لایه پیوند داده به 10 فریم تقسیم شده است و احتمال اینکه هر یک از فریم‌ها صحیح به مقصد برسد 80% است. اگر کنترل خطا در لایه پیوند داده صورت نگیرد، این بسته به طور متوسط چند بار باید ارسال شود تا صحیح به مقصد برسد؟

۱) 10 ۲) 9.31 ۳) 8.31 ۴) 7.31

۲ ـ (*) - یک بسته داده از لایه شبکه به 10 فریم تقسیم می‌شود و احتمال اینکه هر یک از فریم‌ها صحیح به مقصد برسد 0.8 است. اگر کنترل خطا در لایه پیوند داده صورت گیرد، هر فریم به طور متوسط چند بار باید ارسال شود تا صحیح به مقصد برسد؟ کل بسته به طور متوسط چند بار ارسال می‌گردد تا صحیح به مقصد برسد؟ (* : این سوال مربوط به آزمون سراسری نیست و برای درک بهتر سوال ۱ طرح شده است)

۱) هر فریم به طور متوسط 1.25 بار و کل بسته به طور متوسط 12.5 بار.

۲) هر فریم به طور متوسط 1.25 بار و کل بسته به طور متوسط 1.25 بار.

۳) هر فریم به طور متوسط 0.931 بار و کل بسته به طور متوسط 9.31 بار.

۴) هر فریم به طور متوسط 1.25 بار و کل بسته به طور متوسط 9.31 بار.

۳ ـ در یک سیستم انتقال داده از بیت توازن برای کشف خطا و سپس تقاضای ارسال مجدد استفاده می‌شود. اگر از فریم‌های تایید و یا تقاضای ارسال مجدد صرف نظر شود و تنها فریم‌های ارسال داده مدنظر باشد، کارآیی این سیستم در احتمال خطای 10% برای فریم‌های به طول ثابت 32 بایت چیست؟

۱) 99% ۲) 92.25% ۳) 90.5% ۴) 85%

۴ ـ پیغام 1110001101011110 از طریق یک کانال دریافت شده است. هر گاه کد استفاده شده دارای 5 بیت CRC و چند جمله‌ای مولد $g(x)=1+x^2+x^4+x^5$ باشد، کدام یک از موارد ذیل صحیح است؟

۱) خطا وجود ندارد.

۲) خطا وجود دارد و 1 بیتی است.

۳) خطا وجود دارد و 3 بیتی است.

۴) خطا وجود دارد ولی تعداد بیت‌های آن مشخص نیست.

۵ ـ در یک کد بلوکی خطی (LBC) از درجه (۴و۷)، برای پیغام ورودی $D=(d_1d_2d_3d_4)$ بیت‌های کنترل (Parity bits) از روابط زیر به دست می‌آید. هر گاه کلمه کد دریافتی در ورودی دیکدر به صورت $R=(1001001)$ باشد، کلمه کد ارسال شده چگونه بوده است؟ تنها امکان به وجود آمدن یک خطا را در نظر بگیرید.

$C_5 = d_1 \oplus d_2 \oplus d_3$

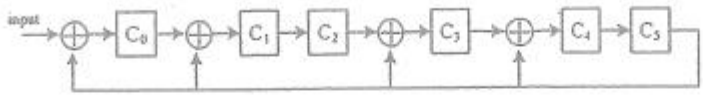
$C_6 = d_1 \oplus d_2 \oplus d_4$

$C_7 = d_1 \oplus d_3 \oplus d_4$

راهنمایی: منظور یک کد است که قابلیت تصحیح یک بیت خطا را دارد و درجه (۴و۷) به معنی $n=7$ و $m=4$ و $r=3$ است. محل بیت‌های داده و افزونه را شماره اندیس آن‌ها از چپ به راست در نظر بگیرید.

۱) 1001001 ۲) 1011001 ۳) 1101001 ۴) 1001101

۶ـ در یک سیستم تشخیص خطا به روش CRC از شیفت رجیستر مطابق شکل استفاده شده است. چند جمله‌ای مولد این CRC چیست؟



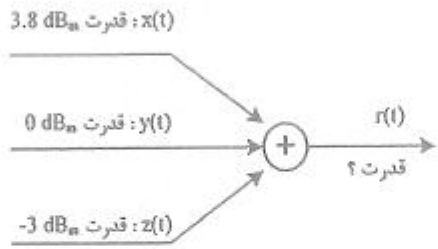
۱) $x^6 + x^4 + x^3 + x + 1$

۲) $x^5 + x^3 + x^2 + 1$

۳) $x^5 + x^3 + x^2 + x + 1$

۴) $x^6 + x^5 + x^3 + x^2 + 1$

۷ـ سه سیگنال تصادفی مستقل با مولفه dc صفر و قدرت $P_X = 3.8\ dB_m$ ، $P_Y = 0\ dB_m$ ، $P_Z = -3\ dB_m$ با یکدیگر جمع شده اند. قدرت سیگنال حاصل چقدر خواهد بود؟



