

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



مدرس:

سپیره برادران
هزاوه

پاییز ۹۶

Network
Operating
System



نحوه دسترسی به مدرس

baradaran.hezaveh@gmail.com
baradaran-hezaveh.blog.ir



نحوه ارزشیابی

کار کلاسی

امتحان میان ترم

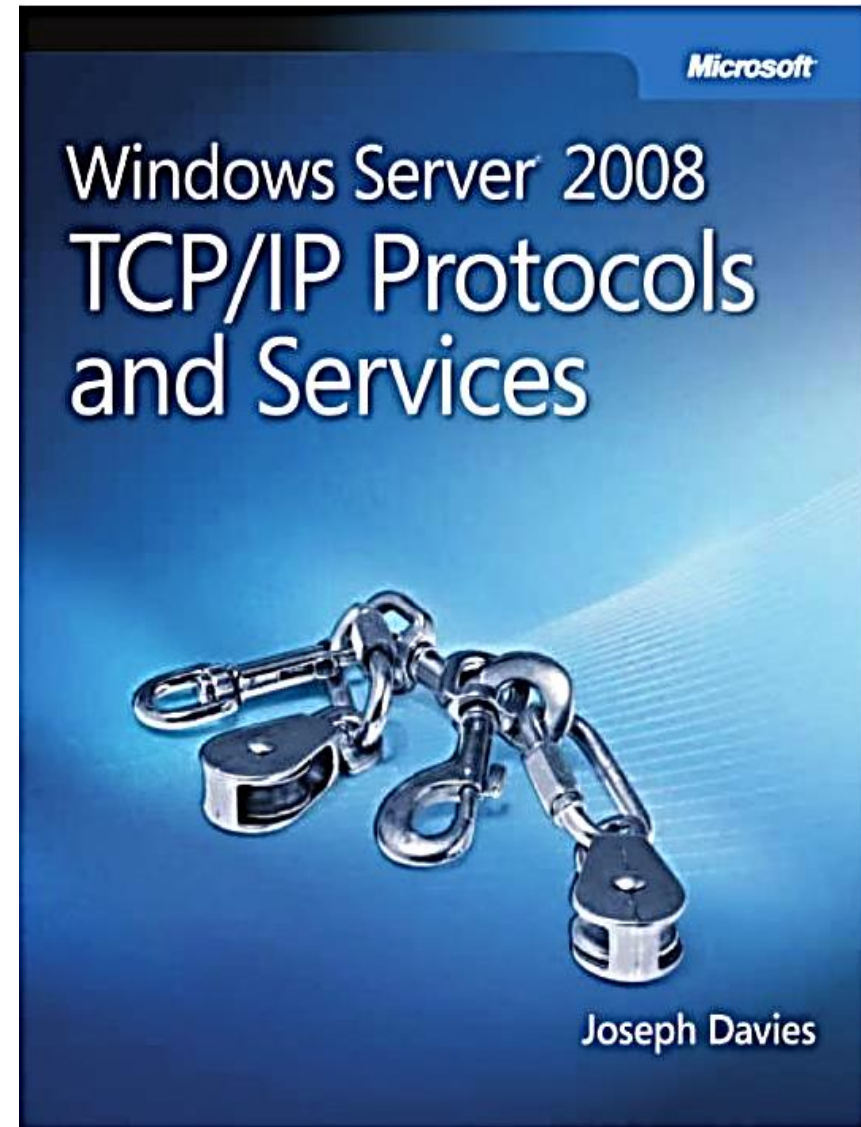
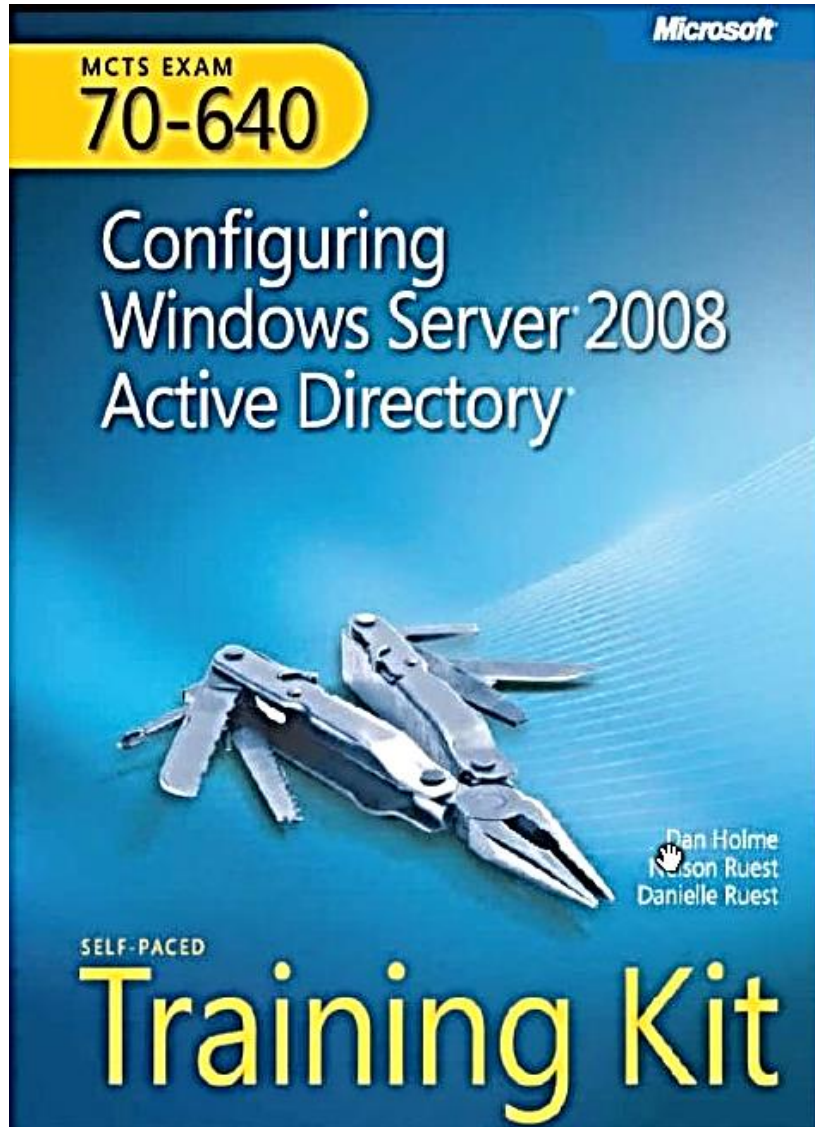
امتحان پایان ترم

۳ نمره

۳ نمره

۱۴ نمره





The Complete Reference

Foreword by
David Greschler,
Director, Integrated
Virtualization Strategy,
Microsoft

Microsoft®

Windows Server® 2008

- ▲ Easily migrate to a physical/virtual Windows infrastructure
- ▲ Configure, administer, and secure resource pools and virtual service offerings
- ▲ Set up and manage ADDS, Server Core, IPv6, and Terminal Services RemoteApps

**Danielle Ruest
Nelson Ruest**



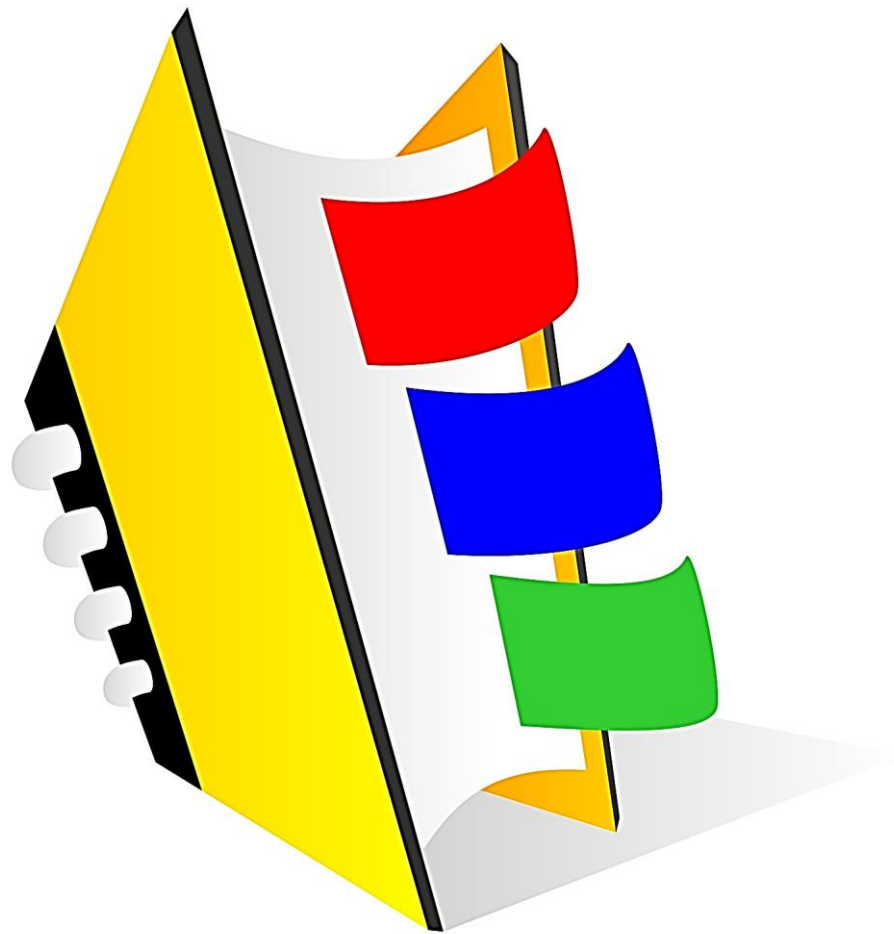
Microsoft

Windows Server 2008 Security



Jesper M. Johansson
and Microsoft MVPs with
the Microsoft Security Team

Resource Kit



رئوس مطالب

❖ مروری بر مفاهیم اولیه شبکه

❖ Active Directory

❖ ISA Server

❖ پیکربندی firewall, Cache Server, Proxy Server, VPN, ...

سخت افزا 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.

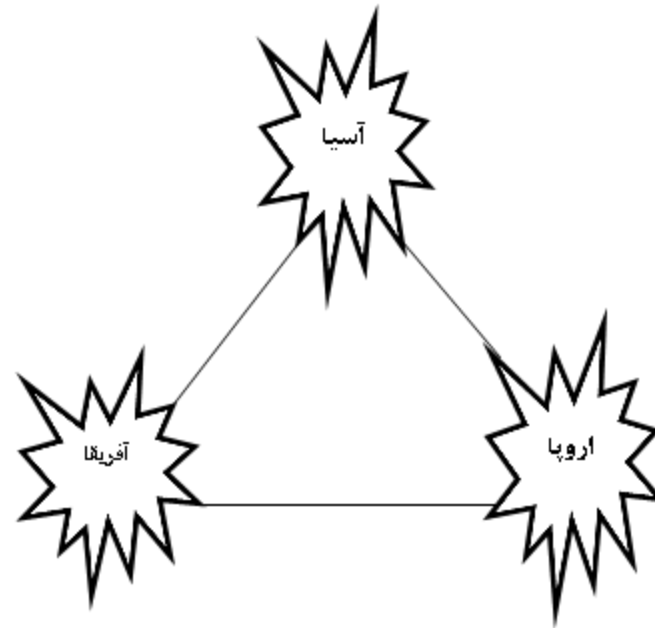
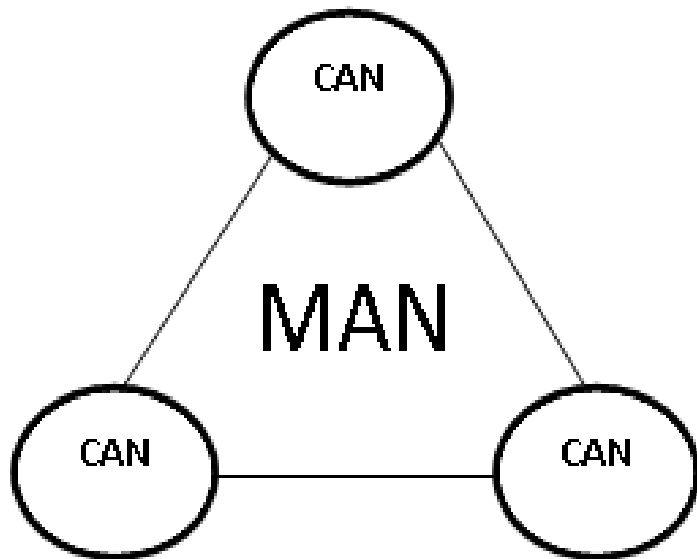
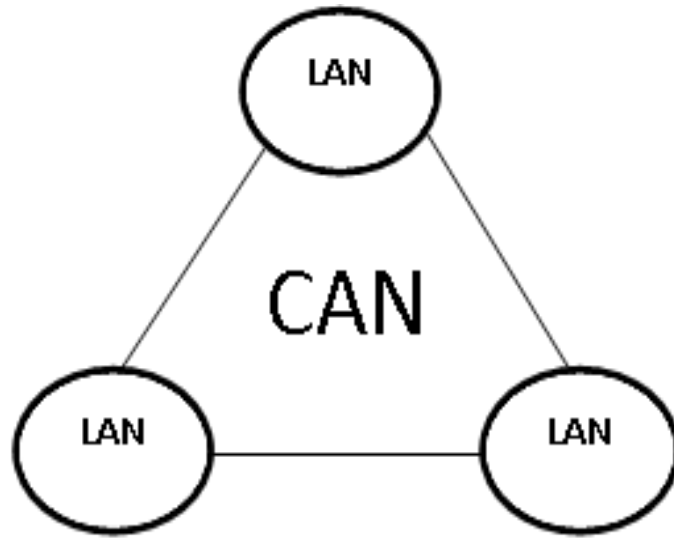
دسته بندی شبکه های رایانه ای

۱. تقسیم بندی شبکه از نظر وسعت جغرافیایی

(Local Area Network) LAN (1)

(Campus Area Network) CAN (2)

(Metropolitan Area Network) MAN (3)



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)

• شبکه اینترنت (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 دستگاه‌های USB برای برقراری ارتباط حتماً به یک کامپیوتر میزبان و واسط نیاز دارند. اما فایر وایر نظیر به نظیر یا Peer-To-Peer است و دستگاه‌های فایر وایر می‌توانند برای ایجاد ارتباط با یکدیگر بدون نیاز به کامپیوتر و به طور مستقیم وارد عمل شوند. فایروایر برای دستگاهی که با حجم زیادی از اطلاعات کار می‌کنند نظیر دوربین‌های فیلم برداری، دستگاه‌های پخش DVD و تجهیزات صدای دیجیتال در نظر گرفته شده و مطلوب است.

