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 پرسنل 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 (ایمیل)، چت، 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.

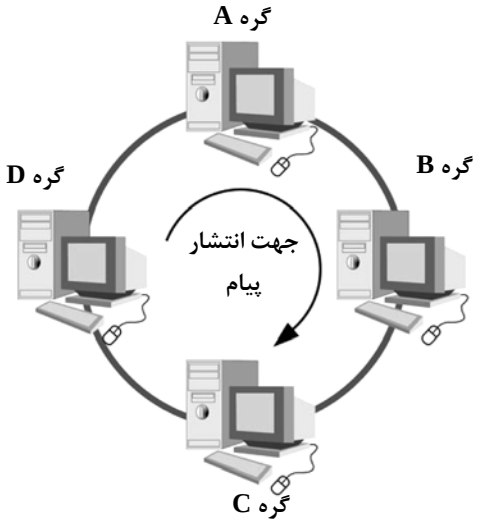
برای غلبه بر مشکلات فوق، معمولاً در توپولوژی حلقه، از دو حلقه در دو جهت متفاوت استفاده می‌شود تا اگر برای یکی از حلقه‌ها مشکلی بروز کرد، بتوان از حلقه جایگزین بهره گرفت.

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.

ویژگی‌های این توپولوژی عبارتند از:

۱ـ هر گره برای اتصال به شبکه، تنها نیاز به یک پورت دارد (البته به غیر از گره مرکزی).

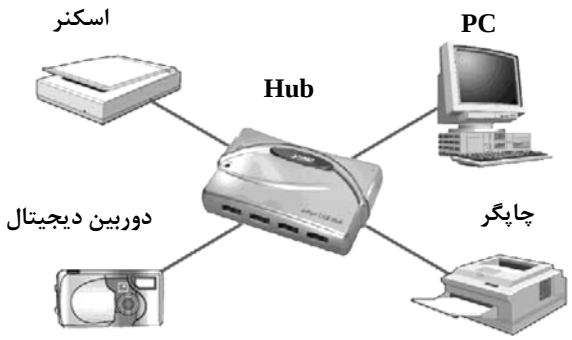
۲ـ عملکرد شبکه به شدت وابسته به گره مرکزی است.

۳ـ اگر گره مرکزی خراب شود، کارکرد کل شبکه مختل خواهد شد. اما اگر یک گره معمولی خراب شود تنها همان گره از شبکه خارج خواهد شد.

۴ـ چناچه نفوذگر موفق شود به گره مرکزی نفوذ کند، خطر بزرگی شبکه را تهدید خواهد کرد.

۵ـ عیب‌یابی در این توپولوژی چندان ساده نیست.

نکته۴: تعداد کابل‌های مورد نیاز در توپولوژی ستاره با n گره (بدون احتساب گره مرکزی)، برابر n است.

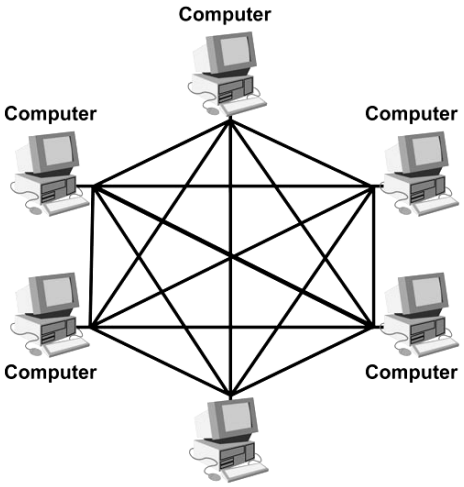


شکل ۳: توپولوژی ستاره

توپولوژی Mesh (مش)

در این توپولوژی که در شکل ۴ نمونه‌ای از آن نشان داده شده است، هر گره به طور مستقیم و بدون هیچ گونه واسطه‌ای، با کلیه گره‌های دیگر در ارتباط است. بنابراین با فرض n گره در توپولوژی، هر گره باید دارای $n-1$ پورت باشد.