۱) $0.8\ dB_m$

۲) $1.2\ mW$

۳) $5.54\ dB_m$

۴) $5.91\ dB_m$

II) کل سوالات انتقال داده (گرایش معماری) سراسری ۸۴:

۸ـ جهت انتقال اطلاعات از دو سیستم همزمان و غیر همزمان با مشخصات زیر استفاده شده است. نسبت راندمان سیستم همزمان به راندمان سیستم غیر همزمان چه مقدار خواهد شد؟

- در سیستم همزمان از فریم به طول ۱۵۰۰ بایت و سربار (overhead) به طول ۵۶ بیت استفاده شده.
- در سیستم غیر همزمان برای هر بایت اطلاعات از یک بیت شروع و یک بیت توقف استفاده شده است.

۱) 0.81 ۲) 1.25 ۳) 2.80 ۴) 5.6

۹ـ یک فرستنده دیجیتال، ابتدا از کدینگ منچستر (Manchester) و سپس از مدولاسیون ASK استفاده می کند. اگر $\frac{S}{N} = 15dB$ و $\frac{E_b}{N_0} = 18dB$ باشد، بهره کلی سیستم (نسبت نرخ ارسال بیت به پهنای باند یا $\frac{R}{B}$) چقدر خواهد بود؟

۱) 0.25 ۲) 0.5 ۳) 1 ۴) 2

۱۰ـ پهنای باند یک سیگنال صحبت 3 kHz است. اگر این سیگنال با نرخ نایکوئیست نمونه برداری شده و سپس با چندی کننده یکنواخت (uniform quantizer) با سیگنال به نویز 31.7 dB چندی شده باشد، نرخ انتقال داده این سیستم چقدر خواهد بود؟

۱) 48 bps ۲) 36 kbps ۳) 30 kbps ۴) 6 kbps

۱۱ـ در یک سیستم تکرار مجدد (ARQ)، فریم ها با طول ثابت ۱۲۰۰ بایت ارسال می‌شود. اگر ۱۶ بیت CRC به این فریم ها اضافه شود و احتمال خطای هر بیت 10^{-5} باشد، راندمان این سیستم چقدر خواهد بود؟

۱) 0.998 ۲) 0.98 ۳) 0.9 ۴) 0.79

۱۲ـ اگر چند جمله ای مولد یک کد کننده CRC، x^3+1 باشد خروجی این کد کننده به ازای ورودی 11011001 چه خواهد بود؟

۱) ۱۱۰۱۱۰۰۱۱۰۱ ۲) ۱۱۰۱۱۰۰۱۰۱۱ ۳) ۱۱۰۱۱۰۰۱۱۰۰ ۴) ۱۱۰۱۱۰۰۱۰۰۱

۱۳ ـ اگر در یک سیستم انتقال داده، توان سیگنال در فرستنده 20 dBm و توان نویز جمع شونده 6.67 mW و تضعیف خط انتقال 3 dB باشد، حداکثر سرعت انتقال بیت چقدر است؟ (فرض کنید پهنای باند خط 1.5 MHz می باشد.)

۱) 3 Mbps ۲) 4.5 Mbps ۳) 5.53 Mbps ۴) 6 Mbps

III) کل سوالات شبکه های کامپیوتری (گرایش IT) سراسری ۸۴:

۱۴ ـ در یک شبکه کامپیوتر، لایه پیوند داده ها خطاهای انتقال را با درخواست ارسال مجدد برای پیام های دریافتی خطادار مرتفع می نماید. فرض کنید احتمال دریافت یک پیام به صورت خطادار P باشد و درخواست ارسال مجدد بدون خطا دریافت گردد. تعداد متوسط ارسال یک پیام برای دریافت بدون خطای آن چقدر است؟

۱) $\frac{1}{1-P}$ ۲) $\frac{1}{1-P^2}$ ۳) $\frac{1}{1-2P}$ ۴) $\frac{1}{(1-P)^2}$

۱۵ ـ یک سیستم TDM آماری از ۸ کانال هر یک با پهنای باند 30 kbps استفاده می کند. اگر هر کانال در ۲۰ درصد موارد مشغول باشد پهنای باند خط برای بهره ۸۰٪ چقدر خواهد بود؟

۱) 48 kbps ۲) 60 kbps ۳) 128 kbps ۴) 240 kbps

۱۶ ـ فرض کنید صوت کد شده به صورت PCM با نرخ ۶۴ کیلو بیت در ثانیه درون سلول های ATM بسته بندی می‌شود. اگر نرخ ارسال داده ۱۵۵ مگابیت در ثانیه باشد، چند سلول می توان بین سلول های صوتی متوالی ارسال کرد؟ (طول هر سلول ATM، ۵۳ بایت می باشد که ۴۸ بایت آن داده و ۵ بایت آن سرآیند می باشد.)

