مقدمه

به نام خداوندی که هستی از اوست

و ما هر چه داریم همه لطف اوست

جزوه حال حاضر حاصل تجربه سال‌های زیاد تدریس در درس شبکه و انتقال داده در دانشگاه‌ها و هم‌چنین کلاس‌های آمادگی برای کنکور کارشناسی ارشد می‌باشد.

در این جزوه سعی بر آن بوده تا مطالب اصلی، مهم و پرتکرار کنکور به صورت برجسته شده مطرح شود و از سردرگمی داوطلبان در انبوه کتب و جزوات جلوگیری کند.

برخلاف آنچه در مورد درس شبکه‌های کامپیوتری به نظر می‌رسد و در دانشگاه‌ها تدریس می‌شود، این درس می‌تواند علاوه بر مباحث تئوریک، در حل مسائل بسیار نیز چالش برانگیز باشد و جهت‌گیری سوالات این درس در چندین سال اخیر کنکور نیز موید این مهم می‌باشد.

در این جزوه ابتدا مقدمات شبکه‌های کامپیوتری و انتقال داده بررسی شده است. در ادامه در مورد آنالیز سیگنال‌ها و عوامل ایجاد خطا به صورت مفهومی بحث شده است. در فصل سوم کدگذاری و مدولاسیون موضوع صحبت واقع شده است. در سایر فصل‌ها کنترل خطا، زیرلایه کنترل دسترسی به رسانه انتقال لایه شبکه و پروتکل اینترنت موردبحث و بررسی قرار گرفته شده است.

در انتها نیز از هر مبحث یک یا چند نمونه از تست‌های مهم کنکور و تالیفی جهت درک بیشتر مفاهیم قرار داده شده است.

امید است که مجموعه حال حاضر مورد توجه شما دانش‌پژوهان و مشتاقان علم قرار گیرد و ختم کلام سخنی از خواجه شیراز:

گرچه راهی است پر از بیم ز ما تا بر دوست — رفتن آسان بود ار واقـف منزل باشـــی

چنگ در پرده همی می‌دهـــد پنـــــد ولـی — وعظت آن‌گاه کند سود که قابل باشی

به امید موفقیت

ابوالفضل طرقی حقیقت

در جدول ذیل دروس به سرفصلهای مهم آن طبقه بندی شده و مشخص شده است که در هر سال از هر مبحث چند تست سوال شده است و دانشجوی محترم می تواند زمان باقیماندهٔ خود را با توجه به اهمیت مباحث مدیریت نماید.

رشته: مهندسی فناوری اطلاعات درس: شبکه‌های کامپیوتری								
ردیف	مبحث	۱۳۸۵	۱۳۸۶	۱۳۸۷	۱۳۸۸	۱۳۸۹	مجموع ۵ سال	نسبت از کل
		تعداد تست	تعداد تست	تعداد تست	تعداد تست	تعداد تست		
1	مفاهیم بنیادی انتقال داده و شبکه	0	0	1	1	0	2	5%
2	آنالیز سیگنالها و عوامل ایجاد خطا	1	2	0	0	0	3	8%
3	استانداردهای واسط	0	0	0	0	0	0	0%
4	کدگذاری و مدولاسیون	0	0	1	2	1	4	10%
5	کنترل خطا	0	1	1	1	1	4	10%
6	کنترل جریان	0	1	1	0	2	4	10%
7	زیرلایه کنترل دسترسی به رسانه انتقال	0	1	1	2	1	5	13%
8	لایه شبکه	5	1	1	1	3	11	28%
9	پروتکل اینترنت	2	2	2	1	0	7	18%
جمع		**8**	**8**	**8**	**8**	**8**	**40**	**100%**

فصل اول

مقدمه‌ای بر انتقال داده‌ها و شبکه‌های کامپیوتری

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.

سیستم‌های باز (Open System) و مدل لایه‌ای

یکی از سبک‌های طراحی ماژولار (پیمانه‌ای) سیستم‌های بزرگ، سبک معماری لایه‌ای است. در این سبک یک سیستم‌های پیچیده به لایه‌هایی تقسیم می‌شود که هر لایه، وظایف مجزای خاص خودش را دارد و به لایه‌بالاتر از خود سرویس داده و از لایه پایین‌تر سرویس می‌گیرد. سرویس‌ها طبق یک واسط استاندارد خاص داده می‌شود. مثلاً وظایف فیزیکی سیستم‌های الکتریکی و مخابراتی در ارسال و دریافت امواج بر روی رسانه باید از وظایف سخت‌افزار کنترل خطا و جریان بر روی پیوند جدا شود و این دو لایه اصولاً از وظایف نرم‌افزارهای مسیریابی و آدرس‌دهی مجزا هستند تا طراحی به صورت مجزا و ساده‌تر صورت گیرد. این امر باعث پیاده‌سازی ساده‌تر، انعطاف بیشتر، نگهداری و عیب‌یابی آسان‌تر و اعمال تغییرات بهتر و سریع‌تر خواهد شد.

موسسه بین‌المللی استاندارد (ISO) یک استاندارد هفت‌لایه‌ای را بوجود آورد که محصولات همه شرکت‌ها بتوانند در لایه‌های مختلف ارتباطی به راحتی به یکدیگر متصل شوند و کار کنند. این استاندارد را اتصال سیستم باز (OSI: Open System Interconnection) گویند. در این استاندارد، هر لایه با لایه متناظر (Peer) خود بر اساس قوانینی به نام Protocol صحبت می‌کند و از سرویس لایه پایین‌تر استفاده می‌کند. به تفاوت بین مفهوم پروتکل و سرویس دقت نمائید. شکل ۱ لایه‌های این استاندارد (ISO/OSI) را نشان می‌دهند.

در مدل لایه‌ای، درخواست ارسال در مبدأ از لایه‌های بالا به سمت لایه‌های پایین جریان پیدا کرده و هر لایه از کاربرد تا پیوند داده، سرآیند (Header) خاص خود را به اطلاعات دریافتی از لایه بالاتر اضافه می‌کند. البته لایه پیوند داده، علاوه بر سرآیند، یک دنباله (Trailer) نیز به انتهای فریم اضافه می‌کند. لایه فیزیکی چیزی به فریم اضافه نمی‌کند. در مقصد همین داده‌ها لایه‌لایه بالا رفته و هر لایه

افزونگی‌های مخصوص خود را بر می‌دارد که این امر یادآور رفتار پشته است که در آن آخرین سرآیند گذاشته شده، اولین سرآیندی است که برداشته می‌شود. اصطلاح پشته پروتکلی (Protocol Stack) به همین دلیل استفاده می‌شود. بدیهی است هرچه تعداد لایه‌ها بیشتر شود، سربار افزونگی سرآیندهای پشته پروتکلی بیشتر می‌شود.

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 ارائه می‌کند)

وظایف: استانداردسازی موارد ذیل:

ـ شکل موج (پالسی ، سینوسی و غیره)

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

ـ دامنه (بر حسب ولت یا آمپر)

ـ عرض بیت (بر حسب µs)

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

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

ـ زمان‌بندی و سیگنالینگ (Timing، Handshake و غیره)

ـ 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 ارائه دهد)

وظائف:

ـ Framing: شناسایی ابتدا و انتهای فریم

ـ Flow Control: تطبیق سرعت فرستنده و گیرنده
- مشکل عدم آمادگی CPU به علت پردازش وقفه قبلی
- مشکل عدم فضای کافی در بافر

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

ـ 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)

وظائف:

ـ مسیریابی در شبکه (Network Routing)

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

ـ جلوگیری از ازدحام (Congestion Control)

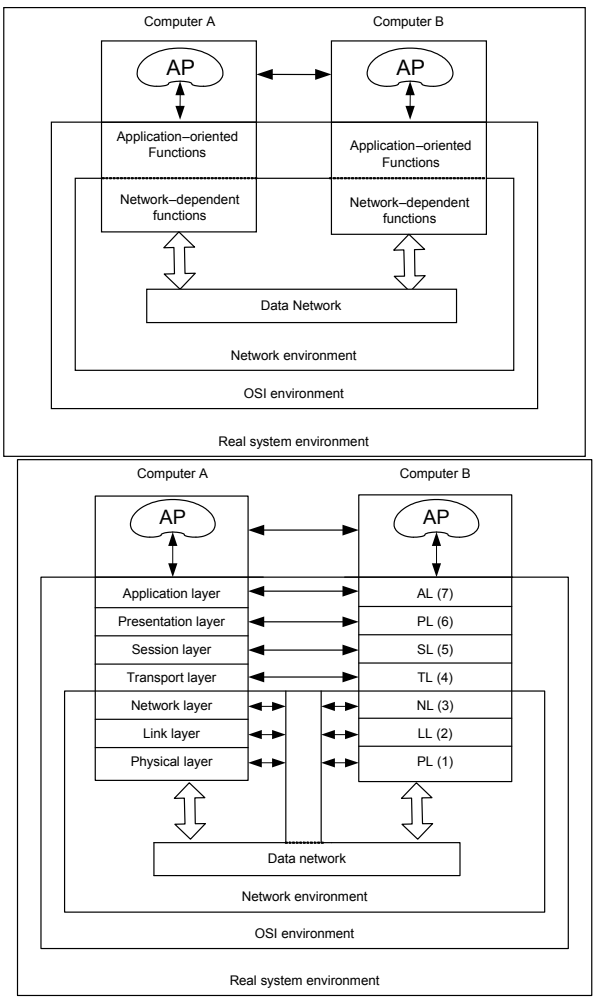
ـ Addressing (مثل IP Address)

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

ـ تطبیق پروتکل‌ها در ارتباطات بین شبکه‌ای (Internetworking)

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

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



شکل ۱. مدل استاندارد هفت‌لایه‌ای ISO/OSI

۴ـ Transport Layer (لایه حمل)

واحد انتقال داده: پیغام (Message)

هدف: انتقال داده End – to – End پیغام‌ها

وظائف:

ـ Connection Management

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

ـ Error Control

ـ Flow Control (تطبیق سرعت میزبان‌های سریع و کند)

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

ـ 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 ارائه)

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:

ـ Data Representation (نحوه بیان داده‌ها و Syntax داده‌ها)

ـ فشرده‌سازی و باز کردن کدها (Compression / Decompression)

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

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

۷ـ Application Layer (لایه کاربرد)

واحد انتقال داده: پیغام

هـدف: 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:

- File Transfer Access of Management: مدیریت ارسال فایل‌ها (مانند FTP)
- Document & Message Interchange : ارسال و دریافت پیغام‌ها و مدارک نظیر E.Mail (مانند SMTP)
- Job (process) Transfer & Manipulation: ارسال فرآیندها در شبکه و اجرای آن‌ها در ماشین‌های دور و به عبارت دیگر Remote login (مانند Telnet)
- تطبیق ترمینال‌های مختلف و متفاوت (Virtual Terminal)
- Direcoty Service: بانک‌های اطلاعاتی Name Server که برای شناسایی طرف مقابل به وسیله نام (به جای آدرس) به کار می‌روند (مانند DNS در اینترنت)
- تعیین این‌که آیا طرف مقابل ارتباط در حال حاضر در دسترس هست یا خیر
- واگذاری اختیارات (Authority) به طرف مقابل
- توافق بر سر مکانیزم‌های خصوصی‌سازی مثل رمزنگاری
- احراز هویت طرف مقابل (Authentication)
- توافق بر سر مسئولیت‌های ترمیم خطا
- شناسایی محدودیت‌ها بر روی Syntax های داده (ساختار داده، مجموعه کارکترها و غیره)

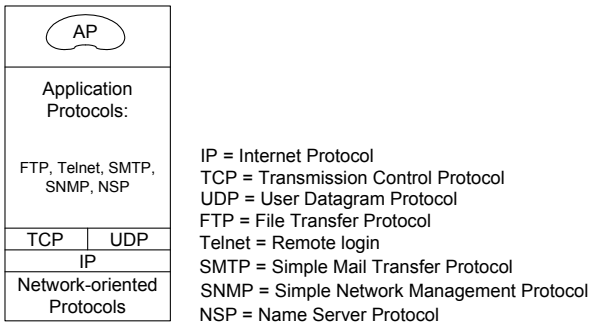
ارتباطات بین شبکه‌ای (Internetworking)

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 ۱ نشان می‌دهد که بسته به لایه‌های متفاوت دو شبکه از چه ابزارهایی برای اتصال آن‌ها استفاده می‌شود:

جدول ۱. ابزارهای ارتباط بین شبکه‌ای

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 ۲ 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.



شکل ۲. مدل لایه‌ای TCP/IP

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.

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.

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 یا CDMA: Code Division Multiple Access)

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 دربانده‌های 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.

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)

فصل دوم

آنالیز سیگنال‌ها و عوامل ایجاد خطا

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)

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

سری فوریه این سیگنال پریودیک به شکل مقابل نوشته می‌شود:

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

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

$$\begin{cases} a_0 = \frac{1}{T_0}\int_0^{T_0} V(t)\,dt \\ a_n = \frac{2}{T_0}\int_0^{T_0} V(t)\,\mathrm{Cosn}\omega_0 t\,dt \\ b_n = \frac{2}{T_0}\int_0^{T_0} V(t)\,\mathrm{Sinn}\omega_0 t\,dt \end{cases}$$

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: منظور از پهنای باند یک سیگنال پریودیک، محدودهٔ فرکانسی مؤلفه‌های آن است. فرض کنید یک سیگنال فقط مولفه‌های a_0 ، a_1 ، a_5 و a_9 را دارد و بقیه ضرایب a_n و b_n صفرند:

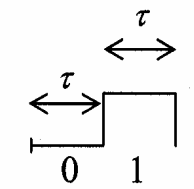
$$\text{Bandwidth} = f_{\text{High}} - f_{\text{Low}} = 9f_0 - 0 = 9f_0$$

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

نکته: منظور از پهنای باند محدود کانال چیست؟

اگر کانال را به صورت ایده‌آل و مستطیل شکل فرض کنیم، فاصله بین کمترین و بیشترین فرکانس‌هایی که از کانال عبور می‌کنند را پهنای باند کانال می‌گویند. معمولاً کانال‌ها تا یک فرکانس حداکثر را از خودشان عبور می‌دهند و اغلب کانال‌ها مثل یک فیلتر پائین‌گذر (Low Pass) عمل می‌کنند و بالاترین فرکانسی که بدون تضعیف از کانال عبور می‌کند را پهنای باند کانال‌های پایین‌گذر می‌نامیم (با فرض اینکه پایین‌ترین فرکانس عبوری صفر است).

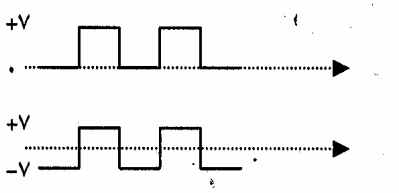
تعریف: سیگنال مربعی به یک سیگنال دیجیتال دو سطحی متناوب گفته می‌شود که عرض قسمت های بالا و پایین آن مساوی (τ) باشد. برای فهم بهتر مطلب، فعلاً فرض کنید که سمبول‌های بالا و پایین، هر کدام معرف یک بیت باشند (خواهید دید که الزاماً اینطور نیست) و بالا 1 و پایین 0 است.



به دو شکل تک‌قطبی و قطبی سیگنال‌های مربعی نگاه کنید:

1) Unipolar (تک قطبی)

2) Polar (قطبی)



سری فوریه سیگنال‌های مربعی تک قطبی و قطبی فوق به صورت زیر است:

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

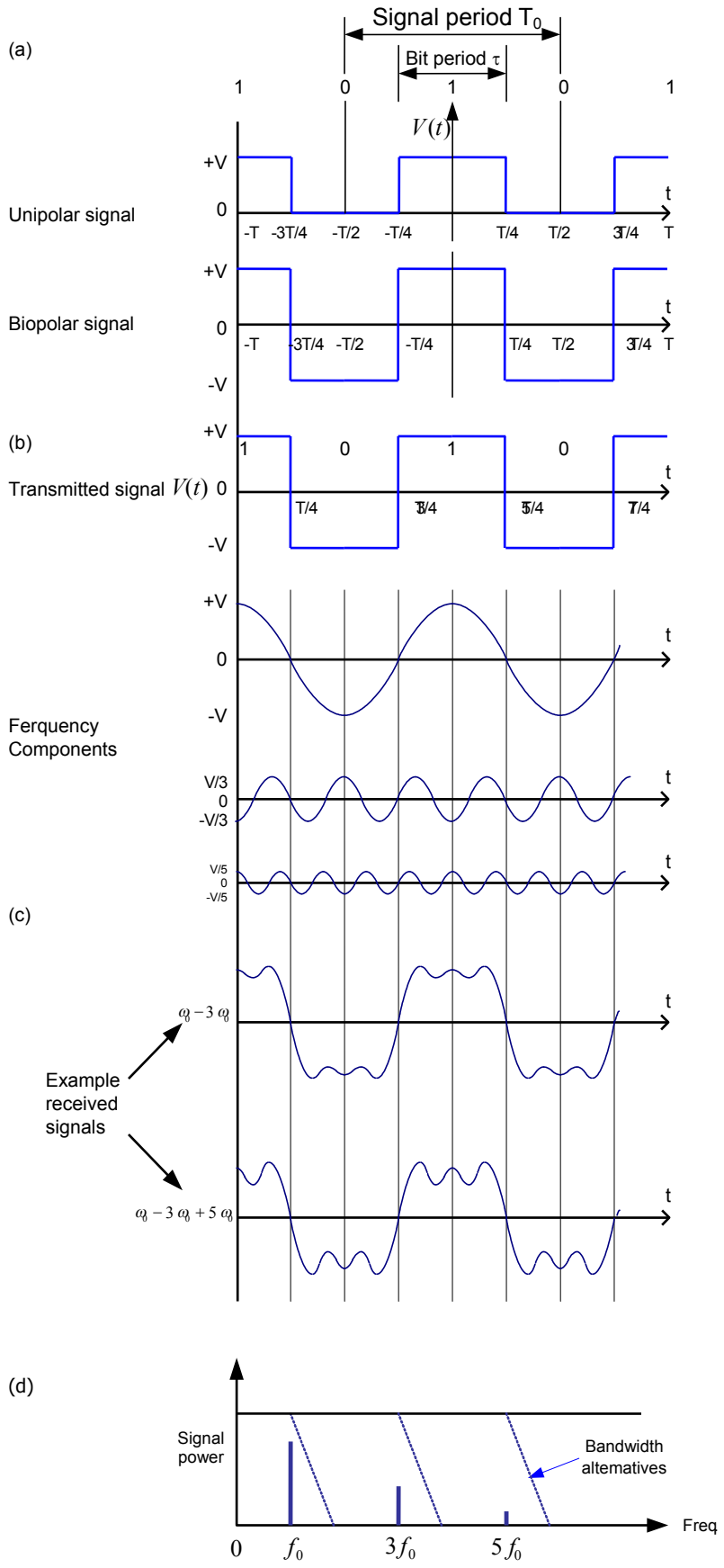
$$\text{Polar} \rightarrow V(t) = \frac{4V}{\pi}\left(\cos\omega_0 t - \frac{1}{3}\cos 3\omega_0 t + \frac{1}{5}\cos 5\omega_0 t - ....\right)$$

نکته: در سری فوریه سیگنال‌های مربعی، فقط هارمونیک‌های فرد $(f_0, 3f_0, 5f_0, ..)$ کسینوسی دیده می‌شوند.

نکته: در سری فوریه سیگنال‌های مربعی، ضرایب (دامنه‌های) هارمونیک‌های فرد $(f_0, 3f_0, 5f_0, ..)$ به صورت نمایی کاهش می‌یابند (با نسبت 1، $\frac{1}{3}$، $\frac{1}{5}$ و ...). بنابراین مهم‌ترین هارمونیک آن، هارمونیک اول است.

نکته: در سری فوریه سیگنال‌های مربعی، ضرایب هارمونیک‌ها، یک در میان، مثبت و منفی است.

به شکل ۳ نگاه کنید و ببینید که چگونه سه نکته فوق را در آن به تصویر کشیده‌ایم. در زیر سیگنال‌های مربعی با فرکانس f_0، هارمونیک‌های اول و سوم و پنجم سیگنال مربعی دیده می‌شوند که فرکانس آنها به ترتیب f_0 ، $3f_0$ و $5f_0$ بوده و دامنه‌های آنها به ترتیب با نسبت 1، $\frac{1}{3}$ و $\frac{1}{5}$ کاهش یافته و مثبت و منفی بودن یک درمیان ضرایب آنها نیز در شکل دیده می‌شود.



شکل ۳. 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)

در قسمت پایین (d) شکل ۳، کانال را به صورت یک فیلتر پایین‌گذر با سه پهنای باند مختلف مشاهده می‌کنید که در حالت اول فقط هارمونیک اول سیگنال را عبور می‌دهد و در حالت دوم، هارمونیک‌های اول و سوم و در حالت آخر، هارمونیک‌های اول و سوم و پنجم را عبور می‌دهد.

در حالت اول که پهنای باند کانال بزرگ‌تر یا مساوی f_0 و کوچک‌تر از $3f_0$ است فقط هارمونیک اول سیگنال از آن عبور می‌کند و در خروجی کانال سیگنال کسینوسی هارمونیک اول ظاهر خواهد شد. در حالت دوم که پهنای باند کانال بزرگ‌تر یا مساوی $3f_0$ و کوچک‌تر از $5f_0$ است فقط هارمونیک‌های اول و سوم سیگنال از آن عبور می‌کند و در خروجی کانال، مجموع سیگنال‌های کسینوسی هارمونیک‌های اول و سوم ظاهر خواهد شد که شکل آن در قسمت (c) شکل ۳ دیده می‌شود. همچنین در حالت سوم که پهنای باند کانال بزرگ‌تر یا مساوی $5f_0$ و کوچک‌تر از $7f_0$ است فقط هارمونیک‌های اول و سوم و پنجم سیگنال از آن عبور می‌کند و در خروجی کانال، مجموع این سه هارمونیک ظاهر خواهد شد که شکل آن نیز در قسمت (c) شکل ۳ دیده می‌شود.

نکته: برای تشخیص سمبول‌های یک سیگنال مبتنی بر سطح در مقصد، از وسط هر سمبول (مثلاً یک بیت) آن نمونه برداشته و سطح آن نمونه را اندازه‌گیری می‌کنند.

نکته: اگر از هارمونیک اول یک سیگنال مربعی و خود سیگنال مربعی با روش فوق نمونه بردارید مشاهده خواهید کرد که برای تشخیص یک سیگنال دیجیتال دو سطحی در مقصد، عبور هارمونیک اول آن کافی است. در واقع از وسط هر بیت یک نمونه‌برداری صورت می‌گیرد و 0 یا 1 بودن آن از هارمونیک f_0 قابل تشخیص است.