نکته۵: گاهی اوقات به حالتی که هر گره به کلیه گره‌ها متصل باشد، full mesh گفته می‌شود.



شکل ۴: توپولوژی مش

ویژگی‌های این توپولوژی عبارتند از:

۱ـ سرعت ارتباط بسیار بالا.

۲ـ اگر مشکلی برای یک لینک اتفاق بیفتد، تنها ارتباط بین دو گره متناظر مختل خواهد شد و تاثیری روی کلیت عملکرد شبکه نخواهد داشت.

۳ـ امنیت بالا.

۴ـ سادگی در عیب‌یابی.

۵ـ مشکل بودن بسط و گسترش شبکه.

۶ـ نیاز به تعداد زیادی کابل و در نتیجه افزایش هزینه.

۷ـ هر گره برای اتصال به شبکه نیاز به پورت‌های زیادی دارد.

کاربرد توپولوژی مش به خاطر ویژگی‌های که دارد معمولاً کاربردهای خاص (مانند نظامی) می‌باشد.

مثال۷: در رابطه با توپولوژی مش کدام گزینه صحیح نیست؟

۱) عیب‌یابی در آن به نسبت به سادگی صورت می‌گیرد.

۲) امنیت در آن فدای سرعت پایین شده است.

۳) برای اتصال به شبکه نیاز به پورت‌های زیادی وجود دارد.

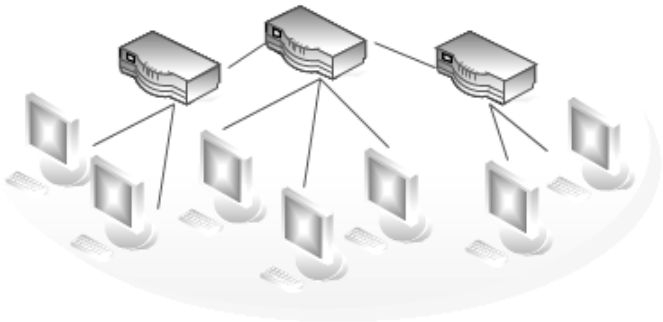
۴) تعداد کابل مورد نیاز زیاد است.

☑ **پاسخ:** گزینه «۲» عیب‌یابی در توپولوژی مش نسبتاً ساده است (گزینه ۱). هر گره نیز برای اتصال مستقیم به بقیه گره‌ها نیاز به n-1 پورت دارد که تعداد زیادی است (گزینه ۳). به همین خاطر هم از تعداد کابل زیادی استفاده می‌کند (گزینه ۴). توپولوژی مش هم امنیت بالایی دارد و هم سرعت زیادی بنابراین گزینه ۲ صحیح است.

نکته۶: تعداد کابل‌های مورد نیاز در توپولوژی مش با n گره، برابر $\frac{n(n-1)}{2}$ است.

توپولوژی Tree (درختی)

کاربرد اصلی این توپولوژی زمانی است که بخواهیم برای گسترش شبکه، چندین هاب را به یکدیگر متصل کنیم. اگر مبحث درخت‌ها از درس ساختمان داده‌ها را به خاطر داشته باشید، تصور شکل این توپولوژی کار چندان مشکلی نخواهد بود. یک نمای فرضی از این توپولوژی مطابق شکل ۵ است. در رابطه با هاب به طور مفصل در فصل چهار بحث خواهیم کرد. به طور خلاصه وظیفه هاب، دریافت، تقویت و ارسال داده‌ها است.