۱) 5192 ۲) 4192 ۳) 3192 ۴) 2192

۱۷ ـ اگر مدل لایه ای دارای n لایه باشد و هر لایه h بیت سرآیند (header) به بسته دریافتی اضافه کند، برای رسیدن به بهره وری ۸۰٪ حداقل طول بسته داده ها بر حسب n و h چقدر باید باشد؟

۱) 8 nh ۲) 6 nh ۳) 4 nh ۴) 2 nh

۱۸ ـ یک کانال ارتباطی ISDN دارای نرخ ارسال داده ۱۲۸ کیلو بیت در ثانیه و تاخیر انتشار یک طرفه ۴۰ میلی ثانیه می باشد. با فرض اینکه طول فریم های Ack بسیار کوچک و قابل صرف نظر باشد. اگر از روش کنترل خطای Go-back N برای کنترل خطا استفاده کنیم و اندازه فریم ها ۱۲۸ بایت باشند، شماره ترتیب مورد نیاز چند بیت باید باشد تا جریان ارسال داده ها قطع نشود؟

۱) 3 بیت ۲) 4 بیت ۳) 5 بیت ۴) 6 بیت

۱۹ ـ کدامیک از عبارت های زیر در مورد مدل لایه ای شبکه های کامپیوتری های صحیح است؟

۱) هر چه تعداد لایه ها بیشتر شود، پیچیدگی طراحی کاهش می یابد.

۲) هر چه تعداد لایه ها بیشتر شود، سربارسیستم کاهش می یابد.

۳) هر چه تعداد لایه ها بیشتر شود، اعمال تغییرات پیچیده تر می‌شود.

۴ هر چه تعداد لایه ها بیشتر شود، پیاده سازی پیچیده تر می‌شود.

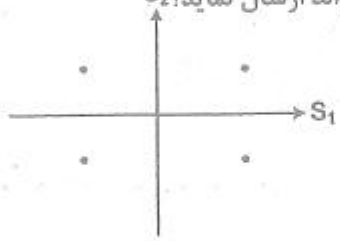
۲۰ ـ یک سیستم ساده تلفنی شامل دو مرکز محلی و یک مرکز راه دور است. مراکز محلی با خطوط یک مگا هرتز به مرکـز راه دور متصل اند. فرض کنید ۱۰درصد تلفن های انجام شده راه دورند و هر گفتگوی تلفنی دارای پهنای باند ۴ کیلوهرتز است. هر یک از مراکز محلی حداکثر چند گفتگوی تلفنی را می تواند در هر لحظه حمایت نماید؟

۱) ۲۵۰ گفتگوی تلفنی
۲) ۱۰۰۰ گفتگوی تلفنی
۳) ۲۵۰۰ گفتگوی تلفنی
۴) بیش از ۳۰۰۰ گفتگوی تلفنی

۲۱ ـ یک کانال تلویزیونی دیجیتال دارای پهنای باند ۶ مگا هرتز است. فرض کنید این کانال بدون نویز بوده و سیگنال های دیجیتال آن دارای ۱۲ سطح می باشند. چه نرخ داده ای به وسیله این کانال قابل ارسال است؟

۱) ۶ مگا بیت در ثانیه
۲) ۱۲ مگا بیت در ثانیه
۳) بیشتر از ۳۶ مگا بیت در ثانیه
۴) بیشتر از ۱۲ مگا بیت در ثانیه و کمتر از ۳۶ مگا بیت در ثانیه

۲۲ ـ یک کانال تلفنی دارای پهنای باند قابل استفاده از ۶۰۰ هرتز الی ۳۴۰۰ هرتز است. فرکانس حامل ۲۰۰۰ هرتز است. فرض کنید یک مودم QAM دارای دیاگرام روبرو باشد. این مودم چه نرخ داده ای را می تواند ارسال نماید؟



۱) کمتر از ۳۰۰۰ بیت در ثانیه
۲) بیشتر از ۴۰۰۰ بیت در ثانیه
۳) بیشتر از ۲۰۰۰ بیت در ثانیه ولی کمتر از ۴۰۰۰ بیت در ثانیه
۴) بیشتر از ۳۰۰۰ بیت در ثانیه ولی کمتر از ۵۰۰۰ بیت در ثانیه

۲۳ ـ یک کانال ارتباطی با پهنای باند ۱ مگا هرتز و نسبت سیگنال به نویز ۱۰۰ دی بی حداکثر چه نرخ داده ای را می توانـد ارسـال کند؟

۱) کمتر از ۲ مگا بیت در ثانیه
۲) بیشتر از ۱۰۰ مگا بیت در ثانیه
۳) بیشتر از ۴۰ مگا بیت در ثانیه ولی کمتر از ۱۰۰ مگا بیت در ثانیه
۴) بیشتر از ۲ مگا بیت در ثانیه ولی کمتر از ۴۰ مگا بیت در ثانیه

