
بسم الله الرحمن الرحيم

Socket Network Programming

مدرس: سپیده برادران هزاوه

پاییز ۹۴

جایگاه درس در رشته کامپیوتر

دروس پیش نیاز: برنامه نویسی شئ گرا - شبکه‌های کامپیوتری

نوع درس: تخصصی (۲ واحد نظری ۱ واحد عملی)

نحوه دسترسی به مدرس

baradaran.hezaveh@gmail.com

baradaran-hezaveh.blog.ir

اهداف درس در رشته کامپیوتر

توانمندسازی دانشجویان در ورود به عرصه‌های تخصصی مهارتی از جمله:

راهبری شبکه در سازمان Network Administrator

طراح معماری شبکه سازمان Networking Architecture Design

مشاور سفارش و خرید تجهیزات شبکه سازمان

رعایت امنیت شبکه سازمان Network Security

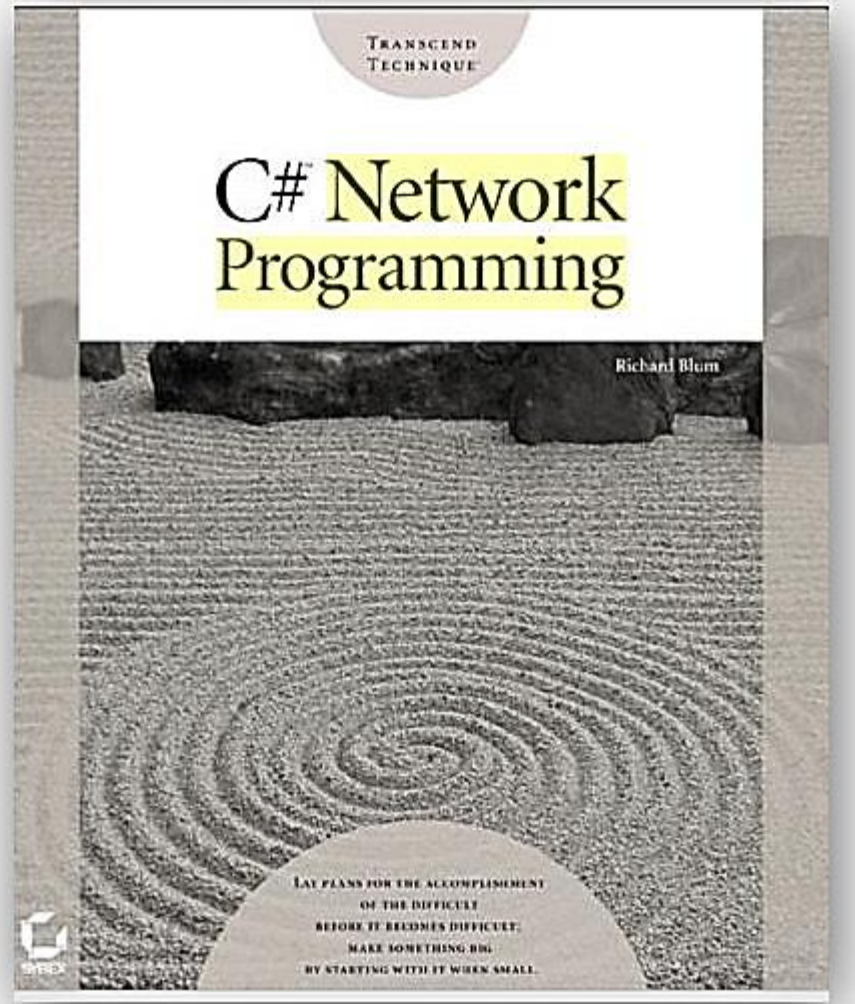
برنامه‌نویسی در محیط شبکه

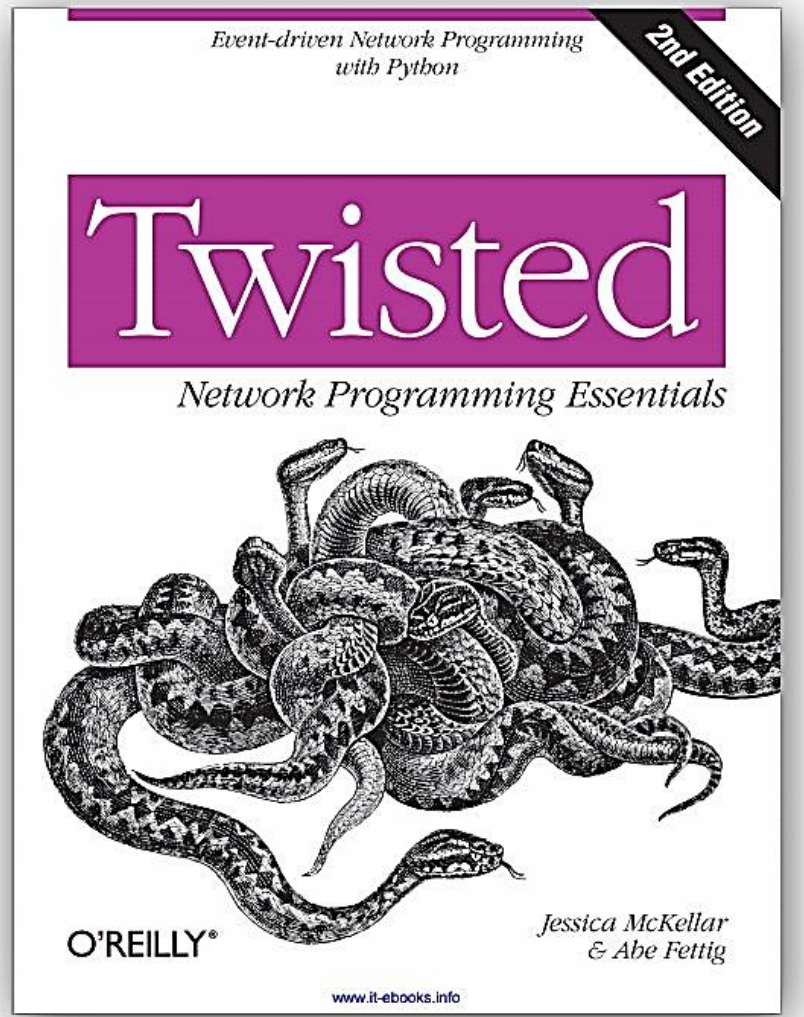
...

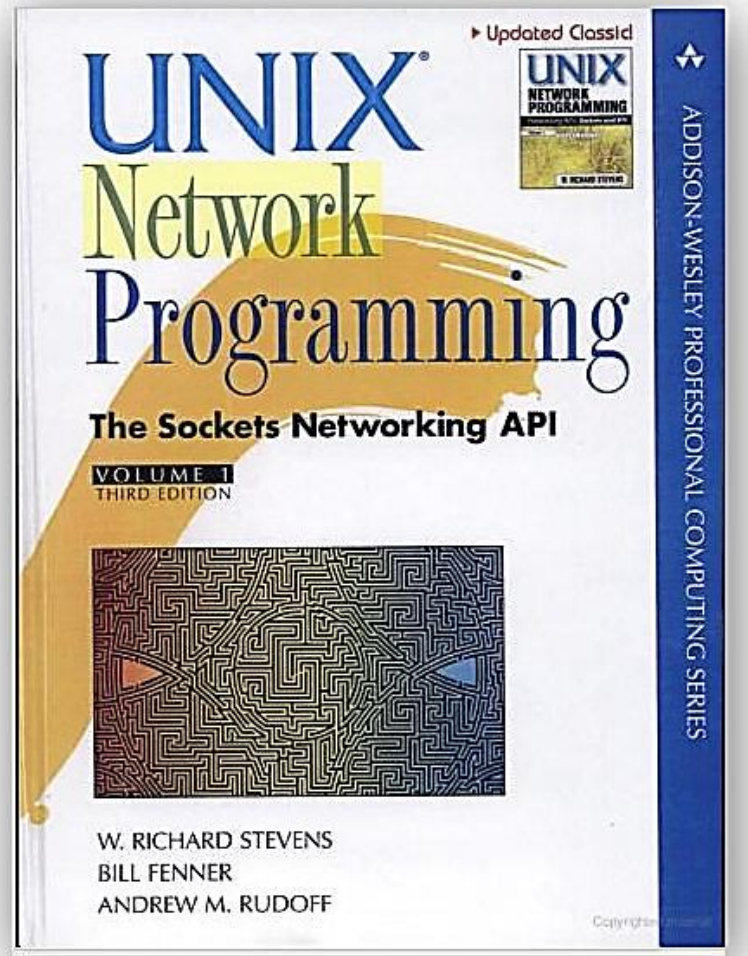
نحوه ارزشیابی

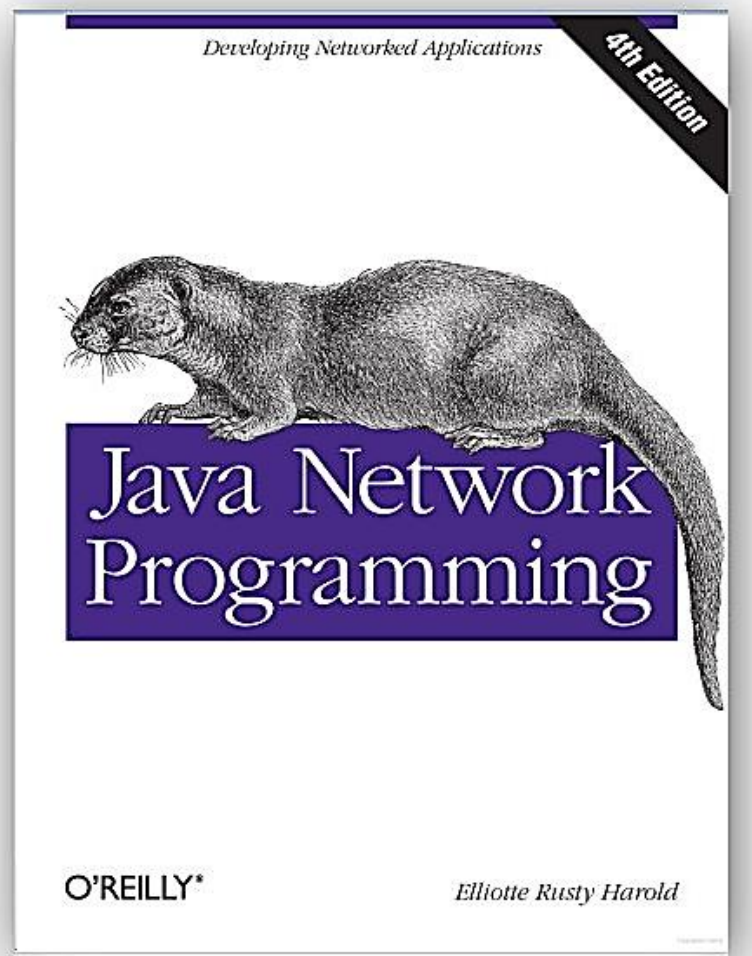
کار کلاسی: تمرین برنامه نویسی و فعالیت کلاسی	۳ نمره
امتحان میان ترم	۳ نمره
امتحان پایان ترم	۱۴ نمره

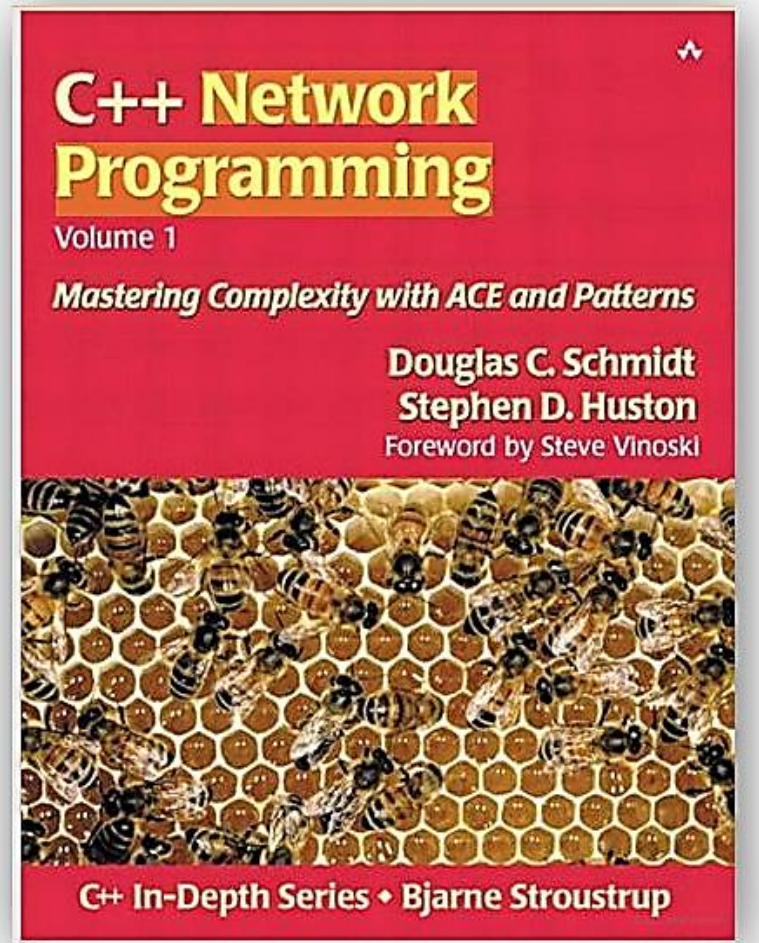
منابع


TRANSCEND
TECHNIQUE
C# Network Programming
Richard Blum
LAY PLANS FOR THE ACCOMPLISHMENT
OF THE DIFFICULT
BEFORE IT BECOMES DIFFICULT;
MAKE SOMETHING BIG
BY STARTING WITH IT WHEN SMALL


Event-driven Network Programming
with Python
2nd Edition
Twisted
Network Programming Essentials
O'REILLY®
Jessica McKellar
& Abe Fettig
www.it-ebooks.info


Updated Classic
UNIX
Network
Programming
The Sockets Networking API
VOLUME 1
THIRD EDITION
W. RICHARD STEVENS
BILL FENNER
ANDREW M. RUDOFF
ADDISON-WESLEY PROFESSIONAL COMPUTING SERIES


Developing Networked Applications
4th Edition
Java Network Programming
O'REILLY
Elliotte Rusty Harold


C++ Network Programming
Volume 1
Mastering Complexity with ACE and Patterns
Douglas C. Schmidt
Stephen D. Huston
Foreword by Steve Vinoski
C++ In-Depth Series • Bjarne Stroustrup

رئوس مطالب

- مروری بر مفاهیم اولیه شبکه
- برنامه نویسی اتصال گرا
- برنامه نویسی بدون اتصال
- همه بخشی و چند بخشی
- پست الکترونیک
- به کارگیری Thread

سخت افزار شبکه

Network(شبکه)

گروهی از رایانه‌ها و دستگاه‌هایی می‌باشد که توسط کانال‌های ارتباطی به هم متصل شده‌اند. شبکه رایانه‌ای باعث تسهیل ارتباطات میان کاربران شده و اجازه می‌دهد کاربران منابع خود را به اشتراک بگذارند. شبکه‌های کامپیوتری مجموعه‌ای از کامپیوترهای مستقل متصل به یکدیگرند که با یکدیگر ارتباط داشته و تبادل داده می‌کنند. مستقل بودن کامپیوترها بدین معناست که هر کدام دارای واحدهای کنترلی و پردازشی مجزا بوده و بود و نبود یکی بر دیگری تاثیرگذار نیست. متصل بودن کامپیوترها یعنی از طریق یک رسانه فیزیکی مانند کابل، فیبر نوری، ماهواره‌ها و... به هم وصل می‌باشند. دو شرط فوق شروط لازم برای ایجاد یک شبکه کامپیوتری می‌باشند اما شرط کافی برای تشکیل یک شبکه کامپیوتری داشتن ارتباط و تبادل داده بین کامپیوترهاست.

مزایای شبکه

- ***تسهیل ارتباطات***: با استفاده از شبکه، افراد می‌توانند به آسانی از طریق رایانامه (E-mail)، پیام‌رسانی فوری، اتاق گفت و گو (Chat room)، تلفن، تلفن تصویری و ویدئو کنفرانس، ارتباط برقرار کنند.
- ***اشتراک گذاری سخت افزارها***: در یک محیط شبکه‌ای، هر کامپیوتر در شبکه می‌تواند به منابع سخت افزاری در شبکه دسترسی پیدا کرده و از آن‌ها استفاده کند؛ مانند چاپ یک سند به وسیله چاپگری که در شبکه به اشتراک گذاشته شده‌است.
- ***اشتراک گذاری پرونده‌ها، داده‌ها و اطلاعات***: در یک محیط شبکه‌ای، هر کاربر مجاز می‌تواند به داده‌ها و اطلاعاتی که بر روی رایانه‌های دیگر موجود در شبکه، ذخیره شده‌است دسترسی پیدا کند. قابلیت دسترسی به داده‌ها و اطلاعات در دستگاه‌های ذخیره سازی اشتراکی، از ویژگی‌های مهم بسیاری از شبکه‌های است.
- ***اشتراک گذاری نرم افزارها***: کاربرانی که به یک شبکه متصل اند، می‌توانند برنامه‌های کاربردی موجود روی کامپیوترهای راه دور را اجرا کنند.

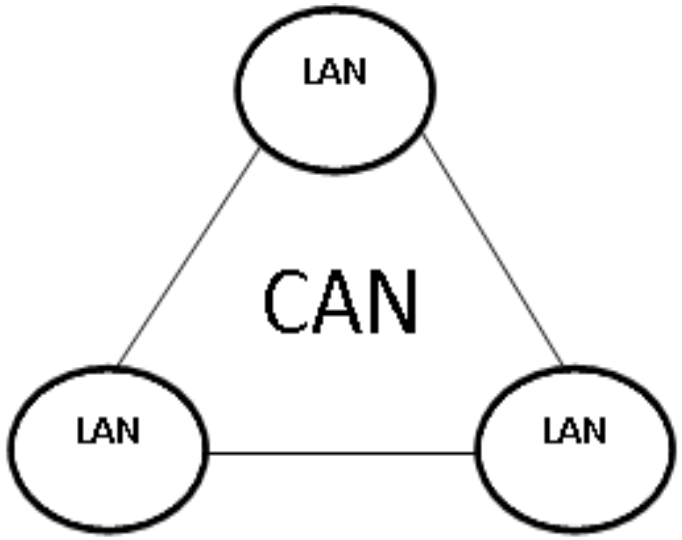
دسته بندی شبکه های رایانه ای

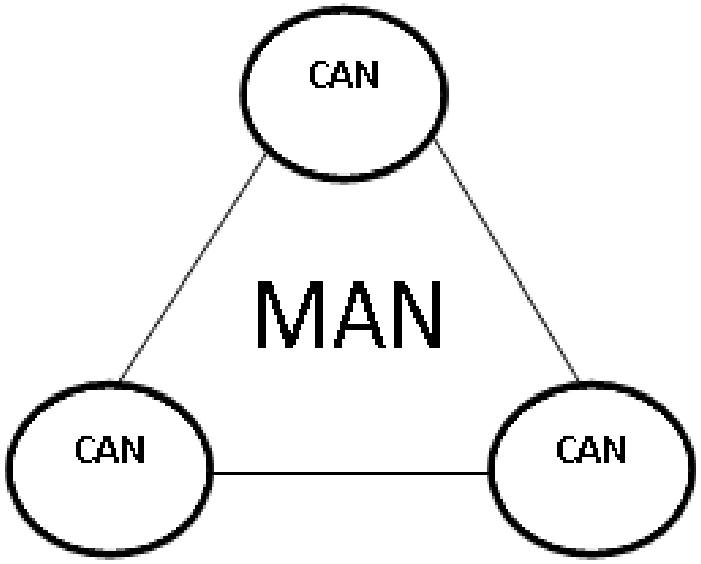
۱. تقسیم بندی شبکه از نظر وسعت جغرافیایی

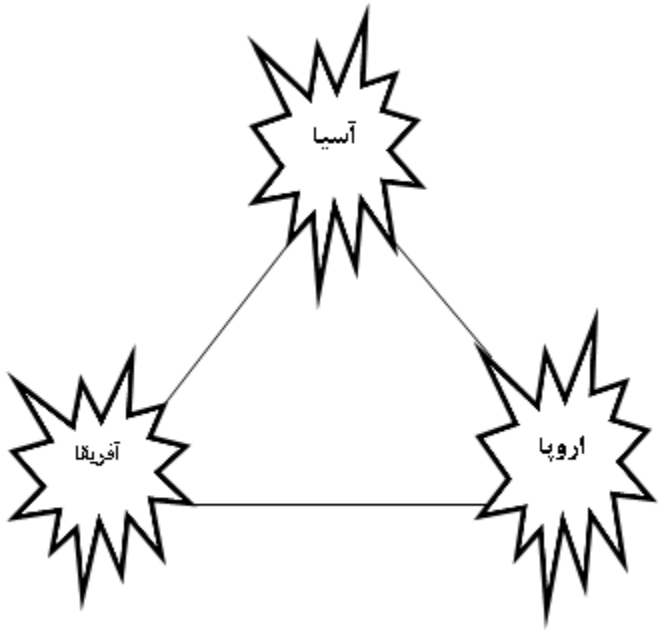
1) LAN (Local Area Network)

2) CAN (Campus Area Network)

3) MAN (Metropolitan Area Network)







۲. تقسیم بندی شبکه از نظر فناوری انتقال

- ✓ شبکه‌های پخش فراگیر
  - Broadcasting پخش عمومی
  - Multicasting پخش گروهی
  - Unicasting
- ✓ شبکه‌های Peer to Peer (Work Group)
- ✓ server base(domain)

۳. تقسیم بندی شبکه از نظر نوع اتصال

- شبکه داخلی یا اینترانت (Intranet)
- شبکه خارجی یا اکسترانت (Extranet)
- شبکه‌اینترنت (Internet)

۱. ممکن است شبکه‌های رایانه‌ای بر اساس اندازه یا گستردگی ناحیه‌ای که شبکه پوشش می‌دهد طبقه‌بندی شوند. برای نمونه «شبکه شخصی» (PAN)، «شبکه محلی» (LAN)، «شبکه دانشگاهی» (CAN)، «شبکه کلان‌شهری» (MAN) یا «شبکه گسترده» (WAN).