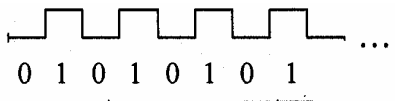
نکته: اگر بخواهیم یک سیگنال مربعی به صورت کاملاً مربعی از یک کانال عبور کند به پهنای باند بی‌نهایت نیاز داریم تا تمامی هارمونیک‌های آن از کانال عبور کنند.

نکته: برای محاسبه حداقل پهنای باند لازم برای عبور یک سیگنال از یک کانال، دو روش وجود دارد:

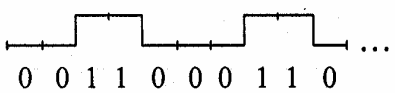
الف) اگر الگوی سیگنال داده شده است، سیگنال را به صورت تکرار آن الگو در نظر بگیرید.

ب) اگر الگوی سیگنال نامشخص است، سیگنال را به صورت ترتیب بدترین حالت (Worst Case Seequence) در نظر بگیرید. چون اگر یک کانال بتواند این سیگنال را عبور دهد، قطعاً سیگنال‌های دیجیتالی تصادفی که نرخ تغییر حالت پایین‌تری دارند را عبور خواهد داد.

مثال ۱: پریود سیگنال .Worst Case Seq مقابل برابر زمان ارسال الگوی 01 است

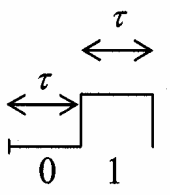


مثال ۲: در شکل مقابل پریود سیگنال برابر زمان ارسال الگوی 00110 است.



مثال ۳: اگر بخواهیم یک سیگنال مربعی دوسطحی را با نرخ 1000bps از یک کانال عبور دهیم، حداقل پهنای باند لازم چقدر است؟

پاسخ: چون الگوی سیگنال داده نشده است، سیگنال را به صورت ترتیب بدترین حالت، یعنی ...010101 در نظر می‌گیریم:



$$\tau = \frac{1}{R}, T_0 = 2\tau$$
$$f_0 = \frac{1}{T_0} = \frac{1}{2\tau} = \frac{R}{2} = \frac{1000}{2} = 500Hz$$

مثال ۴: اگر بخواهیم یک سیگنال مربعی دوسطحی به فرم ...0000111100001111 را با نرخ 1000bps از یک کانال عبور دهیم، حداقل پهنای باند لازم چقدر است؟

پاسخ: خود سیگنال متناوب و مربعی (با دوره تناوب 8τ) است:

$$\tau = \frac{1}{R}, T_0 = 8\tau$$
$$f_0 = \frac{1}{T_0} = \frac{1}{8\tau} = \frac{R}{8} = \frac{1000}{8} = 125Hz$$

مثال ۵: اگر بخواهیم یک سیگنال مربعی دوسطحی به فرم 01010011 را با نرخ 1000bps از یک کانال عبور دهیم، حداقل پهنای باند لازم چقدر است؟

پاسخ: چون الگوی سیگنال داده شده است، سیگنال را به صورت تکرار آن الگو (...0101001101010011) در نظر می‌گیریم:

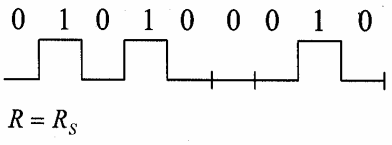
$$\tau = \frac{1}{R}, T_0 = 8\tau$$
$$f_0 = \frac{1}{T_0} = \frac{1}{8\tau} = \frac{R}{8} = \frac{1000}{8} = 125Hz$$

نرخ بیت و نرخ سیگنال

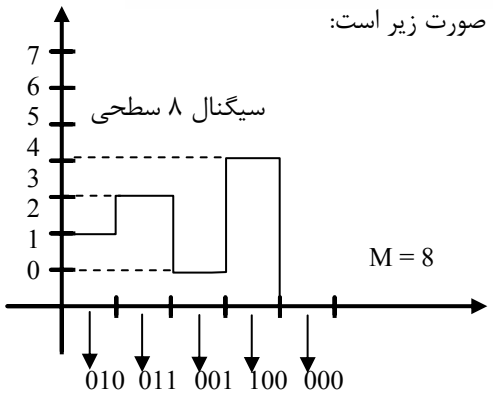
R: نرخ بیت (Bit Rate) : تعداد بیت‌های ارسالی در واحد زمان بر حسب بیت بر ثانیه (bps)

R_s : نرخ سیگنالینگ (Signaling Rate) یا (Baud Rate): تعداد سمبول‌های ارسالی در واحد زمان بر حسب baud یا سمبول بر ثانیه

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



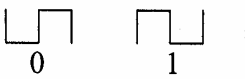
مثال ۲: برای سیگنال چند سطحی (مثلاً ۸ سطحی شکل زیر) رابطه بین R و R_s به صورت زیر است:



$R = R_s \log_2^M$ تعداد سطح سیگنال $\Rightarrow$ مثال ۲ $R = R_s \log_2^8 = 3R_s$

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

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 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 $bps\,Hz^{-1}$)

فرمول نایکوئیست (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

نویز (Noise)

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

SNR: Signal to Noise Ratio (به dB)

S: توان متوسط سیگنال (به W)

N: توان تصادفی نویز (به W)

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

برای محاسبه حداکثر نرخ انتقال کانال در حضور نویز دیگر نمی‌توان از رابطه نایکوئیست 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)

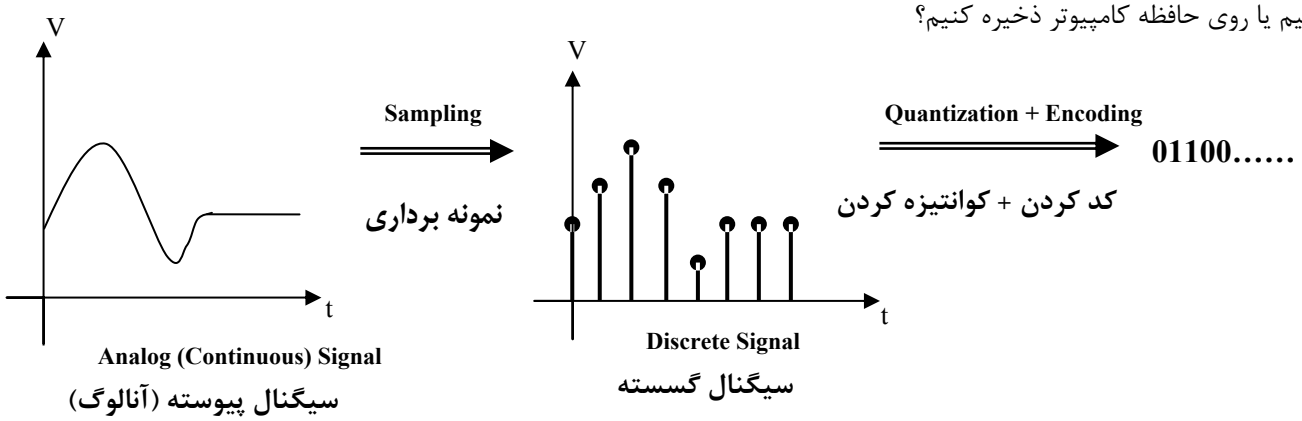
W: پهنای باند کانال (Hz)

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.

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 ۴. 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.

تئوری نایکوئیست (Nyquist)

اگر بالاترین فرکانس یک سیگنال آنالوگ برابر f_h باشد، فرکانس نمونه‌برداری باید حداقل برابر $2f_h$ باشد.

نکته: اگر فرکانس نمونه‌برداری کمتر از $2f_h$ باشد $(f_s < 2f_h)$ موجب روی هم افتادن مولفه‌های طیفی و اختلاط فرکانسی <Aliasing> می‌شود. از نظر تئوری نایکوئیست، نمونه‌برداری با فرکانس‌های بالاتر از $2f_h$ هیچ برتری بر فرکانس $2f_h$ ندارد و بیهوده است.

فصل سوم

Coding و Modulation (کدگذاری و مدولاسیون)

اهداف مدولاسیون 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 (شیفت فرکانسی)

مالتی‌پلکس فرکانسی (FDM)

- تغییر ماهیت سیگنال از دیجیتال به آنالوگ یا برعکس

مدولاسیون دیجیتال به آنالوگ

یک موج سینوسی حامل را در نظر بگیرید. مشخصات موج حامل عبارتند از:

مشخصه دامنه

مشخصه فرکانس

مشخصه فاز

با تغییر در یک یا چند مشخصه از موج حامل می‌توان داده‌های دیجیتال را سوار بر این موج حامل نمود (مدولاسیون). 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.

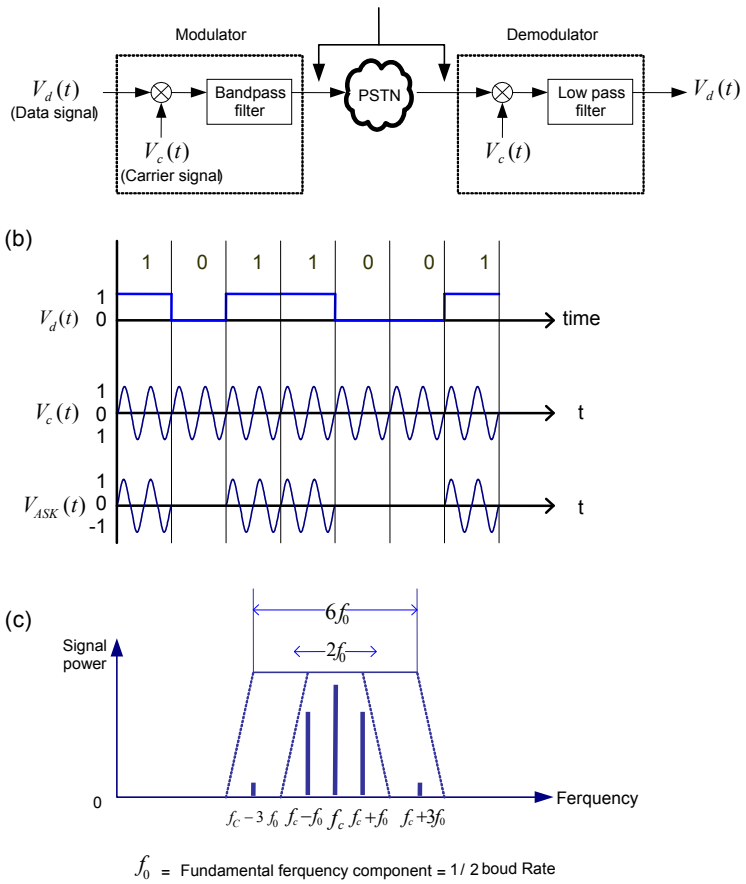
۱ـ۳ـ۴ ASK

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 ۵ عملکرد ASK را نشان می‌دهد.

همان‌طور که قبلا دیدیم $V_d(t)$ (سیگنال باینری که باید ارسال شود) در حالت worst Case Sequence بصورت 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 ۵. مدولاسیون ASK

نکته ۱: با توجه به شکل (b) ۵، Baud Rate سیگنال ASK برابر Bit Rate است و می‌توان نوشت:

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

مطابق شکل (a) ۵، 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: 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: 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 $\left[W = 2f_0 = R(bps) = R_S(baud)\right]$ در نظر می‌گیریم.

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:

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

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

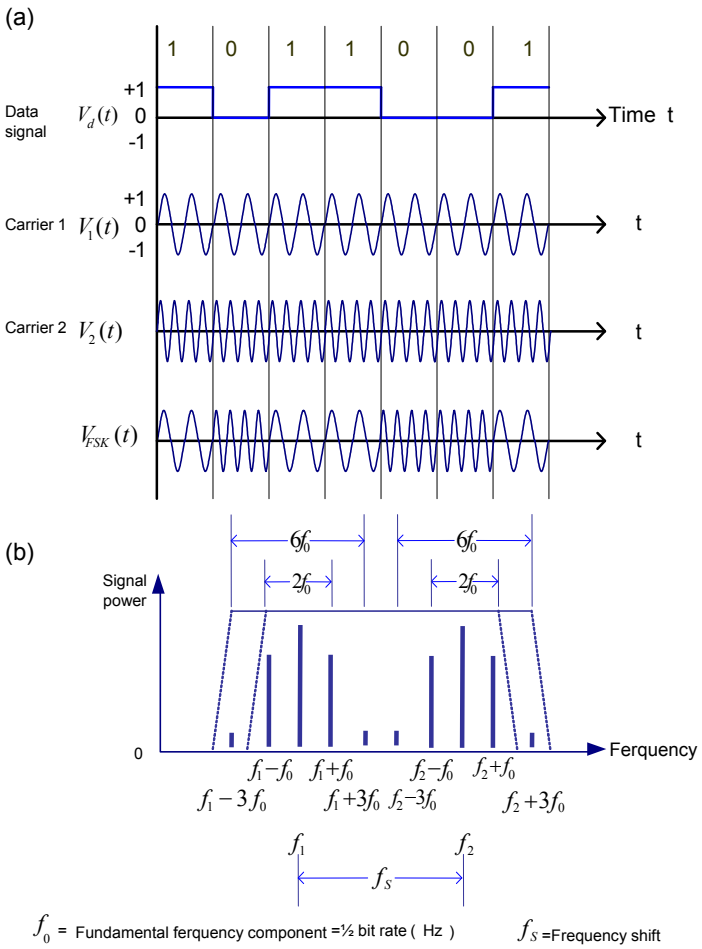
$$+\frac{1}{2}\cos\omega_2 t + \frac{1}{\pi}\left\{\cos(\omega_2 - \omega_0)t + \cos(\omega_2 + \omega_0)t - \frac{1}{3}\cos(\omega_2 - 3\omega_0)t - \frac{1}{3}\cos(\omega_2 + 3\omega_0)t + ...\right\}$$

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

نکته ۲: همان‌طور که در شکل (b)۶ 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 ریر استفاده می‌شود:

$$W = f_s + 2f_0 = f_s + R_s$$



شکل ۶. مدولاسیون FSK

۳ـ۳ـ۴ PSK

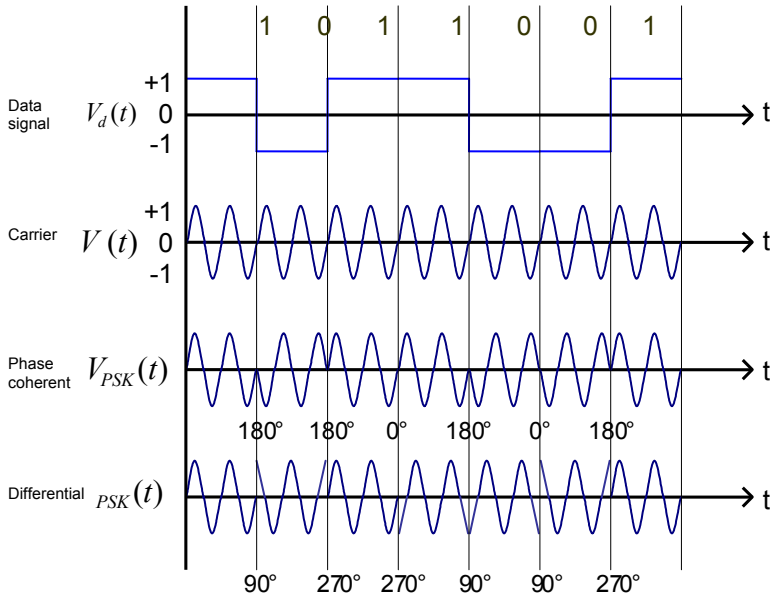
در این نوع مدولاسیون، دامنه و فرکانس ثابت است و 0 و 1 را با شیفت فاز نشان می‌دهند.

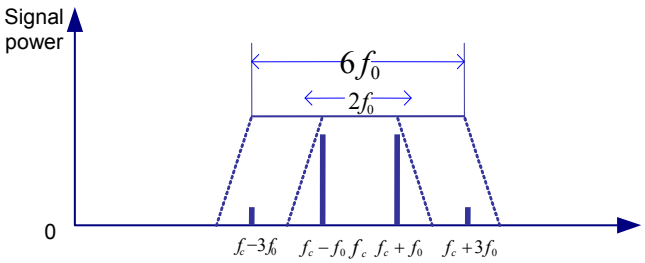
دو روش PSK وجود دارد.

Phase Coherent PSK
Differential PSK

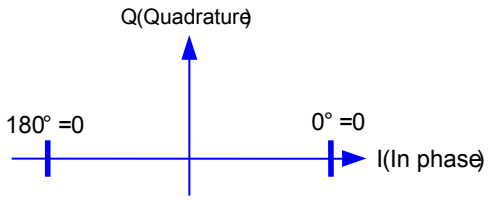
در روش اول، بین صفر و یک 180^0 اختلاف فاز وجود دارد. اشکال این روش این است که گیرنده برای تشخیص صفر و یک به سیگنال حامل مرجع نیاز دارد تا آن را با سیگنال دریافتی مقایسه کند.

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.





f_0 = Fundamental ferquency component =½ bit rate(Hz)



شکل ۷. مدولاسیون ـ PSK

نکته ۱: اگر فرض کنید که مطابق شکل ۷ (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: پهنای باند موردنیاز برای عبور کامل مولفه‌های (دو مولفه) f_0 برابر نرخ بیت است $[W=2f_0=R=R_S]$.

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]

مثلاً چهار تغییر فاز مختلف 0^0، 90^0، 180^0 و 270^0 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.

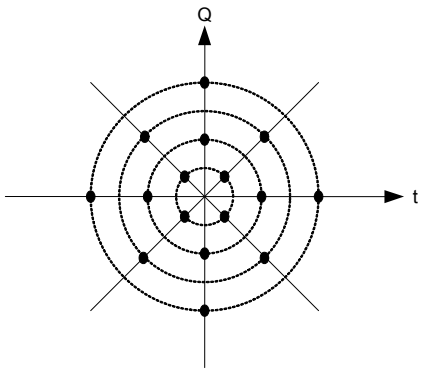
نکته مهم : برای افزایش نرخ بیت، پیشنهاد می‌شود که علاوه بر فاز ، دامنه سیگنال نیز تغییر نماید. این روش QAM نامیده می‌شود که در زیر شرح داده می‌شود.

روش QAM (Quadrature Amplitude Modulation)

دیاگرام فضایی شکل ۸ ,QAM را با 16 سطح سیگنال (هر baud معرف 4 بیت) نشان می‌دهد.

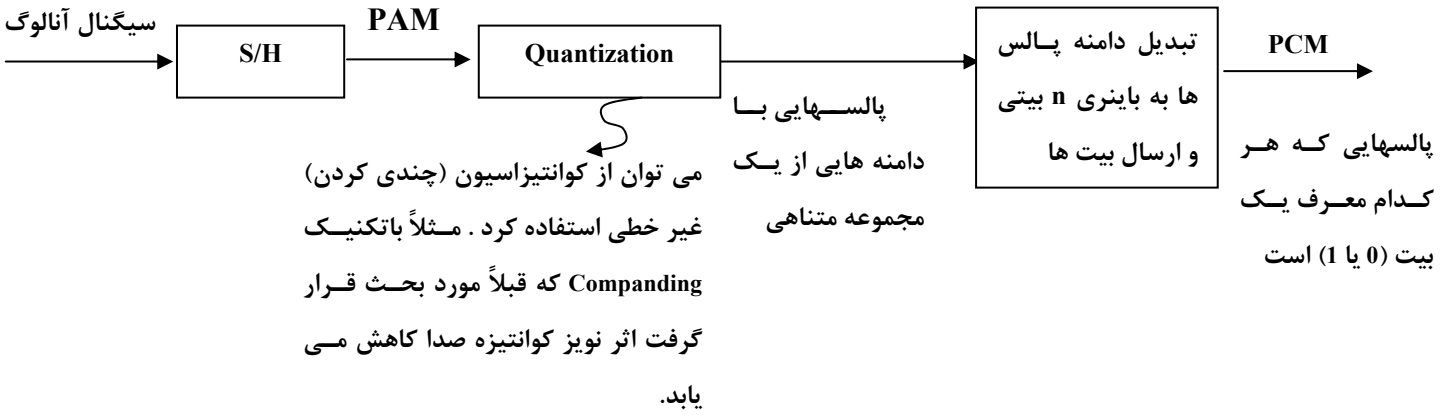
$$16-\text{QAM} \Rightarrow R = R_S \log_2^{16} = 4R_S \qquad (\text{Bit Rate} = 4 * \text{baud Rate})$$

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 ۸. مدولاسیون چند سطحی

مدولاسیون آنالوگ به دیجیتال به روش PCM (Pulse Code Modulation)



شکل۹. 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)]

فصل چهارم

کنترل خطا

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.

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 اعضاء مجموعه می‌باشد.

مثال : برای مجموعه کدهای $\{C_1, C_2, C_3\} = \{0011, 0001, 1100\}$، فاصله همینگ را محاسبه کنید.

$$D(C_1, C_2) = 1 \; , \quad D(C_1, C_3) = 4 \; , \quad D(C_2, C_3) = 3$$

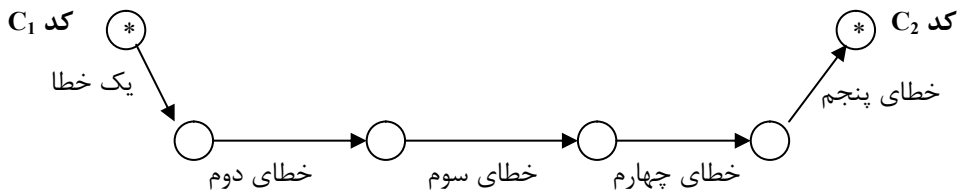
$$D = \text{Min}\{1, 3, 4\} = 1$$

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 ۱۰ 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 ۱۰ . 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:

$$d = D - 1$$

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

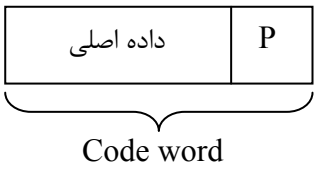
اگر یک یا دو خطا رخ دهد، کد غیر مجازی بوجود می‌آید که به کد مجاز اولیه از سایر کدهای مجاز نزدیکتر (D_{min}) است و علاوه بر تشخیص خطا، تصحیح نیز صورت می‌گیرد و کد اولیه به عنوان کد صحیح انتخاب می‌شود. اما اگر سه خطا رخ دهد، فاصله همینگ کد حاصل با یک کد مجاز دیگر، کمتر از فاصله همینگ آن با کد صحیح اولیه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

$$c = \left\lfloor \frac{D-1}{2} \right\rfloor$$

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: $c = \left\lfloor \frac{D-1}{2} \right\rfloor = \left\lfloor \frac{4-1}{2} \right\rfloor = 1$
- 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.

Parity Bit (بیت توازن)



- 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

Block Checksum

برای افزایش قدرت تشخیص خطا، علاوه بر بیت‌های توازن (مثلاً فرد در مثال زیر) که به ازاء هر کارکتر یک بیت توازن عرضی (سطری) [Transverse (Row) Parity Bits] ارسال می‌شود، یک مجموعه بیت توازن اضافی برای کل کارکترهای فریم نیز ارسال می‌گردد. در شکل ۱۱ 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
بیت های توازن (فرد) عرضی(سطری)	**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 (زوج) طولی(ستونی) یاBCC نیز می‌گویند.