شکل ۵: توپولوژی درخت

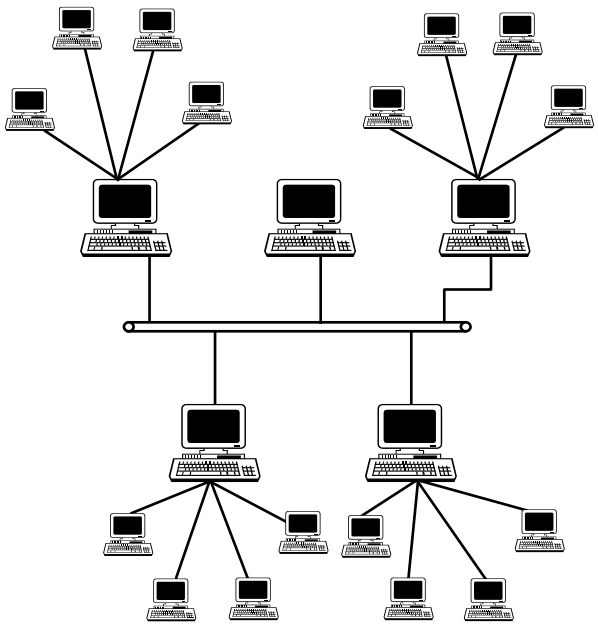
مثال ۸: به منظور گسترش شبکه و اتصال چندین هاب به یکدیگر معمولاً از کدام توپولوژی استفاده می‌شود؟

۱) Ring ۲) Bus ۳) Tree ۴) Mesh

☑ **پاسخ:** گزینه «۳» همان‌طور که اشاره شد کاربرد اصلی توپولوژی Tree زمانی است که بخواهیم برای گسترش شبکه، چندین هاب را به یکدیگر متصل کنیم.

توپولوژی Hybrid (ترکیبی)

در اغلب اوقات و در عمل، از ترکیبی از توپولوژی‌های بحث شده برای ایجاد شبکه استفاده می‌شود. مثالی از این توپولوژی در شکل ۶ قابل مشاهده است.



شکل ۶: توپولوژی ترکیبی

لایه‌بندی و معماری شبکه

اصولاً هدف از **لایه‌بندی شبکه (Network Layering)**، کاهش پیچیدگی‌های طراحی و تفکیک وظایف است. به طوری که با افزایش تعداد لایه‌ها علاوه بر کاهش پیچیدگی طراحی، اِعمال تغییرات، پیاده‌سازی و مطالعه شبکه ساده‌تر صورت می‌گیرد؛ هر چند **سربار (overload)** سیستم افزایش می‌یابد. منظور از سربار، اطلاعاتی است که علی‌رغم آنکه جزو داده اصلی قلمداد نمی‌شوند به دلایل مختلفی (مانند کنترل خطا)، ارسال آن‌ها الزامی است. بدیهی است از یک نظر، هر چه سربار سیستم کم‌تر باشد، از ظرفیت لینک‌های ارتباطی بهره‌برداری مناسب‌تری می‌شود. شایان ذکر است که هر لایه سعی می‌کند امور مربوط به لایه‌های پایین‌تر را از دید لایه‌های بالاتر خود مخفی نگه دارد.

معماری شبکه (Network Architecture)، اصطلاحی است که به مجموعه لایه‌ها و پروتکل‌های موجود در هر لایه اطلاق می‌شود. برای تشریح معماری شبکه‌های کامپیوتری از نظر تئوری، دو مدل مرجع وجود دارد: مدل OSI (Open System Interconnection) و مدل TCP/IP که هر یک از آن‌ها لایه‌بندی متفاوتی را پیشنهاد می‌دهند. وظیفه هر لایه، ارائه سرویس به لایه‌های بالاتر از آن است. بنابراین در اصطلاح به وظیفه هر لایه نسبت به لایه بالایی خود، **سرویس** گفته می‌شود. انجام این وظایف که سرویس نامیده می‌شوند به عهده پروتکل‌هایی است که برای هر لایه وجود دارد. در هر تبادل داده، لایه i ـ ام طرف فرستنده با لایه i ـ ام گیرنده در ارتباط است.