شبکه شخصی (PAN)

«شبکه شخصی» (Personal Area Network) یک «شبکه رایانه‌ای» است که برای ارتباطات میان وسایل رایانه‌ای که اطراف یک فرد می‌باشند (مانند «تلفن»ها و «رایانه‌های جیبی» (PDA) که به آن «دستیار دیجیتالی شخصی» نیز می‌گویند) بکار می‌رود. این که این وسایل ممکن است متعلق به آن فرد باشند یا خیر جای بحث خود را دارد. برد یک شبکه شخصی عموماً چند متر بیشتر نیست. موارد مصرف شبکه‌های خصوصی می‌تواند جهت ارتباطات وسایل شخصی چند نفر به یکدیگر و یا برقراری اتصال این وسایل به شبکه‌ای در سطح بالاتر و شبکه «اینترنت» باشد. ارتباطات شبکه‌های شخصی ممکن است به صورت سیمی به «گذرگاه»های رایانه مانند USB و فایروایر برقرار شود. همچنین با بهره‌گیری از فناوری‌هایی مانند IrDA، «بلوتوث» (Bluetooth) و UWB می‌توان شبکه‌های شخصی را به صورت بی‌سیم ساخت.

فایر وایر دستگاهای USBبرای برقراری ارتباط حتماً به یک کامپیوتر میزبان و واسط نیاز دارند. اما فایر وایر نظیر به نظیر یا Peer-To-Peerاست و دستگاهای فایر وایر می توانند برای ایجاد ارتباط با یکدیگر بدون نیاز به کامپیوتر و به طور مستقیم وارد عمل شوند.فایروایر برای دستگاهایی که با حجم زیادی از اطلاعات کار می کنند نظیر دوربین های فیلم برداری،دستگاهای پخش DvDو تجهیزات صدای دیجیتال در نظر گرفته شده و مطلوب است.

IrDA یک فن‌آوری ارتباطی بی‌سیم مادون قرمز است که توسط انجمن اطلاعات مادون قرمز توسعه داده شده است .کاربرد خاصی از نور مادون قرمز مورد استفاده در ارتباطات است در حالیکه Bluetoothکاربرد ویژه‌ای از امواج رادیوئی برای برقراری ارتباط می‌باشد.

UWB یک روش جدید برای انتقال حجم وسیعی از اطلاعات در فاصله کوتاه در شرایط الکترومغناطیسی دشوار است. در این فناوری فرستنده ها از توان تشعشعی بسیار ناچیزی در یک باند بسیار وسیع استفاده کرده و طوری فعالیت میکنند که تاثیر منفی بر روی ارتباطات رادیویی سامانه های ارتباطی در فرکانسهای به کار رفته ایجاد نشود.فناوری فراپهن باند نسبت به سایر سامانه‌های بی‌سیم داخل ساختمان همچون (Wi-۸۰۲.۱۱b Fi) ودندان آبی(Bluetooth) بدلیل فراهم نمودن نرخ ارسال بالاتر با انرژی کمتر و استفاده بهینه چندین کاربر برتری دارد.

شبکه محلی (LAN)

«شبکه محلی» (Local Area Network) یک «شبکه رایانه‌ای» است که محدوده جغرافیایی کوچکی مانند یک خانه، یک دفتر کار یا گروهی از ساختمان‌ها را پوشش می‌دهد. در مقایسه با «شبکه‌های گسترده» (WAN) از مشخصات تعریف‌شده شبکه‌های محلی می‌توان به سرعت (نرخ انتقال) بسیار بالاتر آنها، محدوده جغرافیایی کوچکتر و عدم نیاز به «خطوط استیجاری» مخابراتی اشاره کرد.

دو فناوری «اترنت» (Ethernet) روی کابل («جفت به هم تابیده بدون محافظ» (UTP)) و «وای‌فای» (Wi-Fi) رایج‌ترین فناوری‌هایی هستند که امروزه استفاده می‌شوند، با این حال فناوری‌های «آرکنت» (ARCNET) و «توکن رینگ» (Token Ring) و بسیاری روشهای دیگر در گذشته مورد استفاده بوده‌اند.

شبکه کلان‌شهری (MAN)

«شبکه کلان‌شهری» (Metropolitan Area Network) یک «شبکه رایانه‌ای» بزرگ است که معمولاً در سطح یک شهر گسترده می‌شود. در این شبکه‌ها معمولاً از «زیرساخت بی‌سیم» و یا اتصالات «فیبر نوری» جهت ارتباط محل‌های مختلف استفاده می‌شود.

Wi-Fi مخفف کلمات Wireless Fidelity و در حقیقت یک شبکه بی‌سیم است که مانند امواج رادیو و تلویزیون و سیستم‌های تلفن همراه از امواج رادیویی استفاده می‌کند. یک روتر (router) بی‌سیم سیگنالها را دریافت، رمزگشایی و به اطلاعات تبدیل می‌کند، حال این اطلاعات با استفاده از یک اتصال سیمی اترنت به اینترنت فرستاده می‌شو دو بالعکس.

شبکه گسترده (WAN)

«شبکه گسترده» (Wide Area Network) یک «شبکه رایانه‌ای» است که نسبتاً ناحیه جغرافیایی وسیعی را پوشش می‌دهد (برای نمونه از یک کشور به کشوری دیگر یا از یک قاره به قاره‌ای دیگر). این شبکه‌ها معمولاً از امکانات انتقال خدمات دهندگان عمومی مانند شرکت‌های مخابرات استفاده می‌کند. به عبارت کمتر رسمی این شبکه‌ها از «مسیریاب»ها و لینک‌های ارتباطی عمومی استفاده می‌کنند. شبکه‌های گسترده برای اتصال شبکه‌های محلی یا دیگر انواع شبکه به یکدیگر استفاده می‌شوند. بنابراین کاربران و رایانه‌های یک مکان می‌توانند با کاربران و رایانه‌هایی در مکانهای دیگر در ارتباط باشند. بسیاری از شبکه‌های گسترده برای یک سازمان ویژه پیاده‌سازی می‌شوند و خصوصی هستند. بعضی دیگر به‌وسیله «سرویس دهندگان اینترنت» (ISP:Internet Service Provider) پیاده‌سازی می‌شوند تا شبکه‌های محلی سازمانها را به اینترنت متصل کنند.

۲. در **شبکه های Broadcast**، انتقال اطلاعات از طریق یک کانال فیزیکی که بین تمام ایستگاه های شبکه مشترک است، انجام می شود. همه ی ایستگاه ها موظفند به طور دائم به خط گوش بدهند؛ برای ارسال نیز مجبورند اطلاعات را بر روی همین کانال منتقل نمایند. بنابراین در چنین شبکه هایی هر ایستگاه باید یک آدرس یکتا داشته باشد تا گیرنده ی پیام بتواند از بین پیام هایی که روی شبکه مبادله می شود، پیام مربوط به خودش را تشخیص داده و برای پردازش های بعدی از روی کانال به حافظه ی اصلی منتقل کند.

در این نوع شبکه امکان ارسال پیام های فراگیر وجود دارد. پیام های فراگیر پیام هایی هستند که از مبدا یک ایستگاه برای تمام یا یک گروه خاص از ایستگاه ها ارسال شود. استفاده از کانال های مشترک برای انتقال اطلاعات بین ایستگاه های شبکه از برخی جهات مشکل آفرین است. انواع شبکه هایی که به صورت اتصال فراگیر مورد استفاده قرار می گیرند:شبکه های بیسیم WiFi، شبکه های ماهواره ای، شبکه های محلی اترنت

مدیریت پیچیده ی کانال

در این شبکه، مدیریت کانال به نحوی که تمام ایستگاه ها بتوانند در یک روال قانون مند و عادلانه، از کانال استفاده کنند، پیچیده است. زیرا در شبکه ها هر ایستگاه عنصری مستقل محسوب می شود و هیچ گونه حاکمیت بیرونی بر آنها وجود ندارد لذا رعایت قانون و نوبت در استفاده از کانال بر عهده ی خود ایستگاه ها است. دقت کنید که در این نوع شبکه ها یک ایستگاه مجاز نیست به محض آنکه داده ای برای ارسال داشت، آن را روی کانال بفرستد بلکه باید بر طبق قواعدی که به نام Medium access Control Protocol مشهور است، خودش را نوبت بندی کرده و سپس اقدام به ارسال نماید. ارسال همزمان دو ایستگاه در این نوع شبکه، منجر به تصادم (Collision) شده و در نتیجه داده های ارسالی خراب و فاقد اعتبار خواهد شد.

امنیت کم

با توجه به آنکه تمام ایستگاه ها موظف به گوش دادن به خط هستند بنابراین اطلاعات روی کانال مشترک توسط تمام ایستگاه ها شنیده می شود. کافی است کسی بخواهد به اطلاعات دیگران دسترسی داشته باشد، در این حالت ایستگاه به راحتی با انتقال تمام یا بخشی از اطلاعات در حال تبادل روی کانال به درون حافظه ی اصلی خودف آن را در اختیار شخصی بیگانه قرار می دهد. به همین دلیل استفاده از شبکه های کانال مشترک، برای ارسال اطلاعات محرمانه زمانی عقلانی خواهد بود که این اطلاعات قبل از ارسال رمزگذاری شده باشد.

کارایی پایین

با توجه به آنکه تمام ایستگاه ها فقط یک کانال در اختیار دارند، لذا فقط سهم کوچکی از کل پهنای باید کانال در اختیار یک ایستگاه قرار می گیرد. اگر داده ها در اثر بروز تصادم یا نویز دچار خرابی شوند وضع به مراتب بدتر خواهد شد.

با تمام این تفاصیل استفاده از کانال های مشترک به عنوان تکنولوژی انتقال بسیار مقرون به صرفه است و به صورت گسترده از آن استفاده می شود. شبکه های ماهواره ای، شبکه ی محلی اترنت (اترنت سنتی) و شبکه ی محلی بی سیم و بلوتوث و وای فای همگی شبکه های نوع Broadcast محسوب می شوند.

شبکه های نقطه به نقطه Peer to Peer

در این نوع شبکه هر سیستم می تواند هم نقش client (سرویس گیرنده) و هم نقش server (سرویس دهنده) را داشته باشد، یعنی هرکاربر مدیر سیستم خودش است، admin وجود ندارد، نیاز به سیستم عامل قدرتمتند نیست و تعداد سیستمها محدود و ضریب امنیت نیز پایین است.

بر خلاف شبکه های با کانال مشترک که مسیر ارتباطی بین ایستگاه ها یکتاست، در شبکه های نقطه به نقطه مسیرهای گوناگونی بین دو ماشین برقرار خواهد بود. لذا بحث انتخاب بهترین مسیر از بین این مسیر مطرح خواهد شد.

server base(domain)

در این نوع شبکه یک سیستم بعنوان سرور در نظر گرفته می شود و دیگر سیستمها بعنوان client سرویس را دریافت می کنند، این نوع تقسیم بندی به یک سیستم عامل و سخت افزار قدرمتند نیاز دارد، امنیت شبکه بالا و تعداد سیستمها نیز نامحدود است.

۳. شبکه داخلیIntranet

یک «شبکه داخلی» مجموعه‌ای از شبکه‌های متصل به هم می‌باشد که از قرارداد IP و ابزارهای مبتنی بر IP مانند «مرورگران وب» استفاده می‌کند و معمولاً زیر نظر یک نهاد مدیریتی کنترل می‌شود. این نهاد مدیریتی «شبکه داخلی» را نسبت به باقی قسمت‌های دنیا محصور می‌کند و به کاربران خاصی اجازه ورود به این شبکه را می‌دهد. به طور معمول‌تر شبکه درونی یک شرکت یا دیگر شرکت‌ها «شبکه داخلی» می‌باشد. به طور مثال شبکه ملی در ایران نوعی از شبکه‌های داخلی (اینترانت) می‌باشد.

شبکه خارجی Extranet

یک «شبکه خارجی» یک «شبکه» یا یک «شبکه متصل» است که به لحاظ قلمرو محدود به یک سازمان یا نهاد است ولی همچنین شامل اتصالات محدود به شبکه‌های متعلق به یک یا چند سازمان یا نهاد دیگر است که معمولاً ولی نه همیشه قابل اعتماد هستند. برای نمونه مشتریان یک شرکت ممکن است که دسترسی به بخش‌هایی از «شبکه داخلی» آن شرکت داشته باشند که بدین ترتیب یک «شبکه خارجی» درست می‌شود، چراکه از نقطه‌نظر امنیتی این مشتریان برای شبکه قابل اعتماد به نظر نمی‌رسند. همچنین از نظر فنی می‌توان یک «شبکه خارجی» را در گروه شبکه‌های دانشگاهی، کلان‌شهری، گسترده یا دیگر انواع شبکه (هر چیزی غیر از شبکه محلی) به حساب آورد، چراکه از نظر تعریف یک «شبکه خارجی» نمی‌تواند فقط از یک شبکه محلی تشکیل شده باشد، چون بایستی دست کم یک اتصال به خارج از شبکه داشته باشد.

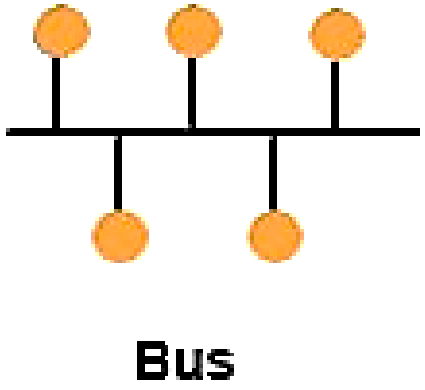
شبکه اینترنت (Internet)

شبکه ویژه‌ای از شبکه‌ها که حاصل اتصالات داخلی شبکه‌های دولتی، دانشگاهی، عمومی و خصوصی در سرتاسر دنیا است. این شبکه بر اساس شبکه اولیه‌ای کار می‌کند که «آرپانت» (ARPANET) نام داشت و به‌وسیله موسسه «آرپا» (ARPA) که وابسته به «وزارت دفاع ایالات متحده آمریکا» است ایجاد شد. همچنین منزلگاهی برای «وب جهان‌گستر» (WWW) است. در لاتین واژه Internet برای نامیدن آن بکار می‌رود که برای اشتباه نشدن با معنی عام واژه «شبکه متصل» حرف اول را بزرگ می‌نویسند.

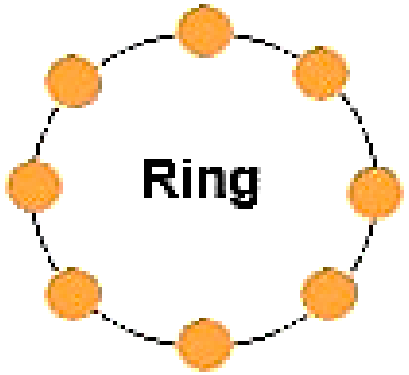
اعضای شبکه اینترنت یا شرکت‌های سرویس دهنده آنها از «آدرسهای IP» استفاده می‌کنند. این آدرس‌ها از موسسات ثبت نام آدرس تهیه می‌شوند تا تخصیص آدرسها قابل کنترل باشد. همچنین «سرویس دهندگان اینترنت» و شرکت‌های بزرگ، اطلاعات مربوط به در دسترس بودن آدرس‌هایشان را بواسطه «قرارداد دروازه لبه» (BGP) با دیگر اعضای اینترنت مبادله می‌کنند.

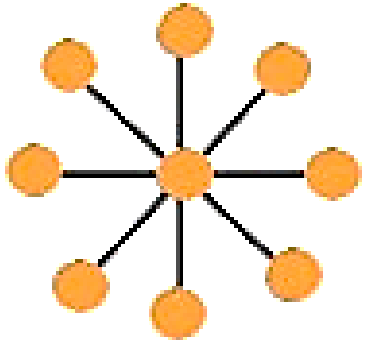
انواع Topology در شبکه

نحوه چیدمان یا اتصال کامپیوترها به یکدیگر را توپولوژی می گویند.



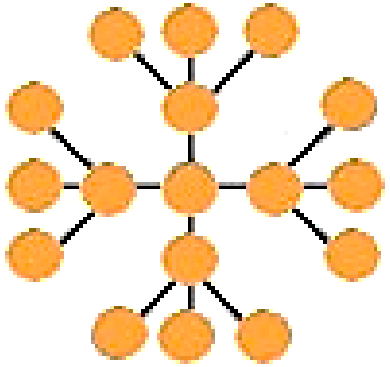
Bus



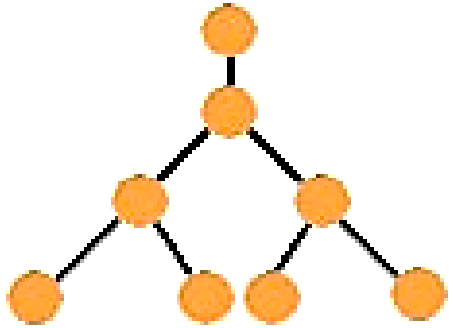


Star

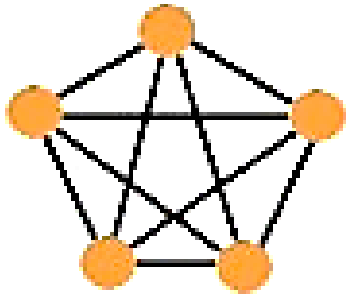
- توپولوژی Bus یا خطی
- توپولوژی Star
- توپولوژی رینگی
- توپولوژی مش(Mesh)
- توپولوژی Hybrid
- توپولوژی Tree



Extended Star



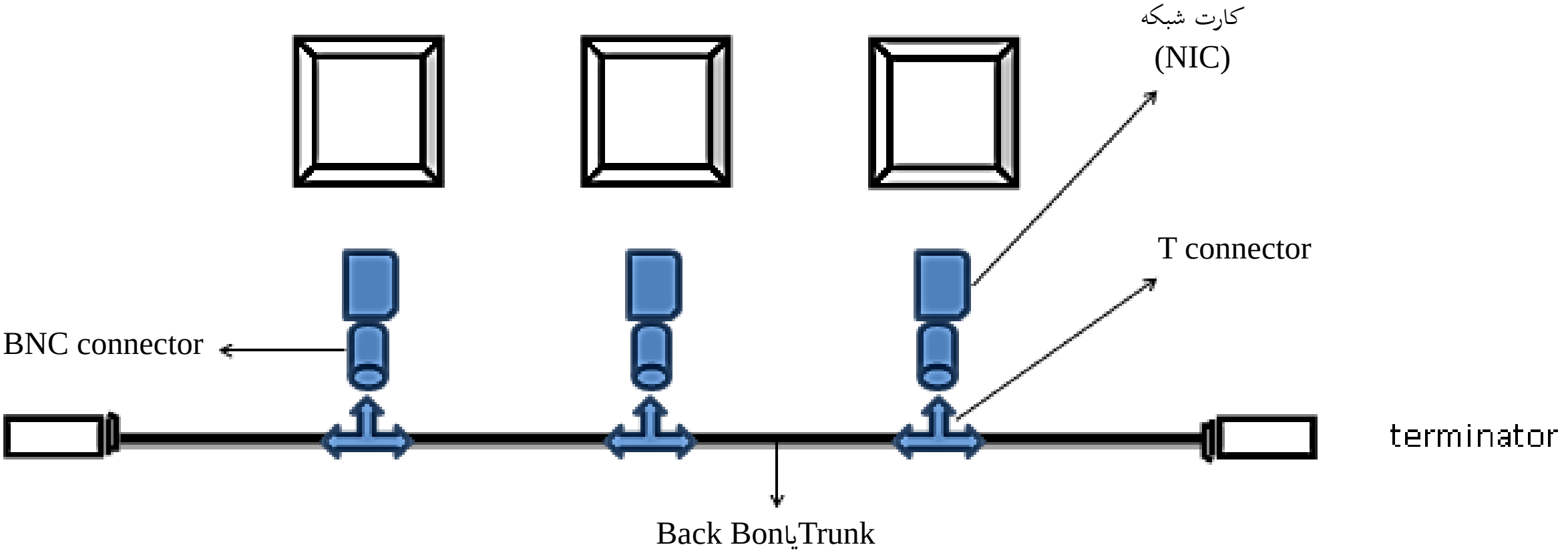
Tree



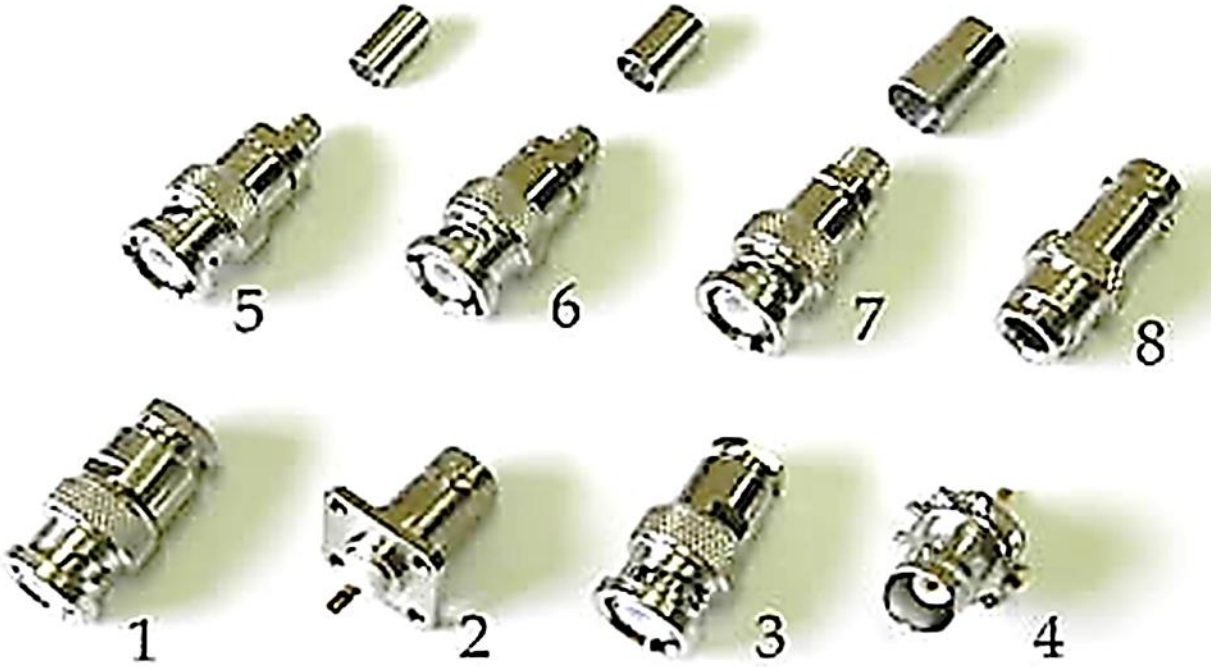
Mesh

توپولوژی Bus یا خطی

در این توپولوژی سیستمها توسط یک رشته کابل (Coaxial) به یکدیگر متصل می گردند دو طرف کابل یک ترمیناتور ۵۰ اهمی مسدود تا از بازگشت سیگنالهای اضافه به کابل جلوگیری نماید و هر سیستم توسط یک کارت شبکه(Network interface card: NIC) ، یک (BNC connector) و نهایتاً با یک (T connector) به کابل شبکه جهت تبادل اطلاعات و استفاده از منابع متصل می شوند