شکل ۱۱ .روش LRC (بیت‌های مشخص شده با دایره نشاندهنده خطاهای غیر قابل تشخیص می‌باشند.)

نکته ۱: از آن‌جا که بیت‌های توازن طولی (ستونی) مانند جمع modulo-2 (مدول ۲) کل بیت‌ها عمل می‌کنند، به این مجموعه بیت‌های توازن ، BCC (Block Checksum 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 شکل۱۱) ، روش LRC (Longitudinal Redundancy Check) نامیده می‌شود.

نکته ۴: BCC می‌تواند انواع دیگری به غیر از جمع Modulo-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 ۱۱ با دایره مشخص شده‌اند دقت نمائید.

Hamming Code

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

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

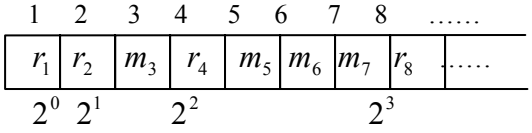
نکته : این قانون به کد همینگ ربطی ندارد و در مورد همه کدهای تصحیح خطا صادق است.

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

$$\boxed{2^r \ge 1 + \binom{n}{1} + \binom{n}{2} + ... + \binom{n}{t}}$$

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 ۱۲ 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 نمائید 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 ۱۲. 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.

Cyclic Redundancy Check : CRC

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 با جمع و تفریق‌های Modulo-2 استفاده 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.

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 نمائید (با خصوصیت تفریق Modulo-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:

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

تفریق Modula-2 مانند XOR

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 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 ۲: 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.)

روش‌های کنترل خطا

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 کارکتر قبلی رسیده است (به طور صحیح)یا خیر و نهایتاً یا داده بعدی را می‌فرستد و یا قبلی را دوباره ارسال می‌کند.

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 انتخـابی (Selective Reject) :** در ایـن 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 طـور صـحیح دریافـت شـده Ack شـماره‌دار می‌فرستد و فرستنده از روی شماره ترتیب Ack ها فریم دارای خطا را پیدا می‌کند (چـون 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

حتماً تا به حال این موضوع مهم پی برده‌اید که باید برای هر فریم شماره ترتیب (شماره شناسایی) در نظـر گرفتـه شـود، در ایـن صـورت مثلاً اگر در روش Idle RQ ، Ackگم شود (loss) و تایمر فرستنده به انتها برسد کند و frame دریافت شده قبلی را مجدداً ارسـال کنـد، 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 Idle RQ ، فقط کافی است که شماره‌ها یکی در میان 0 و 1 باشند.

فصل پنجم

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.

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.

کنترل نرم‌افزاری جریان

روش‌های کلاسیک مختلفی برای کنترل جریان به صورت نرم‌افزاری وجود دارد. مهم‌ترین روش‌های کنترل نرم‌افزاری جریان شامل روش X-ON / X-OFF، روش Stop & Wait (توقف و انتظار) و روش Sliding Window (پنجره لغزنده یا پنجره لغزان) است.

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 کارکتر (سیگنال) X-OFF به فرستنده می‌فرستد تا ارسال را متوقف نماید و با ارسال X- ON به فرستنده اعلام می‌نماید که آماده دریافت داده‌های جدید است و فرستنده می‌تواند شروع به ارسال داده‌ها نماید.

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:

$$U = \frac{\text{زمان مفید مصرف شده برای ارسال فریم داده در فرستنده}}{\text{زمان انتشار Ack + کل زمان لازم برای دریافت فریم از لحظه شروع ارسال}} = \frac{\text{زمان انتقال}}{\text{زمان انتشار + (زمان انتقال + زمان}} = \frac{\text{زمان انتقال}}{\text{(زمان انتشار × ۲) + زمان انتقال}} = \frac{1}{1+2\left(\frac{\text{زمان انتشار}}{\text{زمان انتقال}}\right)}$$

$$U_{S\&W} = \frac{T_f}{T_f + 2T_p} = \frac{1}{1+2\frac{T_p}{T_f}} = \frac{1}{1+2a} \quad , \quad a = \frac{T_p}{T_f} = \frac{\frac{D}{V}}{\frac{L}{R}}$$

که D طول کانال (فاصله بین فرستنده و گیرنده) بر حسب متر و V سرعت انتشار سیگنال در کانال (مضربی از سرعت نور) برحسب متر بر ثانیه و L طول فریم بر حسب بیت و R نرخ ارسال بیت‌ها بر حسب بیت بر ثانیه است.

نکته : عیب اساسی روش توقف و انتظار کارآیی و بهره پایین آن است.

نکته : در رابطه فوق از چهار پارامتر صرف نظر شده است:

۱) خطای فریم ۲) طول Ack ۳) زمان پردازش در فرستنده و گیرنده ۴) سربار Header و Trailer (Overhaed)

اگر 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:

$$U = \frac{1-P_f}{1+2a} \quad ; \quad P_f \text{ (تقریبی)} = L * P_{bit}$$

$$P_f \text{ (دقیق)} = 1-\left(1-P_{bit}\right)^L$$

اگرطول کل فریم (با احتساب سربارسرآیند) را با L یا n_a، طول Ack را با n_f و طول سربار سرآیند فریم را با n_O نشان دهیم و زمان پردازش در مبدأ و مقصد را یکسان و برابر T_{proc} فرض نماییم، راندمان کانال از رابطه زیر بدست می‌آید:

$$U_{S\&W} = \frac{\frac{n_f - n_O}{R} \times (1-P_f)}{T_{proc} + \frac{n_f}{R} + T_p + T_{proc} + \frac{n_a}{R} + T_p} = \frac{T_f \times (1-P_f) \times \frac{n_f - n_O}{n_f}}{T_f + T_a + 2T_p + 2T_{proc}} \quad , \quad T_f = \frac{n_f}{R} \quad , \quad T_a = \frac{n_a}{R} \quad , \quad T_p = \frac{D}{V} \quad , \quad P_f \cong n_f \times P_{bit}$$

روش Sliding Window (پنجره لغزان)

هدف اصلی این روش برطرف کردن مشکل پائین بودن بهره و کارآئی 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:

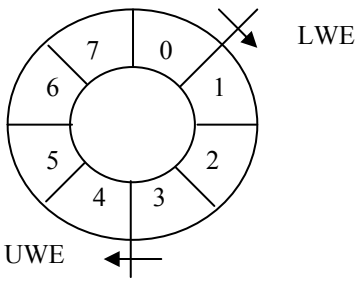
- پنجره گیرنده (پنجره دریافت) : فریم‌های دریافت شده که Ack آن‌ها ارسال نشده، پنجره گیرنده را مشخص می‌کند.
- پنجره فرستنده (پنجره ارسال) : فریم‌هایی که ارسال شده‌اند، بدون دریافت Ack از گیرنده، پنجره فرستنده را مشخص می‌کنند.

نکته ۴: فاکتورهای اندازه فریم، تاخیر انتشار خط ، نرخ بیت ارسالی و اندازه بافرها، حداکثر اندازه پنجره ارسال (W) را تعیین می‌کنند. به شکل ۱۳ 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 ۱۳. پنجره ارسال با اندازه W در پروتکل Go-Back-N

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.

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 $W \geq 1+2a \Rightarrow U = 1$ (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

$$\begin{cases} U = \dfrac{W(1-P_f)}{1+2a} \; ; \; W < 1+2a \\ U = 1-P_f \quad\quad ; \; W \geq 1+2a \end{cases}$$

• بهره یا راندمان پنجره لغزان در کانال دارای خطا با روش کنترل خطای Go-back-N از روابط زیر به دست می‌آید:

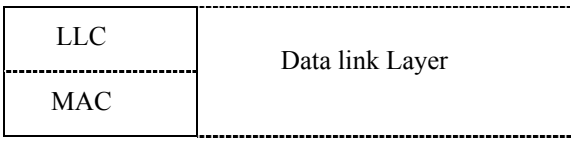
$$\begin{cases} U = \dfrac{1-P_f}{1+2aP_f} \quad\quad\quad\quad\quad ; \; W \geq 1+2a \\ U = \dfrac{W(1-P_f)}{(1+2a)(1-P_f+W*P_f)} \; ; \; W < 1+2a \end{cases}$$

فصل ششم

زیر لایه کنترل دسترسی به رسانه انتقال (MAC Sublayer)

برخی از شبکه‌های کامپیوتری دارای رسانه مشترک بوده 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 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.



MAC : Medium Access Control

LLC : Logical Link Control

انواع شبکه‌های دسترسی چندگانه

- **LAN**
  - (Ethernet) IEEE 802.3
  - (Token bus) IEEE 802.4
  - (Token ring) IEEE 802.5
  - FDDI Token ring
  - (Wireless LAN) IEEE 802.11
- **PAN**
  - (Blue tooth) IEEE 802.15
- **MAN**
  - IEEE 802.16
- **WAN**
  - Mobile Radio Networks

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.

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.

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 Gigabit Ethernet 10) 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.

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.

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)

۶) عدم اعتماد به شنود کانال به علت مشکلات ایستگاه مخفی و ایستگاه آشکار

۷) 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.

آنالیز کنترل دسترسی به کانال در پروتکل‌های مختلف MAC

نکته اصلی کنترل دستیابی به رسانه این 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 $\frac{1}{m}$ فرض شود تاخیر انتظار را در دو روش تخصیص ایستا و پویا با هم مقایسه کنید؟

الف) تخصیص پویا

میانگین زمان ارسال فریم (زمان سرویس) = $\frac{\frac{1}{m}}{R} = \frac{1}{mR}$

میانگین نرخ سرویس = mR

میانگین زمان انتظار یک فریم در صف $= T_{Dynamic} = \frac{1}{mR - \lambda}$

ب) تخصیص ایستا

در این حالت ما نرخ انتقال را بین N کامپیوتر تقسیم می‌کنیم (FDM)

متوسط نرخ ورود بسته از هر کامپیوتر $= \frac{\lambda}{N}$

میانگین زمان ارسال فریم (زمان سرویس) = $\frac{\frac{1}{m}}{\frac{R}{N}} = \frac{N}{mR}$

میانگین نرخ سرویس $= \frac{mR}{N}$

میانگین زمان انتظار یک فریم در صف $= T_{Dynamic} = \frac{1}{\frac{mR}{N} - \frac{\lambda}{N}} = \frac{N}{mR - \lambda}$

$\Rightarrow T_{Static} = N.T_{Dynamic}$

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.

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:

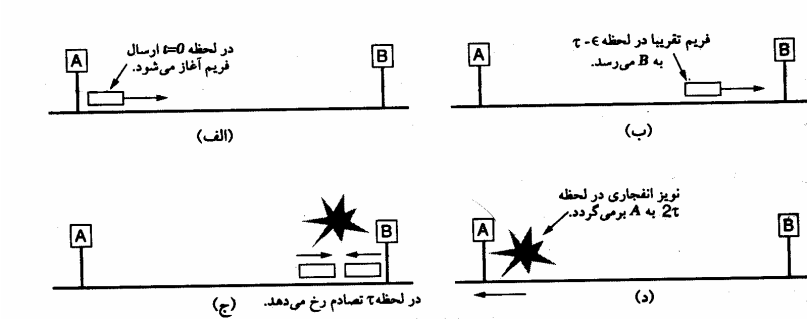
۱) فرض کنید که دو ایستگاه همزمان کانال (حامل) را شنود نمایند (Carreir Sense) و آن را مشغول یابند. اگر هر دو در ادامهٔ شنود برای ارسال اصرار ورزند (Persistant)، هر گاه خط آزاد شود مطمئناً دو ایستگاه همزمان فریم خود را بر روی خط گذاشته و تصادم رخ می‌دهد.

۲) 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 مـی‌شـود؟ پاسـخ 2τ است. بنابراین بازه تشخیص تصادم 2τ می‌باشد. این زمان را (Round Trip Time) یا RTT می‌نامند و در واقع زمـان رفـت و برگشـت سیگنال بر روی خط است.



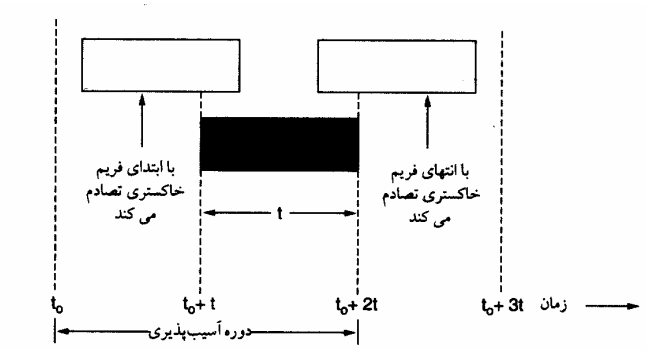
د) دو مدل زمانی برای ارسال فریم‌ها وجود دارد.

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 برابـر 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.)

ALOHA

قدیمی‌ترین پروتکل MAC مربوط به سال 1970 می‌شود که نورمن آبرانسون در دانشگاه هاوایی شبکه‌ای بـه نـام ALOHA طراحـی و پیاده‌سازی کرد که مبتنی بر پخش امواج رادیویی زمینی بود. در این روش فرستنده در هر زمان که بخواهد فریم خود را ارسال می‌کنـد 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 $= e^{-2G}$

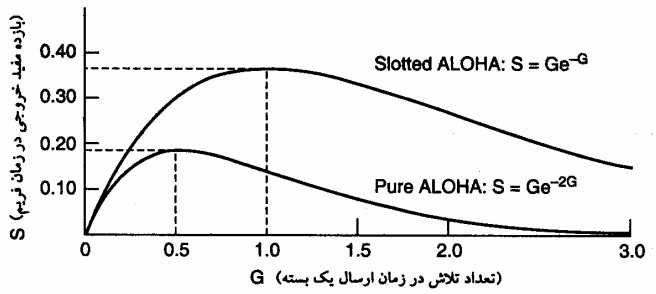
بنابراین بازده (راندمان) کانال در روش ALOHA از رابطه زیر بدست می‌آید:

$$\boxed{U_{ALOHA} = Ge^{-2G}}$$

همیشه راندمان کانال در Slotted ALOHA به صورت زیر خواهد بود:

$$\boxed{U_{Slotted\,ALOHA} = Ge^{-G}}$$

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.



(Carreir Sense Multiple Access) CSMA

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.

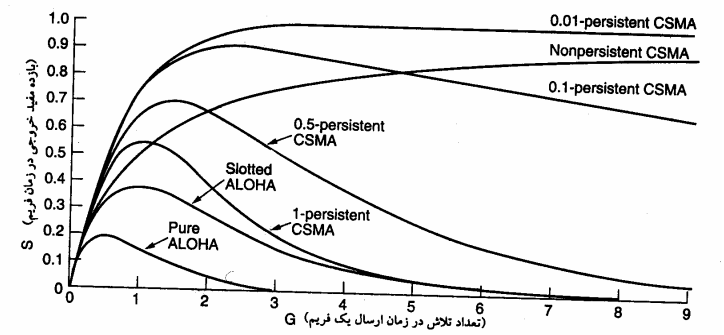
سه نوع پروتکل CSMA وجود دارد.

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.

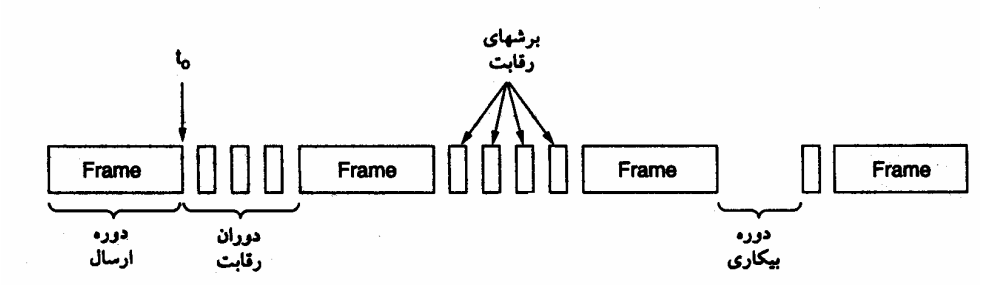


(Carreir Sense Multiple Access with Collision Detection) CSMA / CD

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.

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.

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 سوئیچ‌ها 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 سوئیچ یک یا چند Backplane وجود دارد که با تکنولوژی خاصی (که ربطی به اترنت ندارد) کار می‌کند و پورت‌های ورودی سوئیچ را با سرعت چند گیگابیت در ثانیه به هم متصل می‌کنند. در سوئیچ‌ها عمل Forwarding داریم.

۲) سوئیچ‌ها قابلیت بافر کردن فریم‌ها را در حافظه درون سوئیچ دارند. بدین ترتیب در درون سوئیچ تصادم رخ نمی‌دهد، لذا سوئیچ حوزه تصادم نیست.

نکته : حوزه تصادم در Hub خود Hub و در سوئیچ پورت است.

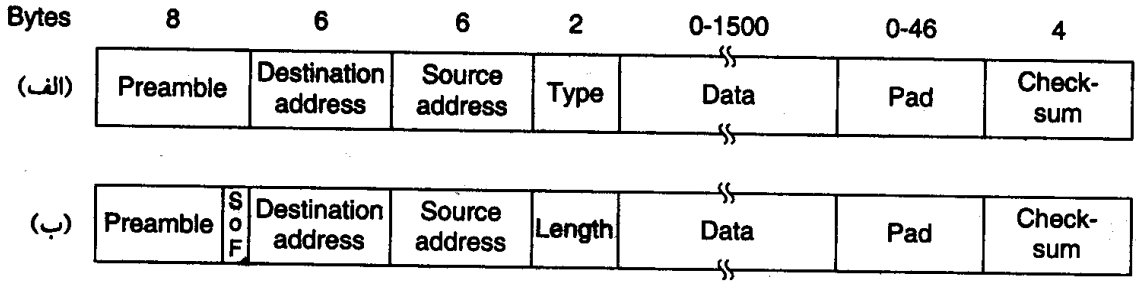
قالب (Format) فریم در اترنت

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.



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 46 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. 46 بیت باقیمانده (به‌غیر از بیت باارزش و بیت مجاور آن) فضایی معادل 2^{46} (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؟

$$\frac{L}{R} \geq RTT \Rightarrow \frac{L}{R} \geq 2T_p + 8T_{Repeater}$$

$$\frac{L}{R} \geq 2\frac{D}{V} + 8T_{Repeater} \Rightarrow \frac{L}{10^7} \geq 2\frac{2500}{3\times10^8} + 8\times4\mu s$$

$$\frac{L}{10^7} \geq 16.7\mu s + 8\times4\mu s \Rightarrow \frac{L}{10^7} \geq 49\mu s \Rightarrow L \geq 490bit$$

$$L \cong 512bit = \frac{512}{8} = 64byte$$

بنابراین طول قسمت داده حداقل باید 46 بایت باشد (فیلد Preamble در محاسبات شرکت نمی‌کند و مابقی فیلدها 18 بایت می‌شود)

۵) فیلد Pad : اگر فیلد داده شما از 46 بایت 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 جزء 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 bute ! یعنی اگر بخواهیم یک بایت داده بفرستیم باید مقدار بسیار زیادی داده اضافی بیهوده ارسال کنیم.

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 می‌دهد 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.

نکته۱ : 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.

بازده یا بهره اترنت

$$U_{Ethernet} = \frac{1}{1+2ae}$$

$$a = \frac{T_P}{T_f} = \frac{\frac{D}{V}}{\frac{L}{R}} \quad , \; e \cong 2.7$$

یا در بعضی از کتابها مثل کتاب گارسیا ;

$$U_{Ethernet} = \frac{1}{1+(2e+1)a}$$

شبکه‌های محلی بی‌سیم (Wireless LAN)

لایه فیزیکی شبکه‌های محلی بی‌سیم به ۶ دسته تقسیم می‌شود:

802.11 با امواج مادون قرمز

این روش مبتنی بر امواج مادون قرمز می‌باشد. 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.

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.

802.11 با تکنیک DSSS (Direct Sequence Spread Spectrum)

این تکنیک نیز با نرخ Mbps 2 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.

802.11a با تکنیک OFDM (Ortogonal Frequency Division Multiplexing)

هنگامی که سازمان FCC قانون منع استفاده از باندهای فرکانسی بالاتر ازISM (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 Mbps 54 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.

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 مودولاسیون تغییرفاز و کدینگ‌های ویژه استفاده شده است (برای بالا بردن سرعت)

802.11 g با تکنیک OFDM جدید

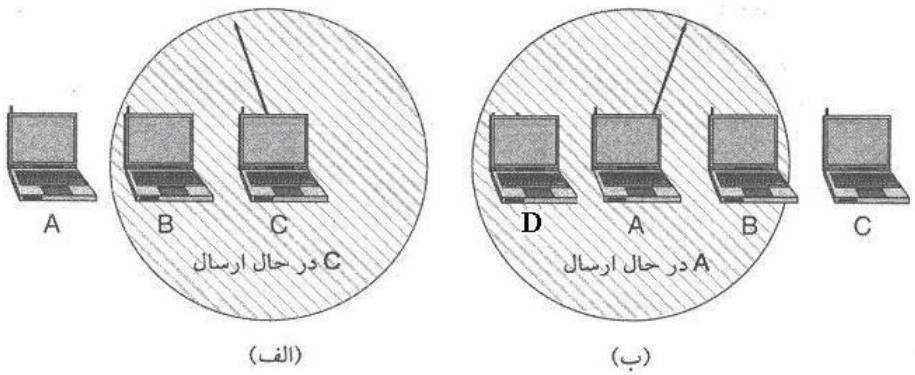
در نوامبر 2001 بالاخره IEEE از بین تکنیک‌های متنوع، مدولاسیون OFDM (مانند 802.11a) را انتخاب کرد با این تفاوت که مانند 802.11b در باند 2.4GHz کار می‌کند و استاندارد IEEE 802.11g را به عنوان آخرین استاندارد ارائه داد. سرعت این شبکه 54Mbps است.

زیر لایه MAC در شبکه‌های محلی بی‌سیم

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.