IV) ۴ سوال از ۷ سوال شبکه های کامپیوتری (گرایش IT) سراسری ۸۳:

۲۴ ـ برای اتصال یک کامپیوتر شخصی به یک کامپیوتر میزبان از یک مودم با نرخ ارسال داده ۵۶ کیلو بیت در ثانیه و تاخیر انتشار یک طرفه ۱۵۰ میلی ثانیه استفاده شده است. اگر اندازه فریم ها ۳۵۰ بایت و شماره ترتیب یک عدد سه بیتی باشد، با فرض اینکه اندازه فریم های Ack بسیار کوچک و قابل صرف نظر می باشد، نرخ ارسال داده موثر با استفاده از روش کنترل خطـا Go-back NARQ چقدر است؟

۱) ۱۲ کیلو بیت در ثانیه
۲) ۲۴ کیلو بیت در ثانیه
۳) ۳۶ کیلو بیت در ثانیه
۴) ۴۸ کیلو بیت در ثانیه

۲۵ ـ یک کانال ارتباطی با پهنای باند ۱ مگا هرتز و نسبت سیگنال به نویز ۱۰۰ دی بی (dB) حداکثر چه نرخ داده ای را می تواند ارسال کند؟

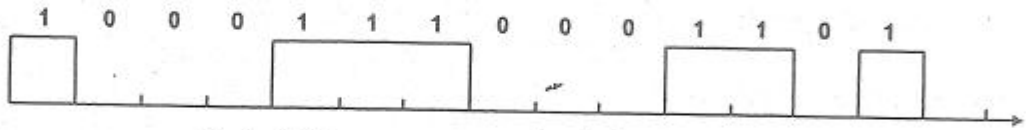
۱) بیشتر از ۱۰۰ مگا بیت در ثانیه

۲) کمتر از ۲ مگا بیت در ثانیه

۳) بیشتر از ۴۰ مگا بیت در ثانیه ولی کمتر از ۱۰۰ مگا بیت در ثانیه

۴) بیشتر از ۲ مگا بیت در ثانیه ولی کمتر از ۴۰ مگا بیت در ثانیه

۲۶ ـ شکل زیر نمایش یک سیگنال ۲ بایتی است که می بایستی از یک کانال با پهنای باند ۸۰۰۰ هرتز ارسال گردد. پهنای هر پالس (بیت) ۵۰ میکرو ثانیه است. حداکثر چند هارمونیک این سیگنال به وسیله این کانال قابل ارسال است؟



۱) ۲ هامونیک ۲) ۴ هامونیک ۳) ۶ هامونیک ۴) ۸ هامونیک

۲۷ ـ یک مودم که از روش QAM (Quadrature Amplitude Modulation) استفاده می کند دارای دیاگرام صورت فلکی در مختصات (۱،۱)، (۱،-۱)، (-۱،۱)، (-۱،-۱) می باشد. با استفاده از این مودم در روی یک خط با ظرفیت ۱۲۰۰ نمونه در ثانیه (band) چه سرعت داده ای را می توان ارسال نمود؟

۱) ۴۸۰۰ بیت در ثانیه ۲) ۲۴۰۰ بیت در ثانیه ۳) ۱۲۰۰ بیت در ثانیه ۴) ۶۰۰ بیت در ثانیه

پاسخ تشریحی سوالات آزمون های سراسری ۸۳ و ۸۴:

۱ ـ گزینه ۲ صحیح می‌باشد.

$P = (0.8)^{10}$ = احتمال درست رسیدن هر ۱۰ فریم = احتمال درست رسیدن پیغام

این یک آزمایش برنولی است که احتمال پیروزی P و احتمال شکست $q = 1 - P$ است. از طرفی تعداد تکرار آزمایش برنولی تا رسیدن به اولین پیروزی یک سری هندسی است.

متوسط تعداد تکرار آزمایش برنولی تا رسیدن به اولین پیروزی، همان متوسط سری هندسی است که آن را می‌دانیم:

$$\text{متوسط} = E(x) = \frac{1}{P} = (\frac{10}{8})^{10} = 9.31$$

نکته : این سؤال بیشتر متکی بر دانش آمار و احتمالِ شما است. تنها نکته‌ای که در مورد انتقال داده‌ها و شبکه های کامپیوتری دارد این است که اگر کنترل خطا در لایه پیوند داده انجام شود و یک فریم دارای خطا باشد، فقط همان فریم مجدداً ارسال می‌شود تا اینکه سالم دریافت شود. اما اگر کنترل خطا در لایه های بالاتر انجام شود، حتی اگر یک فریم دارای خطا باشد، کل بسته باید مجدداً ارسال شود، چون کد تشخیص خطا در سرآمد بسته قرار دارد.

