مدرسان شریف

فصل اول

« مفاهیم پایه شبکه‌های کامپیوتری »

سال‌ها قبل از ایجاد و شکل‌گیری شبکه‌های کامپیوتری، از واژه شبکه، در حوزه‌های مختلف استفاده می‌شد (برای مثال شبکه راه آهن کشور). با این حال از اواسط قرن گذشته بود که شبکه‌های کامپیوتری رشد خود را آغاز کردند. به هر حال آنچه که در این کتاب با یکدیگر بررسی خواهیم نمود، شبکه‌های کامپیوتری می‌باشد. بنابراین از این جا به بعد منظور ما از «شبکه»، «شبکه‌های کامپیوتری» خواهد بود. قبل از شروع بحث، اجازه دهید تا ابتدا تعریفی را برای شبکه‌های کامپیوتری ارائه دهیم.

شبکه‌های کامپیوتری

شبکه کامپیوتری به مجموعه‌ای از تجهیزات (device) به هم مرتبط گفته می‌شود که توانایی تبادل داده و اطلاعات را با یکدیگر داشته باشند. به اعضای شبکه در اصطلاح «گره (node)» گفته می‌شود.

نکته۱: دقت کنید که منظور از «تجهیزات» یا گره، لزوماً کامپیوتر نیست. به‌عنوان مثال یک تلفن همراه یا لپ‌تاپ و یا چند کامپیوتر با چاپگر نیز می‌توانند با همدیگر تشکیل شبکه دهند.

تذکر۱: گاهی اوقات به جای واژه «گره»، از واژه «میزبان (host)» نیز استفاده می‌شود.

اهداف ایجاد شبکه

شاید این سوال برای شما هم به وجود آمده باشد که اصولاً چه نیازی به ایجاد و استفاده از شبکه‌های کامپیوتری وجود دارد؟ در ذیل، برخی از اهداف و کاربردهای شبکه را با همدیگر مرور خواهیم نمود. البته کاربرد شبکه به همین چند مورد محدود نیست و مواردی که در ادامه می‌آید رایج‌ترین آن‌ها می‌باشد.

به اشتراک گذاشتن منابع: منابع، می‌توانند هم به شکل سخت‌افزار باشند و هم نرم افزار. به‌عنوان مثالی برای منابع **سخت‌افزار**، می‌توان به جای آنکه برای هر کامپیوتر حافظه (یا CPU یا چاپگر) جداگانه‌ای در نظر گرفت، حافظه (یا CPU یا چاپگر) مشترکی برای آن‌ها ایجاد کرده و آن را به اشتراک گذاشت که با این کار در هزینه نیز صرفه‌جویی می‌شود.

از طرفی دیگر، منابع می‌توانند به شکل **نرم‌افزاری** نیز باشند. به‌عنوان مثال شرکتی را با 50 پرسُنل در نظر بگیرید. اگر کارمندان این شرکت برای انجام کارهای خود نیاز به نرم‌افزار خاصی داشته باشند، یک راه این است که پشت هر 50 کامپیوتر نشسته و آن نرم افزار خاص را روی تک‌تک دستگاه‌ها نصب نمود که مسلماً پروسه طولانی مدت خواهد بود. اما راه دیگر، به اشتراک گذاشتن آن نرم‌افزار خاص بر روی سرور شبکه شرکت است تا هر فردی که نیاز به آن داشته باشد، از طریق سرور کار خود را انجام دهد. به همین شکل می‌توان هر گونه داده یا اطلاعاتی را نیز که اعضای شرکت به آن نیاز دارند، از طریق شبکه به راحتی در اختیار آن‌ها قرار داد.

ایجاد ارتباط: یکی از اهداف مهم شبکه، ایجاد بستری مناسب برای امکان ارتباط بین افراد مختلف، در مکان‌ها و شرایط گوناگون و در یک کلام، انتقال داده است. پست الکترونیکی یا همان Email (مانند o.mohabati@gmail.com)، چَت، کنفرانس‌های ویدئویی، تلفن‌های اینترنتی و ... مثال‌هایی از این دست هستند.

همان‌طور که ذکر شد سرویس‌های ارائه شده توسط شبکه به همین چند مورد محدود نمی‌شود. به‌عنوان مثال می‌توان خدماتی از قبیل: خرید اینترنتی (تجارت الکترونیک)، موتورهای جستجو، آموزش الکترونیکی، بازی‌های شبکه‌ای و ... را نیز نام برد.

مثال۱: کدام مورد، از اهداف استفاده از شبکه به شمار می‌رود؟

۱) افزایش سرعت ۲) اشتراک منابع ۳) ایجاد ارتباط ۴) همه موارد

☑ **پاسخ:** گزینه «۴» دقت کنید که مواردی مانند افزایش سرعت، افزایش قابلیت اطمینان و سرگرمی نیز می‌توانند از اهداف دیگر شبکه باشند.

زیرشبکه (Subnet)

به مجموعه واسطه‌های میانی و کانال (لینک)ها، زیرشبکه (Subnet) گفته می‌شود. با این تعریف مشخص است که کاربرد اصلی زیرشبکه، انتقال داده‌ها است. منظور از واسطه‌های میانی، دستگاه‌هایی است که برای اتصال گره به شبکه از آن‌ها استفاده می‌شود (مانند کارت شبکه).

تذکر۲: در فصل‌های آتی تعاریف دیگری از زیرشبکه را خواهیم دید.

پروتکل

به مجموعه قوانین و قراردادهایی که بین فرستنده و گیرنده باید تنظیم شود تا بتوانند با هم ارتباط داشته باشند یا در اصطلاح زبان همدیگر را متوجه شوند، پروتکل گفته می‌شود. پروتکل وظایف فرستنده، گیرنده و نحوه ارسال و دریافت داده‌ها را دقیقاً مشخص می‌کند. از انواع پروتکل می‌توان به مواردی مانند: HTTP، FTP، TCP، IP و... اشاره کرد. در فصل‌های آینده بیش‌تر با وظایف پروتکل‌های مختلف آشنا خواهیم شد.

مثال۲: مجموعه قوانینی که باعث می‌شود دو طرف ارتباط با هم رابطه مناسب و مشخصی داشته باشند چه نامیده می‌شود؟

۱) DNS ۲) Subnet ۳) Protocol ۴) Hub

☑ **پاسخ:** گزینه «۳» به مجموعه قوانین و قراردادهایی که بین فرستنده و گیرنده باید تنظیم شود تا بتوانند با هم ارتباط داشته باشند یا در اصطلاح زبان همدیگر را متوجه شوند پروتکل گفته می‌شود.

شبکه‌های کامپیوتری را می‌توان بر اساس معیارهای مختلف طبقه‌بندی نمود. از جمله این معیارها، می‌توان به حوزه و وسعت جغرافیایی تحت پوشش، نحوه سرویس‌دهی و سرویس‌گیری و سیمی یا بی‌سیم بودن آن‌ها اشاره نمود. در ادامه، این موارد را بررسی می‌کنیم.

انواع شبکه از نظر وسعت ناحیه تحت پوشش

از این نظر شبکه‌ها را معمولاً به سه دسته LAN، MAN و WAN تقسیم می‌کنند.

شبکه‌های LAN (Local Area Network) معمولاً وسعت محدودی در حدود یک یا چند ساختمان دارند. حتماً تا به حال متوجه شده‌اید که در برخی نقاط شهر، امکان اتصال به اینترنت بی‌سیم وجود دارد. اغلبِ این شبکه‌ها، از نوع استاندارد IEEE 802.11 هستند که نوعی از شبکه‌های بی‌سیم LAN به شمار می‌روند. احتمالاً در دفتر آموزش دانشکده خود دیده‌اید که چندین کامپیوتر در یک اتاق به یکدیگر و یا به یک چاپگر متصل هستند. در این حالت نیز یک شبکه LAN ایجاد شده که در اکثر مواقع و در چنین حالاتی از پروتکل اِترنت برای برقراری ارتباط استفاده می‌کنند. از خصوصیات شبکه‌های LAN می‌توان به ساده بودن مدیریت، تعداد کم گره‌ها، ارزان بودن، نرخ انتقال بالا و نرخ خطای کم اشاره کرد.

تذکر۳: در مورد مفاهیمی همچون استاندارد 802.11 و پروتکل اِترنت در فصول بعدی توضیح داده خواهد شد.

شبکه‌های MAN (Metropolitan Area Network)، منطقه یک شهر را تحت پوشش خویش قرار می‌دهند. وایمکس (WiMax)که امروزه در کشور ما هم ایجاد شده مثال معروفی از شبکه‌های MAN می‌باشد.

در نهایت **شبکه‌های WAN (World Area Network)**، وسعتی در حد کشور و یا حتی جهان را دارند که از اتصال چندین LAN یا MAN به وجود می‌آیند. اینترنت بهترین مثال برای شبکه‌های WAN می‌باشد. در این شبکه‌ها برخلاف شبکه‌های محلی، مدیریت پیچیده، هزینه بالا و تعداد گره‌ها زیاد است.

در حقیقت اینترنت را می‌توان شبکه‌ای از شبکه‌ها فرض نمود که از اتصال میلیون‌ها شبکه به یکدیگر به وجود آمده است. برخی از رایج‌ترین کاربردهای اینترنت عبارتند از: پست الکترونیکی، موتورهای جستجو، خرید اینترنتی، حراج اینترنتی، ویدئو کنفرانس‌ها، انتقال فایل‌ها، جستجو در وب، بازی‌های تحت شبکه، تلفن اینترنتی، آموزش الکترونیکی (مجازی) و ...

لازم به ذکر است که برخی منابع در این طبقه‌بندی، شبکه‌های دیگری همچون شبکه‌های PAN و یا GAN را نیز در نظر می‌گیرند. **شبکه‌های PAN** (Personal Area Network) از شبکه‌های LAN کوچکتر بوده و وسعت آن‌ها از چندین متر (مثلاً دو سه متر) تجاوز نمی‌کند. به‌عنوان مثال وقتی شما از طریق بلوتوث یا اینفرارد (مادون قرمز) ارتباط برقرار می‌کنید، تشکیل یک شبکه PAN داده‌اید.

شبکه‌های GAN (Global area Network) نیز بزرگتر از WAN در نظر گرفته می‌شوند. معمولاً گستره WAN در حد یک کشور یا قاره در نظر گرفته می‌شود و گستره GAN در حد کره زمین.

انواع شبکه از نظر نحوه سرویس‌دهی (client/server و peer-to-peer)

برخی اوقات نحوه سرویس‌دهی شبکه را «**نرم افزار شبکه**» نیز می‌نامند. در این رابطه می‌توان دو نوع شبکه client/server و peer-to-peer را نام برد.

در **شبکه‌های** client/server، برخی از تجهیزات، نقش سرویس‌دهنده (**سرور**) و برخی دیگر نقش سرویس‌گیرنده (**کِلاینت**) را دارند. به عبارت دیگر هر عنصر شبکه یا سرویس‌گیرنده است یا سرویس‌دهنده. در این حالت باید روی دستگاه سرور، سیستم عامل خاصی نصب شده باشد (مثلاً Windows Server 2003,2008 و یا لینوکس) تا بتواند وظایف خود را در شبکه به درستی انجام داده و به درخواست‌های کلاینت پاسخ درستی دهد. مدیریت در شبکه‌های client/server به خوبی قابل پیاده‌سازی است و به علت وجود همین مدیریت، امنیت آن‌ها به طور معمول، بیش‌تر از شبکه‌های peer-to-peer است. چنانچه تعداد گره‌ها زیاد باشد، از این شبکه‌ها استفاده می‌شود. البته از آنجا که ممکن است با خرابی سرور، کل شبکه از کار بیفتد معمولاً از چندین سرور استفاده می‌شود تا در صورت بروز مشکل برای سرور اصلی، سرورهای دیگر برای سرویس‌دهی آمادگی داشته باشند.

تذکر۴: دقت کنید که منظور از سرور، لزوماً یک کامپیوتر پیشرفته نیست.

این تصور غلطی است که سرور لزوماً باید یک کامپیوتر بسیار قدرتمند باشد. حتی کامپیوتر خانگی شما با سیستم عامل Windows XP و یا مشابه آن نیز در برخی کاربردها می‌تواند نقش سرور را ایفا کند. علاوه بر این تعداد سرورها در شبکه لزوماً، یک عدد نیست. بدین معنی که در یک شبکه می‌توان سرورهای مختلفی را متصور بود از جمله: Web server، File Server، Database Server، Proxy Server ، DNS Server و ... .

در **شبکه‌های** peer-to-peer، هر دستگاه همزمان، ضمن اینکه از برخی دستگاه‌ها سرویس می‌گیرد، به برخی دیگر نیز سرویس ارائه می‌دهد. به عبارت دیگر یک دستگاه هم نقش سرویس‌دهنده را بازی می‌کند هم سرویس گیرنده را. بنابراین در این نوع از سرویس‌دهی، اعضای شبکه برتری خاصی نسبت به همدیگر ندارند.

از مزایای شبکه‌های peer-to-peer ، ارزان قیمت بودن آن‌ها است. ضمناً کار با آن‌ها از آنجا که به سیستم عامل خاصی نیاز ندارند، ساده است. اما عیب بزرگ آن‌ها محدودیت در تعداد گره‌ها (حداکثر 20 عدد) است. در این نوع از شبکه هر فردی مسئول دستگاه خویش است. لذا از قبل باید آموزش‌های لازم به کاربران در این خصوص صورت گیرد.

مثال۳: کدام عبارت در مورد شبکه‌های peer-to-peer صحیح می‌باشد؟

۱) تعدادی از گره‌ها نقش سرور و تعدادی دیگر نقش کلاینت دارند.

۲) هر گره همزمان می‌تواند هم سرور باشد هم کلاینت

۳) تعداد گره‌هایی که نقش سرور دارند با تعداد گره‌هایی که نقش کلاینت دارند برابر می‌باشد.

۴) هیچکدام

☑ **پاسخ:** گزینه «۲» دقت کنید که گزینه «۱» در رابطه با شبکه‌های client/server مصداق دارد. در ضمن در هیچ نوعی از شبکه، هیچ الزامی به برابر بودن تعداد گره‌های سرور با کلاینت وجود ندارد.

مثال۴: کدام گزینه از انواع سرورها در نظر گرفته نمی‌شود؟

۱) DNS ۲) Database ۳) ENDS ۴) Web

☑ **پاسخ:** گزینه «۳» هر سه گزینه دیگر از انواع مختلف سرورها به شمار می‌روند.

توپولوژی شبکه

به نحوه و الگوی چیدمان عناصر شبکه در کنار یکدیگر و چگونگی ارتباط آن‌ها با یکدیگر، در اصطلاح توپولوژی یا همبندی گفته می‌شود. مهمترین انواع توپولوژی عبارتند از: BUS (خطی)، Ring (حلقوی)، Star (ستاره)، Mesh (مش)،Tree (درختی) و Hybrid (ترکیبی) که در ادامه به بررسی آن‌ها می‌پردازیم.

توپولوژی BUS (خطی)

در این نوع توپولوژی، ارتباط بین اعضای شبکه از طریق یک کابل (گذرگاه، باس) مشترک (که گاهاً **ستون فقرات یا backbone** نیز نامیده می‌شود) صورت می‌گیرد؛ بدین معنی که کلیه عناصر شبکه، به آن کابل متصل هستند. هر دستگاهی که بخواهد ارسال داده داشته باشد مجبور است داده‌های خود را روی کابل مشترک قرار داده و از طریق آن داده خود را به مقصد ارسال کند. به دلیل مشکلاتی که این توپولوژی دارد در حال حاضر کاربرد بسیار کمی دارد. از ویژگی‌های توپولوژی باس می‌توان به موارد زیر اشاره نمود:

۱ـ سادگی

۲ـ تعداد کابل‌های مورد استفاده (نسبت به برخی توپولوژی‌ها) کم است.

۳ـ گسترش شبکه ساده است. بدین معنی که برای افزایش گره‌ها و اعضای جدید، کار چندان سختی نباید صورت گیرد. تنها باید عنصر جدید را به کابل مشترک وصل نمود.

۴ـ هر گره برای اتصال به شبکه، تنها نیاز به یک پورت دارد.

۵ـ امنیت پایین: اگر نفوذگر موفق شود کنترل باس را در دست گیرد، به کلیه اطلاعات مبادله شده دسترسی پیدا خواهد کرد.

۶ـ باس در هر لحظه، تنها باید در اختیار یک گره باشد. بدین مفهوم که دو گره به طور همزمان نمی‌توانند برای انتقال داده‌های خود از باس استفاده نمایند. بنابراین اگر باس مشغول باشد تا زمان آزاد شدن آن، هیچ گره‌ای حق آغاز تبادل داده خود را نخواهد داشت؛ در غیر این صورت **تصادم (collision)** رخ خواهد داد که باعث خراب شدن داده‌های ارسالی می‌شود.

۷ـ اگر کابل مشترک صدمه‌ای ببیند، عملکرد کل شبکه مختل خواهد شد.

۸ـ برای جلوگیری از انعکاس سیگنال از انتهای باس، باید در انتهای کابل از **خاتمه دهنده (terminator)** استفاده نمود.

۹ـ سخت و مشکل بودن عیب‌یابی و رفع خطا.

۱۰ـ وجود پدیده تضعیف و محدودیت در طول کابل مشترک

تذکر۵: در فصل چهارم به طور مفصل در خصوص کنترل دسترسی به رسانه‌ی مشترک، صحبت خواهیم نمود.

شکل ۱ نمونه‌ای از یک توپولوژی bus را نشان می‌دهد.

شکل ۱: نمونه‌ای از توپولوژی bus

مثال۵: نیاز به terminator در کدام توپولوژی وجود دارد؟

۱) Ring ۲) Bus ۳) Star ۴) Mesh

☑ **پاسخ:** گزینه «۲» همان‌طور که در بالا ذکر شد استفاده از terminator در توپولوژی Bus رایج است.

توپولوژی Ring (حلقوی)

در این توپولوژی گره‌های شبکه، حلقوی‌وار به یکدیگر متصل شده‌اند. بنابراین هر گره، نقش مسیر و رسانه شبکه را نیز ایفا می‌کند. بدیهی است که در چنین الگویی، هر گره تنها با دو گره دیگر به طور مستقیم در تماس است. حرکت داده‌ها می‌تواند در جهت ساعتگرد و یا پادساعتگرد صورت گیرد.

ویژگی‌های این توپولوژی عبارتند از:

۱ـ تعداد کابل مورد استفاده کم است.

۲ـ هر گره برای اتصال به شبکه، تنها نیاز به دو پورت دارد.

۳ـ حذف پدیده تضعیف (زیرا هر گره اطلاعات دریافتی خود را تکرار می‌کند).

۴ـ در صورت خرابی یکی از کابل‌ها و یا گره‌ها، عملکرد کلی شبکه مختل خواهد شد؛ چرا که امکان ارتباط اعضا با یکدیگر از بین می‌رود.

۵ـ امنیت پایینی دارد.

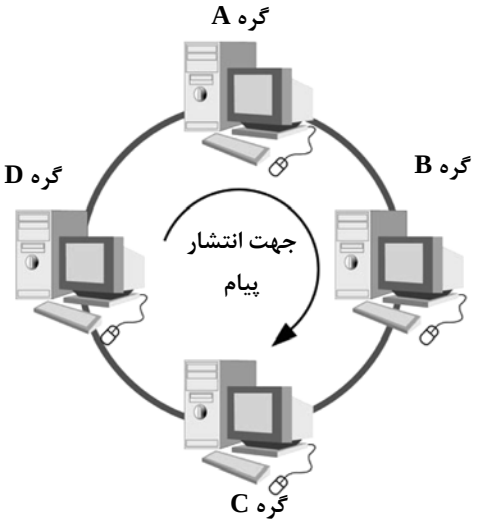
برای غلبه بر مشکلات فوق، معمولاً در توپولوژی حلقه، از دو حلقه در دو جهت متفاوت استفاده می‌شود تا اگر برای یکی از حلقه‌ها مشکلی بروز کرد، بتوان از حلقه جایگزین بهره گرفت.

۶ـ بسط شبکه و افزودن گره‌ی جدید، با از کار افتادن شبکه همراه است.

نکته۲: تعداد کابل‌های مورد نیاز در توپولوژی حلقوی یکطرفه با n گره، برابر n است.

نکته۳: کم‌ترین و بیش‌ترین کابل پیموده شده برای تبادل داده در یک شبکه حلقوی یکطرفه با n گره، به ترتیب عبارتند از: 1 و $n-1$.

شکل ۲ نمونه‌ای از توپولوژی Ring را به تصویر کشیده است.



شکل ۲: نمونه‌ای از توپولوژی Ring

مثال۶: توپولوژی Ring یک طرفه با 5 گره را در نظر بگیرید. در این صورت تعداد کابل‌های مورد نیاز، کم‌ترین و بیش‌ترین تعداد کابل پیموده شده برای تبادل داده به ترتیب از راست به چپ برابر است با:

۱) 4، 1، 4 ۲) 5، 1، 4 ۳) 4، 1، 5 ۴) 5، 1، 5

☑ **پاسخ:** گزینه «۳» در یک توپولوژی Ring با n گره، تعداد کابل‌های مورد نیاز، کم‌ترین و بیش‌ترین کابل پیموده شده برای تبادل داده به ترتیب برابر است با n، 1 و $n-1$. از آنجا که در این تست n برابر 5 می‌باشد. لذا گزینه ۳ صحیح است.

توپولوژی Star (ستاره)

در این توپولوژی (شکل ۳)، کلیه گره‌های شبکه به یک گره مرکزی متصل هستند. کلیه اطلاعات برای آنکه مبادله شوند از گره مرکزی عبور می‌کنند. بنابراین منطقی است که سرعت دریافت و ارسال داده در گره مرکزی بیش‌تر از بقیه گره‌ها باشد. در حقیقت، کابل موجود در توپولوژی باس، در اینجا تبدیل به یک گره شده است. این گره مرکزی معمولاً یک هاب (Hub) یا یک سوییچ (Switch) است. در حال حاضر، استفاده از توپولوژی ستاره، مقبولیت فراوانی یافته است.

تذکر۶: در رابطه با تجهیزاتی مانند هاب و سوییچ در فصل چهارم صحبت خواهیم کرد.

مدرسان شریف

فصل دوم

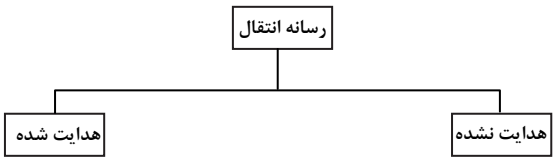
« لایه فیزیکی و انتقال داده »

در این فصل ما به بررسی پایین‌ترین لایه در مدل مرجع OSI و TCP/IP می‌پردازیم. لایه فیزیکی لایه‌ای است که مستقیماً با رسانه شبکه در ارتباط بوده و وظیفه اصلی آن ارسال داده‌هایی است که آن‌ها را از لایه‌های بالاتر از خود دریافت نموده است. به همین علت و برای درک بهتر عملکرد لایه فیزیکی، در این فصل در رابطه با انتقال داده نیز با یکدیگر صحبت خواهیم نمود.

چهارچوب این فصل به قرار زیر است: ابتدا در رابطه با انواع رسانه شبکه صحبت می‌کنیم. سپس به بررسی سیگنال‌های انتقال داده خواهیم پرداخت. مفاهیمی همچون تضعیف، پهنای باند، حداکثر نرخ ارسال، مدولاسیون و انواع آن، مباحث بعدی این فصل را تشکیل می‌دهند. در نهایت با مفهوم مالتی پلکسینگ آشنا خواهیم شد.