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 :

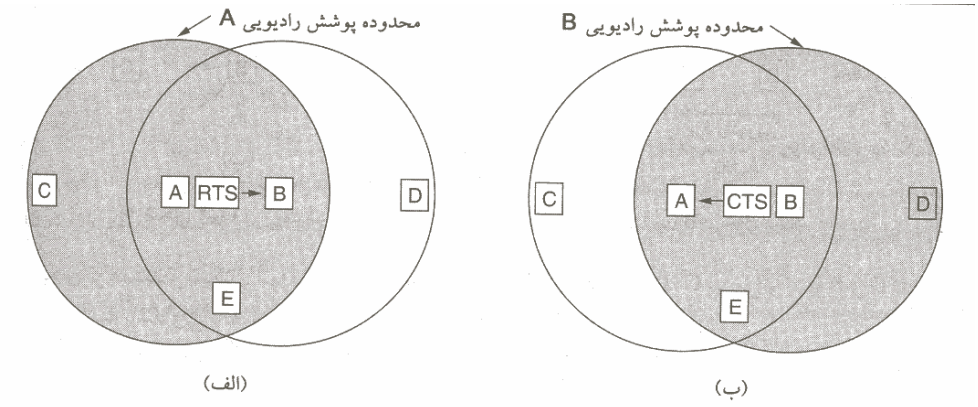
پروتکل مورد استفاده در DCF پروتکل CSMA / CA (Carrier Sense Multiple Access with Collision Avoidance) با امکان اجتناب از تصادم می‌باشد. این پروتکل که در آن هم کانال فیزیکی و هم کانال مجازی شنود می شوند، از دو بخش عمده تشکیل می‌شود:

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:



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. C، B و 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.

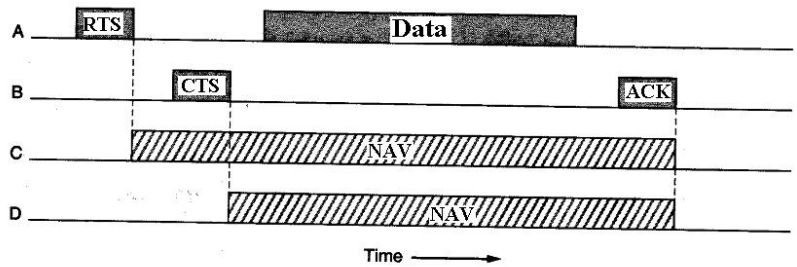
ج) پیشنهاد شده است که الگوریتم عقبگرد نمایی به جای این‌که بر روی یک ایستگاه اعمال شود بر روی یک جریان داده خاص اعمال شود که منظور از جریان داده تعدادی فریم است که در یک مکالمه مشخص با زمان مشخص بین مبدا و مقصد برقرار است.

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.

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.

در زیر شبکه‌های محلی بی‌سیم با شبکه‌های شهری بی‌سیم از جوانب مختلف مقایسه شده است.

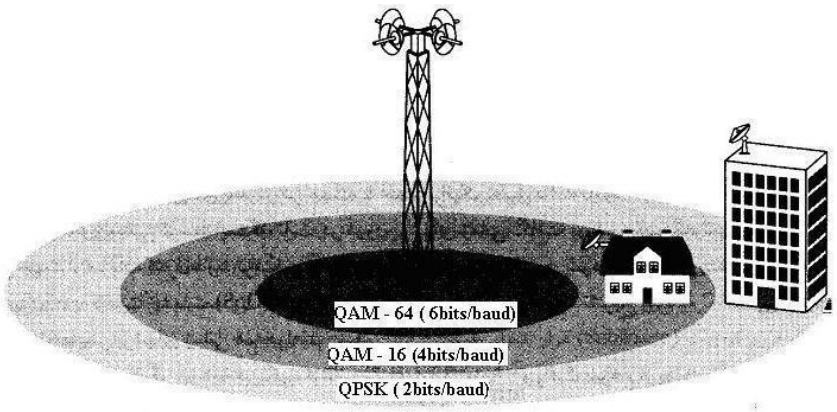
مورد مقایسه	(محلی بی‌سیم) IEEE 802.11	(شهری بی‌سیم) IEEE 802.16
حرکت	کامپیوترهای کیفی متحرکند	ساختمان‌ها ثابت‌اند
شارژ و هزینه	هزینه کمتری می‌دهند	صاحبان ساختمان‌ها پول بیشتری می‌دهند
حالت ارتباطی	Half Duplex	(بدلیل هزینه بیشتری که می‌پردازند) Full Duplex
فاصله	داخل طبقات ساختمان و محل‌های کوچک	2.5 کیلومتر 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.

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.



حساسیت به نویز بالا است و برای فواصل نزدیک باید استفاده شود $\begin{cases} R = \log_2^{64} \times R_s \leftarrow QAM-64 \\ R = 6R_s \end{cases}$

برای فواصل متوسط $\leftarrow R = 4R_s \leftarrow QAM-16$

حساسیت به نویز کمتر است و برای فواصل دورتر استفاده می‌شود. $\leftarrow R = 2R_s \leftarrow Q-PSK$

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.

نکته : تنها شبکه‌ای که در لایه فیزیکی آن با کد همینگ عمل FEC انجام می‌شود 802.16 است.

فصل هفتم

لایه شبکه (Network layer)

همانطور که در فصل اول ذکر شد وظایف لایه شبکه عبارتند از :

- 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 وظائف 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)

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 سوئیچ 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 سوئیچ تلفنی Circuit (مدار) می‌گویند و به روش سوئیچینگ 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 (Packet Loss Ratio) PLR، 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.

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)	بصورت پویا برای هر بسته مستقلاً انجام می‌شود.	فقط یکبار و آن هم در فاز برقرار اتصال و برپاسازی 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.

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) :

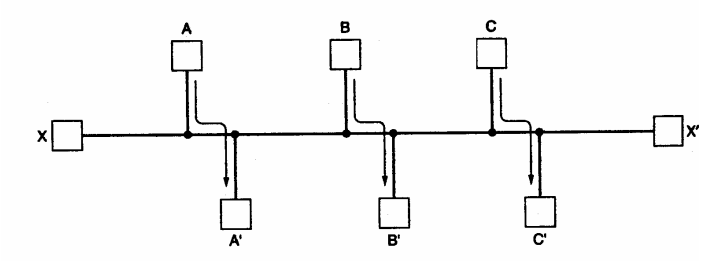
۳) قابلیت تحمل (Robustness) : خرابی سخت‌افزار و نرم‌افزار تاثیری بر عملکرد شبکه نگذارد. (شبکه را از کار نیاندازد)

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 متمرکز و براساس اطلاعات کامل و سراسری انجام می‌شود. مسیریابی مبدأ یکی از انواع مسیریابی متمرکز است.

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 و براساس اطلاعات ناقص محلی 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.

الگوریتم مسیریابی ابتدا کوتاه‌ترین مسیر Shortest Path

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 دائمی

گره دائمی گره‌ایست که برچسب آن مطمئناً کوتاه‌ترین مسیر تا مبدأ را نشان می‌دهد.

الگوریتم:

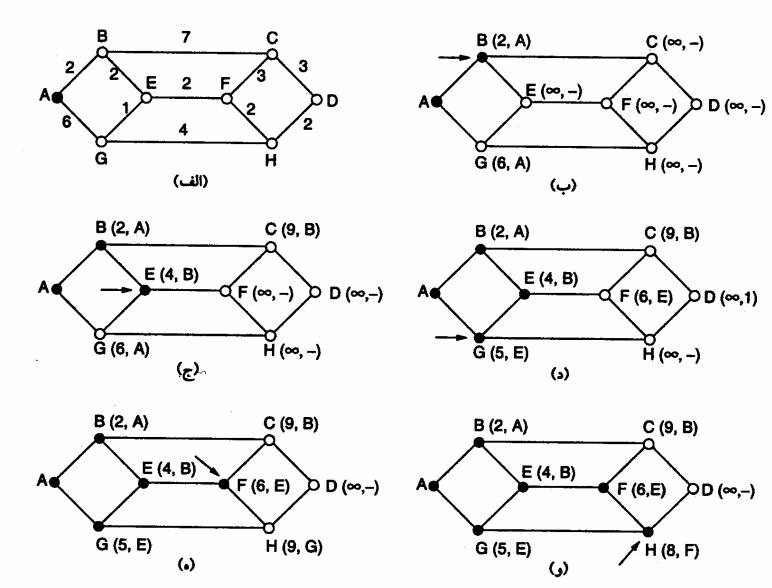
۱) برچسب همه گره‌ها تا مبدا را $(-,\infty)$ قرار دهید (یعنی فاصله آن تا مبدا ∞ و از طریق گره نامشخص)

۲) از گره مبدا شروع می‌کنیم (فرقی کند؛ از مقصد هم می‌توانستیم شروع کرده و تا مبدا ادامه دهیم) آن را دائمی 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 دائمی علامت بزنید

۵) اگر همه گره‌ها دائمی نشده‌اند به قسمت ۳ مراجعه کنید.



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:

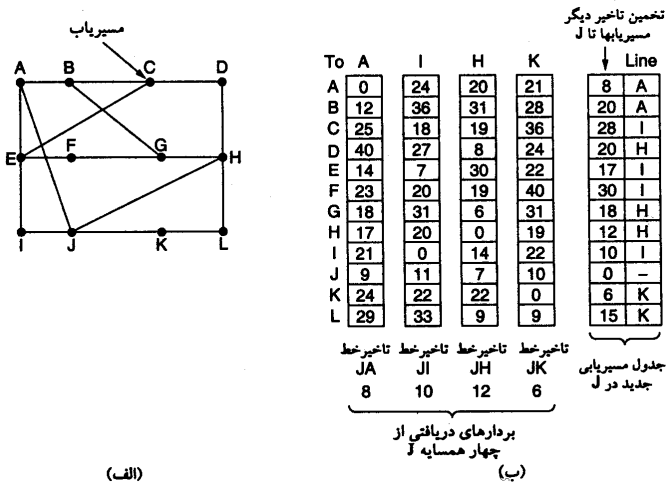
هر مسیریاب یک جدول مسیریابی دارد که به ازای هر مسیریاب موجود در زیر شبکه یک سطر در آن وجود دارد (مراجعه به جدول به کمک اندیس صورت می‌گیرد) در هر سطر دو فیلد زیر وجود دارد:

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.)

اگر هزینه نشان‌دهنده تعداد گام است 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.



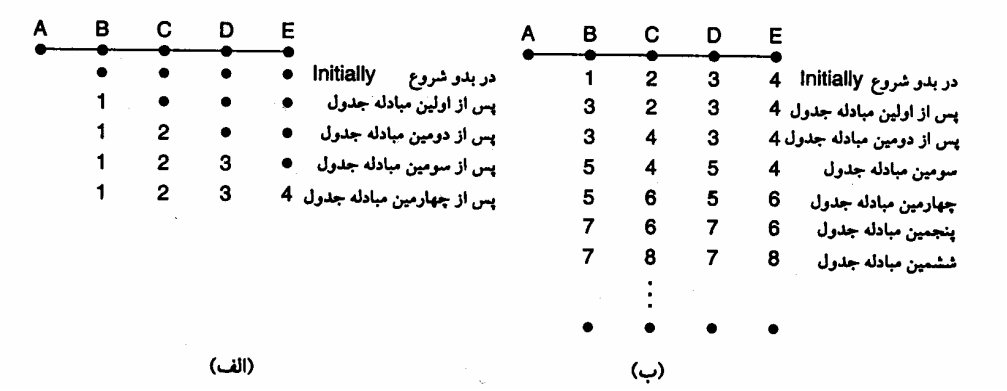
در این شکل می‌بینیم که گره J ابتدا بردار فاصله چهار همسایه خود را (A, I, H, K) را دریافت می‌کند و بر اساس این چهار بردار و فاصله خود از این چهار گره بردار فاصله خود را به روز در می‌آورد.

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.



شکل الف انتشار خبر خوب پیوستن A و شکل ب انتشار خبر بد حذف A را نشان می‌دهد. برای حل این مشکل پیشنهاد شده است که حداکثر فاصله را معین کنیم.

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.

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.

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)

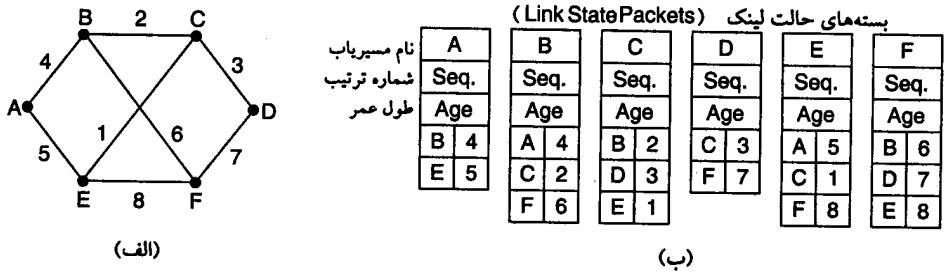
۳) Age یا (Time To Live) TTL کد یک شمارنده است و از مقدار معینی شروع می‌شود و هر دفعه (با عبور از هر مسیریاب یا گذشت یک ثانیه) یک واحد از آن کم می‌شود و هر وقت به صفر رسید این بسته از بین می‌رود.

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.



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.

نکته : 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 .

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.

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.

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 دائمی دارد! اگرچه ممکن است در آن‌جا نباشد (مثل یک تلفن همراه که اگرچه شماره تهران (محل استقرار دائمی) است اما ممکن است اکنون در تبریز باشد)

۲) یک عامل خانگی (Home Agent) که یک برنامه است در محل استقرار دائمی 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.

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 خوب 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.

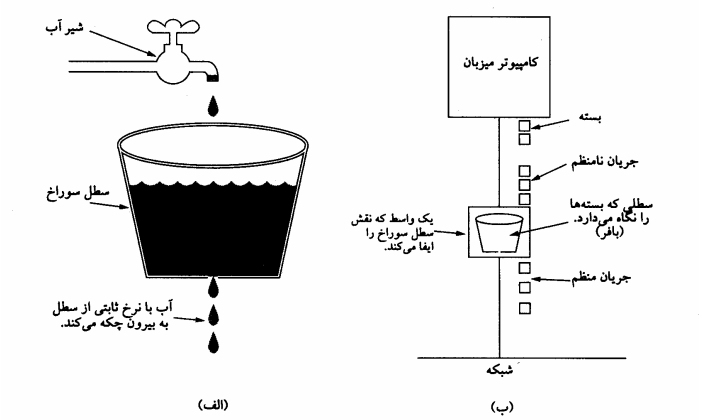
۲) ارسال بسته‌های خاص دعوت به آرامش (Chock) در شرایطی که حجم ترافیک سنگین شده است.

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. جوهرهٔ 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.

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.

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.

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. پیاده‌سازی خدمات DS بسیار آسان است.

سوئیچ برچسب و MPLS [۱]

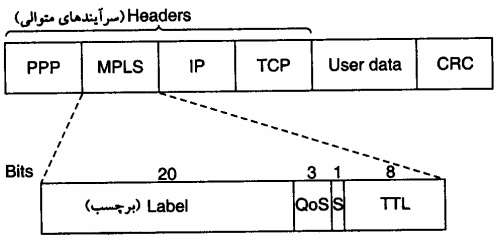
در ابتدای هر بسته یک «برچسب» (Label) اضافه شود و به‌جای آن‌که مسیریابی و هدایت بسته‌ها مبتنی بر آدرس مقصد باشد براساس این «برچسب» انجام شود. با استفاده از این «برچسب» به عنوان یک اندیس در جدول داخلی هر مسیریاب، خط خروجی صحیح و مناسب برای هر بسته پیدا می‌شود. به کمک این روش، مسیریابی بسته‌ها به سرعت انجام 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 Fram 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 سوئیچینگ با نام‌های متنوعی مثل «سوئیچینگ برچسب»[۲] یا « سوئیچینگ علامت»[۳] شناخته می‌شود. در نهایت IETF آن را تحت نام MPLS استاندارد کرد.

مضاف بر این، برخی افراد بین «مسیریابی » و « سوئیچینگ » 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 سوئیچینگ 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 Lable (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 (

---

[۱] Multi Protocol Label Switching

[۲] Label Switching

[۳] Tag Switching

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 سوئیچ‌های 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 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 هشتم

پروتکل اینترنت (IP)

جوهرهٔ اینترنت به گونه ای شکل گرفته است که مجموعه ای از شبکه‌های خودمختار را به همدیگر وصل می‌نماید. قراردادی که حمل و تردّد بسته‌های اطلاعاتی و همچنین مسیریابی صحیح آنها را از مبدأ به مقصد ، مدیریّت و سازماندهی می‌نماید پروتکلIP 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.

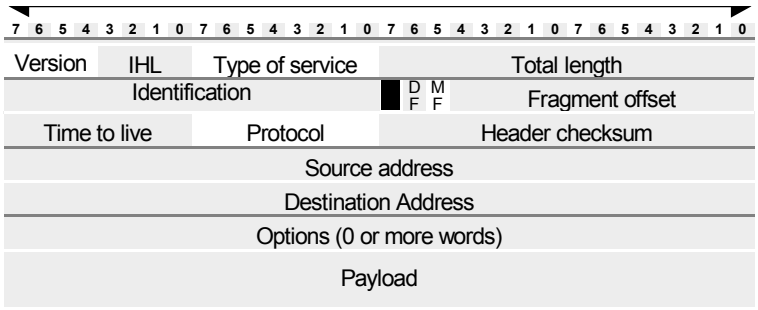
ساده ترین تعریف برای پروتکل IP روی شبکهٔ اینترنت بصورت زیر خلاصه می‌شود: لایهٔ IP یک واحد از داده‌ها را از لایهٔ بالاتر تحویل می‌گیرد؛ به این واحد اطلاعات معمولاً یک "دیتاگرام" گفته می‌شود. امکان دارد طول این دیتاگرام بزرگ باشد ، در چنین موردی لایهٔ IP آنرا به واحدهای کوچکتری که هر کدام "قطعه" (Fragment) نام دارد شکسته و با تشکیل 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.

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.

قالب یک بستهٔ IP

شکل زیر 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.

32 Bits



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 $(0100)_B$ است .

فیلد IHL[1] : این فیلد هم چهاربیتی است و طول کل سرآیند بسته را بر مبنای کلمات ۳۲ بیتی مشخص می‌نماید. غیر از فیلد Options که اختیاری است، وجود تمامی فیلدهای سرآیند الزامی می‌باشد . طول قسمت اجباریِ سرآیند ۲۰ بایت است و بهمین دلیل حداقل عددی که در فیلد IHL قرار می‌گیرد ۵ یا $(0101)_2$ 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 $(1111)_2$ 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. 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 $(111)_2$ در این سه بیت قرار گرفته باشد بالاترین اولویت برای بسته درنظر گرفته می‌شود.

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.

اکثر مسیریابهای تجاری فیلد Type of Service را نادیده می‌گیرند و اهمیتی به محتوای آن نمی‌دهند .

---

۱ IP Header Length
۲ Delay
۳ Throughput

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.

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 حقّ ندارد آن را قطعه قطعه کند، چرا که مقصد قادر به بازسازی دیتاگرام‌های تکه تکه شده نیست.

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.

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 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)

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. بعنوان 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 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 بصورت دو بایت، دوبایت با یکدیگر جمع می‌شود. نهایتاً حاصل جمع به روش "مکمل یک"[1] منفی می‌شود و این عدد منفی در این فیلد از سرآیند قرار می‌گیرد .

---

[1] Don't Fragment

[2] More fragment

در هر مسیریاب قبل از پردازش و مسیریابی ابتدا صحّتِ اطلاعات درون سرآیند بررسی می‌شود و بستهٔ IP فاقد اعتبار 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 حداقّل فیلد TTL از آن بسته عوض خواهد شد.

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 .

فیلد Destination Address : در این فیلد آدرس ۳۲ بیتیِ مربوط به ماشین مقصد که باید بسته IP تحویل آن بشود ، قرار می‌گیرد.

فیلد Payload : در این فیلد داده‌های دریافتی از لایهٔ بالاتر قرار می‌گیرد.

مبحث آدرسها در اینترنت و اینترانت

آدرسهای IP درون یک عدد دودویی ۳۲ بیتی درج می‌شوند ولیکن برای سادگی نمایش به چهار قسمت هشت بیتی[۲] تقسیم و بصورت چهار عدد دهدهی که با نقطه از هم جدا شده‌اند ، نوشته می‌شود؛ بعنوان مثال آدرس زیر یک آدرس IP معتبر می‌باشد که در قالب چهار قسمت دهدهی نوشته شده است:

34.21.225.1

این آدرس بصورت زیر در فیلد آدرس از یک بستهٔ IP تنظیم می‌شود:

00100010	00010101	11100001	00000001

کلاسهای آدرسِ IP

با توجه به آنکه اینترنت مجموعه‌ای از شبکه‌های متصل شده به هم می‌باشد، برای آدرس دادن به ماشینهای میزبان بهتر است ۳۲ بیت آدرسِ IP به قسمتهای زیر تقسیم شود:

آدرس ماشین/آدرس زیرشبکه/آدرس شبکه

الف) آدرس شبکه

ب) آدرس زیر شبکه (درصورت لزوم)

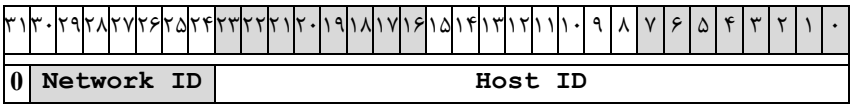
ج) آدرس ماشین میزبان

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:

---

۱ One's Compelement
۲ Octet

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 شبکه‌هائی 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 بصورت قراردادی بعنوان آدرس **"حلقه بازگشت"**[۱] 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:

هر گاه دو بیت پرارزش از آدرس IP مقدار 10 داشته باشد 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 چپِ آن بین ۱۲۸ تا ۱۹۱ باشد ، آن آدرس ، کلاس B خواهد بود:

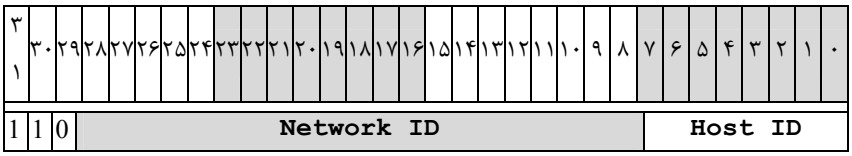
134. 64. 143 . 24

Net ID Host ID

---

[۱] Loopback

آدرس کلاس C : قالب ۳۲ بیتیِ آدرس در کلاس **C** به صورت زیر است:

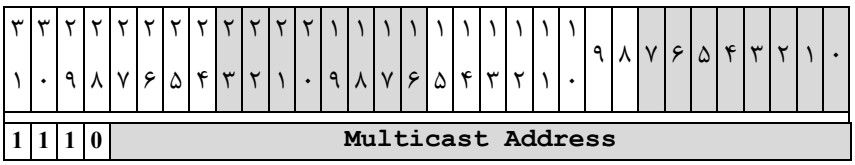


کلاس C مناسب ترین و پرکاربردترین کلاس از آدرس‌های IP است . همانگونه که از شکل مشخص است در این کلاس ، سه بیت پرارزش دارای مقدار 110 است و ۲۱ بیت بعدی از سه بایت سمت چپ برای تعیین آدرس شبکهٔ مورد نظر بکار رفته است . بنابراین در این کلاس می‌توان حدود دو میلیون شبکه را در جهان آدرس دهی کرد و هر شبکه می‌تواند 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

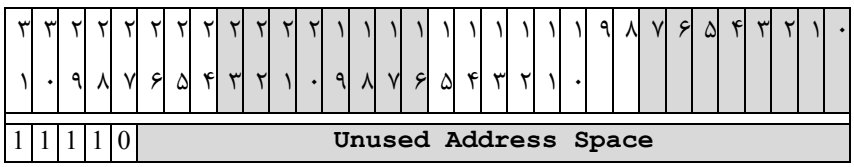
آدرس کلاس D : قالب ۳۲ بیتیِ آدرس در کلاس **D** به صورت زیر است:



در این کلاس ، چهار بیت پرارزش دارای مقدار 1110 است و ۲۸ بیت باقیمانده از کلّ آدرس برای تعیین آدرسهای "چند مقصده"[۱] (آدرسهای گروهی) است .