۲ ـ گزینه ۲ صحیح می‌باشد.

در اینجا احتمال پیروزی (P) در آزمایش برنولی 0.8 است و چون کنترل خطا در لایه پیوند داده است، هر فریم بـه طـور مجـزا تکـرار می‌شود تا صحیح برسد. متوسط تعداد تکرار با توجه به سری هندسی عبارت است از:

$$E(x) = \text{متوسط تعداد تکرار یک فریم تا اینکه صحیح برسد} = \frac{1}{P} = \frac{1}{0.8} = 1.25$$

با توجه به اینکه برای هر فریم از بسته همین قضیه صادق است، کل بسته نیز به طور متوسط 1.25 بار تکرار می‌شود.

۳ ـ گزینه ۳ صحیح می‌باشد.

متاسفانه پاسخ صحیح این سؤال در میان گزینه ها وجود ندارد، اما نزدیک ترین پاسخ به پاسخ صحیح، جوابی اسـت کـه مـدنظر طـراح سؤال بوده است!

پاسخ صحیح:

$$\text{کارایی} = \text{سربار سیستم بدون خطا} \times \text{احتمال صحیح رسیدن فریم‌ها} = \frac{32 \times 8}{32 \times 8 + 1} \times (1 - 0.1) = \%89.6$$

گزینه ۳ به پاسخ صحیح نزدیک تر است.

پاسخ مدنظر طراح سؤال:

اگر صد پیغام ارسال شود، ده پیغام آن دارای خطا بوده و مجدداً ارسال می‌شود:

$$\text{کارایی} = \text{سربار سیستم بدون خطا} \times \frac{\text{تعداد}}{\text{تعداد}} = \frac{32 \times 8}{32 \times 8 + 1} \times \frac{100}{110} = \%90.5$$

اشتباه طراح سؤال در این است که خود پیغام‌های ارسال مجدد نیز ۱۰٪ احتمال خطا و تکـرار شـدن دارنـد و بنـابراین راه حـل اولـی صحیح است. در هر حال، باید گزینه سوم که به پاسخ صحیح نزدیک است را انتخاب کنید.

۴ ـ گزینه ۴ صحیح می‌باشد.

زیرا اگر چند جمله‌ای ارسالی را بر g(x) تقسیم کنید، باقیمانده مخالف صفر خواهد بود، پس خطا وجود دارد. اما در هر حال کد CRC تعداد بیت خطا یا محل وقوع خطا را مشخص نمی‌کند و فقط وقوع خطا را تشخیص می‌دهد.

۵ ـ گزینه ۲ صحیح می‌باشد.

d1	d2	d3	d4	C5	C6	C7
1	0	0	1	0	0	1

$$d_1 \oplus d_2 \oplus d_3 \oplus C_5 = 1 \oplus 0 \oplus 0 \oplus 0 = 1$$
$$d_1 \oplus d_2 \oplus d_4 \oplus C_6 = 1 \oplus 0 \oplus 1 \oplus 0 = 0$$
$$d_1 \oplus d_3 \oplus d_4 \oplus C_7 = 1 \oplus 0 \oplus 1 \oplus 1 = 1$$

چون اشتراک C5 و C7 که خطا را نشان می‌دهند، d1 و d3 است باید یکی از این دو بیت خراب شده باشند، اما اگر d1 خراب شود، C6 نیز خطا را آشکار می‌کند، پس d3 خراب است و کد ارسالی 1011001 بوده است.

۶ ـ گزینه ۱ صحیح می‌باشد.

به متن درس مراجعه کنید.

۷ ـ گزینه ۴ صحیح می‌باشد.

$$P_x(dB_m) = 10\log_{10} P_x(mW) = 3.8\,dB_m \Rightarrow P_x = 2.399\,mW$$
$$P_y(dB_m) = 10\log_{10} P_y(mW) = 0\,dB_m \Rightarrow P_y = 1\,mW$$
$$P_z(dB_m) = 10\log_{10} P_z(mW) = -3\,dB_m \Rightarrow P_z = 0.501\,mW$$
$$P_r = P_x + P_y + P_z = 2.399 + 1 + 0.501 = 3.9\,mW$$
$$P_r(dB_m) = 10\log_{10} 3.9(mW) = 5.91\,dB_m$$

۸ ـ گزینه ۲ صحیح می‌باشد.

$$\text{راندمان سیستم همزمان} = \frac{\text{طول قسمت مفید فریم}}{\text{طول فریم}} = \frac{\text{طول سربار فریم} - \text{طول فریم}}{\text{طول فریم}} = \frac{۱۵۰۰-۷}{۱۵۰۰} = \frac{۱۴۹۳}{۱۵۰۰} = ۰/۹۹۵$$

$$\text{راندمان سیستم غیرهمزمان} = \frac{\text{طول کاراکتر}}{\text{بیت پایان + بیت شروع + طول کاراکتر}} = \frac{۸}{۸+۱+۱} = ۰/۸$$

$$\frac{\text{راندمان سیستم همزمان}}{\text{راندمان سیستم غیرهمزمان}} = \frac{۰/۹۹۵}{۰/۸} = ۱/۲۴ \approx ۱/۲۵$$

۹ ـ گزینه ۲ صحیح می‌باشد.