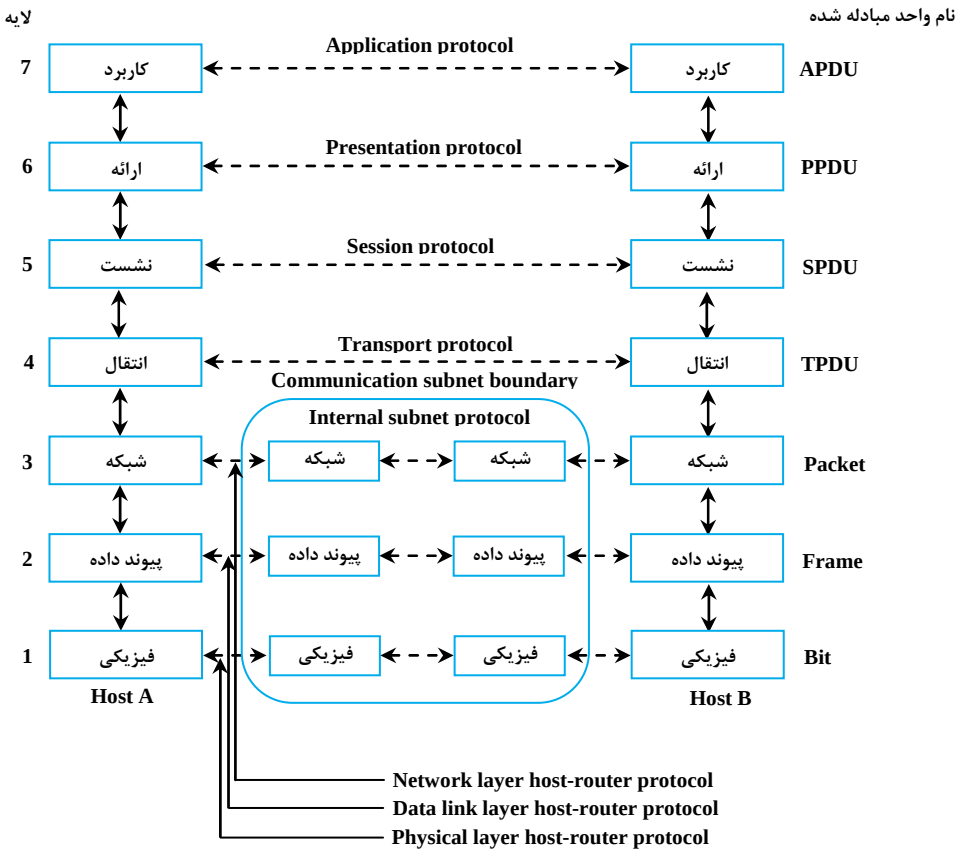
مدل مرجع OSI

به منظور ایجاد سازگاری جهانی بین شبکه‌ها و تجهیزات مربوط به آن‌ها، مدل OSI توسط سازمان استانداردهای بین‌المللی (ISO) در اواسط دهه 1980 معرفی شد. تعداد لایه‌های تعریف شده در این مدل هفت عدد است که در شکل ۷ نشان داده شده است. دلایل مختلفی برای انتخاب 7 لایه ارائه شده است. به‌عنوان مثال مرزبندی بین لایه‌ها باید به گونه‌ای صورت بگیرد که سعی شود کم‌ترین میزان اطلاعات مابین لایه‌ها منتقل شود. علاوه بر این نقش و عملکرد هر لایه باید با توجه به پروتکل‌های موجود تعریف شده و کاملاً مشخص باشد. ضمناً نباید در تنظیم تعداد لایه‌ها مرتکب افراط و تفریط شد!