از این آدرسها برای ارسال یک دیتاگرام به طور همزمان برای چندین ماشین میزبان کاربرد دارد و بمنظور عملیات رسانه ای و چند پخشی بکار می‌رود. توضیح بیشتر در مورد این کلاس در بخشی مجزا ارائه خواهد شد .

آدرس کلاس E : قالب ۳۲ بیتیِ 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 بصورت آزمایشی از این آدرسها استفاده شد ولی تاکنون جهانی نشده‌اند .

[۱] Multicast

آدرسهای خاصّ

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 بعنوان آدرس خودش فرض می‌کند. البته از این آدرس فقط به عنوان آدرس مبداء و برای ارسال یک بسته می‌توان استفاده کرد و گیرندهٔ بسته نمی‌تواند پاسخی به مبداء بسته برگرداند.

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 بعنوان "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[۱]؛ 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.

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؛

برای آنکه بتوان زیرشبکه‌ها[۲] را تفکیک کرد جدای از قسمت آدرس شبکه که کل شبکهٔ دانشگاه شما را مشخص می‌کند بایستی در قسمت مشخصهٔ ماشین میزبان نیز به گونه ای زیر شبکه‌ها مشخص شوند . این کار از طریق مفهومی به نام **"الگوی زیرشبکه"**[۳] انجام می‌شود.

---

[۱] 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.

[۲] Subnetworks

[۳] Subnet Mask

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؟

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, آدرس IP متعلق به دستگاه شما بصورت زیر اختصاص داده شده است :

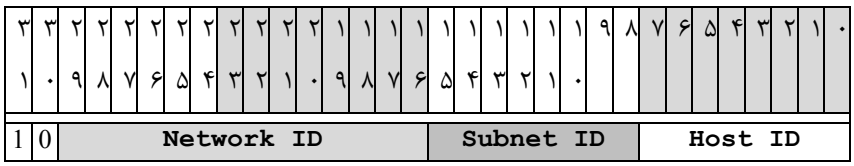
131.55.213.73

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 ، بهمین دلیل فرض کرده است که در فیلد مشخصهٔ ماشین میزبان (Host ID) که در کلاس B دو بایت سمت راست را شامل میشود ، بایت دومِ 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"[۱] 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 بعنوان مشخصهٔ زیر شبکه اختصاص داده شده است و بهمین 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.

---

[۱] Default Gateway

اینجاست که یک الگوی ۳۲ بیتی تعریف می‌شود که یک عدد ۳۲ بیتی و در این مثال بصورت 255.255.255.0 است:

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	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰

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 بسته بایستی 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

حاصل AND این دو آدرس با الگوی زیرشبکه 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 مبدأ می‌خواهد برای ماشینی با آدرس IP زیر بسته ای را ارسال نماید:

131.55.213.84

حاصل AND آدرس ماشین مبدأ و مقصد فوق با الگوی زیرشبکه 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 .

الگوی زیرشبکه در مثالهای بالا ساده‌ترین حالت بود که به آنها **"الگوی زیرشبکهٔ استاندارد"**[۱] گفته می‌شود چرا که الگوها دقیقاً مبتنی بر تقسیمات هشت‌بیتی هستند.

زیر شبکه‌های غیر استاندارد

الگوهای زیرشبکه برای تقسیم فضای آدرس‌دهی در شبکه‌های کلاس A ، B و C به تعدادی زیرشبکه ، تعریف می‌شوند. در مثالهائی که بررسی کردیم الگوی شبکه بصورت زیر تعریف شده بود:

255.255.255.0

حال الگوی زیر را در نظر بگیرید:

255.255.240.0

---

[۱] Standard Subnet Mask

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	۰	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 بعنوان "مشخصهٔ ماشین میزبان" استفاده شده است؛ بدین معنا که با این الگو می‌توان ۱۴ زیر شبکه (2^4-2) تعریف کرد بگونه ای که در هر زیرشبکه ۴۰۹۴ ، (2^{12}-2) ماشینِ میزبان قابل آدرس دهی خواهد بود.

CIDR[1] : مسیریابی بر اساس آدرس‌های بدون کلاس

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.

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

[1] CIDR: Classless InterDomain Routing

[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

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 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 20/(255.255.240.0) 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 – Sanches et al .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.

الگوی نمایش	تعداد آدرس	آخرین آدرس	اولین آدرس	دانشگاه
194.24.0.0/21	2048	194.24.7.	194.24.0.0	Cambridge
194.24.8.0/22	1024	194.24.11.255	194.24.8.0	Edinburgh
194.24.12/22	1024	194.24.15.255	194.24.12.0	در دسترس و آزاد
194.24.16.0/20	4096	194.24.31.255	194.24.16.0	Oxford

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 می دارد، 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.

[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. – م

پروتکل ICMP[۱]

پروتکل IP ، پروتکلی "بدون اتصّال"[۲] و "غیر قابل اعتماد"[۳] است! بدون اتصّال 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"[۴] 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[۵]" 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 مقصدِ بسته آمادگی 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"[۶] 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.

پروتکل ARP[7]

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 لایه اول تشکیل می‌شود؛ لایه اول وظیفه ای در قبال مسیریابی و کارهائی از این قبیل ندارد و فقط با آدرسهای فیزیکی کار می‌کند . بعنوان 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

---

۱ Internet Control Message Protocol
۲ Connectionless
۳ Unreliable
٤ Acknowledgement Message
٥ Time To Live
٦ Congestion

۷ Address Resolution Protocol

آدرس فیزیکی ماشین طرف مقابل (مقصد) معین باشد . (این آدرسها بصورت 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 .

وظیفه پروتکل ARP در اینجا آن است که یک "بسته فراگیر"[۱] روی کل شبکه محلی منتشر کند که این بسته در حقیقت سوال می‌کند:

" کسی که آدرس IP او فلان 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.

پروتکل RARP[۲]

پروتکل ARP برای یافتن آدرس‌های فیزیکی ایستگاههائی 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. بعنوان 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"[۳] 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 بصورت فراگیر و همگانی ارسال شوند و این بسته‌ها توسط مسیریاب هدایت نخوتهد شد.)

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[۴] 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.

---

[۱] Broadcast

[۲] Reverse Address Resolution Protocol

[۳] Local Broadcast

[۴] Network Server

پرسش‌های فصل ۱

الف) مدل لایه‌ای

۱. اگر مدل لایه‌ای دارای n لایه باشد و هر لایه h بیت سرآیند (Header) به بسته دریافتی اضافه کند، برای رسیده به بهره‌وری ۸۰٪ حداقل طول بسته داده‌ها بر حسب n و h چقدر است؟ (IT – سراسری ۸۴)

۱) ۸ nh ۲) ۶ nh ۳) ۴ nh ۴) ۲ nh

۲. کدام‌یک از عبارت‌های زیر در مورد مدل لایه‌ای شبکه‌های کامپیوتری صحیح است؟ (IT – سراسری ۸۴)

۱) هرچه تعداد لایه‌ها بیشتر می‌شود پیچیدگی طراحی کاهش می‌یابد

۲) هرچه تعداد لایه‌ها بیشتر می‌شود سربار سیستم کاهش می‌یابد

۳) هرچه تعداد لایه‌ها بیشتر می‌شود اعمال تغییرات پیچیده‌تر می‌شود

۴) هرچه تعداد لایه‌ها بیشتر می‌شود پیاده‌سازی پیچیده‌تر می‌شود

۳. دلیل (دلایل) استفاده از مدل لایه‌ای برای پیاده‌سازی شبکه‌های کامپیوتری کدام می‌باشد؟ (IT – سراسری ۸۸)

۱) پیاده‌سازی ساده‌تر

۲) پیاده‌سازی ساده‌تر، نگهداری آسان‌تر

۳) پیاده‌سازی ساده‌تر، نگهداری آسان‌تر ، اعمال تغییرات با هزینه کمتر

۴) پیاده‌سازی ساده‌تر ، نگهداری آسان‌تر ، اعمال تغییرات با هزینه کمتر، سربار کمتر

ب) مالتی‌پلکسینگ

۴. یک سیستم TDM آماری از ۸ کانال هر یک با پهنای باند 30Kbps استفاده می‌کند. اگر هر کانال در ۲۰ درصد موارد مشغول باشد، پهنای باند خط برای بهره ۸۰٪ چقدر خواهد بود؟ (IT – سراسری ۸۴)

۱) ۴۸Kbps ۲) ۶۰ Kbps ۳) ۱۲۸ Kbps ۴) ۲۴۰ Kbps

۵. فرض کنید صوت کد شده به صورت PCM با نرخ ۶۴ کیلو بیت در ثانیه درون سلول‌های ATM بسته‌بندی می‌شود. اگر نرخ ارسال داده ۱۵۵ مگابیت در ثانیه باشد، چند سلول می‌توان بین سلول‌های صوتی متوالی ارسال کرد؟ (طول هر سلول ATM ، ۵۳ بایت می‌باشد که ۴۸ باید آن داده و ۵ بایت آن سرآیند می‌باشد) (IT – سراسری ۸۴)

۱) ۵۱۹۲ ۲) ۴۱۹۲ ۳) ۳۱۶۲ ۴) ۲۱۹۲

۶. فرض کنید صوت کد شده به صورت PCM با نرخ ۶۴ کیلوبیت در ثانیه درون بسته‌های با طول ثابت ۵۳ بایت (شامل ۵ بایت سرآیند و ۴۸ بایت داده) بسته‌بندی می‌شود، اگر نرخ ارسال داده ۱۵۵ مگابیت در ثانیه باشد، چند بسته می‌توان بین دوبسته صوتی متوالی ارسال کرد؟ (IT – سراسری ۸۸)

۱) ۱۰۲۴ ۲) ۱۹۲۸ ۳) ۲۰۴۸ ۴) ۲۱۹۲

۷. یک سیستم ساده تلفنی شامل دو مرکز محلی و یک مرکز راه دور است. مراکز محلی با خطوط یک مگا هرتز به مرکز راه دور متصل‌اند. فرض کنید ۱۰ درصد تلفن‌های انجام شده راه دورند و هر گفتگوی تلفنی دارای پهنای باند ۴ کیلو هرتز است. هر یک از مراکز محلی حداکثر چند گفتگوی تلفنی را می‌توانند در هر لحظه حمایت نمایند؟ (IT – سراسری ۸۴)

۱) ۲۵۰ گفتگوی تلفنی ۲) ۱۰۰۰ گفتگوی تلفنی ۳) ۲۵۰۰ گفتگوی تلفنی ۴) بیش از ۳۰۰۰ گفتگوی تلفنی

پاسخ پرسش‌های فصل ۱

۱. گزینه ۳ صحیح است.

$$\frac{m}{m+nh}=\frac{80}{100} \rightarrow m=4nh$$

۲. گزینه ۱پاسخ پرسش است.

۳. گزینه ۳ صحیح است.

۴. گزینه ۲ صحیح است.

داده‌های مسئله به صورت زیر است:

$$TDM \quad , \quad 8\,Channels \qquad R_{max}=30Kbps$$

چون سیستم TDM آماری (ناهمگام یا هوشمند) است، بنابراین از تخصیص پویای کانال استفاده می‌کند و اگر یک کانال از حداکثر زمان خود استفاده نکند مازادش توسط سایر کانال‌ها استفاده می‌شود. از طرفی هر کانالی در ۲۰٪ مواقع مشغول است و بنابراین ظرفیت معادل (C) هر کانال به صورت مقابل به دست می‌آید.

$$C=\%20\times R_{max}=\frac{20}{100}\times 30\times 10^3=6\,Kbps$$

حالا هر ۸ کانال روی هم چقدر مصرف می‌کنند؟

$$6*10^3*8=48\,Kbps$$

باید دید برای بهره‌برداری ۸۰٪ چقدر لازم است؟

%	$Kbps$	
80	48	$\rightarrow x=60Kbps$
100	x	

۵. گزینه ۴ صحیح است.

داده‌های مسئله به صورت زیر است:

$$R_{PCM}=64Kbps=64*10^3\,bps\,,R_{Channel}=155Mbps=155*10^6\,bps\,,L=53\,Byte=424\,bit\,,H=5Byte=40\,bit$$

نرخ بیت مؤثر شبکه با توجه به سربار Headerها به صورت زیر خواهد بود:

$$R_{eff}=\mathrm{R}\times\mathrm{U}=155\mathrm{Mbps}\times\frac{\mathrm{L}-\mathrm{H}}{\mathrm{L}}=155\mathrm{Mbps}\times\frac{53-5}{53}=140.4\mathrm{Mbps}$$

حال می‌خواهیم ببینیم این نرخ بیت ارسالی چند برابر نرخ بیت صوت کد شده PCM است:

$$N = \frac{140.4Mbps}{64Kbps} = \frac{140.4 \times 10^6}{64 \times 10^3} = 2193$$

یعنی همزمان می‌توان 2193 کانال صوتی را به صورت TDM ارسال کرد و بین هر دو بسته صوتی از یک کانال 2192 بسته از کانال‌های دیگر ارسال کرد.

۶. گزینه ۴ صحیح است.

به حل پرسش ۵ مراجعه شود.

۷. گزینه ۳ صحیح است.

داده‌های مسئله به صورت زیر است

$$W_{Telecomm} = 1MHz = 10^6Hz \ , \quad W_{channel} = 4KHz = 4 * 10^3Hz$$

تعداد تماس‌های راه دور هر مرکز:

$$\frac{W_{Telecomm}}{W_{channel}} = \frac{10^6}{4 * 10^3} = 250$$

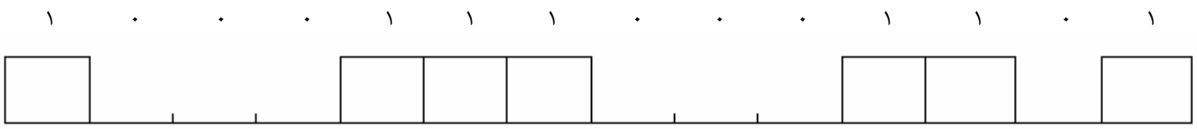
گفته شده فقط ۱۰٪ از تماس‌ها راه دورند، پس کل تماس‌ها ۲۵۰۰ عدد می‌شود:

$$\begin{array}{cc} Calls & \% \\ 250 & 10 \\ x & 100 \end{array} \rightarrow x = 2500$$

پرسش‌های فصل ۲

الف) آنالیز فوریه

۱. شکل زیر نمایش یک سیگنال ۲ بایتی است که می‌بایستی 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؟ (IT - سراسری ۸۳)



۱) ۲ هارمونیک ۲) ۴ هارمونیک ۳) ۶ هارمونیک ۴) ۸هارمونیک

ب) قانون نایکوئیست

۲. یک کانال تلوزیونی دیجیتال دارای پهنای باند ۶ مگا هرتز است. فرض کنید این کانال بدون نویز بوده و سیگنال‌های دیجیتال آن دارای ۱۲ سطح می‌باشند. چه نرخ داده‌ای به وسیله این این کانال قابل ارسال است؟ (IT - سراسری ۸۴)

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

ج) قانون شانون

۳. یک کانال ارتباطی با پهنای باند ۱ مگاهرتز و نسبت سیگنال به نویز ۱۰۰ دسی‌بی (dB) حداکثر چه نرخ داده‌ای را می‌تواند ارسال کند؟ (IT - سراسری ۸۳ و ۸۴)

۱) بیشتر از ۱۰۰ مگابیت در ثانیه

۲) کمتر از ۲ مگابیت در ثانیه

۳) بیشتر از ۴۰ مگابیت در ثانیه ولی کمتر از ۱۰۰ مگابیت در ثانیه

۴) بیشتر از ۲ مگابیت در ثانیه ولی کمتر از ۴۰ مژابیت در ثانیه

پاسخ پرسش‌های فصل ۲

۱. گزینه ۳ صحیح است.

$$T_0 = \tau * 16 = 50 * 10^{-6} * 16 = 800 * 10^{-6}$$
$$f_0 = \frac{1}{T_0} = \frac{1}{800 * 10^{-6}} = 1250$$
$$Harmonic = \left\lfloor \frac{W}{f_0} \right\rfloor = \left\lfloor \frac{8000}{1250} \right\rfloor = 6$$

بنابراین ۶ هارمونیک عبور می‌کند

۲. گزینه ۳ صحیح است.

$$R = 2W \log_2 M \rightarrow \ R = 2 * 6 * \log_2 12 > 36\, Mbps$$

۳. گزینه ۴ صحیح است.

داده‌های مسئله به صورت زیر است:

$$W = 1MHz = 10^6 Hz \ , \ SNR = 100dB$$

مسئله R را می‌خواهد و داریم $R = W * \log_2\left(\frac{S}{N} + 1\right)$ بنابراین باید اول $\frac{S}{N}$ را بدست بیاوریم . از طرفی داریم $SNR = 10 * \log_{10} \frac{S}{N}$

پس :

$$SNR = 10 * \log_{10} \frac{S}{N} \rightarrow 100 = 10 * \log_{10} \frac{S}{N} \rightarrow \frac{S}{N} = 10^{10}$$

$$R = W \log_2\left(1 + \frac{S}{N}\right) = 10^6 \times \log_2(10^{10} + 1) \approx 10^6 \times \log_2(10^{10})$$
$$\approx 10^7 \times \log_2 10 \approx 3.3 \times 10^7 bps \approx 33Mbps$$

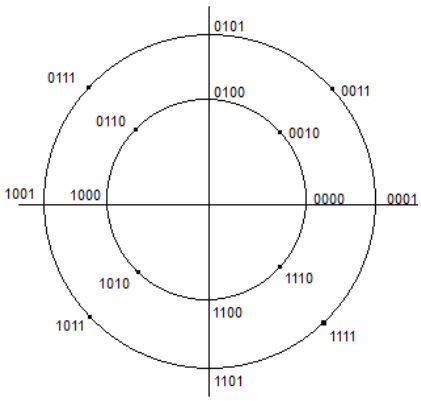
پرسش‌های فصل ۳

مدولاسیون QAM

۱. یک مودم که از روش QAM (Quadrature Amplitude Modulation) استفاده می‌کند دارای دیاگرام به صورتا فلکی در مختصات (۱،۱) ، (۱- ، ۱) ، (۱- ، ۱-) ، (۱ ، ۱-) می‌باشد. با استفاده از این مودم دو روی یک خط با ظرفیت ۱۲۰۰ نمونه در ثانیه (Baud) چه سرعت داده‌ای را می‌توان ارسال نمود. (IT - سراسری ۸۳)

۱) ۴۸۰۰ بیت در ثانیه
۲) ۲۴۰۰ بیت در ثانیه
۳) ۱۲۰۰ بیت در ثانیه
۴) ۶۰۰ بیت در ثانیه

۲. اگر برای ارسال اطلاعات دیجیتال از مدولاسیبون QAM مطابق با شکل زیر استفاده شود، شکل موج تولید شده برای ارسال بیت‌های 1100111100001011<- کدام است؟ (IT - سراسری ۸۷)



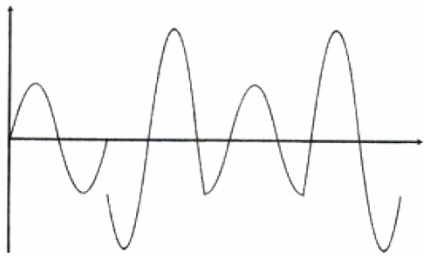
۱)

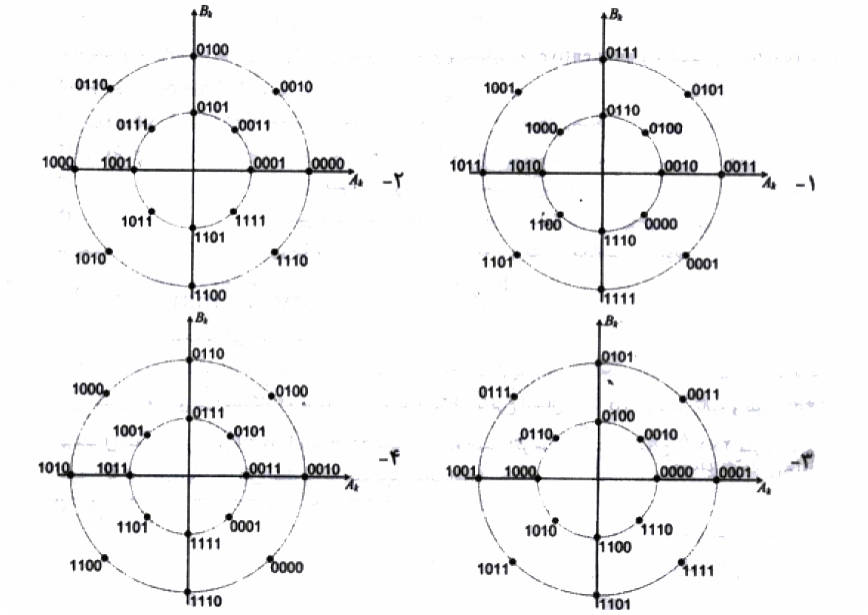
۲)

۳)

۴)

۳. با در نظر گرفتن روش مدلاسیون QAM ($x(t) = A_k Cos2\pi f_c t + B_K Sin2\pi f_c t$) ، اگر شکل موج سیگنال ارسالی برای داده 1100011110001011 ← مطابق زیر باشد، کدام گزینه نمودار فلکی این مدولاسیون می‌باشد؟ (IT - سراسری ۸۹)





پاسخ پرسش‌های فصل ۳

۱. گزینه ۲ صحیح است.

$$M = 4 \rightarrow R = R_S * \log_2 M = 1200 * 2 = 2400\ bps$$

۲. گزینه ۲ صحیح است.

بر اساس شکل داده شده در سوال، ۱۶ سیگنال مختلف وجود دارد (روی دایره ۱۶ نقطه وجود دارد). بر این ۱۶ سیگنال، ۴ بیت قابل ارسال است. ($2^4 = 16$) بنابراین بیت‌های داده شده را ۴ تا ، ۴ تا جدا می‌کنیم:1100/1111/0000/1011 ، از سمت چپ شروع می‌کنیم. هر بخش (۴ تایی) را در شکل نگاه می‌کنیم:

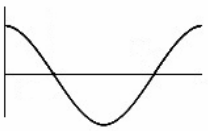
۴ بیت 1100 در دایره کوچک قرار دارد ، یعنی سیگنال متناظر با آن در دامنه کوچک قرار دارد ، بنابراین گزینه‌های ۱ و ۳ غلط هستند.