رسانه انتقال

برای انتقال داده، رسانه‌های فیزیکی مختلفی را می‌توان به کار برد که هر یک ویژگی‌های مخصوص به خود را از نظر پهنای باند، تأخیر، هزینه، سادگی استفاده، نصب و نگهداری دارند. رسانه‌های انتقال به طور کلی به دو دسته هدایت شده (سیمی) و هدایت نشده (بی‌سیم) تقسیم می‌شوند (شکل ۱)

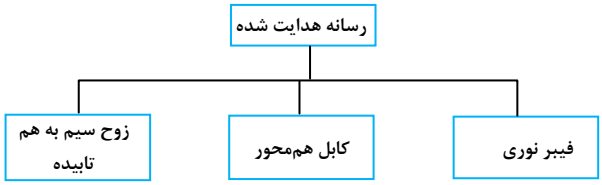


شکل ۱: انواع رسانه انتقال

نکته۱: انتخاب نوع رسانه انتقال به عوامل مختلفی همچون توپولوژی، پهنای باند، فرکانس، مسافت، تضعیف و پارامترهای کیفیت سرویس (QoS) بستگی دارد.

رسانه هدایت شده (سیمی)

رسانه هدایت شده که در حقیقت کانالی را بین یک دستگاه با دستگاه دیگر برقرار می‌سازد، شامل زوج سیم به هم تابیده (Twisted pair)، کابل هم‌محور (Coaxial cable) و فیبر نوری(Fiber optic) می‌باشد (شکل ۲). از آنجا که حرکت سیگنال در طول هر یک از این رساناها مستقیماً از خط سیم صورت می‌گیرد، آن‌ها را هدایت شده می‌نامند. باید دقت کرد که آنچه در زوج سیم به هم تابیده یا کابل هم محور عبور می‌کند، جریان الکتریکی است. داده‌های صفر و یک نیز به همین صورتِ (سیگنال)های الکتریکی نشان داده می‌شوند. این در حالی است که آنچه در فیبر نوری گذر می‌کند، پرتو نور است.



شکل ۲: انواع رسانه هدایت شده (سیمی)

زوج به هم تابیده (twisted pair)

این نوع کابل، از تعدادی زوج سیم مسی عایق‌دار که در حدود 1 میلی متر ضخامت دارند تشکیل شده است. یکی از سیم‌ها به‌عنوان زمین (GND ـ مرجع) و دیگری برای انتقال سیگنال به کار می‌رود. این سیم‌ها به طور مارپیچ، مانند مولکول DNA به یکدیگر تابانیده شده‌اند. علت این تابانیدگی، کاهش اثر تداخل الکتریکی و همچنین ذخیره انرژی می‌باشد. کاربرد اصلی سیم زوج به هم تابیده، در سیستم‌های تلفنی است. استفاده از این نوع کابل تا چندین کیلومتر، نیاز به تقویت کننده ندارد اما برای فاصله‌های طولانی‌تر استفاده از **تکرارکننده (repeater)** مورد نیاز خواهد بود. مقدار تضعیف در سیم زوج به هم تابیده، به فرکانس وابستگی زیادی دارد به طوری که با افزایش آن به شکل نمایی افزایش پیدا می‌کند (در رابطه با تضعیف در همین فصل با هم صحبت خواهیم کرد).

نکته۲: در یک فاصله یکسان، انتقال داده دیجیتال نیاز به تقویت کننده بیش‌تری نسبت به انتقال داده آنالوگ دارد.

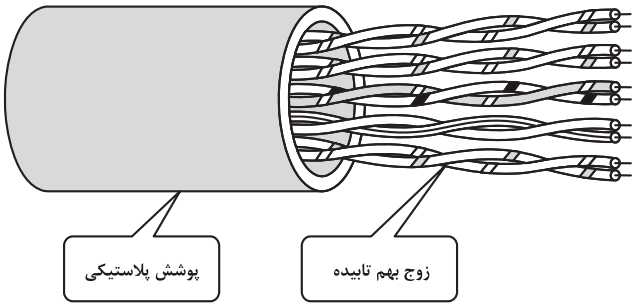
پهنای باند سیم زوج به هم تابیده که می‌توان در انتقال آنالوگ یا دیجیتال از آن استفاده کرد به عواملی همچون ضخامت سیم و مسافت پیموده شده بستگی دارد اما به طور کلی در فاصله‌های چند کیلومتری، پهنای باند چند مگابیت در ثانیه را می‌تواند فراهم آورد. به علت کارایی مناسب و قیمت پایین، سیم زوج‌های به هم تابیده، امروزه کاربرد بسیار گسترده‌ای پیدا کرده‌اند.

نکته۳: چنانچه در سیم زوج به هم تابیده از سیم‌هایی با طول متفاوت استفاده شود، اثر همشنوایی (که یکی از انواع نویز است) کاهش می‌یابد.

سیم زوج به هم تابیده به دو شکل STP و UTP ساخته می‌شود.

کابل Unshielded twisted-pair (UTP)

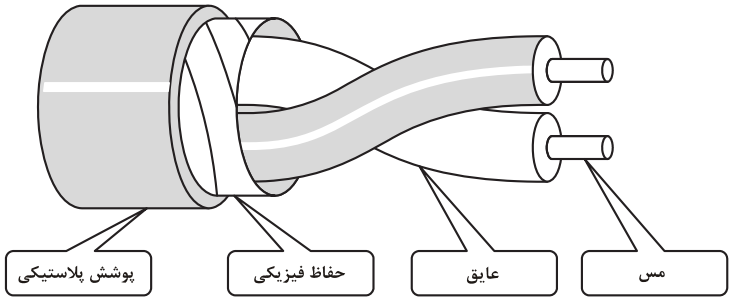
امروزه کابل‌های UTP (شکل ۳) بیش‌ترین استفاده را در انواع معمول رسانه انتقال دارند. هر چند اکثر انواع آن برای سیستم‌های تلفن کاربرد دارند اما تعدادی از آن‌ها را می‌توان برای انتقال داده و صوت نیز به کار برد. کابل‌های UTP با طبقه‌بندی (category)های متفاوتی معرفی می‌شوند؛ مانند CAT5، CAT5-e و CAT-6 که هر کدام از آن‌ها ویژگی مخصوص به خود را دارند. از CAT-1 و CAT-2 برای انتقال آنالوگ و از بقیه طبقه‌ها برای ارسال سیگنال دیجیتال استفاده می‌شود. تفاوت اصلی بین طبقه بندی‌های متفاوت، در میزان پهنای باند و تعداد دورهای تابیده شده در واحد طول است به طوری که با افزایش شماره طبقه‌بندی، موارد فوق افزایش می‌یابد.



شکل۳: کابل UTP

کابل Shielded twisted-pair (STP)

تفاوت STP با UTP در لایه عایق اضافه‌تری است که دارد. این لایه اضافی، منجر به کاهش شدید اثرات نویز در STP نسبت به UTP می‌شود (شکل ۴).



شکل۴: کابل STP

به طور کلی مزایا و معایب زوج سیم به هم تابیده نسبت به دیگر رسانه‌های هدایت شده را می‌توان این گونه بیان نمود (+ به مفهوم ضریب و – به مفهوم عیب است)

+ تکنولوژی کاملاً شناخته شده برای همگان
+ استفاده آسان در شبکه
+ ارزان‌ترین رسانه
+ در دسترس‌ترین رسانه (چون برای تلفن هم کاربرد دارد.)

ـ کم‌ترین مقاومت در برابر با نویز
ـ پهنای باند محدود
ـ محدودیت در بُرد
ـ مستعد نفوذ توسط نفوذگران

مثال۱: کدام گزینه در مورد زوج سیم به هم تابیده صحیح نیست؟

۱) جزو رسانه‌های هدایت شده قلمداد می‌شود.

۲) در برابر نویز در مقایسه با دیگر رسانه‌های مشابه، مقاومت زیادی از خود نشان می‌دهد.

۳) از مشکلات آن پهنای باند محدود و بُرد کوتاه است.

۴) کاربرد بسیار گسترده‌ای دارد.

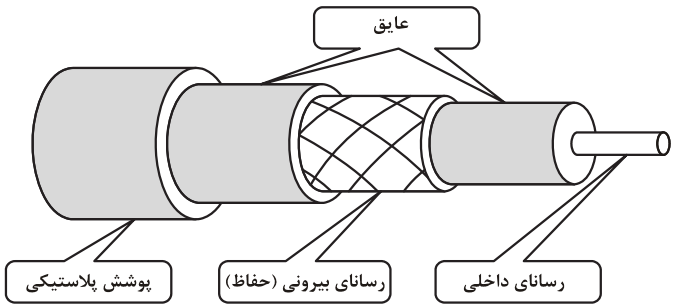
☑ **پاسخ:** گزینه «۲» همان‌طور که اشاره شد، زوج سیم به هم تابیده در مقایسه با دیگر کابل‌ها، کم‌ترین مقاوت را در برابر نویز دارد. صحیح بودن بقیه گزاره‌ها از متن درس قابل بررسی است.

کابل هم محور (Coaxial Cable)

همان‌طور که در شکل ۵ نشان داده شده است، کابل هم محور از دو رسانای سیمی هم مرکز تشکیل شده است که امکان انتقال اطلاعات (چه آنالوگ و چه دیجیتال) را درهر دو جهت فراهم می‌آورد.

نکته۴: با افزایش پهنای باند، تضعیف در کابل هم محور به صورت خطی افزایش می‌یابد.

دو نوع کابل هم‌محور وجود دارد:
50 اهمی و 75 اهمی. کابل‌های 50 اهمی که کاربرد اصلی آن‌ها انتقال داده دیجیتال است به دو صورت نازک (thin) و ضخیم (thick) وجود دارند. قطر هسته کابل‌های نازک و ضخیم به ترتیب برابر 2 و 5 میلی‌متر است. کاربرد اصلی کابل‌های 75 اهمی نیز انتقال داده آنالوگ است.



شکل ۵: کابل هم محور

به طور کلی مزایا و معایب کابل هم محور را نسبت به دیگر رسانه‌های هدایت شده می‌توان این گونه بیان نمود (علامت + به معنای مزیت و علامت ـ به معنای عیب است:

+ هزینه نگه داری پایین

+ سادگی در نصب (نسبت به فیبر نوری)

+ مقاومت بهتر در مقابل نویز در فواصل طولانی (نسبت به زوج سیم به هم تابیده)

ـ محدودیت در بُرد و توپولوژی

ـ امنیت پایین و نفوذپذیری آسان

ـ سختی نصب و اِعمال تغییرات در توپولوژی کابل کشی (نسبت به زوج به هم تابیده)

ـ قیمت بالاتر و نصب مشکل‌تر نسبت به زوج سیم به هم تابیده

تذکر۱: در فصل چهارم مطالب بیش‌تری را درخصوص رسانه‌های شبکه مطالعه خواهیم نمود.

مثال۲: در رابطه با کابل هم محور کدام گزینه صحیح است؟

۱) نسبت به زوج سیم به هم تابیده، در برابر نویز مقاومتر است.

۲) استفاده از آن، سخت‌تر از زوج سیم به هم تابیده است.

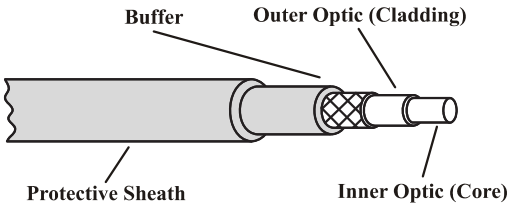
۳) تضعیف در کابل هم محور با افزایش فرکانس به صورت نمایی افزایش می‌یابد.

۴) گزینه‌های ۱ و ۲

☑ **پاسخ:** گزینه «۴» کابل هم محور نسبت به زوج سیم به هم تابیده، در برابر نویز مقاومتر بوده، ضمن آنکه استفاده از آن به راحتی استفاده از زوج سیم به هم تابیده نیست. تضعیف در کابل هم محور نیز به صورت خطی افزایش می‌یابد.

فیبر نوری

پیشرفت‌های اخیر در تکنولوژی نور، امکان ارسال داده توسط پالس‌های نور را فراهم آورده است. همان‌طور که در شکل ۶ دیده می‌شود کابل نوری از هسته (core) و پوشش (cladding) تشکیل شده است. علاوه بر این، یک پوشش خارجی (buffer coating) بر روی این دو قرار می‌گیرد. یک پالس نور به منزله بیت "1" و عدم وجود آن، به منزله بیت "0" می‌باشد. فرکانس نور مرئی، چیزی در حدود 108 مگاهرتز است. بنابراین پهنای باند یک سیستم انتقال نوری به طور بالقوه بسیار بالا است.

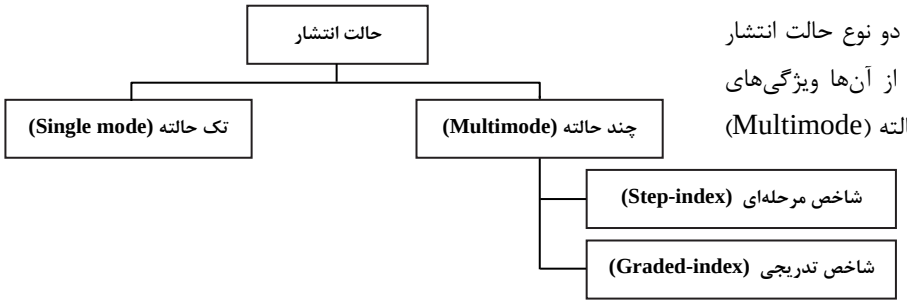


شکل۶: فیبر نوری

نکته۵: میزان تضعیف در فیبر نوری با افزایش پهنای باند ابتدا به شدت افت و با ادامه افزایش پهنای باند به شدت و به صورت نمایی زیاد می‌شود.

منشأ ماده اصلی فیبر نوری که سیلیکن می‌باشد، شن و ماسه است!

همان‌طور که در شکل ۷ نشان داده شده است، دو نوع حالت انتشار نور درون کانال نوری وجود دارد که هر کدام از آن‌ها ویژگی‌های خاص فیزیکی متفاوتی را طلب می‌کنند: چند حالته (Multimode) و تک حالته (single).



شکل ۷: انواع حالات انتشار نور در فیبر نوری

انتشار تک حالته (Single mode)

در انتشار تک حالته، باریکه نور یک خط افقی را طی می‌کند. قطر هسته در این نوع فیبر از انواع دیگر کوچکتر (در حدود 5 تا 10 میکرو متر) بوده و بازتاب در آن کم‌تر اتفاق می‌افتد. در این حالت، تأخیر انتشار پرتوهای مختلف تقریباً برابر بوده و حدوداً صفر است. کلیه پرتوها، «با هم و هم زمان» به گیرنده می‌رسند و بدون تغییر شکل آنچنانی می‌توانند به شکل اولیه خود برگردند. انتشار تک حالته، کم‌ترین میزان تلفات انرژی (تضعیف) را دارد. شکل 8 انتشار تک حالته در فیبر نوری را نشان می‌دهد. البته برای کاهش تضعیف می‌توان از دیودهای لیزری نیز استفاده کرد.

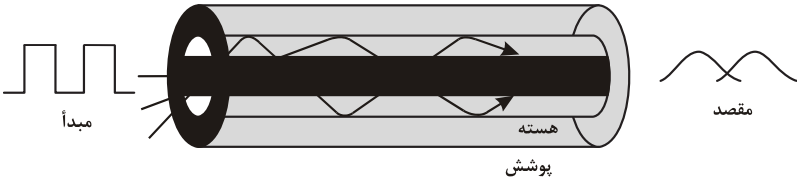
شکل ۸: انتشار تک حالته

فیبر چند حالته (Multimode fiber)

در فیبرهای چند حالته، چندین پرتو از منبع نور تا مقصد، داخل فیبر را از مسیرهای متفاوتی طی می‌کنند. در این فیبرها قطر هسته بیش‌تر شده است (در حدود 50 تا 62.5 میکرو متر). چگونگی حرکت این پرتوها در کابل، به ساختار هسته فیبر بستگی دارد. فیبرهای چند حالته در دو شکل شاخص مرحله‌ای (step-index) و شاخص تدریجی (graded-index) وجود دارند.

فیبر چند حالته step-index

در فیبر چند حالته step-index، چگالی هسته از مرکز تا لبه آن ثابت باقی می‌ماند. پرتو نور از این چگالی ثابت به صورت خط مستقیم رد می‌شود اما زمانی که به سطح بین هسته و پوشش فیبر (cladding) می‌رسد به علت تفاوت ضریب شکست این دو محیط، شکست پیدا کرده و به درون هسته بازتابانیده می‌شود. شکل ۹ فیبر چند حالته step-index را نشان می‌دهد.



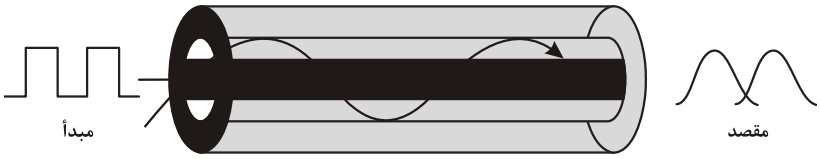
شکل ۹: انتشار چندحالته step-index

نکته۶: پهنای پالسی در سمت گیرنده در حالت Step-index بیشتر از حالات دیگر است.

فیبر چند حالته graded-index

از آنجا که در این حالت تغییر ضریب شکست در طول فیبر نوری، به تدریج صورت می‌گیرد، انحراف سیگنال در درون کابل کم‌تر می‌شود. میزان ضریب شکست در مرکز هسته بیش‌ترین و در جداره‌ها کم‌ترین است. شکل 10 فیبر چند حالته graded -index را نشان می‌دهد.

یکی از کاربردهای مهم فیبر نوری زمانی است که از WDM استفاده شود که در همین فصل و در قسمت مالتی پلکسینگ در رابطه با آن صحبت خواهیم کرد.



شکل ۰ / : انتشار چندحالته graded -index

مثال۳: در کدام حالت انتشار در فیبر نوری، تغییر ضریب شکست در طول فیبر نوری، به تدریج صورت می‌گیرد؟

۱) graded –index ۲) step-index ۳) single mode ۴) گزینه‌های ۲ و ۳

☑ **پاسخ:** گزینه «۱» در حالت graded – index ، تغییر ضریب شکست در طول فیبر نوری، به تدریج صورت می‌گیرد و انحراف سیگنال در درون کابل کم‌تر می‌شود. ضریب شکست در مرکز هسته بیش‌ترین و در جداره‌ها کم‌ترین است.

نکته۷: سرعت انتقال نور در مرکز فیبر، کم‌تر است.

به طور کلی مزایا و معایب فیبر نوری را نسبت به دیگر رسانه‌های هدایت شده می‌توان این گونه بیان نمود:

+ نرخ بیت بالا
+ کم‌ترین میزان تلفات داده در فاصله‌های طولانی
+ نفوذ به آن بسیار مشکل و سخت است (امنیت بالا)
+ مناسب برای استفاده در کابل اصلی (ستون فقرات-backbone) شبکه‌های نقطه به نقطه
+ انتقال مناسب صوت، داده و ویدئو
+ عدم ایجاد تداخل
ـ عدم انعطاف پذیری کابل (شکستگی در صورت فشار برای خم کردن بیش از حد)
ـ نیاز به مهارت برای کار با آن
ـ کمبود استانداردهای جهانی در خصوص آن
ـ هزینه بالای نصب
ـ هر چند پدیده تضعیف در فیبر نوری ناچیز است اما به هر حال تقویت پرتو نور، کار مشکلی است.

مثال۴: بیش‌ترین امنیت و سرعت به ترتیب از راست به چپ متعلق به کدام رسانه هدایت شده است؟

۱) کابل هم محور، فیبر نوری ۲) کابل هم محور، کابل هم محور ۳) فیبر نوری، کابل هم محور ۴) فیبر نوری، فیبر نوری

☑ **پاسخ:** گزینه «۴» امنیت و سرعت بالا از ویژگی‌های مثبت فیبر نوری است.

رسانه هدایت نشده (بی سیم)

در بعضی مواقع و شرایط، اصولاً امکان کابل‌کشی وجود ندارد. رسانه هدایت نشده یا بی‌سیم، بدون استفاده از رسانای فیزیکی، امواج الکترومغناطیسی را منتقل می‌کند. در این نوع از انتقال، امواج در هوا (یا در موارد خاص در آب) پخش همگانی (broadcast) شده و به همین خاطر برای هر کسی که تجهیزات لازم را دراختیار داشته باشد، قابل دریافت هستند. به طور کلی امنیت، یکی از مهم‌ترین چالش‌های شبکه‌های بی‌سیم است. انتقال بی‌سیم به گونه‌های مختلفی می‌تواند صورت گیرد، از جمله: امواج رادیویی، ماکروویو زمینی، ارتباط ماهواره‌ای و تلفن سلولی.

نکته۸: تداخل امواج و کمبود بازه‌های فرکانسی از جمله چالش‌های پیش‌روی انتقال بی‌سیم است.

فصل سوم

« لایه پیوند داده »

پس از مطالعه لایه فیزیکی در فصل گذشته، در این فصل به بررسی و مطالعه لایه پیوند داده می‌پردازیم. این بررسی، شامل مطالعه الگوریتم‌ها و روش‌هایی برای رسیدن به شبکه قابل اطمینان و ارتباط کارا و موثر بین دو ماشین همسایه در لایه پیوند داده می‌باشد.

متاسفانه، مدارهای ارتباطی باعث شکل‌گیری خطا می‌شوند. علاوه بر این، آن‌ها دارای پهنای باند محدودی هستند که باعث ایجاد محدودیت در حداکثر نرخ ارسال می‌شوند. ضمن اینکه وجود لینک ارتباطی باعث ایجاد تاخیر انتشار نیز می‌شود. کلیه این موارد، بر کارایی نرخ انتقال داده اثر سوئی می‌گذارند. پروتکل‌هایی که برای ارتباط استفاده می‌شوند باید کلیه این عوامل را در نظر گیرند. در این فصل با این پروتکل‌ها آشنا خواهیم شد.

وظایف لایه پیوند داده

لایه پیوند داده چندین وظیفه مهم دارد که باید آن‌ها را انجام دهد. این وظایف شامل موارد زیر می‌شود:

۱ـ تامین واسط سرویس مناسب برای لایه بالاتر از خود (لایه شبکه)

۲ـ تعیین چگونگی گروه‌بندی بیت‌های ارسالی توسط لایه فیزیکی در قالب فریم‌ها (فریم بندی)

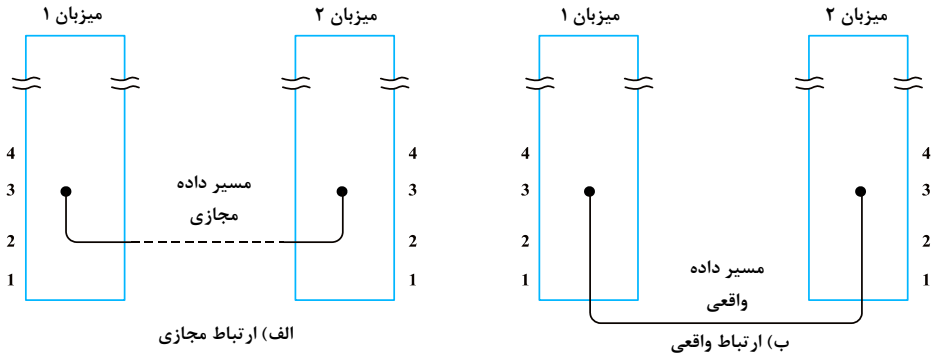
۳ـ تنظیم جریان فریم‌ها به گونه‌ای که یک گیرنده‌ی آهسته، به واسطه دریافت داده‌های بسیار زیاد از فرستنده پرسرعت دچار مشکل نشود (کنترل جریان).

۴ـ بررسی خطاهای انتقال (کنترل خطا)

در ادامه همین فصل، این اهداف را مورد بررسی قرار خواهیم داد. البته لازم به ذکر است که لایه پیوند داده، خود به دو زیر لایه **MAC** و **LLC** تقسیم می‌شود. زیرلایه MAC با لایه فیزیکی و زیر لایه LLC با لایه شبکه در ارتباط است. به عبارت دیگر وظیفه ارائه سرویس به لایه شبکه و مدیریت ارتباطات میان دو کامپیوتر در یک کانال، بر عهده زیرلایه LLC است. زیرلایه MAC نیز دسترسی به رسانه مشترک را مورد توجه قرار می‌دهد. در این رابطه در فصل ۴ بیشتر سخن خواهیم گفت.