IrDA یک فناوری 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 Bluetooth کاربرد ویژه‌ای از امواج رادیویی 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 فرستنده‌ها از توان تشعشعی بسیار ناچیزی در یک باند بسیار وسیع استفاده کرده و طوری فعالیت میکنند که تأثیر منفی بر روی ارتباطات رادیویی سامانه‌های ارتباطی در فرکانسهای به کار رفته ایجاد نشود. فناوری فراپهن باند نسبت به سایر سامانه‌های بی‌سیم داخل ساختمان همچون (Wi-Fi و دندان آبی Bluetooth) دلیل 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 به وسیله «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 خود 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 تفصیل 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 قدرتمند 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 قدرتمند نیاز دارد، امنیت شبکه بالا و تعداد سیستمها نیز نامحدود است.

۳. شبکه داخلی Intranet

یک «شبکه داخلی» مجموعه ای از شبکه های متصل به هم می باشد که از قرارداد IP و ابزارهای مبتنی بر IP مانند «مرورگران وب» استفاده می کند و معمولاً زیر نظر یک نهاد مدیریتی کنترل می شود. این نهاد مدیریتی «شبکه داخلی» را نسبت به باقی قسمت های دنیا محصور می کند و به کاربران خاصی اجازه ورود به این شبکه را می دهد. به طور معمول تر شبکه درونی یک شرکت یا دیگر شرکت ها «شبکه داخلی» می باشد. به طور مثال شبکه ملی در ایران نوعی از شبکه های داخلی (اینترانت) می باشد.

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 نقطه نظر 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.

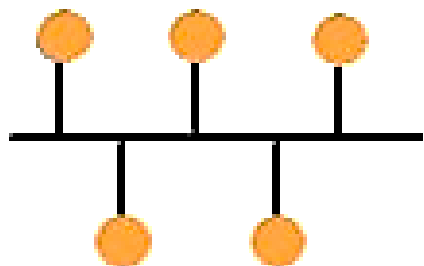
شبکه اینترنت (Internet)

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 به وسیله موسسه «آرپا» (ARPA) که وابسته به «وزارت دفاع ایالات متحده آمریکا» است ایجاد شد. همچنین منزلگاهی برای «وب جهان گستر» (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.

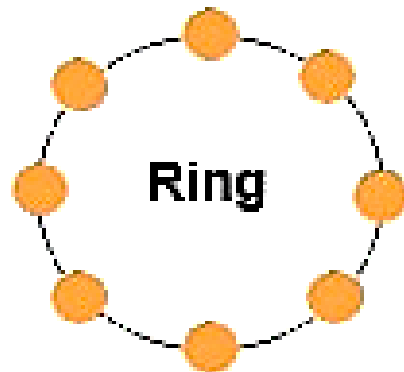
اعضای شبکه اینترنت یا شرکت‌های سرویس دهنده آنها از «آدرسهای IP» استفاده می‌کنند. این آدرس‌ها از موسسات ثبت نام آدرس تهیه می‌شوند تا تخصیص آدرسها قابل کنترل باشد. همچنین «سرویس دهندگان اینترنت» و شرکت‌های بزرگ، اطلاعات مربوط به در دسترس بودن آدرس‌هایشان را بواسطه «قرارداد دروازه لبه» (BGP) با دیگر اعضای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

انواع Topology در شبکه

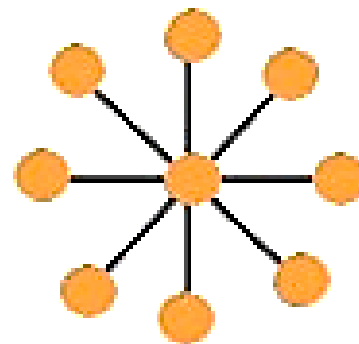
نحوه چیدمان یا اتصال کامپیوترها به یکدیگر را توپولوژی می گویند.



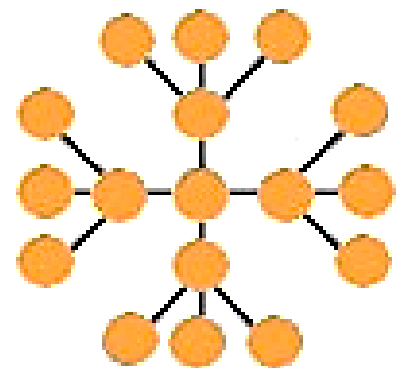
Bus



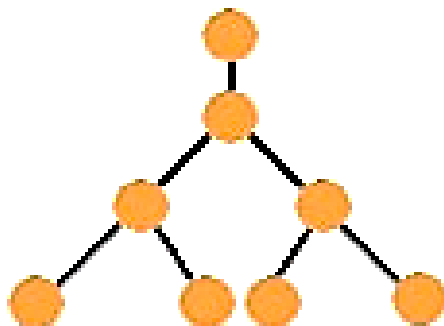
Ring



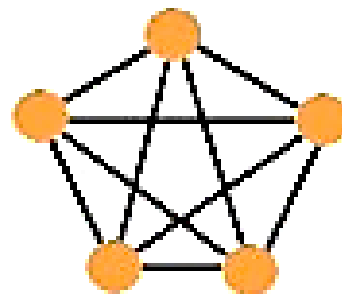
Star



Extended Star



Tree



Mesh

❖ توپولوژی Bus یا خطی

❖ توپولوژی Star

❖ توپولوژی رینگی

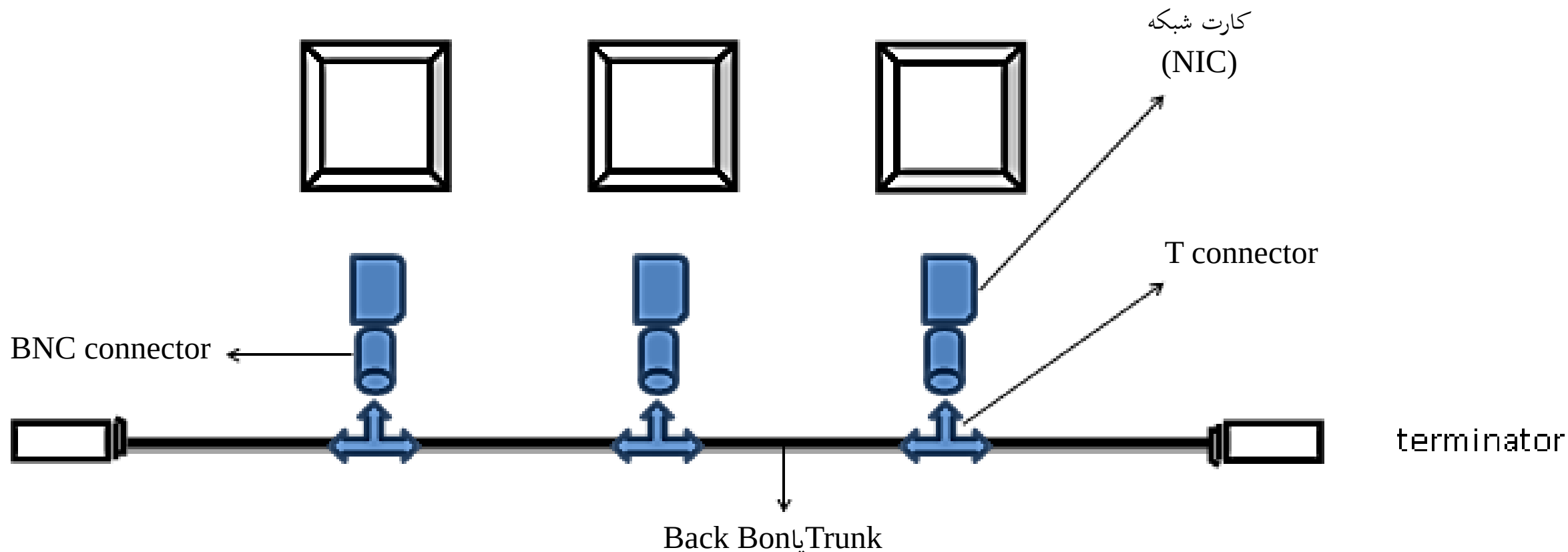
❖ توپولوژی مش (Mesh)

❖ توپولوژی Hybrid

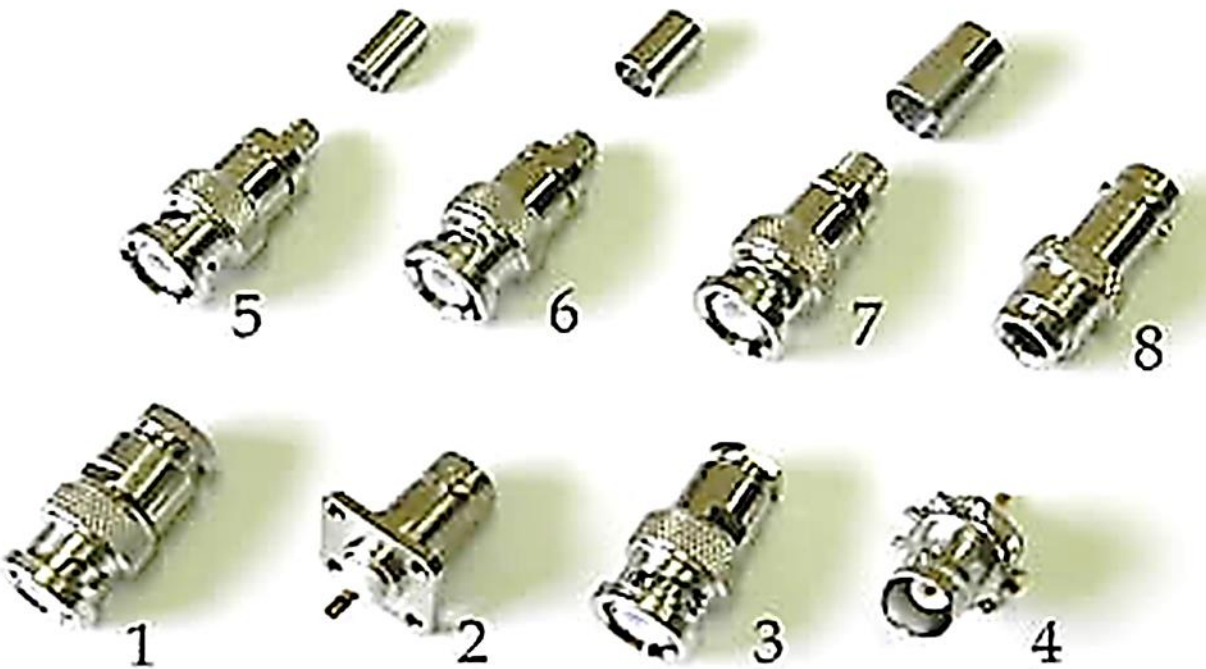
❖ توپولوژی Tree

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



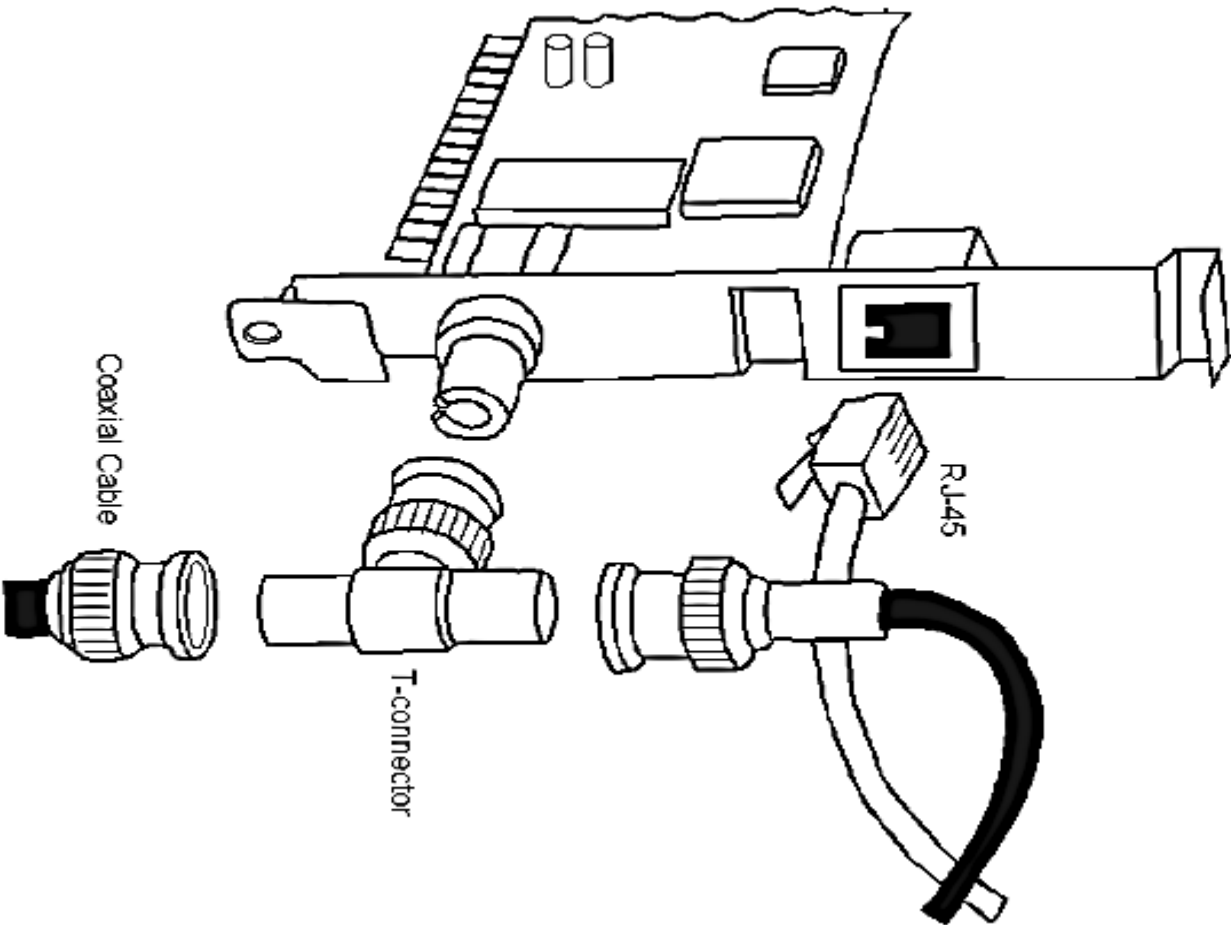
N	Model	Description
1	MT 801	Connector BNC Macho para RG 59 - Solda
2	MT 819	Conector BNC Fêmea com Base Quadrada para Painel
3	MT 812	Conector BNC Macho para RG 58 - Solda
4	MT 804	Conector BNC Fêmea com Rosca para Painel
5	MT 815/58	Conector BNC Macho para RG 58 - Climpar - 50 Ohms
6	MT 815/59	Conector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