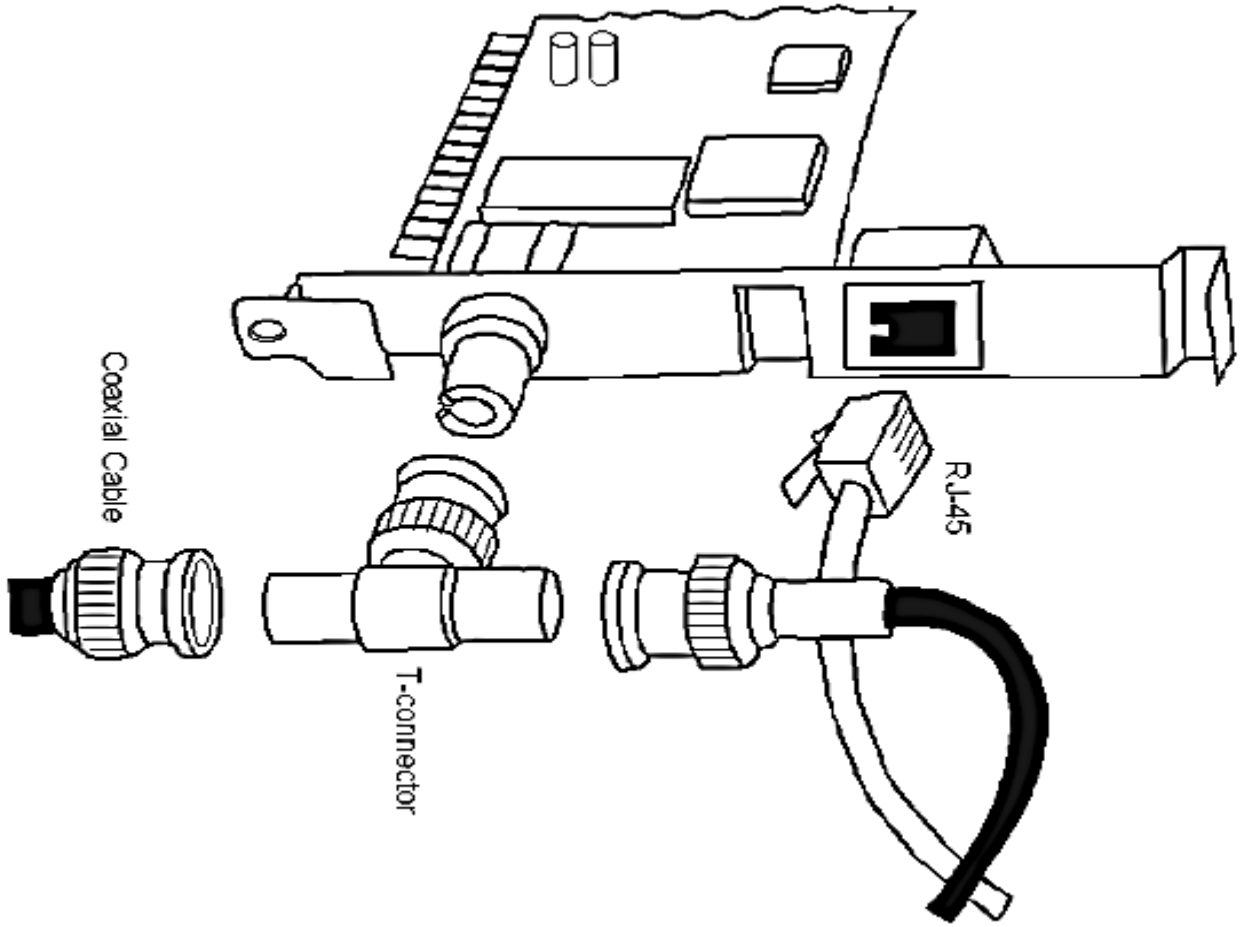
Connector BNC



BNC T Connector

Straight Terminator

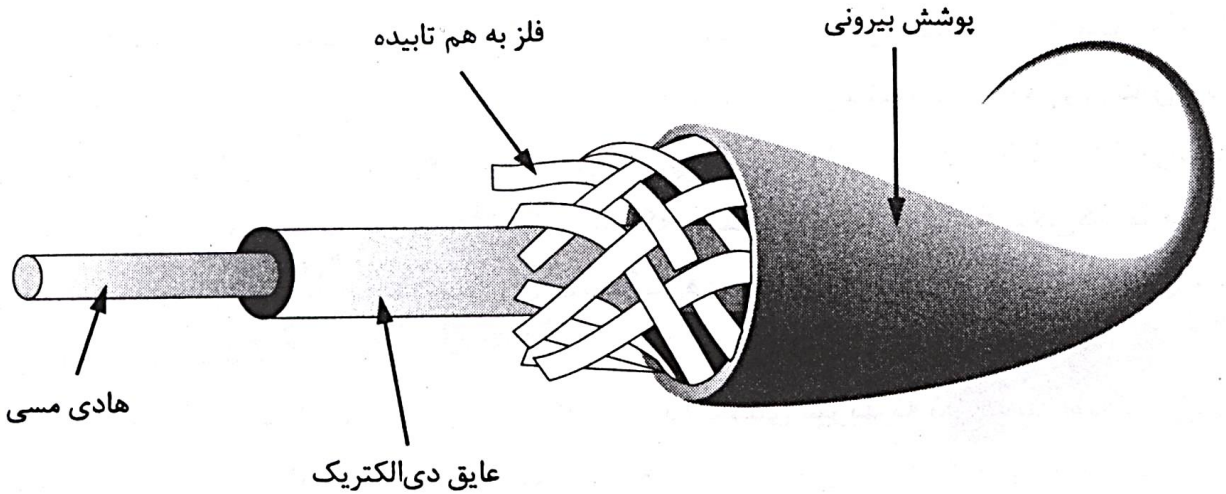
N	Model	Description
1	MT 801	Connector BNC Macho para RG 59 - Solda
2	MT 819	Conector BNC Fêmea com Base Quadrada para Painel
3	MT 812	Conector BNC Macho para RG 58 - Solda
4	MT 804	Conector BNC Fêmea com Rosca para Painel
5	MT 815/58	Conector BNC Macho para RG 58 - Climpar - 50 Ohms
6	MT 815/59	Conector BNC Macho para RG 59 - Climpar - 75 Ohms
7	MT 814	Conector BNC Macho para RG 59 Malha Dupla - Climpar - 75 Ohms
8	MT 805	Connector BNC Fêmea para RG 59 - Solda



کابل Coaxial

اولین فناوریهای تجاری LAN در دهه ۱۹۷۰ معرفی شدند که از کابل کواکس به عنوان رسانه شبکه استفاده می کردند . نام کابل کواکس بر اساس دو هادی انتخاب شده است که یک محور مشترک دارند که از مرکز کابل می گذرد . بسیاری از انواع کابل مسی دو هادی جداگانه دارند و آنها را از هم جدا می سازند . اما کابل کواس گرد است ، و یک هسته مسی در مرکز دارد که اولین هادی را تشکیل می دهد . این هسته است که سیگنالهای واقعی را منتقل می کند . یک لایه از عایق لاستیکی دی الکتریک هسته را در بر می گیرد و آن را از هادی دوم که از شبکه ای از سیمهای به هم تابیده ساخته شده است و به عنوان زمین عمل می کند جدا می کند . در همه کابل های الکتریکی هدایت کنند ه سیگنال و زمین باید همیشه از هم جدا باشند ، و گرنه اتصال کوتاه رخ می دهد و روی کابل نویز ایجاد می کند . کل این ساختار نیز در یک حفاظ عایق قرار می گیرد

کابلهای کواس می توانند هسته مسی یکپارچه و یا به هم تابیده داشته باشند ، و عنوان آنها مشخص کننده این تفاوت است . پسوند U / هسته یکپارچه ، و پسوند A/U هسته به هم تابیده را نشان می دهد . به عنوان مثال در Thin Ethernet می توان از کابل RG-58/U یا RG – 58A/U استفاده کرد .



شبکه های کواکس با استفاده از هم بندی باس کابل کشی می شوند ، که در آن کابل به صورت یک قطعه با دو انتهاست که کامپیوترها در امتداد طول آن به آن وصل می شود . هر سیگنالی که توسط یک ایستگاه کاری به روی کابل ارسال می شود روی باس در هر دو جهت به حرکت در می آید تا به همه کامپیوترهای دیگر و سر انجام به دو انتهای کابل برسد . در هریک از دو انتهای باس باید یک مقاومت خاتمه دهنده وجود داشته باشد که سیگنالهای را که دریافت می کند با صفر کردن ولتاژ آنها خنثی کند . بدون این مقاومت های خاتمه دهنده ممکن است سیگنالها به انتهای کابل برسند و باز در کابل منعکس شوند که منجر به خرابی داده ها می شود .
در مقایسه با سایر انواع کابل ، کابل کواکس برای شبکه های داده تا حدی غیر بهینه نیز هست . شبکه اترنتی که با کابل کواکس ساخته می شود به سرعت ۱۰ Mbps محدود است و هیچ راهی برای ارتقاء آن به یک فناوری سریعتر ، آن طور که در مورد کابل زوج به هم تابیده یا فیبر نوری و Fast Ethernet ممکن است ، وجود ندارد . هرچند ممکن است در شبکه هایی که نصب آنها به سالها پیش بر می گردد کابل کواکس به کار رفته باشد ، اما در حال حاضر تقریباً هیچ Ethernet LAN جدیدی را با آن نصب نمی کنند .

انواع کابل کواکسیال

دو نوع کابل کواکسیال وجود دارد که عبارتند از:

۱. نازک (Thinnet)

۲. ضخیم (Thicknet)

۱. این نوع کابل کواکسیال قابل انعطاف است و قطر آن در حدود ۰/۲۵ اینچ می‌باشد. از آنجا که Thinnet نرم و انعطاف‌پذیر است و کارکردن با آن هم آسان می‌باشد. تقریباً در تمام شبکه‌ها می‌تواند مورد استفاده قرارگیرد. در شبکه‌هایی که از Thinnet استفاده می‌کنند، کابل مستقیماً به کارت شبکه متصل می‌شود. نوع نازک کابل کواکسیال می‌تواند سیگنال‌ها را تا فاصلهٔ تقریبی ۱۸۵ متر (۶۰۷ فوت) ارسال کند، بدون آن که تضعیف شوند. کابل Thinnet جزء کابل‌های خانوادهٔ RG-58 بوده و دارای امپدانس ۵۰ اهم است. امپدانس، مقاومت سیم در برابر جریان متناوب است. تفاوت اصلی میان کابل‌های خانوادهٔ RG-58 هستهٔ مسی در مرکز آنهاست. این هسته می‌تواند به صورت یک مفتول یا چند تار به هم تابیده باشد.

۲. این نوع کابل، کواکسیال انعطاف ناپذیر و قطر آن در حدود ۰/۵ اینچ است (کابل RG – 8/U). گاهی اوقات به کابل Thicknet اترنت استاندارد نیز گفته می‌شود. زیرا اولین نوع کابل کواکسیال بود که در معماری شبکه معروف Ethernet به کار برده شد. هستهٔ مسی این کابل کواکسیال ضخیم‌تر از نوع نازک آن است. نوع ضخیم کابل کواکسیال می‌تواند سیگنال‌ها را بدون تضعیف تا فاصله ۵۰۰ متر (حدود ۱۶۴۰فوت) انتقال دهد. بنابراین با توجه به قابلیت Thicknet در پشتیبانی عمل انتقال داده‌ها در مسافت‌های طولانی، از آن به عنوان ستون اصلی برای اتصال شبکه‌های Thinnet کوچکتر به یکدیگر استفاده می‌شود. بر اساس مشخصه اترنت برای وصل کردن NIC کامپیوترها به کابل RG – 8/U کابل های Attachment Unit Interface (AUI) مورد نیاز است.

نکته:توپولوژی خطی که در آن از کابل thinnet استفاده شده باشد را استاندارد Base2 می گویند.
نکته:توپولوژی خطی که در آن از کابل thiknet استفاده شده باشد را استاندارد Base5 می گویند.

10BASE5 - "Thicknet"

10BASE2 - "Thinnet"

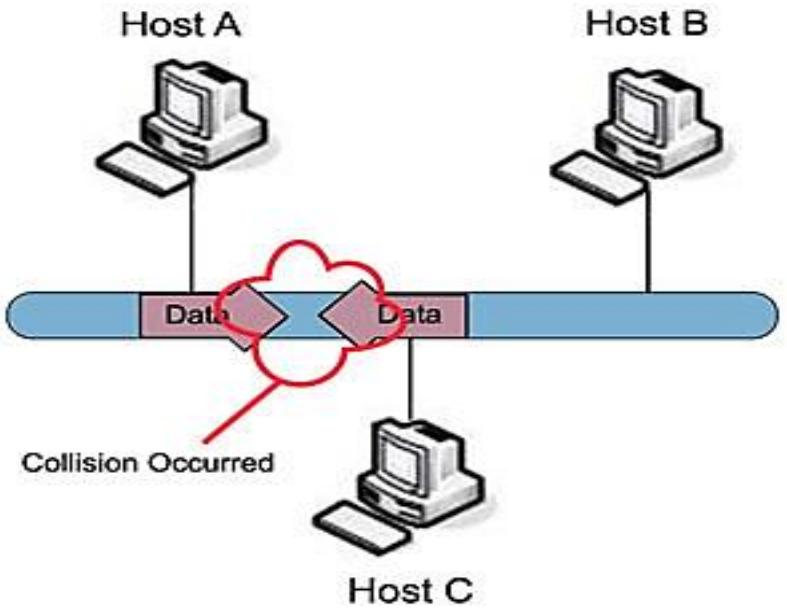
مکانیزم جلوگیری از بروز خطا در شبکه

1) **CSMA/CD** (Carrier Sense Multiple Access /Collision Detection) گوش کردن دائم به خط با آشکار سازی خطا

اگر دوسیستم همزمان اطلاعات را ارسال نمایند برخورد یا Collision رخ می دهد لذا هر سیستمی که زودتر متوجه این برخورد شود سیگنالی به نام Jamming روی کابل ارسال می کند تا به بقیه سیستمها اطلاع دهد که برخورد صورت گرفته و کامپیوتر دیگری اطلاعاتش را ارسال نکند تا ارسال بین سیستمهایی که همزمانی را ایجاد نموده اند صورت گیرد و همزمانی به پایان برسد، سپس دو سیستمی که همزمانی یا برخورد را ایجاد نموده اند بصورت اتفاقی با هم توافق کرده و اطلاعات خود را با فاصله زمانی مقبول ارسال می کنند.

2) **CSMA/CA** (Carrier Sense Multiple Access /Ander Detection)

در این مکانیزم هر سیستمی که قصد انتقال اطلاعات را دارد ابتدا یک Jamming بر روی خط ارسال می کند تا به دیگرکاربران اطلاع دهد قصد ارسال اطلاعاتش را دارد و collision رخ ندهد. نقطه ضعف این مکانیزم ایجاد ترافیک در شبکه است.

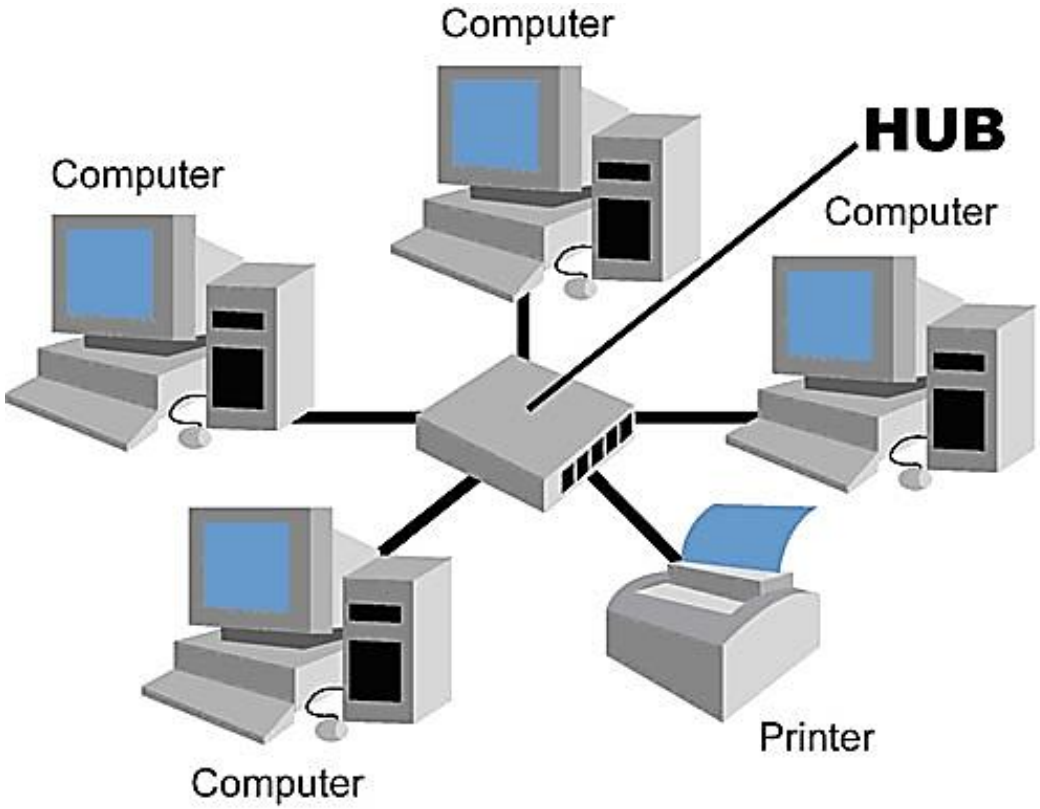


توپولوژی Star

در این توپولوژی برای ارتباط بین کامپیوترها از Hub یا Switch استفاده می شود.

۱. استفاده از Hub در توپولوژی Star

- ✓در این نوع اتصال، ارسال و دریافت یکطرفه (Half Duplex) می باشد یعنی فقط یک سیستم می تواند ارسال و سیستم دیگر دریافت نماید.
- ✓سیگنال روی تمامی پورتها تکرار می شود ولی فقط سیستم مقصد می تواند به اطلاعات دسترسی پیدا نماید زیرا یک آدرس مبدا و یک آدرس مقصد تعریف شده است.



دو نوع هاب وجود دارد

Active کار تقویت سیگنال را نیز انجام می دهد.

Passive کار تقویت سیگنال را انجام نمی دهد و فقط همانند یک جعبه تقسیم عمل می کند.

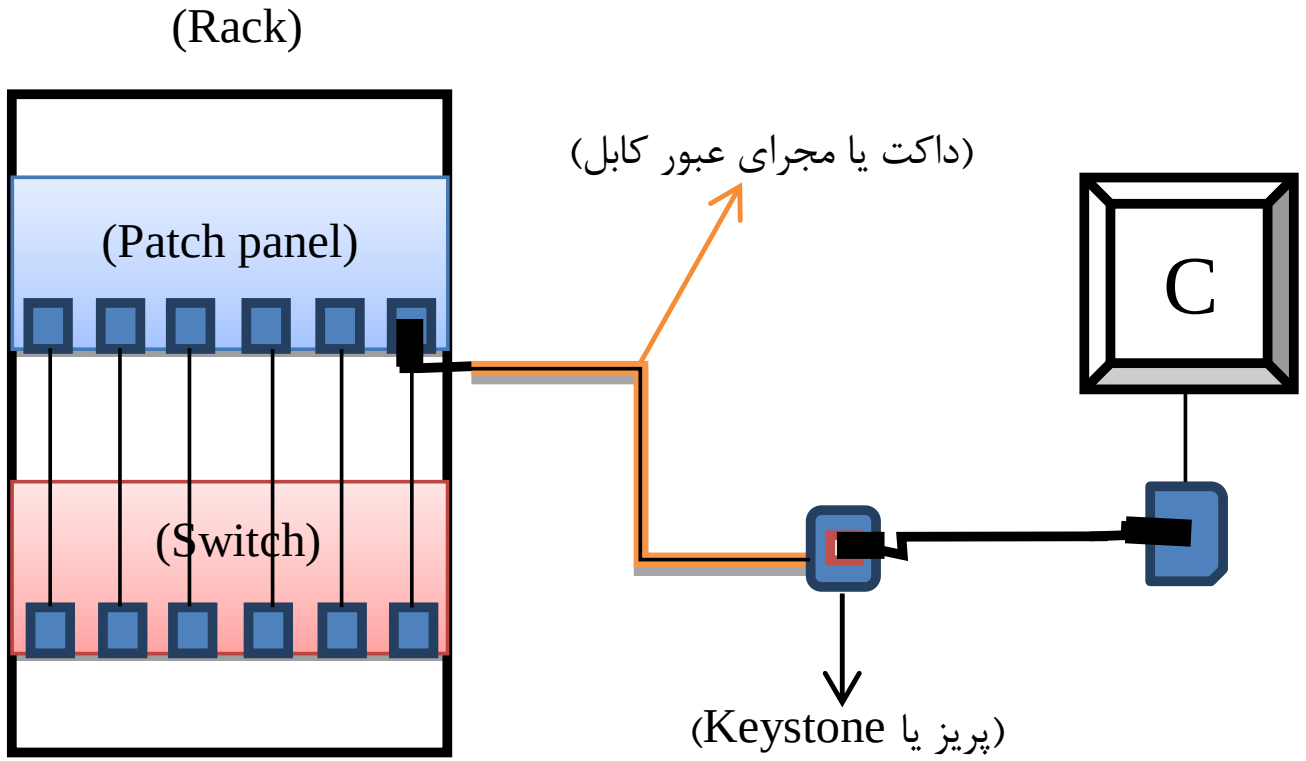
۲. استفاده از از Switch در توپولوژی Star

✓در این نوع اتصال، ارسال بصورت همزمان و دو طرفه Full Duplex نیز امکان پذیر است یعنی هر کاربر در هنگام دریافت می تواند اطلاعات خود را نیز ارسال نمایند.

✓سیگنال روی تمامی پورتها تکرار نمی شود و مستقیماً به سمت مقصد ارسال می گردد.

سوئیچ به لحاظ رقمی گران تر از هاب است به همین دلیل برای محافظت بیشتر آنرا در داخل جعبه ای به نام راک قرار می دهند و آن را به panel Patch متصل می کنند تا از دسترس افراد دور باشد و آسیب نبیند.

نکته:الکتریسیته ساکن در بدن انسان با برخورد به سوئیچ امکان دارد این دستگاه را بسوزاند.



کابل Twisted pair (زوج به هم تابیده شده)

کابل زوج به هم تابیده که در بیشتر شبکه های داده استفاده می شود در یک حفاظ ، چهار جفت سیم مسی عایق بندی شده دارد . هر جفت سیم در هر اینچ به تعداد مختلفی به هم تاب می خورند تا از تداخل الکترومغناطیسی ناشی از سایر جفتها و منابع بیرونی اجتناب شود .