توضیح: در این سؤال پهنای باند را که در جزوه با W نشان داده ایم با حرف B نشان میدهد.

نکته : چون منظور از E_b، انرژی یک بیت است، R همان bit rate است و منظور R_s نمی باشد. لذا فرمول زیر برای کدبندی منچستر نیز برقرار است. حال بدون توجه به عمل مدولاسیون می توان نوشت:

$$\frac{E_b}{N_0}(dB) = SNR(dB) + 10\log_{10}^{\frac{W}{R}} \Rightarrow 18\,dB = 15\,dB + 10\log_{10}^{\frac{W}{R}} \Rightarrow 10\log_{10}^{\frac{W}{R}} = 3\,dB \Rightarrow \frac{W}{R} = 1.995$$

$$\text{بهره کلی سیستم} = \frac{R}{W} = \frac{1}{1.995} = 0.501 \approx 0.5$$

متاسفانه، طراح گزینه یک را انتخاب کرده است. به نظر می رسد به علت کدبندی منچستر این بهره را نصف کرده است که نادرست است. چون در رابطه فوق E_b انرژی یک بیت کامل است.

۱۰ ـ گزینه ۳ صحیح می‌باشد.

$$SNR_{dB}(Quantization) = 20\log_{10}^{2^n} + 1.76 = 6.02n + 1.76 = 31.7 \Rightarrow n \approx 5$$
$$f_{high} = 3kHz \Rightarrow f_s = 2f_{high} = 6K\ sample/\sec. \Rightarrow R = f_s \times n = 30\ kbps$$

۱۱ ـ گزینه ۳ صحیح می‌باشد.

$$\text{احتمال خطای فریم} = P_f = L \times P_{bit} = [(1200 \times 8) + 16] \times 10^{-5} = 0.09616$$

$$\text{راندمان سیستم بدون خطا} \times \text{احتمال درست رسیدن فریم} = \text{راندمان سیستم} = (1 - P_f) \times \frac{1200 \times 8}{(1200 \times 8)16}$$

$$\text{راندمان سیستم} = 0.904 \times 0.998 = 0.902 \approx 0.9$$

۱۲ ـ گزینه ۴ صحیح می‌باشد.

$$G(x) = x^3 + 1 \Rightarrow r = 3$$

$$11011001000 \;\big|\; 1001$$

یا

$$\begin{array}{l} x^{10} + x^9 + x^7 + x^6 + x^3 \;\big|\; x^3 + 1 \\ \underline{x^{10} + x^7} \qquad\qquad x^7 + x^6 + 1 \\ \quad x^9 + x^6 + x^3 \\ \quad \underline{x^9 + x^6} \\ \qquad x^3 \\ \qquad \underline{x^3 + 1} \\ \qquad\quad 1 = R(x) \end{array}$$

$$\Rightarrow \text{کد ارسالی} = 11011001001$$

۱۳ ـ گزینه ۲ صحیح می‌باشد. (به صورت تقریبی)

$$P_T(dB) = 10\log_{10}^{P_T} = 20\,dB_m \Rightarrow P_T = 100\,mW$$
$$\text{تضعیف} = 3\,dB = 10\log_{10}^{\frac{P_T}{P_R}} \Rightarrow \log_{10}^{\frac{100}{P_R}} = 0.3 \Rightarrow P_R = 50.11\,mW$$
$$R_{max} = W\log_2^{1+\frac{S}{N}} = 1.5(MHz) \times \log_2^{1+\frac{50.11}{6.67}} = 1.5 \times 3.08 = 4.63 \approx 4.5\,Mbps$$

۱۴ ـ گزینه ۱ صحیح می‌باشد.

در اینجا یک آزمایش برنولی که احتمال شکست آن P و احتمال پیروزی آن 1-P است باید تکرار شود. تعداد تکرار آزمایش برنولی تا رسیدن به اولین پیروزی یک سری هندسی است که متوسط آن به صورت زیر است.

$$E(x) = \frac{1}{\text{احتمال پیروزی}} = \frac{1}{1\text{-}P}$$

۱۵ ـ گزینه ۲ صحیح می‌باشد.