چون در شکل آنها بخش اول (که مثلا قرار است ۴ بیت اول را عبور دهد) دارای دامنه بزرگ است.

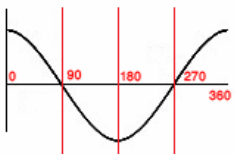
بنابراین تنها گزینه‌های ۲ و ۴ می‌مانند (که ۴ بیت اول آنها دارای دامنه‌های کوچک هستند)

از اینجا به بعد برای تمام ۴ بیت‌ها، اعمال زیر را انجام می‌دهیم:

سیگنال مرجع به صورت زیر است.



برای محاسبه باید اختلاف فازها را روی آن مشخص کرد:



اولین ۴ بیت: 1100 را در نظر می‌گیرم. این چهار بیت در بخش ۲۷۰ درجه مثلثاتی قرار دارد. بنابراین با سیگنال مرجع کوسینوسی ، باید ۲۷۰ درجه اختلاف فاز داشته باشد.

دومین ۴ بیت: 1111 را در نظر می‌گیرم. این چهار بیت در بخش ۳۱۵ درجه مثلثاتی قرار دارد. بنابراین با سیگنال مرجع کوسینوسی ، باید ۳۱۵ درجه اختلاف فاز داشته باشد.

سومین ۴ بیت: 0000 را در نظر می‌گیرم. این چهار بیت در بخش ۰ درجه مثلثاتی قرار دارد. بنابراین با سیگنال مرجع کوسینوسی ، باید ۰ درجه اختلاف فاز داشته باشد.

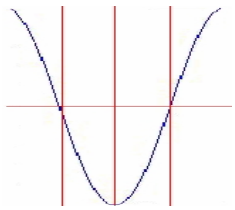
چهارمین ۴ بیت: 1011 را در نظر می‌گیرم. این چهار بیت در بخش ۲۲۵ درجه مثلثاتی قرار دارد. بنابراین با سیگنال مرجع کوسینوسی ، باید ۲۲۵ درجه اختلاف فاز داشته باشد.

البته در این سوال با تشخیص اولین ۴ بیت نیز، گزینه درست قابل تشخیص بوده است

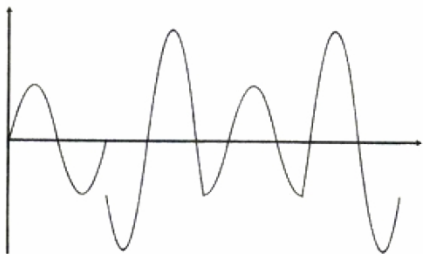
۳. گزینه ۳ صحیح است. (اما در کلید سنجش به غلط گزینه ۴ اعلام شده است)

مدل QAM و در اینجا 16QAM. به این علت که ۴ سیگنال در شکل صورت سوال وجود دارد. و برای و ۱۶ بیت باید ارسال شود. بنابراین باید بیت‌ها را ۴ بیت ، ۴ بیت جدا کنیم : **1100/0111/1000/1011** . بعد از سمت چپ ، ۴ بیت اول باید ارسال شود. باید ببینیم با توجه به سیگنل مرجع کوسینوسی ، کدام شکل جواب خواهد شد

مدل مرجع کوسینوسی به صورت زیر است.

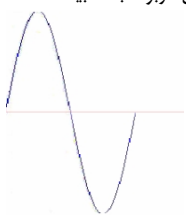


و شکل داده شده در مسئله به صورت زیر است

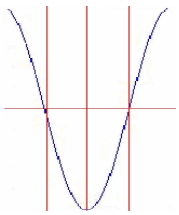


سیگنال اول باید ۴بیت اول (از سمت چپ) یعنی **1100** را عبور دهد، در صورت سوال میبینیم که اولاً دامنه این ۴ بیت کوچک است، بنابراین در جواب‌ها باید بیت‌های **1100** در دایره کوچک باشد. بنابراین یا گزینه ۱ و یا گزینه ۳ درست است.
حالا باید دید که این سیگنال ، نسبت به سیگنال کوسینوسی مرجع چقدر اختلاف فاز دارد، تا از روی آن معلوم شود در کجای دیاگرام فلکی (دایره نقطه‌دار پاسخ) باید این چهار بیت (**1100**) حضور می‌داشته است. برای راحتی کار، سیگنال اول را با سیگنال مرجع کنار هم می‌گذاریم:

سیگنال مربوط به ۴ بیت **1100**



سیگنال مربوط به موج مرجع کوسینوسی



مشاهده می‌شود که سیگنال مربوط به ۴ بیت اول یعنی **1100** با سیگنال مربوط به موج مرجع کوسینوسی ، $\frac{3\pi}{2}$ اختلاف فاز دارد. به همین ترتیب قابل مشاهده است که ۴ بیت دومیعنی **0111**(با دامنه بزرگ) با سیگنال مربوط به موج مرجع کوسینوسی ، $\frac{3\pi}{4}$ اختلاف فاز دارد ، ۴ بیت سومیعنی **1000**(با دامنه کوچک) با سیگنال مربوط به موج مرجع کوسینوسی ، π اختلاف فاز دارد ، ۴ بیت دومیعنی **1011**(با دامنه بزرگ) با سیگنال مربوط به موج مرجع کوسینوسی ، $\frac{5\pi}{4}$ اختلاف فاز دارد

پرسش‌های فصل ۴

کنترل خطا

۱. در یک شبکه کامپیوتر، لایه پیوند داده‌ها خطاهای انتقال را با درخواست ارسال مجدد برای پیام‌های دریافتی خطادارمرتفع می‌نماید. 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؟ (IT - سراسری ۸۴)

۱) $\frac{1}{1-P}$ ۲) $\frac{1}{1-P^2}$ ۳) $\frac{1}{1-2P}$ ۴) $\frac{1}{(1-P)^2}$

۲. برای بالا بردن اطمینان در انتقال داده‌ها، به جای یک بیت توازن از کدی استفاده می‌کنیم که یک بیت توازن برای بیت‌های فرد و یک بیت توازن برای بیت‌های زوج دارد. فاصله همینگ این کد چقدر است؟ (IT - سراسری ۸۶)

۱) ۲ ۲) ۳ ۳) ۴ ۴) ۵

۳. می‌خواهیم با استفاده از کد همینگ پیام‌های ۴ بیتی داده را به نحوی ارسال کنیم که گیرنده بتواند هر خطای یک بیتی را تشخیص و تصحیح کند. بدین منظور تعداد بیت‌های چک کننده مورد نیاز چقدر است؟ اگر پیام 1101<- باشد، کد تولید شده ارسالی چیست؟ (IT - سراسری ۸۷)

۱) ۲ بیت و 101010 ۲) ۲بیت 110101

۳) ۳ بیت و 1010101 ۴) ۳ بیت و 1101011

۴. یک روش کدگذاری قدیمی در ارسال رادیویی استفاده از کدهای با تعداد بیت "۱" برابر است. در کد ۲ از ۵، فقط ۲ بیت از کلمه کد ۵ بیتی "۱" می‌باشد. در صورتی که از کدهای ۲ از ۵ استفاده شود، احتمال عدم تشخیص خطا در گیرنده برابر کدام است؟ (IT - سراسری ۸۸)

۱) $\frac{7}{32}$ ۲) $\frac{8}{32}$ ۳) $\frac{9}{32}$ ۴) $\frac{10}{32}$

۵. یک پیام از لایه بالاتر به ۵ بسته تقسیم شده است. اگر عملیات کنترل خطا در ارسال این بسته صورت نگیرد و احتمال دریافت صحیح بسته در مقصد ۰/۵ باشد، این پیام چند بار باید ارسال شود تا صحیح به مقصد برسد؟ (IT - سراسری ۸۸)

۱) ۴ ۲) ۸ ۳) ۱۶ ۴) ۳۲

۶. در یک کد خطی (۳و۶) بیت‌های چک کننده (check bits) به صورت زیر محسابه می‌شوند

$$b_4 = b_1 + b_2$$
$$b_5 = b_1 + b_3$$
$$b_6 = b_2 + b_3$$

حداقل فاصله همینگ چقدر است؟ (IT - سراسری ۸۹)

۱) ۴ ۲) ۳ ۳) ۲ ۴) ۵

پاسخ پرسش‌های فصل ۴

۱. گزینه ۱ صحیح است.

این یک آزمایش برنولی با احتمال پیروزی 1-P است. تکرار آزمایش برنولی تا رسیدن به اولین پیروزی از تابع توزیع هندسی پیروی می‌کند و در این تابع توزیع، امید ریاضی به صورت زیر خواهد بود:

$$E(x) = \frac{1}{P-1}$$

۲. گزینه ۱ صحیح است.

۳. گزینه ۳ صحیح است.

برای اینکه متوجه بشویم چند کد افزونه نیاز است ، داریم:

$$m + r + 1 \leq 2^r \xrightarrow{m=4} r = 3$$

از طرفی فرمت کدینگ استاندارد همینگ به صورت زیر است. (از آنجا که در صورت سوال، کد دیگری ذکر نشده، منظور فرمت استاندارد است)

$r_1\ r_2\ m_3\ r_4\ m_5\ m_6\ m_7$

که در آن، r_i ها به صرورت زیر به دست می‌آیند

$$r_1 = m_3 \oplus m_5 \oplus m_7$$

$$r_2 = m_3 \oplus m_6 \oplus m_7$$

$$r_4 = m_5 \oplus m_6 \oplus m_7$$

که در آنها r_i کدهای اضافه شده (افزونه‌ها) و m_i ها هم، داده هستند. داده‌های مسئله را نظیر به نظیر بر سر جایش می‌گذاریم: (از چپ به راست)

$r_1\ r_2\ 1\ r_4\ 1\ 0\ 1$

$$r_1 = 1 \oplus 1 \oplus 1 = 1$$

$$r_2 = 1 \oplus 0 \oplus 1 = 0$$

$$r_4 = 1 \oplus 0 \oplus 1 = 0$$

بنابراین داده‌ای که باید ارسال شود $\mathbf{1010101}$ خواهد بود.

۴. گزینه ۳ صحیح است.

صورت این سوال به این معنی است که ، وقتی ۵ بیت داریم، دو تا از این پنج بیت ۱ هستند. با این وجود چه زمانی نمی‌توان خطارا تشخیص داد؟ وقتی که در کد دارای خطا نیز دو بیت ۱ وجود داشته باشد.

تعداد کل حالات $2^5 = 32$ و تعداد کل حالت‌های ممکن دارای دو بیت ۱، $\binom{5}{2} = 10$ است که یک مورد آن صحیح (کد ارسالی) و 9 مورد آن دارای خطا و غیر قابل تشخیص است. به این ترتیب جواب $\frac{9}{32}$ خواهد بود.

۵. گزینه ۳ صحیح است.

چون کنترل خطا در ارسال هر بسته صورت نمی‌گیرد، احتمال درست رسیدن پیام برابر احتمال درست رسیدن هر 5 بسته درون آن است:

$$p = \left(\frac{1}{2}\right)^5 = \frac{1}{32}$$

اگر آزمایش برنولی با احتمال پیروزی p و احتمال شکست (q=1-P) را تکرار کنیم به توزیع هندسی می‌رسیم و میانگین توزیع هندسی از رابطه زیر به دست می‌آید:

$$E(X) = \frac{1}{p} = 32$$

۶. گزینه ۲ صحیح است.

تمام کدهای موجود را بدست می‌آوریم (کلمه کد بدست می‌آید) ، وزن هر کلمه کد را بدست می‌آوریم. کمترین وزن (غیر صفر) کلمه کد، حداقل فاصله همینگ است

$$\begin{matrix} & b_1b_2b_3b_4b_5b_6 \\ & W=0 \rightarrow 0\ 0\ 0\ 0\ 0\ 0 \\ & W=3 \rightarrow 0\ 0\ 1\ 0\ 1\ 1 \\ b_4 = b_1 \oplus b_2 & W=3 \rightarrow 0\ 1\ 0\ 1\ 0\ 1 \\ b_5 = b_1 \oplus b_3 \rightarrow & W=4 \rightarrow 0\ 1\ 1\ 1\ 1\ 0 \\ b_6 = b_2 \oplus b_3 & W=3 \rightarrow 1\ 0\ 0\ 1\ 1\ 0 \\ & W=4 \rightarrow 1\ 0\ 1\ 1\ 0\ 1 \\ & W=4 \rightarrow 1\ 1\ 0\ 0\ 1\ 1 \\ & W=3 \rightarrow 1\ 1\ 1\ 0\ 0\ 0 \end{matrix}$$

$$\xrightarrow{\text{کمترین وزن غیرصفر}} W_{min} = 3 \rightarrow d_{min} = 3$$

پرسش‌های فصل ۵

کنترل جریان

۱. ایستگاه A با نرخ ۱۰ مگابیت در ثانیه داده‌هایی را برای ایستگاه B ارسال می‌کند. ایستگاه B داده‌های دریافتی را در بافر دریافتی خود قرار داده و با نرخ ۹/۲ مگابیت در ثانیه آنها را پردازش می‌کند. اگر ایستگاه B برای کنترل جریان از پیام‌های کنترلی Xoff (Transmission Off) و Xon (Transmission) استفاده کند، با فرض اینکه تأخیر یکطرفه ارتباط ۱۰ میلی ثانیه باشد، ایستگاه B در زمانی که بافر دریافتش چند بایت فضای خالی دارد باید پیام کنترلی Xoff را ارسال کند تا بافرش سرریز نشود. (IT – سراسری ۸۹)

۱) ۴۰۰۰۰ ۲) ۱۰۰۰ ۳) ۲۰۰۰ ۴) ۳۰۰۰

۲. برای کنترل خطا بین دو ایستگاه که توسط یک پیوند ارتباطی با نرخ ارسال ۱۰۰ کیلو بیت در ثانیه و طول ۴۰۰ کیلومتر به هم متصل شده‌اند، ار روش Stop and Wait استفاده شده است. اگر سرعت انتشار امواج $2 * 10^8$ متر بر ثانیه باشد، برای رسیدن به کارایی ۵۰٪ حداقل طول بسته‌ها چند بایت باید باشد؟ (IT – سراسری ۸۹)

۱) ۵۰ ۲) ۴۰۰ ۳) ۲۰۰ ۴) ۱۰۰

۳. 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 فریم‌ها ۳۵۰ بایت و شماره ترتیب یک عدد سه بیتی باشد، با فرض اینکه اندازه فریم‌های Ack بسیار کوچک و قابل صرف نظر می‌باشد، نرخ ارسال داده موثر با استفاده از روش کنترل خطا Go-Back-N ARQ چقدر است؟ (IT – سراسری ۸۳)

۱) ۱۲ کیلو بیت در ثانیه ۲) ۲۴ کیلو بیت در ثانیه ۳) ۳۶ کیلو بیت در ثانیه ۴) ۴۸ کیلو بیت در ثانیه

۴. یک کانال ارتباطی ISDN دارای نرخ ارسال داده ۱۲۸ کیلوبیت در ثانیه و تاخیر انتشار یک طرفه ۴۰ میلی ثانیه می‌باشد. با فرض اینکه طول فریم‌های Ack بسیار کوچک و قابل صرف نظر باشد، اگر از روش کنترل خطای Go-Back-N برای کنترل خطا استفاده کنیم و اندازه فریم‌ها ۱۲۸ بایت باشند، شماره ترتیب مورد نیاز چند بیت باید باشد تا جریان ارسال داده‌ها قطع نشود؟ (IT – سراسری ۸۴)

۱) ۳ بیت ۲) ۴ بیت ۳) ۵ بیت ۴) ۶ بیت

۵. در یک پیوند ارتباطی که دارای نرخ ارسال 128 Kbps و تاخیر انتشار یک طرفه 40msec می‌باشد. حداقل اندازه بافر در سمت دریافت کننده در حالتی که پروتکل ARQ تکرار انتخابی Selective Repeat استفاده می‌شود، اندازه فریم‌ها 128 Byte و زمان Time Out، 100msec است، چقدر باید باشد؟ (IT – سراسری ۸۶)

۱) ۱۵۳۶ بایت ۲) ۱۶۰۰ بایت ۳) ۱۶۶۴ بایت ۴) ۱۲۸۰۰ بایت

۶. در یک پیوند ارتباطی ، اگر نرخ ارسال داده‌ها 1.5 Mbps، نرخ خطای بیتی $P = 10^{-4}$ و تاخیر انتشار 5msecباشد، در پروتکل Selective Repeatبا فرض اینکه اندازه پنجره ارسال به طور مناسب انتخاب می‌شود و سربار هر فریم 100بیت باشد. بهترین اندازه اطلاعات برای رسیدن به کارایی حداکثر چقدر است؟ (IT – سراسری ۸۶)

۱) ۸۰۰ بیت ۲) ۹۰۰ بیت ۳) ۱۰۰۰ بیت ۴) ۱۱۰۰ بیت

۷. با در نظر گرفتن یک کانال بدون خطا با نرخ ارسال ۶۴ کیلو بیت در ثانیه ، اگر فرض کنیم اندازه فریم‌های داده ۱۶۰ بایت ، سربار هر فریم ۱۶ بایت، اندازه فریم‌های ACK ۱۶ بایت و شماره ترتیب ارسال یک عدد ۳ بیتی باشد، با فرض اینکه تاخیر انتشار در این کانال ۲۴۱ میلی‌ثانیه است و گیرنده به محض دریافت فریم داده، پیام ACK را ارسال می‌کند، کارایی پروتکل Go Back N و پروتکل Selective Repeat برای این کانال چقدر است؟ (IT – سراسری ۸۷)

۱) $\eta_{SR} = 14.3\%$ ، $\eta_{GBN} = 25\%$ ۲) $\eta_{SR} = 25\%$ ، $\eta_{GBN} = 14.3\%$

۳) $\eta_{SR} = 28.6\%$ ، $\eta_{GBN} = 50\%$ ۴) $\eta_{SR} = 50\%$ ، $\eta_{GBN} = 28.6\%$

پاسخ پرسش‌های فصل ۵

۱. گزینه ۳ صحیح است.

$$R_{A-Send} = 10Mbps = 10^7 bps\ ,\quad R_{B-Process} = 9.2Mbps = 9.2 * 10^6 bps\ ,\quad T_p = 10ms = 10^{-2}s$$

تعداد بیت‌های خالی در بافر = تعداد بیت‌هایی که در زمان $2T_p$ ایستگاه A برای B ارسال می‌کند – تعداد بیت‌هایی که ایستگاه B در $2T_p$ می‌تواند پردازش کند

$b_{Buffer-B}$: تعداد بیت‌های خالی در بافر

$b_{A\to B}$: تعداد بیت‌هایی که در زمان $2T_p$ ایستگاه A برای B ارسال می‌کند

$b_{B-Process}$: تعداد بیت‌هایی که ایستگاه B در $2T_p$ می‌تواند پردازش کند

$$R_{A-Send} = 10^7 bps \to \frac{s}{2T_p}\ \frac{bit}{b_{A\to B}} \to \frac{s}{2*10^{-2}}\ \frac{bit}{b_{A\to B}} \to b_{A\to B} = 2 * 10^5\ bit$$

$$R_{B-Process} = 9.2 * 10^6 bps \to \frac{s}{2T_p}\ \frac{bit}{b_{B-Process}} \to \frac{s}{2*10^{-2}}\ \frac{bit}{b_{B-Process}} \to b_{B-Process} = 184 * 10^3\ bit$$

$$b_{Buffer-B} = (b_{A\to B} - b_{B-Process}) = (200000 - 184000) = 16000\ \text{bit} = 2000\ Byte$$

۲. گزینه ۱ صحیح است.

داده‌های مسئله به صورت زیر است

$$\text{R} = 100\ \text{Kbps}\ ,\text{D} = 400\ \text{Km}\ ,\text{V} = 2 * 10^8\ ,U_{S\&W} = 0.5$$

$$U_{S\&W} = \frac{1}{1+2a} \to U_{S\&W} = \frac{1}{1+2\frac{T_p}{T_t}} \to 0.5 = \frac{1}{1+2\frac{\frac{D}{V}}{\frac{L}{R}}} \to \frac{1}{2} = \frac{1}{1+2*\frac{\frac{4*10^5}{2*10^8}}{\frac{L}{10^5}}} \to L = 400\ bit$$

در صورت سوال گفته شده طول فریم چند بایت باید باشد:

$$\frac{400}{8} = 50\ Byte$$

۳. گزینه ۲ صحیح است. ***(اگرچه گزینه صحیح وجود ندارد)***

می‌دانیم با شماره ترتیب سه بیتی می‌توان هشت شماره ترتیب داشت (از 0 تا 7) و نیز می‌دانیم در روش Go-Back-N ARQ تعداد شماره ترتیب برابر $\text{W} + 1$ است:

$$\text{W} + 1 = 8 \to \text{W} = 7$$

بنابراین داده‌های مسئله به صورت زیر است:

$$R = 56kbps = 56 * 10^3 bps \ , \quad W = 7 \ , \quad L = 350\,Byte = 350 * 8bit \ , \quad T_P = 150ms = 150 * 10^{-3} s$$

محاسبه کارایی:چون در این مسئله از طول Header یا سرآیند، اندازه Ack و سربار پردازشی و نیز احتمال خطا صرف نظر شده است از رابطه ساده ذکر شده در جزوه پارسه استفاده می‌کنیم:

$$a = \frac{T_P}{T_F} = \frac{T_P}{\frac{L}{R}} = \frac{150 * 10^{-3}}{\frac{350 * 8}{56 * 10^3}} = 3$$

$$U_{GBN} = \frac{W}{1 + 2a} = \frac{7}{1 + 2 \times 3} = 1$$

مسئله نرخ داده موثر را خواسته است: $R_{eff} = U_{GBN} * R = 1 * 56 * 10^3 = 56 * 10^3 bps = 56\,Kbps$

اما متاسفانه این پاسخ در گزینه‌ها موجود نیست و با توجه به گزینه صحیح اعلام شده مشخص می‌شود که طراح این تست یک اشتباه بزرگ داشته است و منظور وی از عبارت شماره ترتیب سه بیتی همان اندازه پنجره سه ($W = 3$) بوده است:

$$U_{GBN} = \frac{W}{1 + 2a} = \frac{3}{1 + 2 \times 3} = \frac{3}{7}$$

$$R_{eff} = U_{GBN} * R = \frac{3}{7} * 56 * 10^3 = 24 * 10^3 bps = 24\,Kbps$$

۴. گزینه ۲ صحیح است.