جفت سیمهای کابل زوج به هم تابیده رنگ بندی خاصی دارند که بر اساس رنگهای تعریف شده در استاندارد TIA/ EIA – T568 – A به شرح زیر هستند . در هرجفت سیم تکرنگ سیگنالها را منتقل می کند و سیم راه راه به عنوان زمین عمل می کند .

Unshielded twisted pair (UTP)

جفت ۱ – آبی تکرنگ و راه راه سفید و آبی

جفت ۲ – نارنجی تکرنگ ، و راه راه سفید و نارنجی

جفت ۳ – سبز تکرنگ ، و راه راه سفید و سبز

جفت ۴ – قهوه ای تکرنگ ، و راه راه سفید و قهوه ای

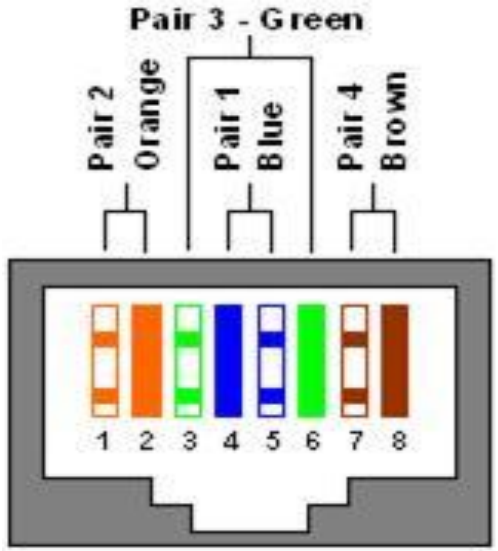
Twisted pair (زوج به هم تابیده شده)= UTP یا STP

از کابل UTP بیشتر از STP استفاده می شود ، بیشتر شبکه های اترنت دفتری از کابل UTP استفاده می کنند. استاندارد TIA /EIA T 568- A – سطوح کارایی را برای کابل UTP تعریف می کند که طبقه خوانده می شود . هر چه درجه بندی طبقه یک کابل بالاتر باشد به این معنی است که آن کابل بهتر است و می تواند داده ها را با سرعت های بالاتری ارسال کند . تفاوت اصلی بین طبقه های مختلف کابل در میزان به هم فشردگی تابهای هر جفت سیم است .

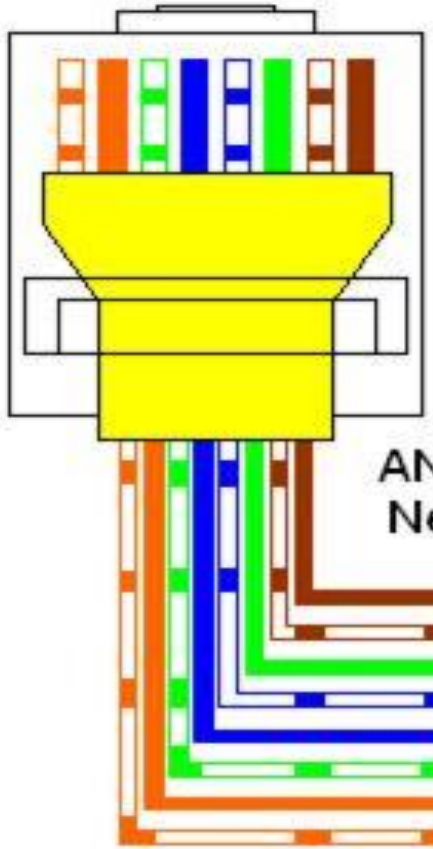
Shielded twisted pair (STP)

- ✓ تقسیم بندی هر یک از گروه های فوق بر اساس نوع کابل مسی و Jack انجام شده است .
- ✓ از کابل های CAT1، به دلیل عدم حمایت ترافیک مناسب، در شبکه های کامپیوتری استفاده نمی گردد .
- ✓ از کابل های گروه CAT2, CAT3, CAT4, CAT5و CAT6 در شبکه ها استفاده می گردد .کابل های فوق ، قادر به حمایت از ترافیک تلفن و شبکه های کامپیوتری می باشند .
- ✓ از کابل های CAT2 در شبکه های Token Ring استفاده شده و سرعتی بالغ بر ۴ مگابیت در ثانیه را ارائه می نمایند .
- ✓ برای شبکه هائی با سرعت بالا (یکصد مگا بیت در ثانیه) از کابل های CAT5 و برای سرعت ده مگابیت در ثانیه از کابل های CAT3 استفاده می گردد.
- ✓ از کابل های CAT3 و CAT4 در شبکه های Token Ring استفاده می گردد .
- ✓ حداکثر مسافت در کابل های CAT3، یکصد متر است .
- ✓ حداکثر مسافت در کابل های CAT4، دویست متر است .
- ✓ کابل CAT6 با هدف استفاده در شبکه های اترنت گیگابیت طراحی شده است . در این رابطه استانداردهائی نیز وجود دارد که امکان انتقال اطلاعات گیگابیت بر روی کابل های CAT5 را فراهم می نماید (CAT5e) کابل های CAT6 مشابه کابل های CAT5 بوده ولی بین ۴ زوج کابل آنان از یک جداکننده فیزیکی به منظور کاهش پارازیت های الکترومغناطیسی استفاده شده و سرعتی بالغ بر یکهزار مگابیت در ثانیه را ارائه می نمایند.

نوع	سرعت	موارد کاربرد
CAT1	حداکثر تا یک مگابیت در ثانیه	سیستم های قدیمی تلفن ، ISDN و مودم
CAT2	حداکثر تا چهار مگابیت در ثانیه	شبکه های Token Ring
CAT3	حداکثر تا ده مگابیت در ثانیه	شبکه های Token ring و BASE-T۱۰
CAT4	حداکثر تا شانزده مگابیت در ثانیه	شبکه های Token Ring
CAT5	حداکثر تا یکصد مگابیت در ثانیه	اترنت (ده مگابیت در ثانیه) ، اترنت سریع (یکصد مگابیت در ثانیه) و شبکه های Token Ring) شانزده مگابیت در ثانیه)
CAT5e	حداکثر تا یکهزار مگابیت در ثانیه	شبکه های Gigabit Ethernet
CAT6	حداکثر تا یکهزار مگابیت در ثانیه	شبکه های Gigabit Ethernet



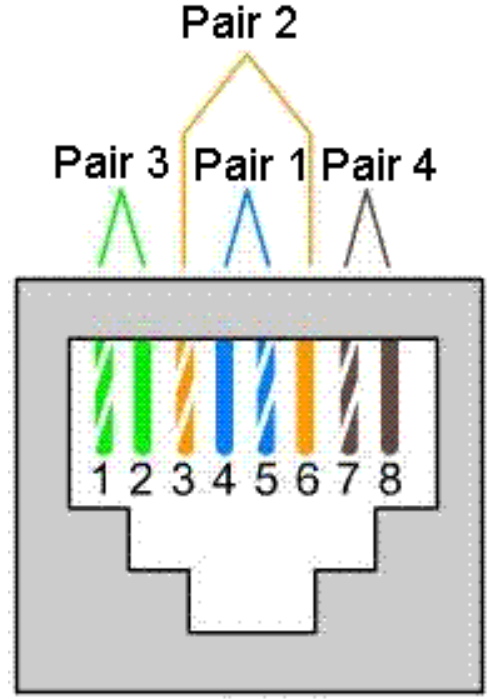
RJ-45 Jack



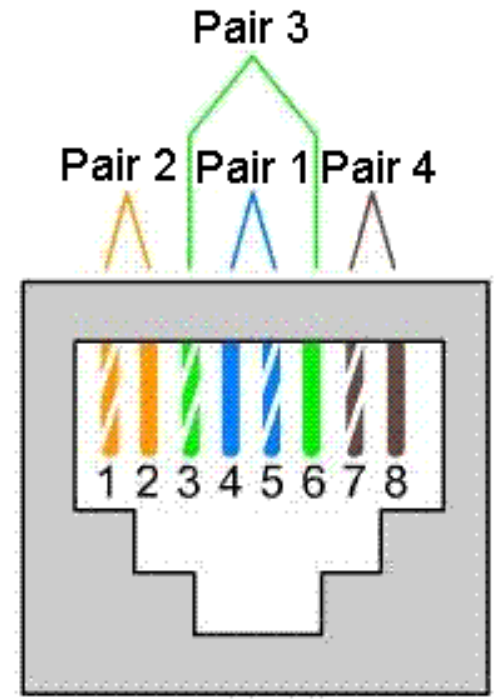
RJ-45 Plug

ANSI/TIA/EIA 568B Network Interface

8. Brown
7. Brown-White
6. Green
5. Blue-White
4. Blue
3. Green-White
2. Orange
1. Orange-White



T568A



T568B

TIA/EIA 568A Wiring

1	Green-White
2	Green
3	Orange-White
4	Blue
5	Blue-White
6	Orange
7	Brown-White
8	Brown

TIA/EIA 568B Wiring

1	Orange-White
2	Orange
3	Green-White
4	Blue
5	Blue-White
6	Green
7	Brown-White
8	Brown

در ساختار چینش رشته های کابل دو استاندارد فراگیر وجود دارد که به استاندارد A و B معروف است. اگر دو سر کابل از استاندارد A و یا از استاندارد B استفاده نماییم، کابل Straight ایجاد می شود و چنانچه یک طرف کابل از استاندارد A و طرف دیگر از استاندارد B استفاده نماییم، کابل Cross را تولید کرده ایم.

در مواقعی که می خواهیم دو دستگاه یکسان را به یکدیگر متصل نماییم از کابل Cross استفاده می کنیم مانند اتصال دو کامپیوتر یا دو روتر به یکدیگر. البته استثناهایی هم وجود دارد مثلا اتصال کامپیوتر به روتر (هم جنس نیستند اما از این کابل استفاده می کنند). در اتصال کامپیوتر به سوییچ یا هاب یا مودم از کابل Straight استفاده می شود. به منظور تفاوت ساختار دستگاه ها در ارسال و دریافت از این دو نوع کابل استفاده می شود.

با تمام توصیف های داده شده این دو مدل قابل تعویض هستند. کارت شبکه های جدید (نه تمامی آن ها) قابلیت هایی از قبیل Auto Sends را دارند به این معنی که تشخیص می دهند که مسیر ارسال و دریافت کدام است .

یکی از دلایل بهم تابیده شدن سیمهای Twisted pair جلوگیری از Crosstalk (همشنوایی) است. به این ترتیب که اثر مغناطیسی سیمها با برخورد به یکدیگر نویز را دفع می کنند.

Crosstalk (همشنوایی) : اثر میدانهای مغناطیسی یک کابل بر کابل مجاور خود می باشد، مانند نویزهایی که کابلهای برق فشار قوی یا رعد و برق ایجاد می کنند.

انواع کابل از نظر مقاوت در برابر نویز

UTP (Unshielded Twisted Pair): این نوع کابل بدون شیلد (روکش داخلی)می باشد.

STP (shielded Twisted Pair): دارای شیلد می باشد و مناسب برای جلوگیری از نویز.

FTP (Foiled Twisted Pair): دارای فویل آلومینیومی که برای جلوگیری از نویز بسیار عالی است.

توپولوژی حلقه ای Ring

در آن رایانه‌های شبکه را با یک کابل تکی به صورت دایره‌ای شکل به هم متصل می‌سازند. در این توپولوژی انتهای پایانی وجود ندارد سیگنالهای دور حلقه در یک جهت حرکت می‌کنند و از تمام رایانه‌ها می‌گذرند. بر خلاف توپولوژی خطی که غیر فعال است هر رایانه شبیه یک تکرار کننده عمل می‌کند و سیگنالهای دریافتی را پس از تقویت به رایانه بعدی می‌فرستد چون سیکنال از تمامی رایانه‌ها می‌گذرد خرابی یک رایانه بر کل شبکه تاثیر می‌گذارد. در این طراحی انتقال اطلاعات به نوعی نوبتی میباشد که با نام token یاد می شود. در توپولوژی رینگ بجای بستن دو سر سیم آنها را به یکدیگر وصل نموده و تشکیل یک حلقه میدهند. همیشه یک بسته کوچک با نام نشانه (Token) در داخل شبکه از یک رایانه به دیگری می‌رود، زمانی که یک رایانه اطلاعاتی جهت ارسال دارد، نشانه را در اختیار گرفته و از چرخش آن داخل شبکه جلوگیری می‌کند، تا زمانیکه نشانه توسط یک رایانه نگه‌داشته شده باشد، تمام رایانه‌های شبکه پذیرای اطلاعاتی خواهند بود که رایانه مالک نشانه ارسال می‌کند.که معایب این نوع توپولوژی این است که اگر قسمتی از کابل اصلی به علتی آسیب ببیند کل شبکه از کار می افتد و عیب یابی آن بسیار وقت گیر می‌باشد و از مزایای آن میتوان به کم هزینه بودن و سادگی شبکه اشاره کرد.

در توپولوژی رینگی از Token Switch استفاده می شود که ساختار حلقه در آن وجود دارد و کار انتقال داده ها را انجام می دهد.

قرار دادن یک Tokenجدید:

اگر Token Frame به هر دلیلی از بین برود یک سیستم مامور می شود تا در صورت صحت از بین رفتن آن یک Token جدید را در شبکه قرار دهد (Supervisor).

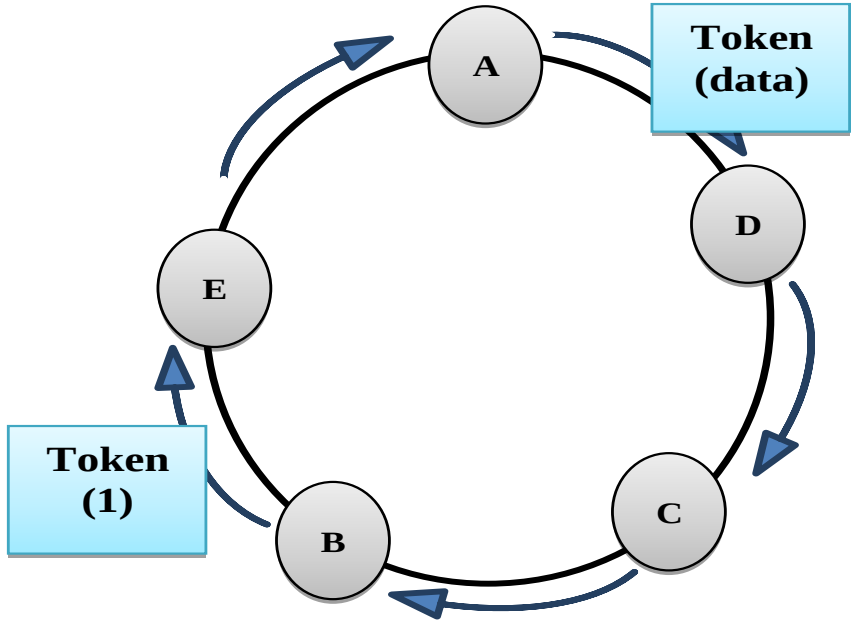
مکانیزم جلوگیری از بروز خطا

1) CSMA/CD (Carrier Sense Multiple Access /Collision Detection)

2) CSMA/CA (Carrier Sense Multiple Access /Ander Detection)

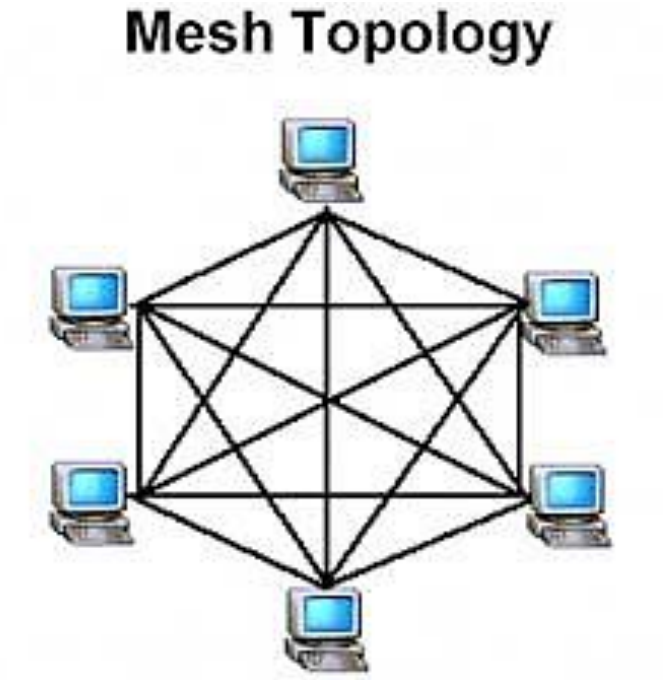
3) Token Passing

مثال: در شکل زیر وقتی قرار است اطلاعات از کامپیوتر A به کامپیوترB ارسال شود اطلاعات در داخل token Frame قرار می گیرد و در مسیر خود به کامپیوتر D منتقل می گردد و بعد از بررسی اگر اطلاعات مربوط به سیستم D نباشد به C پاس داده شده و مجدداً بعد از بررسی به سیستم مقصد پاس داده می شود، پس از رسیدن اطلاعات به مقصد در داخلFrame token، ۰ به ۱ تبدیل شده و مجدداً در حلقه به گردش در می آید و به سمت سیستم ارسال کننده(A) حرکت می نماید و بعد از انتقال به A دیتا حذف و کامپیوتر A مطلع می شود که اطلاعات به کامپیوتر مورد نظر منتقل شده است.



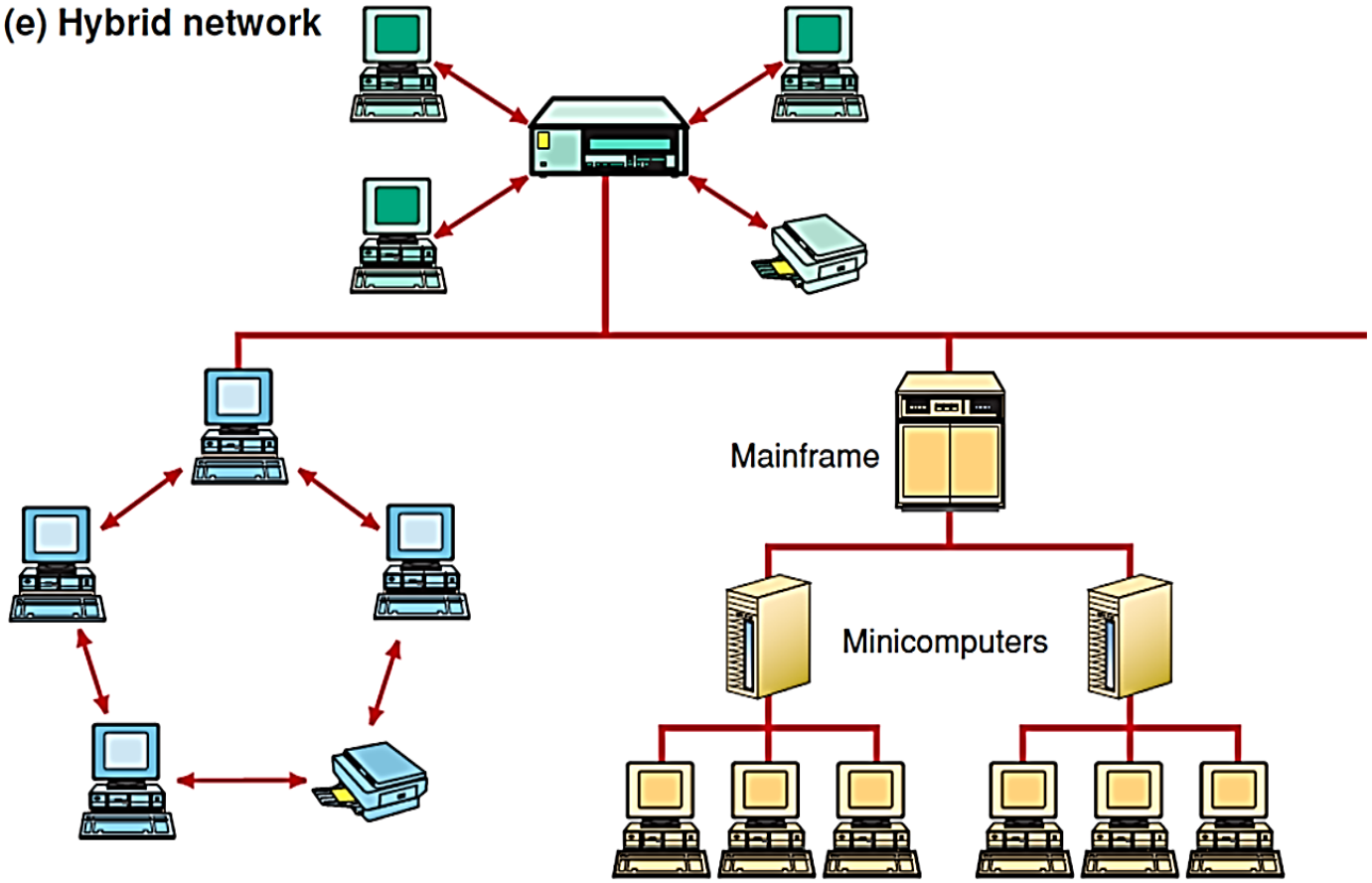
توپولوژی مشبک(Mesh)

در این توپولوژی تمامی سیستم ها بایکدیگر ارتباط مستقیم دارند مانند اینترنت و شکل ظاهری این توپولوژی را مانند یک تار عنکبوت می توان ترسیم کرد، در این آرایش شبکه، نظم مشخصی وجود ندارد و هر یک از رایانه‌ها به یک یا چند رایانه دیگر متصل شده‌اند. این آرایش در واقع نسخه ناقص آرایش اتصال کامل است، لذا هزینه و پیچیدگی کمتری نسبت به روش مذکور دارد.از معایب این توپولوژی میتوان به پیچیدگی و هزینهای بالای آن اشاره کرد و چون شبکه گسترده است عیب یابی آن هم نسبت سخت می‌باشد از مزایای این توپولوژی این است که اگر قسمتی از کابل قطع شود کل شبکه از کار نمی افتد و انتقال اطلاعات به صورت دوبه دو می‌باشد یعنی تمامی کامپیوترها بدون اینکه شبکه مشغول شود میتوانند به یک دیگر اطلاعات ارسال و دریافت کنند که برای اینکه از توژولوژی mesh بتوان از حداکثرنیرو استفاده کرد از دستگاهی به نام روتر یا مسیر یاب استفاده می‌شود که کار این دستگاه این است که باعث می‌شود از خط ها یا مسیر هایی که خالی هستند ارسال اطلاعات انجام داد و در نتیجه این دستگاه باعث سرعت بخشیدن به ارسال اطلاعات می شود.