ارائه سرویس به لایه شبکه

وظیفه لایه پیوند داده، ارائه سرویس به لایه شبکه است. مهمترین سرویس، انتقال داده‌ها از لایه شبکه‌ی ماشینِ منبع، به لایه شبکه‌ی ماشین مقصد است. در ماشین منبع و در لایه شبکه، موجودیتی (entity) که ما آن را پردازش (process) می‌نامیم وجود دارد که تعدادی بیت را برای ارسال به مقصد، به لایه پیوند داده تحویل می‌دهد. وظیفه لایه پیوند داده انتقال این بیت‌ها به ماشین مقصد است به گونه‌ای که آن‌ها بتوانند به لایه شبکه تحویل داده شوند. (شکل ۱ الف).



شکل ۱ : ارتباط مجازی و واقعی

انتقال واقعی، مسیری را دنبال می‌کند که در شکل ۱ـ ب نشان داده شده است. اما مدل ساده‌تر همان است که ارتباط بین دو فرآیند را که از پروتکل پیوند داده استفاده می‌کنند، در نظر بگیریم.

لایه پیوند داده می‌تواند برای ارئه سرویس‌های متفاوتی طراحی شود به طوری که سرویس ارائه شده در هر سیستم، می‌تواند متفاوت با دیگری باشد. با این حال، سرویس‌های معمولی که ارائه می‌شوند عبارتند از:

۱ـ سرویس بدون اتصال بدون تصدیق (Unacknowledged connectionless service)

۲ـ سرویس بدون اتصال با تصدیق (Acknowledged connectionless service)

۳ـ سرویس اتصال‌گرای با تصدیق (Acknowledged connection-oriented service)

در **سرویس بدون اتصال بدون تصدیق**، ماشین منبع، فریم‌های مستقلی را به مقصد ارسال می‌کند؛ بدون آنکه ماشینِ مقصد، دریافت آن‌ها را تصدیق کند. هیچ ارتباطی از قبل بین فرستنده و گیرنده ایجاد نمی‌شود (به فصل ۱ مراجعه کنید). اگر فریمی به خاطر نویز در لینک از دست برود، هیچ تلاشی در لایه پیوند داده برای جبران آن انجام نمی‌شود. **این نوع سرویس زمانی اهمیت پیدا می‌کند که نرخ خطا بسیار پایین باشد** به طوری که بتوان عمل بازیابی را به عهده لایه‌های بالاتر واگذار کرد. علاوه بر این، برای **ترافیک‌های بیدرنگ (real-time)** مانند صوت که در آن‌ها سرعت دریافت داده (نرخ انتقال) از صحت داده دریافتی، اهمیت بیش‌تری دارد، نیز مناسب است. **اغلب LANها** در لایه پیوند داده خود از سرویس بدون اتصال بدون تصدیق استفاده می‌کنند.

مرحله دیگر در سلسله مراتب قابلیت اطمینان، **سرویس بدون اتصال با تصدیق** است. در این سرویس برای هر فریم ارسالی، تصدیق باید به صورت جداگانه دریافت شود. به این وسیله فرستنده متوجه دریافت یا دریافت نشدن فریم‌های ارسالی می‌شود. اگر پیام تصدیق در بازه زمانی مشخصی دریافت نشود، فرستنده مجدداً فریم قبلی را ارسال می‌کند. **این سرویس روی کانال‌های غیر قابل اطمینان مانند سیستم‌های بی‌سیم مفید است. بدیهی است که نرخ ارسال داده در این جا از سرویس بدون اتصال بدون تصدیق کمتر است.**

نکته۱: قابلیت تصدیق در لایه پیوند داده، اختیاری است و نه الزامی. چراکه لایه انتقال می‌تواند همیشه پیغامی را بفرستد و برای تصدیق آن منتظر بماند.

اگر تصدیق قبل از اتمام زمان از پیش تعیین شده، دریافت نشود و اصطلاحاً **time out** اتفاق بیفتد، فرستنده بار دیگر پیغام را می‌فرستد. مشکل این رویکرد این است که اگر فرض کنیم کل پیغام به 10 فریم تقسیم شده باشد و 20 درصد فریم‌ها گم شوند، زمان بسیار زیادی برای ارسال پیغام لازم است.

مهم‌ترین سرویسی که لایه پیوند داده برای لایه شبکه فراهم می‌آورد، **سرویس اتصال گرای با تصدیق** است. علاوه بر ارائه تضمین دریافت هر فریم، این سرویس به ترتیب دریافت شدن فریم‌ها را نیز تضمین می‌کند. در حالی که در سرویس بدون اتصال، ممکن است یک تصدیقِ گم شده، باعث ارسال چندین باره یک فریم شده و بدین ترتیب چند نسخه از آن فریم دریافت شود.

زمانی که سرویس اتصال‌گرا استفاده می‌شود، انتقال شامل سه مرحله جداگانه می‌شود. در اولین مرحله، ارتباطی بین دو طرف انتقال ایجاد می‌شود که در آن مقدارها و شمارش گره‌های مورد نیاز برای تعیین و پی‌گیری اثر (track) هر فریم دریافتی و یا دریافت نشده، مقداردهی اولیه می‌شود. در دومین مرحله، ارتباط اصلی شکل گرفته و داده‌ها مبادله می‌شوند. مرحله سوم نیز خاتمه ارتباط است.

نکته۲: نرخ ارسال داده در سرویس اتصال‌گرای با تصدیق، کم‌تر از سرویس بدون اتصال بدون تصدیق و سرویس بدون اتصال با تصدیق می‌باشد.

تذکر۱: در فصل اول در رابطه با سرویس‌های اتصال‌گرا و بدون اتصال توضیح داده شده است.

مثال۱: کدام گزینه صحیح نیست؟

۱) اغلب LANها در لایه پیوند داده خود از سرویس بدون اتصال بدون تصدیق استفاده می‌کنند.

۲) قابلیت تصدیق در لایه پیوند داده، الزامی است.

۳) سرویس بدون اتصال با تصدیق، روی کانال‌های غیر قابل اطمینان مانند سیستم‌های بی‌سیم مفید است.

۴) سرویس بدون اتصال بدون تصدیق زمانی اهمیت پیدا می‌کند که نرخ خطا بسیار پایین باشد.

☑ **پاسخ:** گزینه «۲» قابلیت تصدیق در لایه پیوند داده، اختیاری است و نه الزامی. با مراجعه به متن درس، درستی گزینه‌های دیگر مشهود است.

روش‌های فریم‌بندی

همان‌طور که پیش از این نیز اشاره شد، منظور از فریم‌بندی، ارسال داده‌ها در یک قالب مشخص و معین برای فرستنده و گیرنده است به طوری که ابتدا و پایان آن‌ها نیز مرزبندی شده باشد. قبل از آغاز بحث تکنیک‌های مختلف فریم بندی، لازم است به دو موضوع مهم اشاره کنیم:

۱ـ در بسیاری از شبکه‌ها، مخصوصاً در WANها، به هدف رسیدن به سطح بالاتری از قابلیت اطمینان و کاراییِ لایه کنترل پیوند داده، اندازه فریم کوچکتر از اندازه بسته انتخاب می‌شود. بنابراین بسته‌ای که قرار است ارسال شود، اغلب اوقات با فریم‌بندی و حدبندی مناسب، به چندین فریم تقسیم می‌شود و سپس به سمت مقصد ارسال می‌شود. از آن طرف، گیرنده نیز باید بتواند با چینش مناسب فریم‌ها، قادر به ادغام آن‌ها و تولید بسته اولیه باشد.

۲ـ بحث فریم‌بندی که در ادامه خواهیم دید، در ارتباط با انتقال سنکرون است (در رابطه با انتقال سنکرون و آسنکرون در همین بخش مفصل صحبت خواهیم کرد).

۳ـ عمل همگام‌سازی که در لایه فیزیکی انجام می‌شود محدود به یک بیت و یا یک کاراکتر است در حالی که انجام همین عمل در لایه پیوند داده، برای همگام‌سازی بلوکی از داده‌ها می‌تواند صورت گیرد.

بی‌کار (idle)	جدا کننده پایانی	دنباله (Trailer)	INFO	سرآیند (Header)	جدا کننده آغازین	بی‌کار (idle)
	فریم					

شکل ۲: فرمت کلی یک فریم

فرمت کلی یک فریم در شکل ۲ نشان داده شده است. در این شکل، فیلد INFO که طول متغیری دارد، حاوی کل بسته یا قسمتی از بسته است که از لایه شبکه به لایه پیوند داده ارسال شده است. موضوع این قسمت، تکنیک‌های مختلف برای فریم بندی یعنی نحوه انتخاب جداساز (delimiter) می‌باشد.

برای فریم‌بندی، معمولاً از یکی از سه روش زیر استفاده می‌شود:

۱ـ فریم‌بندی کاراکترگرا (Character-Oriented Framing)

۲ـ فریم‌بندی بیت‌گرا (Bit -Oriented Framing)

۳ـ فریم‌بندی تخطیِ کدگرا (Code violation -Oriented Framing)

فریم‌بندی کاراکترگرا (Character-Oriented Framing)

این روش یکی از قدیمی‌ترین الگوها برای جداسازی است. فریم‌بندی کاراکترگرا از چهار کاراکتر کنترلی در کد ASCII برای فریم بندی استفاده می‌کند: وضعیت بیکار لینک یا SYN، آغاز متن یا STX (Start of Text)، پایان متن یا ETX (End of Text) و گریز پیوند داده یا DLE (Data Link Escape).

فرض کنید قرار است دو کاراکتر مستقل "MAY" و "2000" با فاصله زمانی مشخص، پشت سر هم ارسال شود. داده ارسالی که عملاً توسط لایه کنترل لایه پیوند داده (DLC) ارسال می‌شود به صورت زیر است:

SYN SYN STX MAY ETX SYN SYN STX 2000 ETX SYN SYN

کاراکتر کنترلی SYN به منزله بیکار بودن (idle) لینک است و معمولاً به‌صورت 01010101 در نظر گرفته می‌شود. وظیفه این کاراکتر کنترلی، همگام‌سازی فرستنده و گیرنده است و در حقیقت به‌عنوان کلاک مشترک بین آن دو عمل می‌کند. بنابراین گیرنده در هر زمان می‌تواند با جستجوی SYN در رشته داده، آغاز داده را شناسایی کند. مشکلی که اینجا ممکن است به وجود آید این است که خود داده‌ای که قرار است ارسال شود، حاوی کاراکترهای کنترلی نیز باشد. در این صورت چگونه می‌توان فهمید که مثلاً کاراکتری مانند SYN، نقش کنترلی دارد یا واقعاً قسمتی از داده است؟

یک روش که **character stuffing** نام دارد به این صورت است که جداکننده‌هایی که در متن داده ظاهر می‌شوند را با جفت کاراکتر کنترلی DLE STX و DLE ETX نشان دهیم. ضمناً اگر کاراکتر کنترلی DLE نیز بخواهد در متن داده قرار گیرد، کافی است قبل از آن، یک DLE دیگر اضافه کنیم. گیرنده نیز به سادگی در صورت مشاهده دو DLE پشت سر هم، اولین DLE را حذف می‌کند. فرض کنید قرار است داده زیر را منتقل نماییم:

"x y DLE z STX"

در صورتی که character stuffing برای ارسال این داده استفاده شود، نتیجه کار در شکل ۳ نشان داده شده است.

SYN	SYN	STX	x	y	DLE	DLE	z	DLE	STX	ETX	SYN	SYN

شکل ۳: مثالی از character stuffing

نکته۳: سربار از رابطه زیر محاسبه می‌شود:

$$\text{سربار} = \frac{\text{تعداد بیت غیر مفید ارسالی (داده‌هایی که جزو اصل داده نیستند اما ارسال می‌شوند)}}{\text{تعداد کل بیت ارسالی}}$$

برای بیان درصد سربار، کافی است کسر بالا را در 100 ضرب نماییم.

مثال۲: یک منبع داده‌ها کاراکترهای ASCII هفت بیتی تولید و از طریق یک سیستم انتقال سنکرون با سرعت 300bps ارسال می‌کند. انتقال به صورت کاراکترگرا بوده و هر فریم از 8 کاراکتر کنترلی و 120 کاراکتر اطلاعات تشکیل شده است. چنانچه به همراه هر کاراکتر یک بیت پریتی در کاراکترها اضافه شود، مقدار کاراکترهای ارسالی در ثانیه (گذردهی) چقدر است؟ (برحسب کاراکتر در ثانیه)

۱) 30 ۲) 36 ۳) 24 ۴) 42

☑ **پاسخ:** گزینه «۲» گذردهی در این حالت برابر است با تعداد کاراکترهای ارسالی در هر فریم تقسیم بر مدت زمان لازم برای ارسال یک فریم (t). از آنجا که هر کاراکتر معادل 7 بیت به علاوه یک بیت پریتی است. تعداد بیت‌های هر فریم (N) برابر است با:

$$N = (120+8)\times(7+1) = 2^{10} = 1024\,\text{bit}$$

برای محاسبه t از تناسب زیر استفاده می‌کنیم:

$$\frac{\text{بیت}}{\text{ثانیه}} : \frac{300}{1} = \frac{2^{10}}{t} \Rightarrow t = \frac{2^{10}}{300}$$

بنابراین گذردهی (TP) برابر می‌شود با:

$$TP = \frac{128}{\frac{2^{10}}{300}} = 37.5 \simeq 36$$

فریم‌بندی بیت گرا (Bit -Oriented Framing)

در فریم‌بندی بیت‌گرا که در پروتکل HDLC استفاده می‌شود، جداساز d، توسط الگوهای بیتی خاصِ "01111110" که **پرچم (فلگ)** نام دارند، انجام می‌شود. در اینجا نیز ممکن است این جداساز در مواقعی جزو داده باشد. در این صورت باید از روش **bit stuffing** استفاده کرد. در این روش، هر گاه فرستنده پنج رشته "1" پشت سر هم را در جریان داده ببیند، یک عدد صفر به رشته اضافه می‌کند. از آن طرف، گیرنده نیز هر جا پس از پنج عدد یکِ متوالی، یک صفر ببیند متوجه می‌شود که این صفر را فرستنده اضافه کرده و آن را حذف می‌کند.

به این نکته دقت کنید که **سربار (overhead) روش بیت‌گرا نسبت به روش کاراکترگرا کمتر است** (منظور از سربار، اطلاعاتی است که جزو داده اصلی نیستند اما بنا بر دلایل مختلف ـ مانند دلایل کنترلی ـ به اجبار باید آن‌ها را نیز همراه داده اصلی انتقال داد). ضمن اینکه در این روش به جای محدود سازی فیلد داده به کاراکترهای 8 بیتی، امکان حضور هر تعداد بیت در فیلد داده، میسر است. هر چند مطابق روال کلی، داده به شکل بایت سازمان‌دهی می‌شود.

نکته۴: تعداد داده‌های ارسالی در روش فریم‌بندی بیت‌گرا مضربی از بایت نمی‌باشد (چرا؟).

مثال۳: فرض کنید در یک سیستمی که از فریم‌بندی بیت‌گرا استفاده می‌کند، گیرنده پیغام 011111100111110010111111O را از فرستنده دریافت می‌کند. در این صورت اصل داده ارسالی چه بوده است؟

۱) 01110101 ۲) 01111110 ۳) 01111001 ۴) 01111101

☑ **پاسخ:** گزینه «۴» گیرنده هر جا پس از پنج عدد یکِ متوالی، یک صفر ببیند متوجه می‌شود که این صفر را فرستنده اضافه کرده و آن را حذف می‌کند. کاراکترهای 01111110 نیز که در ابتدا و انتها آمده است اشاره به ابتدا و انتهای کاراکتر دارند.

فریم‌بندی تخطیِ کدگرا (Code violation -Oriented Framing)

به جای آن که از کاراکترها یا الگوهای بیتی خاص استفاده کنیم، می‌توان عمل فریم‌بندی را در سطح واقعی بیت، در هنگام رمزگذاری و کدینگ بیت‌ها و تبدیل آن‌ها به سیگنال انجام داد. اجازه دهید با یک مثال توضیح بیش‌تری بدهیم. در کدینگ منچستر (که در فصل گذشته آنرا مطالعه کردیم)، هر گذار high به low معرف داده "1" و گذارlow به high معرف داده "0" است. ویژگی اصلی این کد این است که همیشه در وسطِ زمان هر بیت، باید یک گذار اتفاق بیفتد. با تخطی از همین ویژگی (به‌عنوان مثال وجود یک زوج high-high به دنبال یک زوجlow-low)، می‌توان به تعیین جداکننده پرداخت. این الگوی ابتکاری از گذارهای مورد انتظار در وسط زمان هر بیت جلوگیری کرده و می‌تواند مرز و حد فریم را به اطلاع گیرنده برساند. این تکنیک فریم‌بندی که از یک کدینگِ لایه فیزیکیِ غیر معتبر استفاده می‌کند در استانداردهای 802 LAN کاربرد دارد.

قبل از آنکه این بخش را به پایان ببریم باید این نکته را نیز متذکر شویم که از ارسال تعداد کاراکترها یا بیت‌ها در هر فریم ارسالی نیز می‌توان برای آگاه‌سازی گیرنده از انتهای فریم استفاده کرد. این تعداد می‌تواند در سرآیند فریم (frame header) قرار گیرد. به هر حال این روش چندان کاربرد ندارد چراکه خطای بیتی می‌تواند منجر به اشتباهات بزرگ و شدیدی شود. البته اگر این روش به همراه 3 روش قبلی که پیش از این توضیح داده شد استفاده شود، می‌تواند قابلیت اطمینان پروسه فریم‌بندی را تا حد بسیار زیادی ارتقا بخشد. استفاده همزمان از این روش‌های فریم‌بندی در پروتکل‌هایی مانند Token Ring و Ethernet کاربرد دارد.

تذکر۲: پروتکل‌هایی مانند Token Ring و Ethernet در فصل چهارم بررسی خواهند شد.

بحث فریم‌بندی را با بررسی سه روش انتقال سنکرون (همگام) و غیر سنکرون (غیر همگام) و متقارن (Isochronous) به پایان می‌بریم.

مثال۴: کدام گزینه صحیح است؟

۱) فریم بندی تخطیِ کدگرا از قدیمی‌ترین روش‌های فریم بندی محسوب می‌شود.

۲) سربار (overhead) روش بیت‌گرا نسبت به روش کاراکترگرا بیش‌تر است.

۳) ارسال تعداد کاراکترها یا بیت‌ها در هر فریم ارسالی یکی از مطمئن‌ترین روش‌های فریم بندی است.

۴) فریم بندی تخطیِ کدگرا در استانداردهای 802 LAN کاربرد دارد.

☑ **پاسخ:** گزینه «۴» فریم بندی کاراکترگرا از قدیمی‌ترین الگوها برای جداسازی بسته‌های شامل بسته داده است (نادرستی گزینه ۱). سربار (overhead) روش بیت‌گرا نسبت به روش کاراکترگرا کمتر است (نادرستی گزینه ۲). در ارسال تعداد کاراکترها یا بیت‌ها در هر فریم ارسالی به هدف فریم بندی، خطای بیتی می‌تواند منجر به اشتباهات بزرگ و شدیدی شود (نادرستی گزینه ۳).

انتقال سنکرون و آسنکرون

به طور کلی سه حالت اصلی انتقال عبارتند از:

۱ـ انتقال آسنکرون (غیر همگام-Asynchronous) ۲ـ انتقال سنکرون (همگام-Synchronous) ۳ـ انتقال Isochronous

در این کتاب ما به طور کلی انتقال سریال را مورد توجه قرار خواهیم داد که طبق آن، داده‌ها پشت سر هم و از طریق تنها یک کانال ـ به جای چندین خط موازی با هم ـ ارسال می‌شوند. انتقال موازی بیش‌تر در دستگاه‌های I/O و مسیرهای درونی کامپیوترها کاربرد دارد. با استفاده از انتقال سریال، در هر نوبت المان‌های سیگنال از طریق خط ارسال می‌شوند. هر المان سیگنال ـ همان‌طور که در فصل گذشته دیدیم ـ ممکن است:

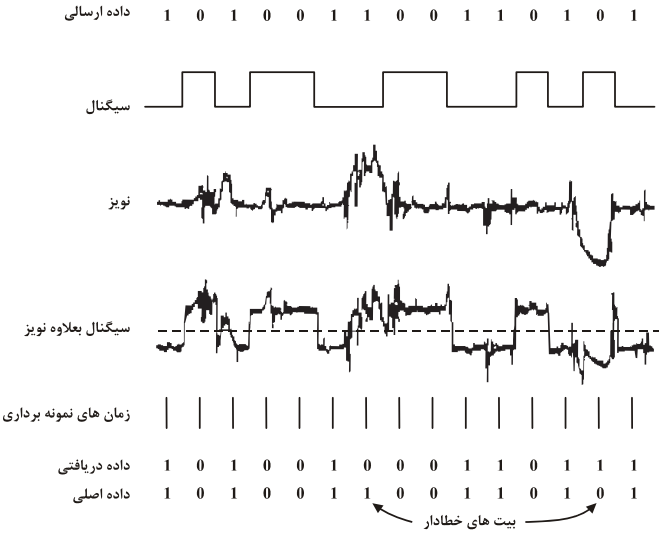
ـ کم‌تر از یک بیت باشد. مانند آنچه در کد منچستر رخ می‌دهد.

ـ برابر با یک بیت باشد. مثال‌های دیجیتال و آنالوگ از این حالت به ترتیب عبارتند از: NRZ-L و FSK.

ـ بیش‌تر از یک بیت باشد. مانند QPSK

برای سادگی بحث، ما حالت دوم را در نظر می‌گیریم؛ یعنی هر المان سیگنال معادل یک بیت باشد. البته ماهیت قضیه با در نظر گرفتن این فرض، خدشه‌دار نخواهد شد.

به شکل ۴ دقت کنید. در این شکل هر دریافت داده دیجیتال، شامل نمونه‌برداری از سیگنال‌های ورودی به ازای هر زمان بیت است تا مقدار باینری آن مشخص شود. یکی از مشکلاتی که در فصول گذشته نیز کاملاً آن را مورد بررسی قرار دادیم، این است که امکان رخداد انواع نویز روی خط و سیگنال وجود دارد که می‌تواند تولید خطا کند. این مسئله برای زمان بندی نیز می‌تواند باعث مشکلاتی شود. برای آنکه گیرنده بتواند نمونه‌برداری بیت‌های دریافتی را به شکل صحیح انجام دهد، باید از زمان ورود و دوره‌ی زمانی (duration) هر بیتی که دریافت می‌کند، آگاه باشد.



شکل ۴: اثر نویز بر سیگنال دیجیتال

فرض کنید فرستنده‌ای که جریانی از بیت‌های داده را ارسال می‌کند، دارای کلاکی است که زمانبندی ارسال بیت‌ها را کنترل و مدیریت می‌کند. برای مثال، اگر قرار باشد داده با سرعت یک میلیون بیت در ثانیه (1 Mbps) ارسال شود، آنگاه یک بیت باید در هر میکروثانیه ($\frac{1}{10^6}$ ثانیه) که توسط کلاک فرستنده محاسبه می‌شود، ارسال شود (می‌توانید با یک تناسب ساده صحت این ادعا را بررسی نمایید). معمولاً گیرنده سعی می‌کند تا نمونه‌برداری را در وسط زمان هر بیت انجام دهد. گیرنده، زمان‌بندی خود را با فاصله‌های زمانی هر بیت تنظیم می‌کند. در مثال ما، نمونه‌برداری باید در هر یک میکرو ثانیه انجام شود.