در مالتی پلکس هوشمند (آماری، ناهنگام) پهنای باند (البته در اینجا منظور نرخ بیت است که به غلط پهنای باند نامیده شده است) تخصیص یافته به هر کانال کمتر از نرخ بیت حداکثر آن کانال است و برابر ظرفیت معادل آن کانال است که از پارامترهای آماری بدست می آید، زیرا ارسال داده ها به صورت ناهمگام بوده و نرخ بیت متغیر داریم. در اینجا حداکثر نرخ بیت هر کانال 30 kbps است که بطور متوسط ظرفیت معادلش برابر ۲۰ درصد این مقدار می باشد:

ظرفیت معادل هر کانال = ۰/۲۰ × ۳۰ kbps = ۶ kbps

مجموع ظرفیت معادل ۸ کانال = ۸ × ۶ = ۴۸ kbps

از آنجا که بهره خط ۸۰٪ است و ۲۰٪ آن هدر می رود میتوان نوشت:

ظرفیت خط × ۰/۸ = ۴۸ kbps

ظرفیت خط = ۶۰ kbps

۱۶ ـ گزینه ۴ صحیح می‌باشد.

$$\text{نرخ داده مورد نیاز برای انتقال صوت} = 64\,kbps \times \frac{53}{48} = 70.66\ kbps$$

ظرفیت خط = 155 Mbps

$$\frac{\text{ظرفیت خط}}{\text{نرخ داده مورد نیاز کانال صوتی}} = \frac{155\times 2^{20}}{70.66\times 2^{10}} = 2.193\times 2^{10} = 2246.03$$

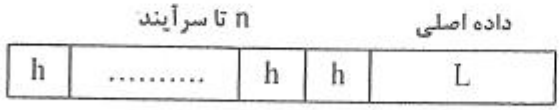
جواب صحیح این است که می توان ۲۲۴۶ صوت با این نرخ را از این کانال عبور داد. لذا به ازای هر سلول از یک کانال صوتی، ۲۲۴۵ سلول دیگر می توان ارسال کرد و سپس سلول صوتی بعدی از همین کانال را فرستاد.

اما اشتباه طراح سؤال دراین است که kbps را به جای 2^{10} برابر 10^3 فرض نموده است و آن را به صورت زیر حل کرده است:

$$\frac{155\times 10^6}{70.66\times 10^3} = 2.193\times 10^3 = 2193$$

در نتیجه بین دو سلول از یک کانال می توان 2192 سلول از کانال های دیگر ارسال کرد.

۱۷ ـ گزینه ۳ صحیح می‌باشد.



L= طول بسته داده اصلی

L+nh= طول بسته ارسالی

$$\text{راندمان (بهره وری)} = \frac{L}{L+nh}\times 100\% = 80\% \Rightarrow \frac{L}{L+nh} = \frac{8}{10} \Rightarrow 2L = 8nh \Rightarrow L = 4nh$$

۱۸ ـ گزینه ۲ صحیح می‌باشد.

$$\text{زمان انتقال یک فریم} = \frac{L}{R} = \frac{128\times 8}{128\times 2^{10}} = \frac{1}{2^7} = 7.81m\ \text{sec}$$

تاخیر انتشار دو طرفه = 2 * 40 = 80 m sec

$$\text{تعداد فریم قابل ارسال در مدت انتشار دو طرفه} = \frac{80}{7.81} = 10.24$$

می دانیم تعداد شماره ترتیب لازم در روش Go-back-N برابر W+1 است که W اندازه پنجره است، از انجا که در مدت زمانی که طول میکشد تا فریمAck مربوط به اولین فریم برگردد می توان بیش از ۱۰ فریم ارسال کرد. بنابراین باید حداقل اندازه پنجره ۱۲ (W=12) باشد و W+1=13 خواهد بود. بنابراین سه بیت کافی نیست زیرا حداکثر ۸ فریم را شماره گذاری می کند و به ۴ بیت نیاز داریم.

۱۹ ـ گزینه ۱ صحیح می‌باشد.

هر چه تعداد لایه ها بیشتر شود، از دیدگاه طراحی سیستم، Modularity بیشتر می‌شود و بنابراین طراحی سیستم ساده تر خواهد شد، زیرا وظایف هر لایه کمتر می‌شود و گزینه اول صحیح است. از طرفی پیاده سازی هر لایه نیز ساده تر خواهد شد و گزینه چهار غلط است. از طرفی چون هر لایه یک سرآیند (Header) به بسته ها اضافه می کند، با افزایش تعداد لایه سربار سرآیندها بیشتر می‌شود و گزینه دوم غلط است. همچنین با افزایش تعداد لایه و افزایش درجه Modularity و ساده تر شدن هر لایه، اعمال تغییرات جدید درسیستم راحت تر خواهد بود و گزینه سوم نیز نادرست است.

۲۰ ـ گزینه ۳ صحیح است.

$$\text{حداکثر تعداد تلفن راه دور هر مرکز محلی در هر لحظه} = \frac{\text{پهنای باند خط}}{\text{پهنای باند کانال صوتی}} = \frac{1MHz}{4KHz} = 250$$

حداکثر کل = ۱۰ × ۲۵۰ = ۲۵۰۰

مکالمات صوتی هر مرکز ← ۲۵۰ = (کل مکالمات صوتی یک مرکز تلفنی) × ٪۱۰

۲۱ ـ گزینه ۳ صحیح است.