توپولوژی Hybrid

تلفیقی از تمام توپولوژیهاست که قصد دارند با یکدیگر در ارتباط باشند مانند اینترنت. از همبندی یک یا چند شبکه با آرایش‌های فیزیکی متفاوت و یا همبندی چندین شبکه که دارای آرایش فیزیکی یکسان است بوجود می‌آید و آرایش فیزیکی شبکه حاصل مشابه آرایش فیزیکی شبکه‌های اولیه نمی‌باشد. این توپولوژی ترکیبی است از چند شبکه با توپولوژی متفاوت که توسط یک کابل اصلی بنام Backbone به یکدیگر مرتبط شده اند.توسط یک پل ارتباطی به نام Bridge به کابل backbone متصل می شود.



توپولوژی Tree

یک گره مرکزی (بالاترین سطح در سلسله مراتب) به دو یا چند گره در سطحی پایین تر با استفاده از یک پیوند نقطه به نقطه متصل است (به عنوان مثال در سطح دو) و گره‌های سطح دو نیز به چندین گره در سطحی پایینتر متصل هستند (برای مثال در سطح سوم). گره مرکزی تنها گرهی است که هیچ گرهی در سطحی بالاتر از خود ندارد. سلسله مراتب درخت متقارن است یعنی تعداد گره‌های متصل به هر گره در سطح پایین تر عدد ثابت f است. عدد f به عنوان عامل شاخه بندی در درخت سلسله مراتب شناخته می‌شود.

نکته ها:

۱) یک شبکه مبنی بر آرایش درختی فیزیکی حتماً باید حداقل سه سطح داشته باشد در غیر این صورت اگر دو سطح داشته باشد نشان دهنده آرایش ستاره است.

۲)اگر یک آرایش درختی عامل شاخه بندی برابر با یک داشته باشد این آرایش نشان دهنده آرایش خطی است.

۳)عامل شاخه بندی مستقل از تعداد کل گره هاست اگر یک گره نیاز به درگاه‌هایی برای اتصال به گره‌های دیگر داشته باشد می‌توان تعداد درگاه‌ها را بدون توجه به تعداد کل گره‌ها کاهش داد. در نتیجه تعداد درگاه‌های مورد نیاز وابسته به عامل شاخه بندی است و در نتیجه می‌توان تعداد درگاه‌ها را بدون توجه به تعداد کل گره‌ها کاهش داد.

۴)تعداد کل پیوندهای نقطه به نقطه در شبکه بر اساس آرایش درختی یکی کمتر از تعداد گره‌های شبکه می‌باشد

۵)اگر نیاز به پردازش اطلاعات توسط گره‌ها در یک آرایش درختی فیزیکی باشد گره‌های سطح بالاتر باید پردازش بیشتری نسبت به گره‌های سطح پایین تر انجام دهند

۶)برای تبدیل توپولوژی ستاره به درختی می توان برای استفاده از پورتهای بیشتر سوئیچ ها را توسط کابل به یکدیگر متصل کرد.

کابل Fiber Optic

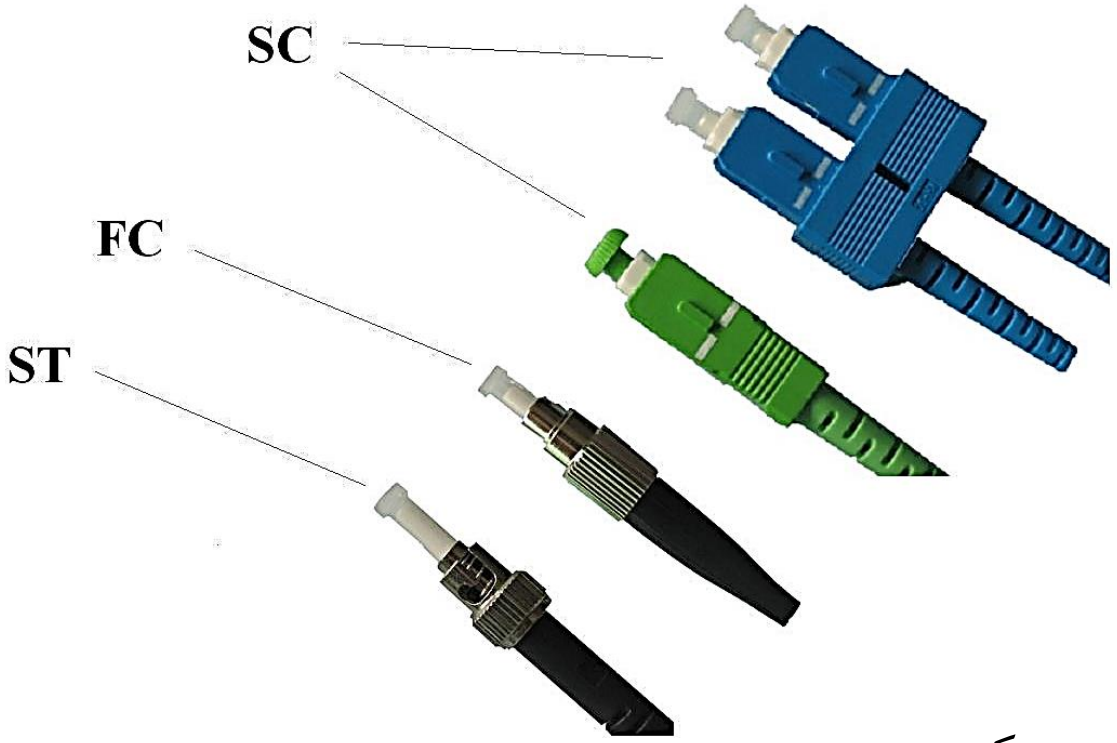
در کابل فیبر نوری از پالسهای نور (فوتونها) برای ارسال سیگنالهای باینری تولید شده توسط کامپیوترها استفاده می شود . ازآنجا که کابل فیبر نوری به جای الکتریسیته از نور استفاده می کند تقریباً هیچ یک از مشکلات ذاتی کابل مسی همچون تداخل الکترومغناطیسی ، مکالمه متقاطع و نیاز به زمین کردن را ندارد . علاوه بر این، تقلیل آن بسیار کمتر است ، و بنابراین کابلهای فیبر نوری را می توان در فواصل بسیار دورتری نسبت به کابل مسی گستراند ، گاهی تا ۱۲۰ کیلومتر .

کابل فیبر نوری برای استفاده در زیر ساختهای شبکه و به خصوص برای اتصالات بین ساختمانها ایده آل است . زیرا در مقابل رطوبت و سایر شرایط خارج ساختمان مقاوم است . فیبر نوری ذاتاً ایمن تر از کابل مسی هم هست ، زیرا مثل مس انرژی الکترومغناطیسی قابل تشخیص ساطع نمی کند ، و بر داشتن مخفیانه اطلاعات از آن تقریباً غیر ممکن است .

کابل فیبر نوری شامل یک هسته است که از شیشه یا پلاستیک ساخته می شود و یک روکش که هسته را در بر می گیرد وروی آن یک لایه حائل پلاستیکی یک لایه از فیبر به منظور محافظت و یک پوشش بیرونی از تفلون یا PVC قرار دارد . وقتی پالسهای نور در هسته حرکت می کنند توسط روکش به عقب و جلو انعکاس داده می شود . بدلیل این انعکاس است که می توان کابل را در گوشه ها خم کرد و سیگنالها می توانند بدون اینکه مسدود شوند به حرکت خود ادامه دهند .

- ✓ حداکثر سرعت تبادل اطلاعات $10^{Gb}/_{s}$ می باشد و بخاطر جنس کابل سرقت اطلاعات در این نوع کابل وجود ندارد.
- ✓ نویز تاثیر کمی بر روی کابل دارد و نور موجود در داخل کابل از نوع laser یا L.E.D می باشد.
- ✓ جوش دادن دو فیبر به یکدیگر را فیوژن می گویند و توسط دستگاههای مخصوص صورت می گیرد.

اتصال دهنده ای که بطور سنتی برای کابل های فیبر نوری به کار می رود اتصال دهند ST نام دارد . این اتصال دهنده یک اتصال دهنده خمره مانند است که ساختار قفل نیزه ای دارد اما اتصال دهنده جدیدی تحت عنوان SC نیز کم کم جای خود را باز کرده است .این اتصال دهنده بدنه ای مربع شکل دارد و با فشار دادن آن به داخل سوکت قفل می شود



SC	Subscriber Connector or Square Connector or Standard Connector
FC	Ferrule Connector or Fiber Channel
ST	Straight Tip

کابل فیبر نوری

Single mode: روی هسته فقط یک سیگنال نوری و تا ۷۰ کیلومترحرکت می کند .

Multi mode: روی هسته چندین سیگنال نوری و تا ۲ کیلومتر حرکت می کند .

مهمترین تفاوت آنها در ضخامت هسته و روکش است . فیبر تک حالته معمولاً ۱۲۵/۳/۸ میکرون است و فیبر چند حالته ۱۲۵/۵/۶۲ میکرون . این ارقام مربوط به ضخامت هسته و ضخامت کل روکش هسته هستند . سیگنالی که در کابل تک حالته منتقل شوند توسط یک لیزر تولید می شود و شامل فقط یک طول موج است . در حالی که سیگنالهای چند حالته توسط یک دیود منتشرکننده نور تولید می شوند و چند طول موج را منتقل می کنند

انتقال سیگنال

دو تکنینک انتقال سیگنالهای کد شده برروی کابل استفاده می شود:

- باند اصلی (Baseband)
- باند سریع (Broadband)

روش انتقال Baseband

سیستمهای Baseband برای انتقال اطلاعات برروی یک کانال منفرد از سیگنالهای دیجیتال استفاده میکنند. سیگنالها به شکل پالسهای متناوبی از الکتریسیته یا نور در کابل جریان پیدا میکنند. در این نوع انتقال اطلاعات ، کل پهنای باند کانال ارتباطی برای انتقال تنها یک سیگنال منفرد داده ای استفاده میشود. منظور از پهنای باند یک کابل، یا یک کانال ، انتقال اطلاعات ، اختلاف بین بیشترین و کمترین فرکانسهایی است که میتوانند برروی کابل حمل شوند.

در حین این که سیگنال طول کابل شبکه را طی میکند دامنه آن شروع به کاهش و اگر طول کابل زیاد، نتیجه سیگنالهایی خواهد بود که بسیار ضعیف شده یا به کلی از بین رفته است بعنوان یک حفاظ در سیستمهای Baseband معمولا از دستگاههای Repeater برای تقویت دامنه سیگنال استفاده میشود.

روش انتقال Broadband

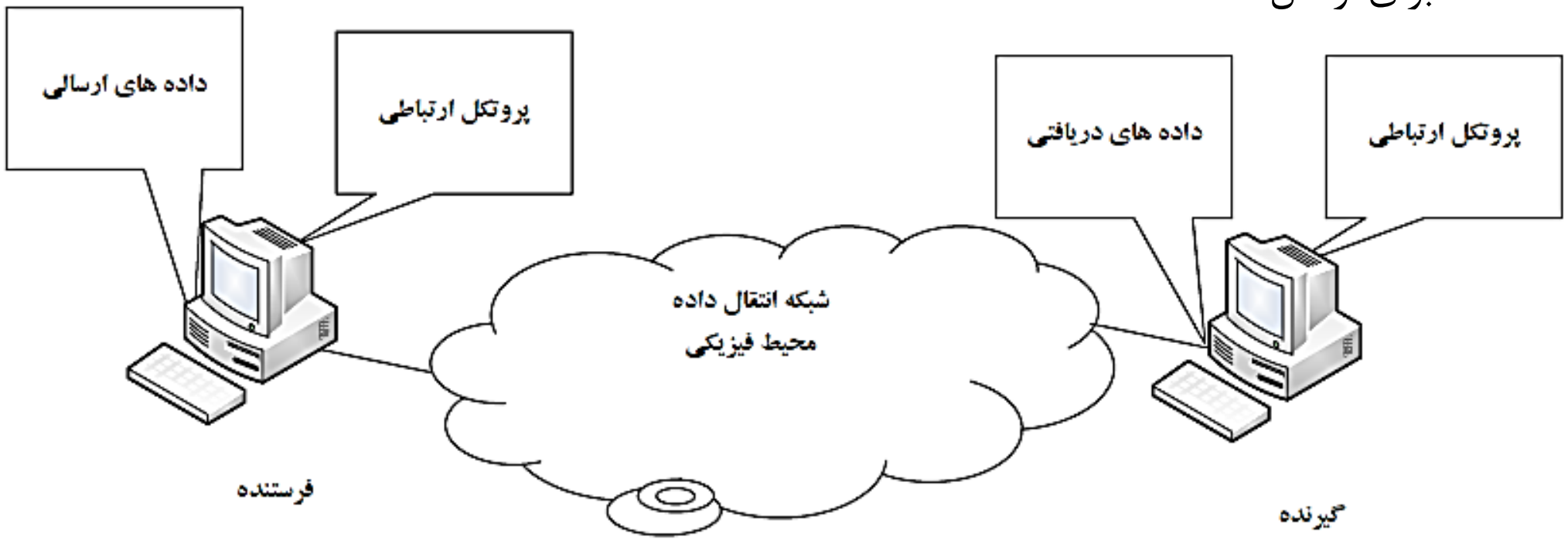
سیستمهای Broadband برای انتقال اطلاعات برروی کابل از سیگنالهای آنالوگ و یک بازه فرکانسی استفاده مینماید. در انتقال آنالوگ سیگنالها یکنواخت و پشت سر هم و دریک جهت برروی رسانه فیزیکی انتقال ، که همان کابل باشد به شکل امواج الکترومغناطیس یا نوری جریان پیدا میکنند. چنانچه پهنای باند کافی برروی رسانه فیزیکی فراهم باشد میتوان از چندین سیستم انتقال آنالوگ همانند تصاویر تلویزیون و داده های شبکه به طور همزمان برروی یک کابل استفاده کرد. درسیستمهای Baseband معمولا برای تقویت دامنه سیگنال از دستگاههای Repeater استفاده میشود که سیگنال گرفته شده در ورودی را در خروجی بازسازی میکند اما در سیستمهای broadband از دستگاههای آمپلی فایر (Amplifier) استفاده می شود که دامنه سیگنال آنالوگ را با مدارهای ترانزیستوری تقویت می کند

نرم افزار شبکه

اجزای اصلی شبکه های انتقال داده

هر سیستم انتقال داده از چهار قسمت اصلی تشکیل شده است که عبارتند از:

- – فرستنده و گیرنده
- – داده های ارسالی
- محیط فیزیکی برای تبادل داده ها
- – پروتکل استفاده شده برای ارسال داده ها



پروتکل

سیستم عامل شبکه از مجموعه کاملی از روش ها و قوانین مشخصی برای انجام هر کار پیروی می کند. این روش ها را پروتکل (Protocol) یا قانون رفتاری گویند. پروتکل ها راهنمای هر فعالیت برای انجام موفقیت آمیز آن هستند.

برای امکان ارتباط سخت افزارها و نرم افزارهای تولیدکنندگان مختلف به ایجاد پروتکل های استاندارد نیاز است. نظیر مدل OSI (Open Systems Interconnection)

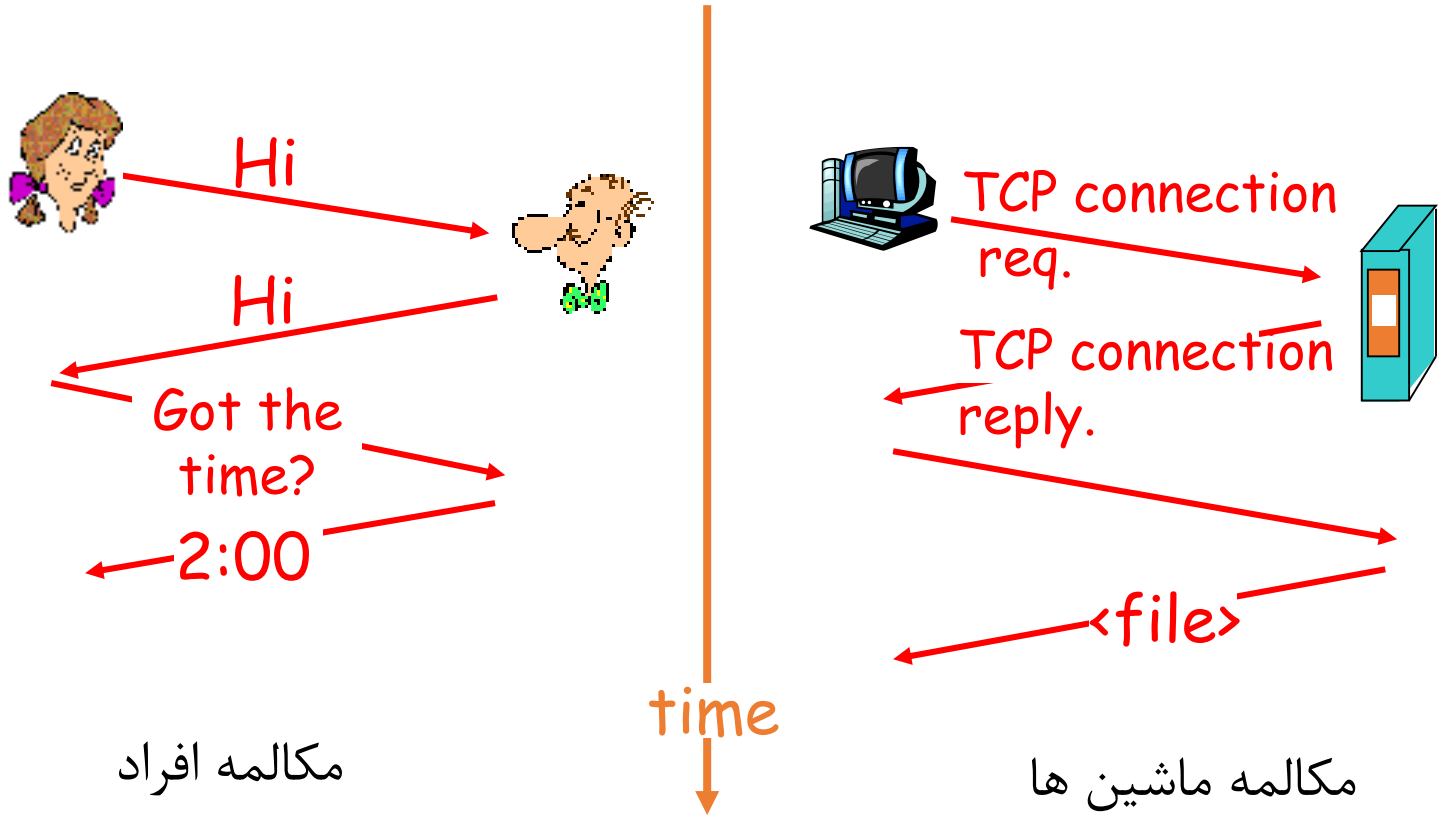
به زبان ساده برای اینکه دو دستگاه بتوانند با همدیگر ارتباط برقرار نمایند احتیاج به زبان واحدی می باشد که تحت آن هر دو دستگاه بتوانند با همدیگر به گفتگو و تبادل اطلاعات بپردازند که با آن پروتکل گویند. زمانی که سرویس‌گیرنده از طریق یک پورت خاص به سرویس‌دهنده وصل شد، می‌توانیم از طریق یک پروتکل به سرویس‌دهنده دسترسی داشته باشیم. پروتکل یک راه از پیش تعریف شده برای گفتگو با سرویس‌دهنده‌است. همچنین پروتکل‌ها متن ساده و قابل درک توسط انسان هستند.

چندین پروتکل می توانند با هم کار کنند که به عنوان پشته (Stack) یا رشته پروتکل ها شناخته می شوند.

پروتکل می گوید که چه چیزی مخابره می شود، چگونه مخابره می شود و چه زمانی مخابره می شود.

المان های کلیدی یک پروتکل عبارتند از: ساختار(syntax)، معنا(semantic) و زمان بندی(timing).

مقایسه پروتکل در ارتباط انسانها و کامپیوترها



در هر دو حال نیاز به مذاکره (hand shaking) بین طرفین برای شروع مکالمه است.

- ✓ برای انجام مذاکره نیاز به داشتن زبان مشترک بین طرفین است.
- ✓ علاوه بر زبان مشترک روال مذاکره نیز بصورت قواعدی باید تعریف شود.
- ✓ TCP یکی از پروتکلهای مورد استفاده در برقراری ارتباط است.

معماری و عملکرد لایه ای

برای برقراری ارتباط مطمئن بین دو پروسه کاربردی، مولفه های سخت افزاری و نرم افزاری زیادی در گیر هستند و وسعت کـار بحـدی زیاد است که باعث می شود امکان قرار دادن آنها در یک قالب ماژول واحد و مستقل میسر نباشـد و بایـد آنهـا را در قالـب چنـدین زیـر سیستم طراحی کرد.

به همین دلیل با توجه به گستره مولفه هایی که پیکره ی یک شبکه کامپیوتری را تشکیل می دهند . معماری یک شبکه کامپیوتری به صورت لایه ای طراحی می شود.

وظیفه هر لایه ارائه سرویسهای خاص به لایه های بالاتر است. این سرویسها فارغ از نوع پیاده سازی و با پنهان نگاه داشـتن جزئیـات آن به لایه بالاتر ارائه می گردد.

مسائلی که در شبکه باید به آنها پرداخت

۱. اولین مساله چگونگی ارسال و دریافت بیتهای داده است

- سیگنال الکتریکی بر روی سیم مسی
- الکترومغناطیسی بر روی کانالهای ماهواره ای
- نوری بر روی فیبر نوری

۲. دومین مساله اهمیت انتقال است: ارتباط بین دو موجودیت را می توان بین سه رده تقسیم بندی کرد:

- Simplex ارتباط یک طرفه (یک طرف همیشه فرستنده طرف دیگر گیرنده)
- Half Duplex ارتباط دو طرفه غیر همزمان (هر دو فرستنده و گیرنده ولی یکی ارسال کننده و دیگری سکوت می کند)
- Full Duplex ارتباط دو طرفه همزمان

۳. مساله سوم وجود خطا و نویز بر روی کانال مخابراتی است. بدین معنا که در حین ارسال اطلاعات بر روی کانال فیزیکی ممکن است بیت ها خراب شود و غیر قابل تشخیص گردد. برای اجتناب از چنین وضعیتی بسته های فاقد اعتبار، دور ریخته شود و مبدا با تشخیص چنین رخدادی آنها را از نو ارسال می کند.