BNC T Connector



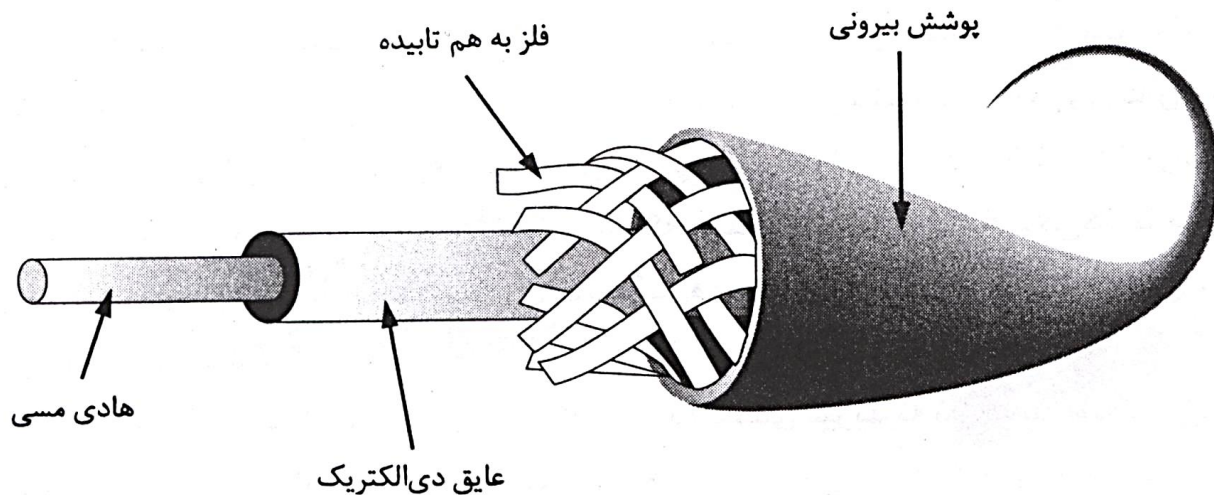
Straight Terminator



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 کواکس 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 کننده سیگنال و زمین باید همیشه از هم جدا باشند ، و گر نه اتصال کوتاه رخ می دهد و روی کابل نویز ایجاد می کند . کل این ساختار نیز در یک حفاظ عایق قرار می گیرد

کابل های کواکس 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 می باشد. از آنجا که Thinnet نرم و انعطاف پذیر است و کارکردن با آن هم آسان می باشد. تقریباً در تمام شبکه ها می تواند مورد استفاده قرارگیرد. در شبکه هایی که از Thinnet استفاده می کنند، کابل مستقیماً به کارت شبکه متصل می شود. نوع نازک کابل کواکسیال می تواند سیگنال ها را تا فاصله تقریبی ۱۸۵ متر (۶۰۷ فوت) ارسال کند، بدون آن که تضعیف شوند. کابل Thinnet جزء کابل های خانواده RG-58 بوده و دارای امپدانس ۵۰ اهم است. امپدانس، مقاومت سیم در برابر جریان متناوب است. تفاوت اصلی میان کابل های خانواده RG-58 هسته مسی در مرکز آنهاست. این هسته می تواند به صورت یک مفتول یا چند تار به هم تابیده باشد.

۲. این نوع کابل، کواکسیال انعطاف ناپذیر و قطر آن در حدود ۵/۰ اینچ است (کابل 8/U – RG). 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. هسته مسی این کابل کواکسیال ضخیم‌تر از نوع نازک آن است. نوع ضخیم کابل کواکسیال می‌تواند سیگنال‌ها را بدون تضعیف تا فاصله ۵۰۰ متر (حدود ۱۶۴۰ فوت) 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 کابل‌های (Attachment Unit Interface (AUI مورد نیاز است.

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

10BASE5 - "Thicknet"



10BASE2 - "Thinnet"



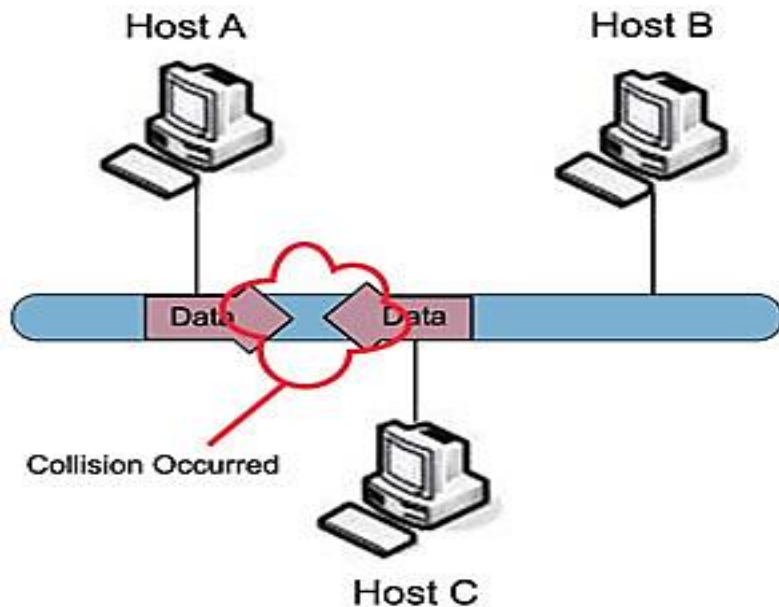
مکانیزم جلوگیری از بروز خطا در شبکه

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

اگر دو سیستم 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 دیگر کاربران اطلاع دهد قصد ارسال اطلاعاتش را دارد و collision رخ ندهد. نقطه ضعف این مکانیزم ایجاد ترافیک در شبکه است.



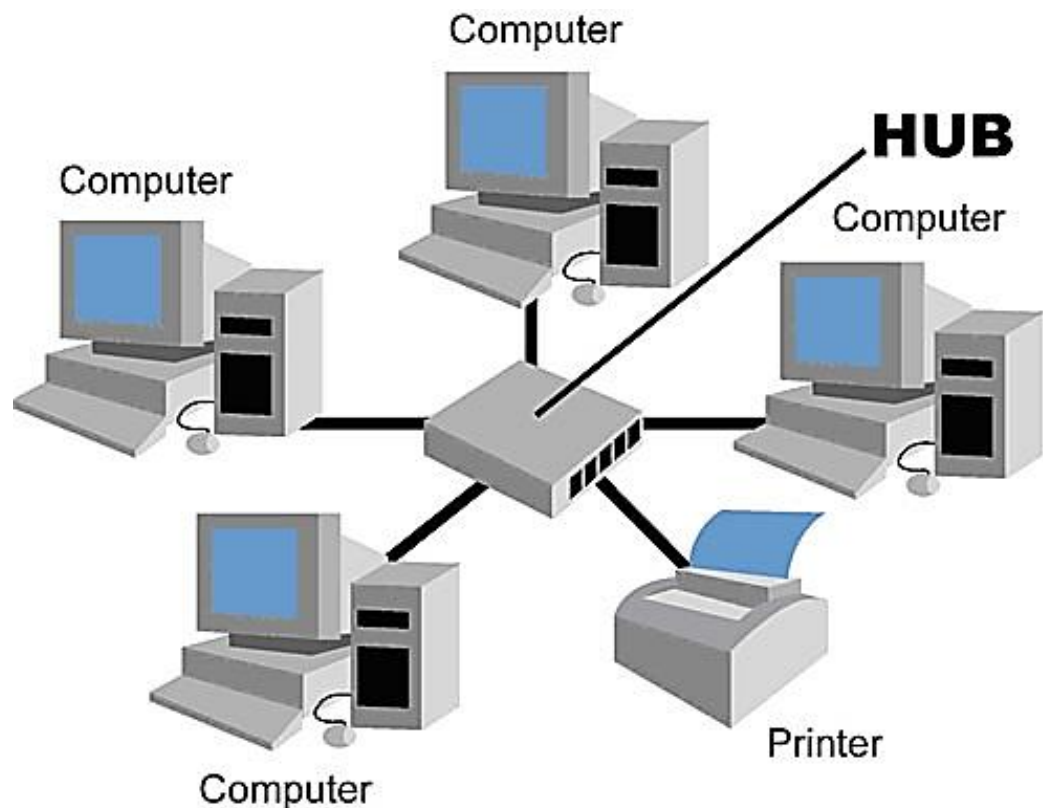
توپولوژی Star

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 پورتهای 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.

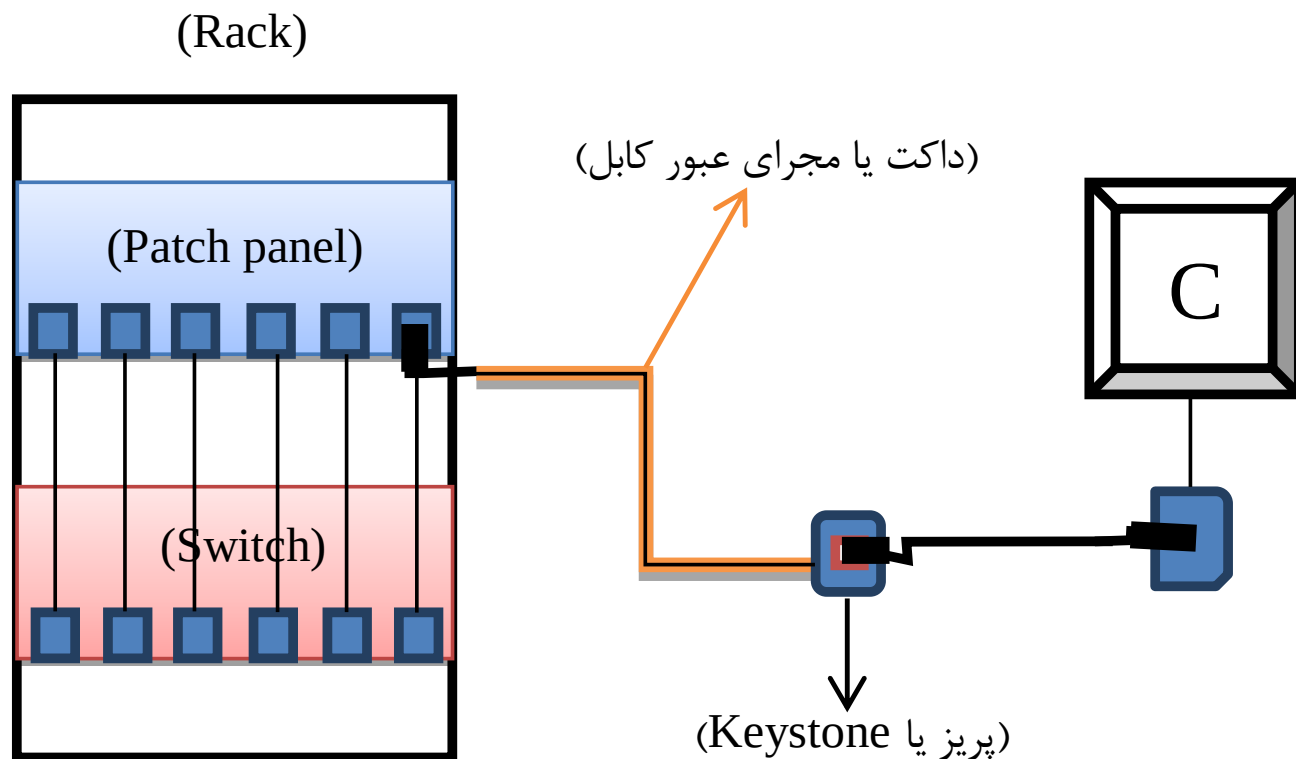
Passive کار تقویت سیگنال را انجام نمی دهد و

فقط همانند یک جعبه تقسیم عمل می کند.

۲. استفاده از 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 پورتهای 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 Patch panel 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 هر جفت 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, CAT5 و 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.

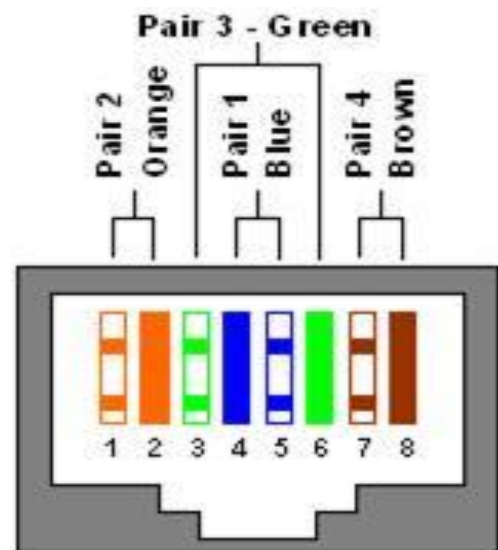
✓ از کابل های CAT3 و CAT4 در شبکه های Token Ring استفاده می گردد .

✓ حداکثر مسافت در کابل های CAT3، یکصد متر است .

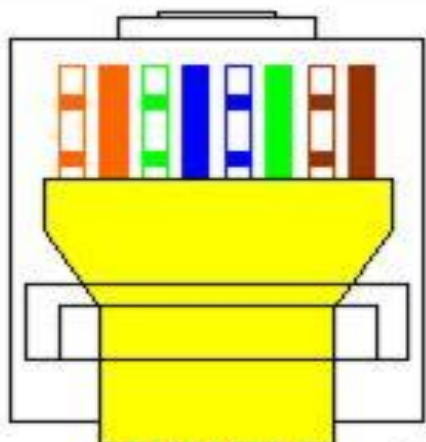
✓ حداکثر مسافت در کابل های CAT4، دویست متر است .

✓ 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



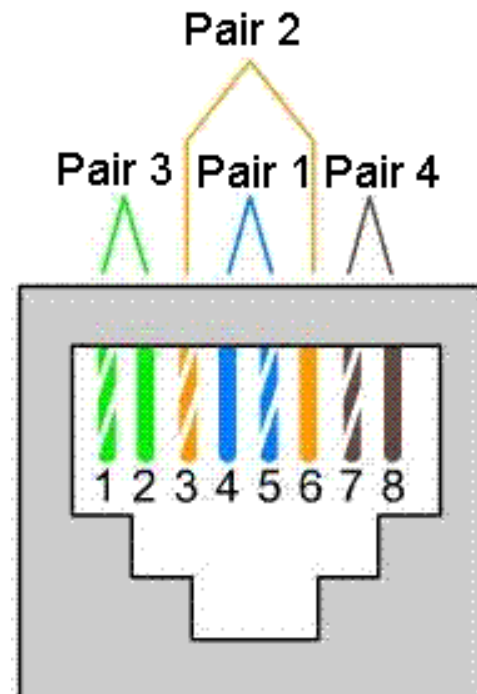
RJ-45 Jack



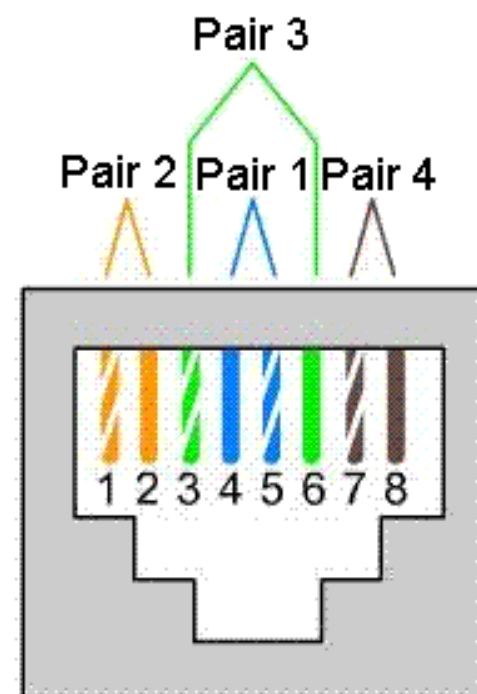
RJ-45 Plug

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 استثنائاتی هم وجود دارد مثلاً اتصال کامپیوتر به روتر (هم جنس نیستند اما از این کابل استفاده می کنند). در اتصال کامپیوتر به سویچ 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 مقاومت 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 سیگنال 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 می‌شود. 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 زمانی که نشانه توسط یک رایانه نگه‌داشته شده باشد، تمام رایانه‌های شبکه پذیرای اطلاعاتی خواهند بود که رایانه مالک نشانه ارسال می‌کند. معایب این نوع توپولوژی این است که اگر قسمتی از کابل اصلی به علتی آسیب ببیند کل شبکه از کار می‌افتد 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 می‌شود که ساختار حلقه در آن وجود دارد و کار انتقال داده ها را انجام می‌دهد.