طبق قانون نایکوییست :

$$R_{\max} = 2W\log_2^M = 2\times 6\times \log_2^{12} = 12\times 3.58 \approx 43\,Mbps$$

۲۲ ـ گزینه ۲ صحیح است.

$$W = 3400 - 600 = 2800$$

از انجا که فرکانس حامل دقیقاً وسط این کانال قرار دارد، کل پهنای باند فوق قابل استفاده است. از طرفی چون دیاگرام صور فلکی دارای چهار نقطه است و از مدولاسیون ۴ سطحی استفاده می کند (M = 4) :

$$W = R_s \Rightarrow R_s = 2800\ baud$$

$$R = R_s\log_2^M = R_s\log_2^4 = 2R_s = 5600bps$$

(با اینکه این سوال ۳ بار در آزمونها تکرار شده است ! اما فقط در سومین بار در پاسخنامه به طور اشتباه گزینه ۴ انتخاب شده است)

۲۳ ـ گزینه ۴ صحیح است.

طبق قانون شانون – هارتلی :

$$R_{\max} = W\log_2^{1+\frac{S}{N}}$$

$$SNR = 100dB = 10\log_{10}^{\frac{S}{N}} \Rightarrow \frac{S}{N} = 10^{10}$$

$$R_{\max} = 1MHz\times \log_2^{1+10^{10}} = 33.21\ Mbps$$

۲۴ ـ گزینه ۲ صحیح می‌باشد.

$$a = \frac{\text{تاخیر انتشار}}{\text{تاخیر انتقال}} = \frac{150ms}{\frac{L}{R}} = \frac{150\times10^{-3}}{\frac{350\times8}{56\times10^{3}}} = \frac{56\times150}{350\times8} = 3$$

از آنجا که روش Go-back-N است :

$$\text{حداکثر شماره ترتیب} = 2^3 = 8 = W+1 \Rightarrow W = 7$$

چون بحث احتمال خطا مطرح نیست:

$$u = \frac{W}{1+2a} = \frac{7}{1+2\times3} = 1$$

بنابراین پاسخ صحیح (56Kbps) وجود ندارد.

طراح سؤال گزینه دو (۲) را پاسخ صحیح اعلام کرده است و این در صورتی است که W را برابر ۳ فرض کنید که با توجه به ۳ بیتی بودن شماره ترتیب نادرست است.

۲۵ ـ گزینه ۴ صحیح است.

طبق قانون شانون – هارتلی :

$$R_{max} = W\log_2^{1+\frac{S}{N}}$$

$$SNR = 100dB = 10\log_{10}^{\frac{S}{N}} \Rightarrow \frac{S}{N} = 10^{10}$$

$$R_{max} = 1MHz\times\log_2^{1+10^{10}} = 33.21\ Mbps$$

۲۶ ـ گزینه ۳ صحیح است.

صورت سؤال سیگنال را ۲ بایتی فرض کرده و الگو ۱۴ بیتی است، اگر پریود را ۱۶ بیت فرض کنیم:

$$T_0 = 16\tau = 16*50\mu s = 800\mu s$$

$$f_0 = \frac{1}{T_0} = \frac{1}{800*10^{-6}} = 1250$$

از آنجا که سیگنال مربعی نیست هم هارمونیک های زوج و هم فرد دارا می باشد. از 8000 Hz، شش هارمونیک f_0 تا $6f_0$ عبور می کند.

اما چنانچه ۱۴ بیت را یک پریود در نظر بگیریم:

$$T_0 = 14\tau = 14*50\mu s = 700\mu s$$

$$f_0 = \frac{1}{700*10^{-6}} = 1428\ Hz$$

پنج هارمونیک f_0 تا $5f_0$ عبور می کند که جزو گزینه ها نیست.

۲۷ ـ گزینه ۲ صحیح است.

نمودار صور فلکی چهار نقطه دارد:

$$M = 4$$

$$R_s = 1200\ baud$$

$$R = R_s\log_2^M = 1200\log_2^4 = 2400\,bps$$

منابع

[1] Andrew S. Tanenbaum, Computer Networks, 4th Edition, Prentice Hall, 2003.

(ترجمه: دکتر حسین پدرام، مهندس احسان ملکیان، شبکه های کامپیوتری، انتشارات نص)

[2] William Stallings, Data and Computer Communications, 8th Edition, Prentice Hall, 2007.

[3] Fred Halsall, Data Communications, Computer Networks, and Open Systems, 4th Edition, Addison wesley.

[4] Behrouz A Forouzan, Data Communications and Networking, McGraw-Hill.

[5] احسان ملکیان ,"مهندسی اینترنت" انتشارات نص