داده‌های مسئله به صورت زیر است:

$$R = 128Kbps = 128 * 10^3 bps \, , T_P = 40ms = 40 * 10^{-3} , L = 128\,Byte = 1024bit$$

$$a = \frac{T_P}{T_F} = \frac{T_P}{\frac{L}{R}} = \frac{40 * 10^{-3}}{\frac{1024}{128 * 10^3}} = 5$$

با توجه به رابطه $U = \frac{W}{1+2a}$، برای رسیدن به راندمان ۱ (البته بدون خطا و با صرف نظر از اندازه Ack، سربار Header و زمان پردازش)، اندازه پنجره باید حداقل برابر $1 + 2a$ باشد:

$$W \geq 1 + 2a \rightarrow W \geq 11 \rightarrow W_{min} = 11$$

اما می‌دانیم که در روش Go-Back-N تعداد شماره ترتیب لازم برابر $W + 1 = 12$ است. یعنی باید ۱۲ شماره ترتیب (از ۰ تا ۱۱) داشته باشیم و برای شمردن تا شماره ۱۱ به ۴ بیت نیاز است.

۵. گزینه ۳ صحیح است.

داده‌های مسئله به صورت زیر است

$$R = 128\ Kbps = 128 * 10^3\ bps \ , T_p = 40\ msec = 4 * 10^{-2}\ s \, , L = 128\ Byte = 1024\ bit \, , T_o = 100\ msec = 10^{-1}\ s$$

$$a = \frac{T_p}{T_t} = \frac{4 \times 10^{-2}}{\frac{L}{R}} = \frac{4 \times 10^{-2}}{\frac{1024}{128 * 10^3}} = 5$$

$$W \geq 1 + 2a \ \rightarrow W \geq 11$$

اما دقت کنید که در این مسئله زمان *Timeout* هم داده شده است و باید دقت کنید که معمولاً زمان *Timeout* کمی بیشتر از زمان $T_t + 2T_p$ یعنی انتقال فریم بعلاوه زمان انتشار فریم و *Ack* (رفت و برگشت) در نظر گرفته می‌شود، یعنی:

$$\frac{T_O}{T_t} > \frac{T_t + 2T_p}{T_t} \quad \hookrightarrow \quad \frac{T_O}{T_t} > 1 + 2a$$

بنابراین با در نظرگرفتن گم شدن Ack، اندازه پنجره کامل (برای راندمان 1) باید در رابطه زیر هم صدق کند:

$$W \geq \frac{T_O}{T_t} \rightarrow W \geq \frac{100 * 10^{-3}}{\frac{1024}{128 * 10^3}} \rightarrow W \geq 12.5 \rightarrow W = \lceil 12.5 \rceil = 13$$

چون از روش Selective Reject استفاده شده است، پنجره گیرنده نیز باید 13 باشد به این معنی است که بافر گیرنده نیز باید مانند فرستنده به اندازه 13 فریم (Frame) جا داشته باشد و چون اندازه هر فریم 128 Byte است پس در کل $13 * 128 = 1664$ بایت فضا لازم است.

۶. گزینه ۳ صحیح است.

گزینه ۳پاسخ تقریبی پرسش و گزینه ۴ پاسخ دقیق آن با ماشین حساب است ! *(پاسخ سازمان سنجش گزینه ۳ می‌باشد)*

داده‌های مسئله به صورت زیر است:

$$P_{bit} = 10^{-4}, R = 1.5\,Mbps, T_P = 5\,msec, H = 100\,bit$$

در رابطه راندمان سیستم پنجره لغزان، اگر اندازه پنجره ارسال به طور مناسب انتخاب شود ($W \geq 1 + 2a$) راندمان برابر یک می‌شود. یعنی اندازه بزرگ پنجره می‌تواند تأخیر انتشار و حتی انتقال Ack و زمان پردازش را جبران کند اما اندازه پنجره هر چقدر بزرگ باشد باز نمی‌تواند سربار Header و اتلاف ناشی از خطای کانال را جبران کند و درنتیجه راندمان به صورت زیر خواهد بود:

$$P_{Frame} = 1 - (1 - P_{bit})^L = 1 - (1 - 10^{-4})^L$$

$$U_{SR} = \left(\frac{L - H}{L}\right)(1 - P_{Frame}) = \left(1 - \frac{100}{L}\right)(1 - 10^{-4})^L$$

برای اینکه مقدار این رابطه حداکثر شود، باید مشتق آن نسبت به Lبرابر صفر باشد:

$$\frac{\mathrm{d}}{\mathrm{dL}} U_{SR} = \left(\frac{100}{L^2}\right)(1 - 10^{-4})^L + (1 - 10^{-4})^L \ln(1 - 10^{-4})\left(1 - \frac{100}{L}\right) = 0$$

اگر استفاده از ماشین حساب آزاد بود، راحت ترین راه این بود که چهار جواب تستی را در رابطه بگذاریم و ماکسیمم آنرا پیدا کنیم:

$$\left(\frac{700}{800}\right)(1 - 10^{-4})^{800} = \frac{7}{8} \times 0.9231 = 0.807723$$

$$\left(\frac{800}{900}\right)(1 - 10^{-4})^{900} = \frac{8}{9} \times 0.9139 = 0.812379$$

$$\left(\frac{900}{1000}\right)(1 - 10^{-4})^{1000} = \frac{9}{10} \times 0.9048 = 0.814349$$

$$\left(\frac{1000}{1100}\right)(1 - 10^{-4})^{1100} = \frac{10}{11} \times 0.8958 = 0.814390$$

حداکثر این رابطه با L=1100 به دست می‌آید و مثلاً برای اطمینان شما با L=1200 نیز آنرا به دست آورده‌ایم که کمتر شده است:

$$\left(\frac{1100}{1200}\right)(1 - 10^{-4})^{1200} = \frac{11}{12} \times 0.8869 = 0.813005$$

از آنجا که در جلسه آزمون استفاده از ماشین حساب غیرمجاز است منظور طراح این بوده است که از رابطه تقریبی زیر برای خطای فریم استفاده کنیم:

$$U_{SR} \approx \left(1 - \frac{100}{L}\right)(1 - 10^{-4}L) = 1 - 10^{-4}L - \frac{100}{L} + 0.01 = 1.01 - \frac{100}{L} - \frac{L}{10000}$$

$$\frac{d}{dL} U_{SR} = \frac{100}{L^2} - \frac{1}{10000} = 0 \rightarrow L^2 = 1000000 \rightarrow L = 1000$$

اگرچه با توجه به نزدیکی اعداد (در حد چهار رقم اعشار!) نمی‌توان به رابطه تقریبی اعتماد کرد و دیدیم جواب آن با جواب رابطه دقیق مطابقت نداشت، به هر حال بدون ماشین حساب گزینه ۳ به دست می‌آید.

۷. گزینه ۱ صحیح است.

داده‌های مسئله به صورت زیر است (زمان پردازش در مبدأ و مقصد داده نشده و برابر صفر در نظر گرفته شده است):

$$L = n_f = 160\ Byte, H = n_o = 16\ Byte,\ n_a = 16\text{Byte}, T_p = 241\ \text{msec}, T_{proc} = 0, R = 64\text{Kbps}$$

راندمان پنجره لغزان در کتاب‌ها به شکل‌های مختلف نوشته شده و در اینجا سه شکل آنرا نوشته‌ایم تا خواننده دچار مشکل نشود:

$$U_{Sliding\,window} = \frac{W \times \frac{n_f - n_o}{R}}{2T_p + 2T_{proc} + \frac{n_f}{R} + \frac{n_a}{R}} = \frac{W \times \frac{n_f}{R} \times \frac{n_f - n_o}{n_f}}{2T_p + 2T_{proc} + \frac{n_f}{R} + \frac{n_a}{R}} = \frac{W \times T_F \times \frac{L - H}{L}}{2T_p + 2T_{proc} + T_F + T_{ACK}}$$

در نتیجه خواهیم داشت:

$$U_{Sliding\,window} = \frac{W \times \frac{n_f}{R} \times \frac{n_f - n_o}{n_f}}{2T_p + 2T_{proc} + \frac{n_f}{R} + \frac{n_a}{R}} = \frac{W \times \frac{160 \times 8}{64 \times 10^3} \times \frac{160 - 16}{160}}{2 \times 241 \times 10^{-3} + \frac{160 \times 8}{64 \times 10^3} + \frac{16 \times 8}{64 \times 10^3}}$$
$$= \frac{W \times 18 \times 10^{-3}}{504 \times 10^{-3}} = \frac{W}{28}$$

اما در مسئله گفته شده که شماره ترتیب ارسال یک عدد ۳ بیتی است، بنابراین تعداد شماره ترتیب $2^3 = 8$ است.

در Go Back N ، پنجره سمت فرستنده برابر W و پنجره سمت گیرنده برابر 1 و مجموع آنها که تعداد شماره ترتیب‌های لازم را تشکیل می‌دهد W+1 است. پس داریم:

$$Sequence\ Number = 8 = W_{GBN} + 1 \rightarrow W_{GBN} = 7$$

در Selective Repeat، پنجره سمت فرستنده برابر W و پنجره سمت گیرنده نیز برابر W و مجموع آنها که تعداد شماره ترتیب‌های لازم را تشکیل می‌دهد 2W است:

$$Sequence\ Number = 8 = 2 \times W_{SR} \rightarrow W_{SR} = 4$$

حال برای محاسبه راندمان واقعی داریم:

$$U_{GBN} = \frac{W}{28} = \frac{7}{28} = .25 \times 100\% \rightarrow \quad U_{GBN} = 25\%$$
$$U_{SR} = \frac{W}{28} = \frac{4}{28} = \frac{1}{7} = .143 \times 100\% \rightarrow \quad U_{GBN} = 14.3\%$$

پرسش‌های فصل ۶

الف) WiFi

۱. کدامیک از استانداردهای زیر در مورد پروتکل برای شبکه‌های محلی بی‌سیم است؟ (IT – سراسری ۸۳)

۱) IEEE 802.11 ۲) IEEE 802.15 ۳) IEEE 802.3 ۴) IEEE 802.16

ب) CSMA و Ethernet

۲. در پروتکل دسترسی به رسانه CSMA/CD اگر طول کانال ۲۵۰۰ متر ، سرعت انتشار $1 * 10^8$ متر در ثانیه و نرخ ارسال داده ۱۰۰ مگابیت در ثانیه باشد، حداقل اندازه فریم‌ها چقدر است؟ (IT – سراسری ۸۳)

۱) ۲۲ بایت ۲) ۶۴ بایت ۳) ۲۵۶ بایت ۴) ۶۲۵ بایت

۳. در توپولوژی باس با پروتکل CSMA/CD فرض کنید طول کانال ۲۵۰۰ متر و نرخ ارسال ۱۰۰ مگابیت در ثانیه باشد. در بدترین حالت، پس از شروع به ارسال یک فریم تا لحظه کشف تصادم، چند بیت داده خراب می‌شود (سرعت انتشار امواج در سیم ۲۰۰ هزار کیلومتر در ثانیه فرض شود) (IT – سراسری ۸۵)

۱) ۵۰۰۰ بیت ۲) ۲۵۰۰ بیت ۳) ۱۲۵۰ بیت ۴) ۵۰۰ بیت

۴. یک روش کنترل دسترسی به رسانه می‌تواند استفاده از مالتی پلکس کردن زمانی ثابت باشد. در این روش به هر ایستگاه یک Slotزمانی در هر سیکل اختصاص داده می‌شود. اگر فرض کنیم اندازه هرSlotمدت زمان لازم برای ارسال 100بیت به علاوه تاخیر انتشار انتها به انتها باشد و با در نظر گرفتن اینکه نرخ ارسال داده‌ها 10 Mbps، طول کانال $8\,Km$ و سرعت انتشار امواج $2 * 10^8\,m/s$باشد ، اگر تعداد 100ایستگاه داشته باشیم حداکثر نرخ ارسال هر ایستگاه چقدر است؟ (IT – سراسری ۸۶)

۱) 20 Kbps ۲) 25 Kbps ۳) 100 Kbps ۴) 50 Kbps

۵. در شبکه‌های Ethernet (استاندارد IEEE 802.3) ، هر ایستگاه زمان backoff را از رابطه $k * t_{minislot}$ محسابه می‌کند. اگر ایستگاه A ، k را از مجموعه {۳و۲و۱و۰} انتخاب کند. چه تعداد تصادم توسط ایستگاه A تشخیص داده شده است؟ (IT – سراسری ۸۸)

۱) ۱ ۲) ۲ ۳) ۳ ۴) ۴

ج) ALOHA

۶. فرض کنید N ایستگاه دارای یک کانال مشترک با نرخ ۶۴ کیلوبیت بر ثانیه با روش کنترل دسترسی ALOHA هستند. اگر هر ایستگاه به طور متوسط نرخ ارسال ۴۶ بایت در ثانیه داشته باشد، حداکثر N چقدر می‌تواند باشد؟ (IT – سراسری ۸۷)

۱) ۱۲۸ ۲) ۶۴ ۳) ۳۲ ۴) ۱۶

۷. ۳۰۰۰ ایستگاه برای تبادل داده‌ها از یک کانال مشترک با نرخ ارسال ۱۲ مگابیت در ثانیه به روش Pure ALOHA استفاده می‌کنند. اگر طول بسته‌ها ۱۰۰ بایت باشد و هر ایستگاه ۵ بسته در ثانیه ارسال کند، حداکثر گذردهی در این پیوند ارتباطی چقدر است؟ (IT – سراسری ۸۹)

۱) e^{-1} ۲) $0.5e^{-1}$ ۳) $0.5e^{-0.5}$ ۴) e^{-2}

۸. ده‌هزار ایستگاه رزرو بلیط هواپیما، برای استفاده از یک کانال واحد به روش Slotted Aloha با هم رقابت می‌کنند. هر ایستگاه به طور متوسط ۱۸ تقاضا در هر ساعت خواهد داشت. برش‌های زمانی (time slot) ۱۰۰ میکروثانیه‌ای هستند. گذردهی در این کانال برابراست با: (IT – سراسری ۸۸)

۱) $\frac{1}{200}e^{-\frac{1}{200}}$ ۲) $\frac{1}{20}e^{-\frac{1}{20}}$ ۳) $\frac{1}{200}e^{-\frac{1}{100}}$ ۴) $\frac{1}{20}e^{-\frac{1}{20}}$

د) Token Ring

۹. فرض کنید یک شبکه Token Ring **با توپولوژی فیزیکی ستاره با ۱۰۰۰ ایستگاه داریم که فاصله هر ایستگاه تا** MAU (Multiple Access Unit) **۱۰۰ متر ، نرخ ارسال ۴ مگابایت در ثانیه ، اندازه فریم‌های داده ۱۰۰۰ بایت باشد. اگر فرض کنیم که سرعت انتشار امواج** $2 * 10^8$ **متر بر ثانیه و تاخیر در هر اسیتگاه ۴ بیت باشد. کارایی این شبکه تقریباً برابر است با: (IT – سراسری ۸۷)**

۱) ٪۸۰ ۲) ٪۶۷ ۳) ٪۵۷ ۴) ٪۵۰

۱۰. در استاندارد IEEE802.8، (Token Ring) **ایستگاهی که در حالت ارسال است پس از دریافت فریم ارسالی خود مشاهده می‌کند بیت‌های** A **و** C **در فیلد وضعیت فریم** (FS) **به ترتیب ۱ و ۰ می‌باشند. این وضعیت نشان‌دهنده آن است که: (IT – سراسری ۸۶)**

۱) ایستگاه گیرنده در شبکه وجود دارد و توانسته فریم را دریافت کند

۲) ایستگاه گیرنده در شبکه وجود ندارد و نتوانسته فریم را دریافت کند

۳) ایستگاه گیرنده در شبکه وجود دارد و بدلیل وجود خطا نتوانسته فریم را دریافت کند

۴) ایستگاه گیرنده در شبکه وجود دارد و بدلیل نامشخص نتوانسته فریم را دریافت کند

پاسخ پرسش‌های فصل ۶

۱. گزینه ۱ صحیح است.

۲. گزینه ۴ صحیح است.

داده‌های مسئله به صورت زیر است:

$$D = 2500\,m \quad , \quad V = 1 * 10^8 \frac{m}{s} \quad , \quad R = 100Mbps = 10^8 bps$$

بنابراین داریم:

$$T_p = \frac{D}{V} = \frac{2500}{1 * 10^8} = 25 * 10^{-6} s \rightarrow RTT = 2T_p = 50 * 10^{-6}$$

$$\frac{L}{R} \geq 2\frac{D}{V} \rightarrow \frac{L_{min}}{R} = 2\frac{D}{V} = \text{RTT} = 50 * 10^{-6} \rightarrow L_{min} = 50 * 10^{-6} * 10^8 = 5000 \text{ bit} = \frac{5000}{8} Byte = 625\ Byte$$

۳. گزینه ۲ صحیح است.

داده‌های مسئله به صورت زیر است:

$$D = 2500\,m \quad , \quad V = 2 * 10^8 \frac{m}{s} \quad , \quad R = 100Mbps = 10^8 bps$$

بنابراین داریم:

$$T_p = \frac{D}{V} = \frac{2500}{2 * 10^8} = 12.5 * 10^{-6} s \rightarrow RTT = 2T_p = 25 * 10^{-6}$$

$$\frac{L}{R} \geq 2\frac{D}{V} \rightarrow \frac{L_{min}}{R} = 2\frac{D}{V} = \text{RTT} = 25 * 10^{-6} \rightarrow L_{min} = 25 * 10^{-6} * 10^8 = 2500 \text{ bit}$$

۴. گزینه ۱ صحیح است.

داده‌های مسئله به صورت زیر است

$$\text{R} = 10\text{Mbps}, \text{D} = 8\ \text{Km}, \text{V} = 2 * 10^8 \frac{\text{m}}{\text{s}}, \text{n} = 100$$

صورت مسئله گفته است ، زمان Slot یعنی T_{Slot} برابر با مدت زمان ارسال 100 بیت به علاوه تاخیر انتشار انتها به انتها (یعنی T_p) است.

بنابراین داریم:

$$T_{Slot} = T_p + T_{t-100} = \frac{D}{V} + \frac{100}{R} = \frac{8 \times 10^3}{2 \times 10^8} + \frac{100}{10^7} = 5 * 10^{-5}\ s$$

یعنی زمان هر Slot ، $5 * 10^{-5}$ است. حال باید ببینیم، در هر ثانیه چند Slot داریم (تناسب) :

$$\begin{array}{cc} sec & Slot \\ 5 * 10^{-5} & 1 \\ 1 & x \end{array} \rightarrow x = 2 * 10^4$$

یعنی در هر ثانیه $2 * 10^4$ ، Slot وجود دارد

باید ببینیم سهم هر ایستگاه چقدر می‌شود:

$\frac{2*10^4}{n} = \frac{2*10^4}{100} = 200$ یعنی به هر ایستگاه ، ۲۰۰ Slot می‌رسد.

باید دقت شود، نوع Multiplexingزمانی است، بنابراین در هر لحظه فقط یک استگاه می‌تواند اطلاعات را ارسال کند. (کل پهنای باند به او تعلق دارد)، از طرفی بر طبق صورت مسئله اندازهSlotهر کانال ارتباطی به اندازه ارسال ۱۰۰ بیت به علاوه T_p است. (که T_pبرای تمامی بیت‌ها اتفاق می‌افتد) پس انگار هر کانال در بهترین حالت می‌تواند همان 100 بیت مربوط ارسال کند. پس حداکثر سرعت در هر ایستگاه ، میزان تعداد Slotاش (*200*) ضربدر تعداد *100* بیت می‌شود : $200 * 100 = 20\ Kbps$

۵. گزینه ۲ صحیح است.

کلاً از بازه $\{0, 2^k - 1\}$ انتخاب خواهد شد.

۶. گزینه ۳ صحیح است.

چه زمانی N حداکثر است؟ وقتی که راندمان در بیشترین حالت باشد. داریم:

$R_{eff} = U_{ALOHA} * R$

از طرفی باید $U_{ALLOHA}^{Max} = 0.184$ و بنابراین:

$U_{ALOHA}^{Max} = 0.184 \rightarrow \frac{R_{eff}}{R} = 0.184 \rightarrow \frac{N*46*8}{64*10^3} = 0.184 \rightarrow N = 32$

۷. گزینه ۴ صحیح است.

داده‌های مسئله به صورت زیر است

$R = 12\ Mbps\ , L = 100\ Byte\ , \lambda = 5\ , n = 3000$

تعداد ارسال تمامی ایستگاه‌ها در واحد زمان (در اینجا ثانیه) $G = \frac{n\lambda L}{R} = \frac{3000*5*(100*8)}{12*10^6} = 1$

و داریم:

$U_{ALLOHA} = Ge^{-2G} = e^{-2}$

۸. گزینه ۱ صحیح است.

$$\begin{array}{lll} Request & s & \\ 18*10^4 & 3600 & \rightarrow x = 50 \\ x & 1 & \end{array}$$

یعنی تمامی ایستگاه‌ها (روی هم) ۵۰ درخواست در ثانیه تولید می‌کنند

$$\begin{array}{lll} Request & s & \\ 50 & 1 & \rightarrow x = \frac{1}{200} \\ x & 100*10^{-6} & \end{array}$$

یعنی تمامی ایستگاه‌ها (روی هم) به طور میانگین $\frac{1}{200}$ درخواست در هر Slot تولید می‌کنند که همان G است.

داریم: $U_{Sloted\ ALOHA} = Ge^{-G} = \frac{1}{200}e^{-\frac{1}{200}}$

۹. گزینه ۴ صحیح است.

باید دقت شود که در صورت سوال گفته شده این شبکه Token Ring از MAU استفاده می‌کند. باید دقت کرد که اگرچه یک سیم بین هر ایستگاه و دستگاه MAU قرار دارد اما، سیگنال‌ها دوبار از این سیم یا کابل عبور می‌کنند (یکبار برای ورود به هر ایستگاه و یکبار برای خروج از آن). بنابراین از آنجا که فاصله بین هر ایستگاه و MAU ، ۱۰۰ متر ذکر شده، پس ۲۰۰=۱۰۰×۲ باید در نظر گرفته شود.

داده‌های مسئله به صورت زیر است:

$$n = 1000\ ,D = (2 * 100) * n = 2 * 10^5\ ,R = 4\ Mbps\ ,L = 1000\ Byte\ ,V = 2 * 10^8\ ,T_{Station} = \frac{b}{R} = \frac{4}{4 * 10^6} = 10^{-6}\ s$$

دقت دوم این است که تاخیر انتشار Token Ring ، نباید به صورت $2T_P$ در نظر گرفته شود. علت این است که در Ring برای رسیدن دوباره سیگنال از فرستنده به سمت خودش، نیازی نیست دوبار طول کانال طی شود بنابراین داریم:

$$T_P = \frac{D}{V} = \frac{2 * 10^5}{2 * 10^8} = 10^{-3}\ s$$

$$T_{Ring} = T_P + n * T_{Station} = 10^{-3} + 1000 * 10^{-6} = 2 * 10^{-3}\ s$$

$$T_F = \frac{L}{R} = \frac{1000 * 8}{4 * 10^6} = 2 * 10^{-3}\ s$$

$$U_{Ring} = \frac{T_F}{T_O} = \frac{T_F}{T_F + T_{Ring}} = \frac{2 * 10^{-3}}{2 * 10^{-3} + 2 * 10^{-3}} = 0.5$$

۱۰. گزینه ۴ صحیح است.