قرار دادن یک **Token** جدید:

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

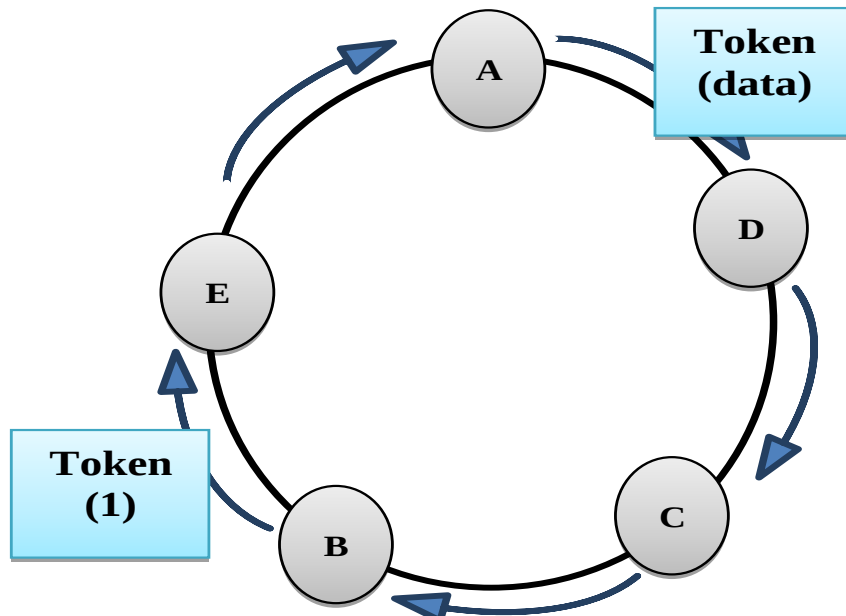
مکانیزم جلوگیری از بروز خطا

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

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

Token Passing (3)

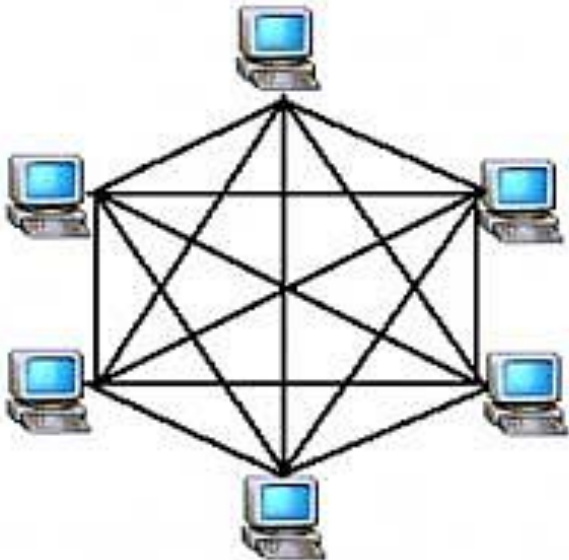
مثال: در شکل زیر و قتی قرار است اطلاعات از کامپیوتر A به کامپیوتر B ارسال شود اطلاعات در داخل token Frame قرار می گیرد و در مسیر خود به کامپیوتر D منتقل می گردد و بعد از بررسی اگر اطلاعات مربوط به سیستم D نباشد به C پاس داده شده و مجدداً بعد از بررسی به سیستم مقصد پاس داده می شود، پس از رسیدن اطلاعات به مقصد در داخل Frame 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 سیستم‌ها بایکدیگر ارتباط مستقیم دارند مانند اینترنت و شکل ظاهری این توپولوژی را مانند یک تار عنکبوت می‌توان 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 هزینه‌های 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 نمی‌افتد و انتقال اطلاعات به صورت دوطرفه دو می‌باشد یعنی تمامی کامپیوترها بدون اینکه شبکه مشغول شود میتوانند به یک دیگر اطلاعات ارسال و دریافت کنند که برای اینکه از توپولوژی mesh بتوان از حداکثر نیرو استفاده کرد از دستگاهی به نام روتر یا مسیر یاب استفاده می‌شود که کار این دستگاه این است که باعث می‌شود از خط‌ها یا مسیرهایی که خالی هستند ارسال اطلاعات انجام داد و در نتیجه این دستگاه باعث سرعت بخشیدن به ارسال اطلاعات می‌شود.

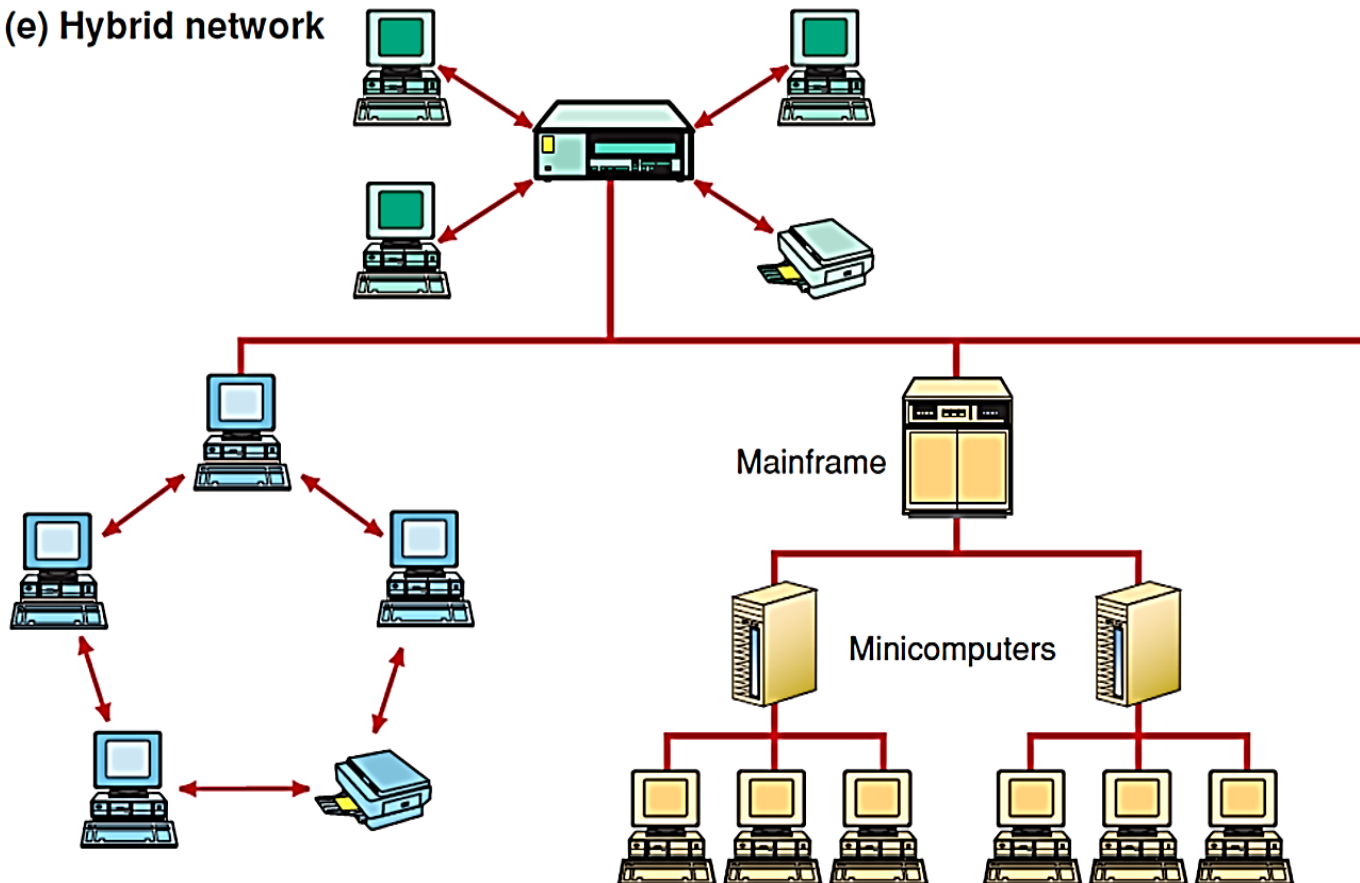
Mesh Topology



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 شده‌اند. توسط یک پل ارتباطی به نام Bridge به کابل backbone متصل می‌شود.

(e) Hybrid network



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 می‌توان برای استفاده از پورتهای بیشتر سوئیچ‌ها را توسط کابل به یکدیگر متصل کرد.

در کابل فیبر نوری از پالسهای نور (فوتونها) برای ارسال سیگنالهای باینری تولید شده توسط کامپیوتر ها استفاده می شود . از آنجا 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 براین، تقلیل آن بسیار کمتر است، و بنابراین کابل های فیبر نوری را می توان در فواصل بسیار دورتری نسبت به کابل مسی گستراند ، گاهی تا ۱۲۰ کیلو متر .

کابل فیبر نوری برای استفاده در زیر ساخت های 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 .

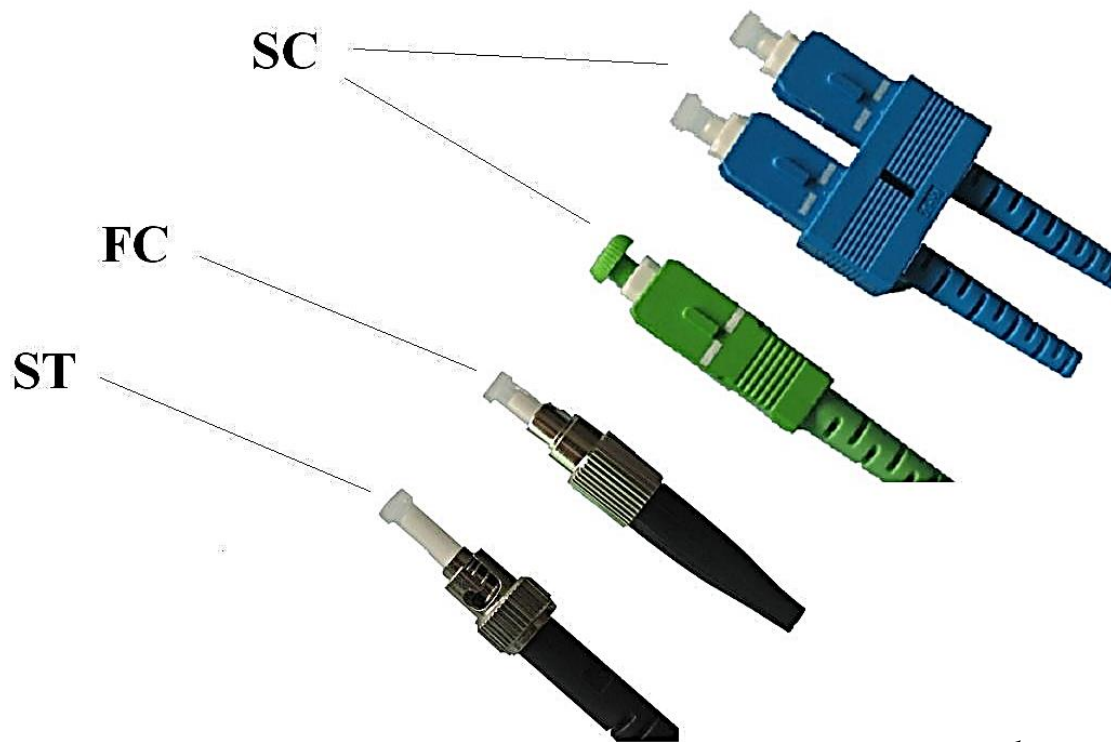
کابل فیبر نوری شامل یک هسته است که از شیشه یا پلاستیک ساخته می شود و یک روکش که هسته را در بر می گیرد و روی آن یک لایه حائل پلاستیکی یک لایه از فیبر به منظور محافظت و یک پوشش بیرونی از تفلون یا PVC قرار دارد . وقتی پالسهای نور در هسته حرکت می کنند توسط روکش به عقب و جلو انعکاس داده می شود . بدلیل این 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 دهند ه 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 کیلومتر حرکت 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 تکنیک انتقال سیگنالهای کد شده بر روی کابل استفاده می شود:

❖ باند اصلی (Baseband)

❖ باند سریع (Broadband)

روش انتقال Baseband

سیستمهای Baseband برای انتقال اطلاعات بر روی 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 بر روی 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 بر روی کابل از سیگنالهای آنالوگ و یک بازه فرکانسی استفاده مینماید. در انتقال آنالوگ سیگنالها یکنواخت و پشت سر هم و در یک جهت بر روی رسانه فیزیکی انتقال، که همان کابل باشد به شکل امواج الکترومغناطیس یا نوری جریان پیدا میکنند. چنانچه پهنای باند کافی بر روی رسانه فیزیکی فراهم باشد میتوان از چندین سیستم انتقال آنالوگ همانند تصاویر تلویزیون و داده های شبکه به طور همزمان بر روی یک کابل استفاده کرد. در سیستمهای 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 تولید کنندگان مختلف به ایجاد پروتکل های استاندارد نیاز است. نظیر مدل OSI (Open Systems Interconnection)