اگر گیرنده زمان‌بندی خود را با توجه به کلاک خاص خودش انجام دهد، آنگاه چنانچه کلاک گیرنده و فرستنده دقیقاً با هم تنظیم نشوند، احتمال بروز مشکل وجود خواهد داشت. اگر این اختلاف تنها در حدود 1% هم باشد (کلاک گیرنده 1% سریعتر یا کندتر از کلاک فرستنده باشد)، آنگاه اولین نمونه‌برداری، 0.01 زمانِ بیت ($0.01\mu s$)، از مرکز بیت فاصله خواهد گرفت (مرکز بیت، به اندازه $0.5\mu s$ نسبت به آغاز و انتهای بیت قرار گرفته است). پس از 50 مورد نمونه‌برداری یا تعدادی بیش‌تر، گیرنده ممکن است با خطا مواجه شود؛ چراکه نمونه‌برداری در زمان اشتباهی صورت می‌گیرد. ($50\times 0.01 = 0.5\mu s$) برای اختلاف زمان‌بندی‌های کمتر، ممکن است خطا در زمان دیرتری رخ دهد اما به هر حال، در نهایت اگر فرستنده جریان بزرگی از داده را ارسال کند و در این بین، عمل همگام سازی بین فرستنده و گیرنده انجام نشود، گیرنده، همزمانی خود را با فرستنده از دست خواهد داد.

نکته۵: اگر سرعت نمونه‌برداری در فرستنده را با T، درصد اختلاف ساعت گیرنده و فرستنده را با ΔT و حداکثر تعداد نمونه‌برداری که در آن خطایی به وجود نیاید را با n نشان دهیم آنگاه می‌توان نوشت:

$$n \le \frac{T}{2\Delta T}$$

مثال۵: اگر سرعت نمونه‌برداری در فرستنده برابر یک میکروثانیه بوده و اختلاف کلاک گیرنده با فرستنده دو درصد باشد، حداکثر تعداد نمونه برداری که در آن خطایی به وجود نیاید چقدر است؟

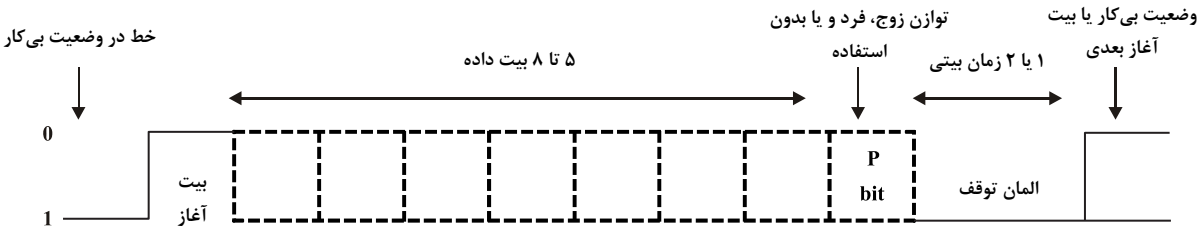
۱) 50 ۲) 100 ۳) 25 ۴) 200

☑ **پاسخ:** گزینه «۳»

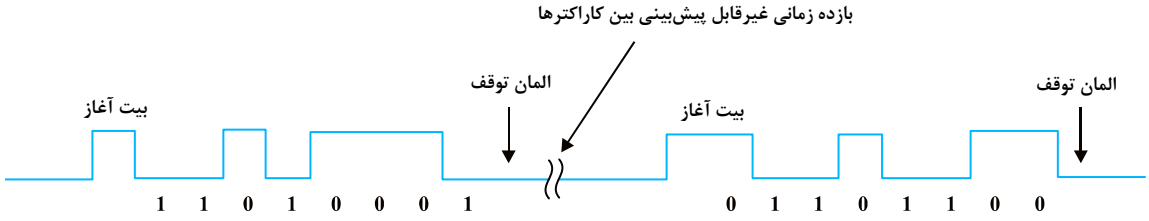
$$n \le \frac{T}{2\Delta T} \rightarrow n \le \frac{1}{2\times 0.02} = 25$$

انتقال آسنکرون (غیر همگام ــ Asynchronous)

رویکردهای مختلفی برای رسیدن به همگامی و همزمانی مورد نظر، رواج دارد. اولین روش انتقال آسنکرون نامیده می‌شود. اساس این روش این است که برای پیشگیری از بروز مشکل در زمان‌بندی، جریان بزرگی از داده‌ها بدون وقفه ارسال نشود. بلکه در هر نوبت، داده‌ها به صورت «تک کاراکتر، تک کاراکتر» ارسال می‌شوند (هر کاراکتر شامل 5 تا 8 بیت است). تعداد بیت‌های هر کاراکتر، بستگی به کد استفاده شده دارد. به‌عنوان مثال در کد IRA، هر کاراکتر، هفت بیتی است. در کد دیگری به نام Extended Binary Coded Decimal Interchange Code (EBCDIC) که در ابر کامپیوتر (mainframe)های IBM کاربرد دارد، هر کاراکتر شامل 8 بیت است. زمان‌بندی و همگام‌سازی باید در هر کاراکتر حفظ شود. به این صورت، گیرنده در ابتدای هر کاراکترِ جدید، فرصت همزمان سازی مجدد را خواهد داشت. مثالی از ارتباط آسنکرون، نوع ارتباط بین کامپیوتر و صفحه کلید است.



الف) فرمت کاراکتر



ب) جریان کاراکتر هشت بیتی آسنکرون

فصل چهارم

« روش‌های کنترل دسترسی به رسانه و اجزای شبکه »

حتماً از فصل اول به خاطر دارید که فناوری انتقال داده به دو صورت انتشاری و نقطه به نقطه است. یکی از مسائلی که انتقال داده با آن دست به گریبان است، کنترل دسترسی به گذرگاه مشترک است. لایه پیوند داده که در فصل قبل آن را به طور مفصل مطالعه کردیم از دو زیر لایه تشکیل شده است: زیرلایه **LLC** (**Logical Link Control**) که وظیفه اصلی آن، سرویس‌دهی به لایه بالاتر (یعنی لایه شبکه) است و زیر لایه **MAC** (**Medium Access Control**) که در این فصل به آن خواهیم پرداخت. پروتکل‌هایی که دسترسی به کانال به اشتراک گذاشته شده را کنترل و مدیریت می‌کنند، در زیر لایه MAC قرار دارند. این زیرلایه، به خصوص در LANها و حالات انتقالی full-duplex و half duplex، اهمیت پیدا می‌کند چراکه تقریباً همگی آن‌ها از کانالی با دسترسی چندگانه (Multi-Access Channel)، استفاده می‌کنند. در مقابل، WANها (به جز شبکه‌های ماهواره‌ای) از لینک‌های نقطه به نقطه بهره می‌برند. از آنجا که کانال‌های دسترسی چندگانه و LANها وابستگی زیادی به هم دارند، ما در این بخش در رابطه با LANها، معماری پروتکل آن‌ها که توسط استاندارد IEEE 802 مشخص می‌شود و همچنین شبکه‌های ماهواره‌ای صحبت خواهیم نمود.

به طور کلی اختصاص کانال می‌تواند به دو شکل ایستا (static) و پویا (dynamic) انجام شود که در ادامه همین فصل آن‌ها را مفصلاً بررسی خواهیم نمود. اما قبل از آن لازم است تذکر دهیم که از دیدی دیگر، مدیریت دسترسی به کانال مشترک می‌تواند به سه شکل دیگر نیز طبقه‌بندی شود:

۱- تصادفی ۲ـ توزیع شده و ۳ـ متمرکز. از جمله **روش‌های تصادفی** می‌توان به مواردی همچون انواع پروتکل‌های ALOHA و CSMA اشاره کرد. پروتکل‌هایی نیز که از مفهوم Token استفاده می‌کنند، از جمله **روش‌های توزیع شده** به شمار می‌روند. در نهایت روش‌های مبتنی بر مفهوم سرکشی (Polling) نیز جزو **روش‌های متمرکز** هستند. در روش‌های تصادفی عمل کنترل، توسط تک تک گره‌ها به شکل مستقل انجام می‌شود. در روش توزیع شده، کنترل به شکل مشترک توسط کلیه گره‌ها صورت می‌پذیرد. روش‌های متمرکز که در آن‌ها عمل کنترل و مدیریت تنها توسط یک گره مرکزی صورت می‌پذیرد، به علت مشکلاتی که دارند، امروزه کاربرد چندانی در شبکه‌های کامپیوتری ندارند. از جمله معایب روش متمرکز می‌توان به کندی و هزینه بالای آن اشاره کرد. مشکل دیگر این است که در صورت خرابی گره مرکزی، کل عملیات به اشتراک گذاری رسانه، مختل می‌شود.

ما در این فصل ضمن آشنایی با روش‌های نام برده شده، با اجزای مختلف شبکه نیز آشنا می‌شویم.

مثال۱: کدام یک از روش‌های زیر، جزو روش‌های تصادفی به شمار می‌روند؟

۱) ALOHA و Polling ۲) Token و CSMA ۳) ALOHA و CSMA ۴) Token و Polling

☑ **پاسخ:** گزینه «۳» پروتکل‌های ALOHA و CSMA از جمله روش‌های تصادفی به شمار می‌روند. Polling و Token نیز به ترتیب بر روش‌های متمرکز و توزیع شده دلالت دارند.

تخصیص کانال ایستا (Static Channel Allocation)

کانالی را فرض کنید که دو ایستگاه سوویچینگ تلفن را به یکدیگر متصل کرده است. این کانال معمولاً باید تعداد زیادی از تماس‌ها را همزمان انتقال دهد. یک روش قدیمی برای تخصیص چنین کانالی (که telephone trunk نامیده می‌شود) مابین چندین کاربر، استفاده از روش FDM است که در فصل دوم با آن آشنا شدیم. اگر N کاربر وجود داشته باشد، پهنای باند می‌تواند به N بخش برابر تقسیم شود تا هر کاربر از سهم خود استفاده کند. از آنجا که هر کاربر باند فرکانس جداگانه‌ای دارد، تداخلی بین کاربران به وجود نمی‌آید. FDM تنها زمانی که تعداد کاربران کم و ثابت باشد و هر کدام از آن‌ها نیز بارِ (load) ترافیکی بالایی داشته باشد (مانندcarries switching offices)، مکانیزم ساده و موثری برای تخصیص کانال است. اما اگر تعداد فرستنده‌ها زیاد و غیر ثابت باشد و در نتیجه ترافیک نرخ بیت متغیری داشته باشد و یا اینکه الگوی ترافیکی به شکل **انفجاری** (**bursty**) باشد، استفاده از FDM بدون مشکل نخواهد بود.

تذکر۱: منظور از الگوی ترافیکی انفجاری، ترافیکی است که گاهی اوقات بسیار کم بوده و سپس در پاره‌ای از اوقات ناگهان رشد قابل توجهی می‌کند و مجدداً این رویه تکرار می‌شود.

اگر پهنای باند به N بخش تقسیم شود و کم‌تر از N کاربر تمایل به برقراری ارتباط داشته باشند، بخش‌های بسیاری بدون استفاده باقی می‌مانند و در واقع تلف می‌شوند. از طرف دیگر، اگر بیش از N کاربر بخواهند تبادل داده داشته باشند، به علت کمبود پهنای باند، باید از برخی کاربران، حق استفاده از کانال گرفته شود.

به هر حال حتی اگر فرض کنیم که تعداد کاربران مقدار ثابت N باشد، تقسیم کانال به صورت زیرکانال‌های ایستا و غیر قابل تغییر، مسلماً کارایی لازم را نخواهد داشت. مشکل اینجا است که زمانی که برخی از کاربران غیر فعال باشند، پهنای باند آن‌ها عملاً از دست می‌رود. در این حالت، نه تنها خود آن کاربران از آن قسمت از پهنای باند استفاده‌ای نمی‌کنند؛ بلکه هیچ کاربر دیگری نیز امکان استفاده از آن‌ها را نخواهد داشت. از این گذشته، در بسیاری از سیستم‌های کامپیوتری، ترافیک داده، اغلب به شکل انفجاری است. لذا اکثر کانال‌ها در اغلب زمان‌ها، بدون استفاده باقی می‌مانند. ضعف کارایی FDM استاتیک را به راحتی می‌توان توسط محاسبه ساده‌ای از **تئوری صف** (**Queuing Theory**) نشان داد.

نکته۱: با استفاده از تئوری صف ثابت می‌شود که میزان انتظار در صف در صورت استفاده از روش ایستا و با فرض وجود N عدد ایستگاه، N برابر حالتی است که از روش پویا استفاده کنیم.

در علم شبکه اغلب فاکتورها به صورت میانگین در نظر گرفته می‌شوند. به عنوان مثال: میانگین نرخ تولید بسته در واحد زمان (α)، میانگین انتظار در صف (T) و ... در تئوری صف از مفاهیم توزیع‌های احتمال برای مدل‌سازی ترافیک ورودی شبکه استفاده می‌شود. از جمله معروف‌ترین این توزیع‌ها، توزیع نمایی و پواسون است.

چنانچه میانگین نرخ ورود اطلاعات (بسته‌ها) در واحد زمان α و میانگین نرخ ارائه سرویس برابر μ باشد آن‌گاه مدت زمان انتظار در صف در حالت پویا برابر می‌شود با:

$$T = \frac{1}{\mu - \alpha}$$

دقت کنید که میانگین نرخ ارائه سرویس، عکس میانگین زمان ارائه سرویس (T_s) می‌باشد. منظور از T_s در اینجا همان t_{trans} است.

با توجه به تعاریف فوق و علم احتمال، میانگین فاصله زمانی ورودی بسته‌ها به داخل شبکه برابر $\frac{1}{\alpha}$ و میانگین زمان سرویس‌دهی برابر $\frac{1}{\mu}$ خواهد بود.

مثال۲: کابل به اشتراک گذاشته شده‌ای که 100 ایستگاه از آن استفاده می‌کنند را در نظر بگیرید. اگر میانگین نرخ ورود بسته‌ها به کابل برابر 1000 بسته در ثانیه و پهنای باند برابر 1Gbps باشد، میانگین مدت زمان انتظار در صف به ترتیب از راست به چپ چنانچه از روش تخصیص ایستا و پویا استفاده کنیم تقریباً برابر کدام گزینه است؟ (طول هر بسته برابر 1kb است)

۱) $1ms$ و $10\mu s$ ۲) $10\mu s$ و $1ms$ ۳) $1\mu s$ ،$1ms$ ۴) $1ms$ ،$1\mu s$

☑ **پاسخ:** گزینه «۲» $L = 10^3 b$ و $R = 10^9 bps$ و $\alpha = 1000$ و $N = 100$

$$\mu = \frac{1}{T_s} = \frac{R}{L} = \frac{10^9}{10^3} = 10^6$$

میانگین مدت زمان انتظار در صف برای حالت پویا برابر است با:

$$T = \frac{1}{\mu - \alpha} = \frac{1}{10^6 - 10^3} = \frac{1}{999 \times 10^3} \simeq 10^{-5}\,sec = 10\mu\,sec$$

طبق نکته ذکر شده کافی است عدد بدست آمده را ضرب در N (یعنی 1000) کنیم تا میانگین مدت زمان انتظار در صف در حالت ایستا بدست آید. به عنوان توضیح بیشتر و علت این مسئله باید گفت که در حالت ایستا مقدار R (پهنای باند) بر N تقسیم شده و مقدار α نیز بر N تقسیم می‌شود.

آیا می‌توانید به این مثال بدون راه حل پاسخ دهید؟! (به نکته ۱ مراجعه کنید)

تذکر۲: علاقمندان به مطالعه بیش‌تر آگاه باشند که تئوری صف در برخی از دانشگاه‌ها در مقطع کارشناسی ارشد در قالب درس ارزیابی کارایی شبکه‌های کامپیوتری، تدریس می‌شود.

روش دیگری که برای تخصیص کانال ایستا می‌توان متصور بود، همان روش TDM است که در آن، کاربر در زمان‌های مشخصی می‌تواند به کانال دسترسی پیدا کند. به هر ترتیب، روش تخصیص کانال ایستا در اکثر موارد روش بهینه‌ای به شمار نمی‌رود و به عبارتی بهتر، استفاده بهینه‌ای از پهنای باند کانال نمی‌کند. گزینه بهتر، استفاده از تخصیص کانال پویا می‌باشد.

نکته۲: حذف رخداد تصادم و مدیریت ساده‌تر کانال، مزیت‌های تخصیص کانال ایستا به شمار می‌روند.

مثال۳: در مورد استفاده از روش FDM برای به اشتراک گذاری رسانه مشترک، کدام گزینه صحیح نیست؟

۱) زمانی که تنها تعداد کم و ثابتی از کاربران وجود داشته باشند که هر کدام از آن‌ها بار (load) ترافیکی پایینی داشته باشند، مکانیزم ساده و مؤثری برای تخصیص کانال است.

۲) اگر الگوی ترافیکی به شکل انفجاری (bursty) باشد، استفاده از FDM کارا نیست.

۳) یک روش قدیمی محسوب می‌شود.

۴) در صورت استفاده از آن اکثر کانال‌ها در اغلب زمان‌ها، بدون استفاده باقی می‌مانند.

☑ **پاسخ:** گزینه «۱» زمانی که تنها تعداد کم و ثابتی از کاربران وجود داشته باشند که هر کدام از آن‌ها بار (load) ترافیکی بالایی داشته باشند (مانندcarries switching offices)، مکانیزم ساده و مؤثری برای تخصیص کانال است.

مثال۴: کدام یک از گزاره‌های زیر صحیح می‌باشد؟

الف) روش تخصیص کانال ایستا در اکثر موارد روش بهینه‌ای به شمار نمی‌رود.

ب) FDM و TDM نمونه‌هایی از تخصیص کانال ایستا هستند.

۱) فقط الف ۲) فقط ب ۳) هر دو ۴) هیچ کدام

☑ **پاسخ:** گزینه «۳» همان‌طور که گفته شد، FDM و TDM از آنجا که نمونه‌هایی از تخصیص کانال ایستا هستند، کارایی بالایی ندارند.

مثال۵: یک روش کنترل دسترسی به رسانه، می‌تواند استفاده از مالتی پلکس کردن زمانی ثابت باشد. اگر فرض کنیم اندازه هر slot، مدت زمان لازم برای ارسال 100 بیت به علاوه تأثیر انتشار انتها به انتها باشد و با در نظر گرفتن این که نرخ ارسال داده‌ها 10Mbps، طول کانال 8km و سرعت انتشار امواج $2\times10^8\ \mathrm{m/s}$ باشد، اگر تعداد 100 ایستگاه داشته باشیم حداکثر نرخ ارسال هر ایستگاه چقدر است؟ (برحسب kbps)

۱) 20 ۲) 25 ۳) 100 ۴) 50

☑ **پاسخ:** گزینه «۱»

$$R=10^7\ \mathrm{bps},\ d=8\times10^3\ \mathrm{m},\ V=2\times10^8\ \mathrm{m/s},\ N=100$$

ابتدا مدت زمان هر slot را محاسبه می‌کنیم.

$$t_{slot}=\frac{d}{v}+\frac{100}{R}=\frac{8\times10^3}{2\times10^8}+\frac{10^2}{10^7}=4\times10^{-5}+10^{-5}=5\times10^{-5}\mathrm{s}$$

حال تعداد slotهای موجود در یک ثانیه را با یک تناسب ساده محاسبه می‌کنیم:

$$\frac{\text{ثانیه}}{\text{اسلات}}:\frac{5\times10^{-5}}{1}=\frac{1}{x}\Rightarrow x=2\times10^4$$

بنابراین برای کل ایستگاه‌ها در هر ثانیه 2×10^4 اسلات وجود دارد. در این صورت در هر ثانیه برای هر ایستگاه $\frac{2\times10^4}{100}=200$ اسلات وجود خواهد داشت. از طرفی حداکثر میزان داده‌ای که هر ایستگاه می‌تواند در بازه زمانی خویش ارسال کند برابر 100 بیت است. لذا حداکثر نرخ ارسال هر ایستگاه در کل برابر می‌شود با $100\times200=20\mathrm{kbps}$

تخصیص کانال پویا (Dynamic Channel Allocation)

قبل از آنکه به بررسی روش‌های مختلف تخصیص کانال پویا بپردازیم، بهتر است مسئله تخصیص را قاعده بندی کنیم. 5 فرضیه زیر، پایه و اساس مطالب این بخش هستند (دقت کنید که تنها یکی از فرضیات 4 و 5 و همچنین یکی از فرضیات 6 و 7 قابل انتخاب است. بنابراین تعداد کل فرضیات، همان 5 عدد می‌شود):

۱ـ مدل ایستگاه: مدل ما شامل N ایستگاه مستقل از هم می‌باشد (کامپیوترها، تلفن‌ها، وسایل ارتباط شخصی و ...) که هر یک به نوبه خود توسط برنامه یا کاربری که دارند، فریم‌هایی را برای ارسال تولید می‌کنند. احتمال آنکه یک فریم در طول بازه زمانی Δt تولید شود برابر است با $\nu\Delta t$ که ν برابر با مقدار نرخ ورود یک فریم جدید است و مقدار ثابتی دارد. به محض تولید فریم، ایستگاه بلوکه شده و تا زمانی که فریم با موفقیت ارسال شود، هیچ کاری انجام نمی‌دهد.

۲ـ فرض کانال منفرد (Single): کانال مشترکی وجود دارد که همه می‌توانند از آن استفاده کنند. کلیه ایستگاه‌ها می‌توانند از طریق همین کانال به ارسال و دریافت داده مشغول شوند. از نظر سخت‌افزاری کلیه ایستگاه‌ها مشابه هستند اما از نظر نرم‌افزاری و پروتکل‌هایی که در آن‌ها در حال اجرا است، می‌توانند با هم متفاوت باشند.

۳ـ فرض تصادم (Collision): اگر دو فریم همزمان با هم ارسال شوند و سیگنال‌های آن‌ها با هم برخورد کنند، اصطلاحاً گفته می‌شود که تصادم به وجود آمده است. همه ایستگاه‌ها می‌توانند بروز تصادم را تشخیص دهند. فریمی که با تصادم مواجه شده باشد، مجدداً باید ارسال شود. خطای دیگری غیر از آنچه تصادم باعث می‌شود، وجود ندارد.

۴ـ زمان پیوسته (Continuous Time): فریم‌ها در هر زمانی می‌توانند ارسال شوند. به عبارتی دیگر لحظه‌ی آغاز ارسال فریم، هر موقعی می‌تواند باشد.

۵ـ بازه (اِسلات)های زمانی: زمان به فاصله‌های گسسته که اِسلات (slot) نام دارد، تقسیم می‌شود. ارسال فریم، همیشه باید در یک اسلات زمانی آغاز شود. اسلات ممکن است شامل 0، 1 یا تعداد بیش‌تری فریم باشد که به ترتیب متناظر با حالاتِ: اسلات بیکار (idle)، ارسال موفق یا تصادم است.

نکته۳: احتمال بروز تصادم در حالت بازه‌های زمانی، نصف حالت زمان پیوسته می‌باشد.

۶ـ تشخیص حامل یا گوش دادن (Carrier Sense): ایستگاه‌ها می‌توانند قبل از آنکه از کانال استفاده کنند، با "گوش دادن" به آن متوجه شوند که آیا در حال حاضر، کانال توسط ایستگاه دیگری در حال استفاده است یا خیر. تا زمانی که کانال به حالت بیکار تغییر حالت دهد و آزاد شود، هیچ ایستگاهی نمی‌تواند از آن استفاده کند.

۷ـ عدم تشخیص حامل (No Carrier Sense): ایستگاه‌ها قبل از آنکه بخواهند از کانال استفاده کنند، نمی‌توانند از وضعیت آزاد بودن یا نبودن آن مطلع شوند. بنابراین بدون توجه به وضعیت کانال، داده خود را روی آن ارسال می‌کنند. بنابراین تنها پس از ارسال است که می‌توانند پی به موفق بودن یا نبودن ارسال انجام شده ببرند.