۴. با توجه به آنکه در زیر ساخت شبکه مسیر های مختلفی بین مبداء و مقصد وجود دارد بنابراین پیدا کردن بهترین مسیر و هدایت بسته ها از طریق آن مسیر از مسائل طراحی شبکه می باشد همچنین پیامهای بزرگ ممکن است کوچک شده و از مسیر های متنوعی به مقصد برسد دریافت و بازسازی پیام از وظایف به شمار می آید.

۵. هماهنگی سرعت بین مبداء و مقصدکه این موضوع با عنوان " کنترل جریان" Flow Control مورد بحث قرار می گیرد.

۶. چون ماشینهای فرستنده و گیرنده متعددی در شبکه وجود دارد، مسائلی مثل ازدحام ، تداخل ، تصادم در شبکه بوجود می آید که این مشکلات در سخت افزار و نرم افزار باید حل شود.

۷. توزیع داده بین پروسه های اجرا شده بر روی یک ماشین واحد، تضمین امنیت داده های در حال جریان، مدیریت نشستها بین دو پروسه از مسائلی هستند که در سطح نرم افزار صورت می گیرند.

سه مفهوم مهم شبکه: لایه، معماری و آدرس

لایه: به منظور تکفیک عملیات لازم برای انتقال داده تعدادی لایه در یک سیستم شبکه تعریف می شوند که هر لایه وظیفه خاصی را برای انتقال داده به عهده دارد و مجموعه لایه ها با کمک یکدیگر عمل انتقال داده به صورت صحیح را تضمین می کنند.

معماری شبکه: به مجموعه لایه ها و پروتکل های پیاده سازی شده در هر لایه معماری شبکه می گویند.

آدرس: یک پیغام دارای قسمت هایی مانند آدرس کامپیوتر مبدا، آدرس کامپیوتر مقصد، داده و دیگر قسمت های کنترلی است.

اصول طراحی لایه ای

- ✓ هر لایه وظیفه مشخصی دارد
- ✓ هر گاه سرویسهایی که باید ارائه شوند از نظر ماهیت متفاوت باشند، باید لایه به لایه و جداگانه طراحی شود.
- ✓ هر لایه با توجه به قراردادها و استانداردهای جهانی مشخص شود.
- ✓ تعداد لایه ها نباید آنقدر زیاد باشدکه تمایز لایه ها از دیدگاه سرویسهای ارائه شده نامشخص باشد و آنقدر کم باشد که وظایف و خدمات لایه ها پیچیده و نامشخص گردد.
- ✓ در هر لایه جزئیات لایه زیرین نادیده گرفته می شود و لایه های بالایی از یک روال ساده و ماژولار از خدمات لایه زیرین خود استفاده نماید
- ✓ باید مرزهای بین هر لایه به گونه ای انتخاب شود که جریان اطلاعات بین لایه ها حداقل باشد.

لایه های همتا Peer

در صورتیکه تمام ماشینها از مدل لایه ای استفاده کنند و تمام لایه های مورد نیاز خود را یکسان پیاده سازی کنند و دو ماشین A و B بخواهند با یکدیگر ارتباط برقرار کنند لایه nام از ماشین A با لایه nام از ماشین B لایه همتا هستند. لایه های همتا بر روی ماشین در حال تعامل هستند . به عبارت دیگر هر پردازشی که در لایه nام صورت می گیرد در لایه nام ماشین دیگر قابل درک است .

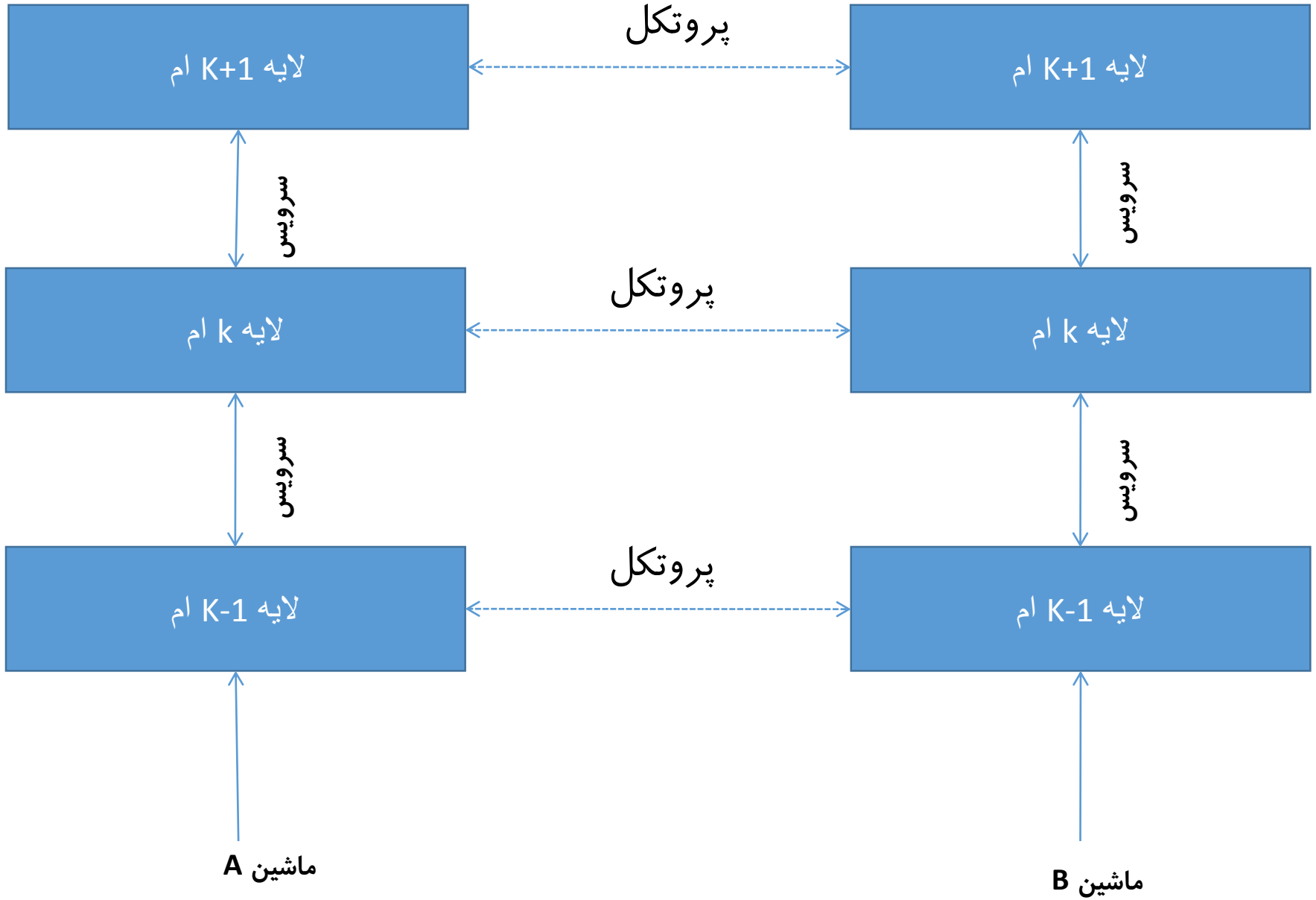
Service

مجموعه کارهایی که یک لایه برای لایه بالاتر از خود انجام می دهد سرویس گفته می شود.

سرویس فقط می گوید که یک لایه چه خدمات و کارهائی را برای کاربر خود انجام میدهد ولی هیچ چیز در خصوص چگونگی آن نمی گوید.

سرویس در واقع بین دو لایه مجاور تعریف می شود لایه پائینی لایه (k-1) ارائه دهنده سرویس و لایه بالایی لایه (k) مصرف کننده آن سرویس است.

سرویس و پروتکل



عملیات پایه

تعریف یک : سرویسهایی که یک لایه به لایه بالاتر خود ارائه می نماید در قالب تعدادی از عملیات پایه یا Primitivesتوصیف می شود .

تعریف دو: در حقیقت عملیات پایه به مثابه توابع سیستمی هستند که لایه بالاتر برای سرویس گرفتن از لایه های زیرین آنها را فراخوانی می کند. حتی اگر لایه پائین تر در سطح سخت افزار طراحی شده باشد باز هم فراخوانی سرویسها و ماژولهای سخت افزاری عملیات پایه را توصیف می کند.

Interface (واسط)

مجموعه عملیات پایه که در یک لایه در جریان است به واسط یا اینترفیس آن لایه شهرت دارد

هرآنچه یک لایه در اختیار لایه بالاتر خود قرار دهد در قالب یک واسط شسته و رفته توصیف می شود. این واسط باید بیشترین شفافیت ، کمترین پیچیدگی و جامع ترین شکل ممکن را داشته باشد.

پشته پروتکلی

به کلیه پروتکلهای تعریف شده در لایه های یک شبکه کامپیوتری که عملکرد صحیح شبکه را تضمین می کند اصطلاحا پشته پروتکلی گفته می شود

PDU(Protocol Data Unit)

"در معماری لایه ای شبکه، یک قطعه داده از لایه K+1 تحویل لایه kام می گردد"

به قطعه داده ای که در هر لایه پس از پردازشهای لازم در قالب یک ساختمان داده استاندارد و مشخص سازمان دهی شده و تحویل لایه زیرین می شود به طور عام و انتزاعی PDU گفته می شود.

در بسیاری از موارد به جای استفاده از واژه PDU از واژه Packet استفاده می شود در صورتیکه این واژه اسم خاص واحد اطلاعاتی تشکیل شده در لایه شبکه از مدل مرجع OSI است.

کپسوله سازی اطلاعات

هر لایه پس از دریافت قطعه داده از لایه فوقانی آنرا در قالب یک PDU سازماندهی و تحویل لایه زیرین می دهد. تشکیل PDU مستلزم اضافه کردن چند فیلد اطلاعاتی به ابتدای و گاهی به انتهای داده است با افزوده شدن این فیلدها قطعه داده دارای هویت شده و لایه همتا در ماشین گیرنده قادر به درک آن است. این فرآیند اصطلاحا کپسوله سازی اطلاعات گفته می شود.

بسته (Packet)

به یک قطعه اطلاعات دارای هویت و شناسنامه که در ماشین مبداء سازماندهی شده و توسط زیر ساخت شبکه هدایت و تحویل می شود اصطلاحا بسته گفته می شود. هرگاه اندازه بسته کوچک و ثابت باشد به آن سلول نیز گفته می شود.

Header & Trailer

به مجموعه اطلاعاتی که به ابتدای فیک واحد اطلاعاتی افزوده می شود اصطلاحا سرآیند و به اطلاعاتی که به انتهای آن افزوده می شود پی آیند اطلاق می شود سرآیندو پی آیند دارای الگوی استاندارد شده ای هستند و در توصیف پروتکل هر لایه مشخص می شوند.

SAP

از آنجا که یک موجودیت در لایه K ممکن است به چندین موجودیت در لایه K+1 سرویس دهد لذا این موجودیتها در لایه K+1 باید شناسایی و دارای هویت شوند طبعا این موجودیتها دارای ادرس یکتا هستند به این آدرس اصطلاحا آدرس SAP گفته می شود مثل شماره PORT.

معماری پروتکلها در شبکه های کامپیوتری

معماری پشته پروتکلهای شبکه بر پایه مدل لایه ای است:

_مجموعه ای از لایه ها بصورت پشته ای.

_وظایف هر لایه توسط یک پروسه انجام می گیرد. هر پروسه با شماره لایه مربوط تعریف می شود.

_هر دو پروسه هم سطح در دو سوی یک ارتباط بر اساس پروتکل تعریف شده با هم محاوره دارند.

_پروتکل فرمت و نحوه پردازش اطلاعات تبادل شده بین دو پروسه هم سطح را تعریف می کند.

هر entity پیاده سازی یکی از لایه هاست .
در مدل لایه ای هر لایه 3 نوع interface دارد :
Interface با لایه بالا
Interface با لایه پایین
Interface با لایه هم سطح خودش در طرف مقابل

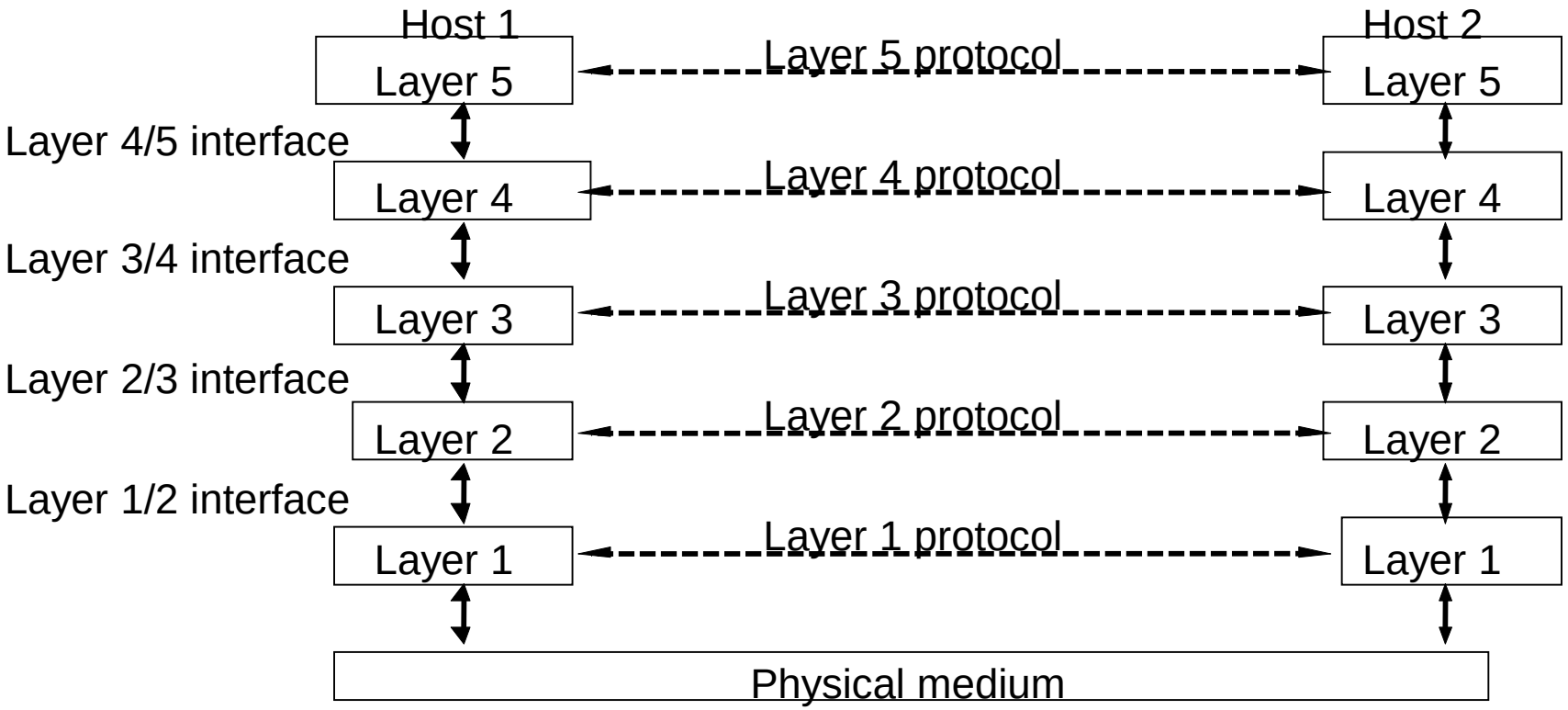
مفهوم پشته از آنجا می آید که پروتکل های مربوط به هر لایه را بصورت پشته روی یکدیگر می چینیم تا با عبور از لایه های مختلف شبکه، در هر لایه، پروتکل مناسب و خاص همان لایه اجرا شود.

مدل لایه ای

هر لایه به لایه بالای خود سرویس می دهد و از لایه پایین سرویس می گیرد.

بین هر دو لایه یک رابط سرویس (Service Interface) تعریف می شود.

ارتباط بین پروسه های هم سطح از دید لایه های پایین شفاف است.



ارتباط دو عنصر هم تراز در دو طرف به صورت peer-to-peer است . اطلاعاتی را که می خواهیم بوسیله عنصر هم سطح در سمت دیگر پردازش شود در Header قرار می دهیم .
ارتباط به لایه های بالا و پایین در Header تعریف نمی شود بلکه توسط توابع نرم افزاری و service interface اینکار صورت می گیرد.

از دید هر لایه ارتباط مستقیم بین آن لایه در دو طرف ارتباط وجود دارد و از وجود لایه های زیرین بی اطلاع است.

مدل مرجع Reference Model

مدل مرجع عبارتست از یک توصیف انتزاعی معماری لایه ای شامل توصیف تعداد ، حدود لایه ها و خدمات و عملیاتی پایه در هر لایه و توصیف دقیق مفهوم خدمات بدون آنکه به مقوله پیاده سازی آنها بپردازد.

مدلهای مرجع معروف:

1. OSI
2. AppleTalk
3. TCP/IP
4. IPX
5. SNA
6. DECNet

مدل مرجع OSI

با گسترش شبکه ها و برپایی شبکه هایی با سخت افزار و نرم افزارهای متفاوت نوعی ناسازگاری بـرای ارتبـاط و انتقـال داده بین شبکه های مختلف ایجاد شد.

برای حل این مشکل سازمان ISO مدلی را به نام OSI ایجاد کرد تا از نظر ارتباط و سازگاری بین شبکه های مختلف مشکلی پیش نیاید.

یک سیستم باز مجموعه ای از پروتکل ها است که دو سیستم متفاوت را قادر می سازد تا علیرغم تفاوت موجود در تکنولوژی های زیربنایی آنها با یکدیگر به مخابره داده بپردازند.

مدل OSI وظایف و توابع شبکه را که در هر لایه انجام می شود مشخص می کند. در این مدل هفت لایه مختلف بـا وظـایف متفاوت وجود دارد.

جداسازی وظایف و توابع شبکه را لایه سازی Layering می نامند.

تقسیم وظایف شبکه به لایه ها مزایای زیر را دارد:

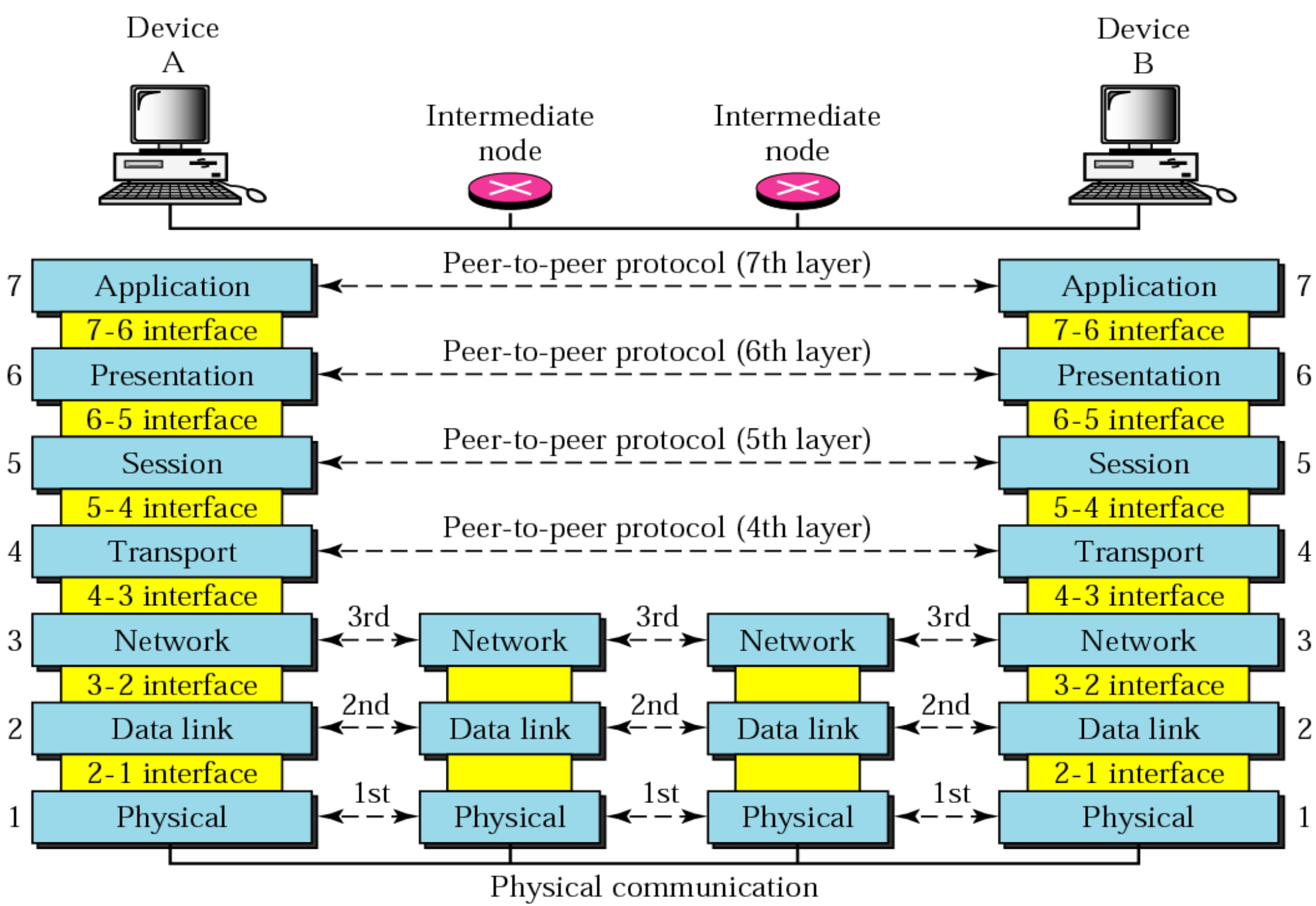
۱- یک شبکه ارتباطی به اجزا کوچک تر و ساده تر تقسیم می شود.

۲- تغییرات در هر لایه بر دیگر لایه ها تاثیر نمی گذارد بنابراین سرعت خطایابی افزایش می یابد.