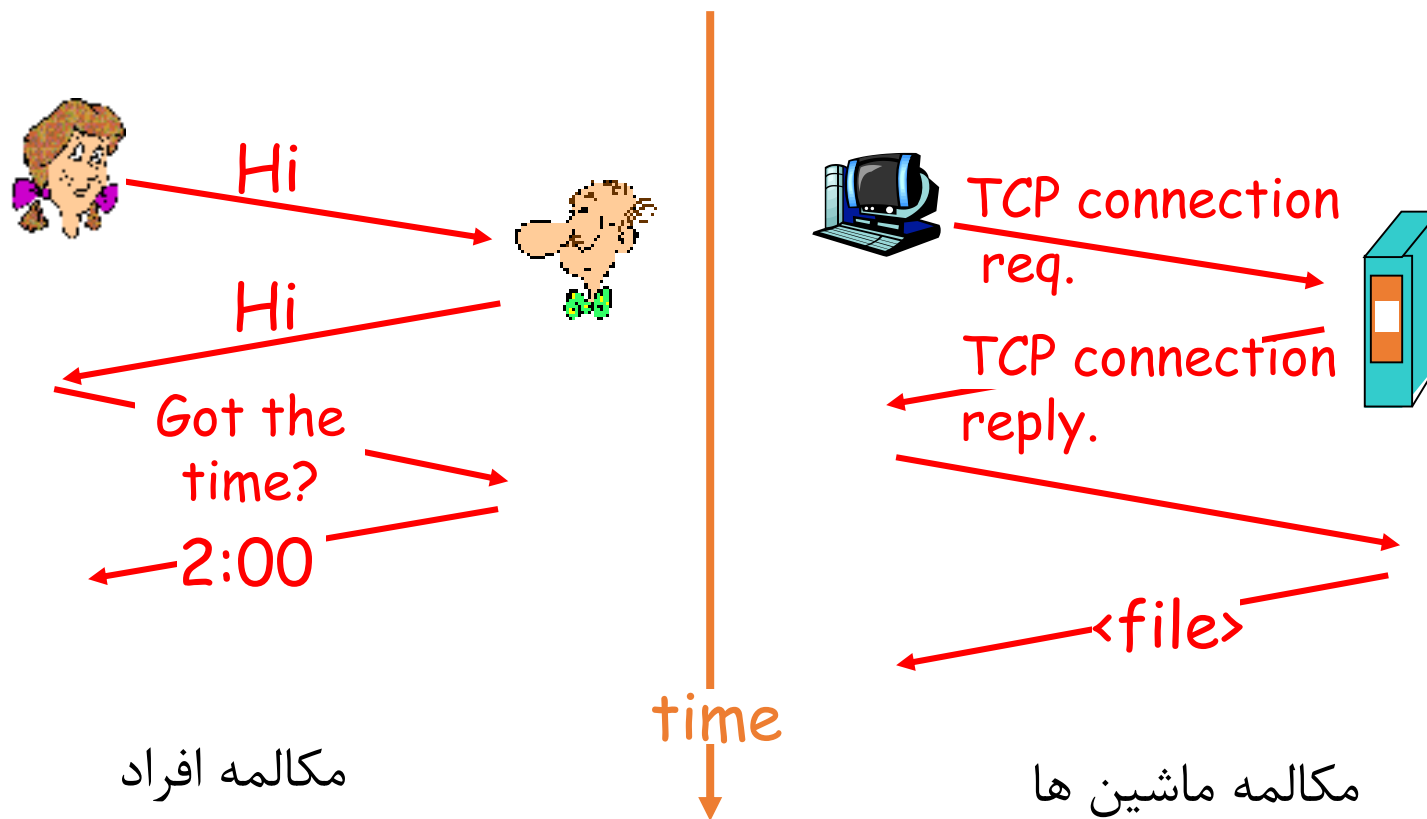
به زبان ساده برای اینکه دو دستگاه بتوانند با همدیگر ارتباط برقرار نمایند احتیاج به زبان واحدی می باشد که تحت آن هر دو دستگاه بتوانند با همدیگر به گفتگو و تبادل اطلاعات بپردازند که با آن پروتکل گویند. زمانی که سرویس گیرنده از طریق یک پورت خاص به سرویس دهنده وصل شد، می توانیم از طریق یک پروتکل به سرویس دهنده دسترسی داشته باشیم. پروتکل یک راه از پیش تعریف شده برای گفتگو با سرویس دهنده است. همچنین پروتکل ها 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 درگیر هستند و وسعت کار بحدی زیاد است که باعث می شود امکان قرار دادن آنها در یک قالب مازول واحد و مستقل میسر نباشد و باید آنها را در قالب چندین زیر 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 داشتن جزئیات 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 مسیرهای مختلفی بین مبدا 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 مسیرهای متنوعی به مقصد برسد دریافت و بازسازی پیام از وظایف سطح نرم افزار به شمار می آید.

۵. هماهنگی سرعت بین مبدا و مقصد که 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 قراردادهای استانداردهای جهانی مشخص شود.
- ✓ تعداد لایه ها نباید آنقدر زیاد باشد که 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 .

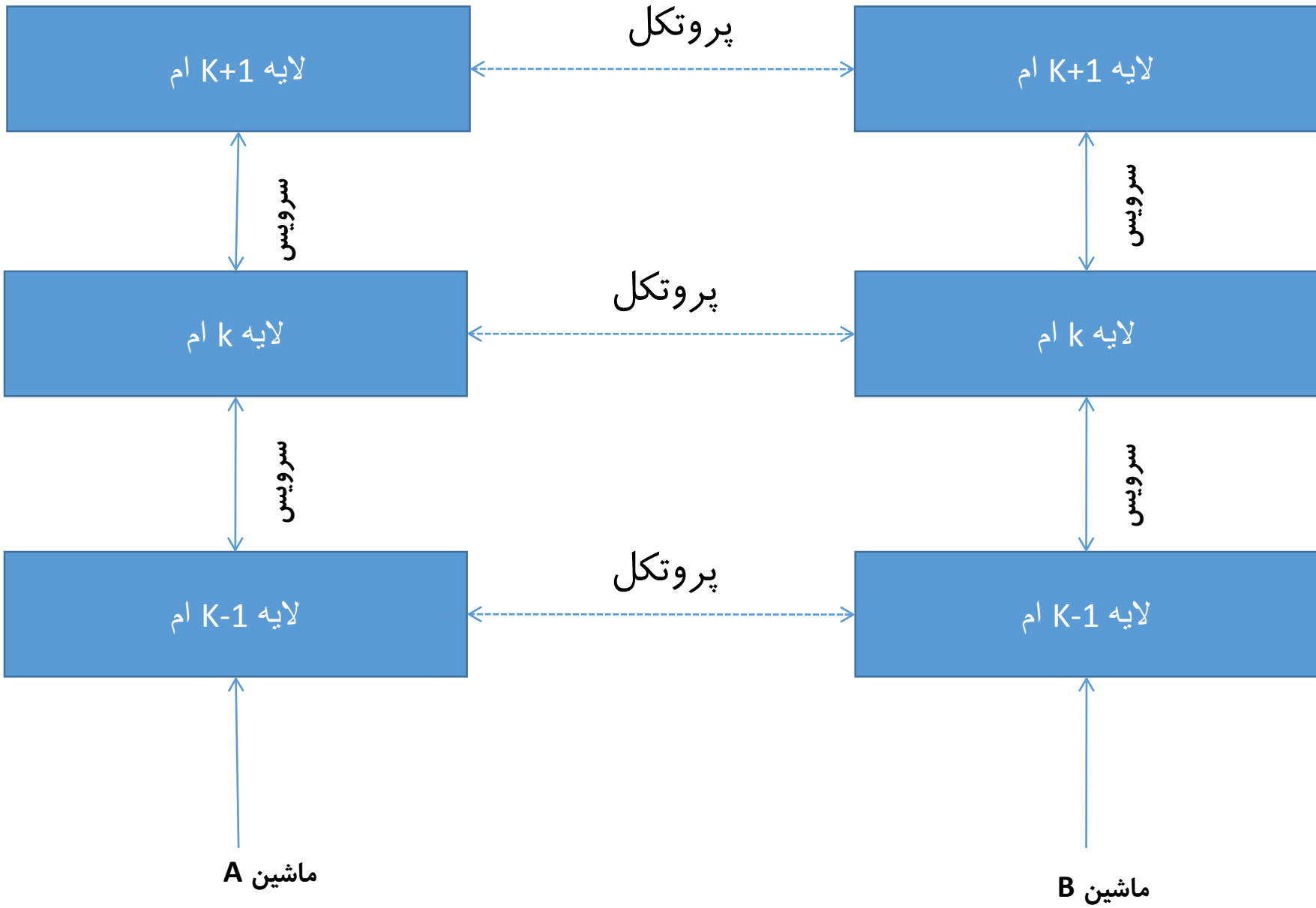
Service

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 کارهایی 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 Primitives توصیف 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 اصطلاحاً پشته پروتکلی گفته می شود

PDU(Protocol Data Unit)

”در معماری لایه ای شبکه، یک قطعه داده از لایه $K+1$ تحویل لایه k ام 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 اصطلاحاً کپسوله سازی اطلاعات گفته می شود.

بسته (Packet)

به یک قطعه اطلاعات دارای هویت و شناسنامه که در ماشین مبدا سازماندهی شده و توسط زیر ساخت شبکه هدایت و تحویل می شود اصطلاحاً 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 یک واحد اطلاعاتی افزوده می شود اصطلاحاً سرآیند و به اطلاعاتی که به انتهای آن افزوده می شود پی آیند اطلاق می شود سرآیند و 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 طبعاً این موجودیتها دارای آدرس یکتا هستند به این آدرس اصطلاحاً آدرس SAP گفته می شود مثل شماره PORT.

معماری پروتکلها در شبکه های کامپیوتری

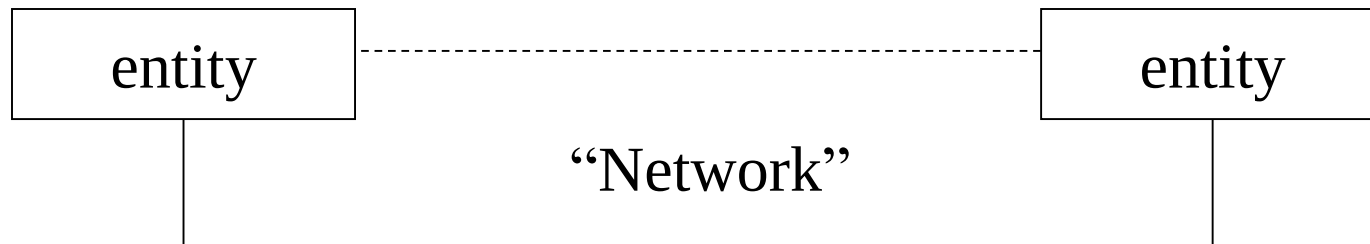
معماری پشته پروتکلهای شبکه بر پایه مدل لایه ای است:

_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.

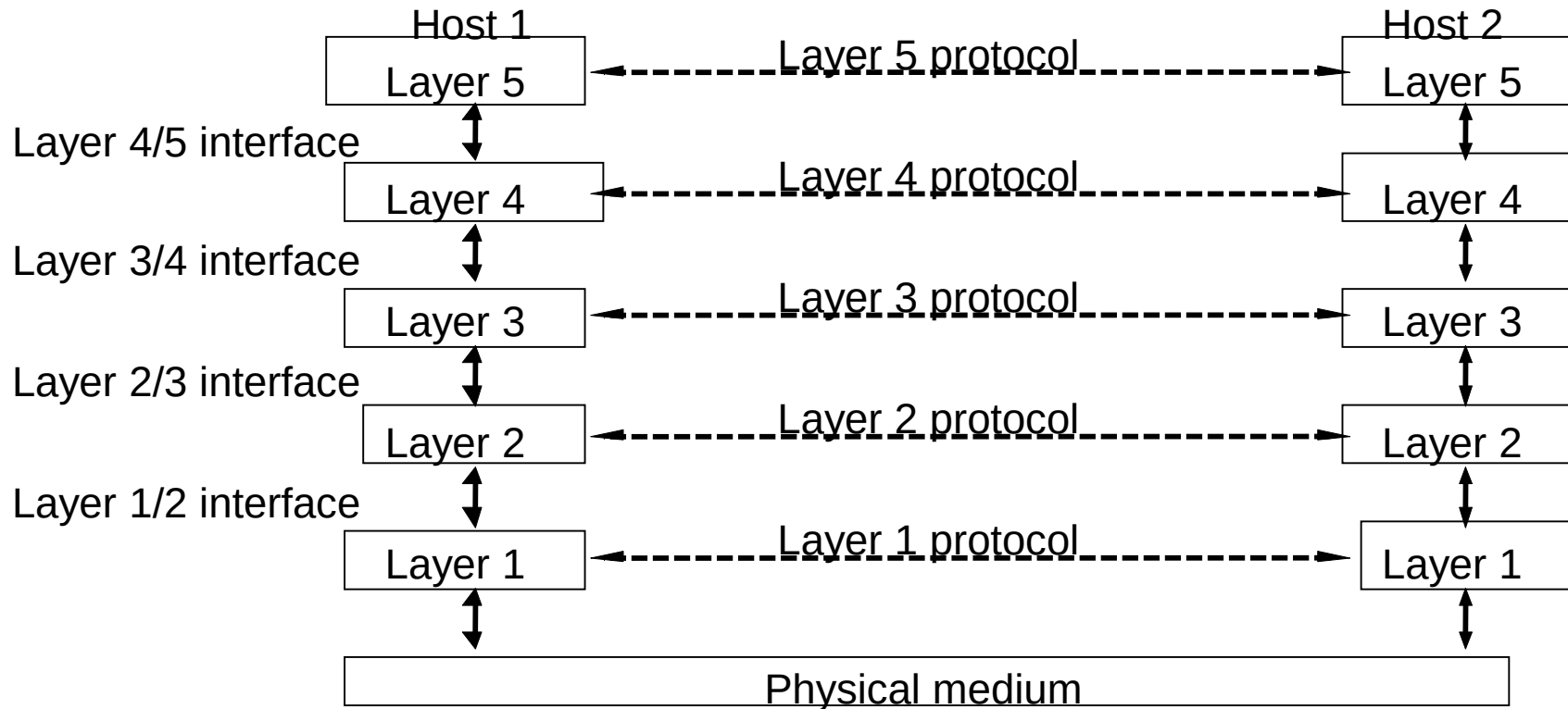


هر entity پیاده سازی یکی از لایه هاست .
در مدل لایه ای هر لایه 3 نوع interface دارد :
Interface با لایه بالا
Interface با لایه پایین
Interface با لایه هم سطح خودش در طرف مقابل

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:

OSI.1

AppleTalk.2

TCP/IP.3

IPX.4

SNA.5

DECNet.6

مدل مرجع OSI

با گسترش شبکه ها و برپایی شبکه هایی با سخت افزار و نرم افزارهای متفاوت نوعی ناسازگاری برای ارتباط و انتقال 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 با وظایف متفاوت وجود دارد.