انواع پروتکل‌های دسترسی تخصیص پویا

امروزه پروتکل‌های بسیاری برای تخصیص بندی کانال مشترک، شناخته شده است. در ادامه این فصل، ما با معروف‌ترین آن‌ها آشنا خواهیم شد.

ALOHA

تاریخچه این روش که قدیمی‌ترین روش دسترسی به کانال مشترک نیز می‌باشد، به سال 1970 میلادی برمی‌گردد. جالب است بدانیم که در آمریکا و هاوایی، واژه ALOHA به معنای سلام و درود می‌باشد. این پروتکل، به دو شکل Pure ALOHA و Slotted ALOHA وجود دارد.

Pure ALOHA

ایستگاه کاربر **هر وقت** داده‌ای برای ارسال داشته باشد، بدون آنکه کانال را بررسی کند، داده خود را ارسال می‌کند. امکان بروز تصادم در چنین حالتی وجود دارد، چرا که این احتمال وجود دارد که سیگنال‌های متفاوتی از چندین فرستنده مختلف، روی کانال مشترک به طرف مقصد خویش انتشار می‌یابند. گیرنده با توجه به آنکه انتقال، موفقیت‌آمیز بوده یا خیر، پیام‌های ACK یا NACK را ارسال می‌کند (فرکانسACK/NAK، معمولاً متفاوت با فرکانس ارسال کانال انتقال است). وجود تصادم، به معنای ضرورت ارسال مجدد است. فرستنده، ارسال مجدد را پس از تاخیر زمانی **اتفاقی** (random) انجام می‌دهد (البته برای جریان‌های پیوسته، مانند صوت و ویدئو، ارسال مجدد انجام نمی‌شود). ضمناً گیرنده از زمان دقیق ارسال مطلع است.

ایده کلی Pure ALOHA به‌صورت زیر است:

۱ـ اگر بسته‌ای برای ارسال داری، بدون بررسی کانال، آن را ارسال کن.

۲ـ اگر بسته‌ها با تصادم مواجه شدند، پس از گذشتن زمان تصادفی، آن‌ها را مجدداً ارسال کن.

تذکر۳: کشف تصادم با گوش کردن به کانال جداگانه دیگری که نقش بازخورد (feedback) را دارد، انجام می‌شود.

مثال۶: در کدام روش تخصیص کانال، ایستگاه هر زمانی که داده‌ای برای ارسال پیدا کرد، آن را بدون توجه به وضعیت کانال ارسال می‌کند؟

۱) روش‌های ایستا ۲) Pure ALOHA ۳) Slotted ALOHA ۴) CSMA/CD

☑ **پاسخ**: گزینه «۲» در Pure ALOHA ، ایستگاه کاربر هر وقت داده‌ای برای ارسال داشته باشد، آنرا ارسال می‌کند. گزینه‌های سوم و چهارم را در ادامه درس بررسی خواهیم کرد.

گذردهی پروتکل Pure ALOHA

هدف این قسمت، بررسی مقداری کارایی در پروتکل ALOHA است. فرض می‌کنیم که طول بسته‌ها ثابت بوده و ارسال بسته در زمان واحدی انجام می‌شود. منظور از **گذردهی** یا **throughput** که آن را با S نشان می‌دهیم، تعداد بسته‌هایی است که با موفقیت (بدون تصادم) در واحد زمان ارسال شده‌اند. منظور از بار **اِعمال شده (G یا offered load)**، تعداد تلاش‌ها برای ارسال بسته‌ها **در هر واحد زمانی** است. منظور از هر **واحد زمانی**، زمان لازم برای انتقال یک بسته است (t_{trans}).

تذکر۴: $S < G$ می‌باشد، اما مقدار S به G بستگی دارد.

با استفاده از مفهوم توزیع پواسون، احتمال آنکه k ارسال در t واحد زمانی به وقوع بپیوندد برابر است با: $P[k,t] = \frac{(Gt)^k \times e^{-Gt}}{k!}$

ظرفیت پروتکل دسترسی چندگانه برابر است با ماکزیمم مقدار S بر روی مقادیر مختلف G. یعنی داریم:

$S =$ احتمال ارسال موفق × نرخ تلاش‌های صورت گرفته برای ارسال بسته

$= G \times$ احتمال آن که هیچ بسته دیگری با تلاش صورت گرفته همپوشانی پیدا نکند

$= G \times$ احتمال آن که هیچ تلاشی برای ارسال در دو واحد زمانی انجام نشود

$= Ge^{-2G}$

بنابراین گذردهی Pure ALOHA برابر است با: $\mathbf{S = Ge^{-2G}}$

که در آن S یا گذردهی برابر است با تعداد بسته‌هایی است که با موفقیت (بدون تصادم) در واحد زمان ارسال شده‌اند و G معرف تعداد تلاش‌ها برای ارسال بسته‌ها در هر واحد زمانی است.

مثال۷: تعدادی کاربر برای ارسال بسته‌های خود که 100 بایت طول دارند، روی یک لینک با ظرفیت 12Mbps، با استفاده از روش Pure ALOHA با هم رقابت می‌کنند. اگر فرض کنیم تعداد بسته‌های ارسالی هر کاربر در هر ثانیه، 5 عدد باشد و گذردهی نیز به‌صورت $S = e^{-2}$ بدست آمده باشد، تعداد کاربران کدام است؟

۱) 300 ۲) 200 ۳) 3000 ۴) 2000

☑ **پاسخ:** گزینه «۳» با توجه به گذردهی داده شده و مقایسه آن با فرمول گذردهی روش Pure ALOHA ، می‌توان نتیجه گرفت که مقدار G برابر یک بوده است. همان‌طور که گفتیم، G تعداد تلاش‌ها برای ارسال بسته‌ها در هر واحد زمانی است و هر واحد زمانی برابر است با t_{trans}.

$$t_{trans} = \frac{L}{R} = \frac{100 \times 8}{12 \times 10^6} = \frac{2}{3} \times 10^{-4} \text{ sec}$$

بنابراین تعداد تلاش‌هایی که در طول $\frac{2}{3} \times 10^{-4}$ ثانیه رخ می‌دهد برابر 1 (همان G) است. حالا می‌خواهیم تعداد تلاش‌های صورت گرفته در هر ثانیه (و نه هر واحد زمانی)، را محاسبه کنیم. هر کاربر در هر ثانیه، 5 بسته ارسال می‌کند لذا با فرض وجود N کاربر، تعداد کل بسته‌های ارسالی در هر ثانیه برابر می‌شود با: $5 \times N$. حال با استفاده از یک تناسب ساده داریم:

$$\frac{\text{بسته}}{\text{ثانیه}} : \frac{5N}{1} = \frac{1}{\frac{2}{3} \times 10^{-4}} \Rightarrow N = 3000$$

با توجه به اثبات فرمول گذردهی روش Pure ALOHA داریم:

احتمال ارسال موفق (در بار اول): e^{-2G}

احتمال ارسال موفق پس از بروز n تصادم: $(1 - e^{-2G})^n e^{-2G}$

تعداد تلاش برای ارسال موفق: e^{2G}

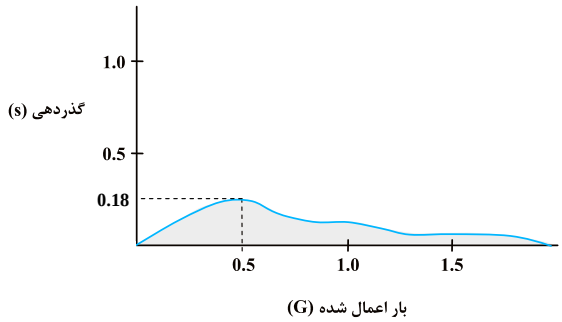
زمان آسیب‌پذیری: $2t_{trans}$

اِرلانگ (Erlang)، واحد بدون بعدی است که برای اندازه‌گیری گذردهی از آن استفاده می‌شود. به جریان ترافیک یک بسته در هر زمان انتقال، اِرلانگ گفته می‌شود.

نکته۴: در بهترین شرایط و زمانی که از کانال بیش‌ترین استفاده شود، گذردهی روش pure ALOHA به ازای $G=\frac{1}{2}$ بدست آمده و برابر 18% (0.18) یا همان $\frac{1}{2e}$ می‌باشد.

به عبارتی دیگر می‌توان گفت که بیش‌ترین گذردهی روش Pure ALOHA برابر با 0.18 اِرلانگ است.

شکل ۱، رابطه بین S و G را در پروتکل Pure ALOHA نشان می‌دهد.



شکل ۱: گذردهی (S) بعنوان تابعی از بار اعمالی (G) در پروتکل Pure ALOHA

مثال۸: فرض کنید در کانالی با ظرفیت 1Mbps، از روش Pure ALOHA استفاده شده باشد. در این صورت کدام گزینه نمی‌تواند مقدار گذردهی این کانال باشد؟

۱) 200Kbps ۲) 180Kps ۳) 100Kbps ۴) 135Kps

☑ **پاسخ:** گزینه «۱» دقت کنید که ماکزیمم گذردهی 0.18، مربوط به لایه فیزیکی ظرفیت کانال است؛ بنابراین اگر شما یک لینک با ظرفیت 1Mbps نیز خریداری کنید اما از روش Pure ALOHA استفاده کنید، حداکثر گذردهی نمی‌تواند از $180\text{Kbps}(1\text{Mbps}\times 0.18)$ بیش‌تر شود! لذا در این حالت دسترسی به 200Kbps غیر ممکن است.

پروتکل Slotted ALOHA

این پروتکل که **reservation ALOHA** یا **r-ALOHA** نیز نامیده می‌شود، نیاز به کلاک مشترک بین ایستگاه زمینی و ماهواره دارد. هر سه سیستم (گیرنده، ماهواره و فرستنده)، هر n میلی ثانیه یکبار به تبادل بسته‌ها مشغول می‌شوند. این رویه، از یک سیستم انتقال سنکرون تبعیت می‌کند یعنی گره‌ها باید با یکدیگر سنکرون باشند (اما در Pure ALOHA گره‌ها با یکدیگر سنکرون نبودند). در Slotted ALOHA، زمان به قسمت‌هایی که آن را اِسلات (slot) می‌نامیم، تقسیم می‌شود. شروع ارسال فریم‌ها تنها در آغاز هر اسلات امکان پذیر است (اما در Pure ALOHA، در هر زمانی می‌توانست ارسال آغاز شود). اندازه هر اسلات برابر است با زمان انتقال بسته (transmission time). هر وقت که بسته‌ای برای انتقال آماده شد، باید تا اسلات بعدی صبر کند.

ایده کلی Slotted ALOHA به صورت زیر است:

۱ـ اگر داده‌ای برای ارسال داری، صبر کن تا نوبت اسلات زمانیت برسد. آنگاه بدون بررسی کانال، داده را ارسال کن.

۲ـ اگر بسته‌ها با تصادم مواجه شدند، پس از گذشتن زمان تصادفی، آن‌ها را مجدداً ارسال کن.

مثال۹: کدام گزینه در مورد پروتکل Slotted ALOHA صدق نمی‌کند؟

۱) شروع ارسال فریم‌ها تنها در آغاز هر اسلات امکان پذیر است.
۲) اندازه هر اسلات برابر است با زمان رفت و بازگشت بسته.
۳) این پروتکل نیاز به کلاک مشترک بین ایستگاه زمینی و ماهواره دارد.
۴) نام دیگر آن reservation ALOHA یا r-ALOHA می‌باشد.

☑ **پاسخ:** گزینه «۲» اندازه هر اسلات برابر است با زمان انتقال بسته (transmission time). با توجه به متن درس، سایر گزینه‌ها صحیح هستند.

مدرسان شریف

فصل پنجم

« لایه شبکه »

همان‌طور که در فصل اول اشاره شد، حیاتی‌ترین نقش لایه شبکه، مسیریابی بسته‌ها و تامین کیفیت سرویس (QoS) در شبکه است. البته از دیگر وظایف این لایه کنترل جریان، کنترل ازدحام، ایجاد و انحلال تبادل داده در روش‌های اتصال‌گرا، نگاشت و تطبیق پروتکل‌ها به جهت امکان ارتباط بین شبکه‌ای (internetworking) و ... است. اما به هر حال وظیفه اصلی این لایه، انتقال پیام و داده از مبداء به مقصد است. بدیهی است برای نیل به این هدف ممکن است داده از گام‌ها (هاپ[hop]ها) و مسیریاب‌های بسیاری عبور کند. لازم به ذکر است که هدف این لایه، با هدف لایه پیوند داده که در فصول قبل با آن آشنا شدیم، کاملاً متفاوت است. لایه پیوند داده، سودای کم‌تری در سر می‌پروراند و تنها هدف آن، انتقال داده از یک طرف سیم تا طرف دیگر آن (نقطه به نقطه) است. در حالی که وظیفه لایه شبکه انتقال داده به صورت انتقال میزبان به میزبان (منبع به منبع) می‌باشد.

تذکر۱: واژه hop در اصطلاح مسیریابی، به تعداد مسیریاب‌هایی اطلاق می‌شود که بسته از آن‌ها عبور می‌کند.

زیرشبکه (subnet)

زیرشبکه به شبکه‌ای گفته می‌شود که بخشی از یک شبکه بزرگتر را تشکیل داده است. البته بر اساس مدل مرجع OSI، به لایه‌های پایینی لایه انتقال (transport)، نیز زیر شبکه گفته می‌شود (یعنی لایه‌های شبکه، پیوند داده و فیزیکی).

تذکر۲: در فصل اول، تعریف دیگری را برای زیرشبکه شاهد بودیم.

زمانی که در زیر شبکه، تعداد بسته‌های موجود بسیار زیاد شود، پدیده ازدحام (congestion) رخ می‌دهد. در این فصل در رابطه با مفاهیم ذکر شده و کنترل ازدحام صحبت خواهیم کرد.

ارائه سرویس به لایه انتقال

لایه شبکه از طریق «واسطِ لایه شبکه-لایه انتقال»، به لایه انتقال، سرویس ارائه می‌دهد. این واسط به دلیل اینکه در حقیقت واسطی است میان حامل (carrier) و مشتری (customer)، از جنبه دیگری نیز اهمیت دارد. به بیان دیگر واسط «لایه شبکه-لایه انتقال»، مرز انتهایی زیرشبکه است. حامل، اغلب اوقات پروتکل‌ها و واسط‌های لایه‌های شبکه و بالاتر از آن را کنترل می‌کند و وظیفه آن تحویل بسته‌هایی است که توسط مشتریانش به آن واگذار شده است. به همین خاطر تعیین این واسط، از اهمیت خاصی برخوردار است. سرویس‌های لایه شبکه، با توجه به اهداف کلان زیر طراحی می‌شوند:

۱ـ سرویس‌ها باید مستقل از توپولوژی زیرشبکه باشند.

۲ـ تعداد، نوع و توپولوژی زیرشبکه باید از دید لایه انتقال پنهان نگهداری شوند.

۳ـ آدرس‌های شبکه‌ای که در دسترس لایه انتقال قرار دارند، حتی در طول LANها و WANها باید از طرح شماره‌ای (numbering plan) یکسان استفاده کنند. بنابراین سیستم آدرس‌دهی استاندارد و مشخصی مورد نیاز است.

مثال۱: در طراحی لایه شبکه کدام گزینه صحیح است؟

۱) آدرس‌های شبکه‌ای که در دسترس لایه انتقال قرار دارند، در LANها و WANها باید از طرح شماره‌ای (numbering plan) غیر یکسان استفاده کنند.

۲) بهتر است موارد مربوط به زیرشبکه (مانند تعداد، نوع و توپولوژی آن) از دید لایه انتقال پنهان باشد.

۳) بهتر است سرویس‌ها به توپولوژی زیرشبکه وابستگی داشته باشند.

۴) ۱و ۲

☑ **پاسخ:** گزینه «۲» همان‌طور که ذکر شد، آدرس‌های شبکه‌ای که در دسترس لایه انتقال قرار دارند، حتی در طول LANها و WANها باید از طرح شماره‌ای (numbering plan) یکسان استفاده کنند (نادرستی گزینه ۱). سرویس‌ها نیز باید مستقل از توپولوژی زیرشبکه باشند (نادرستی گزینه ۳).

اما سوال محوری که اینجا می‌تواند مطرح شود این است که لایه شبکه باید سرویس اتصال‌گرا (connection-oriented) را ارائه نماید یا سرویس بدون اتصال (connectionless) را ؟

تذکر۳: سرویس‌های اتصال‌گرا و بدون اتصال در فصل اول مورد مطالعه قرار گرفت.

یک گروه (که جامعه اینترنتی[Internet Community]مثالی از آن است) اعتقاد دارد که وظیفه‌ی زیرشبکه، صرفاً انتقال بیت‌ها است و نه بیش‌تر. از نقطه نظر آن‌ها (که بر پایه تجربه عملی 30 ساله با شبکه‌های کامپیوتری عملی و واقعی قرار دارد)، زیرشبکه‌ها صرف نظر از طرز طراحی آن‌ها، ذاتاً غیرقابل اطمینان هستند. لذا میزبان‌ها باید با این واقعیت کنار آمده و خودشان عملیات کنترل خطا (یعنی تشخیص و تصحیح خطا) و کنترل جریان را انجام دهند. طبق این عقیده، سرویس‌های شبکه بدون اتصال می‌شوند و تنها شامل بسته‌های ارسال و دریافت ساده به اضافه موارد جزئی دیگر می‌باشند. در عمل، نیازی به مرتب کردن بسته‌ها و کنترل جریان نیست چراکه خود میزبان‌ها این کار را انجام می‌دهند و انجام دوباره‌ی این اعمال، بهره خاصی را نتیجه نمی‌دهد. علاوه بر این، هر بسته باید حاوی آدرس کامل مقصد باشد زیرا هر بسته مستقل از بسته‌های قبلی خود (در صورت وجود) ارسال می‌شود.

گروه دیگر (که شرکت‌های تلفنی مثالی از آن است)، اعتقاد دارند که زیرشبکه باید قابل اطمینان بوده و سرویس اتصال‌گرا را ارائه دهد. طبق این عقیده، ارتباطات باید خواص زیر را داشته باشند:

۱ـ قبل از ارسال داده، پروسه لایه شبکه در طرف فرستنده باید با لایه متناظرش در طرف مقصد، ارتباطی را تنظیم (set up)کند. این ارتباط که شناسه منحصر به فردی را بدست می‌دهد، تا زمانی که کل داده ارسال شود، مورد استفاده قرار گرفته و در نهایت آزاد می‌شود.

۲ـ وقتی ارتباطی تنظیم شد، دو پردازش می‌توانند در خصوص پارامترهای کیفیت و هزینه سرویس ارائه شده، وارد مذاکره شوند.

۳ـ انتقال داده در هر دو جهت صورت گرفته و بسته‌ها طبق ترتیب، تحویل داده می‌شوند.

۴ـ کنترل جریان به طور خودکار اِعمال می‌شود تا از ارسال بیش از حد سریع داده‌ها از طرف فرستنده و به مشکل افتادن گیرنده جلوگیری شود.

سایر ویژگی‌ها همانند تضمین تحویل، تأیید صریح تحویل و اولویت بالای بسته‌ها اختیاری هستند. سرویس بدون اتصال مشابه سیستم پست و سرویس اتصال‌گرا مانند سیستم تلفن است.

بحث بین اتصال‌گرا و بدون اتصال به این بستگی دارد که بخواهیم پیچیدگی را در کجا در نظر بگیریم.

نکته۱: در سرویس اتصال‌گرا، پیچیدگی در لایه شبکه (زیر شبکه) و در سرویس بدون اتصال، این پیچیدگی در لایه انتقال (میزبان) اعمال می‌شود.

طرفداران سرویس بدون اتصال می‌گویند که در صورت استفاده از این سرویس، توان مصرفی محاسبه کاهش یافته و دلیلی برای اعمال پیچیدگی بر روی میزبان‌ها وجود ندارد. ضمن اینکه برای برخی کاربردها مانند دیجیتال کردن صوت و داده‌های بلادرنگ، سرعت مهمتر از دریافت صحیح است.

اما از طرفی دیگر، طرفداران سرویس اتصال‌گرا می‌گویند که کاربران علاقه‌ای به اعمال پیچیدگی بر روی پروتکل‌های لایه انتقالِ ماشین‌های خود ندارند، بلکه آنچه آن‌ها می‌خواهند شبکه قابل اطمینان و یک ارتباط بدون مشکل (trouble-free) است.

مثال۲: کدام گزینه صحیح نیست؟

۱) انتقال در لایه شبکه، به صورت میزبان به میزبان (منبع به منبع) است.

۲) در سرویس بدون اتصال، پیچیدگی در لایه انتقال (میزبان) اعمال می‌شود.

۳) در سرویس اتصال‌گرا، پیچیدگی در لایه شبکه (زیر شبکه) اعمال می‌شود.

۴) جامعه اینترنتی با روش اتصال‌گرا موافق است.

☑ **پاسخ:** گزینه «۴» جامعه اینترنتی [Internet Community] اعتقاد دارد که وظیفه زیر شبکه صرفاً انتقال بیت‌ها است و نه چیزی بیش‌تر. از نقطه نظر آن‌ها زیرشبکه‌ها صرف نظر از طرز طراحی آن‌ها، ذاتاً غیرقابل اطمینان هستند. لذا میزبان‌ها باید با این واقعیت کنار آمده و خودشان عملیات کنترل خطا (یعنی تشخیص و تصحیح خطا) و کنترل جریان را انجام دهند. بنابراین جامعه اینترنتی طرفدار روش بدون اتصال است.

دو مسئله اصلی در اینجا قابل توجه است:

۱ـ شبکه اتصال‌گرا باشد (و نیاز به مرحله setup داشته باشد) و یا بی‌اتصال (بدون نیاز به setup)

۲ـ شبکه قابل اطمینان باشد (بدون تلفات داده، تکرار در داده‌ها یا بسته‌های ناسالم) یا غیر قابل اطمینان (امکان گم شدن بسته‌ها، تکرار در داده‌ها و یا دریافت بسته‌های ناسالم وجود داشته باشد).

از جنبه تئوری، چهار حالت ممکن است اتفاق بیفتد. اما دو ترکیب اتصال‌گرای قابل اطمینان و بدون اتصال غیرقابل اطمینان، بیش‌تر از بقیه حالات در کانون توجه قرار می‌گیرد.

نکته۲: اینترنت، لایه شبکه بدون اتصال دارد و در مقابل، شبکه‌های ATM ، دارای لایه شبکه اتصال‌گرا هستند.

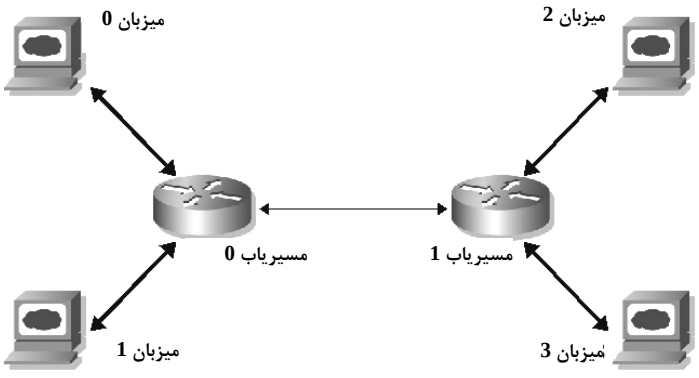
شاید این سوال برای شما پیش آمده باشد که چگونه اینترنت روی زیر شبکه‌ای که بر پایه ATM قرار دارد، کار می‌کند. پاسخ این است که میزبان مبدأ، ابتدا یک ارتباط لایه شبکه ATM را به طرف میزبان مقصد ایجاد کرده و سپس بسته‌های مستقل را از روی آن ارسال می‌کند (جدول ۱). هر چند این روش کار می‌کند اما مسلماً کم بازده است. زیرا برخی عملیات در هر دو لایه انجام می‌شوند. برای مثال لایه شبکه ATM تحویل مرتب بسته‌ها را تضمین می‌کند اما با این حال، TCP همچنان مکانیزم کامل خود را برای مدیریت به ترتیب کردن بسته‌ها از ترتیب خارج شده انجام می‌دهد (در رابطه با TCP در فصل بعد صحبت خواهیم کرد).