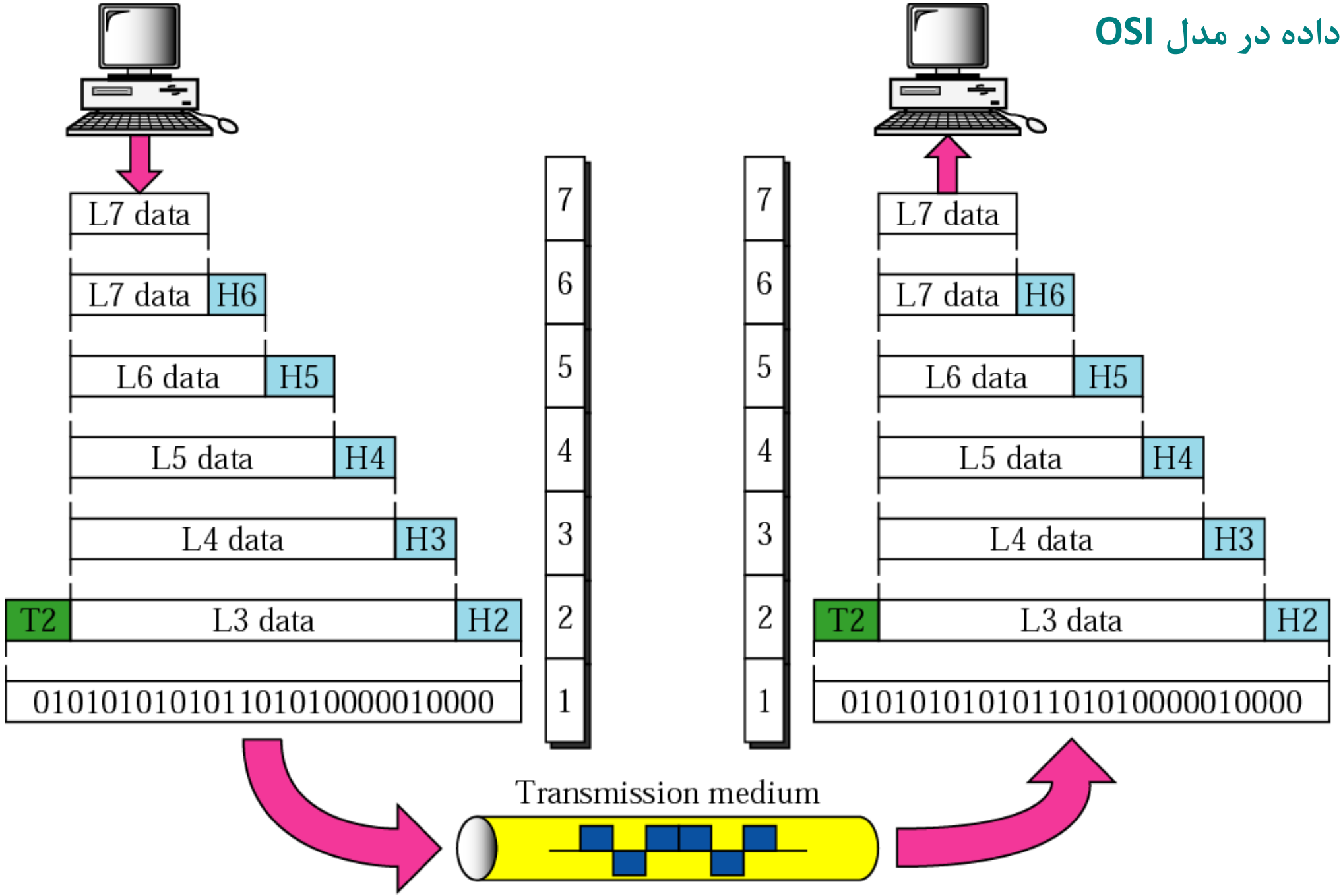
۳- با تقسیم یک شبکه به اجزا کوچک تر فهم آن ساده تر می شود.

هر رابط مشخص می کند یک لایه چه اطلاعات و سرویس هایی را باید به لایه بالاتر از خود بدهد.

پروسه ای در هر ماشین در سطح یک لایه با پروسه نظیر خود در ماشین دیگر داده ای را رد و بدل می کند به این دو پروسه پروسه های نظیر به نظیر می گویند.


Device A
Device B
Intermediate node
Intermediate node
Peer-to-peer protocol (7th layer)
Peer-to-peer protocol (6th layer)
Peer-to-peer protocol (5th layer)
Peer-to-peer protocol (4th layer)
7 Application
7-6 interface
6 Presentation
6-5 interface
5 Session
5-4 interface
4 Transport
4-3 interface
3 Network
3-2 interface
2 Data link
2-1 interface
1 Physical
3rd
2nd
1st
Physical communication

تبادل داده در مدل OSI



هدرها در لایه های ۲و۳و۴و۵و۶ به داده ها اضافه می شوند دنباله ها Trailer فقط در لایه دوم اضافه می شوند.

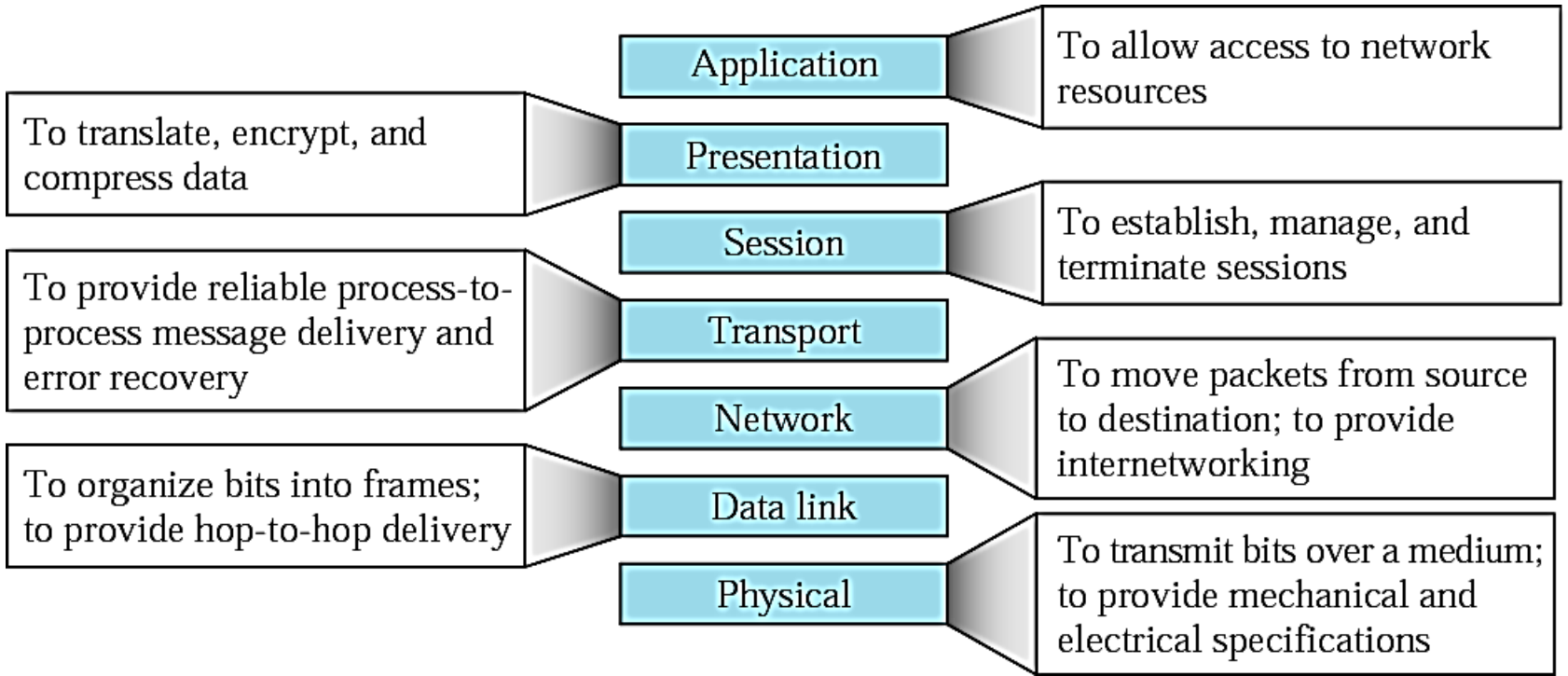
بخش داده یک بسته در لایه، کل داده دریافتی از لایه بالاتر که شامل اطلاعات و هدرها و دنباله های اضافه شده بـه آن مـی باشـد را در برمی گیرد. به این عمل کپسوله بندی می گویند.

در مدل OSI هر لایه به لایه بالاتر خود سرویس می دهد و از لایه پایین تر سرویس می گیرد.

هر لایه جزئیات و اتفاقات لایه پایین تر را از دید لایه بالاتر مخفی می کند.

در هنگام انتقال داده بین هر دو لایه متناظر یک ارتباط نظیر به نظیر ایجاد می شود و پروتکل هـای موجـود در لایـه هـای متنـاظر بـه انتقال داده می پردازند. این داده ها به نام PDU واحد داده پروتکل نامیده می شوند.

PDUدرلایه های ۵،۶،۷ پیغام نـام دارد و در لایـه انتقـال قطعـه segment و در لایـه سـوم بسـته packet و در لایـه دوم قـاب یـا فریم Frame نامیده می شود.



مبانی برنامه‌سازی سوکت

در شبکه های کامپیو تری ، برنامه های متعددی در یک زمان با یکدیگر مرتبط می گردند.

زمانیکه چندین برنامه بر روی یک کامپیوتر فعال می گردند پروتکل TCP/IP می بایست از روشی به منظور تمایز یک برنامه از برنامه دیگر استفاده نماید بدین منظور از سوکت برای مشخص نمودن یک برنامه خاص استفاده می گردد.

سوکت Socket چیست

با یک بیان ساده می توان گفت که سوکت به ترکیب یک آدرس ماشین (IP) و یک شماره درگاه (Port) گفته می شود.

در برقراری ارتباط بین کامپیوتر ها در یک شبکه دو چیز بسیار مهم است:

۱) آدرس ماشینی که می خواهیم اطلاعاتی از ان بگیریم یا به آن ارسال کنیم.

۲) برنامه ای از آن ماشین که در خواست اطلاعات کرده یا اینکه می خواهیم اطلاعاتی از آن برنامه کسب کنیم.

این دو یعنی آدرس ماشین و شماره برنامه به وسیله سوکت در شبکه مشخص می شوند.

برکلی سوکت

TCP/IP برای اولین بار درسیستم عامل یونیکس معرفی شد و در نگارش های بعدی این سیستم عامل که توسط دانشگاه برکلی توسعه پیدا کرد ، یک رویه برنامه نویسی نیز همراه TCP/IP ارائه شد تا کاربران بتوانند به وسیله آن برنامه های تحت شبکه با استفاده از این پشته پروتکلی ایجاد کنند. این رویه برنامه نویسی به صورت استاندارد برای برنامه نویسی شبکه درآمد و بقیه زبان های توسعه و سیستم عامل نیز از این استاندارد برای پشتیبانی از برنامه نویسی شبکه استفاده کردند.

WinSock

WinSock یا Windows Socket یک رویه (InterFace) برنامه نویسی است که در قالب یک DLL (Dynamic Link Library) در سیستم عامل ویندوز برای برنامه نویسی شبکه و ساخت برنامه هایی که بتوانند با شبکه محاوره داشته باشند معرفی شده است

خدماتی که یک لایه به لایه بالاتر می دهد ممکن است به یکی از گونه های زیر باشد:

- ❖ درخواست سرویس (Request)
- ❖ اقدام لازم برای انجام سرویس (Introduction)
- ❖ ارسال پاسخ سرویس (Response)
- ❖ قبول درخواست (Confirm)

انواع ارتباط لایه های متناظر دو کامپیوتر

ارتباط مابین دو کامپیوتر می تواند به یکی از دو صورت زیر باشد:

- ❖ اتصال گرا (Connection Oriented)
- ❖ غیر اتصال گرا (Connection Less)

در سیستم **اتصال گرا** ابتدا درخواست اتصال ارسال شده و در صورت موافقت طرف مقابل ارتباط برقرار می شود (مثل چیزی که در سیستم تلفن وجود دارد) به این سیستم Data Stream نیز گفته می شود.

اما در سیستم **غیر اتصال گرا** بدون نیاز به موافقت طرف مقابل بسته ها ارسال می شوند (مانند سیستم پست) به این سیستم Data Gram می گویند.

TCP و UDP

در پشته پروتکلی TCP/IP دو نوع ارتباط می توان با کامپیوتر راه‌دور ایجاد کرد:

- ❖ اتصال به کامپیوتر راه دور به وسیله سوکت Data Stream
- ❖ اتصال به کامپیوتر راه دور بدون نیاز به سوکت Data Gram

به بیان غیر رسمی به نوع ارتباط اول (اتصال گرا) ارتباط از نوع TCP گویند و اگر نوع برقرای ارتباط به حالت Data Gram (غیر اتصال گرا) باشد به آن UDP گویند.

کاربرد حالت اتصال گرا در مواقعی است که نیاز به برقراری یک ارتباط امن بین دو ماشین فرستنده و گیرنده داشته باشیم یعنی از صحت دریافت اطلاعات در ماشین گیرنده مطمئن شویم.

اما حالت غیر اتصال گرا (UDP) مواقعی استفاده می شود که خیلی دریافت اطلاعات توسط ماشین گیرنده اهمیتی نداشته باشد.

در زیر انواع ارتباط بین لایه های دو ماشین را می بینید:

- Connection Oriented (Data Stream)
  - Ack (reliable)
    - Message Stream
    - Byte Stream
  - Not Ack (unreliable)
- Connection Less (Data Gram)
  - Ack (reliable)
  - Not Ack (unrilabel)
  - Request & Reply

کیفیت سرویس دهی یک شبکه Quality of service

سرویس که یک شبکه ارائه می دهد باید دارای یک کیفیت خوب و قابل قبول باشد. از لحاظ کیفیت ارائه سرویس شبکه ها دو نوع می باشند:

- کاربر قبل از استفاده از شبکه در مورد کیفیت با شبکه توافق می کند.
- شبکه هیچ تضمینی در مورد کیفیت نکرده ولی سعی می کند حداکثر کیفیت را ارائه دهد.

پارامترهای ارزیابی کیفیت سرویس

۱. مدت زمان ایجاد ارتباط (Connection Establishment).
۲. احتمال قطع ارتباط (Connection Establishment Failure Probability)
۳. پهنای باند عملی قابل استفاده کاربر (Through Put).
۴. زمان انتقال داده (Transit Delay) .
۵. نرخ خطا (Error Ratio) .
۶. امنیت (Security) .
۷. اولویت بندی (Priority) .

مدل هفت لایه OSI

- وقتی مباز به سطوح مختلفی از انتزاع است ، لایه ای باید ایجاد شود.
- هر لایه باید وظیفه مشخص داشته باشد.
- وظیفه هر لایه باید با در نظر گرفتن قراردادهای استاندارد جهاتی انتخاب شود.
- مرزهای لایه باید برای به حداقل رساندن جریان اطلاعات از طریق واسط ها انتخاب شوند.
- تعداد لایه ها باید آنقدر باشد که نیازی به قراردادن وظایف متمایز در یک لایه نباشد.

در ادامه هر لایه از مدل را به نوبت ، با شروع از لایه پایین مورد بحث قرار می دهیم. توجه داشته باشید که خود مدل OSI یک معماری شبکه نیست زیرا خدمات و قراردادهایی را که باید در هر لایه مورد استفاده قرار گیرد را مشخص نمی کند. فقط مشخص می کند که هر لایه چه عملی باید انجام دهد. ISO استاندارد هایی برای تمام لایه ها نیز تولید کرده است، گر چه این ها بخشی از خود مدل مرجع نیستند. هر کدام به عنوان استانداد جهانی منتشر شده اند.

لایه فیزیکی Physical

لایه فیزیکی به انتقال بیت های خام بروی کانال ارتباطی مربوط می شود. اصول طراحی حکم می کند که وقتی بیت ۱ از یک طرف ارسال می شود، در طرف دیگر بیت ۱ دریافت شود، نه بیت صفر. سوال های خاصی که مطرح می شوند عبارتند از : برای نمایش، یک و صفر به چه ولتاژی نیاز است، هر بیت چند نانو ثانیه دوام دارد، آیا انتقال در هر دو جهت به صورت همزمان صورت گیرد، اتصال اولیه چگونه برقرار می شود، وقتی ارتباط دو طرفه قطع شود، اتصال چگونه خاتمه یابد، و واسط شبکه چند پایه دارد و هر پایه به چه منظوری مورد استفاده قرار می گیرد.

در اینجا مدل طراحی با واسط مکانیکی،الکتریکی، و واسط های زمانی و رسانه انتقال فیزیکی که در زیر لایه فیزیکی قرار دارند، سرو کار دارد.

لایه پیوند داده ها Data link

وظیفه اصلی لایه پیوند داده ها این است که با امکانات انتقال اطلاعات خام، خطی را از دید لایه فیزیکی، به خط بدون خطا تبدیل کند. این کار را با شکستن داده های ورودی به قاب های داده (Data Frame) – معمولا به اندازه چند صد بایت یا چند هزار بایت– انتقال ترتیبی قاب ها، و پردازش قاب ها و اعلام وصول قاب هایی که از طرف گیرنده ارسال می شود، انجام می دهد.

مسئله دیگری که در لایه پیوند داده ها وجود دارد، چگونگی حفظ یک فرستنده سریع در دام یگ ماشین گیرنده کند است. برای اینکه انتقال دهنده بداند که گیزنده در آن واحد چه میزان از فضای بافر را در اختیار دارد، باید از راهکار تنظیم ترافیک استفاده شود. غالبا تنظیم ترافیک و پردازش خطا مجتمع می شوند.

شبکه های پخشی مسئله دیگری در لایه پیوند داده ها دارند : چگونگی کنترل دستیابی به کنال مشترک. یعنی اینکه چگونه چندین ماشین که در یک شبکه قرار دارند بتوانند برای ارسال و در یافت از یک کابل مشترک استفاده کنند.

زیر لایه خاصی از لایه پیوند داده ها، به نام زیر لایه کنترل دستیابی به رسانه (MAC) با این مسئله سرو کار دارد.

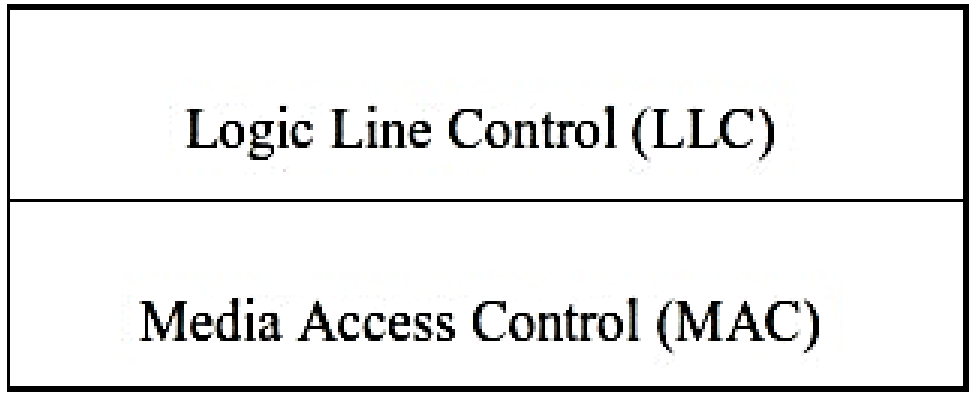
نگاهی دقیق تر به لایه پیوند داده ها و معرفی الگوریتم های مورد استفاده در آن

لایه پیوند داد ها از دو زیر لایه تشکیل شده است (شکل زیر).

این دو زیر لایه از پایین به بالا MAC و LLC نام دارند. در این حالت LLC با لایه Network در ارتباط است و MAC با لایه فیزیکی.

LLC لایه شبکه را قادر می سازد با انواع سرعتها، کابلها و تپولوژی های کار کند.

کار اصلی زیرلایه MAC کنترل دستیابی به لایه فیزیکی است.



نمایش ساختار داخلی لایه پیوند دادها

زیر لایه LLC

وقتی اطلاعات بر روی رسانه ارسال می شود باید با به کار گیری روش هایی مانع از برخورد و ادغام دو بسته اطلاعاتی با هم شویم. یعنی اینکه اگر یک بسته بزرگ به ۱۰ بسته کوچک ۱۰۰ بایتی شکسته شود و این ۱۰ بسته را به ترتیب برای ماشین گیرنده ارسال کنیم کامپیوتر گیرنده با روشی متوجه ابتدا و انتهای بسته اول شود و بسته دوم را نیز تشخیص دهد چون همان طور که می دانید هنگام ارسال اطلاعات روی خط چیزی جز صفر و یک بر روی کابل یا رسانه ارتباطی نیست و باید با روشی ابتدا و انتهای بسته ها برای کامپیوتر راه دور مشخص شود. به کار بستن این مکانیزم ها بر عهده زیر لایه LLC از لایه پیوند داده ها می باشد.

روش های ممانعت از ادغام بسته ها در زیر لایه LLC

- *Character Count.*
- *Starting & Ending Characters , With Character Stuffing.*
- *Starting & Ending Flags , with bit Stuffing.*
- *Physical Coding violation.*

روش اول Character Count

در این روش در اولین بایت یک فریم تعداد بایتهای آن فریم را تععین می کنیم به عنوان مثال اولین بایت فریم زیر مشخص می کند که چهار بایت بعد نیز مربوط به همین فریم است (شکل ۳-۱):

نمایش عملکرد تکنیک Character Count

به این بایت اصطلاحا Character Count می گویند.

ضعف این روش این است که اگر بایت اول آسیب ببیند تا انتهای عمل ارسال تمام اطلاعات به درستی دریافت نمی شوند. و تنها حسن آن هم سادگی روش است.

روش دوم Starting & Ending Characters, with Character Stuffing

در این روش ابتدا و انتهای هر فریم یکسری نشانه اضافه می کنیم یعنی ابتدا و انتها را با چند بایت خاص مش خص می کنیم

DLE برای نشانه گزاری ، STX شروع فریم ، ETX انتهای فریم

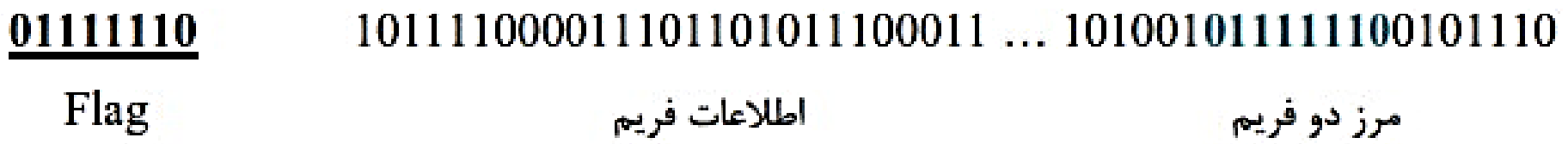
DLE	ETX						DLE	STX

هر گاه که الگوی نشانه گزاری در خود داده های موجود در فریم نیز وجود داشته باشد، باعث ایجاد اختلال در تشخیص ابتدا و انتهای بسته می شود برای حل این مشکل در فرستنده هر گاه الگوی نشانه وجود داشت این الگو را در بدنه دوبار تکرار می شود و در گیرنده اگر دو بار پشت سر هم الگوی نشانه دریافت شود گیرنده متوجه می شود که این جزئی از خود اطلاعات بسته است در نتیجه یکی از آنها را دور ریخته و دیگری را در بسته قرار می دهد.