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

تقسیم وظایف شبکه به لایه ها مزایای زیر را دارد:

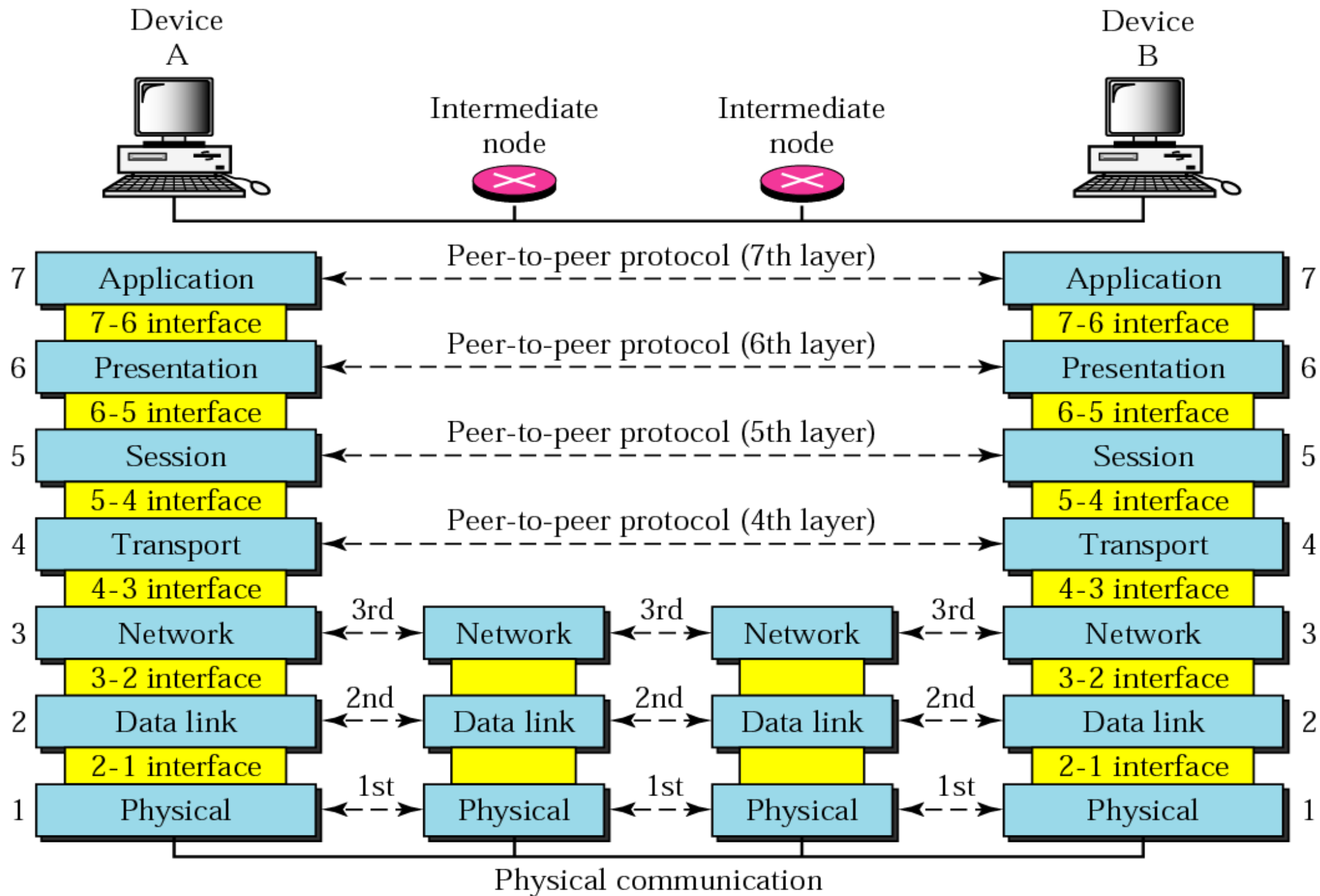
۱- یک شبکه ارتباطی به اجزا کوچک تر و ساده تر تقسیم می شود.

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

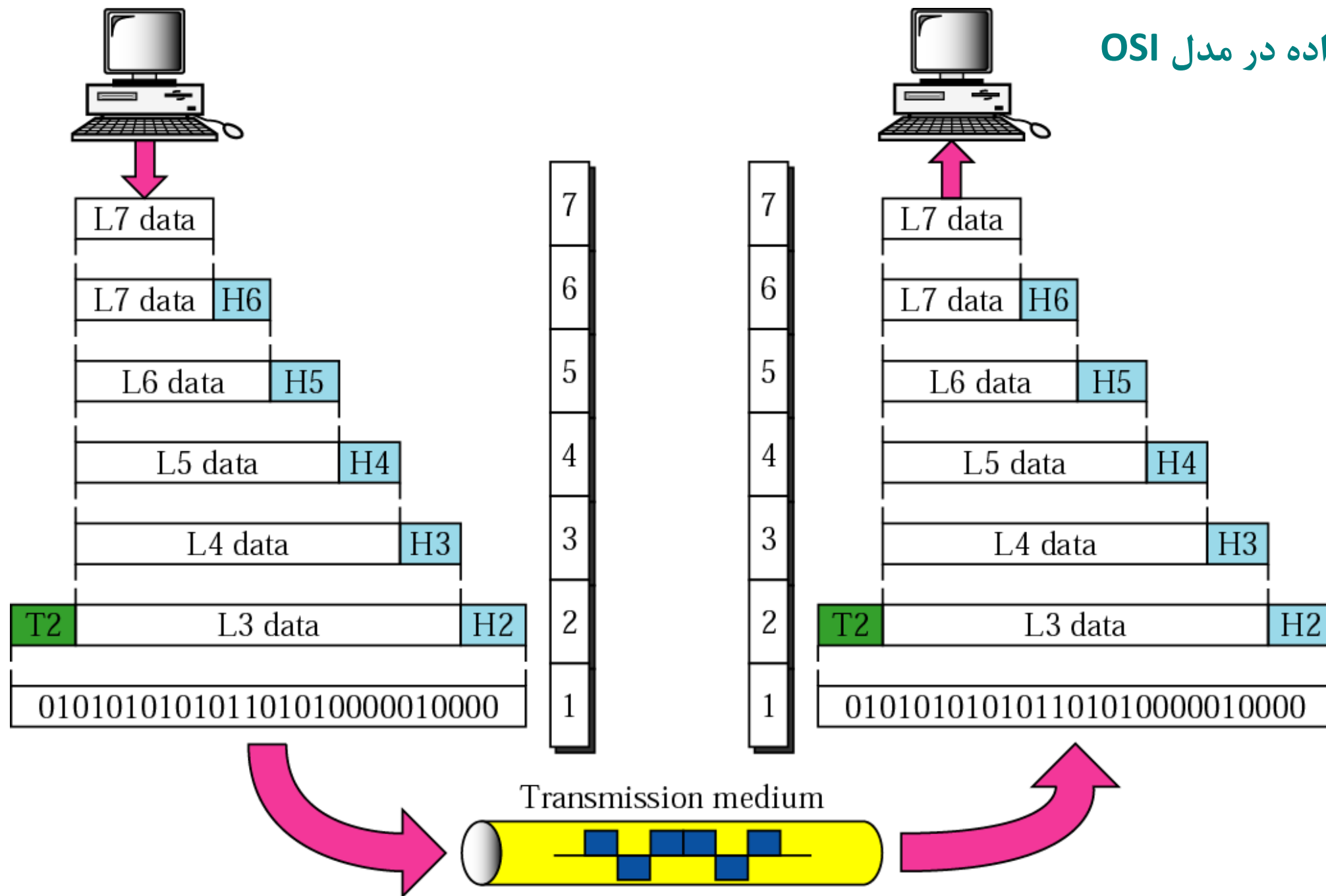
۳- با تقسیم یک شبکه به اجزا کوچک تر فهم آن ساده تر می شود.

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.



تبادل داده در مدل OSI

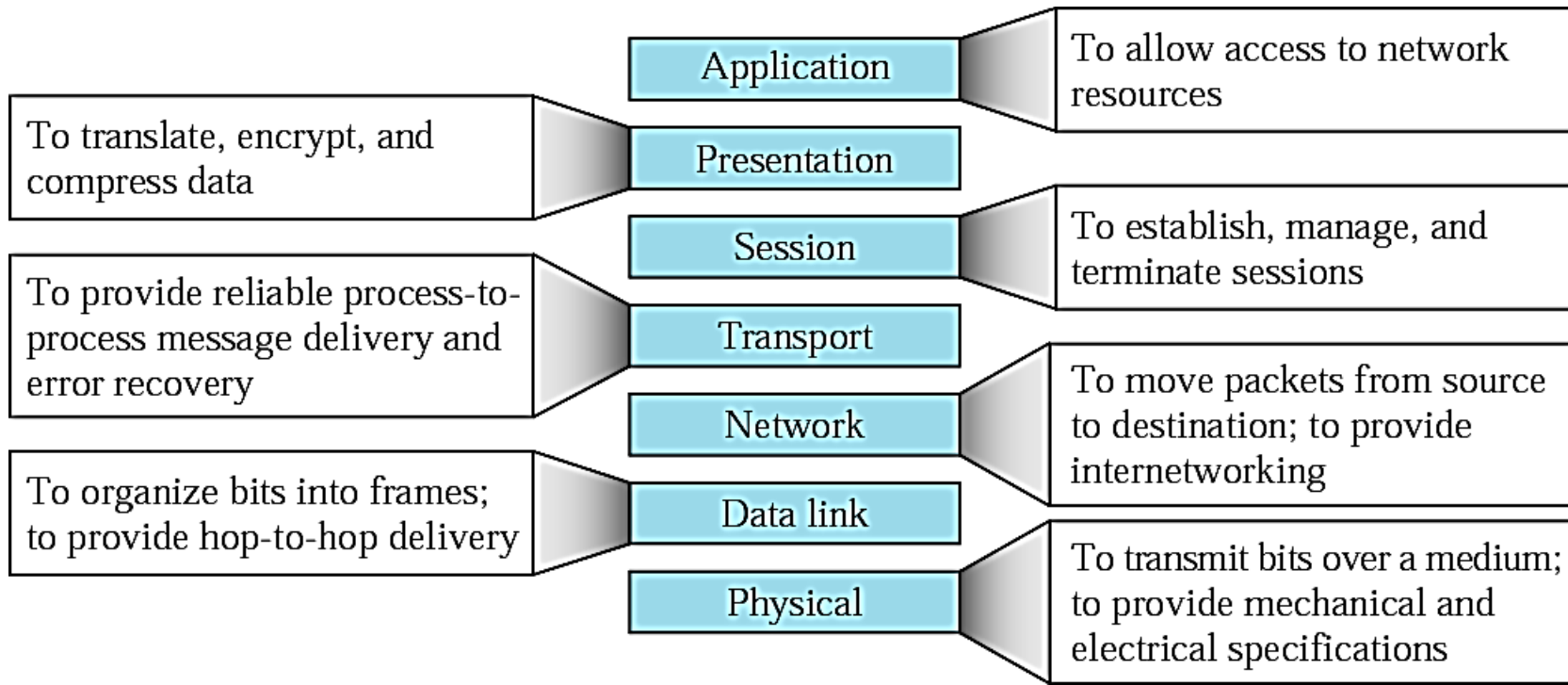


هدرها در لایه های ۲ و ۳ و ۴ و ۵ و ۶ به داده ها اضافه می شوند دنباله ها Trailer فقط در لایه دوم اضافه می شوند.
بخش داده یک بسته در لایه، کل داده دریافتی از لایه بالاتر که شامل اطلاعات و هدرها و دنباله های اضافه شده به آن می باشد را در برمی گیرد. به این عمل کپسوله بندی می گویند.

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 های موجود در لایه های متناظر به انتقال داده می پردازند. این داده ها به نام PDU واحد داده پروتکل نامیده می شوند.

PDU در لایه های ۵، ۶، ۷ پیغام نام دارد و در لایه انتقال قطعه segment و در لایه سوم بسته packet و در لایه دوم قاب یا فریم Frame نامیده می شود.



لایه ها در مدل OSI

لایه فیزیکی

وظیفه اصلی این لایه انتقال بیتها بر روی کانال مخابراتی است. در این لایه واحد اطلاعات بیت است و این واحد هیچ درکی از محتوی پیام ندارد. تنها چیزی که متوجه می شود بیتهای صفر و یک می باشد.

لایه فیزیکی مسئول جابجایی بیت ها از یک گره به گره بعدی است.

لایه فیزیکی به موارد دیگر هم رسیدگی می کند:

۱- تعیین نوع محیط فیزیکی و رابط بین وسایل و محیط انتقال.

۲- نمایش بیت ها: داده لایه فیزیکی دنباله ای از بیت ها است.

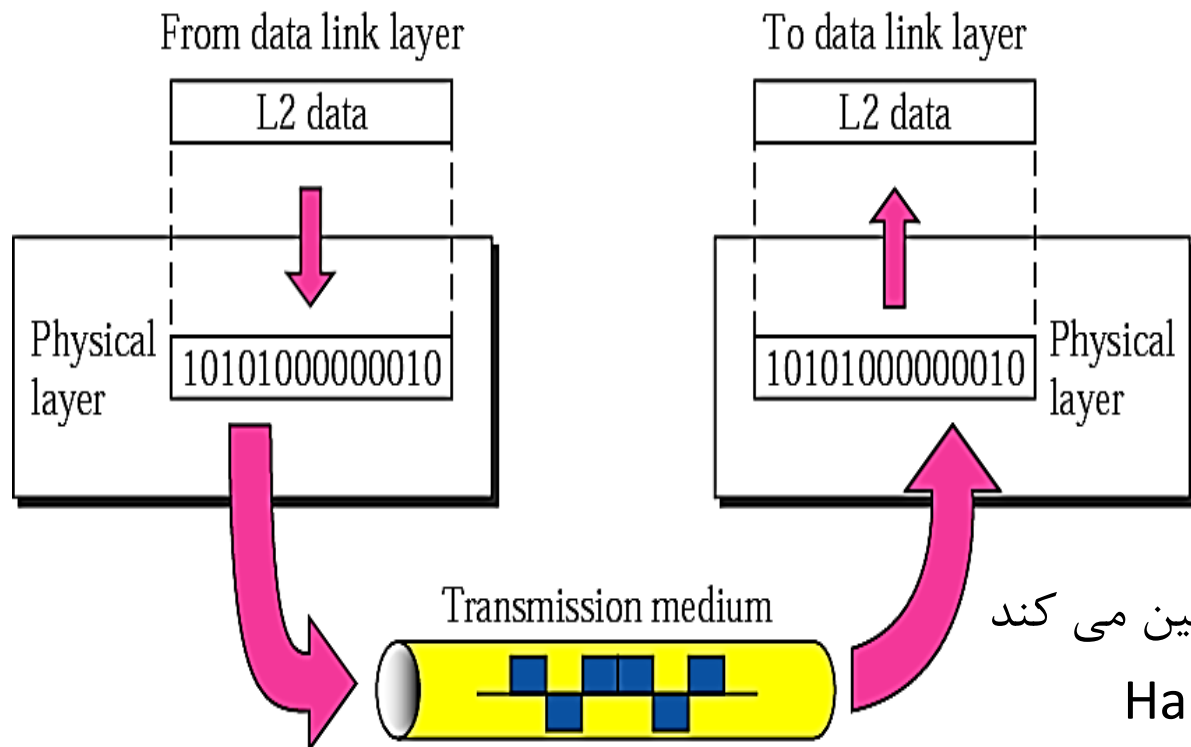
برای انتقال بیتها باید آنها را به صورت سیگنال الکتریکی یا نوری درآورد. چگونگی تبدیل صفرها و یک ها به سیگنال را سیگنال سازی یا Encoding می گویند.

۳- نرخ بیت: تعداد بیتی که در هر ثانیه ارسال می شود.

۴- حالت انتقال: لایه فیزیکی جهت انتقال اطلاعات بین دو وسیله را تعیین می کند

که می تواند به صورت یک طرفه simplex، نیمه دو طرفه Half duplex

یا کاملاً دو طرفه Full duplex باشد.



پارامترهای مطرح در لایه فیزیکی

- ماهیت فیزیکی خط انتقال
- چگونگی نمایش بیتها در قالب سیگنالی متناسب با کانال
- ظرفیت کانال فیزیکی و نرخ ارسال
- نوع مدولاسیون
- چگونگی کوپلاژ فرستنده و گیرنده
- مسائل مکانیکی و الکتریکی

لایه پیوند داده

وظیفه این لایه آن است که با استفاده از مکانیزمهای کشف و کنترل خطا داده ها را روی یک کانال انتقال که بدلیل وجود نویز ذاتا دارای خطاست بدون خطا و مطمئن به مقصد برساند.

ماهیت خطا به گونه ایست که قابل رفع نیست ولی می توان تدابیری وجود دارد که از سلامت داده ها اطلاع یابد و داده های خراب را دور بریزد

1. با استفاده از Parity

2. Checksum

3. CRC

رسیدن و یا نرسیدن اطلاعات نیز از زمره وظایف این لایه است

آدرس دهی فیزیکی، تعیین نحوه دسترسی به رسانه و مدیریت کانال وظیفه این لایه است. لایه فیزیکی به کمک این لایه به یک لینک ارتباطی قابل اطمینان تبدیل می شود.

سایر وظایف لایه پیوند داده:

1. کنترل جریان flow control

2. کنترل خطا error control

3. کنترل دسترسی: وقتی که دو یا چند وسیله به لینک مشترکی متصل می شوند باید مشخص شود در هر لحظه چه کسی می تواند از آن لینک استفاده کند.

PDU ارسالی از لایه پیوند داده ها در اصطلاح با اسم خاص "فریم" یا "قاب" گفته می شود.

از وظایف لایه پیوند داده مقابله با تصادم است از جمله قرارداد هایی که در این لایه قرار داده شده زیر لایه MAS است که در اصطلاح آن را لایه دو و نیم نیز می نامند.

راه اندازی سرویس گیری و کنترل سخت افزار در لایه فیزیکی بر عهده لایه پیوند داده است و در سطح سخت افزار صورت می گیرد.

لایه شبکه

این لایه مسئول تحویل بسته های اطلاعات از ماشین مبدا در یک شبکه به ماشین مقصد در شبکه دیگر است.

آدرس دهی منطقی، کنترل ازدحام (congestion control)، مسیریابی بین کامپیوترهای فرستنده و گیرنده، تحویل داده به گیرنده به صورت نامطمئن از وظایف این لایه است.

مهمترین وظیفه این لایه مسیریابی است هرگاه یک قطعه داده دارای هویت و شناسنامه تحویل این لایه شود ابتدا باید مشخص گردد که مقصد نهایی آن همین ماشین است و محتوی بسته باید تحویل لایه بالاتر گردد یا برای رسیدن به مقصد نهایی خود از طریق کانال دیگری به بیرون ارسال گردد.

در این لایه داده های دریافتی از لایه بالاتر باید در قالب بسته هایی با ساختار استاندارد سازماندهی شود (Packet) با توجه به آنکه مسیرهای گوناگونی وجود دارد. لذا این لایه وظیفه دارد هر بسته اطلاعاتی را پس از دریافت به مسیری هدایت کند تا آن بسته به مقصد برسد.

لایه انتقال

این لایه مسئول تحویل پیغام از برنامه مبدا به برنامه مقصد است.

لایه شبکه یک بسته اطلاعاتی را به ماشین مقصد می رساند و لایه انتقال کل پیغام را به برنامه مقصد (در ماشین مقصد) می رساند.

ارائه سرویس برای تحویل داده به صورت مطمئن همراه با کشف خطای انتقال کنترل جریان داده، شکستن و قطعه قطعه کردن اطلاعات و شماره گذاری آنها برای این که قطعه ای گم نشود یا دوباره دریافت نشود از وظایف این لایه است.

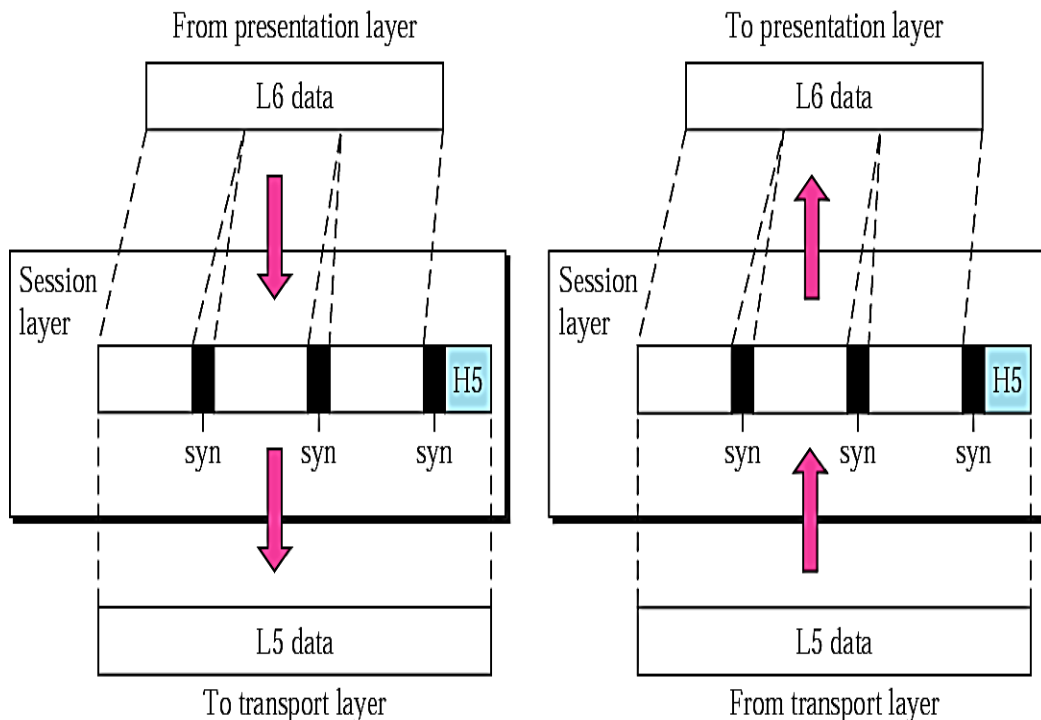
لایه انتقال می تواند اتصال گرا (connection-oriented) یا فاقد اتصال (connectionless) باشد.

گرفتن داده از لایه های بالاتر و تقسیم آن به قطعات کوچکتر و ارسال آن به لایه شبکه و حصول اطمینان از دریافت صحیح آنها.
ایزوله کردن لایه های بالاتر در برابر تغییرات اجتناب ناپذیر سخت افزاری
این لایه اولین لایه است که لایه های همتا با هم ارتباط نظیر به نظیر با یکدیگر برقرار می کنند.

لایه جلسه کاری session

ایجاد، مدیریت و اتمام جلسه بین دو کامپیوتر، همزمان سازی تبادل داده بین فرستنده و گیرنده با قرار دادن نقاط واری از وظایف این لایه است.

این لایه به اجازه می دهد تا کاربران در ماشینهای مختلف نشست برقرار شود.



1. کنترل دیالوگ Dialog control اینکه نوبت چه کسی است
2. مدیریت نشانه token management جلوگیری از تداخل اعمال مهم
3. سنکرون کردن Synchronization کنترل عملیات انتقال طولانی مدت و از سر گیری از نقطه قطع شده

لایه نمایش

تبدیل کدهای مختلف داده (ترجمه)

رمزگذاری داده در سمت فرستنده و رمزگشایی آن در سمت گیرنده

فشرده سازی داده و از حالت فشرده خارج کردن از وظایف این لایه است. در این لایه تمرکز بر روی ساختار و مفهوم پیام است کامپیوترهایی که دارای ساختار متفاوت هستند برای آنکه بتوانند با یکدیگر ارتباط برقرار کنند باید بر روی ساختار پیام به صورت مشخص و استاندارد توافق کنند که از وظایف لایه نمایش مدیریت این ساختارها در سطح بالاست

لایه کاربرد

این لایه سرویس های شبکه ای لازم را برای برنامه های کاربردی و کاربران فراهم می کند.

برنامه های مرورگر وب، ایمیل، انتقال فایل و ... در این لایه قرار دارند.

با وجود مشخص شدن وظایف هر لایه مدل OSI یک معماری شبکه نیست زیرا پروتکل های آن پیاده سازی نشده اند. بسیاری از پروتکل های مورد نیاز کاربران در لایه کاربرد قرار دارد نظیر

HTTP

FTP

SMTP,POP3

NNTP

پشته پروتکلی TCP/IP

پشته پروتکل TCP/IP قبل از مدل OSI ساخته شد به همین لایه های پشته پروتکل TCP/IP منطبق با لایه های مدل OSI نیستند.

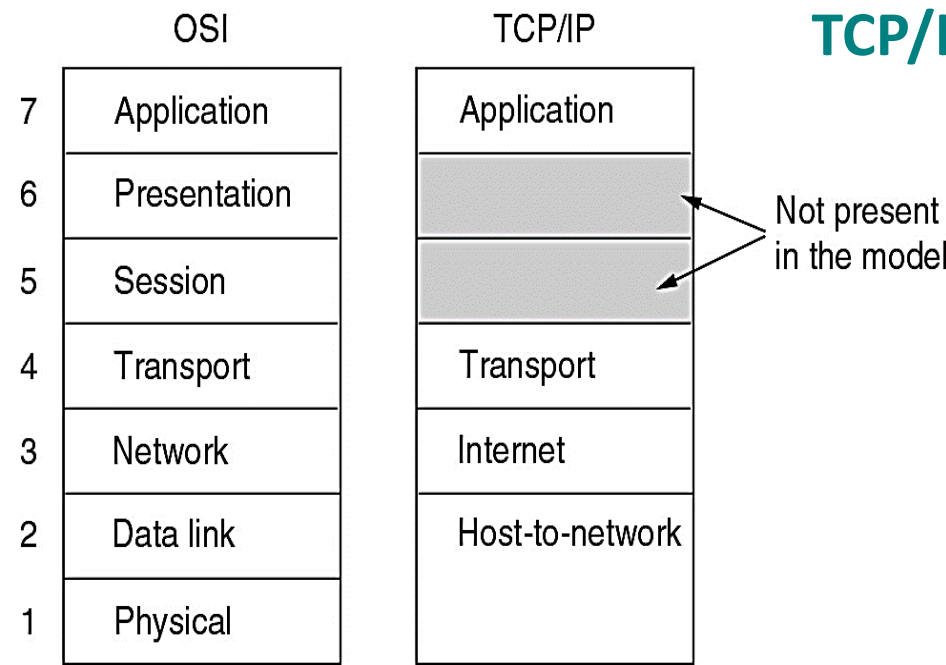
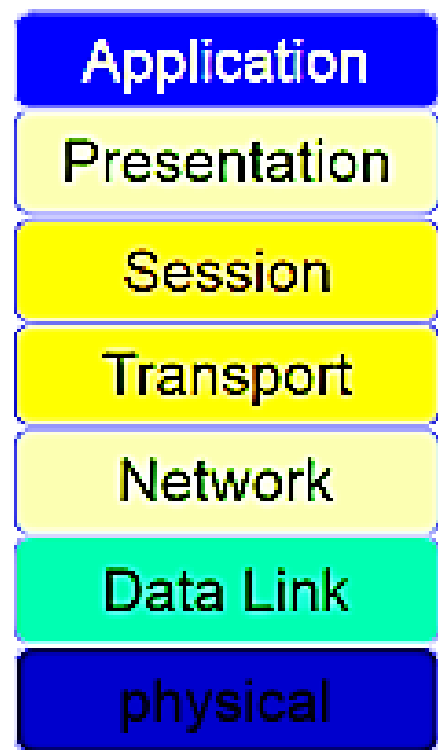
وزارت دفاع آمریکا این مدل را به عنوان مدل مرجع ایجاد کرد چون به شبکه ای نیاز داشت تا تحت هر شرایطی حتی جنگ هسته ای پایدار بماند.

پشته پروتکل TCP/IP از ۴ لایه ساخته شده است: فیزیکی، پیوند داده، شبکه انتقال و کاربرد.

این پشته از ماجول هایی ساخته شده که کدام کار خاصی را انجام می دهد.

ماجول ها به هم وابسته نیستند اما با هم کار می کنند.

مدل مرجع TCP/IP



لایه کاربرد: پیاده سازی پروسه های کاربردی در میزبانها.
لایه حمل: ارسال انتها به انتهای مطمئن بین پروسه های کاربردی.
لایه شبکه: آدرس دهی در سطح شبکه و مسیریابی.
لایه میزبان شبکه: آدرس دهی ترمینالها در سطح شبکه محلی وساخت فریم های مناسب فضای انتقال فیزیکی و کنترل دسترسی به فضای انتقال.
لایه فیزیکی: سخت افزار و تجهیزات فیزیکی مخابرات داده.

در مدل پنج لایه TCP/IP سه لایه بالای مدل OSI با هم ترکیب شده اند. لایه اینترنت internet layer

انتخاب در این لایه ، یک شبکه Packet switching مبتنی بر ارتباط غیر متصل انتخاب شد در واقع این لایه سنگ بنای معماری TCP/IP است .
وظیفه اصلی این لایه اینست که به ماشینها اجازه دهد بسته های خود را روی شبکه و به سمت مقصد بفرستد.
این لایه رسیدن بسته ها را به سمت مقصد تضمین نمی کند.
پیامها را مرتب نمی کند و این وظیفه به عهده لایه های بالاتر است.
فرمت بسته ها در این لایه به صورت IP تعریف می شود.(Internet Protocol)

لایه انتقال

وظایف این لایه مشابه وظایف لایه انتقال مدل OSI است .
انتقال به صورت نقطه به نقطه صورت می گیرد.
دو پروتکل اصلی در این مدل وجود دارد

1. TCP (Transmission Control Protocol)

2. UDP (User Datagram Protocol)

وظایف مشترک بین لایه های مدل مرجع اینترنت

مالتی پلکس کردن

کنترل خطا

کنترل استفاده از منابع

همگام سازی بین فرستنده و گیرنده و کنترل جریان ارسال داده

آدرس دهی و نامگذاری به منظور شناسایی پروسه های متناظر

+در سطح لایه ۲ بصورت گره به گره

+در سطح لایه ۳ بصورت ترمینال به ترمینال

+در سطح لایه ۴ و ۵ بصورت نرم افزار به نرم افزار

تفاوت ها و شباهت های ما بین OSI و TCP/IP

✓ هر دو مدل به صورت لایه ای طراحی شده اند.

✓ هر دو لایه دارای لایه های انتقال و شبکه شبیه یکدیگر هستند.

✓ هر دو از تکنولوژی سوئیچ بسته استفاده می کنند.

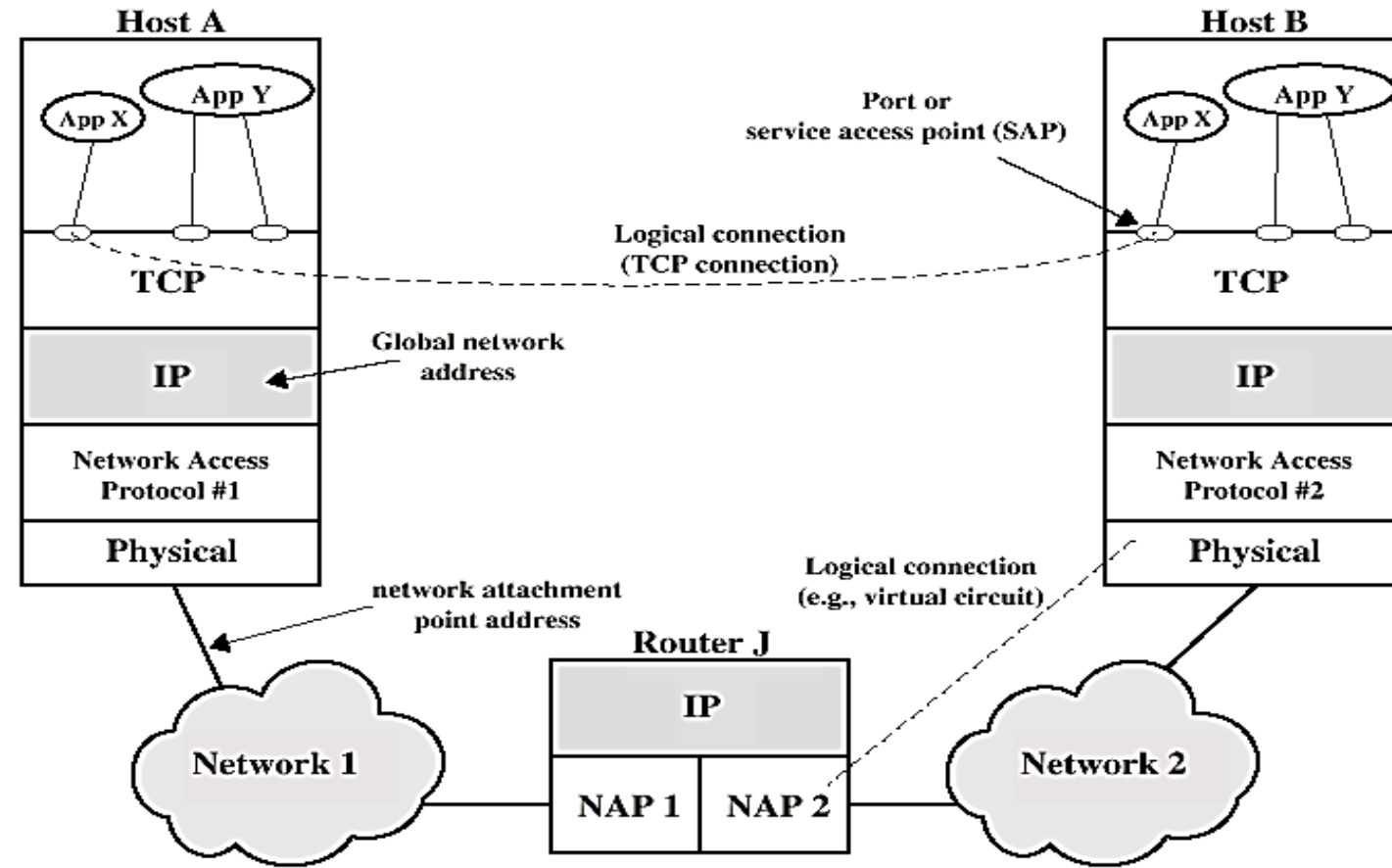
✓ تفاوت های دو مدل:

✓ مدل TCP/IP لایه ارائه و جلسه OSI را در لایه کاربردی ادغام کرده است.

✓ مدل TCP/IP لایه پیوند داده و فیزیکی را در یک لایه قرار داده است.

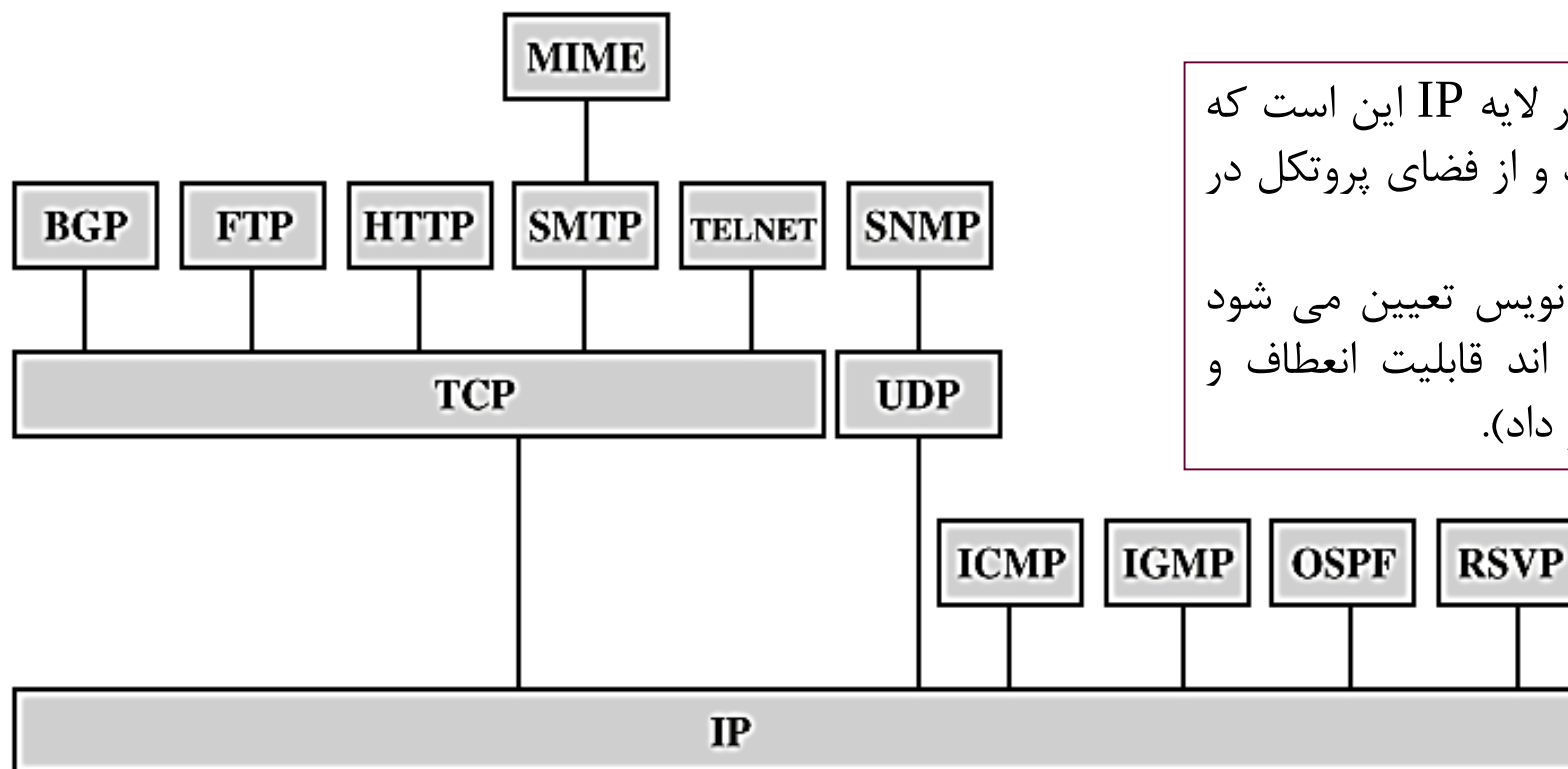
✓ TCP/IP به علت تعداد لایه های کمتر ساده تر به نظر می رسد.

✓ پروتکل TCP/IP استاندارد اینترنت است در حالی که اکنون از پروتکل های SNA (پیاده سازی OSI) استفاده نمی شود.



پروتکلها در اینترنت

در شکل زیر تعدادی از پروتکل‌های مورد استفاده در لایه های مختلف در اینترنت نشان داده شده اند:



علت قرار گرفتن ICMP, IGMP, OSPF, RSVP در لایه IP این است که برای این پروتکل ها port number تعریف نمی شود و از فضای پروتکل در هدر IP استفاده می کنند .

با توجه به اینکه port number ها توسط برنامه نویس تعیین می شود سایر پروتکل های کاربردی در TCP قرار گرفته اند قابلیت انعطاف و گسترش مناسبی دارند. (اینها را نمی توان در IP قرار داد).

از پروتکل‌های مورد استفاده در شبکه های کامپیوتری می توان به TCP, IP, UDP, HTTP, FTP, BGP و RSVP اشاره کرد.

BGP = Border Gateway Protocol
FTP = File Transfer Protocol
HTTP = Hypertext Transfer Protocol
ICMP = Internet Control Message Protocol
IGMP = Internet Group Management Protocol
IP = Internet Protocol
MIME = Multi-Purpose Internet Mail Extension

OSPF = Open Shortest Path First
RSVP = Resource ReSerVation Protocol
SMTP = Simple Mail Transfer Protocol
SNMP = Simple Network Management Protocol
TCP = Transmission Control Protocol
UDP = User Datagram Protocol

پروتکل IP

Internet Protocol

مدل Best Effort بر مبنای روش دیتاگرام برای ارسال بسته ها از مبدا به مقصد

مسیریابی بر اساس آدرسهای ۳۲ بیتی IP

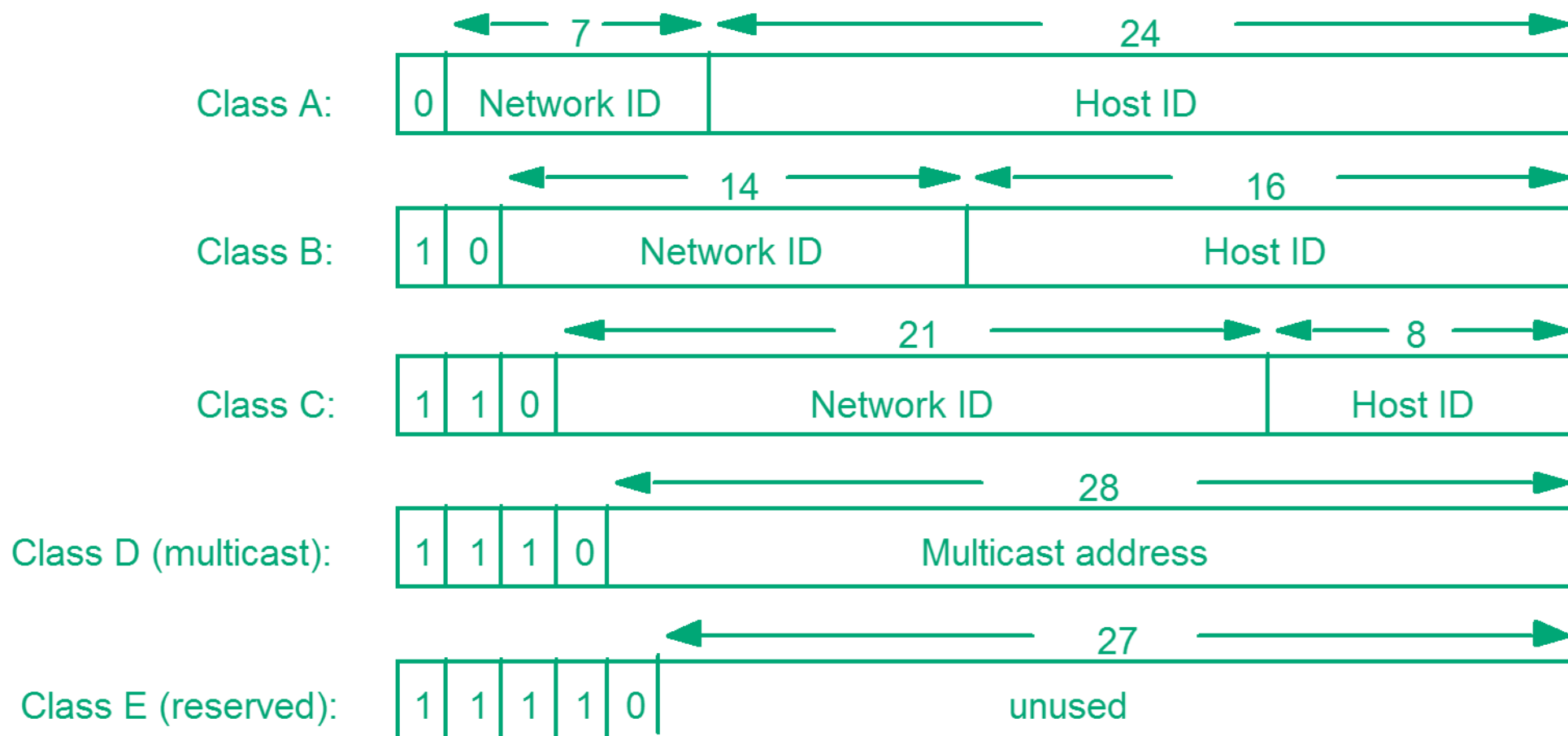
فرمت بسته های IP بشکل زیر است:

0	4	8	16	19	24	31
VERS	H. LEN	SERVICE TYPE	TOTAL LENGTH			
IDENTIFICATION			FLAGS	FRAGMENT OFFSET		
TIME TO LIVE		TYPE	HEADER CHECKSUM			
SOURCE IP ADDRESS						
DESTINATION IP ADDRESS						
IP OPTIONS (MAY BE OMITTED)					PADDING	
BEGINNING OF DATA ⋮						

IP - بیست و یک بیت سرآمد ثابت با اضافه یک بخش با طول متغیر به بسته اضافه می کند.

آدرس دهی در اینترنت

چهار نوع آدرس A، B، C، D در اینترنت استفاده می شود که با پیشوندهای مختلف از هم مشخص می شوند:



در حال حاضر برای آنکه فضای آدرس بصورت قابل انعطاف و با راندمان بیشتری استفاده شود، نوع classless استفاده می شود. در این نوع، بخش network ID در آدرس از این قواعد پیروی نمی کند و می تواند هر طول دلخواهی داشته باشد (مقدار حداقل آن ۲ بیت و مقدار حداکثر آن به طول بخش host ID بستگی دارد).

پروتکل TCP

یک پروتکل اتصال گرا است قابل اعتماد است (Connection Oriented Best Effort) است. پروتکل IP یک سرویس connectionless غیر قابل اتکا ارائه می کند. پروتکل TCP بر روی IP قرار گرفته و با اجرای الگوریتم پنجره لغزان یک سرویس connection-oriented قابل اتکا reliable به لایه بالای خود ارائه می کند.

اجازه می دهد تا جریانی از بایتها بدون خطا از یک کامپیوتر به کامپیوتر دیگر فرستاده شود. جریان بایت را به صورت بسته در آورده و به لایه اینترنت تحویل داده می شود. در ماشین مقصد این پروتکل بسته ها را به یکدیگر الحاق کرده تا جریانی از بیتها را بدست آورد. کنترل جریان داده نیز در این لایه صورت می گیرد و فرستنده سریع سرعت خود را با گیرنده کند هماهنگ می کند.