جدول ۱: **اجرای TCP/IP روی زیرشبکه**

E-mail	FTP	...
	TCP	
	IP	
	ATM	
	Datalink	
	Physical	

سوویچینگ و انواع آن

یک سوال اساسی که باید به آن پاسخ داد، چگونگی انتقال داده‌ها در داخل شبکه است. زمانی که اندازه شبکه بزرگ می‌شود، به طوری که تعداد زیادی دستگاه در آن قرار گرفته باشد، استفاده از گذرگاه مشترک برای پخش همگانی، مناسب و مقدور نیست. ضمن اینکه اگر بخواهیم از اتصال مستقیم نیز استفاده کنیم، قطعاً تعداد کابل‌های مورد نیاز بسیار زیاد خواهد شد. برای حرکت و انتقال بسته‌ها در شبکه‌های بزرگ باید از عمل سوویچینگ (که برخی اوقات مسیریابی نیز نامیده می‌شود) استفاده نمود (شکل۱). در این مفهوم، سوویچ‌ها ادواتی هستند که برای مسیریابی به کار می‌روند و باعث اتصال گره‌های شبکه به یکدیگر به صورت غیرمستقیم می‌شوند. هر سوویچ دارای تعدادی پورت ورودی و تعدادی پورت خروجی است. وظیفه سوویچ، دریافت اطلاعات از پورت‌های ورودی و هدایت آن‌ها به پورت‌های خروجی است. حتماً می‌توانید حدس بزنید که در مفهوم واقعی شبکه، منظور ما از سوویچ، همان مسیریاب می‌باشد.



شکل ۱: **اتصال گره‌های شبکه توسط سوویچ‌ها**

سه روش کلی برای سوییچینگ وجود دارد: سوییچینگ مداری، سوییچینگ پیغامی و سوییچینگ بسته‌ای.

سوییچینگ مداری (circuit switching)

در سوییچینگ مداری، قبل از آنکه تبادل داده آغاز شود، ابتدا یک مسیر (مدار) بین فرستنده و گیرنده تنظیم می‌شود که کل تبادل داده تا آخر، از طریق همان مسیر صورت می‌گیرد. این مسیر، تنها به فرستنده و گیرنده اختصاص داده می‌شود و ارتباط دیگری به طور معمول حق استفاده از آن را نخواهد داشت. نکته‌ای که باید در این روش به آن توجه داشت این است که در سوییچینگ مداری حتی اگر فرستنده و گیرنده با همدیگر داده‌ای مبادله نکنند، تا زمانی که مسیر را آزاد نکنند، آن مسیر اشغال باقی خواهد ماند. مثال واضح از سوییچینگ مداری، تماس تلفنی در شبکه عمومی سوییچ تلفن یا PSTN(Public Switch Telephone Network) است. زمانی که شما مشغول صحبت هستید، اگر فرد دیگری با شما تماس بگیرد، بوق اشغال خواهد شنید. ضمن اینکه حتی اگر کسی پشت تلفن شما فوت کند (!) و یا اصلاً حرفی هم نزند، خطِ شما همچنان اشغال باقی خواهد ماند تا زمانی که شما گوشی را در جای خود قرار داده و یا تماس را قطع کنید.

بدیهی است که فاز ایجاد مدار اولیه زمان‌بر است. ضمناً در سوییچینگ مداری داده‌ها، بدون آنکه نیاز به بسته‌بندی داشته باشند، به صورت جریانی از بیت‌ها (bit stream) انتقال می‌یابند.

سوییچینگ مداری از به اشتراک گذاشتن خطوط ارتباطی، پشتیبانی چندانی نمی‌کند. اما در عوض به خاطر همین موضوع، می‌تواند کارایی و به طور کلی کیفیت سرویس (QoS) را تضمین کند. به‌عنوان مثال می‌تواند با توجه به فاصله و سرعت موجود، ارسال داده را در یک بازه زمانی مشخص تضمین دهد. البته این گونه هم نیست که در سوییچینگ مداری اصلاً امکان به اشتراک گذاری وجود نداشته باشد. روش‌های FDM و TDM که قبل از این مطالعه کردیم، روش‌هایی هستند که در سوییچینگ مداری برای اشتراک گذاری از آن‌ها استفاده می‌شود.

مثال ۳: کدام گزینه در مورد سوییچینگ مداری صحیح نیست؟

۱) این روش از اشتراک گذاری پشتیبانی چندانی نمی‌کند.

۲) نمی‌تواند کارایی (مانند زمان تحویل بسته‌ها) را تضمین کند.

۳) حتی اگر داده‌ای مبادله نشود، خط ارتباطی تا زمان آزاد نشدن، اشغال باقی می‌ماند.

۴) قبل از آنکه تبادل داده آغاز شود، ابتدا یک مسیر بین فرستنده و گیرنده تنظیم می‌شود.

☑ **پاسخ:** گزینه «۲» از آنجا که خط رزرو شده به طور معمول برای یک ارتباط استفاده می‌شود، امکان محاسبه زمان مورد نیاز برای ارسال داده با تخمین مناسبی با استفاده از فرمول $x = vt$ وجود دارد. لذا کارایی در سوییچینگ مداری به طور معمول تضمین می‌شود. گزاره‌های دیگر طبق متن درس صحیح هستند.

سوییچینگ پیغامی (Message Switching)

انتقال داده سوییچینگ پیغامی که در سال 1961 معرفی شد، در حقیقت نسخه قدیمی‌تر سوییچینگ بسته‌ای قلمداد می‌شود. در سوییچینگ پیغامی، کل پیام‌ها توسط هر هاپ در هر نوبت منتقل می‌شوند. هر پیغام برای خود موجودیت مستقلی به شمار می‌رود. لذا این امکان وجود دارد که داده‌ها خارج از نوبت دریافت شوند. ضمن اینکه هر پیغام دارای اطلاعات مربوط به آدرس بوده که در هر سوییچ، از این اطلاعات برای تصمیم‌گیری ارسال به سوییچ بعدی استفاده می‌شود. هر پیغام قبل از ارسال در سوییچ ذخیره شده و پس از آن ارسال می‌شود (stop & forward).

زمانی که از این روش سوییچینگ استفاده می‌شود مابین فرستنده و گیرنده از قبل مسیری تنظیم نمی‌شود. بلکه هر زمان که فرستنده بلوکی از داده را برای ارسال داشته باشد، ابتدا آن بلوک در مسریاب ذخیره شده و سپس به هاپ بعدی ارسال می‌شود. همان طور که اشاره شد، مسیریاب ابتدا منتظر می‌ماند تا کل پیغام را دریافت کند و پس از حصول اطمینان از سالم بودن، آن را ارسال می‌کند. در غیر این صورت و در صورت تشخیص خطا، پیغام مجدداً ارسال می‌شود.

ملاحظه می‌شود این روش برای کاربردهای بلادرنگ نمی‌تواند مفید باشد چرا که تا زمانی که کل پیغام شکل نگیرد، از ارسال آن خودداری می‌شود و به همین دلیل ممکن است تاخیرات طولانی به وجود آید.

سوییچینگ پیغام، **transactional** می‌باشد. بدین معنی که می‌تواند داده را ذخیره کرده و فرمت و نرخ بیت آنرا عوض کرده و سپس آنرا به فرم اولیه و یا شکل دیگری در بیاورد. سوییچینگ پیغامی داده‌ها را از چندین منبع، مالتی پلکس کرده و ارسال می‌کند.

از آنجا که سوییچینگ پیغامی هر پیغام را در گره‌های میانی ذخیره می‌کند، تاخیرِ کلِ ارسالِ انتها به انتها، به طول پیغام و تعداد گره‌های میانی وابسته است. هر گره میانی می‌تواند به نوبه خود باعث افزایش تاخیر به میزان حداقل تاخیر انتقال ورودی یا خروجی‌اش شود. دقت کنید که گره‌ها به علت استفاده از تکنولوژی‌های متفاوت، می‌توانند تاخیرهای انتقال متفاوتی با همدیگر داشته باشند. علاوه بر تاخیر انتقال باید تاخیر انتشار را که به موجب طی کردن مسیر حاصل می‌شود نیز در نظر داشت.

سوییچینگ پیغامی همچنان در ترافیک‌های دورنگاری استفاده می‌شود. البته نسخه بهبود یافته آن که همان سویچینگ بسته‌ای است، به طور گسترده کاربرد دارد.
امتیازات سوییچینگ پیغامی عبارتند از:

ـ کانال‌های داده می‌توانند مابین ارتباطات مختلف به اشتراک گذاشته شوند و در نتیجه استفاده بهینه‌تری از پهنای باند شود.

ـ پیغام‌ها می‌توانند در زمانی که تراکم و ازدحام شبکه بالا می‌رود، موقتاً در سوییچ‌ها ذخیره شوند.

ـ برای مدیریت ترافیک می‌توان از اولویت گذاری استفاده کرد.

ـ آدرس‌دهی پخش همگانی به دلیل آنکه پیغام‌ها را به چندین مقصد تحویل می‌دهد، از پهنای باند استفاده بهینه‌تری می‌کند.

اما اگر بخواهیم اشاره‌ای نیز به مشکلات این روش داشته باشیم باید بگوییم که نداشتن سقفی برای حداکثر اندازه پیغام‌ها یک مشکل اساسی برای این روش به شمار می‌رود.

این مشکل مخصوصاً زمانی که اندازه پیغام‌ها بالا می‌رود خودنمایی می‌کند. با افزایش سایز پیغام‌ها بدیهی است که تاخیر نیز افزایش می‌یابد. ضمناً اگر پیغامی دچار مشکل و خطا شود باید دوباره مجدداً ارسال شود. حال اگر اندازه پیغام بزرگ بوده باشد باید حجم عظیمی از اطلاعات دوباره ارسال شود. از این گذشته باید حافظه موجود در سوییچ‌ها نیز گنجایش ذخیره پیغام‌های بزرگ را داشته باشد. به همین دلیل پیغام‌ها معمولاً در هارددیسک سوییچ‌ها (و نه RAM) ذخیره می‌شوند.

نکته۳: هر چند در سوییچینگ پیغامی زمانی برای ایجاد مسیری بین فرستنده و گیرنده صرف نمی‌شود اما با این حال سرعت آن کم‌تر از سوییچنگ مداری می‌باشد.

مثال۴: کدام گزینه در مورد سوییچینگ پیغامی صحیح نیست؟

۱) اگر زمانی که پورت خروجی سوییچ اشغال باشد، پیغامی وارد سوییچ شود، پیغام از دست خواهد رفت.

۲) یکی از ویژگی‌های سوییچینگ پیغامی، transactional بودن آن است.

۳) امکان از ترتیب خارج شدن داده در آن محتمل است.

۴) در زمانی که تراکم و ازدحام شبکه بالا می‌رود، پیغام‌ها می‌توانند موقتاً در سوییچ‌ها ذخیره شوند.

☑ **پاسخ:** گزینه «۱» به علت آنکه در سوییچینگ پیغامی، پیغام‌های دریافتی بافر می‌شوند، حتی در صورت مشغول بودن مسیرهای خروجی، از دست نخواهند رفت. می‌توان سوییچینگ پیغامی را مثالی از سیستم تاخیری (delay system) و یا سیستم صفی (queuing system) در نظر گرفت.

سوییچینگ بسته‌ای (Packet Switching)

در روش سوییچینگ بسته‌ای، قبل از آغاز تبادل داده، مسیر مشخصی بین فرستنده و گیرنده رزرو نمی‌شود. در این روش کل داده، به قطعات کوچکتری به نام **بسته** تقسیم شده و این بسته‌ها به ترتیب ارسال می‌شوند. البته لزومی ندارد که طول کلیه بسته‌ها برابر باشد. در برخی از شبکه‌ها مانند **ATM (Asynchronous Transfer Mode)** که طول کلیه بسته‌ها برابر است، به هر بسته اصطلاحاً یک **سلول** گفته می‌شود. بنابراین در این روش بسته‌ها با محدودیت طول مواجه هستند به طوری که اندازه ماکزیمم بسته‌ها توسط شبکه مشخص می‌شود. باید دقت کرد که مسیریابی برای هر بسته، به صورت جداگانه صورت می‌پذیرد. به همین خاطر ممکن است کل بسته‌ها از مسیر واحدی عبور نکنند و با گذر از مسیرهای متفاوتی به دست مقصد برسند. در این روش به راحتی می‌توان خط ارتباطی را بین چندین ارتباطِ مختلف، به اشتراک گذاشت. اما در عوض، دیگر امکان ارائه تضمین کیفیت سرویس وجود ندارد. ضمن اینکه به خاطر اینکه هر بسته ممکن است مسیر متفاوتی برای رسیدن به مقصد طی کند، ترتیب ارسال بسته‌ها لزوماً با ترتیب دریافت آن‌ها در گیرنده یکسان نیست. یعنی اگر بسته A قبل از بسته B فرستاده شده باشد، لزومی ندارد که در هنگام دریافت نیز A زودتر از B دریافت شود؛ بلکه چه بسا ممکن است ابتدا B دریافت شود و سپس A. به این امر که دریافت بسته‌ها با ترتیب ارسالشان یکسان نباشد، از **ترتیب خارج شدن یا out-of-order** گفته می‌شود. معمولاً حل این مشکل به پروتکل‌های لایه‌های بالاتر (انتقال)، واگذار می‌شود.

همان‌طور که در شکل ۲ نیز نشان داده شده است، در سوییچنگ بسته‌ای زمان‌های دریافت و ارسال بسته با یکدیگر همپوشانی (overlap) دارند. یعنی هر گره همزمان با دریافت یک بسته، می‌تواند مشغول ارسال بسته دیگری باشد. به همین خاطر میزان تاخیر در سوییچنگ بسته‌ای کم‌تر از سوییچنگ پیغامی است.

نکته۴: برای ترافیک‌های از نوع انفجاری در عمل استفاده از سوییچینگ بسته‌ای مناسب‌تر است.

منظور از ترافیک انفجاری، ترافیکی است که شدت آن با گذر زمان به شدت افت و خیز دارد. یعنی در هر زمان یا نزدیک به صفر است یا خیلی زیاد. اگر برای چنین ترافیکی از سوییچینگ مداری استفاده شود، در زمان‌هایی که ترافیک چندانی وجود ندارد، خط بدون دلیل اشغال باقی می‌ماند و بدین شکل کارایی و بهره‌وری لینک مربوطه، به شدت افت می‌کند.

مثال۵: کدام گزینه در مورد سوییچینگ بسته‌ای صحیح نیست؟

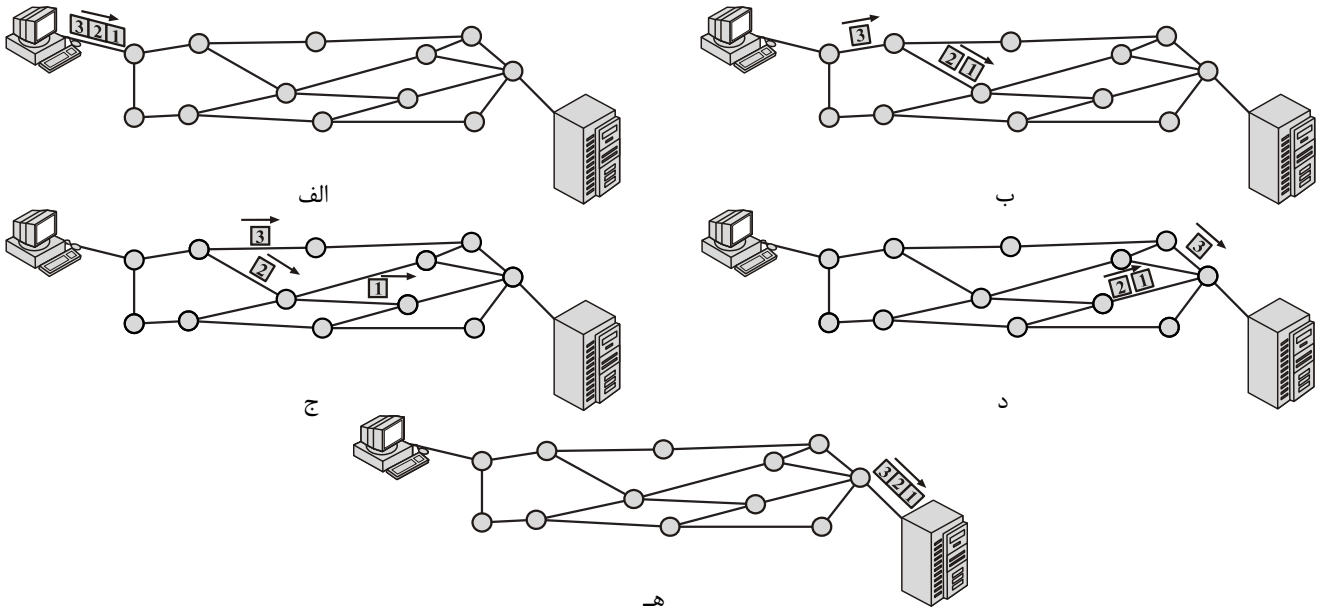
۱) برای ترافیک‌های نوع انفجاری انتخاب مناسبی به شمار نمی‌رود.
۲) احتمال out-of-order شدن بسته‌ها در آن وجود دارد.
۳) ممکن است هر بسته از مسیر متفاوتی نسبت به سایر بسته‌ها ارسال شود.
۴) قبل از آغاز تبادل داده، مسیر مشخصی بین فرستنده و گیرنده رزرو نمی‌شود.

☑ **پاسخ:** گزینه «۱» برای ترافیک‌های از نوع انفجاری استفاده از سوییچینگ بسته‌ای نسبت به سوییچینگ مداری مناسب‌تر است.

اما آیا راهی وجود دارد که بتوان رفتار سوییچینگ مداری را در سوییچینگ بسته‌ای شبیه سازی نمود؟ پاسخ مثبت است. سوییچینگ بسته‌ای خود دو نوع مختلف دارد: شبکه‌های داده‌گرام (Datagram) و شبکه‌های مدار مجازی (Virtual Circuit Network).

شبکه‌های داده‌گرام (Datagram Networks)

در این نوع از شبکه‌ها، که دقیقاً مصداق بارز سوییچینگ بسته‌ای می‌باشند، آدرس مقصد در هر بسته، هاپ بعدی را معین می‌کند و مسیرهای طی شده برای بسته می‌تواند با مسیر مربوط به بسته‌های دیگر کاملاً متفاوت باشد. زیرا با گذشت زمان و تغییر شرایط ممکن است مسیرِ بهترِ قبلی، دیگر بهترین مسیر نباشد. این که کدام مسیر را باید به‌عنوان بهترین مسیر در نظر گرفت، به فاکتورهای مختلفی همچون: هزینه، تاخیر کم‌تر، ترافیک کم‌تر و .... بستگی دارد. در انتقال داده‌گرام، هر بسته برای خود موجودیت مستقلی از سایر بسته‌ها به شمار می‌رود، حاوی سرآیندی است و شامل اطلاعات کاملی از گیرنده و فرستنده مورد نظر می‌باشد. گره‌های میانی، این سرآیند را مورد بررسی قرار داده و با توجه به محتویات آن، لینک مناسبی را که به مقصد بعدی متصل است، انتخاب می‌کنند. در این سیستم، بسته‌ها از مسیر از پیش تعیین شده‌ای عبور نمی‌کنند و گره‌های میانی (که اغلب همان مسیریاب‌ها هستند)، نیازی ندارند تا در رابطه با مسیرهای پیموده شده توسط بسته‌های قبلی اطلاعاتی را ذخیره کنند. نمونه‌ای از شبکه‌های داده‌گرام در شکل ۲ نشان داده شده است.



شکل ۲: سوییچینگ بسته‌ای: داده‌گرام

گاهی اوقات کاربرد (Application)ی که در شبکه در حال اجرا می‌باشد، به تضمین کارایی، نیاز مبرم دارد. به‌عنوان مثال کاربردهای بلادرنگ (real-time) حتماً به تضمین زمانی نیاز دارند. اما برخی دیگر از کاربردها انعطاف بیش‌تری از خود- به‌عنوان مثال نسبت به زمان ـ نشان می‌دهند و به سعی و کوششی که شبکه از خود نشان می‌دهد، اکتفا می‌کنند. اصطلاحاً به شبکه‌هایی که هیچ تضمینی نمی‌دهند اما نهایت سعی خود را برای بهتر انجام دادن وظایف محول شده صورت می‌دهند، **Best Effort** گفته می‌شود. شبکه‌های داده‌گرام، نمونه‌ای از شبکه‌های best effort هستند که معمولاً به شکل سرویس بدون اتصال هستند.

نکته۵: در حال حاضر، شبکه داده‌گرام، رایج‌ترین روش سوییچنگ است که اینترنت هم از آن استفاده می‌کند.

فصل ششم

« لایه انتقال »

لایه انتقال به‌عنوان قلب و هسته کلیه پروتکل‌های ساختار سلسله مراتبی، از اهمیت خاصی برخوردار است. وظیفه این لایه، صرف نظر از شبکه فیزیکی، تامین امکان انتقال داده مقرون به صرفه و **قابل اطمینان** از ماشینِ مبدا تا ماشین مقصد است. بدون لایه انتقال، دیگر چیزی از مفهوم لایه‌بندی شبکه باقی نخواهد ماند. در این فصل به بررسی این لایه خواهیم پرداخت.

تا اینجا دیدیم که هدف و چگونگی ارسال داده در لایه‌های گوناگون، متفاوت می‌باشد. واحد داده در لایه انتقال، سگمنت (segment) نام دارد. جدول ۱، وضعیت ارسال داده در هر لایه را لیست کرده است. خاطر نشان می‌سازیم که واحد داده در لایه کاربرد، پیغام (message) می‌باشد.

جدول ۱: **وضعیت ارسال داده در سه لایه انتقال، شبکه و پیوند داده**

لایه	واحد داده	آدرس استفاده شده	نحوه تحویل داده
انتقال	سگمنت	شماره پورت	تحویل سگمنت به صورت پروسس به پروسس (انتها به انتها)
شبکه	داده‌گرام	آدرس IP	تحویل داده‌گرام به صورت میزبان به میزبان (منبع به منبع)
پیوند داده	فریم	آدرس MAC (فیزیکی)	تحویل فریم به صورت نقطه به نقطه (گره به گره)
فیزیکی	بیت		تحویل بیت به صورت نقطه به نقطه (گره به گره)

مثال۱: نحوه انتقال داده در کدام لایه‌ها به ترتیب میزبان به میزبان و پروسس به پروسس است؟ (به ترتیب از راست به چپ)

۱) پیوند داده، شبکه ۲) شبکه، پیوند داده ۳) شبکه، انتقال ۴) انتقال، شبکه

☑ **پاسخ:** گزینه «۳» با توجه به جدول ۱، نحوه انتقال داده در لایه شبکه به صورت میزبان به میزبان و در لایه انتقال به صورت پروسس به پروسس است.

سرویس‌های پایه(Primitives Service)

سرویس‌های پایه به کاربر (مثلاً برنامه کاربردی)، اجازه دسترسی به سرویس انتقال را می‌دهند. هر سرویس انتقال، سرویس‌های پایه خود را دارد. در این بخش، ابتدا یک مثال ساده و فرضی از سرویس انتقال را بررسی کرده و در ادامه یک مثال واقعی را مطالعه خواهیم نمود.

سرویس انتقال، شبیه به سرویس شبکه می‌باشد؛ اما این دو، تفاوت‌هایی نیز با یکدیگر دارند. مهمترین تفاوت این است که سرویس شبکه، برای مدل کردن سرویس ارائه شده برای شبکه‌های واقعی می‌باشد. در شبکه‌های واقعی، امکان گم شدن بسته‌ها وجود دارد.

نکته۱: سرویس‌های شبکه به طور کلی غیر قابل اطمینان هستند. در مقابل، سرویس (اتصال گرای) انتقال، قابل اطمینان است.

شبکه‌های واقعی، عاری از خطا نیستند و این دقیقاً هدف اصلی لایه انتقال می‌باشد: **تامین سرویس قابل اطمینان بر روی یک شبکه غیر قابل اطمینان.**

به‌عنوان یک مثال، دو پروسه را در نظر بگیرید که توسط خطِ لوله‌هایی (pipes) در UNIX با هم در ارتباط هستند. تصور آن‌ها از ارتباط مابین خود، یک ارتباط کامل است. آن‌ها علاقه‌ای ندارند در رابطه با تصدیق‌ها، گم شدن بسته‌ها، ازدحام و یا موارد دیگر، چیزی بدانند. تنها چیزی که برای آن‌ها مهم است این است که یک ارتباطِ صد درصد قابل اطمینان داشته باشند. پروسه A، داده را در یک طرف خط لوله قرار داده و پروسه B آن داده را از طرف دیگر دریافت می‌کند. این همان وظیفه‌ای است که بر عهده سرویس انتقال اتصال‌گرا گذاشته شده است. عملکرد این سرویس باید به گونه‌ای باشد که کاربران، شبکه را بدون خطا تصور نمایند. از طرفی دیگر، لایه انتقال می‌تواند سرویس غیر قابل اطمینان را نیز ارائه دهد.

تفاوت دوم بین سرویس شبکه و سرویس انتقال آن است که هر کدام برای چه کاربردی طراحی شده‌اند. سرویس لایه شبکه، تنها توسط موجودیت‌های انتقال (transport entities) استفاده می‌شود. تعداد کاربرانی که به طور مستقیم، درگیر کار با سرویس شبکه می‌شوند، ناچیز است. برای کاربر، کار با سرویس انتقال باید ساده و راحت باشد.

مثال۲: کدام گزینه جزو تفاوت‌های سرویس شبکه و سرویس انتقال به شمار نمی‌رود؟

۱) هر کدام برای اهداف جداگانه‌ای طراحی شده‌اند.

۲) سرویس انتقال بر خلاف سرویس شبکه همیشه قابل اطمینان رفتار می‌کند.

۳) تعداد کاربرانی که به طور مستقیم، درگیر کار با سرویس شبکه می‌شوند، ناچیز است.

۴) سرویس شبکه، برای مدل کردن سرویس ارائه شده به شبکه‌های واقعی می‌باشد.

☑ **پاسخ:** گزینه «۲» لایه انتقال می‌تواند سرویس غیر قابل اطمینان را در صورت استفاده از سرویس بدون اتصال، ارائه دهد. درستی سایر گزینه‌ها با توجه به متن درس بدیهی است.

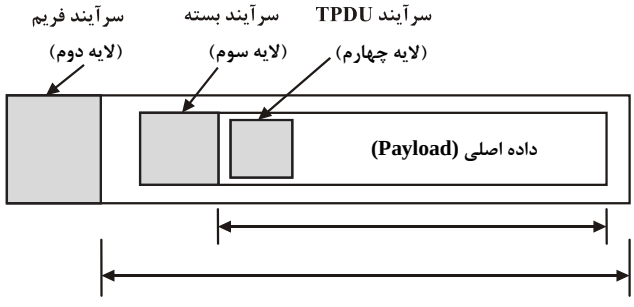
برای روشن‌تر شدن مفهوم «سرویس انتقال»، پنج سرویس پایه‌ای موجود در جدول ۲ را در نظر می‌گیریم.

***جدول ۲:* سرویس‌های پایه‌ای سرویس انتقال**

شماره	نام سرویس پایه	TPDU ارسالی	مفهوم
۱	LISTEN	-	بلوکه شده تا زمانی که یک پروسه اقدام به ارتباط نماید.
۲	CONNECT	CONNECTION REQ	تلاش فعالانه برای ایجاد ارتباط
۳	SEND	DATA	ارسال اطلاعات
۴	RECEIVE	-	بلوکه شده تا زمانی که DATA TPDU دریافت شود.
۵	DISCONNECT	DISCONNECT	طرف مربوطه، تمایل به رها کردن ارتباط دارد.

برای اینکه با کاربرد این سرویس‌ها آشنا شویم، یک اپلیکِیشِن (کاربرد) با یک سرور و چندین کلاینت راه دور را در نظر بگیرید. در ابتدا سرور، در حال اجرای سرویس LISTEN است تا زمانی که یک کلاینت، پیامی را صادر کند. کلاینت زمانیکه بخواهد با سرور صحبت کند، سرویس پایه CONNECT را اجرا می‌کند. موجودیتِ انتقال، این سرویس پایه را با بلوکه کردن تماس گیرنده و ارسال یک بسته به سرور انجام می‌دهد. پیام لایه انتقال با محصورسازی در payload این بسته برای موجودیت انتقالِ سرور ایجاد می‌شود.

واحد داده‌ای که از یک موجودیت انتقال به موجودیت انتقال دیگری انتقال می‌یابد، **TPDU**(**Transport Protocol Data Unit**) نامیده می‌شود. TPDUها در داخل بسته‌ها جای می‌گیرند. خود بسته‌ها نیز به نوبه خود در فریم جای می‌گیرند. لایه پیوند داده، سرآیند فریم را بررسی کرده و محتویات فریم را که به لایه‌های بالاتر خود مربوط است به آن‌ها ارسال می‌کند. لایه شبکه نیز کار مشابهی را انجام داده و بسته را به لایه انتقال واگذار می‌کند. شکل ۱ موقعیت TPDU را نشان می‌دهد.



***شکل ۱:* TPDU، بسته و فریم**

اجازه دهید به مثال کلاینت ـ سرور خودمان برگردیم. اعلام CONNECT توسط کلاینت، منجر به ارسال CONNECTION REQUEST TPDU به سرور می‌شود. زمانی که این پیام دریافت شود، موجودیت انتقال بررسی می‌کند که آیا سرور در حالت LISTEN بلوکه شده یا خیر. سپس آن سرور را از حالت بلوکه خارج کرده و CONNECTION ACCEPTED TPDU را به کلاینت بر می‌گرداند. زمانی که TPDU دریافت شود، کلاینت از حالت بلوکه خارج شده و ارتباط برقرار می‌شود. اکنون داده می‌تواند با استفاده از SEND و RECEIVE مبادله شود.

مثال ۳: در کدام یک از سرویس‌های پایه، TPDU ارسالی وجود ندارد؟

۱) LISTEN و CONNECT
۲) RECEIVE و DISCONNECT
۳) LISTEN و RECEIVE
۴) CONNECT و DISCONNECT

☑ **پاسخ:** گزینه «۳» با توجه به جدول ۲، در سرویس‌های پایه LISTEN و RECEIVE هیچ گونه TPDU ارسالی وجود ندارد.

نکته۲: دقت نمایید که حتی در ساده ترین شکلِ تبادل داده تک جهته، لایه شبکه پیچیده‌تر از لایه انتقال است.

هر بسته‌ی داده‌ای که ارسال می‌شود، تصدیق می‌شود. تصدیق‌ها در لایه انتقال، توسط موجودیت‌های انتقال با استفاده از پروتکل لایه شبکه مدیریت می‌شوند و توسط کاربرانِ انتقال، قابل مشاهده نیستند. به طور مشابه، موجودیت‌های انتقال نیز باید نگران تایمرها و ارسال‌های مجدد باشند. هیچ‌کدام از این موارد، توسط کاربران انتقال، قابل مشاهده نیست. از دید کاربر انتقال، ارتباطِ پیش رو، کاملاً قابل اطمینان است. میزبان‌های مبدأ و مقصد این‌گونه تصور می‌کنند که مابین آن‌ها ارتباط مستقیم و بدون واسطه‌ای وجود دارد. حتی در صورت بروز مشکل در لایه‌های پایینی، لایه‌های بالاتر ممکن است متوجه مشکل پیش‌آمده نشوند. ارسال هر بیت، معادل دریافت همان بیت است. این توانایی در پنهان نمودن پیچیدگی، دلیل لایه‌بندی پروتکل‌ها به‌عنوان ابزاری قدرتمند می‌باشد.

زمانی که دیگر نیازی به ارتباط نباشد، باید خط آزاد شود. قطع ارتباط، دو گونه مختلف دارد: نامتقارن و متقارن. در نوع **نامتقارن (asymmetric)** هر کاربرِ انتقال می‌تواند پیام DISCONNECT را صادر نماید که نتیجه آن، ارسال DISCONNECT TPDU به موجودیت انتقال راه دور است. به محض دریافت این پیام، ارتباط قطع می‌شود.

در گونه **متقارن (symmetric)**، هر طرف به طور مستقل از دیگری، برای پایان دادن به ارتباط باید آن را قطع کند. زمانیکه یک طرف DISCONNECT می‌کند، معنی‌اش آن است که داده‌ی دیگری برای ارسال ندارد اما همچنان به دریافت داده از طرف دیگر ادامه می‌دهد. در این مدل، ارتباط تنها زمانی قطع می‌شود که هر دو طرف، عمل DISCONNECT را انجام دهند. در ادامه همین فصل بیش‌تر در این رابطه صحبت خواهیم کرد.

حال اجازه دهید مرور مختصری نیز بر روی مجموعه سرویس‌های پایه دیگری داشته باشیم:

سوکِت‌های پایه، که گاهاً **توابع پایه** نیز نامیده می‌شوند، مجموعه سرویس‌های پایه دیگری هستند که در Berkeley UNIX و TCP استفاده می‌شوند. این سوکت‌ها در جدول ۳ گردآوری شده‌اند.

جدول ۳: سوکت‌های پایه برای TCP

سوکت پایه	مفهوم
SOCKET	ایجاد یک نقطه پایانی ارتباطی جدید(new communication end point)
BIND	الحاق یک آدرس محلی به پروسس در حال تشکیل
LISTEN	اعلام تمایل به دریافت اتصال؛ اعلام اندازه صف
ACCEPT	بلوکه کردن تماس گیرنده تا زمانی که تلاش برای ارتباط دریافت شود.
CONNECT	تلاش فعالانه برای ایجاد ارتباط
SEND	ارسال داده روی ارتباط
RECEIVE	دریافت داده روی ارتباط
CLOSE	آزاد کردن ارتباط

چهار تابع پایه که در جدول ۳ لیست شده‌اند، توابعی هستند که در طرف سرور اتصال‌گرا به ترتیب اجرا می‌شوند. تابع پایه Socket، یک نقطه پایانی ارتباطی برای فرایند مورد نظر تعیین می‌کند. علاوه بر این مشخص کردن مواردی همچون پروتکل ارتباط، اتصال‌گرا بودن یا بی اتصال بودن ارتباط، فرمت آدرس‌دهی، آماده‌سازی حافظه مورد نیاز و ... بر عهده این تابع است. وظیفه تابع Bind اختصاص شماره پورت به پروسس در حال شکل‌گیری است. با اختصاص این شماره پورت، پروسس طرف کلاینت می‌تواند با پروسس طرف سرور، ارتباط برقرار کند. تابع Listen منتظر دریافت درخواستی از طرف کلاینت باقی می‌ماند و این کار را با گوش کردن به لایه شبکه انجام می‌دهد. پس از اجرای این سه تابع، تابع Accept اجرا می‌شود.

نکته۳: ثبت شماره پورت در طرف کلاینت الزامی نیست چرا که سرور نیازی به دانستن آن ندارد.

مثال۴: تعیین آدرس پورت، وظیفه کدام تابع پایه است؟

۱) Socket ۲) Bind ۳) Listen ۴) Accept

☑ **پاسخ:** گزینه «۲» وظیفه تابع پایه‌ای Bind، اختصاص شماره پورت به پروسس در حال شکل‌گیری است.

تفاوت‌های لایه پیوند داده و لایه انتقال

تفاوت‌های مهمی مابین لایه پیوند داده و لایه انتقال وجود دارد:

۱ـ دو مسیریاب در لایه پیوند داده، مستقیماً از طریق کانال فیزیکی به هم وصل هستند. در حالی که به جای این کانال فیزیکی در لایه انتقال، کل زیرشبکه قرار می‌گیرد.

۲ـ تفاوت دیگر بین لایه پیوند داده و لایه انتقال، **امکان ذخیره سازی باری (potential existence of storage capacity)** در زیر شبکه لایه انتقال است. زمانی که مسیریاب فریمی را ارسال می‌کند، آن فریم ممکن است به مقصد برسد و یا گم شود اما نمی‌تواند جایی خود را پنهان کند و ناگهان در 30 ثانیه بعد سروٌکله‌اش پیدا شود! اگر زیر شبکه از **داده‌گرام** و مسیریابی مناسبی استفاده کند، این احتمال وجود دارد که بسته برای لحظاتی دخیره شده و سپس ارسال شود. البته قابلیت **ذخیره‌سازی** بسته‌ها صرف نظر از امتیازاتی که می‌تواند داشته باشد، گاهاً ممکن است فاجعه‌بار باشد. ضمن اینکه نیاز به پروتکل‌های خاصی برای این کار می‌باشد.

۳ـ بافرینگ و کنترل جریان در هر دو لایه لازم است. اما تعداد زیادی از اتصالات در لایه انتقال که آن هم به صورت پویا مدام در حال تغییر است، نیاز به رویکرد متفاوتی را نسبت به آنچه که در لایه پیوند داده داشت، طلب می‌کند.

مثال۵: در مورد تفاوت‌های لایه پیوند داده، لایه انتقال و لایه شبکه کدام گزینه صحیح نیست؟

۱) پیچیدگی لایه انتقال بیش‌تر از لایه شبکه است.

۲) امکان ذخیره‌سازی باری از تفاوت‌های لایه پیوند داده و لایه انتقال به شمار می‌رود.

۳) بافرینگ و کنترل جریان در هر دو لایه پیوند داده و انتقال لازم است اما با رویکردهایی متفاوت.

۴) هیچکدام

☑ **پاسخ:** گزینه «۱» حتی در ساده‌ترین شکل تبادل داده تک جهته، لایه شبکه پیچیده‌تر از لایه انتقال است. سایر گزینه‌ها، تفاوت‌ها را به درستی ذکر کرده‌اند.

آدرس‌دهی (Addressing)

زمانی که یک پردازشِ اپلیکیشن (کاربرد) می‌خواهد ارتباطی را با یک اپلیکیشن راه دور دیگر برقرار کند، باید مشخص شود که کدام آدرس انتقال می‌خواهد به کدام پردازش متصل شود. در اینترنت این نقاط انتهایی، زوج آدرس‌های IP و پورت‌های محلی می‌باشند. در شبکه‌های ATM، آن‌ها AAL-SAPS نامیده می‌شوند. ما از اصطلاح **TSAP (Transport Service Access Point)** استفاده می‌کنیم. نقاط انتهایی متشابه در لایه شبکه، **NSAP (Network Service Access Point)** نام دارند. آدرس‌های IP که در فصل قبل با آن‌ها آشنا شدیم، مثالی از NSAP ها هستند.

یک سناریوی ممکن برای ارتباط انتقال روی یک لایه شبکه اتصال‌گرا با توجه به شکل ۲، به قرار زیر است:

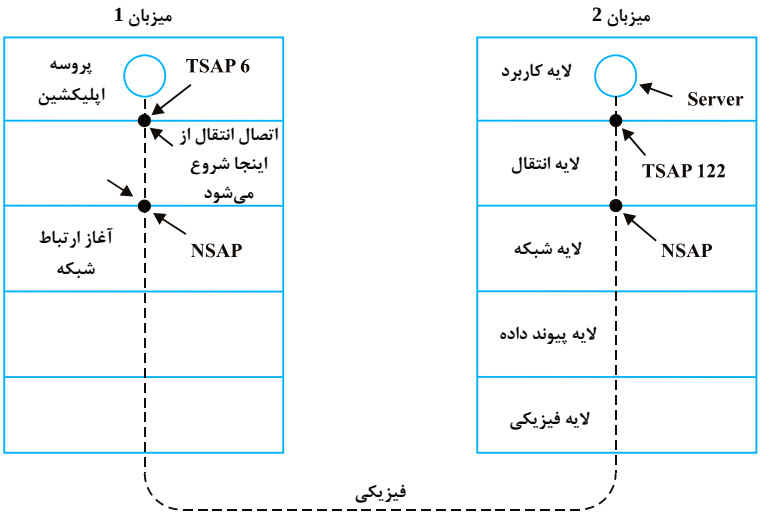
۱ـ پروسه‌ی سرور در میزبان شماره 2، با اتصال به TSAP 122، برای یک تماس دریافتی به انتظار می‌نشیند. چگونگی اتصال پروسه به TSAP، خارج از بحث مدل شبکه است و کاملاً وابسته به سیستم عامل می‌باشد. برای مثال تماسی مانند LISTEN، می‌تواند استفاده شود.

۲ـ یک پروسه اپلیکیشنِ خواهان در میزبان 1، درخواست CONNECT را با مشخص کردن TSAP 6 به‌عنوان مبدا و TSAP 122 به‌عنوان مقصد، صادر می‌کند.

۳ـ موجودیت انتقال در میزبان 1، آدرس شبکه‌ای را روی ماشین خود انتخاب کرده و اتصال شبکه‌ای را ایجاد می‌کند. با استفاده از این اتصال شبکه، موجودیت انتقال میزبان 1 می‌تواند با موجودیت انتقال 2 ارتباط برقرار کند.

۴ـ اولین چیزی که موجودیت انتقال میزبان 1 به نظیر خود در میزبان 2 می‌گوید، این است: «سلام! من می‌خواهم ارتباطی بین TSAP 6 خودم و TSAP 122 متعلق به تو ایجاد کنم؛ نظر تو چیست؟»

۵ـ پس از این، موجودیت انتقالِ میزبان 2 از سرور موجود در TSAP 122 جویا می‌شود که آیا مایل به پذیرش ارتباط جدیدی می‌باشد یا خیر. اگر موافقت لازم صورت گیرد، ارتباطِ انتقال ایجاد می‌شود.



شکل ۲: **TSAP، NSAP و ارتباط شبکه**

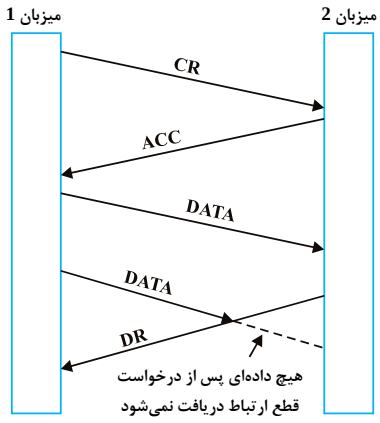
ایجاد یک ارتباط (Establishing a Connections)

ایجاد یک ارتباط به نظر ساده می‌رسد اما در عمل باید دانست که این کار چندان هم ساده نیست. در نگاه اول شاید این طور به نظر رسد که تنها کافی است موجودیت انتقال، یک CONNECTION REQUEST TPDU را به مقصد ارسال کند و منتظر پاسخ CONNECTION ACCEPTED بماند. مشکل زمانی رخ می‌دهد که در شبکه احتمال گم شدن، ذخیره شدن و تکراری شدن بسته‌ها (duplicate packets) وجود داشته باشد.

در بخش‌های بعدی (پروتکل TCP) بیشتر در خصوص ایجاد ارتباط صحبت خواهیم کرد.

آزادسازی یک ارتباط (Releasing a Connection)

آزادسازی ارتباط از ایجاد آن ساده‌تر است. با این حال حتی این کار هم پیچیده‌تر از آن چیزی است که به نظر می‌رسد. همانطور که پیش از این نیز اشاره شد، دو روش برای خاتمه یک ارتباط وجود دارد: آزادسازی غیرمتقارن (Asymmetric) و متقارن (Symmetric). یک مثال از **آزاد سازی غیرمتقارن**، تماس تلفنی است. زمانی که یکی از طرفین به تماس خاتمه می‌دهد، ارتباط قطع می‌شود. در **آزادسازی متقارن**، به هر ارتباط، مانند دو ارتباط تک جهته‌ی مجزا از هم نگاه می‌شود که برای قطع آن، باید هر دو طرف به طور مستقل اقدام به قطع ارتباط نمایند.



شکل ۳: **قطع ناگهانی ارتباط و از دست رفتن داده در آزادسازی غیرمتقارن**

نکته۴: از آنجا که قطع ارتباط غیرمتقارن به طور ناگهانی صورت می‌گیرد، می‌تواند منجر به از دست رفتن داده شود.

سناریویی را که در شکل ۳ نشان داده شده است، در نظر بگیرید. پس از برقراری ارتباط، میزبان 1، یک TPDU ارسال می‌کند که به طرز صحیح توسط میزبان 2 دریافت می‌شود. سپس میزبان 1، TPDU دیگری را ارسال می‌کند. متاسفانه میزبان 2، قبل از آنکه TPDU ارسال شده را دریافت کند، پیام DISCONNECT را صادر می‌کند. نتیجه این امر، قطع ارتباط و از دست رفتن داده خواهد بود.

واضح است که برای افزایش قابلیت اطمینان و جلوگیری از، از دست رفتن داده به پروتکل آزادسازی پیشرفته‌تری نیاز است. یک روش، استفاده از آزادسازی متقارن است که در آن هر طرف، مستقل از طرف دیگر، روند آزادسازی را انجام می‌دهد. در این حالت، میزبان حتی پس از ارسال DISCONNECT TPDU، می‌تواند به روند واگذاری داده ادامه دهد.

نکته۵: روش متقارن، زمانی می‌تواند کار خود را انجام دهد که هر پردازش، میزان داده مشخصی برای ارسال داشته و زمان ارسال نیز مشخص باشد.

مدرسان شریف

فصل هفتم

« لایه‌های بالاتر(نشست، ارائه و کاربرد)»

با توجه به مطالبی که در فصل‌های قبل و تا بدین جا مطالعه کردیم، در این فصل به مطالعه لایه‌های بالاتر خواهیم پرداخت. البته از فصل اول به خاطر دارید که طبق معماری TCP/IP تنها یک لایه باقی مانده است که آن هم لایه کاربرد می‌باشد. حتی در لایه کاربرد نیز برای انجام کاربردهای مختلف، نیاز به پشتیبانی از پروتکل‌های گوناگون وجود دارد. ما بحث خود را با امنیت آغاز می‌کنیم. همانطور که خواهیم دید تنها یک پروتکل برای امنیت پیشنهاد نشده است؛ بلکه تعداد زیادی از مفاهیم و پروتکل‌ها برای تضمین خصوصی‌سازی مورد نیاز خواهد شد. بحث دوم در رابطه با DNS است که وظیفه کنترل و مدیریت اسامی در اینترنت را بر عهده دارد. پس از آن نوبت به مفهوم مدیریت شبکه می‌رسد و سرانجام به بررسی برخی کاربردهای واقعی همچون ایمیل، WWW، HTTP و HTML خواهیم پرداخت.

تذکر: همانطور که در مقدمه کتاب نیز اشاره شد، از این فصل تا به حال آنچنان سوالی در آزمون ارشد طراحی نشده است.

امنیت شبکه

یکی از مهمترین مسائل مربوط به شبکه، امنیت آن است. امنیت شبکه، بحث بسیار گسترده‌ای است که هر چه از آن نوشته شود، هنوز حرف‌های ناگفته بسیاری باقی می‌ماند.

اغلبِ مشکلات امنیتی را افراد بدخواهی به وجود می‌آورند که قصد سوءاستفاده و یا آسیب رساندن به هدفی را دارند. برخی از رایج‌ترین این موارد، در جدول ۱ گردآوری شده است. با توجه به این جدول کاملاً مشاهده می‌شود که حفظ امنیت شبکه، شامل موارد گسترده‌ای می‌شود. بدیهی است که این جدول را به راحتی می‌توان گسترش داد.

***جدول ۱:* برخی از افراد مهاجم و انگیزه آن‌ها**

فرد	انگیزه
دانش آموز یا دانشجو	سرگرمی و سَرَک کشیدن به ایمیل افراد
هَکر	تست میزان امنیت؛ سرقت داده
تاجر	کشف استراتژی‌های بازاریابی رقیب
حسابدار	اختلاس مالی از شرکت
جاسوس	سرقت اطلاعات نظامی

مسائل و مشکلات پیرامون امنیت را می‌توان در 4 حوزه طبقه بندی کرد:

۱ـ **اختفا (Secrecy):** هدف، پنهان کردن و مخفی نمودن اطلاعات و دور از دست نگه داشتن آن‌ها در مقابل کاربران غیر مجاز است.

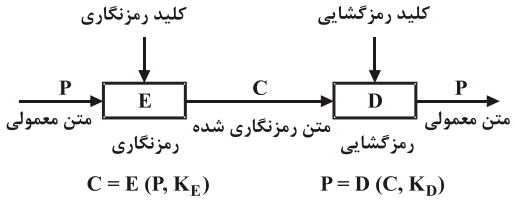
۲ـ **تصدیق (Authentication):** هدف از تصدیق، تعیین هویت فرد است؛ آن هم قبل از آنکه به واسطه ارتباطی که قرار است با آن شکل بگیرد، داده‌های مهم تحویل شوند.

۳ـ **کنترل صحت و جلوگیری از انکار (Nonrepudiation and Integrity Control):** جلوگیری از انکار در ارتباط با امضاها (signatures) است: از کجا می‌توان مطمئن بود که فرستنده واقعی داده، همان فرستنده‌ای است که ما فکر می‌کنیم؟ از کجا معلوم که مبداء داده، فرد سودجویی نباشد؟

۴ـ امنیت فیزیکی (Physical Security): مهم‌ترین و اساسی‌ترین کلیه سطوح امنیتی، امنیت فیزیکی می‌باشد که در حقیقت سنگ بنای امنیت را تشکیل می‌دهد. چراکه هدف از آن، امنیت‌سازی تکنولوژی مورد استفاده در تجهیزات می‌باشد تا بتوانند در مقابل سرقت یا از دست رفتن داده (مانند رفتن برق)، از خود مقاومت نشان دهند. مسئولیت امنیت فیزیکی بر عهده فاکتورهای بسیاری است. این سطح از امنیت، در حالی که اهمیت فوق‌العاده‌ای دارد، معمولاً دچار بی‌مهری قرار می‌گیرد.

رمزنگاری (Cryptography)

رمزنگاری تاریخچه جذاب و طولانی دارد. در طول تاریخ، طبقات مختلفی از افراد، عادت به رمزنگاری داشته‌اند: نظامی، دیپلمات، خاطره نویس و ... . شکل ۱ یک سیستم رمزنگاری را نشان داده است.



شکل ۱: یک سیستم رمزنگاری

پیام P، که پیام ساده و بدون رمز (plaintext) است با پارامتری شدن به وسیله یک کلید (K_E)، توسط یک تابع (E)، رمزنگاری می‌شود. نتیجه‌ی حاصل، یک پیام رمزنگاری شده است که Cryptogram یا Cipher text نامیده می‌شود. پیام رمزنگاری شده روی لینک ارتباطی، به طرف گیرنده ارسال می‌شود. گیرنده با استفاده از تابع (D) و کلیدی دیگر (K_D)، پیام را رمزگشایی می‌کند. اگر کلید رمزنگاری و رمزگشایی مشابه باشند، سیستم را **تک کلیده یا متقارن (Symmetric)** می‌گوییم یعنی: $K = K_E = K_D$. اما اگر این دو با هم متفاوت باشند، سیستم، **دو کلیده یا غیرمتقارن** (Asymmetric) خواهد بود یعنی: $K_E \# K_D$.

به عمل رمزنگاری Cryptography و به عمل رمزگشایی Cryptoanalyses گفته می‌شود. این دو با یکدیگر، بخشی از علم Cryptology را شکل می‌دهند.

جانشانی نشانه‌ها (Substitution Ciphers)

در روش جانشانی نشانه‌ها حرف یا گروهی از حروف، جانشین یک حرف یا گروهی از حروف دیگر می‌شود. به مثال زیر دقت کنید:

متن اصلی: a b c d e f g h I j k l m n o p q r s t u v w x y z

متن رمزنگاری شده: Q WE R T Y U I O P A S D F G H J K L Z X C V B N M

رمزنگاری قیصری (Caesar Cipher)

در این روش، هر حرف در متن با حرف دیگری که k حرف بعد از آن در ترتیب آلفا بت قرار دارد جایگزین می‌شود. نسخه اصلی رمزنگاری قیصری، از $K = 3$ استفاده می‌کند. بنابراین: $a \to d, b \to e, \ldots$. در این صورت اگر حروف a تا z را از 1 تا 26 شماره گذاری نماییم (تعداد حالات یا $N = 26$)، آنگاه تابع رمزنگاری با استفاده از کلید k برابر خواهد بود با: $E = (P + K) \bmod N$

جانشانی تک آلفا بتی (Mono Alphabetic Substitution)

در یک روش مرسوم‌تر، کلیه حروف با توجه به یک جدول تبدیل می‌شوند. در این حالت کلید آن چیزی است که توسط تبدیل کاراکتر(character map) نشان داده می‌شود. مثلاً طبق یک جدول مفروض، a تبدیل به t می‌شود. در این حالت برای به دست آوردن کلید، باید $26! = 4 \times 1026$ حالت مختلف را مورد بررسی قرار داد. حتی کامپیوتری که در هر میکرو ثانیه یک حالت را می‌تواند چک کند، برای بررسی کامل حالات، به 1013 سال نیاز خواهد داشت!!!

شکستن رمزنگاری تک آلفا بتی (Breaking Mono-Alphabetic Ciphers)

تکرار حروف، ترکیب دو حرف و یا ترکیب‌های سه‌تایی در انگلیسی و اکثر زبان‌های دنیا معمول است. با محاسبه تکرار کل حروف و ترکیبات در متن رمزنگاری شده، متخصص رمزنگاری می‌تواند متن اصلی را بدون زحمت زیاد، بازیابی نماید.

رمزنگاری به روش جابجایی (Transposition Ciphers)

مکان حروف در رمزنگاری به روش جابجایی، جا به جا شده و شیفت داده می‌شوند و به همین دلیل، ترتیب آن‌ها به هم می‌خورد. از دید ریاضیات، برای رمزنگاری محل و موقعیت کاراکترها، از یک تابع دوسویه(Bijective Function) استفاده می‌شود. از تابع معکوس نیز برای رمزگشایی استفاده می‌شود. در اینجا اطلاعات تکراری کمک چندانی برای کشف رمز نخواهند کرد. به مثال زیر دقت کنید:

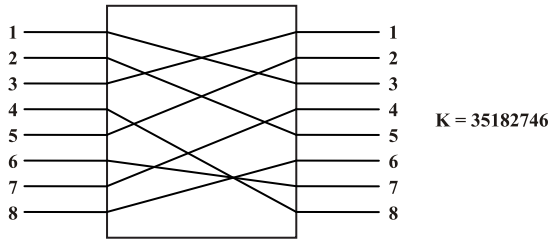
متن اصلی:Communication .is. easy

متن رمزنگاری شده: Cuan, yont.emiiiamcoss

لازم به ذکر است که پیاده‌سازی‌های مختلفی تا به حال برای رمزنگاری به روش جابجایی پیشنهاد شده است.

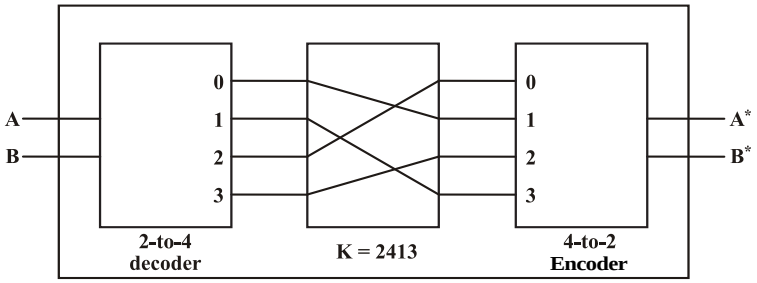
تولید رمزها (Product Ciphers)

برای تعویض حروف از جعبه P (P-Box) استفاده می‌شود (p اول permutation به معنای جایگشت است). یک جعبه P در شکل ۲ نشان داده شده است. این شکل، n ورودی و n خروجی دارد. متون کاراکتری معمولاً توسط کدهای 8 بیتی (ASCII) نشان داده می‌شوند. کلید K، موقعیت جدید را برای هر بیت ورودی تعیین می‌کند.



شکل ۲: P -Box

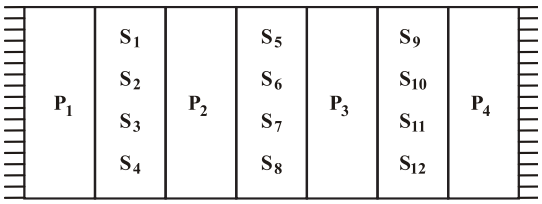
اگر یک رمزنگار بخواهد از هر جانشانی برای هر کاراکتر 8 بیتی به کاراکتر 8 بیتی دیگری پشتیبانی کند، نیاز به جدولی با 256 مدخل کاراکتری خواهد داشت. طول کل کلید برای توصیف جدول، به $256*8=2048$ می‌رسد. برای کاهش این حجم، همان‌طور که شکل ۳ نشان داده است، یک P-Box مابین یک رمزگشا (decoder) و رمزنگار (encoder)، محصور (encapsulated) می‌شود (جعبه S).



شکل ۳: جعبه‌های S

از واحدهای پشت سر هم جعبه‌های Product Ciphers P و Product Ciphers S ، برای افزایش قدرت الگوهای رمزنگاری استفاده می‌شود. مثالی از یک Product Ciphers، DES (Data Encryption Standard) است که توسط موسسه ملی علم و فناوری National Institute of Science and Technology (NIST) در سال 1977 ایجاد شد.

اصل رمزنگاری به‌صورت زیر است: کلیه پیام‌ها باید شامل افزونگی (redundancy) باشند تا از فریب گیرنده‌ها توسط نفوذگرها برای عمل بر روی پیام‌های اشتباه جلوگیری به عمل آید. شکل ۴ یک Product Ciphers را نمایش می‌دهد.



شکل ۴: یک Product Ciphers

الگوریتم‌های کلید امنیت (Secret Key Algorithms)

رمزنگاری‌های جدید از اصول مشابهی که در روش‌های قدیمی استفاده می‌شد، مانند جابجایی و جانشانی بهره می‌برند اما با این حال تفاوت‌هایی نیز با نیاکان خود دارند. در گذشته، رمزنگارها برای امنیت خود باید از الگوریتم‌های ساده‌ای که بر مبنای کلیدهای بسیار طولانی قرار داشت، استفاده می‌کردند. اما امروزه قضیه برعکس شده است به گونه‌ای که الگوریتم رمزنگاری باید به گونه‌ای پیچیده باشد که حتی خبره‌ترین افراد هم قادر به رمزگشایی آن نباشند. جابجایی و جانشانی می‌توانند توسط مدار ساده‌ای پیاده‌سازی شوند. شکل ۲ وسیله‌ای را که P-box نام دارد، نشان می‌دهد که برای جابجایی 8 بیت ورودی مورد استفاده قرار می‌گیرد. اگر این هشت بیت ورودی از بالا به پایین 01234567 در نظر گرفته شوند آنگاه ۸ بیت خروجی این P-box برابر می‌شود با 36071245. با سیم‌بندی مناسب داخلی، یک P-box می‌تواند برای هر نوع جابجایی مورد استفاده قرار گیرد و آن را با سرعت بالایی انجام دهد.

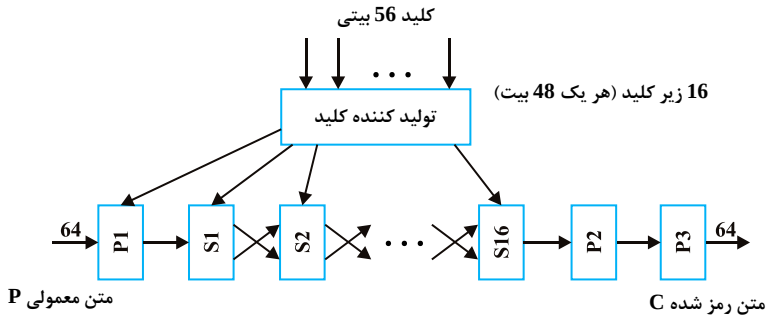
جانشانی می‌تواند توسط جعبه‌های S (S-boxes) که در شکل ۳ نشان داده شده است، انجام شوند. در این مثال، ورودی، یک متن ساده 2 بیتی است و متن رمزنگاری شده دو بیتی دیگر، خروجی را تشکیل می‌دهد. دو بیت ورودی، یکی از 4 خطوط موجود را از اولین مرحله انتخاب کرده و آن را به مقدار 1 تنظیم (set) می‌کنند. کلیه خطوط دیگر برابر 0 می‌شود. دومین مرحله یک P-box است. در سومین مرحله ورودی انتخاب شده، مجدداً به شکل دودویی رمزنگاری می‌شود. مجدداً با سیم‌بندی مناسب P-box داخل S-box، هر نوع جانشانی قابل اجرا خواهد بود.

توان واقعی این اجرا تنها زمانی آشکار می‌شود که تعدادی جعبه را به شکل 4 به‌صورت سری به یکدیگر متصل کنیم. در این مثال، 12 خط ورودی توسط مرحله اول، جابه جا شده‌اند. از نظر تئوری، این امکان وجود دارد که مرحله دومی را داشت که یک S-box باشد که عدد 12 بیتی را به عدد دیگر 12 بیتی نگاشت کند. اما چنین تجهیزاتی نیاز به $2^{12} = 4096$ سیم متقاطع در مرحله میانی خود خواهد داشت. به جای این، ورودی به 4 گروه 3 بیتی تقسیم می‌شود که هر یک مستقل از دیگری جانشانی می‌شود. هر چند کاربرد این روش گسترده نیست اما روش قدرتمندی به شمار می‌رود.

استاندارد رمزنگاری داده یا DES(Data Encryption Standard)

الگوریتم DES در اوایل دهه هفتاد توسط IBM توسعه یافت. DES یک مثال از Product Ciphers است که عمل رمزنگاری را به‌صورت بلوک‌گرا (block-oriented) انجام داده و بلوک‌های 64 بیتی را رمزنگاری می‌نماید. یک کلید 56 بیتی، رمزنگاری را کنترل می‌کند. کلید 56 بیتی، به 16 زیر کلید 48 بیتی برای کنترل 16 جانشانی در یک تراشه DES تبدیل می‌شود (شکل ۵). پروسه رمزنگاری، شامل 19 مرحله در تراشه DES است. اولین مرحله، جابجایی با استفاده از قانون جابجایی ثابتی است که با 16 جایگزینی و در نهایت 2 جابجایی نهایی دنبال می‌شود. در هر مرحله جانشانی، پرارزش‌ترین و کم‌ارزش‌ترین بیت‌های بلوک‌های 32 بیتی با هم تعویض می‌شوند. 32 بیت پرارزش قبلی تحت کنترل زیر کلید (subkey)، جانشانی و جابجا می‌شوند و نتیجه، به مرحله بعد ارسال می‌شود. اشکال این روش این است که کلید رمزنگاری و رمزگشایی مشترک است.

لازم به ذکر است که طول کلید اولیه پیشنهاد شده توسط IBM ، 128 بیت بوده است. با این حال آژانس امنیت ملی ایالات متحده، طول 56 بیتی را پیشنهاد داد.



شکل ۵: تولید متن رمزنگاری شده DES

حالات کاری DES

حالات کاری DES عبارتند از:

- **Electronic Code Book (ECB)** : هر بلوک از متن رمزنگاری شده، به طور مستقل از سایر بلوک‌ها رمزنگاری می‌شود. به همین خاطر، هر بلوک متن رمز شده با یک بلوک متن ساده مطابقت دارد؛ دقیقاً مانند یک کتاب رمزی (codebook).
- **Chain Block Cipher (CBC)** : ECB از درج بلوک‌های تکراری جلوگیری نمی‌کند چراکه نسبت به هر بلوک به طور مستقل رفتار می‌کند. ضعف دیگر آن این است که الگوهای بلوک‌های متنی مشابه، بلوک‌های متنی رمز شده‌ی مشابهی را تولید می‌کنند.

دقت کنید که رشته 32 بیتی، ابتدا باید به داده 48 بیتی تبدیل شود. سپس عمل XOR با کلید 48 بیتی انجام می‌شود و نتیجه باید به 32 بیت تبدیل شود. در تمام مراحل، 16 کلید 48 بیتی از روی کلید 56 بیتی ساخته می‌شوند.

در جهت بهبود DES برای جریان‌های ارتباطی، هر بلوک 64 بیتی با متن رمز شده 64 بیتی قبلی، XOR شده و وارد تراشه DES می‌شود. علاوه بر یک کلید امنیت مشترک، فرستنده و گیرنده باید در مورد بردار اولیه (initial vector) که باید با اولین بلوک جریان پیام XOR شود، با هم به توافق برسند.

- **Cipher Feedback Mode (CFM)** : CFM حالت جایگزین DES، برای کاراکترهای 8 بیتی محسوب می‌شود. کاراکتر ورودی با کم ارزش‌ترین بایت خروجی DES، XOR شده و سپس روی لینک ارتباطی ارسال می‌شود.

برای جمع آوری بیت‌های لازم برای بلوک رمزنگاری 64 بیتی، کاراکترهای خروجی توسط شیفت رجیستر گردآوری می‌شوند. هر کاراکترِ ورودی در شیفت رجیستر پیش رفته و یک رمزنگاری DES جدید را تحریک (trigger) می‌کند. به همین دلیل کاراکتر ورودی بعدی با خروجی جدید DES، XOR می‌شود. روش CFM برای استفاده در خطوط سریال مناسب است.

رمزنگاری با کلیدهای عمومی و خصوصی

همانطور که اشاره شد، اشکال DES این است که فرستنده و گیرنده از کلید مشترکی استفاده می‌نمایند. سوالی که پیش می‌آید، چگونگی توزیع کلیدها مابین زوج‌های ارتباطاتی است.

در رمزنگاری و به شکل کلی آن، هر کاربر باید دارای دو کلید باشد:

۱ـ کلید عمومی: از کلید عمومی برای رمزنگاری پیامی که قرار است به کاربر ارسال شود، استفاده می‌شود.

۲ـ کلید خصوصی: از این کلید، برای رمزگشایی پیام استفاده می‌شود.

سیستم‌های کلید خصوصی

در سال 1976، Diffie و Hellman پیشنهاد استفاده از الگوریتم‌های رمزنگاری E و رمزگشایی D را دادند، به طوری که:

۱ـ $D(E(P)) = P$

۲ـ استخراج D از E بسیار سخت است.

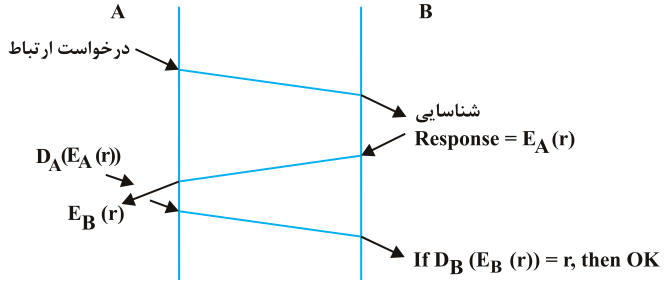
۳ـ E نمی‌تواند توسط حمله افراد نخبه شکسته شود. تحت این شرایط، E می‌تواند عمومی باشد در حالی که D به طور محرمانه نگهداری می‌شود.

فرستنده A را در نظر بگیرید که می‌تواند با استفاده از رمزنگاری کلید عمومی، یک کلید محرمانه را برای گیرنده B ارسال کند. ابتدا A ، کلید عمومی B (E_B) را از یک بانک اطلاعاتی عمومی بازیابی می‌کند. با داشتن E_B ، اکنون A می‌تواند پیامی که شامل کلید K برای B است را رمزنگاری کند. تنها ایستگاه B کلید رمزگشایی محرمانه (D_B) خود را در اختیار دارد که توسط آن می‌تواند متن اصلی و بوسیله آن، K را بازیابی کند.

از آنجا که سیستم‌های رمزنگاری متقارن (symmetric) با کلید مشترک K، سریعتر از الگوهای کلید عمومی نامتقارن (asymmetric) اجرا می‌شوند، A و B تصمیم می‌گیرند که به جای تکنیک کلید عمومی، از یک الگوریتم کلید محرمانه مشترک برای باقیمانده ارتباط خود استفاده نمایند.

تصدیق هویت (Authentication)

منظور از تصدیق هویت، شناسایی یا تعیین هویت(identification) و تصدیق (verification) است. شناسایی یا تعیین هویت، پروسه‌ای است که توسط آن هر فرد، مشخصه‌ی به خصوصی را برای خود مدعی می‌شود. در حالی که تصدیق، پروسه‌ای است که توسط آن صحت و سقم این ادعا مورد بررسی قرار می‌گیرد.



شکل ۶: تکنیک‌های تصدیق هویت

پروسه تصدیق هویت با توجه به شکل ۶ و با استفاده از کلید عمومی به شکل زیر انجام می‌شود. ایستگاه A یک درخواست ارتباط (connection request) را به B ارسال می‌کند. B، نتیجه بررسی صلاحیت (challenge) A را با رمزنگاری یک عدد تصادفی r با کلید عمومی E_AA به A برمی‌گرداند. فقط A قادر است تا پیام بررسی صلاحیت را با کلید خصوصی خودش(D_A)، رمزگشایی نماید. A نتیجه را یا به‌صورت باز یا به صورت رمزنگاری شده با کلید عمومی B، ارسال می‌کند. اکنون B می‌تواند بررسی کند که آیا عدد تصادفی به طرز صحیحی رمزگشایی شده است یا خیر.

الگوریتم RSA

بر پایه ایده Diffie و Hellman یک الگوی رمزنگاری عمومی توسط Rivest، Shamir و Adleman در سال 1978 ابداع شد که RSA نام گرفت. در این الگو کلیدهای متفاوتی که از یکدیگر قابل اشتقاق نیستند، الگوی رمزنگاری E و رمزگشایی D را انجام می‌دهند. RSA یکی از انواع الگوریتم‌های نامتقارن است. در الگوریتم نامتقارن (بر خلاف متقارن)، از کلیدهای متفاوتی برای رمزنگاری و رمزگشایی استفاده می‌شود. اشاره داشتیم که کلید رمزنگاری را کلید عمومی و کلید رمزگشایی را کلید خصوصی می‌نامند.

در الگوریتم RSA ابتدا داده‌ها را به قسمت‌های دو کاراکتری تقسیم می‌کنیم. هر کاراکتر را نیز به عدد تبدیل می‌کنیم. به‌عنوان مثال A به 01، B به 02، C به 03 و... تبدیل می‌شود. در این روش انتخاب کلید عمومی و خصوصی به‌صورت زیر است :

۱ـ دو عدد اول p و q انتخاب می‌شوند (تا جایی که می‌توانند باید بزرگ باشند(دویست رقمی))

۲ـ اعداد n و z به‌صورت زیر محاسبه می‌شوند:

$$n = p \times q$$

$$z = (p-1) \times (q-1)$$

۳ـ عدد d را به گونه‌ای انتخاب می‌کنیم که نسبت به z اول باشد.

۲ـ بر اساس d، عدد e به گونه‌ای انتخاب می‌شود که رابطه روبه‌رو برقرار باشد:

$$(e \times d) \bmod (z) = 1$$