پرسش‌های فصل ۷

الف) مدل‌های سوئیچینگ

۱. کدامیک از موارد زیر در مورد تکنیک انتقال سوییچینگ بسته‌ای صحیح نمی‌باشد؟ (IT - سراسری ۸۵)

۱) بالا بردن کیفیت سرویس
۲) استفاده مناسب از منابع شبکه
۳) پشتیبانی مؤثر از سرویس‌های پیام کوتاه
۴) پشتیبانی مؤثر از ترافیک‌های با نرخ بیت متغیر

۲. کدام‌یک از عبارات در مورد مکانیزهای مدیریت ترافیک در شبکه‌های کامپیوتری با تکنیک انتقال سوییچینگ بسته‌ای صحیح نمی‌باشد؟ (IT - سراسری ۸۹)

۱) کنترل ازدحام
۲) مسیریابی با محدودیت به منظور حداکثر نمودن گذردهی
۳) مدیریت صف و زمانبندی بسته‌ها
۴) مسیریابی کوتاه‌ترین مسیر

ب) کنترل ازدحام

۳. کدام‌یک از عبارات زیر در مورد روش‌های کنترل ازدحام پیشگیرانه (prevention) و واکنشی (reaction) در شکبه‌های کامپیوتری صحیح می‌باشد؟ (IT - سراسری ۸۹)

۱) در روش‌های کنترل ازدحام پیشگیرانه استفاده از بهینه ظرفیت پیوندهای شبکه صورت می‌پذیرد.
۲) در روش‌های کنترل ازدحام واکنشی کنترل پذیرش مکالمه وجود دارد
۳) در روش‌های کنترل ازدحام واکنشی کیفیت سرویس‌دهی تضمین نمی‌شود
۴) در روش‌های کنترل ازدحام پیشگیرانه دریافت بازخورد از وضعیت ازدحام وجود دارد.

ج) مسیریابی

۴. کدامیک از موارد زیر از ویژگی‌های الگوریتم‌های مسیریابی مبدأ (Source Routing) نمی‌باشد؟ (IT - سراسری ۸۵)

۱) کنترل حفظ ترتیب ارسال بسته‌ها توسط مبدأ
۲) عدم نیاز به نگهداری جداول میسریابی در مسیریاب‌های میانی
۳) عدم نیاز به انجام عملیات مسیریابی توسط مسیریاب‌های میانی
۴) قابلیت تطبیق بالا در برابر تغییرات توپولوژی شبکه به دلیل خرابی گره‌ها و پیوندها

۵. کدامیک از موارد زیر در مورد روش‌های مسیریابی بردار فاصله (Distance Vector) و وضعیت پیوند (Link State) صحیح نمی‌باشد؟ (IT - سراسری ۸۵)

۱) در الگوریتم‌های مسیریابی بردار فاصله در صورتی می‌توان بهترین مسیر به سمت گره مقصد را محاسبه کرد که هزینه‌های گره‌های همسایه به سمت مقصد را داشته باشیم.
۲) در الگوریتم‌های مسیریابی بردار فاصله سرعت همگرایی در برابر تغییرات نسبت به الگوریتم‌های مسیریابی وضعیت کمتر است.
۳) در الگوریتم‌های مسیریابی وضعیت پیوند پایگاه داده‌ای از وضعیت پیوندهای شبکه در هر گره نگهداری می‌شوند.
۴) در الگوریتم‌های مسیریابی وضعیت پیوند هر گره نیازی به دانستن توپولوژی شبکه ندارد.

۶. در الگوریتم مسیریابی بردار فاصله (Distance Vector) **فرض کنید یک مسیریاب همانند** A**دقیقاً به سه مسیریاب** B**و** C**و** D**در ارتباط مستقیم است. طبق جداول ارسالی همسایه‌ها برای** A**هزینه رسیدن به گره** J **در شبکه به شرح زیر گزارش شده است:**

$(B \to J)20\,ms$ $(C \to J)75\,ms$ $(D \to J)110\,ms$

هزینه A تا همسایه‌ها طبق آمار زیر اندازه‌گیری شده است.

$(A \to B)95\,ms$ $(A \to C)90\,ms$ $(A \to D)60\,ms$

در جدول مسیریابی A هزینه و پورت رسیده به گره J کدامیک از گزینه‌های زیر درج خواهد شد؟ (IT - سراسری ۸۵)

۱) B و ۲۰ ۲) C و ۷۵ ۳) B و ۱۱۵ ۴) C و ۹۰

۷. شبکه فرضی زیر را در نظر بگیرید. اعداد بر روی هر لینک بیانگر هزینه آن لینک می‌باشد. چنانچه جدول مسیریابی مسیریاب‌های شبکه به صورت زیر باشد، در این صورت جدول جدید مسیریابی A **با استفاده از روش بردار فاصله کدام است؟** (IT - **سراسری ۸۸**)

مسیریاب A

گام بعدی	فاصله	مقصد
B	۵	net 1
C	۴	net 2
B	۵	net 3
D	۶	net 4
C	۵	net 5

مسیریاب D

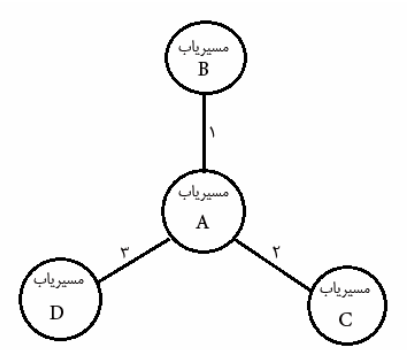
گام بعدی	فاصله	مقصد
A	۲	net 1
I	۱	net 3
H	۳	net 4
H	۱	net 8

مسیریاب C

گام بعدی	فاصله	مقصد
F	۲	net 2
A	۷	net 3
F	۳	net 5
G	۱	net 7

مسیریاب B

گام بعدی	فاصله	مقصد
K	۴	net1
S	۴	net 3
E	۳	net 6



۱)

گام بعدی	فاصله	مقصد
B	۵	net 1
C	۴	net 2
B	۵	net 3
D	۶	net 4
C	۵	net 5
B	۴	net 6

۳)

گام بعدی	فاصله	مقصد
B	۵	net 1
C	۴	net 2
D	۴	net 3
D	۶	net 4
C	۵	net 5
B	۴	net 6
B	۳	net 7

۲)

گام بعدی	فاصله	مقصد
B	۵	net 1
C	۴	net 2
D	۴	net 3
D	۶	net 4
C	۵	net 5
B	۴	net 6
B	۳	net 7
D	۴	net 8

۴)

گام بعدی	فاصله	مقصد
B	۵	net 1
C	۴	net 2
D	۴	net 3
D	۶	net 4
C	۵	net 5
B	۴	net 6
D	۴	net 7

۸. کدام‌یک از گزینه‌های زیر در مورد روش‌های مسیریابی مبتنی بر Datagram صدق می‌کند؟ (IT – سراسری ۸۵)

۱) بسته‌ها الزاماً به ترتیب ارسال به مقصد خواهند رسید.

۲) هر بسته به آدرس کامل و سراسری مبدأ و مقصد نیاز دارد.

۳) احتمال گم شدن بسته‌ها ناشی از اشتباه در عمل مسیریابی وجود ندارد.

۴) قبل از ارسال بسته‌ها منابع لازم در زیر شبکه رزور و هماهنگ خواهد شد.

۹. کدام‌یک از موارد زیر جزو معیارهای ارزیابی الگوریتم‌های مسیریابی نمی‌باشد؟ (IT – سراسری ۸۵)

۱) تحویل سریع و صحیح بسته‌ها

۲) قابلیت تطبیق با تغییرات توپولوژی شبکه

۳) قابلیت ایجاد ، نگهداری و رهاسازی اتصالات بین هر زوج گره مبدأ و مقصد

۴) توانایی هدایت بسته‌ها به دور از پیوندهایی که به طور موقتی دارای ازدحام هستند.

پاسخ پرسش‌های فصل ۷

۱ ـ گزینه ۱ صحیح است.

۲ ـ گزینه ۴ صحیح است.

۳ ـ گزینه ۳ صحیح است.

۴ ـ گزینه ۴ صحیح است.

۵ ـ گزینه ۴ صحیح است.

۶ ـ گزینه ۳ صحیح است.

کمترین طول مسیر از طریق گره B به دست می‌آید:

$$A \xrightarrow{20} B \xrightarrow{95} J \quad + \quad \Rightarrow \quad A \xrightarrow{115} J$$

۱۰. گزینه ۲ صحیح است.

در شکل، A با D با فاصله ۳ وجود دارد و مسیریاب D با net 8 هم با هزینه ۱ وجود دارد. بنابراین A با هزینه ۴ به net 8 ارتباط دارد. همچنین در این سوال می‌توان دقت کرد که فقط در گزینه ۲، net 8 وجود دارد.

۱۱. گزینه ۲ صحیح است.

۱۲. گزینه ۳ صحیح است.

پرسش‌های فصل ۸

الف) IP

۱. نقش فیلد Time To Live (TTL)در سرآمد (Header) بسته‌های IP چیست؟ (IT – سراسری ۸۵)

۱) مشخص کننده حداکثر زمانی که گیرنده باید به فرستنده پاسخ دهد.

۲) مشخص کننده حداکثر تعداد گامی که بسته می‌تواند در شبکه طی کند تا به مقصد برسد.

۳) مشخص کننده حداکثر زمانی که مسیریاب‌های میانی باید بسته را به سمت مقصد ارسال کند.

۴) مشخص کننده حداکثر زمانی که در صورت از بین رفتن بسته، مسیریاب میانی باید آنرا به مبدأ اطلاع دهد.

۲. فرض کنید یک مسیریاب بسته‌ای به طول ۱۶۸۰ بایت دریافت می‌کند که باید از طریق شبکه‌ای با MTU ، ۵۷۶ بایت به سمت مقصد هدایت (forward) کند. این بسته‌ها حداقل به چند تکه (fragment) شکسته خواهد شد؟ (IT – سراسری ۸۹)

۱) ۴ ۲) ۵ ۳) ۳ ۴) ۶

۳. دلایل سلسله مراتبی کردن آدرس IP به NetID و HostID چیست؟ (IT – سراسری ۸۵)

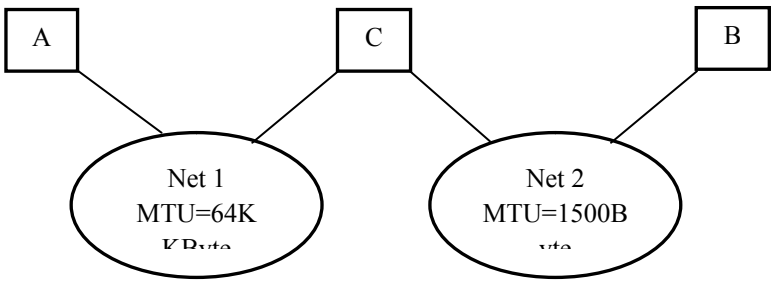
۱) استفاده مؤثر از فضای آدرس‌دهی

۲) اختصاص مؤثر آدرس‌های IP به کاربران مختلف

۳) سهولت انجام عملیات مسیریابی و کاهش اندازه جداول مسیریابی

۴) هیچکدام

۴. با توجه به شکل زیر بیان کنید حداکثر اندازه بسته‌های IP دریافتی در میزبان‌های A و B و مسیریاب C به ترتیب چقدر است؟ (IT – سراسری ۸۶)



۱) ۱۵۰۰ بایت ، ۱۵۰۰ بایت ، ۱۵۰۰ بایت

۲) ۶۴ کیلوبایت ، ۱۵۰۰ بایت ، ۶۴ کیلو بایت

۳) ۱۵۰۰ بایت ، ۱۵۰۰ بایت ، ۶۴ کیلوبایت

۴) ۶۴ کیلوبایت ،۶۴ کیلوبایت ، ۶۴ کیلو بایت

۵. یک مسیر یاب IP را در نظر بگیرید که بسته‌ای حاوی ۶۰۰ بایت داده را دریافت می‌کند. این مسیریاب باید این بسته را به شبکه‌ای با حداکثر واحد انتقال (MTU) ۲۰۰ بایت ارسال کند. با فرض اینکه سرآیند (Header) بسته‌های IP ۲۰ بایت است، کدام یک از گزینه‌های زیر صحیح است؟ (IT - سراسری ۸۷)

(۱

	Total Length	ID	DF	MF	Fragment Office
Original Packet	600	X	0	0	0
Fragment 1	200	X	0	1	0
Fragment 2	200	X	0	1	200
Fragment 3	200	X	0	0	400

(۲

	Total Length	ID	DF	MF	Fragment Office
Original Packet	620	X	0	0	0
Fragment 1	196	X	0	1	0
Fragment 2	196	X	0	1	176
Fragment 3	196	X	0	1	352
Fragment 4	92	X	0	0	528

(۳

	Total Length	ID	DF	MF	Fragment Office
Original Packet	600	X	0	0	0
Fragment 1	200	X	0	1	0
Fragment 2	200	X	0	1	25
Fragment 3	200	X	0	0	50

(۴

	Total Length	ID	DF	MF	Fragment Office
Original Packet	620	X	0	0	0
Fragment 1	196	X	0	1	0
Fragment 2	196	X	0	1	22
Fragment 3	196	X	0	1	44
Fragment 4	92	X	0	0	66

ب) CIDR

۶. اگر جدول مسیر یابی در یک مسیریاب با توانایی CIDR به صورت زیر باشد، گام بعدی برای بسته‌ای با آدرس مقصد 196.94.19.135 چیست؟ (IT - سراسری ۸۳)

Net	Mask	Next Hop
196.80.0.0	255.240.0.0	A
196.96.0.0	255.240.0.0	B
196.104.0.0	255.252.0.0	C
128.0.0.0	128.0.0.0	D
64.0.0.0	192.0.0.0	E

۱) A

۲) B

۳) C

۴) D

۷. اگر جدول مسیریاب با توانایی CIDR (Classless Interdomain Routing) **به صورت زیر باشد ، گام بعدی برای بسته‌ای با آدرس مقصد** 196.94.19.135 **چیست؟** (IT – **سراسری ۸۷**)

Net	Mask	Next Hop
196.80.0.0	255.240.0.0	A
196.96.0.0	255.240.0.0	B
128.0.0.0	128.0.0.0	C
64.0.0.0	196.0.0.0	D

۱) A ۲) B ۳) C ۴) D

ج) ICMP

۸. پروتکل ICMP**چیست و در چه لایه‌ای قرار دارد؟** (IT – **سراسری ۸۶**)

۱) مدیریت لایه انتقال و در لایه انتقال قرار دارد ۲) مدیریت لایه اینترنت و در لایه اینترنت قرار دارد

۳) مدیریت لایه کاربرد و در لایه کاربرد قرار دارد ۴) کنترل پیام لایه اینترنت و در لایه اینترنت قرار دارد

د) ARP

۹. کدام‌یک از موارد زیر در مورد پروتکل ARP **صحیح نمی‌باشد** (IT – **سراسری ۸۵**)

۱) پروتکل ARP آدرس فیزیکی را با استفاده از یک تابع نگاشت بدست آورد.

۲) پروتکل ARP در تکنولوژی شبکه‌های مختلف (نظیر Ethernet و ATM) متفاوت است.

۳) هر درایه جدول ARP دارای طول عمر است و در صورتی که پس از مدتی هیچگونه فعالیتی نداشته باشد پاک خواهد شد.

۴) هیچکدام

ه) TCP

۱۰. فرض کنید برای انتقال یک فایل به اندازه یک مگابایت از TCP**بر روی یک پیوند با نرخ** 100**مگابیت در ثانیه و زمان** RTT100**میلی ثانیه استفاده می‌کنیم. اگر اندازه** Advertise Window**دریافت کننده** 64**کیلو بایت باشد، بافرض اینکه اندازه سگمنت برابر** 1**کیلو بایت است و هیچگونه ازدحام** (Congestion) **و از دست دادن** (Lost) **وجود ندارد، زمان ارسال این فایل چقدر خواهد بود؟** (IT – **سراسری ۸۶**)

۱) 0.1 ثانیه ۲) 1.5 ثانیه ۳) 1.6 ثانیه ۴)2.2 ثانیه

۱۱. نقش بیت SYN **در سرآیند سگمنت‌های پروتکل** TCP **چیست؟** (IT – **سراسری ۸۷**)

۱) برای درخواست خاتمه ارتباط است ۲) برای درخواست برقراری ارتباط است

۳) برای درخواست سکرون شدن یک طرف ارتباط است ۴)برای درخواست سنکرون شدن دو طرف ارتباط است

۱۲.در پروتکل TCP **در فاز** slow start **، اندازه پنجره ازدحام تا زمانی که اولیت از دست رفتن** (loss) **تشخیص داده می‌شود،** ..... (IT – **سراسری ۸۸**)

۱) هر RTT دوبرابر می‌شود ۲) هر RTT به اندازه یک MSS اضافه می‌شود

۳) هر RTT به اندازه MSS اضافه می‌شود. ۴) تغییری نمی‌کند

پاسخ پرسش‌های فصل ۸

۱. گزینه ۲ صحیح است.

۲. گزینه ۱ صحیح است.

اندازه Headerکه در MTUبه داده اضافه می‌شود ، ۲۰ بایت است ، پس داریم :

$$MTU = Data + Header \rightarrow 576 = Data + 20 \rightarrow Data = 556$$

$$\left\lceil \frac{1680}{556} \right\rceil = 4$$

بسته‌ها به این صورت ارسال می‌شوند : $(556 + 20) + (556 + 20) + (556 + 20) + (12 + 20)$

۳. گزینه ۳ صحیح است.

۴. گزینه ۳ صحیح است.

۵. گزینه ۴ صحیح است.

سرآیند را از میزان هر بسته کم می‌کنیم تا مشخص شود چقدر داده وجود دارد $200 - 20 = 180$

این میزان داده‌ها (با توجه به Offset مربوط به IP که ۸ بایتی است) چند Offset می‌شود $\left\lfloor \frac{180}{8} \right\rfloor = 22$

باید این تعداد ، چند بایتی باشند؟ $22 * 8 = 176$

بنابراین داریم: $600 = 176 + 176 + 176 + 72$

به هر کدام از این بسته‌ها هم ۲۰ بایت هدر اضافه می‌شود پس: $620 = 196 + 196 + 196 + 92$

برای محسابه Fragment Offset داریم :

اولین ۱۷۶ بایت که Fragment Offset ندارد. دومی $\frac{176}{8} = 22$ ، سومی $\frac{176+176}{8} = 44$ ، چهارمی $\frac{176+176+176}{8} = 66$

۶. گزینه ۱ صحیح است.

راه کلاسیک حل مسئله:باینری اعداد مسئله را به بدست می‌آوریم :

196.94.19.135=11000100.01011110.00010011.10000111

	Net	Mask	Next Hop			Net	Mask	Next Hop
1	196.80.0.0	255.240.0.0	A	-	1	11000100.01010000.0.0	11111111.11110000.0.0	A
2	196.96.0.0	255.240.0.0	B	>	2	11000100.01100000.0.0	11111111.11110000.0.0	B
3	196.104.0.0	255.252.0.0	C		3	11000100.01101000.0.0	11111111.11111100.0.0	C
4	128.0.0.0	128.0.0.0	D		4	10000000.0.0.0	10000000.0.0.0	D
5	64.0.0.0	192.0.0.0	E		5	01000000.0.0.0	1100000000.0.0	E

باید ببینیم حاصل *AND* کدام *Net* با *Mask* مربوط به خودش ، برابر با حاصل *AND* آدرس داده شده با *Mask* هر یک از *Net* های داده شده است (در این شبکه‌ها اصلا *Net*های 128.0.0.0 را محاسبه نمی‌کنیم)

	NetAND Mask
1	11000100.01010000.0.0
2	11000100.01100000.0.0
3	11000100.01101000.0.0
4	-
5	-

	IPAND Mask	Next Hop
1	11000100.01010000.0.0	A
2	11000100.01000000.0.0	B
3	11000100.00000000.0.0	C
4	-	D
5	-	E

راه تستی حل مسئله: به آدرس IPداده شده در مسئله و آدرس‌های داده شده در Routerدقت کنید. تنها گزینه ۱ می‌تواند صحیح باشد. علت این است: آدرس 196.94.19.135 با شبکه‌های 196.80.0.0 و 196.96.0.0 و 196.104.0.0 در عدد 196 مشترک‌اند. به عدد دوم (که معادل ۸ بیت دوم است) ، مراجعه می‌کنیم. عدد دوم آدرس داده شده در مسئله 94 و عدد دوم داده شده برای شبکه اول 80 ، برای شبکه دوم 96 و برای شبکه سوم 104 می‌باشد. بنابراین آدرس IP داده شده تنها می‌تواند در شبکه اول حضور داشته باشد. زیرا $80 < 94 < 96$. به عنوان مثال، در صورتی که می‌شد در شبکه دوم (196.96.0.0) قرار می‌گرفت، باید عدد دوم آن برابر یا بزرگتر از 96 می‌شد. که در سوال اینطور نیست. بنابراین در مسایل شبیه این، می‌توان اعداد را به ترتیب از سمت چپ به راست، به گونه‌ای که بیان شد، مقایسه کرد.

۷. گزینه ۱ صحیح است.

باینری اعداد مسئله را به بدست می‌آوریم :

196 .94 .19 . 135 = 11000100 .01011110 .00010011 . 10000111

	Net	Mask	Next Hop
1	196.80.0.0	255.240.0.0	A
2	196.96.0.0	255.240.0.0	B
3	196.104.0.0	255.252.0.0	C
4	128.0.0.0	128.0.0.0	D
5	64.0.0.0	192.0.0.0	E

->

	Net	Mask	Next Hop
1	11000100.01010000.0.0	11111111.11110000.0.0	A
2	11000100.01100000.0.0	11111111.11110000.0.0	B
3	11000100.01101000.0.0	11111111.11111100.0.0	C
4	10000000.0.0.0	10000000.0.0.0	D
5	01000000.0.0.0	1100000000.0.0	E

باید ببینیم حاصل *AND* کدام *Net* با *Mask* مربوط به خودش ، برابر با حاصل *AND* آدرس داده شده با *Mask* هر یک از *Net* های داده شده است (در این شبکه‌ها اصلا *Net*های 128.0.0.0 را محاسبه نمی‌کنیم)

	Net AND Mask
1	11000100.01010000.0.0
2	11000100.01100000.0.0
3	11000100.01101000.0.0
4	-
5	-

	IP AND Mask	Next Hop
1	11000100.01010000.0.0	A
2	11000100.01000000.0.0	B
3	11000100.00000000.0.0	C
4	-	D
5	-	E

۸. گزینه ۲ صحیح است.

۹. گزینه ۱ صحیح است.

۱۰. گزینه ۴ صحیح است.

۱۱. گزینه ۲ صحیح است.

۱۲. گزینه ۱ صحیح است.