لازم به ذکر است که امروزه ارزش مدل OSI تنها از نظر تئوری است و در عمل به خاطر مشکلاتی که (بخصوص در مقابل مدل دیگر) دارد از آن استفاده چندانی نمی‌شود. در حقیقت مدل OSI را به طور کلی نباید مدلی برای معماری شبکه در نظر گرفت چراکه تعدادی از پروتکل‌های مربوط به آن، ساخته نشدند. کارشناسان دلایل شکست مدل OSI را به مواردی همچون لایه‌بندی بیش از اندازه، سیاست و زمان‌بندی نادرست نسبت می‌دهند. ازدیاد لایه‌بندی نیز در لایه‌های بالاتر مشهود است. از آنجا که قبل از OSI، مدل TCP/IP (که در ادامه بررسی می‌شود) وجود داشت، به دلایل مختلف از جمله وحشت از سلطه جهانی شرکت IBM (که حامی مدل OSI بود)، اغلب شرکت‌ها تمایل به استفاده از TCP/IP پیدا کردند.

به هر حال همچنان مدل OSI، ارزش تئوری خود را به خصوص در زمینه آموزشی، حفظ کرده است.

نکته ۷: آخرین سرآیند اضافه شده به داده در فرستنده، اولین سرآیندی است که در طرف گیرنده برداشته می‌شود. به همین دلیل معمولاً از اصطلاح پشته پروتکل (stack protocol) استفاده می‌شود.



شکل ۷: هفت لایه مدل OSI

در ادامه، هر لایه مدل OSI را توضیح می‌دهیم:

۱ـ **لایه فیزیکی (Physical Layer)**: انتقال داده‌ها در قالب واحد داده (بیت) و به شکل سیگنال الکتریکی یا پالس نوری، توسط این لایه صورت می‌گیرد. این لایه بر خلاف لایه‌های دیگر مستقیماً با سخت افزار در ارتباط است.

۲ـ **لایه پیوند داده (Data Link Layer)**: این لایه وظایف مهمی را بر عهده دارد که از جمله آن‌ها می‌توان به کنترل خطا، کنترل جریان، کنترل ازدحام، کنترل دسترسی به رسانه مشترک و ... اشاره کرد. لایه پیوند داده پس از دریافت اطلاعات از لایه بالاتر از خود، آن را آماده تحویل به لایه فیزیکی می‌کند.

۳ـ **لایه شبکه (Network Layer)**: حیاتی‌ترین نقش این لایه، مسیریابی بسته‌ها و تحویل نامطمئن آن‌ها در شبکه است. از دیگر وظایف این لایه، شکستن داده به تعدادی بسته کوچکتر (و بالعکس) و شماره‌گذاری بسته‌ها می‌باشد.

۴ـ **لایه انتقال (Transport Layer)**: مسئولیت تضمین تحویل بسته‌ها به گیرنده (ارسال قابل اطمینان)، مهمترین وظیفه این لایه است.

۵ـ **لایه نشست یا جلسه (Session Layer)**: از 22 سرویسی که این لایه ارائه می‌دهد، می‌توان به مواردی همچون کنترل دیالوگ (dialog control)، همگام‌سازی (Synchronization)، مدیریت نشانه (Token Management)، تفکیک دیالوگ،گزارش خطا (exception reporting) و ... اشاره کرد.

۶ـ **لایه ارائه (Presentation Layer)**: وظیفه این لایه ایجاد امکان ارتباطِ با مفهوم، بین گره‌ها است (فشرده‌سازی و غیر فشرده‌سازی، رمزنگاری و رمزگشایی و ...).

۷ـ **لایه کاربرد (Application Layer)**: بالاترین لایه در مدل OSI است که با کاربر مستقیماً در ارتباط است. به همین خاطر پروتکل‌های این لایه برای کاربران معمولی، شناخته شده‌تر هستند مانند: HTTP، FTP، SMTP و ...

مثال۹: کنترل خطا جزو وظایف کدام لایه در مدل OSI است؟

۱) پیوند داده ۲) کاربرد ۳) فیزیکی ۴) ارائه

☑ **پاسخ:** گزینه «۱» لایه پیوند داده وظایف مهمی را بر عهده دارد که از جمله آن‌ها می‌توان به کنترل خطا و کنترل جریان اشاره کرد.

مدل مرجع TCP/IP

همان‌طور که قبلاً هم اشاره کردیم، مدلی که در عمل به عنوان استاندارد اینترنت مورد استفاده قرار می‌گیرد، مدلTCP/IP است که تاریخچه شکل‌گیری آن توسط وزارت دفاع ایالات متحده، حتی به قبل از مدل OSI می‌رسد. در این مدل، سه لایه بالایی مدل OSI با هم ترکیب شده و تشکیل لایه کاربرد را داده (Application) و دو لایه پایینی (پیوند داده و فیزیکی) نیز پس از ادغام، تشکیل یک لایه را می‌دهند. بنابراین این مدل دارای چهار لایه خواهد شد:

۱ـ لایه دسترسی به شبکه ۲ـ لایه شبکه ۳ـ لایه انتقال ۴ـ لایه کاربرد.

البته برخی منابع، از ادغام دو لایه پایینی اجتناب کرده و به این ترتیب مدل TCP/IP را پنج لایه در نظر می‌گیرند:

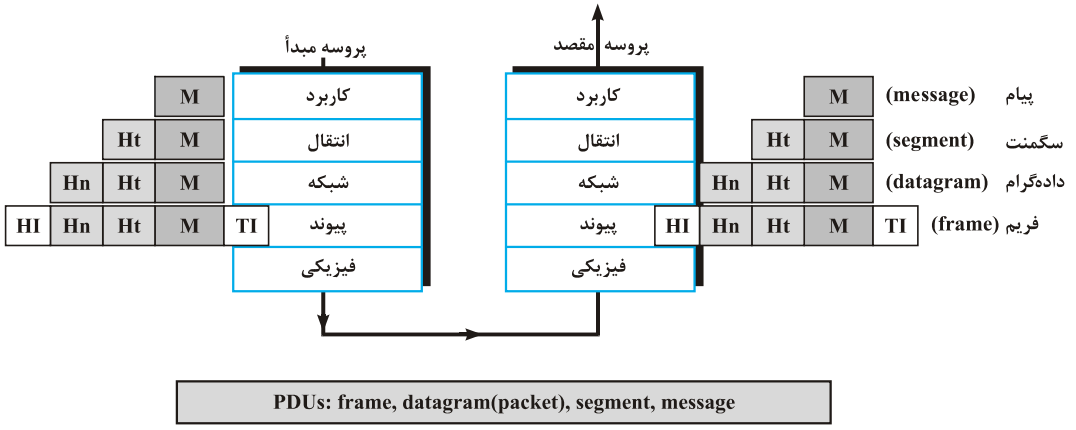
۱ـ لایه فیزیکی ۲ـ لایه پیوند داده ۳ـ لایه شبکه ۴ـ لایه انتقال ۵ـ لایه کاربرد. شکل ۸ مدل TCP/IP را در کنار مدل OSI نشان داده است. همان‌طور که گفته شد برای هر لایه در معماری شبکه، پروتکل‌هایی مشخص شده است؛ به عنوان مثال: اِترنِت برای لایه‌های یک و دو، IP برای لایه 3، TCP و UDP برای لایه 4 و HTTP، FTP، SMTP برای لایه 5.

تذکر۷: ما در فصول آتی به طور مفصل لایه‌های ذکر شده را همراه با پروتکل‌های آن‌ها بررسی خواهیم نمود. برای اثبات این ادعا بد نیست نگاهی به فهرست کتاب بیندازید!

مدل TCP/IP مثالی از **استانداردهای defacto** می‌باشد. استانداردهای defacto استانداردهایی هستند که به شکل غیر رسمی مورد مقبولیت گسترده قرار گرفته‌اند. در مقابل این، **استاندارد dejour** قرار دارد که به شکل رسمی معرفی می‌شود. مدل OSI مثالی از استانداردهایdejour است.

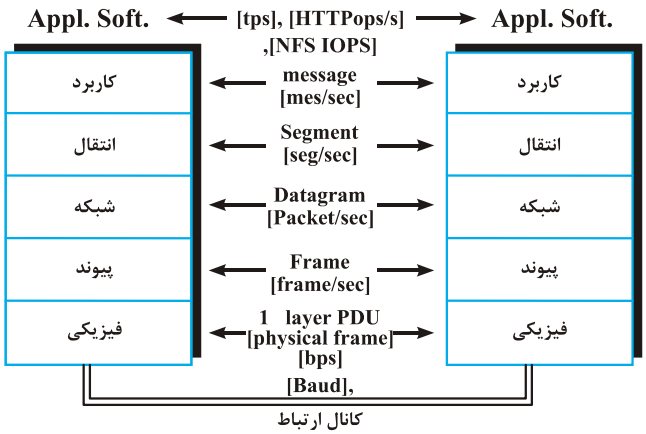
شکل ۸: **مدل OSI در مقابل TCP/IP**

در فرستنده، داده‌ها از لایه‌های بالایی به سمت لایه‌های پایینی حرکت می‌کنند و در حین این انتقال، هر لایه یک سری داده اضافی که **سرآیند** (**header**) خوانده می‌شود به ابتدای داده اصلی اضافه می‌کند (البته گاهی اوقات به غیر از header، به انتهای داده، Trailer نیز اضافه می‌شود). در سمت گیرنده با دریافت داده و حرکت آن به سوی لایه‌های بالاتر، هر لایه سرآیند مخصوص به خود را حذف می‌کند. این روند در شکل ۹ نشان داده شده است. دقت کنید که واحد داده (که به طور کلی PDU نامیده می‌شود) در هر لایه نام متفاوتی دارد. به طوری که نام واحد داده که در لایه کاربرد، پیام (message) است در لایه فیزیکی به بیت تغییر پیدا می‌کند.



شکل ۹: الحاق و جداسازی سرآیند به داده در هر لایه

شکل ۱۰ واحد داده در هر لایه را به طور نمایان‌تری نشان داده است.



شکل ۱۰: واحد داده در هر لایه

نکته۸: نحوه ارتباط لایه‌های فیزیکی با یکدیگر به صورت واقعی و فیزیکی است در حالی که لایه‌های متناظر دیگر، به شکل منطقی با هم در ارتباط هستند.

تذکر۸: با مفهوم baud در فصل دوم آشنا خواهیم شد.

مثال۱۰: نام واحد داده در لایه شبکه چیست؟

۱) فریم ۲) داده‌گرام ۳) سگمنت ۴) پیام

☑ **پاسخ:** گزینه «۲» نام واحد داده در لایه شبکه، داده‌گرام می‌باشد. (به شکل ۱۰ توجه کنید)

سرویس‌های اتصال‌گرا و بدون اتصال (Connection-oriented & connection-less)

به طور کلی نحوه سرویس‌دهی در شبکه را می‌توان به دو صورت اتصال‌گرا و بدون اتصال در نظر گرفت.

در روش **اتصال‌گرا**، قبل از آنکه تبادل داده اصلی آغاز شود، یک سری اطلاعات اولیه، مابین فرستنده و گیرنده مبادله می‌شود. به این فاز اولیه ارتباط که در آن تبادل داده‌های اولیه صورت می‌گیرد، در اصطلاح **دست‌دهی** (**handshaking**) گفته می‌شود. در صورتی که فرستنده و گیرنده آمادگی خود را برای تبادل داده در فاز handshaking اعلام نمایند، ارتباط آغاز می‌شود. به عبارتی دیگر، تبادل داده در این روش با هماهنگی قبلی بین فرستنده و گیرنده صورت می‌گیرد.