ایراد این روش در این است که برای مشخص کردن ابتدا و انتهای فریم حداقل به چهار بایت نیاز داریم که این خود باعث به هدر رفتن بخشی از فضای بسته ارسالی می شود.

روش سوم Starting & Ending Flags, with Bit Stuffing

برای مشخص کردن ابتدا و انتهای فریم از یک Flag (پرچم) یک بایتی استفاده می کنند. از لحاظ کارایی با روش Starting & Ending Characters , With Character Stuffing تفاوتی ندارد اما سربار (Over Head) آن کمتر می باشد



ضعف این روش در این است که با تغییر یک بیت ممکن است الگوی flag تغییر کند و کل اطلاعات ارسالی اشتباه دریافت شوند.

روش چهارم Physical coding Violation

در زمان های خاص لبه پایین رونده (قسمتی از شکل موج کلاک سیستم که از بالا به پایین افت ولتاژ می کند) به عنوان یک و لبه بالا رونده به عنوان صفر تلقی خواهد شد. برای مشخص کردن ابتدا و انتهای فریم ها از حالاتی که در کد کردن معنایی ندارد استفاده می شود. یعنی اگر در زمان های مورد نظر تغییر نداشته باشد نه صفر است و نه یک و به این حالت Violation گفته می شود.

اگر به اندازه دو یا سه فریم تغییری در موج نباشد، فرض خواهد شد که پایان فریم است.

این روش بسیار مناسب می باشد و توسط لایه فیزیکی نیز به راحتی قابل اجراست.

معمولا در کاربرد های عملی ترکیبی از روش های گفته شده استفاده می شود (به طور معمول ترکیب روش های ۱ و ۳ و یا ۱ و ۴).

روش های کشف و اصلاح خطا در زیر لایه LLC

در این قسمت الگوریتم ها وشیوه های مختلف تشخیص و اصلاح خطا در یک مجموعه از بیت ها را بررسی میکنیم.

خطا معمولا ناشی از تبدیل یک مقدار در حین انتقال به یک مقدار دیگر است، مثلا تبدیل صفر به یک و یا بلعکس. در شبکه معمولا فقط از مکانیزم های تشخیص خطا استفاده می شود. در صورت مشاهده خطا در خواست ارسال مجدد می کنند و از اصلاح خطا خود داری می شود.

عوامل ایجاد خطا در شبکه

- پارازیت و نویز های خارجی.
- تغییر شکل پالس ارسالی (مثلا به علت تضعیف).

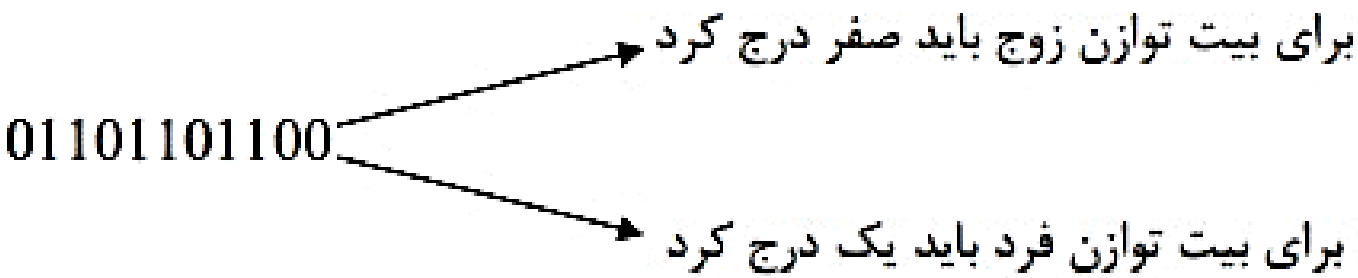
روش های مختلف و گاه متضادی برای تشخیص و اصلاح خطا در شبکه وجود دارد در زیر به مهمترین آنها اشاره شده است :

بیت توازن Parity

ساده ترین روش تشخیص خطا استفاده از یک بیت اضافی به اسم Parity است.

اگر Parity زوج داشته باشیم مقدار این بیت طوری انتخاب خواهد شد که همراه کل مجموعه بیت ها، تعداد بیت های یک زوج باشد. و اگر Parity فرد داشته باشیم طوری بیت های یک را انتخاب می کنیم که تعدا آنها فرد باشد.

مثال:



ضغف این روش در این است که اگر تعداد خطاهای اتفاق افتاد مضربی از دو باشد در (بیت توازن زوج) دیگر نمی توان خطا را تشخیص داد.

روش Hamming Distance برای تشخیص خطا

تعریف فاصله همینگ:

تعداد اختلاف بین بیتهای متناظر در رشته همطول را فاصله همینگ گویند.

مثال:

0110101

1010010

فاصله همینگ دو عدد بالا برابر ۵ می باشد.

نکته:

اگر برای چند رشته بخواهیم فاصله همینگ را بدست آوریم کوچکترین فاصله بین جفت، جفت آنها را به عنوان فاصله همینگ دسته اعداد در نظر می گیریم.

نکته:

اگر فاصله همینگ برابر $d+1$ باشد آنگاه تا d بیت خطا در انها را می توان تشخیص داد.

نکته:

اگر فاصله همینگ برابر $2d+1$ باشد آنگاه تا d خطا را می توان در انها اصلاح کرد.

روش Inter Living

این روش برای ارسال n عدد فریم استفاده می شود. وبه جای ارسال تک تک فریم ها پشت سر هم ابتدا بیت یک کلیه فریم ها را ارسال می کند، و بعد بیت دو و... را ارسال می کند (شکل ۶-۱).

در این روش از بیت توازن هم برای سطر ها یعنی (فریم ها) و هم برای ستون ها استفاده می شود.

1	2	...	k
1	2	...	k
1	2	...	k
1	2	...	k

حسن این روش در این است که هر گاه در یک ارسال حتی بیش از یک خطا داشته باشیم باز هم برای هر فریم حداکثر یک خطا خواهیم داشت و با استفاده از بیت Parity (توازن) که خطا را چک می کنند، برای هر خانه که خطا داشته باشد هم بیت توازن افقی و هم بیت توازن عمودی خطا را معلوم کرده و در این صورت بیت دارای خطا مشخص و اصلاح می شود.

و ضعف این روش این است که باید تمام فریم ها ارسال شوند تا اطلاعات موجود در گیرنده قابل استفاده باشند.

این روش برای ارسال یک فایل مناسب است اما برای کارهای بلادرنگ (Real Time) مثل ارتباطات صوتی و تصویری ایجاد مشکل می کند. در شبکه تلفن همراه ایران برای کشف خطا از این روش استفاده می شود.

روش CRC

در ای روش فریم داده را به یک Generator تقسیم کرده و باقیمانده تقسیم را به فریم اضافه می کنند و همراه آن به سمت گیرنده ارسال می شود. در گیرنده نیز کل فریم (همراه با باقیمانده) را دوباره بر Generator تقسیم می کنند اگر خطایی روی نداده باشد باقیمانده صفر خواهد بود، در غیر این صورت خطایی در زمان ارسال روی داده است.

این روش محل ایجاد خطا را مشخص نمی کند.

نکته:

در این روش فرستنده و گیرنده باید بر روی Generator توافق داشته باشند.

Generator های معروف:

CRC12 : G = X^12 + X^11 + X^3 + X^2 + X^1 + 1

CRC – CCIT : G = X^16 + X^12 + X^5 + 1 مورد استفاده در شبکه تلفن

CRC16 : G = X^16 + X^15 + X^2 + 1

خطا های زیر را می توان با استفاده از این روش کشف کرد:

- یک یا دو خطا.
- تعداد خطا های فرد.
- خطا های پشت سر هم کمتر از ۱۶.

حسن این روش نسبت به روش های گفته شده دیگر :

- تعداد بیت های اضافه شده تابع طول فریم نیست.
- باقیمانده در انتهای فریم اضافه می شود. این امر باعث پیاده سازی آسان این روش می شود.

نکته:

در کارتهای شبکه امروزی معمولا از روش CRC استفاده می شود، و عمل محاسبه باقیمانده بر عهده کارت شبکه می باشد.

برای اندازه گیری میزان خطا در یک کانال ارتباطی تعداد خطا را در یک میلیون بار ارسال محاسبه کرده و آن را به عنوان شاخص در نظر می گیرند.

معمولا هنگام ارسال بسته از یک hop به hop دیگر باید فرستنده به یک نحوی از رسیدن بسته به مقصد مطلع شود. به همین منظور در لایه پیوند داده ها یکسری پروتکل ها در نظر گرفته شده است. کاربرد این پروتکل ها علاوه بر کشف خطا می تواند قدرت گیرنده را برای دریافت بسته ها نیز در نظر بگیرد.

پروتکل توقف و انتظار Stop & Wait

در این پروتکل فرستنده پس از ارسال یک فریم یک مدت زمانی را منتظر رسیدن پاسخ (Ack) از طرف گیرنده می شود. این کار را با تنظیم یک زمانسنج انجام می دهد. هر گاه زمان تایمر به صفر برسد و پاسخی

برای بسته ارسالی دریافت نشود ، فرض می کند که بسته یا خراب شده یا به مقصد نرسیده است. در این هنگام مبادرت به ارسال مجدد بسته می نماید.

استفاده از این تکنیک در مواردی که فاصله بین فرستنده و گیرنده زیاد است، و همچنین خط دارای درصد خطای بالایی باشد مقرون به صرفه نیست.

پروتکل پنجره های لغزان Sliding Windows

در پروتکل Stop & Wait یک فریم ارسال می شود و سپس فرستنده منتظر رسیدن جواب از گیرنده باقی می ماند، در این حالت مقداری از زمان ماشین فرستنده به بطالت خواهد گذشت. در صورتی که هر ماشین موجود در شبکه بتواند در یک زمان محدود خط را در دست داشته باشد این پروتکل با شکست مواجه خواهد شد.

برای رفع این مشکل پروتکل پنجره های لغزان معرفی شده است، کارکرد این پروتکل به نحوی است که فرستنده هر بار به جای ارسال یک بسته می تواند یک تعداد مشخص از بسته ها (یا اصطلاحا یک پنجره از بسته ها) را ارسال کند و سپس منتظر جواب مربوط به آن تعداد از پنجره ها باشد.

بعد از اینکه فرستنده جواب مربوط به رسیدن صحیح پنجره را از گیرنده دریافت کرد بر روی n تعداد بسته دیگر رفته و آنها را ارسال می کند و دوباره برای دریافت جواب منتظر می ماند.

در این روش گیرنده Ack مربوط به آخرین بسته را ارسال می نماید.

یک نقطه ضعف این روش در این است که اگر یکی از بسته (بجز بسته آخر) در طول عملیات ارسال آسیب ببیند دیگر نمی توان تشخیص داد که کدام بسته بوده است.

برای حل این مشکل از مکانیزم های زیر استفاده می شود:

- ❖ مکانیزم برگشت به n
- ❖ مکانیزم تکرار انتخابی

مکانیزم برگشت به n

در این روش گیرنده اگر تمام فریم های یک پنجره را به طور صحیح دریافت کرد پاسخی برای فرستنده مبنی بر دریافت صحیح اطلاعات ارسال می کند. اما به محض اینکه در یک بسته خطایی را تشخیص داد یا اینکه بسته ای در طول عملیات ارسال گم شود دیگر مابقی بسته ها را نیز دریافت نخواهد کرد و Ack آخرین بسته ای را که صحیح دریافت کرده است را به فرستنده ارسال می کند.

فرستنده نیز با دریافت پاسخ گیرنده متوجه می شود که باید بر روی کدام بسته برود و روند ارسال را از چه بسته ای ادامه دهد.

با کمی دقت بر روی این روش متوجه می شویم که فرستنده باید تا پایان عملیات ارسال تمام بسته ها را در حافظه خود نگه دارد، تا در صورت لزوم مجددا به ارسال آنها مبادرت ورزد.

حسن این روش در پیاده سازی و مدیریت آسان آن می باشد اما همانطور که قبلا نیز گفته شد ممکن است بعد از کشف خطا در یک بسته بقیه بسته های دنباله آن را نیز که خطا ندارد هم دور ریخته شود. که این باعث کندی در عملیات ارسال می شود.

مکانیزم تکرار انتخابی

روش دیگر در برخورد با خطا های روی داده در بسته ها در روش پنجره های لغزان استفاده از مکانیزم تکرار انتخابی می باشد.

در این روش پس از کشف یک خطا در یک بسته دیگر بسته های بعدی دور ریخته نمی شوند بلکه آنها نیز توسط گیرنده دریافت خواهند شد، و برای اینکه بسته دارای خطا دوباره توسط فرستنده ارسال شود در حین دریافت بسته ها با یک Ack به فرستنده اطلاع می دهد که بسته ای که در آن خطا روی داده است را مجددا ارسال نماید.

در این روش از پهنای باند کانال استفاده مطلوب تری صورت می گیرد اما مدیریت بسته ها ، Ack و ترتیب ارسال ، دریافت و چینش بسته ها پیچیده تر می شود.

زیر لایه MAC

وظیفه اصلی لایه MAC کنترل دسترسی ماشین ها به لایه فیزیکی (کانال ارتباطی) است.

هنگام ارسال اطلاعات برروی کابل در صورت نبود مدیریت بر لایه فیزیکی ممکن است مشکلاتی در روند ارسال و دریافت اطلاعات به وجود آید، مثلا ارسال اطلاعات توسط دو یا چند ماشین به صورت همزمان.

قبل از بررسی مکانیزم های موجود در زیر لایه MAC برای مدیریت بر روی رسانه فیزیکی پارامترهای مربوط به یک کانال ارتباطی را معرفی می کنیم:

- Delay (مدت زمانی که یک فرستنده باید صبر کند تا کانال در اختیارش گزارده شود).
- Through Put (هیچ گاه کابل نباید بیکار یا خالی از فریم باشد).

روش ارسال اطلاعات بر روی کابل

همانطور که می دانید در یک شبکه در هر زمان تنها یک ماشین می تواند مبادرت به ارسال اطلاعات نماید. زیرا در صورتی که چند ماشین به صورت همزمان اطلاعات خود را بر روی کانال قرار دهند بسته های اطلاعاتی که به صورت سیگنال های الکتریکی بر روی کانال وجود دارند با یکدیگر برخورد می کنند و از بین می روند.

برای کم کردن Delay و همچنین افزایش Through Put در یک شبکه مکانیزم هایی پیشنهاد شده است که در اینجا نمونه هایی از آنها را بررسی می کنیم.

روش Aloha

در این روش هر کامپیوتر به محض اینکه اطلاعاتی برای ارسال داشته باشد شروع به ارسال آن خواهد نمود.

مزایا:

Delay در این روش صفر است.

معایب:

اگر دو یا چند کامپیوتر همزمان مبادرت به ارسال اطلاعات نمایند بسته ها با یکدیگر تداخل کرده و از بین می روند.

روش الوهای برهه ای Stetted Aloha

برای بهتر کردن روش آلوها زمان انتقال را به قسمت های (برهه های) مجزایی تقسیم می کنند که هر قسمت برای ارسال یک قاب در نظر گرفته می شود.

در این روش اگر ماشینی قصد ارسال اطلاعات را داشته باشد دیگر نمی تواند در هر زمانی اطلاعات را

ارسال کند بلکه فقط ارسال اطلاعات در مرز بین دو برهه امکان پذیر است.

در این روش تاخیر ارسال اطلاعات تقریبا برابر نصف زمان یک برهه است.

روش CSMA (Carrier Sense Multiple Access)

کارایی روش های آلوها و آلوهای برهه ای بسیار کم می باشد و این به آن جهت است که هر ایستگاه به دلخواه خود عمل انتقال را انجام می دهد و به عملکرد سایر ایستگاه ها توجهی ندارد. در یک شبکه محلی این امکان وجود دارد که هر ایستگاه تشخیص دهد سایر ایستگاه ها مشغول به چه کاری هستند. بنابراین بر طبق این مکانیزم در فرستنده ای که قصد ارسال اطلاعات را دارد قبل از انجام عمل ارسال ابتدا به خط گوش می دهد اگر خط خالی باشد شروع به ارسال اطلاعات می کند. این نوع ارسال را اصطلاحا CSMA گویند.

برای بالا بردن کارایی در این روش فرستنده می تواند به هر چیزی که ارسال می کند نیز گوش دهد و به محض این که یک تداخل را مشاهده کرد دیگر چیزی ارسال نمی کند. به این مکانیزم CD (Collision Detection) گویند.

پروتکل های مختلفی بر مبنای CSMA/CD طراحی شده اند که در زیر مثال هایی از این نوع پروتکل ها آمده است :

- 1 - Persistent
- non - Persistent
- p - Persistent

پروتکل های بدون اختلال Collision free

با وجود این که در روش CSMA/CD وقتی که یک ماشین کانال ارتباطی را در دست گرفت دیگر اختلالی در ارسال اطلاعات به وجود نمی آید، اما باز هم ممکن است در زمان رقابت برای در دست گرفتن کانال در بین ماشین ها اختلالاتی در روند ارسال به وقوع بپیوندد. و این موضوع برروی کارایی کانال تاثیر منفی می گذارد.خصوصا هنگامی که طول کابل ارتباطی زیاد باشد و همچنین اندازه بسته ها نیز کوچک باشند.

نکته:

روش های متعددی وجود دارد که باعث می شوند که اختلالات در هنگام رقابت برای تصاحب خط از بین برود.

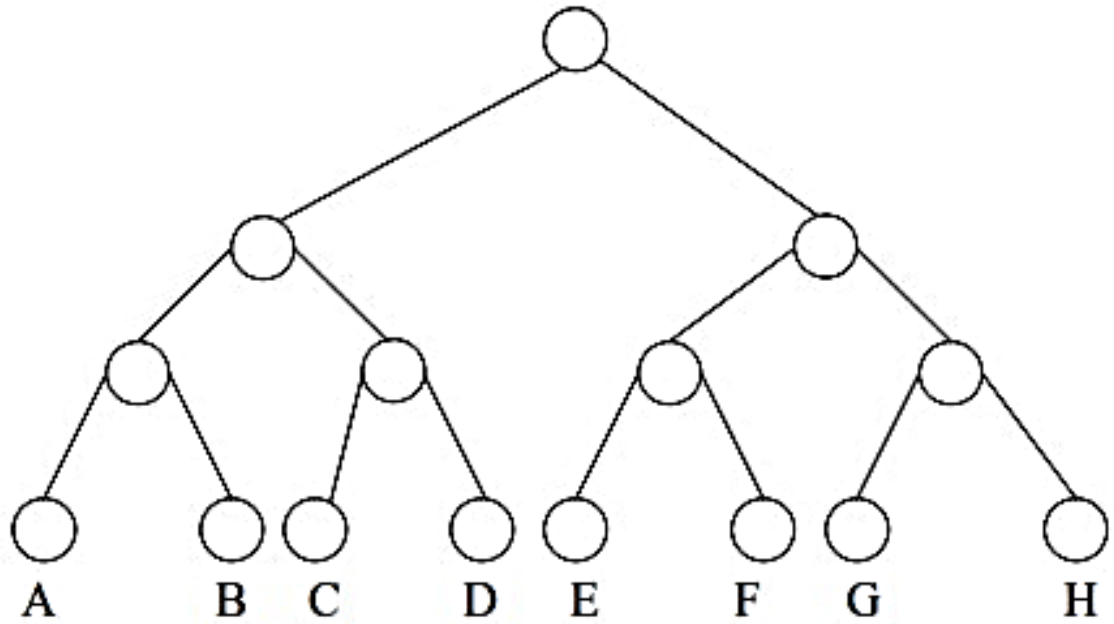
از پروتکل هایی که از مکانیزم Collision Free استفاده می کنند می توان نوع های زیر را نام برد:

- پروتکل نگاشت بیتی
- پروتکل درختی

در اینجا به دلیل اهمییت پروتکل درختی به شرح آن می پردازیم:

در پروتکل درختی از یک درخت دودویی استفاده کرده و ایستگاه های موجود در شبکه را به عنوان برگ های آن در نظر می گیریم، و به صورت زیر عمل می کنیم:

در ابتدا به کلیه ماشین ها (برگ ها) اجازه ارسال اطلاعات داده می شود، اگر فقط یک ماشین داده ای برای ارسال داشته باشد که اختلالی در روند ارسال روی نمی دهد و داده ها به صورت صحیح بر روی کانال ارسال می شوند. اما اگر اختلالی پیش بیاید به زیر درخت چپ فقط اجازه ارسال داده می شود و این روند به صورت بازگشتی ادامه می یابد تا دیگر ماشینی در شبکه نباشد که در عملیات ارسال اختلالی ایجاد کند



ساختار درخت دودویی در شبکه برای پروتکل درختی

لایه شبکه Network

وظیفه لایه شبکه ، کنترل عمل زیر شبکه است. مسئله اصلی در اینجا، تعیین چگونگی هدایت و مسیر یابی بسته ها از منبع به مقصد است.

بسته ها می توانند مبتنی بر جدول های ثابتی باشند که بر مبنای شبکه سیم کشی شده ای است که به ندرت تغییر می کند. آن ها را می توان در آغاز هر عمل ارسال و یا دریافتی مشخص کرد.

در دید دیگر می توان مسیر ها را به صورت پویا مشخص کرد تا در هر بار ارسال بهترین و بهینه ترین مسیر و کم ازدهام ترین مسیر بین فرستنده و گیرنده انتخاب شود.

اگر همزمان بسته های زیادی در زیر شبکه وجود داشته باشند. مسیر عبور را مثل سر بطری تنگ می کنند و عبور مشکل می شود.

کنترل این ازدهام نیز از وظایف لایه شبکه است. بطور کلی، کیفیت، خدمات (تاخیر، زمان انتقال و...) به لایه شبکه مربوط می شود.

وقتی بسته ای برای رسیدن به مقصد مجبور است از شبکه ای به شبکه دیگر برود، مشکلات زیادی ممکن است به وجود آید. ممکن است شیوه آدرس دهی در دو شبکه کتفاوت باشد. ممکن است به علت بزرگی بیش از حد بسته، آن را نپذیرد. پروتکل های ارتباطی ممکن است متفاوت باشند و مشکلات دیگری از این قبیل ممکن است در شبکه ها رخ دهد. از بین بردن این مشکلات برای برقراری اتصال بین دو شبکه ناهمگون، از وظایف لایه شبکه است.

در شبکه های توزیعی، مسئله مسیریابی، چندان مشکل نیست و لذا حضور لایه شبکه بسیار کمرنگ است یا اصلا وجود ندارد.

الگوریتم های مسیریابی

الگوریتم های مسیر یابی که وظیفه آنها هدایت بسته ها از مبدا به مقصد است، قسمتی از نرم افزار لایه شبکه بوده ، که معین می کند بسته رسیده باید به کدام مسیر ارسال شود.

الگوریتم های مسیر یابی مختلفی وجود دارد که در زیر به برخی از آنها اشاره می کنیم: