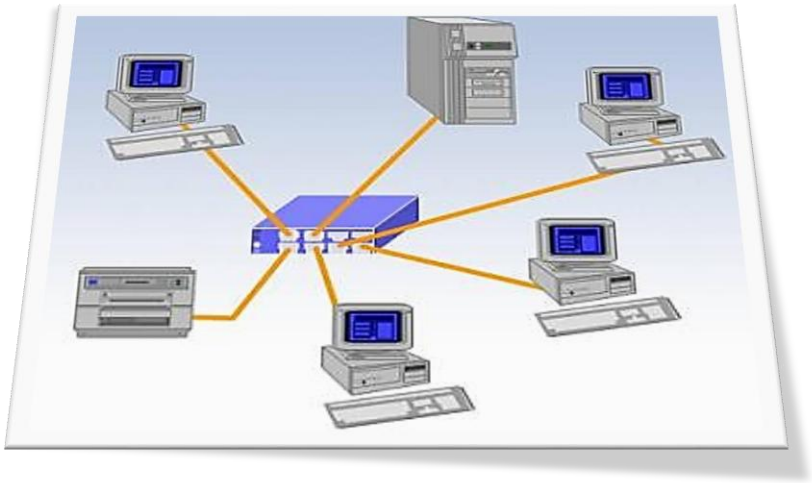
موسسه آموزش عالی کوشیار رشت



شبکه های محلی کامپیوتر

مدرس :مهندس علی زواره

۱۳۹۴

فهرست عنوان ها

تاریخچه پیدایش شبکه

در سال ۱۹۵۷ نخستین ماهواره، یعنی اسپوتنیک توسط اتحاد جماهیر شوروی سابق به فضا پرتاب شد. درهمین دوران رقابت سختی ازنظر تسلیحاتی بین دو ابرقدرت آن زمان جریان داشت و دنیا در دوران رقابت سختی ازنظر تسلیحاتی بین دو ابر قدرت آن زمان جریان داشت و دنیا در دوران جنگ سرد به سر می برد.وزارت دفاع امریکا در واکنش به این اقدام رقیب نظامی خود، آژانس پروژه های تحقیقاتی پیشرفته یا آرپا (ARPA) را تاسیس کرد. یکی از پروژه های مهم این آژانس تامین ارتباطات در زمان جنگ جهانی احتمالی تعریف شده بود. در همین سال ها در مراکز تحقیقاتی غیر نظامی که بر امتداد دانشگاه ها بودند. تلاش برای اتصال کامپیوترها به یکدیگر در جریان بود.

در آن زمان کامپیوتر های Mainframe از طریق ترمینال ها به کاربران سرویس می دادند. در اثر اهمیت یافتن این موضوع آژانس آرپا (arpa)منابع مالی پروژه اتصال دو کامپیوتر از راه دور به یکدیگر را در دانشگاه mit برعهده گرفت. در اواخر سال ۱۹۶۰ اولین شبکه کامپیوتری بین چهار کامپیوتر که دو تای آنها درmit . یکی در دانشگاه کالیفرنیا و دیگری در مرکز تحقیقاتی استنفورد قرار داشتند، راه اندازی شد. این شبکه آرپانت نامگذاری شد. در سال ۱۹۶۵ نخستین ارتباط راه دور بین دانشگاه mit و یک مرکز دیگر نیز برقرار گردید.

در سال۱۹۷۰ شرکت معتبر زیراکس یک مرکز تحقیقاتی در پالوآلتو تاسیس کرد. این مرکز در طول سال ها مهمترین فناوری های مرتبط با کامپیوتر را معرفی کرده است و از این نظر به یک مرکز تحقیقاتی افسانه ای بدل گشته است. این مرکز تحقیقاتی که پارک (parc) نیز نامیده می شود، به تحقیقات در زمینه شبکه های کامپیوتری پیوست.

تا این سال ها شبکه آرپانت به امور نظامی اختصاص داشت. اما در سال۱۹۷۲ به عموم معرفی شد. در این سال شبکه آرپانت مراکز کامپیوتری بسیاری از دانشگاه ها و مراکز تحقیقاتی را به هم متصل کرده بود. در سال ۱۹۷۲ نخستین نامه الکترونیکی از طریق شبکه منتقل گردید. در این سال ها حرکتی غیر انتفاعی به نام merit که چندین دانشگاه بنیان گذار آن بوده اند. مشغول توسعه روش های اتصال کاربران ترمینال ها به کامپیوتر مرکزی یا میزبان بود. مهندسان پروژه merit در تلاش برای ایجاد ارتباط بین کامپیوترها، مجبور شدند تجهیزات لازم را خود طراحی کنند. آنان با طراحی تجهیزات واسطه برای مینی کامپیوتر decpop-11 نخستین بستر اصلی یا backbone شبکه کامپیوتری را ساختند. تا سال ها نمونه های اصلاح شده این کامپیوتر با نام **pcp** یا primary communications processor نقش میزبان را در شبکه ها ایفا می کرد. نخستین شبکه از این نوع که چندین ایالت را به هم متصل می کرد michnet نام داشت.

روش اتصال کاربران به کامپیوتر میزبان در آن زمان به این صورت بود که یک نرم افزار خاص بر روی کامپیوتر مرکزی اجرا می شد. و ارتباط کاربران را برقرار می کرد. اما در سال ۱۹۷۶ نرم افزار جدیدی به نام Hermes عرضه شد که برای نخستین بار به کاربران اجازه می داد تا از طریق یک ترمینال به صورت تعاملی مستقیما به سیستمMERIT متصل شوند. این، نخستین باری بود که که کاربران می توانستند در هنگام برقراری ارتباط از خود بپرسند:کدام میزبان؟

از وقایع مهم تاریخچه شبکه های کامپیوتری، ابداع روش سوئیچینگ بسته ای یاPacket switching است. قبل از معرفی شدن این روش از سوئیچینگ مداری یا Circuit Switching برای تعیین مسیر ارتباطی استفاده می شد. اما در سال ۱۹۷۴ با پیدایش پروتکل ارتباطی tcp/ip از مفهوم Packet switching استفاده گسترده تری شد. این پروتکل در سال ۱۹۸۲ جایگزین پروتکل ncp شد و به پروتکل استاندارد برای آرپانت تبدیل گشت. در همین زمان یک شاخه فرعی بنام MILnet در آرپانت همچنان از پروتکل قبلی پشتیبانی می کرد و به ارائه خدمات نظامی می پرداخت.

با این تغییر و تحول، شبکه های زیادی به بخش تحقیقاتی این شبکه متصل شدند و آرپانت به اینترنت تبدیل گشت. در این سال ها حجم ارتباطات شبکه ای افزایش یافت و مفهوم ترافیک شبکه مطرح شد. مسیریابی در این شبکه به کمک آدرس هایIP به صورت۳۲ بیتی انجام می گرفت. هشت بیت اول آدرس IP به شبکه های محلی تخصیص داده شده بود که به سرعت مشخص گشت تناسبی با نرخ رشد شبکه ها ندارد و باید در آن تجدید نظر شود. مفهوم شبکه های LAN و شبکه

های WAN در سال دهه ۷۰ میلادی از یکدیگر تفکیک شدند. در آدرس دهی۳۲ بیتی، بقیه ۲۴ بیت آدرس به میزبان در شبکه اشاره می کرد. در سال ۱۹۸۳ سیستم نامگذاری دامنه ها (Domain Name System) به وجود آمد و اولین سرویس دهنده نامگذاری (NAME SERVER) راه اندازی شد و استفاده از نام به جای آدرس های عددی معرفی شد. دراین سال تعداد میزبان های اینترنت از مرز ده هزار عدد فراتر رفته بود.

دلایل استفاده از شبکه

۱- استفاده مشترک از منابع :

استفاده مشترک از یک منبع اطلاعاتی یا امکانات جانبی رایانه، بدون توجه به محل جغرافیایی هریک از منابع را استفاده از منابع مشترک گویند.

۲-کاهش هزینه:

متمرکز نمودن منابع و استفاده مشترک از آنها و پرهیز از پخش آنها در واحدهای مختلف و استفاده اختصاصی هر کاربر در یک سازمان کاهش هزینه را در پی خواهد داشت.

۳-قابلیت اطمینان:

این ویژگی در شبکه ها بوجود سرویس دهنده های پشتیبان در شبکه اشاره می کند، یعنی به این معنا که می توان از منابع گوناگون اطلاعاتی و سیستم ها در شبکه نسخه های دوم و پشتیبان تهیه کرد و در صورت عدم دسترسی به یک از منابع اطلاعاتی در شبکه " بعلت از کارافتادن سیستم " از نسخه های پشتیبان استفاده کرد. پشتیبان از سرویس دهنده ها در شبکه کارآیی،،فعالیت وآمادگی دایمی سیستم را افزایش می دهد.

۴-کاهش زمان :

یکی دیگر از اهداف ایجاد شبکه های رایانه ای، ایجاد ارتباط قوی بین کاربران از راه دور است ; یعنی بدون محدودیت جغرافیایی تبادل اطلاعات وجود داشته باشد. به این ترتیب زمان تبادل اطلاعات و استفاده از منابع خود بخود کاهش می یابد.

۵- قابلیت توسعه :

یک شبکه محلی می تواند بدون تغییر در ساختار سیستم توسعه یابد و تبدیل به یک شبکه بزرگتر شود. در اینجا هزینه توسعه سیستم هزینه امکانات و تجهیزات مورد نیاز برای گسترش شبکه مد نظر است.

۶- ارتباطات :

کاربران می توانند از طریق نوآوریهای موجود مانند پست الکترونیکی و یا دیگر سیستم های اطلاع رسانی پیغام هایشان را مبادله کنند، حتی امکان انتقال فایل نیز وجود دارد .

تعریف پروتکل

عبارت است ازایجاد زبان مشترک جهت ارتباط بین کامپیوترها و صرف نظر از نوع سخت افزار،سیستم عامل و نرم افزار کامپیوتر (قراردادی بین چند کامپیوتر که می خواهند با هم ارتباط بر قرار کنند)که باید قرار داد مشترک به کار ببرند.

سیگنال

در شبکه های کامپیوتری برای انتقال ارتباط ممکن است از رسانه های مختلفی استفاده شود بسته به نوع رسانه مورد استفاده اطلاعات می بایست به سیگنال های متناسب طراحی شود .به عنوان مثال اگر رسانه فیبر نوری استفاده کنیم به پالس نوری تبدیل می شود.

نوع رسانه	سیگنالها
سیم مسی	الکتریکی
فیبرنوری	پالت نور
بی سیم	الکترومغناطیسی

سرویس های ارائه شده توسط یک پروتکل

۱- اعلام دریافت بسته(Packet acknowledgment)به این منظور که گیرنده پس از دریافت بسته تصدیق دریافت آن را به فرستنده ارسال می کند.

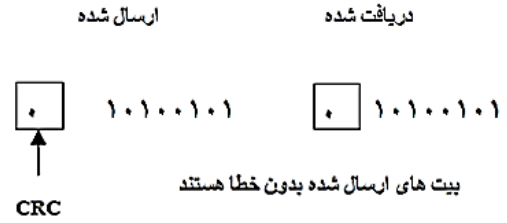
۲- بخش بندی یا تقسیم بندی اطلاعات (Segmentation)عبارتند از تقسیم بندی اطلاعات که فرستنده می خواهد به کامپیوتر گیرنده بفرستد به قسمت های کوچکتر که به این قسمت ها بسته یا Packet می گویند. کنترل جریان یا Flow) (Controlاز این امکان جهت کنترل سرعت ارسال و دریافت بسته ها فرستنده و گیرنده استفاده می شود.

نکته: این امکان می تواندسرعت ارسال کنترل کند یا افزایش یا کاهش یابد.

Header سرآیند یا گیرنده	Packet بسته	Tailer ته آیند یا فرستنده

۳- قابلیت تشخیص خطا (Error Detection): پروتکل می بایست امکانی جهت تشخیص خطا در بسته های ارسالی ودریافتی داشته باشد. تا تعیین کند بسته مورد نظر سالم به مقصد رسیده است یا نه.یکی از ساده ترین روش های تشخیص خطا روش CRCمی باشد در این روش بیتهای ارسالی با یکدیگر XORمی شوند و در سمت مقابل گیرنده نیز اطلاعات را XORکرده و با کد CRCدریافتی مقایسه می کند و خطا زا تشخیص می دهد.

A	B	A XOR B
۰	۰	۰
۰	۱	۱
۱	۰	۱
۱	۱	۰



۴- امکان تصحیح خطا یا(Error Correction):در پروتکل می بایست امکانی جهت تصحیح خطا جهت تصحیح خطای احتمال وجود داشته باشد.دراین صورت پروتکل قادر به تشخیص وتصحیح خطا می باشد.یکی از روشهای **تشخیص خطا کد همیلتون** می باشد.

۵- فشرده سازی داده ها(Data Compression):پروتکل می بایست امکاناتی جهت حذف اطلاعات تکراری در داده ارسالی داشته باشد به این منظور که تا حد امکان حجم اطلاعات ارسالی را کم کند.

۶- کد گذاری یا رمز نگاری داده(Data Encryption):پروتکل می بایست دارای امکاناتی جهت محافظت داده ها در مقابل دسترسی غیر مجازی باشد یکی از مهمترین روشهای این کار رمز نگاری داده ارسالی است.

نحوه طراحی یک پروتکل

به طور کلی برای طراحی یک سیستم روشهای مختلفی وجود دارد که عبارتند از:

۱- طراحی ماژولار

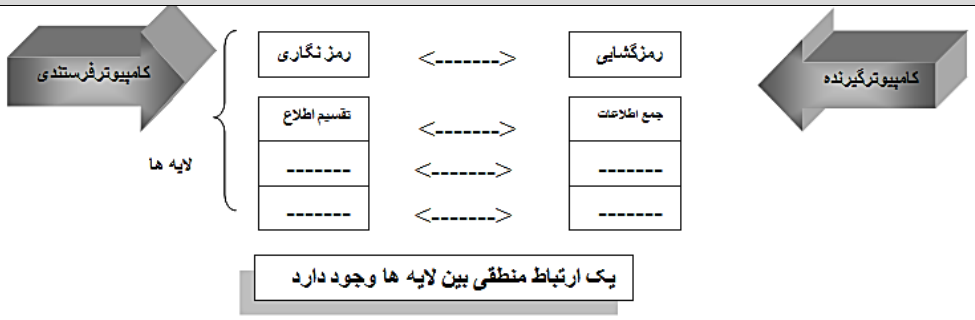
۲- طراحی لایه ای

۳- طراحی کلاینت سرور

در طراحی پروتکل از روش طراحی لایه ای استفاده می شود به این صورت که هر کدام از لایه ها وظیفه خاصی از سرویس های پروتکل را بر عهده گرفته و انجام می دهد . در این روش هیچکدام از لایه ها قادر به انجام وظایف لایه دیگر نیستند.

همچنین ارتباط بین لایه ها با کمترین داده قابل تبادل انجام می شود در هر دو سمت گیرنده و فرستنده می بایست از تعداد لایه های مشابهی استفاده شود هر لایه در گیرنده عکس عمل انجام شده در فرستنده را انجام می دهد .

نکته: تعداد لایه های پروتکل در دریافت ودر ارسال باید با هم برابر باشد.



انواع شبکه ها:

شبکه پهن باند(Broad Band) وشبکه تک باند(Base Band):

همان طور که می دانید در ارسال اطلاعات داده ها به قسمتهای کوچکتر به نام بسته یا Packet تقسیم می شود درشبکه های تک باند در هر لحظه تنها یکی از این (سیگنال) Packetدرحال انتقال می باشد مثل شبکه اینترنت ،ولی در شبکه های پهن باند می توان در هر لحظه چندین Packetرا ارسال کرد .به عنوان مثال در شبکه های تلویزیونی می توان علاوه بر دریافت هم زمان چند برنامه تلویزیونی از اینترنت هم استفاده کرد. از شبکه های پهن باند هیچگاه در شبکه های LANاستفاده نشده اما به عنوان راه حلی جهت ارسال اطلاعات در شبکه های Wan مورد توجه متخصصین قرار گرفته است.

انواع روشهای برقراری ارتباط

۱. سوئچینگ مداری (Circuit Switching)
۲. سوئچینگ پیام(Message Switching)
۳. سوئچینگ بسته یا سلول(Packet OR Cell Switching)

سوئیچینگ مداری (Circuit Switching)

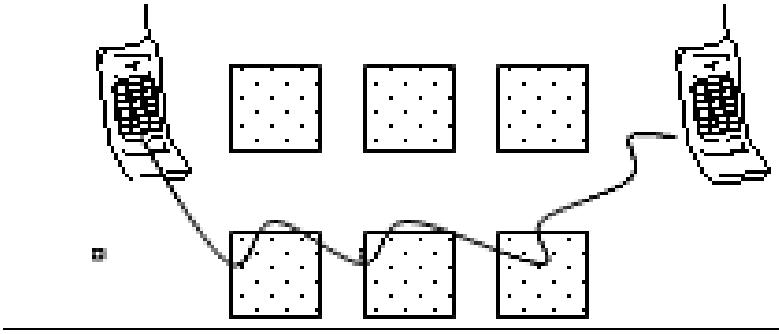
روشی است که در آن بین دو ماشین یک اتصال فیزیکی دائم وجود دارد و ماشین از این رسانه فیزیکی برای تبادل و انتقال اطلاعات استفاده می نمایند . مانند : بسترهای تلفن مخابرات (انتقال صدا) بدین ترتیب خطوط ارتباطی گیرنده و فرستنده از

نظر الکتریکی به هم متصل بوده و یک مدار بسته وجود دارد . در عمل سوئیچینگ برای برقرار شدن ارتباط نیاز به یک عمل شماره گیری داریم . در سیستم های Digitalاین عمل توسط چند رله انجام می شود .

حال ممکن است سوالی پیش آید مبنی بر اینکه آیا این روش سوئیچینگ برای شبکه قابل استفاده می باشد یا خیر ؟

به علت وجود شماره گیری این گونه از سوئیچینگ برای شبکه های کامپیوتری استفاده نمی شود ، زیرا عمل شماره گیری باعث تلف شدن زمان شده و برخی از داده ها منتقل نمی شوند .

در روش سوئیچینگ مداری بین دو نود که یک مسیر ارتباطی دارد نمی توانیم ماشین های دیگر را متصل کنیم. وتا زمان بسته بودن این کانال ارتباطی این عمل مقدورنمی باشد.



سوئیچینگ مدراری به دلایل زیر در شبکه های کامپیوتر ی استفاده نمی شود :

- شماره گیری (اتلاف وقت)
- بسته بودن مسیر ارتباطی و در صورت باز بودن هم یک Node می تواند با یک Node دیگر ارتباط برقرار کند
- اتصال فیزیکی همیشه باید برقرار باشد
- خطوط انتقال سوئیچینگ مداری صوت (آنالوگ ، پیوسته) است . ولی در شبکه های Digital گسسته می باشد .

سوئیچینگ پیامی (Message Switching)

در این سوئیچینگ که تنها برای انتقال داده استفاده می شود همانند روش سوئیچینگ مداری یک ارتباط ثابت و دائمی با مرکز Switchوجود دارد که در مرکز Switchیک کامپیوتر با تعداد Portهای زیادی قرار داده شده است که وظیفه دارد کلیه ورودی ها و خروجی ها را انجام دهد . "این کامپیوتر مجهز به حافظه اصلی و حافظه جانبی می باشد "

چند نمونه از سوئیچینگ پیام :

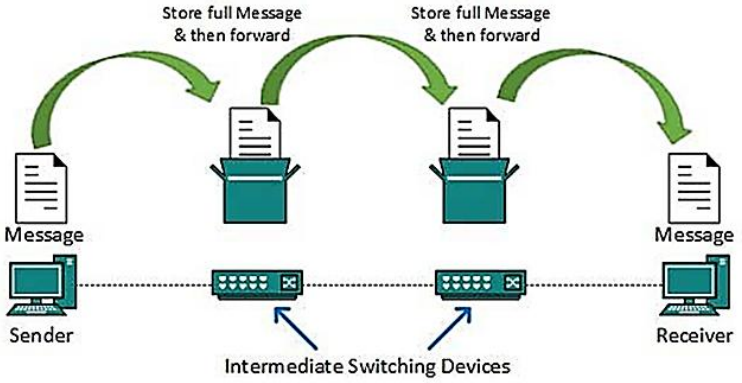
- سیستم انتقال صوت در تلفن همراه
- سیستم انتقال اطلاعات در پیجر

در اینگونه از روشهای سوئیچینگ هر ایستگاه که تمایل به انتقال اطلاعات داشته باشد پس از آماده سازی داده های خود یک شناسنامه به این داده ها اضافه کرده و آنها را در قالب پیام به مرکز سوئیچ (کامپیوتر مرکزی) می فرستد . در این روش هیچ ایستگاهی مجبور نیست قبل از ارسال پیام اقدام به برقراری ارتباط فیزیکی نماید و به محض اینکه داده ها آماده ارسال شد عمل انتقال صورت می پذیرد به همین علت این ایستگاه ها هیچ وقت اشغال نمی باشد .

تذکر : بر خلاف روش های مداری اگر دو پیام از دو ایستگاه متفاوت برای یک ایستگاه واحد ارسال شود هر دو پیام با یک تاخیر زمانی به مقصد تحویل داده می شود . با توجه به نکات بالا روش پیام سریع تر و کارآمدتر از مداری است و اشغال کانال وجود ندارد . در سوئیچینگ پیام مسیر فیزیکی است ولی به جای سوئیچ از کامپیوتر استفاده می شود و با شماره گیری می توانیم اطلاعات را به کامپیوتر بفرستیم وکامپیوتر اطلاعات را به مقصد برساند .

مشکلات سوئیچینگ پیام :

- به دلیل اندازه حافظه و طول پیام
- هر مرکز سوئیچ باید حافظه زیادی داشته باشد
- در صورت خرابی در ارسال بیت های داده امکان ارسال مجدد وجود داشته باشد
- هر مرکز وظیفه دارد کلی پیام را دریافت و سپس آن را به کانال مناسب در خواست شده هدایت نماید .

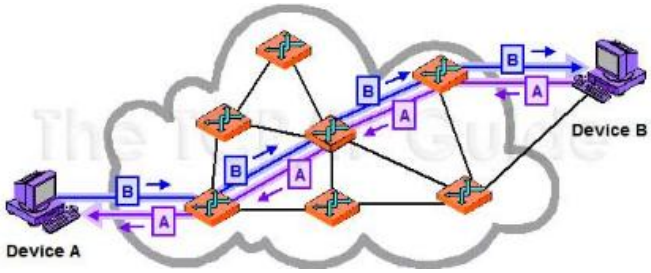


سوئچینگ بسته (Packet OR Cell Switching)

با توجه به مشکلات سوئیچینگ پیام روش دیگری به نام سوئیچینگ بسته یا سلول مطرح می گردد . در سوئیچینگ پیام مشکلاتی نظیر محدودیت پیام یا طول پیام و همچنین کمبود حافظه باعث شده است که روش سلول و بسته مطرح شود .

تعریف سوئیچینگ بسته یا سلول : Packet & Cell

روشی است همانند سوئیچینگ پیام با همان ساختار به طوریکه از یک کامپیوتر در جهت جابه جایی پیام ها و داده ها استفاده می شود . با این تفاوت که ارسال کننده پیام را به اندازه های مساوی و کوچکتر تقسیم می کند و سپس آن ها را ارسال می کند . در سوئیچینگ سلول طول پیام ثابت است . و در شبکه ها استفاده می شود .



انواع ارتباطها

۱- Simplex یکطرفه مثل :رادیو

۲- Half Duplex دوطرفه غیر همزمان: مثل بی سیم

۳- Full Duplex دوطرفه همزمان: مثل تلفن

تقسیم بندی شبکه ها

۱ – براساس نوع اتصال

شبکه های رایانه ای را می توان با توجه به تکنولوژی سخت افزاری و یا نرم افزاری که برای اتصال دستگاه های شبکه استفاده می شود، دسته بندی کرد ;مانند فیبر نوری، اترنت، شبکه بی سیم، ارتباط خط نیرو یا G.hn.

اترنت با استفاده از سیم کشی فیزیکی دستگاه ها را به هم متصل می کند. دستگاه های مستقر معمول شامل هاب ها، سوئیچ ها، پل ها و یا مسیریاب ها هستند.

تکنولوژی شبکه بی سیم برای اتصال دستگاه ها، بدون استفاده از سیم کشی طراحی شده است. این دستگاه ها از امواج رادیویی یا سیگنالهای مادون قرمز به عنوان رسانه انتقال استفاده می کنند.

فناوری IIU-T G.hn از سیم کشی موجود در منازل (کابل هم محور، خطوط تلفن و خطوط برق) برای ایجاد یک شبکه محلی پر سرعت (تا۱ گیگابیت در ثانیه) استفاده می کند.

۲–بر اساس تکنولوژی سیم کشی

۱ – **زوج به هم تابیده(Twisted Pair):** زوج به هم تابیده یکی از بهترین رسانه های مورد استفاده برای ارتباطات راه دور می باشد. سیم های زوج به هم تابیده، سیم تلفن معمولی هستند که از دو سیم مسی عایق که دو به دو به هم پیچ خورده اند درست شده اند. از زوج به هم تابیده برای انتقال صدا و داده ها استفاده می شود. استفاده از دو سیم به هم تابیده به کاهش تداخل و القا الکترومغناطیسی کمک می کند. سرعت انتقال داده، دامنه ای از۲ مگابیت در هر ثانیه تا ۱۰۰ مگابیت در هر ثانیه دارد.

۲– کابل هم محور (Coaxial): کابل هم محور به طور گسترده ای در سیستم های تلویزیون کابلی، ساختمان های اداری، و دیگر سایت های کاری برای شبکه های محلی، استفاده می شود. کابل ها یک رسانای داخلی دارند که توسط یک عایق منعطف محور شده اند، که روی این لایه منعطف نیز توسط یک رسانای نازک برای انعطاف کابل، به هم بافته شده است. همه این اجزا، در داخل عایق دیگری جاسازی شده اند. لایه عایق به حداقل رساندن تداخل و اعوجاج کمک می کند. سرعت انتقال داده، دامنه ای از ۲۰۰ میلیون تا بیش از ۵۰۰ میلیون بیت در هر ثانیه است.

۳–بر اساس تکنولوژی بی سیم

۱–ریز موج(مایکروویو) زمینی: ریز موج های زمینی از گیرنده ها و فرستنده های زمینی استفاده می کنند. تجهیزات این تکنولوژی شبیه به دیش های ماهواره است، مایکروویو زمینی از دامنه های کوتاه گیگاهرتز استفاده می کند، که این سبب می شود تمام ارتباطات به صورت دید خطی محدود باشد. فاصله بین ایستگاههای رله (تقویت سیگنال) حدود۳۰ مایل است. آنتن های ریز موج معمولا در بالای ساختمان ها، برج ها، تپه ها و قله کوه نصب می شوند.

۲– ماهواره های ارتباطی: ماهواره ها از ریز موج های رادیویی که توسط جو زمین منحرف نمی شوند، به عنوان رسانه مخابراتی خود استفاده می کنند. ماهواره ها در فضا مستقر هستند; به طور معمول ۲۲۰۰۰ مایل (برای ماهواره های Geosynchronous) بالاتر از خط استوا، این سیستم های در حال چرخش به دور زمین، قادر به دریافت و رله صدا، داده ها و سیگنال های تلویزیونی هستند.

۳- تلفن همراه: سیستم های تلفن همراه از چندین فناوری ارتباطات رادیویی استفاده می کنند. این سیستم ها به مناطق مختلف جغرافیایی تقسیم شده اند. هر منطقه دارای فرستنده های کم قدرت و یا دستگاه های رله رادیویی آنتن برای تقویت تماس ها از یک منطقه به منطقه بعدی است.

۴- شبکه های محلی بی سیم : شبکه محلی بی سیم از یک تکنولوژی رادیویی فرکانس بالا(مشابه سلول دیجیتالی) و یک تکنولوژی رادیویی فرکانس پایین استفاده می کند. شبکه های محلی بی سیم از تکنولوژی طیف گسترده، برای برقراری ارتباط میان دستگاه های متعدد در یک منطقه محدود، استفاده می کنند. نمونه ای از استاندارد تکنولوژی بی سیم، موج رادیویی IEEE است.

۵- ارتباطات مادون قرمز: ارتباط فروسرخ، سیگنال های بین دستگاه ها را در فواصل کوچک (کمتر از ۱۰ متر) به صورت همتا به همتا (رو در رو) انتقال می دهد; در خط انتقال نباید هیچ گونه شی ای قرار داشته باشد.

۴-بر اساس اندازه

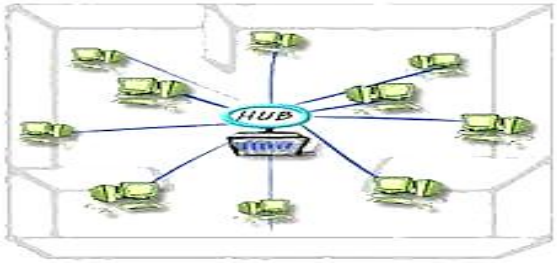
ممکن است شبکه ها ی رایانه ای براساس اندازه یا گستردگی ناحیه ای که شبکه پوشش می دهد طبقه بندی شوند. برای نمونه شبکه شخصی(pan)، شبکه دانشگاهی (can)، شبکه کلان شهری (man)، شبکه گسترده (wan) و شبکه های متصل.

۱-شبکه شخصی(Personal Area Network): یک شبکه رایانه ای است که برای ارتباطات میان وسایل رایانه ای که اطراف یک فرد می باشند (مانند تلفن ها و رایانه های جیبی(pda) که به آن دستیار دیجیتالی شخصی نیز می گویند) بکار می رود. این که این وسایل ممکن است متعلق به آن فرد باشند یا خیر جای بحث خود را دارد. برد یک شبکه شخصی عموما چند متر بیشتر نیست. موارد مصرف شبکه های خصوصی می تواند جهت ارتباطات وسایل شخصی چند نفر به یکدیگر و یا برقراری اتصال این وسایل به شبکه ای در سطح بالاتر و شبکه اینترنت باشد.

ارتباطات شبکه های شخصی ممکن است به صورت سیمی به گذرگاه های رایانه مانندusb و FireWire برقرار شود. همچنین با بهره گیری از فناوری هایی مانند IrDA، بلوتوث و UWB می توان شبکه های شخصی را به صورت بیسیم ساخت.

۲- شبکه های محلی(Local Area Network): یک شبکه رایانه ای است که محدوده جغرافیایی کوچکی مانند یک خانه، یک دفتر کار یا گروهی از ساختمان ها را پوشش می دهد. در مقایسه با شبکه های گسترده (WAN) از مشخصات تعریف شده شبکه های محلی می توان به موارد زیر اشاره کرد:

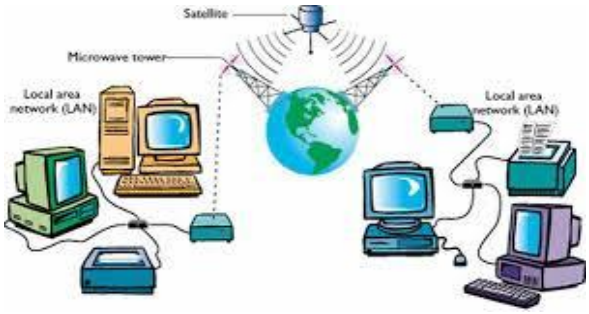
۱. سرعت (نرخ انتقال) بسیار بالاتر از Wan
۲. محدوده جغرافیایی کوچکتر و عدم نیاز به خطوط استیجاری مخابراتی
۳. امنیت بالاتر
۴. تعداد کامپیوتر کمتر
۵. مدیریت راحت تر



دو فناوری اترنت (Ethernet) روی کابل جفت به هم تابیده بدون محافظ (utp) و وای فای (wi-fi) رایج ترین فناوری هایی هستند که امروزه استفاده می شوند، با این حال فناوری های آرکنت(arcnet) و توکن رینگ(Token Ring) و بسیاری روشهای دیگر در گذشته مورد استفاده بوده اند.

۳-شبکه کلان شهری (Metropolitan Area Network): یک شبکه رایانه ای بزرگ است که معمولا در سطح یک شهر گسترده می شود، در این شبکه ها معمولا از زیر ساخت بیسیم و یا اتصالات فیبر نوری جهت ارتباط محل های مختلف استفاده می شود. به عبارک دیگر شبکهman، به شبکه هایی ما بین شبکه های lan وwan گفته می شود و یک راه تشخیص آن، این است که از تجهیزات مخابراتی آنچنانی استفاده نمی شود. مثلا اگر شرکتی در یک شهر دارای چند شعبه باشد و بخواهید آن شعبه ها را به یکدیگر متصل کند، یک چنین شبکه ای ایجاد می کند.

۴-شبکه گسترده(Wide Area Network): یک شبکه رایانه ای است که نسبتا ناحیه جغرافیایی وسیعی را پوشش می دهد(برای نمونه از یک کشور به کشوری دیگر یا از یک قاره به قاره ای دیگر). این شبکه ها معمولا از امکانات انتقال خدمات دهندگان عمومی مانند شرکت های مخابرات استفاده می کند. به عبارت کمتر رسمی این شبکه ها از مسیریاب ها و لینک های ارتباطی عمومی استفاده می کنند.



شبکه متصل(Internetwork):دو یا چند شبکه یا زیرشبکه(subnet) که با استفاده از تجهیزاتی که در لایه ۳ یعنی لایه شبکه مدل مرجع osi (این لایه را در فصل های بعدی معرفی خواهیم نمود) عمل می کنند; مانند یک مسیریاب، به یکدیگر متصل می شوند تشکیل یک شبکه از شبکه ها یا شبکه متصل را می دهند. همچنین می توان شبکه ای که اتصال داخلی میان شبکه های عمومی، خصوصی، تجاری، صنعتی یا دولتی به وجود می آید را شبکه متصل نامید. در کاربردهای جدید، شبکه های به هم متصل شده از قراردادip استفاده می کنند. بسته به اینکه چه کسانی یک شبکه را مدیریت می کنند و اینکه چه کسانی در این شبکه عضو هستند، می توان سه نوع شبکه متصل دسته بندی نمود;

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

- شبکه اینترنت(Internet)

شبکه های داخلی یا خارجی ممکن است که اتصالاتی به شبکه اینترنت داشته و یا نداشته باشند. در صورتی که این شبکه ها به اینترنت متصل باشند در مقابل دسترسی های غیرمجاز از سوی اینترنت محافظت می شوند. خود شبکه اینترنت به عنوان بخشی از شبکه داخلی یا شبکه خارجی به حساب نمی آید، اگرچه که ممکن است شبکه اینترنت به عنوان بستری برای برقراری دسترسی بین قسمت هایی از یک شبکه داخلی خدماتی را ارائه دهد.

۱-*شبکه داخلی (Internet)*یک شبکه داخلی مجموعه ای از شبکه های متصل به هم می باشد که از قرارداد ip مانند مرورگرهای وب استفاده می کند و معمولا 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.

۲-*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 شبکه های متعلق به یک یا چند سازمان یا نهاد دیگر است که معمولا، ول نه همیشه، قابل اعتماد هستند. برای نمودن مشتریان یک شرکت ممکن است که دسترسی به بخش هایی از شبکه داخلی آن شرکت داشته باشند که بدین ترتیب یک شبکه خارجی درست می شود، چرا که از نقطه نظر امنیتی این مشتریان برای شبکه قابل اعتماد به نظر نمی رسند. همچنین از نظر فنی می توان یک شبکه خارجی را در گروه شبکه های دانشگاهی، کلان شهری، گسترده یا دیگر انواع شبکه(هر چیزی غیر از شبکه محلی) به حساب آورد، چرا که از نظر تعریف یک شبکه خارجی نمی تواند فقط از یک شبکه محلی تشکیل شده باشد، چون بایستی دست کم یک اتصال به خارج از شبکه داشته باشد.

۳-*شبکه اینترنت(Internet)* شبکه ویژه ای از شبکه ها که حاصل اتصالات داخلی شبکه های دولتی، دانشگاهی، عمومی و خصوصی در سرتا سر دنیا است، این شبکه براساس شبکه اولیه ای کار می کند که آرپانت(arpanet) نام داشت و به وسیله موسسه آرپا(arpa) که از وابسته به وزارت دفاع ایالات متحده آمریکا است ایجاد شد. همچنین منزلگاهی برای وب جهان گستر(www) است. در لاتین واژهInternet برای نامیدن آن بکار می رود که برای اشتباه نشدن با معنی عام واژه شبکه متصل حرف اول را بزرگ می نویسند.

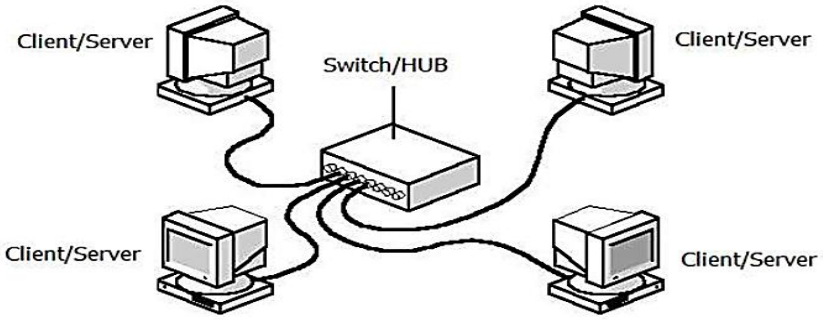
۵-بر اساس لایه شبکه

ممکن است شبکه های رایانه ای مطابق مدلهای مرجع پایه ای که در صنعت به عنوان استاندارد شناخته می شوند مانند مدل مرجع ۷ لایه osi ومدل ۴ لایه tcp/ip، براساس نوع لایه شبکه ای که در آن شبکه ای در آن عمل می کنند طبقه بندی شوند. این دو مورد در فصلی جداگانه بررسی می شوند.

۶-بر اساس معماری کاربری

ممکن است شبکه های رایانه ای براساس معماری کاربری که بین اعضای شبکه وجود دارد طبقه بندی شود، برای نمونه معماری های Active Networking، مشتری - خدمت گذار (Client-Server) و همتا به همتا Peer-To-Peer(گروه کاری).

- (peer-to-peer)Work Grop
- شبکه های peer-to-peer؛ اگر در یک شبکه ای، سیستم ها همزمان علاوه بر ارایه ی سرویس، از سرویس های بقیه هم استفاده کنند یا به عبارتی به طور همزمان هم سرویس دهنده باشند و هم سرویس گیرنده، در این صورت می گوییم مدل سرویس دهی در شبکه به صورت peer-to-peer یا نظیر به نظیر است.(به اختصاص ptp).



معرفی مدل Peer-to-Peer(نظیر به نظیر)

در شبکه های نظیر به نظیر، سرویس دهنده اختصاصی وجود نداشته و سلسله مراتبی در رابطه با کامپیوتر ها رعایت نمی گردد. تمام کامپیوتر ها معادل و همتراز می باشند. هر کامپیوتر در شبکه هم به عنوان سرویس گیرنده و هم به عنوان سرویس دهنده ایفای وظیفه نموده و امنیت به صورت محلی و بر روی هر کامپیوتر ارائه می گردد.(هر کامپیوتری مسئول تعیین امنیت و سیاست های کاری خود می باشد). کاربر هر یک از کامپیوترهای شخصی می نماید که چه داده ای بر روی کامپیوتر خود را به اشتراک قرار دهد. شبکه های نظیر به نظیر،Workgroup نیز نامیده می شوند. واژه Workgroup، نشان دهنده یک گروه کوچک(معمولا ۱۰ و یا کمتر) از کامپیوترهای مرتبط با یکدیگر است. شبکه های نظیر به نظیر، گزینه ای مناسب برای محیط هایی با شرایط زیر می باشند:

۱.حداکثر تعداد کاربران ۱۰ و یا کمتر.

۲. کاربران منابع وچاپگرها را به اشتراک گذاشته و در این راستا، سرویس دهندگان خاصی وجود ندارد.

۳.امنیت متمرکز مورد نظر نباشد.

۴.رشد سازمان و شبکه براساس آنالیزشده، محدود باشد.

۵.این نوع شبکه ساده ترین و سریعترین روش شبکه سازی به ویژه در محیط های ویندوز می باشد که ابزار خاصی لازم نداشته و دارای مزایای زیر می باشد:

۶.هزینه راه اندازی و نگهداری پایین تر

۷.سرعت بیشتر در راه اندازی

۸.عدم نیاز به یک کامپیوتر مجزا به عنوان سرور

شبکه سازی به روش نظیر به نظیر

برای ایجاد چنین شبکه ای تجهیزات زیر لازم است:

۱. کارت شبکه.

۲. کابل شبکه.

۳. سوکت از نوع استاندارد rj45 که به سر کابل ها وصل می شود.

۴. میانگاه(Hub) با سوئیچ(Switch) در صورتی که بیش از دو رایانه را بخواهید شبکه کنید.

۵. نرم افزار مناسب: به عنوان مثال سیستم عامل ویندوز به تنهایی می تواند کافی باشد.

۶. برخلاف حالت Client/Server در این روش کامپیوتر های شخصی می توانند بدون Server به هم متصل شده و تبادل اطلاعات نمایند، پس از نصب مراحل سخت افزاری فقط کافی است که سرویسهای شبکه را در ویندوز و یا سیستم عامل های دیگر همچون لینوکس نصب کرده و دیسک گردان ها (درایو ها) را به اشتراک گذارند.

۷. ادعا می شود که امنیت آن از روشClient/Server بالاتر است. (اما نقیض این صحبت را جلوتر اعلام خواهیم کرد)

۸. نیاز به Administrator (مدیر شبکه) ندارد.

یکی از کاربردهای شبکه نظیر به نظیر دسترسی یافتن از طریق رایانه شخصی خود به پرونده هایی است که ر سخت دیسک رایانه دیگری قرار دارد.

Peer to Peer Network

ویژگی ها

به نظر میرسد تنها ویژگی این نوع شبکه ها نصب و راه اندازی فوق آسان و همچنین هزینه ی کم باشد.

معایب

۱.Low Security: در قسمت قبل چرایی پایین بودن امنیت این شبکه ها را باهم بررسی کردیم.

۲. No Centralize Manage: در این نوع شبکه ها، هیچ گونه مدیریت مرکزی وجود ندارد. به عنوان مثال در صورت اضافه شدن یک کاربر جدید، باید User وPass آن را، در LSDهمه ی کامپیوتر ها به صورت دستی وارد کرد و این یعنی فاجعه!

۳. Limit10: تعداد کاربران در این نوع شبکه ها محدود است و بهترین حالت آن تا ۱۰ کاربر است.

دامنه یا Domain در Server based یا client – server

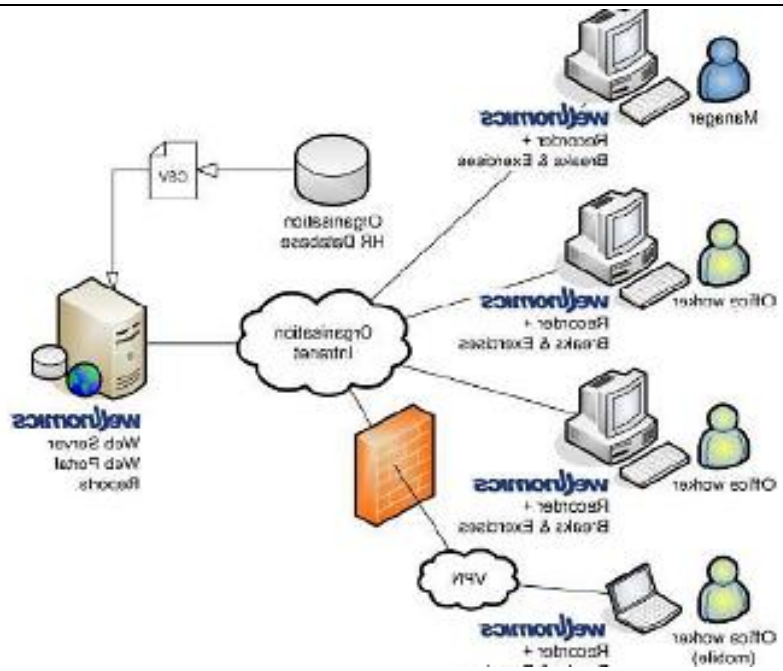
اگر در یک شبکه تعدادی از سیستم ها فقط در نقش سرویس دهنده و تعدادی فقط در نقش سرویس گیرنده ظاهر شوند در این صورت می گوییم که مدل سرویس دهی آن شبکه به صورت server –Based (به اختصارSB) است.

معرفی شبکه های server Based یا Client-server

به موازات رشد شبکه و افزایش کاربران و منابع موجود، یک شبکه نظیر به نظیر قادر به پاسخگوئی به حجم بالای تقاضا برای منابع اشتراکی نخواهد بود. به منظور هماهنگی با افزایش تقاضا و ارائه سرویس های مورد نیاز، شبکه ها می بایست ازسرویس دهندگان اختصاصی استفاده نمایند. یک سرویس دهنده اختصاصی، صرفا به عنوان یک سرویس دهنده درشبکه ایفای وظیفه می نماید(نه به عنوان یک سرویس گیرنده).

شبکه های سرویس گیرنده – سرویس دهنده، به عنوان مدلی استاندارد برای برپاسازی شبکه مطرح شده اند. به موازات رشد یک شبکه (تعداد کامپیوتر ها متصل شده، فاصله فیزیکی، ترافیک موجود) می توان تعداد سرویس دهندگان در شبکه را افزایش داد. با توزیع مناسب فعالیت های شبکه بین چندین سرویس دهنده، کارآیی شبکه به طرز محسوسی افزایش خواهد یافت.

سرویس دهی در این شبکه توسط سیستم هایی صورت می گیرد که اصطلاحا سرویس دهنده یا server نامیده می شوند. سیستم هایی که از این سرویس استفاده می کنند اصطلاحا سرویس گیرنده یاclient نامیده می شوند. برای سرویس گیرنده ها اصطلاحاWorkstation نیز به کار می رود.

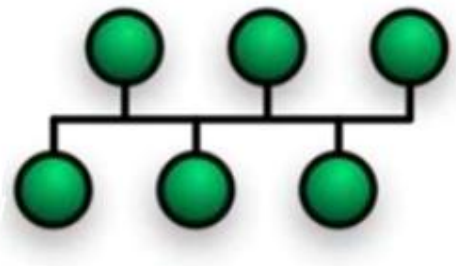


۷–بر اساس همبندی

ممکن است شبکه های رایانه ای نوع همبندی شبکه طبقه بندی شوند مانند: شبکه خطی(Bus)، شبکه ستاره (Star)، شبکه حلقه ای (Ring)، شبکه توری (Mesh)، شبکه ستاره–باس (star-Bus)، شبکه رختی (Tree)، یا شبکه سلسله مراتبی (Hierarchical) و غیره. همبندی شبکه را می توان براساس نظم هندسی ترتیب داد. همبندی های شبکه طرح های منطقی شبکه هستند، واژه منطقی در اینجا بسیار پرمعنی است. این واژه به این معنی است که همبندی شبکه به طرح فیزیکی شبکه بستگی ندارد. مهم نیست که رایانه ها در یک شبکه به صورت خطی پشت سر هم قرار گرفته باشند، ولی زمانیکه از طریق یک هاب به یکدیگر متصل شده باشند تشکیل همبندی ستاره می کنند نه باس. و این عامل مهمی است که شبکه ها در آن فرق می کنند، جنبه ظاهری و جنبه عملکردی. توپولوژی ها در فصلی جداگانه بررسی می شوند.

ممکن است شبکه های رایانه ای نوع همبندی شبکه طبقه بندی شوند مانند: شبکه خطی(Bus)، شبکه ستاره (Star)، شبکه حلقه ای (Ring)، شبکه توری (Mesh)، شبکه ستاره–باس (star-Bus)، شبکه رختی (Tree)، یا شبکه سلسله مراتبی (Hierarchical) و غیره. همبندی شبکه را می توان براساس نظم هندسی ترتیب داد. همبندی های شبکه طرح های منطقی شبکه هستند، واژه منطقی در اینجا بسیار پرمعنی است. این واژه به این معنی است که همبندی شبکه به طرح فیزیکی شبکه بستگی ندارد. مهم نیست که رایانه ها در یک شبکه به صورت خطی پشت سر هم قرار گرفته باشند، ولی زمانیکه از طریق یک هاب به یکدیگر متصل شده باشند تشکیل همبندی ستاره می کنند نه باس. و این عامل مهمی است که شبکه ها در آن فرق می کنند، جنبه ظاهری و جنبه عملکردی. توپولوژی ها در فصلی جداگانه بررسی می شوند.

- **آرایش خطی(BUS)**

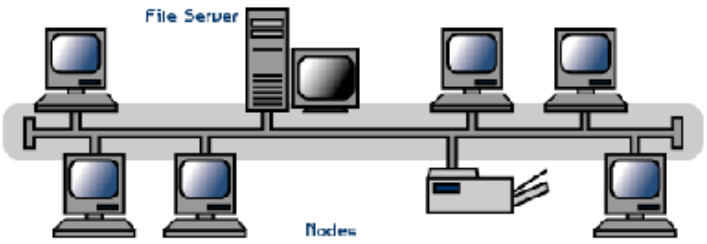


شبکه ای که همبندی گذرگاهی استفاده می کند معمولا دارای یک کابل واحد(معمولا کابلCoaxial) و بلند بوده که دستگاه های مختلف شبکه به آن متصل هستند(توسط-T Connector) و در هر واحد زمانی تنها یک رایانه امکان ارسال اطلاعات را دارد. در این روش کلیه رایانه های متصل به خط، اطلاعات ارسال شده را دریافت می کنند(روش Broadcast)،

ولی تنها رایانه ای که آدرس مقصد بسته داده متعلق به او است این اطلاعات را ذخیره می نماید و بقیه رایانه ها از بسته صرف نظر می کنند. راه اندازی آن آسان است و به این منظور از یک رشته کابل کواکسیال استفاده می شود و هر سیستم به کمک یک کانکتور به شبکه متصل می شود. ابتدا و انتهای شبکه با ترمیناتور بسته می شود. اما نگهداری از آن با مشکلاتی همچون خطا یابی مشکل همراه است به همین دلیل تقریبا منسوخ شده است.

مزایای توپولوژی BUS

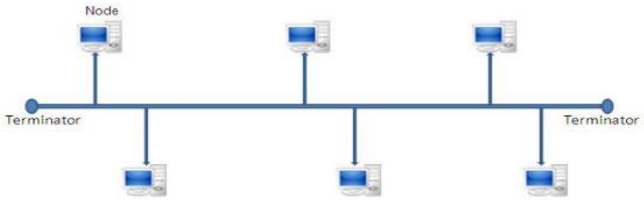
کم بودن طول کابل. به دلیل استفاده از یک خط انتقال جهت اتصال تمام کامپیوترها، در توپولوژی فوق از کابل کمی استفاه می شود. موضوع فوق باعث پایین آمدن هزینه نصب و ایجاد تسهیلات لازم در جهت پشتیبانی شبکه خواهد بود.



ساختار ساده. توپولوژی BUS دارای یک ساختار ساه است. ر مدل فوق صرفا از یک کابل برای انتقال اطلاعات استفاده می شود.

توسعه آسان. یک کامپیوتر جدید را می توان براحتی در نقطه ای از شبکه اضافه کرد. در صورت اضافه شدن ایستگاههای بیشتر در یک سگمنت، می توان از تقویت کننده هایی به نام Repeater استفاده کرد.

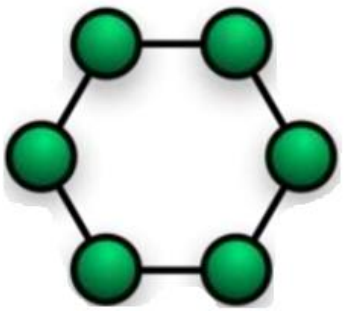
معایب توپولوژی BUS



مشکل بودن عیب یابی. با اینکه سادگی موجود در توپولوژی BUS امکان بروز اشتباه را کاهش می دهند، ولی در صورت بروز خطا، کشف آن ساده نخواهد بود. در شبکه هایی که از توپولوژی فوق استفاده می نمایند، کنترل شبکه در هر گره دارای مرکزیت نبوده و در صورت بروز خطا می بایست نقاط زیادی به منظور تشخیص خطا بازدید و بررسی گردند.

ایزوله کردن خطا مشکل است. در صورتی که یک کامپیوتر در توپولوژی فوق دچار مشکل گردد، می بایست کامپیوتر را در محلی که به شبکه متصل است رفع عیب نمود. در موارد خاص می توان یک گره را از شبکه جدا کرد. در حالتی که اگر اشکال در محیط انتقال باشد، تمام یک سگمنت می بایست از شبکه خارج گردد.

- **آرایش حلقوی (Ring)**



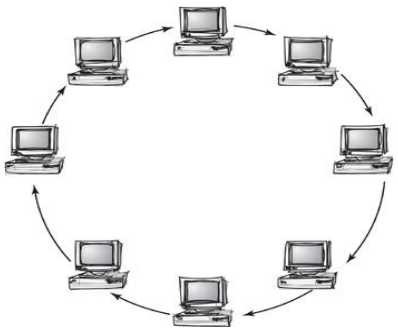
این همبندی توسط شرکت IBM اختراع شد و کلیه رایانه ها به گونه ای به یکدیگر متصل هستند که مجموعه آنها یک حلقه را تشکیل می دهد. همیشه یک بسته کوچک با نام نشانه(Token) در داخل شبکه از یک رایانه به دیگری می رود، زمانی که یک رایانه اطلاعاتی جهت ارسال دارد، نشانه را در اختیار گرفته و از چرخش آن داخل شبکه جلوگیری می کند، تا زمانیکه نشانه توسط یک رایانه نگه داشته شده باشد، تمام رایانه های شبکه پذیرای اطلاعاتی خواهند بود که رایانه مالک نشانه ارسال می کند. 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 می باشد و از مزایای آن، می توان به کم هزینه بودن و سادگی شبکه اشاره کرد.

این توپولوژی بر روی نوع دستیابی تاثیر می گذارد. هر گره در شبکه دارای مسئولیت عبور دادن داده ای است که از گره مجاور دریافت داشته است. قبل از اینکه یک گره بتواند داده خود را ارسال نماید، می بایست به این اطمینان برسد که محیط انتقال برای استفاده قابل دستیابی است.

مزایای توپولوژی RING

کم بودن طول کابل. طول کابلی که در این مدل بکار گرفته می شود، قابل مقایسه با توپولوژی BUS نبوده و طول کمی را در بردارد. ویژگی فوق باعث کاهش تعداد اتصالات (کانکتور) در شبکه شده و ضریب اعتماد به شبکه را افزایش خواهد داد.

نیاز به فضائی خاص جهت انشعابات در کابل کشی نخواهد بود. به دلیل استفاده از یک کابل جهت اتصال هر گره به گره همسایه اش، اختصاص محل هایی خاص به منظور کابل کشی ضرورتی نخواهد داشت.



مناسب جهت فیبرنوری. استفاده از فیبر نوری باعث بالا رفتن نرخ سرعت انتقال اطلاعات در شبکه است. چون در توپولوژی فوق ترافیک داده ها در یک جهت است، می توان از فیبرنوری به منظور محیط انتقال استفاده کرد. در صورت تمایل می توان در هر بخش از شبکه از یک نوع کابل به عنوان محیط انتقال استفاده کرد. مثلا در محیط های اداری از مدل های مسی و در محیط های کارخانه از مدل فیبرنوری استفاده کرد.

معایب توپولوژی RING

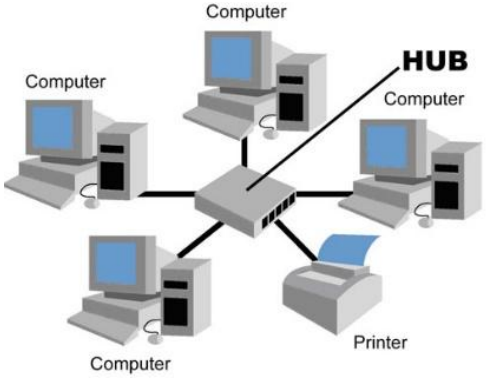
اشکال در یک گره باعث اشکال در تمام شبکه می گردد. در صورت بروز اشکال در یک گره، تمام شبکه با اشکال مواجه خواهد شد. و تا زمانیکه گره معیوب از شبکه خارج نگردد، هیچگونه ترافیک اطلاعاتی را روی شبکه نمی توان داشت.

اشکال زدایی مشکل است. بروز اشکال در یک گره می تواند روی تمام گره های دیگر تاثیر گذار باشد. به منظور عیب یابی می بایست چندین گره بررسی تا گره مورد نظر پیدا گردد.

تغییر در ساختار شبکه مشکل است. در زمان گسترش و یا اصلاح حوزه جغرافیائی تحت پوشش شبکه، به دلیل ماهیت حلقوی شبکه مسائلی به وجود خواهد آمد.

- **آرایش ستاره ای (Star)**

در این نوع همبندی کلیه رایانه ها به یک کنترل کننده مرکزی به نام میانگاه (Hub) و یا سوئیچ (Switch) متصل می شوند و هرگاه رایانه ای بخواهد با رایانه دیگری تبادل اطلاعات کند رایانه مبدا اطلاعات را به میانگاه/سوئیچ ارسال نموده و اطلاعات از طریق آن به رایانه مقصد انتقال می یابد.



نکته ها:

۱) یک پیوند نقطه به نقطه را می توان به عنوان حالت خاصی از یک شبکه با آرایش ستاره در نظر گرفت. در نتیجه ساده ترین شبکه که براساس آرایش ستاره ساخته می شود را می توان یک گره که به یک گره دیگر از طریق یک پیوند نقطه به نقطه متصل است در نظر گرفت انتخاب یک گره به عنوان میانگیر به دلخواه ممکن است.
۲) ساده ترین نوع شبکه براساس آرایش ستاره علاوه بر شبکه توضیح داده شده در فوق، یک میانگیر(Hub) متصل به دو گره می باشد.

۳) با وجود این که می توان آرایش ستاره را با استفاده از یک هاب (Hub) یا سوئیچ (Switch) براحتی پیاده سازی نموده، اما به کار بردن یک کامپیوتر یا یک اشتراک مشترک نیز برای میانگیر کافی است. به هر حال چون در بیشتر نمایش های آرایش ستاره یکی از این ابزار ویژه نشان داده شده است، در نتیجه ممکن است این ابهام به وجود آید که حتما باید از یکی از این ابزار استفاده نمود در حالی که مثلا سه کامپیوتر متصل به یکدیگر بدون استفاده از هیچ ابزار ویژه ای نیز خود یک شبکه با آرایش ستاره است.

۴) شبکه های ستاره را می توان به صورت پخشی (Broadcast) با دسترسی چندگانه (Multicast) یا غیر پخشی با دسترسی چندگانه (NBMA) توصیف نمود که وابسته به توانایی میانگیر در ارسال سیگنال های موجود به تمام گره های تابع یا ارسال سیگنال به صورت جداگانه برای هر ارتباط است.

مزایای توپولوژی STAR

سادگی سرویس شبکه. توپولوژی star شامل تعدادی از نقاط اتصالی در یک نقطه مرکزی است. ویژگی فوق تغییر در ساختار و سرویس شبکه راآسان می نماید. در هر اتصال یک دستگاه. نقاط اتصالی در شبکه ذاتا مستعد اشکال هستند. در توپولوژی star اشکال در یک اتصال، باعث خروج آن خط از شبکه و سرویس و اشکال زدایی خط مزبور است. عملیات فوق تاثیری در عملکرد سایر کامپیوتر های موجود در شبکه نخواهد گذاشت.

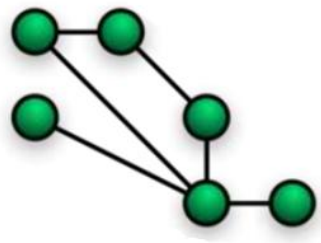
کنترل مرکزی و عیب یابی. با توجه به این مسئله که نقطه مرکزی مستقیما به هر ایستگاه موجود در شبکه متصل است، اشکالات و ایرادات در شبکه به سادگی تشخیص و مهار خواهند گردید. روش های ساده دستیابی. هر اتصال در شبکه شامل یک نقطه مرکزی و یک گره جانبی است. در چنین حالتی دستیابی به محیط انتقال جهت ارسال ودریافت اطلاعات دارای الگوریتمی ساده خواهد بود.

زیاد بودن طول کابل. به دلیل اتصال مستقیم هرگره به نقطه مرکزی، مقدار زیادی کابل مصرف می شود. هزینه کابل نسبت به تمام شبکه، کم است، اما تراکم در کانال کشی جهت کابل ها و مسائل مربوط به نصب و پشتیبانی آن ها، به طور قابل توجهی هزینه ها را افزایش خواهد داد.

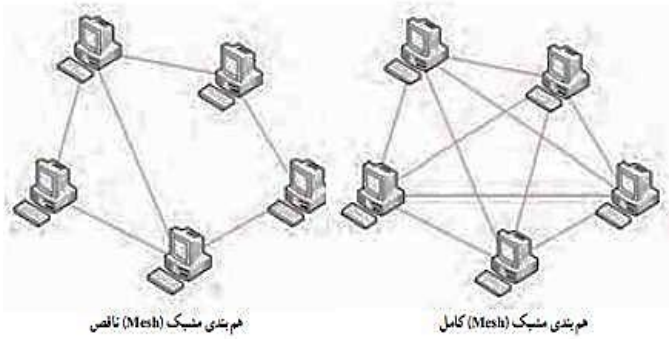
مشکل بودن توسعه. اضافه نمودن یک گره جدید به شبکه مستلزم یک اتصال از نقطه مرکزی به گره جدید است. با اینکه در زمان کابل کشی پیش بینی های لازم جهت توسعه در نظر گرفته می شود، ولی در برخی حالات نظیر زمانی که طول زیادی از کابل مورد نیازبوده و یا اتصال مجموعه ای از گره های غیرقابل پیش بینی اولیه، توسعه شبکه را با مشکل مواجه خواهد کرد.

وابستگی به نقطه مرکزی. در صورتی که نقطه مرکزی (هاب یا سوئیچ) در شبکه با مشکل مواجه شود، تمام شبکه غیرقابل استفاده خواهد بود.

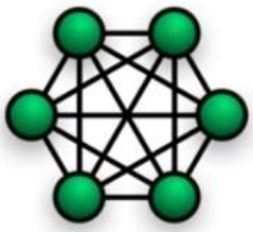
- **آرایش مشبک (Mesh)**



دراین آرایش شبکه نظم مشخصی نداشته و هر یک از رایانه ها به یک یا چند رایانه دیگر متصل شده اند. این آرایش در واقع نسخه ناقص آرایش اتصال کامل است، لذا هزینه و پیچیدگی کمتری نسبت به روش مذکور دارد. از معایب این توپولوژی می توان به پیچیدگی و هزینه ی بالای آن اشاره کرد و چون شبکه گسترده است عیب یابی آن هم نسبت سخت می باشد. 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 می باشد; یعنی تمامی کامپیوترها بدون اینکه شبکه مشغول شود می توانند به یک دیگر اطلاعات ارسال و دریافت کنند که برای اینکه از توپولوژی Mesh بتوان از حداکثر استفاده را برد، از دستگاهی به نام روتر یا مسیریاب استفاده می شود که کار این دستگاه این است که باعث می شود از خط ها و مسیرهایی که خالی هستند ارسال اطلاعات انجام داد و در نتیجه این دستگاه باعث سرعت بخشیدن به ارسال اطلاعات می شود.

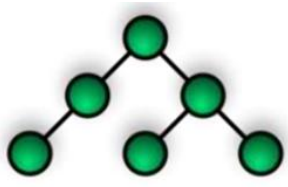


اتصال کامل(Fully Connected)

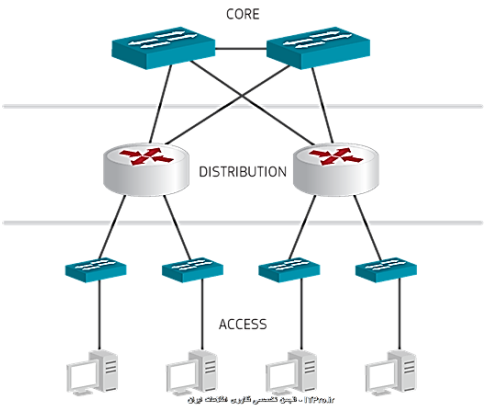


در این آرایش تمام رایانه های شبکه مستقیمابه همدیگر متصل هستند، عمده ترین اشکال این روش پیچیدگی و هزینه بالای این اتصالات است. مزیت این روش ارسال سریع و بی واسطه اطلاعات از هر رایانه دیگر می باشد. در این حالت اگر n کامپیوتر داشته باشیم ، به $\frac{n(n-1)}{2}$ کابل نیاز خواهد بود.

- **آرایش درختی (Tree) یا آرایش سلسله مراتبی**



در آرایش درختی یک گره مرکزی (بالاترین سطح در سلسله مراتب) که ریشه نام دارد، 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 گره های سطح دونیز به چندین گره در سطحی پایین تر متصل هستند(برای مثال در سطح سوم). گره مرکزی تنها گره ای است که هیچ گره ای در سطحی بالاتر از خود ندارد. سلسله مراتب درخت متقارن است یعنی تعداد گره های متصل به هر گره در سطح پایین تر عدد ثابت F است. عدد F به عنوان عامل شاخه بندی در درخت سلسله مراتب شناخته می شود.



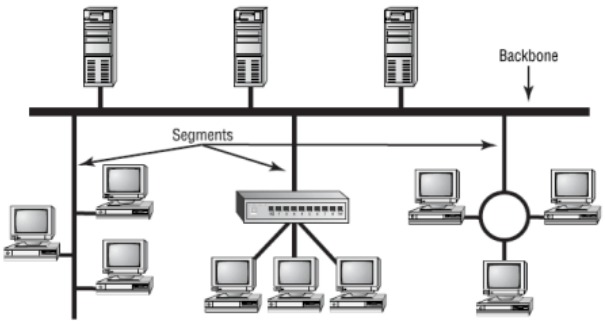
نکته ها:

۱) یک شبکه مبتنی برآرایش درختی فیزیکی حتما 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 ها است. اگر یک گره نیاز به درگاه هایی برای اتصال به گره های دیگر داشته باشد، می توان تعداد درگاه ها را بدون توجه به تعداد کل گره ها کاهش داد. در نتیجه تعداد درگاه های مورد نیاز وابسته به عامل شاخه بندی است و در نتیجه می توان تعداد درگاه ها را بدون توجه به تعاد کا گره ها کاهش داد.

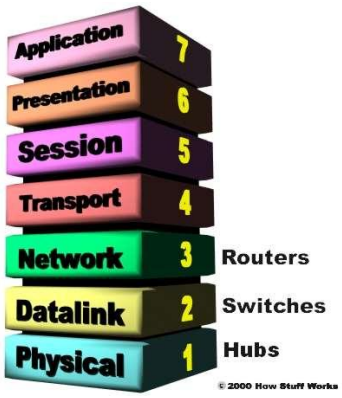
۴) تعداد کل پیوندهای نقطه به نقطه در شبکه براساس آرایش درختی یکی کمتر از تعداد گره های شبکه می باشد.
۵) اگر نیاز به پردازش اطلاعات توسط گره ها در یک آرایش درختی فیزیکی باشد گره های سطح بالاتر باید پردازش بیشتری نسبت به گره های سطح پایین تر انجام هند.

- **آرایش ترکیبی(Hybride)**



آرایش ترکیبی نوعی از آرایش های شبکه است که از همبندی یک یا چند شبکه با آرایش های فیزیکی متفاوت و یا همبندی چندین شبکه که دارای آرایش فیزیکی یکسان است به وجود می آید و آرایش فیزیکی شبکه حاصل مشابه آرایش فیزیکی شبکه های اولیه نمی باشد (مثلا آرایش فیزیکی شبکه ای که از همبندی چندین شبکه براساس آرایش فیزیکی ستاره بدست می آید ممکن است با توجه به نحوه اتصال شبکه ها به صورت ترکیبی از آرایش های ستاره و خطی یا ستاره و درختی باشد در حالی که اگر چنین شبکه با آرایش خطی توزیع شده به یکدیگر متصل گردند شبکه حاصل آرایش خطی توزیع شده را به خود خواهد گرفت) 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

لایه های شبکه



مدل OSI و TCP/IP

نحوه مبادله داده ها در دو کامپیوتر

آیا تاکنون برای شما این سوال مطرح شده است که نحوه مبادله اطلاعات بین دو کامپیوتر موجود در یک شبکه به چه صورت است؟

در سالهای آغازین طراحی شبکه، مشکل عمده ای که وجود داشت نا سازگاری بین محصولات تولید شده توسط شرکت های بزرگ تولید کننده تجهیزات شبکه بود. این مشکل زمانی آغاز گردید که شرکت hp تصمیم به تولید یک محصول شبکه ای نمود و این محصول یا محصولات مشابه سایر شرکت ها (مثلا IBM) سازگار نبود. برای حل این مشکل نیاز به یک مدل مرجع برای تبادل اطلاعات در شبکه احساس می شد تا اینکه کمیته IEEE به منظور جلوگیری از عدم هماهنگی بین محصولات، پیشگام تعریف یک استاندارد برای محصولات شبکه شد و در سال ۱۹۸۴ مدل مرجع OSI را معرفی کرد. مدل فوق، همانند یک دستورالعمل اجرائی بوده و عملیات لازم در زمان ارسال و یا دریافت داده را برای یک کامپیوتر مشخص می نماید. به منظور آشنائی و آنالیز فرآیند مبادله داده بین دو کامپیوتر موجود در یک شبکه به بررسی یک نمونه مثال کاربردی خواهیم پرداخت.

زمانی که یک اتومبیل در کارخانه ای تولید می گردد، یک نفر تمامی کارها را انجام نخواهد داد. تولید یک اتومبیل براساس یک خط تولید انجام شده و همزمان با حرکت اتومبیل در خط تولید هر شخص بخش های متفاوتی را به آن اضافه نموده و زمانی که به انتهای خط تولید می رسیم، اتومبیل مورد نظر تولید و آماده استفاده خواهد بود.

وضعیت فوق در رابطه با داده ارسالی از یک کامپیوتر به کامپیوتر دیگر نیز صدق می کند. مدل OSI، قوانین لازم به منظور مبادله اطلاعات بین کامپیوترها را فراهم می نماید و داده ها در حین حرکت در هر لایه با توجه به مجموعه رهنمودهایی که OSI مشخص کرده است، تغییر شکل پیدا کرده و در نهایت از حالتی که در کامپیوتر قابل استفاده است به حالتی که از طریق کابل شبکه قابل ارسال باشد تبدیل می گردند و به این ترتیب داده ها از کامپیوتر مبدا قادر به ارسال به سایر کامپیوترها خواهد بود.

ساختار لایه ها در مدل OSI (Open System I nterconnection)

همانطور که گفته شد، کمیته IEEE به منظور جلوگیری از عدم هماهنگی بین محصولات و در نتیجه ناتوانی در برقراری ارتباط بین شبکه ای مدل مرجع OSI را معرفی کرد. این استاندارد تمامی فعالیتهایی را که ثابت می شد اطلاعات از طریق شبکه و از کامپیوتری به کامپیوتر دیگر منتقل شود را در یک ساختار ۷ لایه ای در بر می گرفت. هر کدام از بین لایه ها

مسئولیت انجام عملیات خاصی را برعهده دارند و در حقیقت ارسال و دریافت اطلاعات از طریق این لایه ها در کامپیوتر های فرستنده و گیرنده انجام خواهد شد.

هنگام بررسی فرآیندانتقال اطلاعات بین دو کامپیوتر، مدل هفت لایه ای OSI روی هر یک از کامپیوترها پیاده سازی می گردد. در تحلیل این فرآیند ها می توان عملیات انتقال اطلاعات را بین لایه های متناظر مدل OSI واقع در کامپیوترهای مبدا و مقصد در نظر گرفت. این تجسم از انتقال اطلاعات را انتقال مجازی (Virtual) می نامند. اما انتقال واقعی اطلاعات بین لایه های مجاور مدل OSI واقع در یک کامپیوتر انجام می شود.

در کامپیوتر مبدا اطلاعات از لایه فوقانی به طرف لایه تحتانی مدل OSI حرکت کرده و از آنجا به لایه زیرین مدل OSI واقع در کامپیوتر مقصد ارسال می شوند. در کامپیوتر مقصد اطلاعات از لایه های زیرین به طرف بالاترین لایه مدل OSI حرکت می کنند. عمل انتقال اطلاعات از یک لایه به لایه دیگر در مدل OSI از طریق واسطه ها یا Interface ها انجام می شود. این واسطه ها تعیین کننده سرویس هایی هستند که هر لایه مدل OSI می تواند برای لایه مجاور فراهم آورد.

هفت لایه مدل OSI

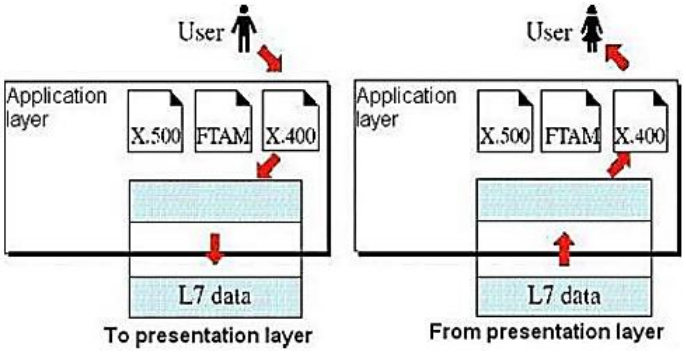
۱. لایه کاربردی
۲. لایه نمایش
۳. لایه جلسه
۴. لایه انتقال
۵. لایه شبکه
۶. لایه اتصال داده
۷. لایه فیزیکی

۱ –لایه کاربردی (Application layer)

این آخرین لایه در اصل لایه ای است که کاربر تمام موارد قابل مشاهده را در آن مشاهده می کند. در این لایه دستگاه های فرستنده و گیرنده تعریف می شوند، کیفیت سرویس دهی و امنیت مشخص می شود. این لایه تامین کننده سرویس های پشتیبانی برنامه های کاربردی نظیر انتقال فایل، دسترسی به بانک اطلاعاتی و پست الکترونیکی است.

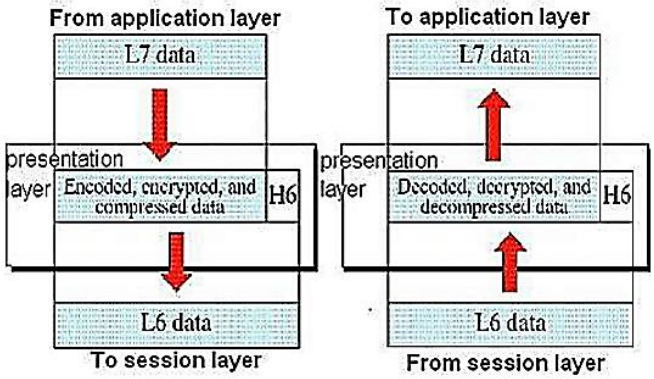
تعدادی شناخته شده ترین پروتکلهای لایه کاربردی عبارتند از :

- **DNS** (سیستم نام دامنه) برای تبدیلات دامنه های اینترنت
- **FTP** (پروتکل انتقال فایل) برای انتقال فایل
- **SMTP** (پروتکل ساده انتقال پستی) برای e-mail
- **SMB** (قطعه پیغام سرور) برای اشتراک فایلهای در شبکه ویندوز
- **NFS** (سیستم فایل شبکه) برای اشتراک فایل در یونیکس
- **Telnet** برای شبیه سازی ترمینال



۲– لایه نمایش (Presentation Layer)

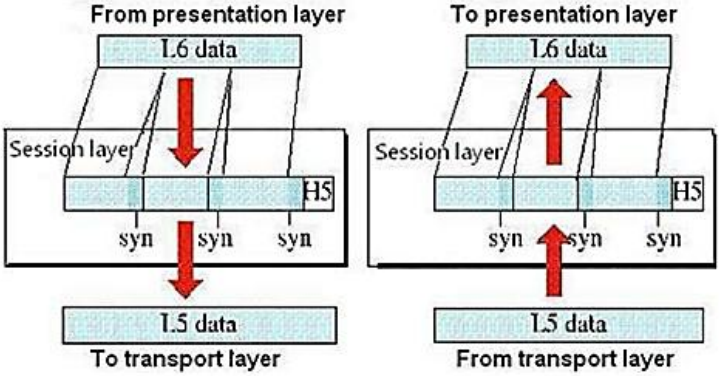
این لایه وظیفه فشرده سازی و رمزنگاری داده ها را برعهده دارد. فشرده سازی اطلاعات به منظور کاهش حجم اطلاعات ارسالی بر روی خطوط انتقال می باشد.
بنابراین در این لایه قبل از اینکه اطلاعات تحویل لایه پایین تر شود می بایست براساس استانداردهای موجود فشرده شده و به لایه زیرین تحویل داده شود و در سوی دیگر اطلاعات دریافتی از لایه زیرین در این لایه پس از مشخص شدن قالب فشرده سازی، از حالت فشرده و کد شده خارج شده و به لایه بالاتر تحویل داده می شود. سرویس های MP3 و JPEG و GIF را می توان به عنوان نمونه ای از سرویسهای لایه ششم نام برد.



۳– لایه جلسه یا نشست (Session Layer)

لایه ای است برای مدیریت ارتباط بین دو کاربر و در واقع ارائه کننده جلسه بین دو کاربر میباشد. لایه جلسه یکسری قرار دادهایی را به اجرا می گذارد. مانند بررسی Username و Password کاربر در طول استفاده. در واقع این لایه بر برقراری اتصال بین دو برنامه کاربردی روی دو کامپیوتر مختلف واقع در شبکه نظارت دارد. همچنین تامین کننده همزمانی فعالیت های کاربر نیز هست.
لایه نشست، اجازه برقراری سه نوع انتقال را صادر میکنند:
– **Simplex** : در این حالت، داده ها فقط در یک جهت حرکت میکنند.
– **Half Duplex** : در این حالت، داده ها در هر دو جهت حرکت میکنند ولی در هر لحظه فقط در یک جهت، یا رفت یا برگشت.
– **Full Duplex :** در این حالت، داده ها در آن واحد میتوانند هم در جهت رفت و هم در جهت برگشت حرکت کنند.

نکته : در عمل، فرق بین لایه های نشست و نمایش و کاربردی بسیار کمرنگ میشود و چند پروتکل معمول در این لایه ها جاری میشوند. برای مثال، SMB (پروتکل مدیریت قطعه سرور که اساس اشتراک فایل در ویندوز است) در هر سه لایه کار میکند.

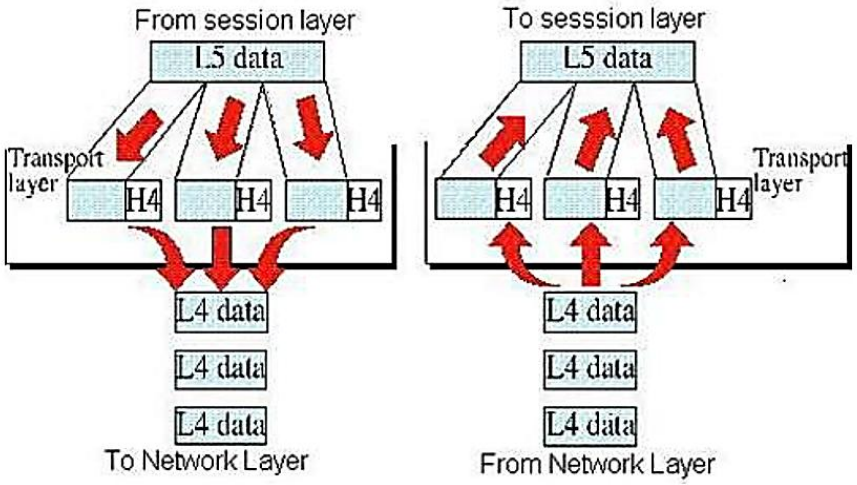


۴- لایه انتقال (Transport Layer)

لایه انتقال، لایه ای است که در آن میتوانید دو پروتکل معروف شبکه را پیدا کنید : TCP (بطور عادی همراه با IP) و SPX (بطور عادی همراه با IPX). بطوریکه از نام لایه نیز مشخص است، لایه انتقال در رابطه با انتقال اطلاعات از یک کامپیوتر به کامپیوتر دیگر است.

هدف اصلی لایه انتقال حصول اطمینان از انتقال مطمئن و بدون خطای داده ها است. لایه انتقال این کار با ایجاد ارتباطاتی بین ابزارهای شبکه جهت ارسال رسید پکت های رسیده و درخواست مجدد برای ارسال پکت های ناموفق انجام میدهد. در بسیاری از موارد، پروتکل لایه انتقال، پیغام های بزرگ را به پکت های کوچکتر مستقیم میکند که میتوانند روی شبکه بهتر جابجا شوند. پروتکل لایه انتقال این پکت های ریز را در مقصد دوباره سرهم بندی کرده و اطمینان حاصل میکند که پکت های ارسالی بدون کم و کسر به مقصد رسیده اند.

در برخی از کاربردها، سرعت و تاثیرگذاری، مهمتر از قابلیت اطمینان میباشد. در چنین مواردی، یک پروتکل بدون ارتباط مورد استفاده قرار میگیرد. پروتکل بدون ارتباط، نیازی به تحمل دردسر ایجاد ارتباط قبل از ارسال پکت ندارد. TCP یکی از پروتکلهای ارتباطی لایه انتقال است. پروتکل معادل بدون ارتباط در این لایه که همراه با TCP کار میکند، UDP نام دارد.



۵- لایه شبکه (network layer)

در لایه شبکه، عمل مسیردهی پیغام های شبکه از یک کامپیوتر به کامپیوتر دیگر انجام میشود. دو پروتکل معروف لایه سوم عبارتند از : IP (که معمولا همراه با TCP است)، IPX (که بطور عادی با SPX همراه است که هنگام استفاده از شبکه ناول با ویندوز بکار میرود).

آدرس دهی منطقی

بطوریکه میدانید، هر ابزار شبکه یک آدرس MAC منحصربفرد دارد که در کارخانه و هنگام ساخت به دستگاه اختصاص داده میشود. هنگامی که کارت شبکه ای را در کامپیوتر خود نصب میکنید، آدرس MAC کارت شبکه تثبیت شده و غیرقابل تغییر میشود. ولی آیا شاید شما بخواهید از روش آدرس دهی دیگری برای دسترسی به ابزار های روی شبکه استفاده کنید. در این حالت، مفهوم آدرس دهی منطقی به میان می آید. آدرس منطقی به شما این امکان را میدهد تا به ابزارهای شبکه با استفاده از آدرس هایی که خودتان اختصاص میدهید، دسترسی پیدا کنید.

آدرس های منطقی توسط پروتکل های لایه شبکه مانند IP و IPX ایجاد میشود. پروتکل لایه شبکه آدرس های منطقی را به آدرس های MAC معادل ترجمه میکند. برای مثال، اگر شما از IP بعنوان پروتکل لایه شبکه استفاده کنید، ابزارهای روی شبکه آدرس های IP مانند 207.120.67.32 خواهند داشت. چون پروتکل IP باید از یک پروتکل لایه اتصال داده استفاده

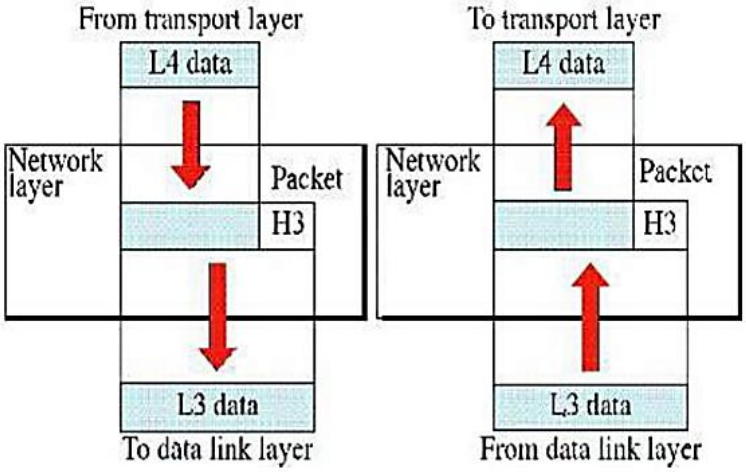
کند تا قادر به ارسال پکت ها بع ابزارهای مختلف باشد، پس باید دانش ترجمه آدرس های IP را به آدرس های فیزیکی ابزارهای شبکه داشته باشد.

آدرس های لایه اتصال داده (آدرس های MAC) در کارخانه اعمال میشوند و قابل تغییر نمیباشند. آدرس لایه شبکه (IP) در هنگام شبکه بندی اختصاص داده میشود و قابل تغییر است.

پروتکلی قابل مسیردهی نامیده میشود که از آدرس هایی استفاده کند که شامل یک قسمت شبکه و یک قسمت میزبان باشند. هر پروتکلی که از آدرس های فیزیکی استفاده کند، قابل مسیردهی نیست، چون آدرس های فیزیکی نشان نمیدهند که ابزار به کدام شبکه تعلق دارد.

کارهایی که در این لایه انجام می شود را به صورت زیر دسته بندی کرد :

۱. تهیه آدرس منطقی منحصر به فرد که برای هر بخش از شبکه در نظر گرفته می شود و با آدرس MAC متفاوت است.
۲. مسیریابی داده و پیدا کردن بهترین مسیر از بین چند مسیر.
۳. کنترل خطا، کنترل ارتباط و ترتیب بندی بسته ها.

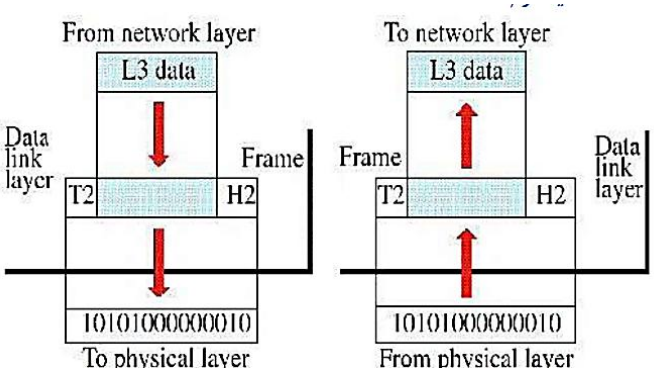


لایه اتصال داده (Data link layer)

این لایه پایین ترین لایه ای است که مربرط به بیت های در حال جابجایی روی شبکه میباشد. پروتکل های اتصال داده، مواردی مانند اندازه هر پکت داده، رسیدن پکت ها به مقصد مورد نظر و عدم ارسال پکت ها از سوی نادها روی شبکه بصورت همزمان را کنترل میکنند. در این لایه شناسایی و اصلاح خطای ابتدایی نیز انجام میگیرد تا اطمینان حاصل شود که داده های دریافت شده، همان داده های ارسال شده باشند. اگر خطای غیرقابل اصلاحی رخ دهد، استاندارد اتصال داده تعیین میکند که ناد چگونه باید در از خطای رخ داده شده اطلاع پیدا کند و دوباره به انتقال داده ها بپردازد.

در این لایه، هر دستگاه روی شبکه ادرسی بنام آدرس کنترل رسانه یا MAC دارد. این آدرس معمولا بطور سخت افزاری در هر ابزار شبکه وجود دارد و توسط سازنده در آن تعبیه میشود.

آدرس های MAC منحصربفرد هستند. هیچ دو ابزار شبکه ساخت هر سازنده ای در هر جای جهان، نمیتوانند آدرس MAC یکسانی داشته باشند.



یکی از مهمترین عملکردهای لایه اتصال داده، فراهم کردن روشی است که پکت ها بتوانند با امنیت روی رسانه فیزیکی ارسال شوند بدون اینکه ناد های دیگر با ارسال همزمان داده ها، ایجاد مزاحمت نمایند. دو روش از معروف ترین روش های این کار csma/cd و token passing میباشند. شبکه های اترنت از csma/cd استفاده میکنند و شبکه های توکن رینگ از روش توکن پسینگ.

دونوع اصلی ابزارهای لایه اتصال داده که در شبکه ها بطور معمول استفاده میشوند، بریج ها و سویچ ها میباشند. یک بریج تقویت کننده هوشمندی است که آدرس های MAC ناد های آنسوی پل را میشناسد و میتواند پکت ها را با توجه به این آدرس دهی هدایت کند. سویچ، هاب هوشمندی است که آدرس MAC را بررسی میکند و پورتی که باید پکت به آن ارسال شود را شناسایی میکند.

نحوه کار csma/cd

یکی از عملکردهای مهم لایه اتصال داده، حصول اطمینان از عدم ارسال پکت ها از سوی دو کامپیوتربطور همزمان میباشند. اگر چنین حالتی اتفاق بیفتد، سیگنال ها به یکدیگر برخورد کرده وارتباط قطع میشود. این مشکل در اترنت به کمک تکنیکی بنام csma/cd یا « دسترسی چندگانه حس انتقال با اصلاح تصادم » حل شده است. این اصطلاح با اینکه پیچیده است، ولی اگر آنرا به چند قسمت تقسیم کنیم، مفهوم ساده ای بدست خواهد آمد.

حس انتقال، یعنی هنگامی که دستگاهی میخواهد پکتی را روی شبکه بفرستد، ابتدا رسانه شبکه را بررسی میکند تا ببیند که آیا فرد دیگری در حال ارسال داده روی رسانه هست یا نه. اگر هیچ ارسالی احساس نشد، کامپیوتر به آزاد بودن شبکه پی برده و پکت خود را ارسال میکند.

دسترسی چندگانه، یعنی اینکه هیچ چیزی از ارسال پکت ها توسط دو یا چند سیستم بطور همزمان جلوگیری نکند. البته هر وسیله قبل از ارسال داده ها، کابل را از جهت ترافیک کنترل میکند. با این حال، فرض کنید که دو دستگاه هر دو این کنترل را انجام میدهند و بار ترافیکی پیدا نمی کنند وهر دو همزمان پکت های خود را ارسال میکنند. این مانند حالتی است که شما و یک ماشین دیگر همزمان به تقاطع میرسید. بعد از کمی تعارف، هر دوی شما حرکت کرده و از تقاطع عبور خواهید کرد.

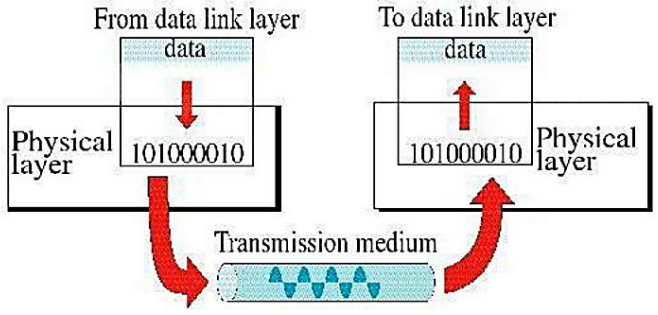
شناسایی تصادم یعنی اینکه پس از ارسال پکت توسط دستگاه، دستگاه دقت میکند که پکت به پکت دیگری برخورد کرده یا نه. اگر احتمال برخورد وجود داشته باشد یا برخورد انجام شود، دستگاه پس از مدت زمانی تصادفی، دوباره بسته خود را ارسال میکند. چون این زمان تصادفی است، پس هرگز دو پاکت به هم برخورد نخواهند کرد.

csma/cd برای شبکه های کوچک بخوبی کار میکند. پس از اینکه شبکه دارای حدود ۳۰ کامپیوتر شد، تصادم پکت ها بسیار بیشتر خواهد شد و شبکه کند خواهد شد. در چنین حالتی شبکه باید به دو یا چند بخش مجزا از هم تقسیم شود که اصطلاحا دامنه های تصادم نامیده میشوند.

لایه فیزیکی (Physical layer)

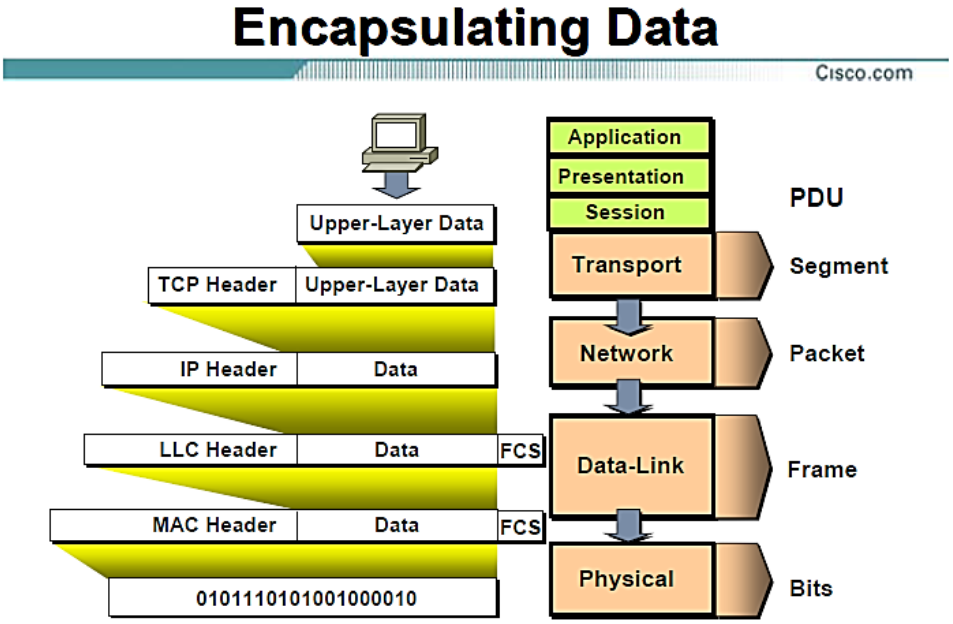
در این لایه اطلاعات دریافتی از لایه های بالاتر تبدیل به یک سری بیتهای ۰ و ۱ شده و جهت انتقال برروی بستر ارتباطی، تبدیل به سیگنال الکتریکی و یا موج نوری خواهند شد.

در این لایه هیچ پردازشی بر اطلاعات ارسالی و یا دریافتی صورت نمی گیرد. نکاتی که در این لایه مورد اهمیت می باشد نوع بستری ارتباطی و پهنای باند مربوط به آن و نرخ ارسال اطلاعات و نوع مدولاسیون مورد اهمیت می باشد.



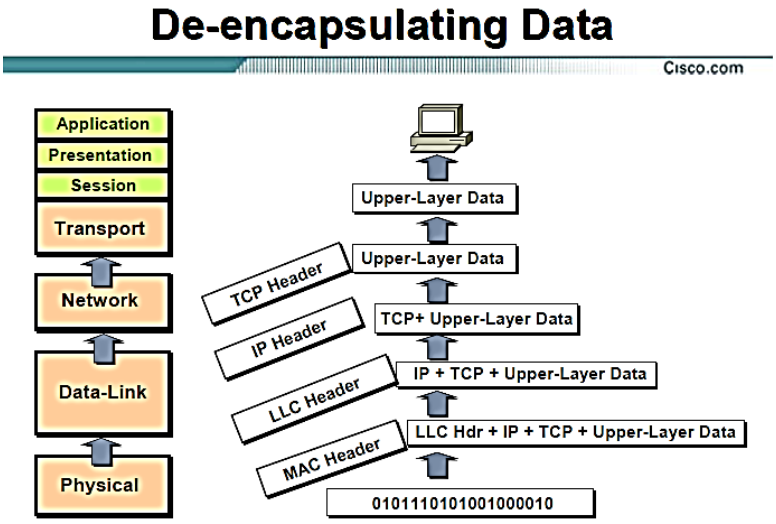
کارت شبکه به عنوان یک واسط ارتباطی در این لایه، اطلاعات دریافتی از لایه بالاتر را دریافت و پس از تبدیل به بیتهای صفر ویک، تحویل بستر ارتباطی می دهد.

در لایه دوم یا Data Link Layer با اضافه شدن LLC Header و Mac Header به آن بسته بندی جدیدی به نام Frame خواهیم داشت و در نهایت فریم ها تبدیل به یک سری بیتهای ۰ و ۱ شده و جهت انتقال روی بستر ارتباطی به سیگنالهای الکتریکی و یا نوری تبدیل می شوند.



بسته بندی کردن داده ها در هر لایه به سمت گیرنده

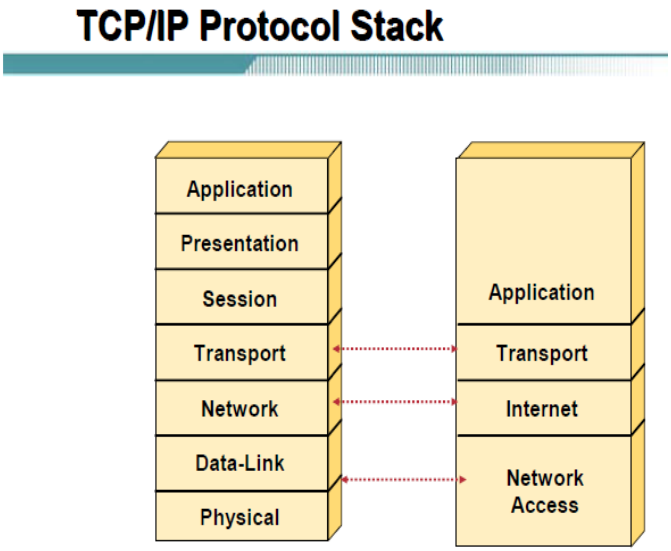
تا به اینجا هفت لایه osi و پروسه مربوط به آن را از لایه هفتم تا لایه اول بررسی کردیم . از سوی دیگر زمانیکه بیتهای ۰ و ۱ توسط لایه یک (physical layer) دریافت شدند در اختیار لایه دوم قرار می گیرند تا با مشخص شدن mac header و LLC header و رفع نیاز های لایه دوم در اختیار لایه سوم قرار گیرد. در لایه سوم هر کدام از پکتها بررسی شده وپس از مشخص شدن آدرس مبدا و مقصد ، تحویل لایه بالاتر، transport layer داده می شود. در این لایه با توجه به tcp header و یا udp header ، شماره پورت مورد نظر و نحوه دریافت اطلاعات مشخص شده و در نهایت با مشخص شن فرمت و باز شدن داده های فشرده و کد شده در اختیار لایه هفتم و نرم افزارهایی چون مرورگر web قرار می گیرد.



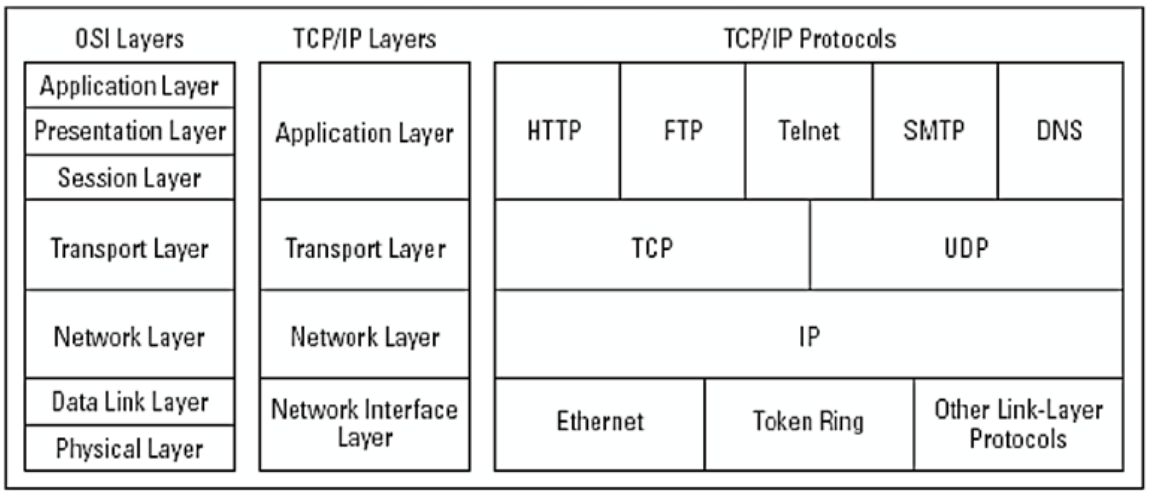
پروتکل چهار لایه TCP/IP

محصـــول پروژه تحقیقاتی شـــبکه arpanet مربوط به آژانس پروژه های تحقیقاتی دفاعی (darpa) وابســـته به وزارت فاع امریکا می باشد . این معماری که مروزه اساس شبکه جهانی اینترنت به حساب می آید یک معماری چهار لایه ای به شرح زیر می باشد :

- Application
- Transport
- Internet
- (Network Access) Network Interface



ساختار کلی لایه های مدل OSI و TCP/IP



معماری شبکه

معماری یک شبکه بیانگر استانداردهای تعریف شده درخصوص نحوه اتصال کامپیوتر ها با یکدیگر و نحوه ارسال اطلاعات می باشد. به عبارت دیگر، *معماری شبکه مجموعه ای از استاندارد هایی است که نوع کابل کشی. اتصالات. توپولوژی. نحوه دسترسی به خطوط انتقال و سرعت انتقال را مشخص می کند.* بنابراین هنگام راه اندازی یک شبکه ، باید ابتدا معماری شبکه مشخص شود و سپس باتوجه به استاندارد هایی که معماری شبکه مشخص میکند، قطعات و اتصالات شبکه خریداری و پیکربندی گرد.

شناخت استانداردها

یک استاندارد، توافقی بر اساس یک تروتکل است. در روزهای آغازین شبکه های کامپیوتری . هر سازنده کامپیوتر پروتکل های شبکه بندی مختص خود را ایجاد میکرد. در نتیجه ، امکان ترکیب قطعات از سازندگان مختلف در یک شبکه وجود نداشت .

بنابراین استاندارد ها بوجود آمدند. استاندارد ها پروتکل های تعریف شده در مقیاس صنعتی هستند که به یک سازنده خاص محدود نمیشوند. با پروتکلهای استاندارد، میتوانید قطعات ساخت سازندگان مختلف را با همخوانی کامل استفاده کنید. تا زمانی که قطعه ای از استانداردهای خاص پیروی کند، میتواند درون شبکه قرار گرفته و کار کند.

سازمانهای بسیاری در رابطه را تهیه استاندارد های شبکه بندی فعالیت میکنند که پنج سازمان از مهمترین سازمانهای استاندارد سازی را معرفی میکنیم :

- **انسیتوی استانداردهای ملی امریکا(ANSI) :** سازمان رسمی استاندارد ها در ایالات متحده .
- **انسیتوی مهندسی الکتریک و الکترونیک (IEEE) :** سازمانی بین المللی که چندین استاندارد کلیدی شبکه را منتشر کرده است. استاندارد رسمی برای سیستم شبکه بندی اترنت که بطور رسمی 3 . 802 IEEE نام گرفته است، از این جمله میباشد.
- **سازمان بین المللی استاندارد سازی (ISO) :** تشکیلات متشکل از بیش از ۱۰۰ سازمان استانداردسازی از سطح جهان .
- **نیروی کاری مهندسی اینترنت (IETF) :** سازمانی که مسئول پروتکلهای کاربردی اینترنت میباشد .
- **کنسرسیوم وب (W3C) :** سازمانی بین المللی که کنترل کننده ایجاد و توسعه استاندارد های وب است .

انواع معماری شبکه

- Ethernet
- Token Ring
- FDDI
- Wireless

پروتکل اترنت

همانطور که میدانید، اولین دو لایه از مدل OSI با ساختار فیزیکی شبکه ارتباط دارند، به این مفهوم که تعیین میکنند کدام ابزارهای شبکه میتوانند اطلاعات را از دستگاهی به دستگاه دیگر ارسال کنند. محبوب ترین پروتکل برای لایه های فیزیکی و اتصال داده ، اترنت است.

اترنت از اوایل دهه ۱۹۷۰ تا کنون به شکل های مختلفی ارائه شده است. وضعیت فعلی اترنت توسط استاندارد IEEE بنام 3 . 802 تعریف شده است. حالات مختلفی از اترنت در سرعت های مختلف و روی رسانه های مختلف مورد استفاده قرار

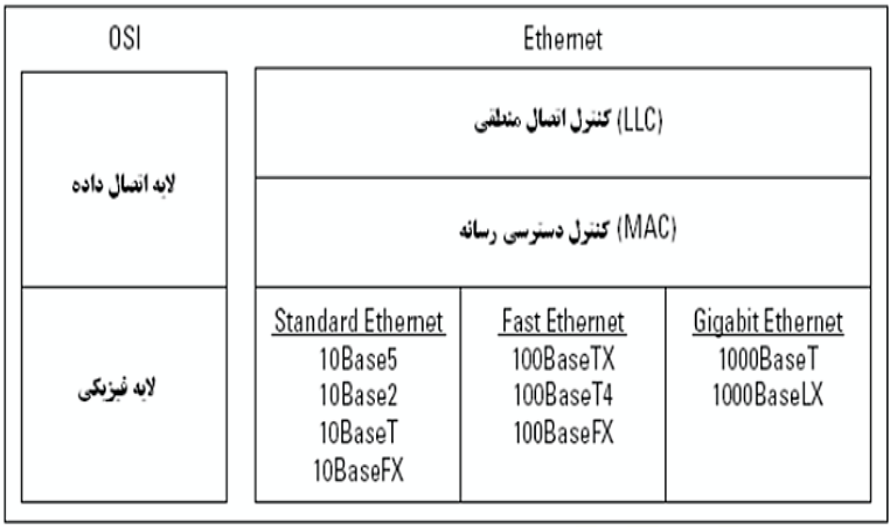
میگیرند. چون تمام نسخه های اترنت باهم سازگاری دارند، میتوانید در یک شبکه با استفاده از ابزارهایی مانند سویچ ها، بریج ها و هاب ها ترکیبی از ارتباطات را با رسانه های مختلف و سرعت های مختلف ایجاد کنید.

سرعت انتقال واقعی اترنت بصورت میلیون بیت بر ثانیه یا Mbps اندازه گیری میشود. اترنت در سه سرعت مختلف وجود دارد. ۱۰ مگابیت بر ثانیه که اترنت استاندارد است، ۱۰۰ مگابیت بر ثانیه که اترنت سریع است و ۱۰۰۰ مگابیت بر ثانیه که اترنت گیگابیت نامیده میشود. بیاد داشته باشید که سرعت های بیان شده، در واقع سرعت های حداکثری هستند که در شرایط ایده آل شبکه بدست می آیند. در دنیای واقعی، جریان عبوری اترنت به سختی به این میزان ماکزیمم میرسد.

اترنت در دو لایه ابتدایی مدل OSI کار میکند. این استاندارد، لایه اتصال داده را به دو لایه مجزا تقسیم میکند که کنترل اتصال منطقی(LLC) و کنترل دسترسی رسانه (MAC) نامیده میشوند.

اترنت استاندارد

اترنت استاندارد، اترنت اصلی است. این اترنت با سرعت 10Mbps کار میکند که در دهه ۱۹۷۰ سریع بحساب می آمد، ولی امروزه از استاندارد های بسیار کند است. چون هزینه اترنت سریع در سالهای اخیر بسیار کاهش یافته، بنابراین این استاندارد جایگزین اترنت استاندارد در بسیاری از شبکه های جدید شده است. با این حال، شبکه هایی نیز وجود دارند که هنوز از اترنت استاندارد استفاده میکنند.



اترنت استاندارد در چهار طبقه بندی با توجه به نوع کابل مورد استفاده برای شبکه بندی قرار میگیرد:

- **10Base5 :** کابل اصلی اترنت که ضخیم (به ضخامت انگشت شست) و سنگین بود و کار با آن بسیار مشکل بود. این کابل امروزه فقط در موزه های IT به چشم میخورد.
- **10Base2 :** این نوع نازکتر از کابل کواکسیال (کابل آنتن) در دهه ۸۰ محبوبیت یافت و تا اوایل دهه ۹۰ رایج بود. هنوز هم مقدار زیادی از کابل های 10Base2 مورد استفاده قرار میگیرد، ولی در شبکه های جدید خیلی کم مورد استفاده قرار میگیرد. این کابل نیز مانند کابل استاندارد، اجبارا توپولوژی خطی را تحمیل میکند.
- **10BaseT :** کابل های جفت تابیده بدون پوشش(UTP) در دهه ۹۰ رواج یافتند چون نصب آنها بسیار ساده تر بود و کابلهای سبک تر و مطمئن تر بودند و انعطاف پذیری را برای طراح شبکه بوجود می آورند. شبکه های 10BaseT از توپولوژی ستاره ای به کمک هاب ها بعنوان مرکز ستاره استفاده میکنند. حداکثر طول کابل 10BaseT فقط ۱۰۰ متر است و میتوان برای طولانی تر کردن مسیر، هاب ها را بصورت زنجیره ای بهم متصل کرد. کابل 10BaseT چهار جفت سیم دارد که دور هم تابیده شده اند. چون 10BaseT فقط از دو جفت سیم استفاده میکند، پس دو جفت دیگر اضافص هستند.

- **10BaseFL :** کابلهای فیبرنوری با استاندارد 10BaseFL در سرعت 10Mbps پشتیبانی میشدند. چون نسخه های جدید و سریع فیبرنوری وجود دارد، 10BaseFL بسیار کم مورد استفاده قرار میگیرد.

اترنت سریع

اترنت سریع به اترنتی اطلاق میشود که با سرعت 100Mbps کارمیکند که ۱۰ برابر سریعتر از اترنت استاندارد است. سه نوع مختلف اترنت سریع عبارتند از :

- **100BaseT4:** این پروتکل سرعت انتقال 100Mbps را روی همان کابل UTP شبکه های 10BaseT4 ایجاد میکند. برای این کار، هر چهار جفت سیم موجود در کابل مورد استفاده قرار میگیرند. 100BaseT4 عمل ارتقای شبکه موجود 100BaseT4 را به 100Mbps تسهیل میکند.
- **100BaseTX :** معمولترین استاندارد مورد استفاده برای شبکه های اداری امروزی، 100BaseTX میباشد که سرعت 100Mbps را فقط روی جفت سیم از کابل UTP درجه بالاتر را امکان پذیر میکند. کابلی که درجه بالاتری نسبت به 10BaseT دارد، Category5 یا در اصطلاح بازار CAT5 نامیده میشود. بسیاری از شبکه های جدید با کابلهای CAT5یا کابلهای بهتر شبکه بندی میشوند.

100BaseFX : نسخه فیبرنوری اترنت که با سرعت 100Mbps کار میکند. چون کابل فیبرنوری گران است و نصب آن مشکل تر است، زیاد برا یکامپیوترها وشبکه های شخصی مورداستفاده قرار نمیگیرد . این اتصال معمولا بعنوان ستون فقرات شبکه استفاده میشود. برای مثال، یک ستون فقرات فیبرنوری معمولا برای اتصال گروه های کاری مختلف به سرور ها و روترها مورد استفاده قرار میگیرد.

اترنت گیگابایت

اترنت گیگابیت اترنتی است که با سرعت 100Mbps کار میکند که ۱۰۰ برابر سریعتر از اترنت استاندارد میباشد. این اتصال در شبکه های بسیار بزرگ برای ایجاد ستون فقرات بین سرورها و شبکه مورد استفاده قرار میگیرد. در برخی موارد، اترنت گیگابیت حتی برای اتصال کامپیوتر های رومیزی که نیاز به شبکه بندی سریع دارند مورد استفاده قرار میگیرد. اترنت گیگابیت در دو حالت وجود دارد :

- **100BaseT** : که میتواند روی کابل CAT5 ایجاد شود، ولی کابلهای درجه بالاتر مانند CAT5e یا CAT6 بهتر عمل میکنند و قابل اطمینان ترند.
- **1000BaseLX** : که همین اتصال از طریق فیبرنوری است.

به عنوان مثال پهنای باند ارائه شده توسط اترنت در ابتدا ۱۰ مگابیت در ثانیه بود و برای کامپیوتر های شخصی دهه ۸۰ که دارای سرعت پائین بودند، کافی بنظر می آمد؛ ولی در اوایل سال ۱۹۹۰ که سرعت کامپیوتر های شخصی و اندازه فایل ها افزایش یافت. مشکل پائین بودن سرعت انتقال داده بهتر نمایان شد. اکثر مشکلات فوق به کم بودن پهنای باند موجود مربوط می گردید. در سال ۱۹۹۵ موسسه IEEE ، استانداردی را برای اترنت با سرعت ۱۰۰ مگابیت در ثانیه معرفی نمود. این روال ادامه یافت و در سال های ۱۹۹۸ و ۱۹۹۹ استاندارد هایی برای گیگابیت نیز ارائه گردید. تمامی استانداردهای ارائه شده با استاندارد اولیه اترنت سازگار می باشند. به عنوان مثال یک فریم اترنت می تواند از طریق یک کارت شبکه با کابل کواکسیال ۱۰ مگابیت در ثانیه از یک کامپیوتر شخصی خارج و بر روی یک لینک فیبر نوری اترنت ۱۰ گیگابیت در ثانیه ارسال و در انتها به یک کارت شبکه با سرعت ۱۰۰ مگابیت در ثانیه برسد. تا زمانی که بسته اطلاعاتی بر روی شبکه های اترنت باقی است در آن تغییری داده نخواهد شد. موضوع فوق وجود استعداد لازم برای رشد و گسترش اترنت را به خوبی نشان می دهد. بدین ترتیب امکان تغییر پهنای باند بدون ضرورت تغییر در تکنولوژی های اساسی اترنت همواره وجود خواهد داشت.

مفهوم پهنای باند (Band Width):

در سیستم های انتقال آنالوگ ، پهنای باند به حد فاصل بین پایین ترین و بالاترین فرکانسی که یک رسانه می تواند از خود عبور دهد گفته می شود. (پهنای باند بر حسب فرکانس و با واحد هرتز بیان می شود) (300HZ – 300HZ) در سیستم های انتقال دیجیتال ، پهنای باند به ظرفیت انتقال اطلاعات گفته می شود و با واحد bps(بیت در ثانیه) سنجیده می شود. از عوامل موثر در پهنای باند : طول ، قطر و جنس کابل است، پهنای باند با طول کابل نسبت معکوس و با قطر کابل نسبت مستقیم دارد. یعنی هرچه طول کابل بیشتر شود پهنای باند کمتر شود و هرچه قطر کابل بیشتر شود پهنای باند نیز بیشتر است.

برای انتقال اططلاعات میتوان به دو روش از پهنای باند استفاده کرد :

۱. تک باند (Base Band)
۲. باند پهن (Band Broad)

۱. در روش Base Band (تک باند)، از تمام پهنای باند برای ارسال یا دریافت اطلاعات استفاده می شود. به این معنی که در روش تک باند رسانه در هر لحظه فقط میتواند یک سیگنال را از خود عبور دهد در نتیجه ارسال نوبتی می شود و اطلاعات پشت سرهم و به صورت سریال ارسال می شوند. این روش انتقال دلیل به وجود آمدن مفهوم بسته (Packet) است. در شبکه های محلی از این روش برای انتقال اطلاعات استفاده می شوند. بدین ترتیب که از دو رشته کابل استفاده می شود که یکی برای ارسال و دیگری دریافت اطلاعات را انجام میدهد. اطلاعات به صورت بسته های مشخص پشت سر هم قرار میگیرند و ارسال شده و دریافت میگردد. (تمام سیستم های انتقال دیجیتال از روش Base Band استفاده میکنند) (کابل هم محور UTP)

۲. در روش Band Broad (باند پهن) ، یک رسانه (کابل) میتواند در آن واحد یک یا چند سیگنال را به طور همزمان عبور دهد. هر سیگنال به صورت جداگانه ارسال می شود و تداخل بین سیگنال هایی متفاوت به وجود نمی آید. از این روش در سیستم های انتقال آنالوگ استفاده می شود و رسانه می تواند در آن واحد سیگنالهای متفاوتی را با فرکانس های مختلف از خود عبور دهد. از این روش در شبکه تلویزیون های کابلی و شبکه های WAN استفاده میگردد. (کابل هم محور – فیبر نوری) .

مفهموم سرعت انتقال اطلاعات

مقدار اطلاعاتی که در واحد زمان توسط تجهیزات شبکه ارسال می شود گفته می شود (مثلا کارت شبکه 100 Mbps) . سرعت انتقال اطلاعات با پهنای باند رابطه مستقیم دارد. هر چه پهنایباند بیشتر شود سرعت انتقال اطلاعات نیز بیشتر می شود و بر عکس .

نکته : پهنای باند، ظریفت انتقال یک رسانه یا یک کابل است. در صورتی که سرعت انتقال، سرعت ارسال اطلاعات در واحد زمان است.

Token Ring

شبکه Token Ring از نظر ظاهری یک شبکه ستاره ای است ولی به صورت Token Passing کار میکند. در این شبکه یک حلقه منطقی به وجود می آید و Token در امتداد حلقه حرکت کرده و به کامپیوتر ها میرسد. هر کامپیوتری که به ارسال اطلاعات نیاز داشته باشد. Token را نگه داشته و اطلاعات خود را به سوی مقصد ارسال میکند. اطلاعات ارسال شده در همان حلقه مجازی و در امتداد حرکت Token مسیر خود را طی میکند تا به کامپیوتر مقصد برسد. کامپیوتر مقصد در صورت صحیح بودن اطلاعات ارسالی، در جواب یک بسته به نام Acknowledge به کامپیوتر مبدا ارسال می کند. کامپیوتر مبدا نیز Token اصلی را از بین برده و یک Token جدید تولید می نماید و آن را در امتداد مسیر Token قبلی به حرکت در می

آورد.

این پروسه به همین صورت ادامه خواهد یافت.

در شبکه Token Ring در محل اتصال کامپیوتر ها به جای هاب از دستگاهی بنام MAU استفاده می شود. سرعت انتقال اطلاعات در این شبکه 16 Mbps یا 4 Mbpsاست. کارت های 16 Mbps می توانند با سرعت 4 Mbps نیز فعالیت کنند. در شبکه Token Ring از کابل های زوج به هم تابیده استفاده می شود. اگر از کابل UTP در این توپولوژی استفاده شود، حداکثر طول کابل میتوانند ۴۵ متر باشد و این شبکه فقط با سرعت ۴ مگابیت در ثانیه کار می کند و اگر از کابل STP استفاده شود. حداکثر طول کابل ۱۰۱ متر و با سرعت ۱۶ مگابیت در ثانیه اطلاعات منتقل می شود.

FDDI (Fiber Distributed Data Interface)

Fddi، تکنولوژی یک شبکه با سرعت ۱۰۰ مگابیت در ثانیه است که برای ارتباط از فیبر نوری استفاده میکند. در این تکنولوژی به جای فیبر نوری از کابل مسی نیز می توان استفاده کرد ولی در صورت استفاده از کابل مسی طول کابل کمتر می شود. Fddi به عنوان Backbone در محل هایی که تعداد زیادی کامپیوتر در آن قرار دارد، استفاده می شود. از جمله این محیط ها می توان به دانشگاه ها اشاره کرد. در fddi میتوان ۵۰۰ گره را در مسافت ۱۰۰ کیلومتر به یکدیگر متصل کرد. توپولوژی فیزیکی این شبکه حلقوی است. نحوه به وجود آمدن این حلقه به این صورت است که یک حلقه ۱۰۰ کیلومتری از فیبر ساخته می شود و در هر ۲ کیلومتر یک تقویت کننده قرار میگیرد. برای جلوگیری از اختلالاتی که در اثر قطع شدن فیبر نوری به وجود می آید، از دو حلقه فیبرنوری در کنار هم استفاده می شود تا در صورتی که یکی از رشته ها قطع شود، رشته دوم وارد عمل شده و جایگزین رشته اول شود.

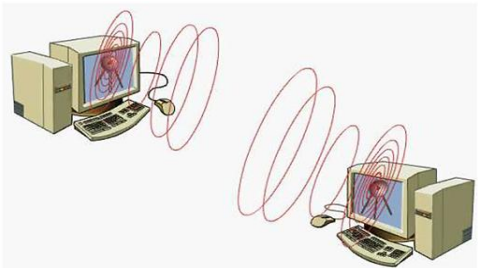
شبکه بدون سیم (Wireless)

شبکه بدون بی سیم. شبکه ای است که امواج رادیویی Broad Bandبرای مرتبط کردن کامپیوتر ها به یکدیگر استفاده می کند. از سیستم بیسیم معمولا در شبکه های Wan استفاده می شود. کاربران آن می تواند مرتبط کردن دو یا چند شبکه محلی، ارائه سرویس اینترنت و سرویس های دیگر باشد. شبکه بیسیم برای برقراری بین کامپیوتر هایی که نزدیک یکدیگر قرار دارند نیز استفاده می شود که در اینصورت نوعی شبکه به نام Pan بکار می رود. در شبکه های Pan نیازی به استفاده از تجهیزات خاص شبکه نیست و فقط با نصب دو کارت شبکه Pan روی دو کامپیوتر که در فاصله مناسب از یکدیگر قرار گرفته اند، می توان یک شبکه را راه اندازی کرد. از مزایای شبکه های بیسیم این است که نیازی به نصب کابل شبکه و تجهیزات آن نیست و سرعت انتقال اطلاعات نیز می تواند تا سرعت ۵۲ مگابیت در ثانیه افزایش پیدا کند. شبکه های بی سیم به ۲ طریق می توانند با یکدیگر ارتباط برقرار کنند.

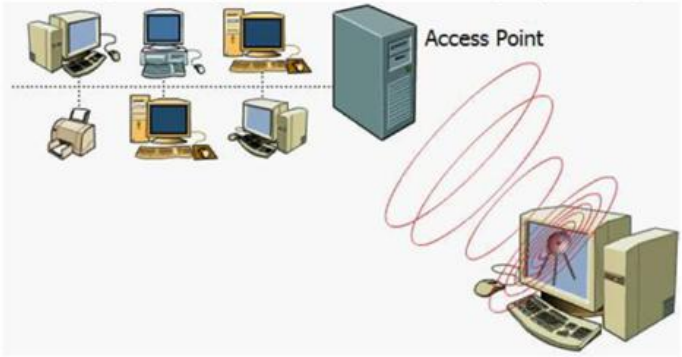
۱- Ad hoc: در این روش، دو یا چند کامپیوتر توسط کارت شبکه بی سیم و به صورت مستقیم(Peer to Peer) به یکدیگر متصل می شوند.

در این روش به هیچ عنصر سخت افزاری دیگری نیاز نمی باشد و همچنین الگوریتم مسیریابی به صورت توزیع شده و توسط تمامی کامپیوتر ها انجام می گیرد. لذا می توان در حرکت از این نوع شبکه استفاده نمود و مثلا هر کامپیوتر در یک اتومبیل جدا بوده و اتومبیل ها نیز در حال حرکت باشند.

به عبارت دیگر AD Hoc استانداردی است که ارتباط بی سیم بین رایانه و تجهیزات جانبی مانند رایانه جیبی PDAs ، تلفن همراه یا رایانه کیفی را برقرار می سازد.



۲– Infra- Structure : در این روش می توان کامپیوتری که کارت شبکه بیسیم دارد را به یک شبکه سیمی متصل نمود. بدین منظور کافی است که به یکی از سیستم های شبکه سیمی یک سخت افزار به نام Access Point یا به اختصار AP نصب کرد و از طریق آن با کامپیوتری به کارت شبکه بیسیم دارد ارتباط برقرار نمود. در این روش، بر عکس روش ad hoc ، یک نقطه مرکزی وجود دارد که به عنوان محور بوده و به عنوان محل اتصال کامپیوتر ها شناخته می شود.



انواع آدرس IP

در حال حاظر، دو نسخه IP در حال استفاده می باشد: IP نسخه ۴ و IP نسخه ۶ که هر یک نشانی IP را به روش متفاوتی ارائه می نمایند.

آدرس IP نسخه ۴

یک آدرس IPV4 از ۳۲ بیت (۰ یا ۱) تشکیل شده است. این بیت ها به چهار قسمت (که Octer یا Quad نامیده می شود) تقسیم شده اند و در هر قسمت حاوی یک بایت (۸ بیت) می باشد.

سه روش رایج جهت نمایش IP وجود دارد :

- ده دهی (مبنای ده) ، مانند 130.57.30.56
- دو دویی (مبنای دو) ، مانند 10000010.00111001.00011110.00111000
- شانزده دهی (مبنای شانزده) ، مانند 82 39 1E 38

همه مقادیری که در بالا مشاهده می نمایید، بیانگر آدرس IP یکسانی می باشند. با ۳۲ بیت موجود در آدرس های ipv4، مجموعا تعداد ۴۰۲۹۴۰۹۶۷۰۲۹۴ – $۲^{۳۲}$ آدرس از این نوع قابل ایجاد می باشد.

ساختار آدرس IP

بطور کلی آدرس های IP از دو شناسه تشکیل شده اند. یکی شناسه شبکه (NetworkID) و دیگری شناسه میزبان (HostID) . هر کدام از این شناسه ها بسته به نوع کلاس آدرس IP تعیین می شوند.

شناسه شبکه

این شناسه ، آدرس یک زیر شبکه را تعیین نموده و برای کلیه میزبان هایی که در یک زیر شبکه قرار دارند یکسان می باشد.

شناسه شبکه در واقع یک ساختار سلسله مراتبی یا لایه ای به آدرس های شبکه می دهد. به عنوان مثال آدرس 130.57.30.56 را در نظر بگیرید. این آدرس از کلاس B بوده و دو قسمت اول آن به عنوان شناسه شبکه در نظر گرفته می شود، بنابراین کلیه کاربردانی که در زیر شبکه ای با این آدرس قرار داشته باشند دو قسمت اول آدرس IP آنها با 130.57 شروع می شود.

شناسه میزبان

آدرس یک دستگاه یا میزبان در شبکه است و برای هر میزبان عددی منحصر بفرد می باشد. در مثال قبل، دو قسمت دوم از آدرس متعلق شناسه میزبان می باشد، بنابراین در آدرس هایی مانند 130.57.30.56 ، آدرس 30.56. بیانگر شناسه میزبان زیر شبکه ای با آدرس 130.57 می باشد.

کلاس های ادرس IP

بطور کلی سه کلاس آدرس دهی قابل اختصاص به کاربران توسط طراحان اینترنت به کار گرفته شده است. این کلاس ها با نام های A ، B و C شناخته می شوند. برای شبکه های خیلی بزرگ که متشکل از چندین زیرشبکه می باشند از کلاس A، و برای شبکه های بسیار کوچک از کلاس C استفاده می شوند. شبکه های متوسط نیز از کلاس B جهت آدرس دهی به کاربران خود استفاده می نمایند. تقسیم بندی آدرس های IP به آدرس های شبکه و آدرس های میزبان (NetID و HostID) نیز بر اساس همین کلاس بندی ها انجام می شود. در جدول۱-۱ خلاصه ای از مشخصات این سه کلاس آورده شده است.

کلاس	بیت های قاب زیرشبکه	الگوی بیتی راهنما	مقدار اولین اکتت۱ در آدرس	تعداد شبکه های قابل اختصاص	حداکثر میزبان ها در هر شبکه
A	8	0	1-126	126	16,777,214
B	16	01	128-191	16,384	65,534
C	24	110	192-223	2,097,152	254

جدول ۱-۱

همانظور که در جدول مشاهده می کنید، ستونی جهت نشان دادن الگوی بیت های راهنما برای هر کلاس در نظر گرفته شده است. این بیت ها در واقع بیت های شروع آدرس های هر کلاس را نشان می دهند.به عنوان مثال، آدرس 126.X.X.X را در کلاس A در نظر بگیرید. قسمت اول این آدرس عدد 126 است که معادل دودویی آن 01111110 می باشد، بنابراین در ستون مربوطه، الگوی شروع این آدرس ها با 0 نشان داده شده است. در کلاس های B وC نیز اکتت اول کلیه آدرس ها به ترتیب با الگوی 01 و110 آغاز می شوند و با تغییر آدرس ها در هر کلاس، به غیر از بیت های ذکر شده، سایر بیت ها تغییر می کنند. استفاده از این الگوهای بیتی در مسیریاب ها بسیار پرکاربرد می باشد زیرا این دستگاه ها می توانند با خواندن قسمت اول این آدرس ها الگوی بیتی آنها را بدون نیاز به دانستن سایر بیت ها تشخیص داده و از کلاس آن آدرس و همچنین قاب زیر شبکه۱ آن اگاهی یابند.

بعضی از آدرس های ip برای کاربردهای خاصی در نظر گرفته شده اند و قابل اختصاص به کاربران شبکه نمی باشند (البته به غیر از آدرس های خصوصی). در جدول ۲-۱این آدرس ها به همراه کاربر آنها آورده شده است.

آدرس	کاربرد
آدرس 0.0.0.0	بسته به قاب زیر شبکه، بیانگر همین شبکه(شبکه یا زیر شبکه ای که درحال حاظر در آن قرار دارید)یا همین میزبان می باشد.
آدرس هایی که با 127شروع می شوند	این آدرس ها برای تست های LOOPBACK استفاده می شوند و به یک میزبان اجازه می دهند تا پیغام های تست را بدون اینکه ترافیکی در شبکه ایجاد کند، برای خود ارسال نماید.
آدرس255.255.255.255	این آدرس برای ارسال پیغام ها به تمام کاربران شبکه (Multicasting) استفاده می شود و با نام های Limited broadcast و ahh-1s broadcast نیز شناخته می شود.
آدرس های **10.0.0.0 تا 10.255.255.255** **172.16.0.0 تا 172.31.255.255** **192.168.0.0 تا 192.168.255.255**	این آدرس ها به عنوان آدرس های خصوصی/نامعتبر۲ برای کلاس های A، B و C در نظر گرفته شده اند. آدرس های خصوصی در استاندارد RFC 1918 تعریف شده و قابل استفاده در اینترنت نمی باشند. از این آدرس ها در سرورهای NAT و شبکه های IP غیرمتصل به اینترنت (شبکه های داخلی یا همان شبکه های خصوصی)استفاده می شود.
آدرس های 169.254.0.0 با قاب زیرشبکه255.255.0.0	این آدرس ها فقط در ارتباطات نقطه به نقطه میان دستگاه ها در یک شبکه به کار رفته و از قابلیت ارسال پیغام ها توسط مسیریاب برخوردار نمی باشند. این آدرس ها ، آدرس های 1APIPA گفته می شود.

جدول ۲-۱: آدرس های IP با کاربرد های خاص

کلاس A

در کلاس A بایت اول (۸بیت اول از سمت چپ) برا یآدرس شبکه وسه بایت باقیمانده برای آدرس های میزبان استفاده می شود و فرمت آدرس های این کلاس به صورت **Network.Host.Host.Host** می باشد. به عنوان مثال در آدرس 92.22.102.70 عدد *92 آدرس شبکه* و *22.102.70 آدرس میزبان* را نشان می دهند. در این مثال، هر دستگاه در شبکه دارای یک آدرس متمایز به همراه آدرس شبکه 49 می باشد.

در کلاس A می توان از ۱۲۶ زیرشبکه استفاده نمود. علت این است که آدرس شبکه در این کلاس یک بایت است و اولین بیت از آن (با صفر) رزرو شده است، بنابراین هفت بیت باقیمانده در این بایت قابل استفاده می باشند. این بدین معناست که بیت های تشکیل دهنده این کلاس حداکثر می توانند دارای مقدار ۱۲۸ باشند(هر کدام از این هفت بیت می توانند مقدار ۰ یا ۱ را اختیار کنند که در مجموع ۲۷ یا ۱۲۸ موقعیت را فراهم می نمایند)، البته آدرس هایی که با 00000000 (بایت اول با بیت های صفر) و 01111111 (معادل با ۱۲۷ که آدرس هایLoopback می باشند) شروع می شوند، رزرو شده هستند. بنابراین از ۱۲۸ موقعیت، دو موقعیت رزرو شده و در نهایت ۱۲۶ – ۲– ۱۲۸ موقعیت در دسترس است، پس تعداد زیرشبکه های قابل آدرس دهی در کلاس A برابر با ۱۲۶ می باشند.

در این کلاس سه بایت آخر آدرس (۲۴ بیت آخر) تعلق به آدرس میزبان می باشند، به این معنا که ۲۱۶، ۷۷۷، ۱۶ – ۲۲۴ ترکیب متمایز از این ۲۴ بیت وجود دارد. چون آدرس های 0.0.0 و 255.255.255 رزرو شده هستند در نهایت تعداد ۲۱۶، ۷۷۷، ۱۶ – ۲۲۴ آدرس قابل اختصاص به میزبان ها در کلاس a موجود می باشد.

کلاس B

در کلاس B، دو بایت اول به عنوان آدرس شبکه و دو بایت باقیمانده به عنوان آدرس میزبان در نظر گرفته می شوند. فرمت آدرس های این کلاس به صورت **Network.Network.Host.Host** می باشد. به عنوان مثال در آدرس 130.57.30.56، *آدرس شبکه برابر با 130.57* و *آدرس میزبان نیز 30.56* می باشد.

تعداد بیت های آدرس شبکه در کلاس B برابر ۱۶ بیت می باشد، بنابراین تعداد۶۵،۵۳۶ –۲۱۶ ترکیب متمایز از بیت ها وجود دارد. اما با توجه به نظر طراحان اینترنت مبنی بر اینکه آدرس های این کلاس باید با بیت های 01 شروع شوند، در نهایت ۱۴ بیت قابل استفاده است. بنابراین تعداد زیرشبکه ها در کلاس برابر با ۶۵،۵۳۶ – ۲۱۴ می باشد.

در کلاس B دو بایت آخر به عنوان آدرس میزبان در نظر گرفته می شود، این دو بایت نیز از ۱۶ بیت تشکیل شده اند، بنابراین ۶۵،۵۳۶ –۲۱۶ ترکیب متمایز برای آنها وجود دارد. چون آدرس های 0.0. و 255.255. (آدرس هایی که دو قسمت آخر آنها به شکل مذکور می باشد) رزرو شده هستند، تعداد میزبان های قابل آدرس دهی در این کلاس برابر با ۵۳۴،۶۵ –۲ – ۲۱۶ خواهد بود.

کلاس C

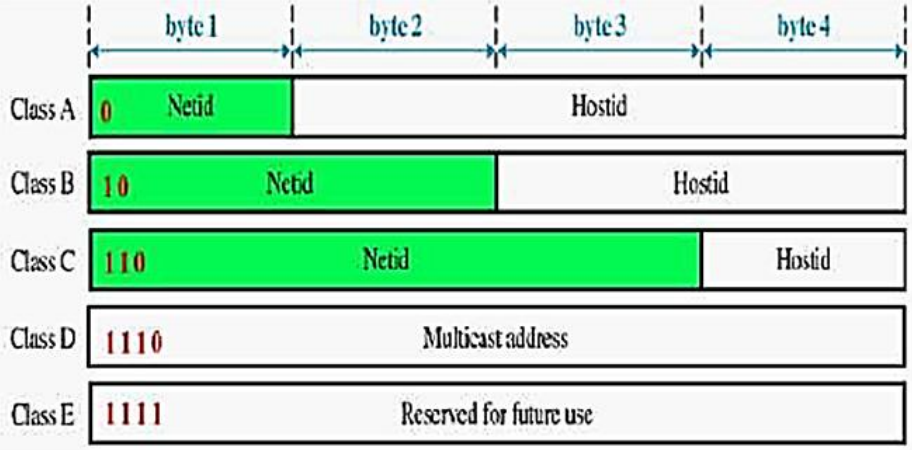
در کلاس c سه بایت اول به عنوان آدرس شبکه و یک بایت باقیمانده به عنوان آدرس میزبان درنظر گرفته می شود. فرمت آدرس ها در این کلاس به صورت Network.Network.Network.Host می باشد. به عنوان مثال در آدرس 198.21.74.102، *آدرس شبکه 198.21.74* و *آدرس میزبان 102* می باشد.

آدرس های کلاس c به سه بیت ۱۱۰ آغاز می شوند، بنابراین از ۲۴ بیتی که تشکیل دهنده آدرس شبکه در این کلاس هستند، بیت کسر شده و در نهایت تعداد ۲۱ بیت (قابل دستکاری) باقی می ماند.

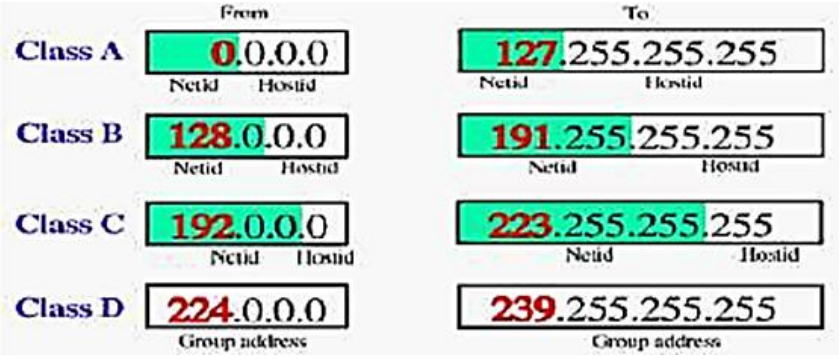
پس تعداد ۲،۰۹۷،۱۵۲ – ۲۲۱ زیر شبکه در کلاس C قابل ایجاد می باشد. الگوی بیتی ۱۱۰ نشان دهنده عد ۱۹۲ (11000000) بوده و با دستگاری سایر بیت ها تا عدد ۲ (11011101) نیز قابل مقدار دهی می باشد، بنابراین روشی ساده برای تشخیص آدرس های کلاس c این است که اکتت اول با اعداد بین ۱۹۲ تا ۲۲۳ شروع شده باشد صرف نظر از اینکه اکتت های دوم و سوم دارای چه مقادیری باشند.

در کلاس C بایت آخر به عنوان آدرس میزبان در نظر گرفته می شود. پس با اشتن ۸ بیت تعداد ۲۵۶ – ۲۸ آدرس متمایز وجود خواهد داشت. چون و آدرس 0. و 255. رزرو شده هستند در نهایت تعداد ۲۵۴ آدرس قابل اختصاص به میزبان ها در کلاس c قابل دسترسی می باشد.

دو کلاس دیگر از آدرس های IP، کلاس های D وE هستند. آدرس های کلاس D به آدرس های Multicast یا چند پخشی معروف هستند و برای موارد Multicasting یا ارسال پیغام ها به صورت همزمان به بیش از یک کاربر (چندبخشی) در شبکه استفاده می شوند. دامنه این آدرس ها از 224.0.0.0 تا 239.255.255.255 می باشد. آدرس های کلاس E نیز جهت استفاده در آینده رزرو شه اند و دامنه آنها از 240.0.0.0 تا 255.255.255.255 می باشد. آدرس های این کلاس جهت موارد آزمایشی مورد استفاده قرار می گیرد. شکل زیر تصویر بهتری از کلاس های آدرس IP به شما می دهد.



تصویر زیر نیز محدوده هر کلاس IP را نشان می دهد.



آدرس IP نسخه ۶

IPv6 نسخه بازسازی شده IPv4 است که به دلیل مواجه شدن با مشکل کمبود آدرس های IPv4 ایجاد شد. در بحث IPv4 گفتیم که این آدرس ها از ۳۲ بیت تشکیل شده اند، بنابراین کل آدرس های موجود در این نوع برابر با ۴،۲۹۶،۹۶۷،۲۹۶ – ۲۳۲ می باشند.

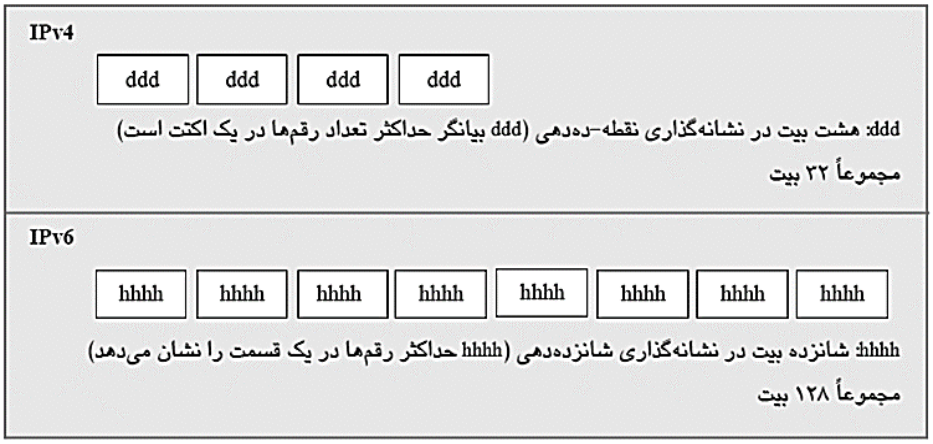
در IPv6 تعداد بیت های تشکیل هنده آدرس به ۱۲۸ بیت افزایش یافته است که با استفاده از آن می توان ۳۴۰،۲۸۲،۳۶۶،۹۲۰،۹۳۸،۴۶۳،۴۶۳،۳۷۴،۶۰۷،۴۳۱،۷۶۸،۲۱۱،۴۵۶ – ۲۱۲۸ (یا ۱۰۳۸ * ۳,۴) آدرس کختلف ایجاد نمود. در ویندوز های ویستا و سرور ۲۰۰۸ به بعد، از این آدرس ها به خوبی پشتیبانی می شود. آدرس های IPv4 بورت چهار اکتت که دارای مقادیر ده دهی و یا مقادیر دودویی متناظر با آنها هستند نمایش داده می شوند. در IPv6 شیوه نمایش آدرس ها متفاوت خواهد بود. ۱۲۸ بیت تشکیل دهنده این آدرس ها به هشت قسمت ۱۶ بیتی تقسیم شده و هر قسمت با ترکیبی از اعداد 0تا 9 وحروفa تا f (a=10، b=11، c=12، d=13، e=14، f=15) نشان داده می شود. در واقع این اعدادو حروف، آدرس IP را به صورت شانزده دهی(مبنای ۱۶) نشان می دهند. یک آدرس IPv6 به صورت زیر می باشد:

2001:0db8:0000:0000:1234:0000:a9fe:133e

معادل دودویی هر قسمت از آدرس بالا به ترتیب (از چپ به راست) به صورت زیر نشان داده می شود:

0010 0000 0000 0001 :0000 0000 0000 0000 : 0000 0000 0000 0000 :0000 1101 1011 1000 : 0001 0011 0011 1110 :0001 0011 0100 : 0000 0000 0000 0000 : 1010 1001 1111 1110 :0010 0011 0100

در شکل زیر مقایسه آدرس های IPv4و IPv6 نشان داده شده است.



انواع تجهیزات شبکه

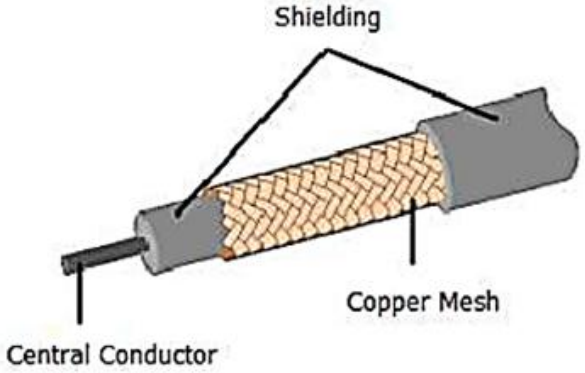
تجهیزاتی که در این بخش با آن آشنا می شوید:

- کابل شبکه – Cable
- کارت واسط شبکه – NIC
- تکرار کننده – Repeater
- هاب – HUB
- سوئیچ – Switch
- پل – Bridge
- دروازه – Gateway
- مسیر یاب – Router

کابل های شبکه

کابل کواکسیال

یکی از مهمترین محیط های انتقال در مخابرات کابل کواکسیال و یا هم محور می باش. این نوع کابل ها از سال ۱۹۳۶ برای انتقال اخبار و اطلاعات در دنیا به کار گرفته شده اند. در این نوع کابل ها، دو سیم تشکیل هنده یک زوج، از حالت متقارن خارج شده و هر زوج از یک سیم ر مغز و یک لایه مسی بافته شده در اطراف آن تشکیل می گرد. ماده ای پلاستیکی این دو هادی را از یکدیگر جدا می کند و مانع از تماس دو هادی در تمام طول کابل با یکدیگر می شود.



مزایای کابل های کواکسیال:

- قابلیت اعتماد بالا
- ظرفیت بالای انتقال، حداکثر پهنای باند ۳۰۰ مگاهرتز
- دوام وپایداری خوب
- پایین بودن مخارج نگهداری
- قابل استفاده در سیستم های آنالوگ و دیجیتال
- هزینه پائین در زمان توسعه
- پهنای باند نسبتا" وسیع که مور استفاده اکثر سرویس های مخابراتی از جمله تله کنفرانس صوتی وتصویری است.

معایب کابل های کواکسیال :

- مخارج بالای نصب
- نصب مشکل تر نسبت به کابل های بهم تابیده
- محدودیت فاصله
- نیاز به استفاده از عناصر خاص برای انشعابات

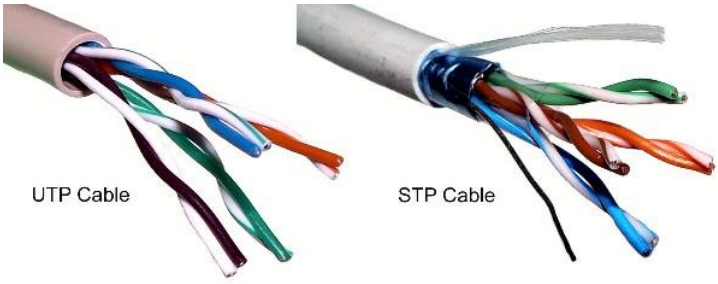
از کانکتورهای BNC (Bayone -Neil- Concelman) به همراه کابل های کواکسیال استفاده میگردد. اغلب کارت های شبکه دارای کانکتور های لازم در این خصوص می باشند.

کابل UTP (Unshielded Twisted Pair)

متداولترین نوع کابلی که در انتقال اطلاعات استفاده می گردد. کابل های به هم تابیده می باشند. این نوع کابل ها دارای دو رشته سیم به هم پیچیده بوده که هر دو نسبت به زمین دارای یک امپدانس یکسان می باشند. بدین ترتیب امکان تاثیر پذیری این نوع کابل ها از کابل های مجاور و یا سایر منابع خارجی کاهش خواهد یافت.

کابل های بهم تابیده دارای دو مدل متفاوت: STP (Shielded Twisted Pair) وUTP (Unshielded Twisted Pair) می باشند. کابل UTP نسبت به کابل STP به مراتب متداول تر بوده ودر اکثر شبکه های محلی استفاده می گردد.

کیفیت کابل های UTP متغییر بوده و با توجه به مشخصه ها و سطوح کارایی به گروه های خاصی، طبقه بندی میشوند(Category). هرچه درجه بندی طبقه یک کابل بالاتر باشد به این معنی است که آن کابل بهتر است و می تواند داه ها را با سرعت بالاتری ارسال کند.



جدول انواع مدل های کابل UTP

نوع	نرخ انتقال	فرکانس	بیشترین طول	تعداد جفت	کاربرد
CAT1	1 Mbps	1 MHZ	90 meters	1 pair	Telephone and ISDN
CAT2	4 MHZ	1 MHZ	90 meters	2 pairs	Token Ring
CAT3	10 MHZ	16 MHZ	100 meters	3 or 4 pairs	10BaseT (Can reach 100 Mbps with 100VGAnyLAN)
CAT4	16 MHZ	16 MHZ	100 meters	4 pairs	Toke Rig
CAT5	10 MHZ 1 Gbps if Using all 4 pairs	100 MHZ	100 meters	4 pairs	10BaseT and 100BaserT 155 Mbps ATM Gigabit Ethernet
CAT5E	100 Mbps	100 MHZ	100 meters	4 pairs	Gigabit Ethernet
CAT6	4-10 Gbps	250 MHZ	100 meters	4 pairs	Gigabit Ethernet, uses all 4 pairs

به یاد داشته باشید که یکی از تفاوت های موجود بین طبقه های مختلف UTP، تعداد زوج سیم های موجود در کابل می باشد. در ضمن هر جفت سیم رنگ بندی خاصی دارد که مطابق استاندارد های خاصی تعریف شده اند. به عنوان مثال،کابل Cat5 که امروزه متداولترین نوع کابل Utp می باشد دارای ۴ جفت زوج سیم می باشد که رنگ بندی آنها عبارتند از:

جفت۱: آبی و سفید آبی

جفت۲: نارنجی و سفید نارنجی

جفت۳: سبز و سفید سبز

جفت۴: قهوه ای و سفید قهوه ای

مزایای کابل های بهم تابیده :

- سادگی ونصب آسان
- انعطاف پذیری مناسب
- دارای وزن کم بوده و براحتی بهم تابیده می گردند.

معایب کابل های بهم تابیده :

- تضعیف فرکانس
- بدون استفاده ازتکرار کننده ها، قادر به حمل سیگنال درمسافت های طولانی نمی باشند.
- پایین بودن پهنای باند

- به دلیل پذیرش پارازیت، در محیط های الکتریکی سنگین به خدمت گرفته نمی شوند.

کانکتور استاندارد برای کابل های UTP، از نوع RJ-45 می باشد. کانکتور فوق شباهت زیادی به کانکتور های تلفن (RJ-11) دارد. هر یک از پین های کانکتور فوق می بایست به درستی پیکربندی گردند.
(RJمخفف Registered jack می باشد)

اصول کابل کشی

کابل کشی شبکه یکی از مراحل مهم در زمان پیاده سازی یک شبکه کامپیوتری است که می بایست با دقت، ظرافت خاص و پایبندی به اصول کابل کشی ساخته یافته، انجام شود. با رعایت اصول کابل کشی ساخت یافته، در صورت بروز اشکال در شبکه، تشخیص و اشکال زائی آن با سرعتی مناسبی انجام خواهد شد.
اترنت عموما با استفاده از هشت کابل هادی به همراه هشت پین ماژولار Plugs/Jacks ، داده را حمل می کند. کانکتور استاندارد، RJ-45 نامیده شده و مشابه کانکتور استاندارد RJ-11 است که در تلفن استفاده می گردد. یک رشته کابل Cat5 شامل چهار زوج سیم بهم تابه است که هر زوج دارای و رشته سیم با رنگ هایی خاص است. (یک رشته رنگی و یک رشته سفید و رنگ رشته زوج مربوط). زوج های در نظر گرفته شده برای Ethernet10 وEthernet100 به رنگ نارنجی و سبز می باشند. از دو زوج دیگر(رنگ قهوه ای و آبی) نیز می توان به منظور یک خط اترنت دوم و یا اتصالات تلفن استفاده نمود.
به منظور کابل کشی کابل های UTP از دو استاندارد متفاوت با نام T-568B(یا EIA) و T-568A (یا AT&T، 258A). استفاده می گردد. تنها تفاوت موجود بین آنان ترتیب اتصالات است.

- **شماره پین های استاندارد T568B (کلاس B)**

کد رنگ ها در استاندارد T568B

کاربرد	رنگ	شماره پین
TxData +	سفید / نارنجی	یک
TxData -	نارنجی	دو
RecvData +	سفید/ سبز	سه
	آبی	چهار
	سفید/آبی	پنج
RecvData -	سبز	شش
	سفید/قهوه ای	هفت
	قهوه ای	هشت

- **شماره پین های استاندارد T568A (کلاس A)**

در استاندارد T568A، اتصالات سبز و نارنجی برعکس شده است، بنابراین زوج های یک و دو بر روی چهار پین وسط قرار می گیرند.

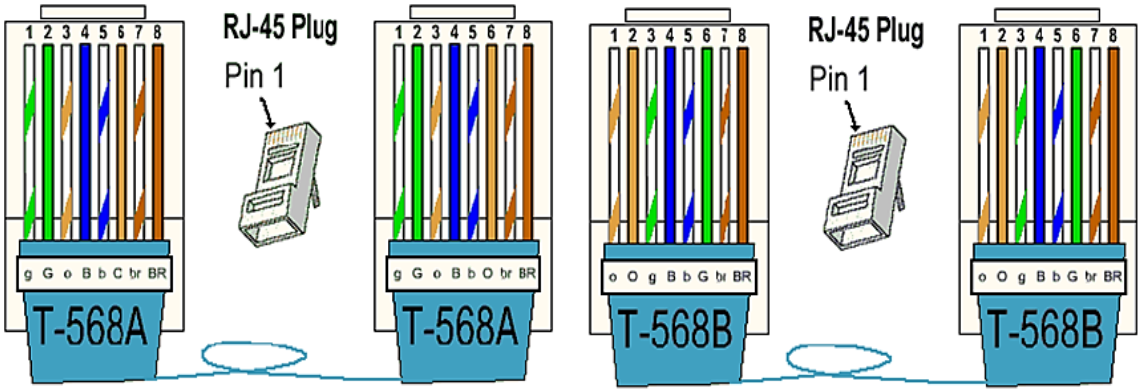
کد رنگ ها در استاندارد T568A

کاربرد	رنگ	شماره پین
+RecvData	سفید / سبز	یک
-RecvData	سبز	دو
+TxData	سفید/ نارنجی	سه
	آبی	چهار
	سفید/آبی	پنج
-TxData	نارنجی	شش
	سفید/قهوه ای	هفت
	قهوه ای	هشت

ایجاد یک کابل Straight

متداولترین کاربرد یک کابل Straight، اتصال بین یک کامپیوتر و هاب/ سوئیچ است. شکل زیر یک اتصال استاندارد Straight در کابل های CAT5 را نشان می دهد که از آن به منظور اتصال یک PC به هاب و یا سوئیچ استفاده می گردد. البته همانطور که در شکل زیر نیز مشاهده می کنید رنگ بندی و آرایش هر دو سر کابل CAT5 متناظر و مطابق استاندارد T568B صورت گرفته است.

البته کابل های Straight را به صورت T568A نیز می توان ایجاد نمود.



ایجاد کابل Cross-Over

کابل های کراس CAT5 UTP که از آنان با نام Cross-Over نیز نام برده می شود، یکی از متداولترین کابل های استفاده شده پس از کابل های Straight می باشند. با استفاده از کابل های فوق، می توان دو کامپیوتر را بدون نیاز به هاب و یا سوئیچ به یکدیگر متصل نمود. به عبارت دیگر، هاب عملیات Cross-Over را به صورت داخلی انجام می دهد، در زمانی که یک کامچیوتر را به یک هاب متصل می نماییم، صرفا به یک کابل Straight نیاز می باشد. در صورتی که قصد اتصال دو کامپیوتر به یکدیگر را بدون استفاده از یک هاب داشته باشیم، می بایست عملیات Cross-Over را به صورت دستی انجام داد و کابل مختص آن را ایجاد نمود.

چرا به کابل های Cross-Over نیاز داریم؟

در زمان مبادله داده بین دو دستگاه (مثلا کامپیوتر) ، یکی از آنان به عنوان دریافت کننده و دیگری به عنوان فرستنده ایفای وظیفه می نماید. تمامی عملیات ارسال داده از طریق کابل های شبکه انجام می شود. یک کابل شبکه از چندین رشته سیم دیگر تشکیل می گردد. از برخی رشته سیم ها به منظور ارسال داده و از برخی دیگر به منظور دریافت داده استفاده می شود. براب ایجاد یک کابل Cross-Over از رودیکرد فوق استفاده شده و TX (ارسال) یک سمت به RX (دریافت) سمت دیگر، متصل می گردد. شکل زیر نحوه انجام عملیات را نشان می دهد:

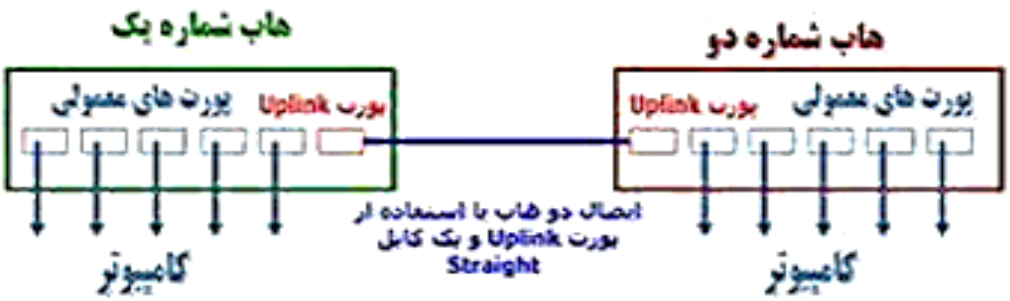
کابل Cross-Over CAT5

به منظور ایجاد کابل های کراس CAT5 صرفا از یک روش استفاده می گردد. همانگونه که قبلا اشاره گردید، یک کابلCross-Over پین TX سمت را به پین RX سمت دیگر متصل می نماید (و برعکس) . شکل زیر شماره پین های یک کابل CAT5 معمولی Cross-Over را نشان می دهد.

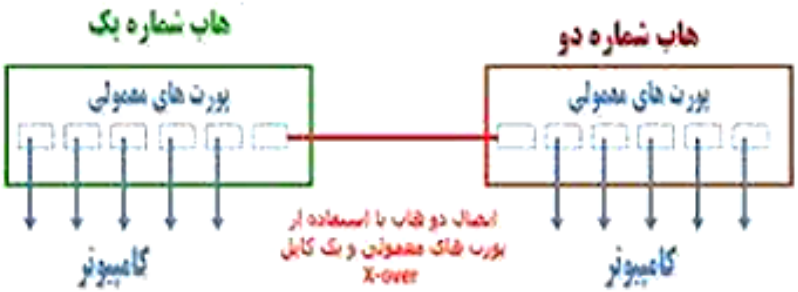
همانگونه که در شکل فوق مشاهده می گردد در کابل های Cross-Over صرفا از پین های شماره یک، دو، سه و شش استفاده می گردد. پین های یک ودو به منزله یک زوج بوده و پین های سه و شش زوج دیگر را تشکیل می دهند. از پین های چهار، پنج، هفت و هشت استفاده نمی گردد. (صرفا از چهار پین برای ایجاد یک کابل Cross-Over، استفاده می گردد.)

مورد استفاده از کابل های Cross-Over

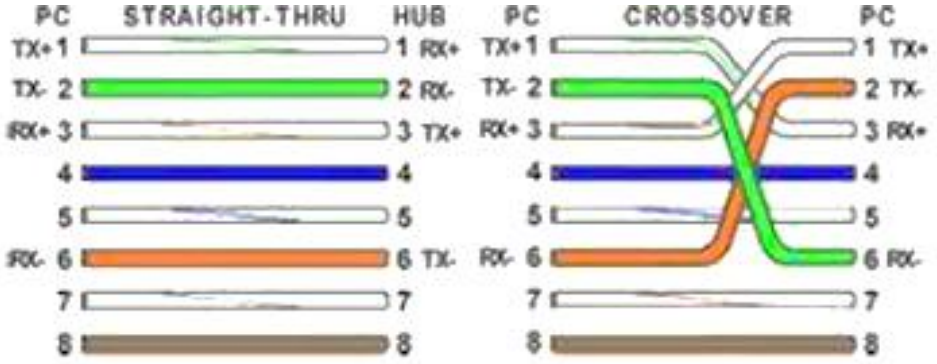
از کابل های Cross-Over صرفا به منظور اتصال دو کامپیوتر استفاده نمی شود و می توان از آنپان در دستگاه های متفاوتی نظیر سوئیچ و یا هاب نیز استفاده نمود. در صورتی که قصد داشته باشیم و هاب را به یکیگر متصل نماییم، معمولا از پورت Uplink استفاده می گرد. یعنی پورت های Uplink دو هاب را توسط یک کابل Straight به هم وصل می کنیم. شکل زیر نحوه اتصال و هاب به یکدیگر با استفده از یک کابل Straight و از طریق پورت Uplink را نشان می دهد :



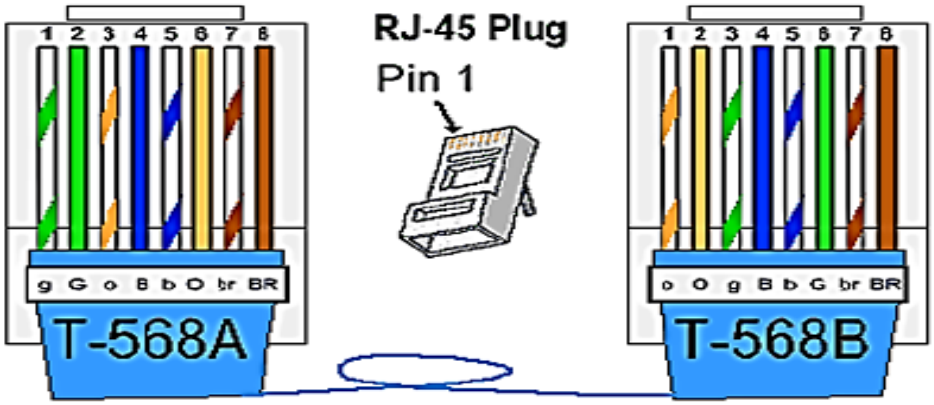
با توجه به وجود Uplink، نیازی به استفاده از یک کابل Cross-Over نخواهد بود. به عبارت دیگر پورت های Uplink از داخل و به طور سخت افزاری، عمل Cross را انجام می دهند. در صورتی که امکان استفاده از پورت Uplink وجود نداشته باشد و بخواهیم و هاب را با استفاده از پورت های معمولی به یکدیگر متصل نماییم، می توان از یک کابل Cross-Over استفاده نمود. شکل زیر نحوه اتصال دو هاب به یکدیگر با استفاده از یک کابل Cross-Over را و بدون استفاده از پورت Uplink نشان می دهد :



شکل زیر تفاوت موجود بین شماره پین های یک کابل Straight وCross-Over را نشان می دهد :



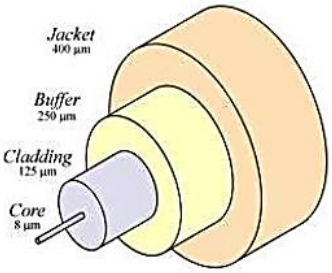
به عبارت دیگر، برای ایجاد یک کابل Cross کافیست رنگ بندی یک سر کابل را مطابق استاندارد کلاس a و رنگ بندی سردیگر کابل را مطابق استاندارد کلاسb در نظر گرفته و سوکت بزنید. به این ترتیب سیم های ارسال در هر طرف به سیم های دریافت در طرف دیگر منتهی می شوند و برعکس.

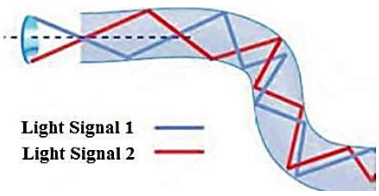


فیبر نوری

یکی از جدیدترین محیط های انتقال در شبکه های کامپیوتری، فیبر نوری است. کابل فیبرنوری برخلاف همه کابل هایی که تاکنون بحث کردیم، براساس سیگنال های الکتریکی که در هادی مسی جریان می یابند، نمی باشد؛ بلکه در کابل فیبرنوری از پالس های نور (فوتون ها) برای ارسال سیگنال های باینری تولید شده توسط منبع نورانی (دیود لیزری و یا دیودهای ساطع کننده نور) استفاده می شود. از آنجا که کابل فیبر نوری از نور به جای الکتریسیته استفاده می کند، تقریبا هیچ یک از مشکلات ذاتی کابل مسی همچون تداخل الکترومغناطیسی و نیاز به زمین کردن را ندارد.

کابل فیبر نوری از یک میله استوانه ای که هسته نامیده می شود و جنس آن از سیلیکات است تشکیل می گردد. شعاع استوانه بین دو تا سه میکرون است. روی هسته، استوانه دیگری (از همان جنس هسته) که غلات نامیده می شود، استقرار می یابد. ضریب شکست هسته را با M1 و ضریب شکست غلاف را با M2 نشان داده و همواره M1>M2 است. در این نوع فیبرها، نور در اثر انعکاسات کلی در فصل مشترک هسته و غلاف، انتشار پیدا خواهد کرد.





مزایای فیبر نوری:

- حجم و وزن کم
- پهنای باند بالا
- تلفات سیگنال کم و در نتیجه فاصله تقویت کننده ها زیاد می گردد.

- مصون بودن از اثرات القا های الکترومغناطیسی مدارات دیگر
- آتش زا نبودن آنها به دلیل عدم وجود پالس الکتریکی در آنها
- موصون بودن در مقابل عوامل جوی و رطوبت
- سهولت در امر کابل کشی و نصب
- استفاده در شبکه های مخابراتی آنالوگ و دیجیتال
- مصونیت در مقابل پارازیت

معایب فیبرنوری:

- به راحتی شکسته شده و می بایست دارای یک پوشش مناسب باشند. مسئله فوق با ظهور فیبر های تمام پلاستیکی و پلاستیکی/شیشه ای کاهش پیدا کرده است.
- اتصال دو بخش از فیبر یا اتصال یک منبع نور به فیبر، فرآیند دشواریاست. در چنین حالتی می توان از فیبر های ضخیم تر استفاده کرد اما این مسئله باعث تلفات زیاد و کم شدن پهنای باند می گردد.
- از اتصالات T شکل در فیبرنوری نمی توان جهت گرفتن انشعاب استفاده نمود. در چنین حالتی فیبر می بایست بریده شده و یک Detector اضافه گر. دستگاه فوق می بایست قادر به دریافت و تکرار سیگنال را اشته باشد.
- تقویت سیگنال نوری یکی از مشکلات اساسی در زمینه فیبرنوری است. برای تقویت سیگنال میبایست سیگنال های نوری به سیگنال های الکتریکی تبدیل، تقویت و مجددا" به علائم نوری تبدیل شوند.

کارت واسط شبکه (NIC)

کارت شبکه، یکی از مهمترین عناصر سخت افزاری در زمان پیاده سازی یک شبکه کامپیوتری است. هر کامپیوتر موجود در شبکه (سرویس گیرندگان و سرویس دهندگان)، نیازمند استفاده از یک کارت شبکه است. کارت شبکه، ارتباط بین کامپیوتر و محیط انتقال (نظیر کابل های مسی و یا فیبر نوری) را فراهم می نماید. اکثر مادربورد های امروزی که از آنان در کامپیوتر های شخصی استفاده می گردد، دارای یک کارت شبکه OnBoard می باشند. کامپیوتر های قدیمی و یا کامپیوتر های جدیدی که دارای اینترفیس شبکه های OnBoard نمی باشند ، در زمان اتصال به شبکه، می بایست بر روی آنان یک کارت شبکه نصب گردد. شکل زیریک نمونه کارت شبکه را که دارای یک پورت RJ-45 است را نشان می دهد.

کامپیوتر ها جهت اتصال به هم و استفاده از برنامه های هم و اشتراک برنامه ها از نظر سخت افزاری احتیاج به کارت شبکه یا LAN Card دارند. که بطور معمول در بازار دو نوع کارت معمول می باشد. یک قسم آنها کارت های ۱۰ در ۱۰ بوده و قسم دیگر کارتهای ۱۰ در ۱۰۰ میباشند. جهت کنترل اتصال درست کارت شبکه به کامپیوتر می توانید روی آیکون My Computer کلیک راست نموده و از قسمت Propertiesپوشه Device Manager را انتخاب نمایید. در بین ابزار های نصب شده طبق شکل باید در قسمت Network Adapters، نام و مشخصات کارت شبکه شما وجود داشته باشد.

اگر در این بخش علامت سوال یاتعجب به شکل زرد رنگ وجود داشته باشد، نشان می دهد که راه اندازه (Driver) کارت شبکه شما ناقص بوده و درست نصب نشده است و بایستی طبق روش های Hardware Settings آنرا برداشته (Remove) و مجددا نصب نمایید و یا از قسمت Add New Hardware، در بخش Control Panel، درایور یا راه انداز مناسب و صحیح آن را نصب نمایید. توجه نمایید که بعد از نصب کارت شبکه،آیکون Network Neighborhood در روی میط کار (Desktop) مشاهده خواهد شد. از آنجایی که ما معمولا دو نوع شبکه BNC وHUB را مورد استفاده قرار می دهیم بر روی اکثر کارت ها جهت اتصال هر ونوع رابط وجود دارد. کارت های OnBoard، معمولا فقط جای HUB را دارند.

وظایف کارت شبکه

۱-برقراری ارتباط لازم بین کامپیوتر و محیط انتقال

۲- تبدیل داده: داده ها بر روی گذرگاه (Bus) کامپیوتر به صورت موازی حرکت می نمایند. نحوه حرکت داده ها بر روی محیط انتقال شبکه به صورت سریال است. ترانسیور کارت شبکه (یک ارسال کننده و یا دریافت کننده)، داده ها را از حالت موازی به سریال و بالعکس تبدیل می نماید.

۳-ارائه یک آدرس منحصر به فرد سخت افزاری: آدرس سخت افزاری (MAC) درون تراشه ROM موجود بر روی کارت شبکه نوشته می گردد. آدرس MAC در واقع یک زیر لایه از یک Data Link مدل مرجع OSI می باشد. آدرس سخت افزاری موجود بر روی کارت شبکه، یک آدرس منحصربه فرد را برای هر یک از کامپیوتر های موجود در شبکه، مشخص می نماید. پروتکل هایی نظیر TCP/IP از یک سیستم آدرس دهی منطقی (آدرسIP)، استفاده می نمایند.در چنین مواردی قبل از دریافت داه توسط کامپیوتر، می بایست آدرس منطقی به آدرس سخت افزاری ترجمه گردد.

۴-کپسوله کردن داده ها: کارت شبکه و درایور آن مجموعا قبل از انتقال اطلاعات باید داده هایی را که توسط پروتکل لایه شبکه تولید شده است، در یک فریم کپسوله کنند. عمل دیگری که کارت شبکه در این زمینه انجام می دهد خواندن محتوای فریم های دریافت شده از شبکه و انتقال داده های آنها به پروتکل مناسب در لایه شبکه می باشد.

۵-کد گذاری و کد گشایی سیگنال ها: کارت شبکه مسئول پیاده سازی روش کد گذاری لایه شبکه می باشد که در آن اطلاعات باینری تولید شده در لایه شبکه که حالا در فریم، کپسوله شده است را به بارهای الکتریکی یعنی ولتاژهای الکتریکی، پالس های نور یا هر نوع سیگنالی که رسانه شبکه استفاده می کند تبدیل می کند. از طرف دیگر کارت شبکه سیگنال های دریافت از شبکه را برای پروتکل های لایه بالاتر به اطلاعات باینری تبدیل می کند.

۶-بافر کردن داده ها: کارت های شبکه هر زمان فقط یک فریم داده را روی شبکه می فرستند یا از آن دریافت می کنند، بنابراین در خود بافری دارند که تا زمان کامل و آماده شدن یک فریم برای پردازش، داده هایی که از طرف کامپیوتر با شبکه در یافت می کنند را ذخیره کنند.

۷-تبدیل سریال به موازی و برعکس: ارتباطات بین کامپیوتر و کارت شبکه به صورت موازی انجام می شود، مگر در کارتهای شبکه USB که ارتباط با کامپیوتر در آنها به صورت سریال است. اما ارتباطات شبکه ای به صورت سریال انجام می شوند، بنابراین کارت شبکه مسئول تبدیل این دو روش انتقال اطلاعات به همدیگر می باشد.

۸-روند نصب یک کارت شبکه، شامل قراردادن کارت داخل کامپیوتر، پیکربندی کارت برای استفاده از منابع سخت افزاری مناسب، و نهایتا نصب درایور کارت می باشد که بسته به توانایی ها و نوع کامپیوتر از نظر قدیمی یا جدید بودن این پروسه می تواند بسیار ساده و یا بسیار پر دردسر باشد.

توجه: قبل از لمس کردن قطعات داخلی کامپیوتر یا درآوردن کارت شبکه از بسته محافظ مخصوص آن، دست خود را با ورقه فلزی دور منبع تغذیه کامپیوتر تماس دهید یا اینکه از دستکش های مخصوص استفاده کنید تا به دلیل تخلیه الکترواستاتیکی به قطعات آسیبی واردنشود.

انواع کارت شبکه

واسط شبکه کابل های UTP به شکل سوکت RJ-45 و برای کابل های کواکسیال، کانکتور BNC یا AUI می باشد، البته در بعضی موارد می توان از فرستنده هایی بی سیم هم استفاده کرد.

کارت شبکه به کمک درایو خود موظف به انجام اغلب وظایف پروتکل های لایه پیوند– داده و فیزیکی می باشد و زمان خرید باید کارت متناسب با پروتکلی که برای لایه پیوند–داده انتخاب کرده اید (مثل اترنت یا Token Ring) را خریداری کنید و توجه داشته باشید که این نوع کارت را نمی توان به جای یکدیگر استفاده کرد. نکته دیگریکه زمان خرید باید مورد توجه قرار پیرد انتخاب کارتی است که علاوه بر تناسب با پروتکل لایه پیوند–داده، از گونه مورد نظر آن پروتکل هم پشتیبانی کند.

فراموش نکنید که کارت شبکه منتخب شما باد با اسلات باس کامپیوتری که قرار است در آن نب شود، متناسب باشد و دارای کانکتور مخصوص رسانه شبکه باشد.

غیر از کارت های شبکه ای که مختص اتصال کامپیوتر ها به شبکه های محلی سرویس گیرنده/ دهنده استاندارد هستند، انواع دیگری وجود دارند که کامپیوترها و دستگاه های دیگری را به شبکه های بخصوصی بنام شبکه ذخیره ناحیه ای یا SAN (Storage Area Network) متصل می کنند، یک SAN شبکه ای مجزا است که مختص ارتباطات بین سرورها و دستگاههای ذخیره سازی خارجی، از قبیل RAID می باشد. اغلب کارت های شبکه SAN بجای اترنت و Token Ring از پروتکل دیگری بنام Fiber Channel استفاده میکنند. برای اتصال کارت شبکه به Motherboard نیز دو نوع اسلات PCI وISA داریم. اسلات های PCI به مراتب از اسلات های ISA سریع تر هستند و دارای قابلیت خود پیکربندی می باشند، بنابراین کارت هایی که از این استاندارد استفاده می کنند متداول ترند. اما در صورتیکه کامپیوتر تان فقط دارای اسلات ISA باشد به ناچار می توانید از کارت های شبکه ISA استفاده کنید. در سیستم های قابل حمل تنها انتخاب، کارت های PC Card می باشد. این نوع کارت ها مختص اسلات های PCMCIA می باشند و در این نوع اسلات ها قرار می گیرند. اما در صورتیکه سیستم شما از استاندارد CardBus پشتیبانی می کند، زمان خرید باید کارتی را انتخاب کنید که آن هم از این استاندارد پشتیبانی کند. CardBusاستاندارد است که برای لوازم جانبی PC Card، بازدهی معادل بازدهی استاندارد PCI مهیا میکند.

در بازار کارت های شبکه ای که از پورت USB برای اتصال به کامپیوتر استفاده می کنند هم وجود دارد، اما روابط USB قدیمی، حداکثر می تواند در سرعت ۱,۲ مگابیت در ثانیه کار کند که حتی در مقایسه با استاندارد ISA کند است. همیشه سرعت انتقال داده در کارت شبکه شما باید با تجهیزات دیگر شبکه متناسب باشد.

کارت های شبکه متناسب با نوع کابلی که پشتیبانی می کنند دارای انواع مختلف کانکتور می باشند. بعضی از NICها (کارت های شبکه) بیش از یک کانکتور کابل دارند که شما را قادر به انتخاب رسانه شبکه مطلوب می کنند. به عنوان مثال، کارت هایی وجود دارند که دارای سه کانکتور AUI، BNC و RJ45 می باشند و کارت مرکب نامیده می شوند. این نوع کارت ها از کارت هایی که فقط یک کانکتور دارند به مراتب گران ترند. توجه داشته باشید که همزمان فقط از یکی کانکتورها می توانید استفاده نمایید.

انتخاب کارت شبکه

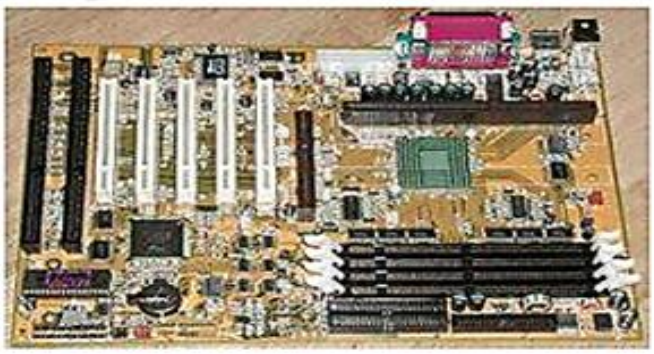
برای انتخاب یک کارت شبکه، می بایست پارامترهای متعددی را بررسی نمود:

سازگاری با معماری استفاده شده در شبکه: کارت های شبکه دارای مدل های متفاوتی با توجه به معماری استفاده شده در شبکه (اترنت، Token ring) می باشند. اترنت، متداولترین معماری شبکه در حال حاظر است که در شبکه هایی با ابعاد بزرگ و کوچک، استفاده می گردد.

سازگاری با Throughput شبکه: در صورتی که یک شبکه اترنت سریع (سرعت100 Mbps) پیاده سازی شده است، انتخاب یک کارت اترنت با سرعت 10 Mbps تصمیم مناسبی در این رابطه نخواهد بود. اکثر کارت های شبکه جدید قادر به سوئیچینگ اتوماتیک بین سرعت های 10و100 Mbps می باشند (اترنت معمولی و اترنت سریع)

سازگاری با نوع اسلات های خالی مادربورد: کارت های شبکه دارای مدل های متفاوتی با توجه به نوع اسلات مادربورد می باشند. کارت های شبکه PCI درون یک اسلات خالی PCI و کارت هایی از نوع ISA در اسلات های ISA نصب می گردند. کارت شبکه می بایست متناسب با یکی از اسلات های خالی موجود بر روی مادربورد، انتخاب گردد. اسلات آزاد به نوع مادربورد بستگی داشته و در این رابطه گزینه های متعددی نظیر ISA،PCI وEISA می تواند وجود داشته باشد.

شکل زیر یک نمونه مادربورد را که دارای اسلات های ISA وPCI است، نشان می دهد:



ساختار کارت واسط شبکه (NIC)

کارت های شبکه از نظر ساختاری به چند دسته تقسیم بندی میشوند. از لحاظ استاندارد مورد استفاده سه نوع کارت شبکه وجود دارند این دسته بندی براساس نحوه ارتباط با مادربورد به شرح زیر است:

1. ISA/EISA: Architecture Standard Industry / Extended ISA
2. PCI Peripheral Components Industry :
3. USB: Universal Synchronous Bus

- **ISA:** تجهیزات ISA تا سالهای ۱۹۹۹ و۲۰۰۰ تولید می شدند. اما این تجهیزات به دلیل نواقصی زیادی که داشت با شکست مواجه شد. دو دلیل عمده این شکست به شرح زیر است:

۱- اسلات های ISA ی نصب شده روی مادربورد با نصب سرعت Bus مادربورد کار می کردند؛ که نتیجه آن کاهش خواندن و فرستادن اطلاعات به RAM بود.

۲- در هر لحظه تنها یک اسلات اجازه استفاده از باس مادربورد را داشت و در صورتیکه دو اسلات همزمان به انتقال داده روی مادربورد می پرداختند، هر دو از عمل خارج میشدند.

- **PCI:** از مزایای این فناوری از بین رفتن دو مشکل عمده تکنولوژی ISA بود. در این فناوری هر اسلات با سرعت باس مادربورد و همزمان با اسلات های دیگر نیز میتوانست کار کند.

- **USB:** کارتهای واسط را میتوان به نوعی سه دسته دانست که دسته سوم استفاده از ورودی های USB می باشد. تکنولوژی استفاده شده در این تجهیزات عینا شبیه به PCI میباشد. (گذرگاه فراگیر(گسترده) همزمان)

- کارت مخصوص برای توپولوژی BUS:

البته کارت فوق چند سیستم را Support می کند.

- کارت مخصوص برای توپولوژی Star:

کارت های شبکه ای نیز وجود دارد که به صورت Wireless (بی سیم) به کار می روند.

- کارت مخصوص برای توپولوژی Mesh:

- کارت هایی نیز وجود دارد که در USB 1 نصب می شوند.

تکرار کننده (Repeater)

وسیله ای در تجهیزات شبکه است که در مدارات ارتباطی (معمولا شبکه Bus) مورد استفاده قرار می گیرد و تضعیف سیگنال ها را از طریق تقویت یا تولید مجدد آنها کاهش می دهد تا سیگنال ها با همان شکل اول به راه خود ادامه دهند. بدین ترتیب می توان سیگنال را بدون کاستی به فواصل دورتری فرستاد. این وسیله حداکثر فاصله ای را که کابل شبکه محلی می تواند گسترده شود افزایش دهد. استفاده از یک تکرارگر یک شبکه محلی را به دو قسمت نمی کندو شبکه تقابلی نمی سازد. از آنجا که تکرارگرها با سیگنال های فیزیکی واقعی سروکار دارند و در جهت تفسیر داده ای که انتقال می دهند تلاشی نمی کنند، این تجهیزدر لایه فیزیکی یعنی اولین لایه از مدل مرجع OSI عمل می کند.

این وسیله در واقع نوع خاصی از HUB است که فقط دارای ۲ پورت است.

۱. کار تکرارگر تقویت سیگنال های بین دو شبکه یا سگمنت های یک شبکه که فاصله ی زیادی از هم دارند می باشد.

۲. این قطعه در دو نوع Passive و Activer قابل دسترسی بوده است :

۱,۲. Passive Repeater: این نوع Repeater دو تا پورت دارد که هر یک به یک کابل شبکه متصل هستند و سیگنالی که از یک کابل دریافت کرده است از خود عبور می دهد و بر روی کابل دیگر می فرستد. به این ترتیب هیچگونه تغییری در سیگنال به وجود نیامده و تقویتی صورت نگرفته است بلکه Repeater مانند یک کانکتور (اتصال دهنده) عمل می کند و نیاز به منبع تغذیه و برق ندارد.

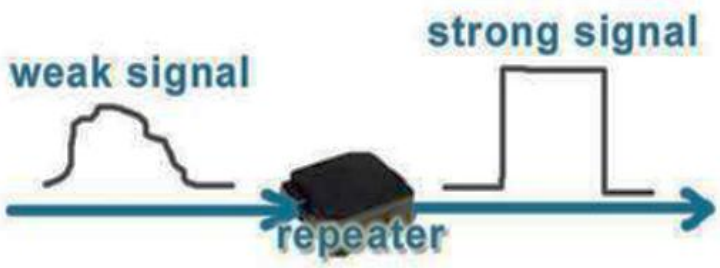
۲,۲. Active Repeater: در این نوع Repeater سیگنال دریافت شده را مجددا تقویت و بازسازی می کند، به طوری که به نظر می رسد که سیگنال جدید است. البته برای انجام چنین عملیاتی نیاز به منبع تغذیه و برق دارد.

به یاد داشته باشید که عملکرد Repeater ها صرفا الکتریکی است و در لایه فیزیکی شبکه (لایه اول) عمل می کنند. به عبارت دیگر Repeater ها فقط سیگنال های الکتریکی ورودی را تقویت میکنند و بیرون می دهند و هیچ درکی از داده ها ندارند و قار به هیچ نوع فیلتر کردن اده ها نیز نیستند.

اما تفاوت های دیگری نیز بین دو مدل Passiver وActive وجود دارد :

نوع اول علاوه بر سیگنال هر چیز دیگری حتی نویز امواج ناخواسته که به همراه سیگنال اصلی که دارای اطلاعات است می باشند (Passive). مثلا در امواج صوتی نویزی که باعث افت کیفیت صدا و شنیدن اصوات اضافه می شود را هم تقویت می کند.

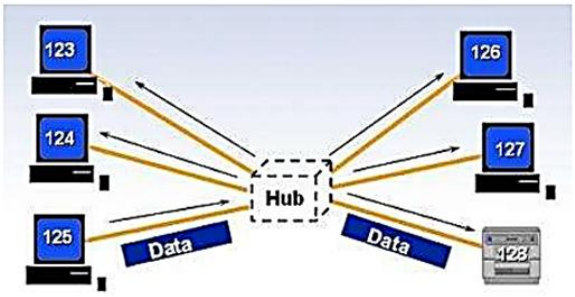
اما تکرار کننده ی نوع Active، سیگنال را قبل از ارسال بازدید کرده و چیز های اضافه را خارج می کند و مثلا دیگر نویز را تقویت نمی کند.



هاب (hub)

هاب به وسیله ای گفته می شود که خطوط ارتباطی را در یک نقطه مرکزی به یکدیگر متصل می کند و اتصالات مشترکی برای تمامی وسایل فراهم می آورد. هاب در مرکز شبکه های Star قرار می گیرد و تمام کامپیوتر های موجود در شبکه توسط یک کابل مستقل به آن متصل می شوند. هاب در حقیقت از ترکیب چندین Repeater ساخته شده است به این ترتیب که هر یک از پورت های هاب، حکم یک Repeater را دارند. به عبارت دیگر یک پالس ورودی به یکی از پورت های، به همه پورت های خروجی ارسال می شود.

انواع HUB



سه نوع هاب رایج وجود دارد:

الف – هاب فعال (Active):

که مانند آمپلی فایر عمل می کند و باعث تقویت مسیر عبور سیگنال می شود و از تصادم و برخورد سیگنال ها در مسیر جلوگیری به عمل می آورد. این هاب نسبتا قیمت بالایی دارد.

ب – غیرفعال (Passive):

که برخلاف نوع اول که در مورد تقویت انتقال سیگنال ها فعال است، این هاب منفعل بوده و هیچ برنامه و رفتاری جهت جلوگیری از تصادم ندارد.

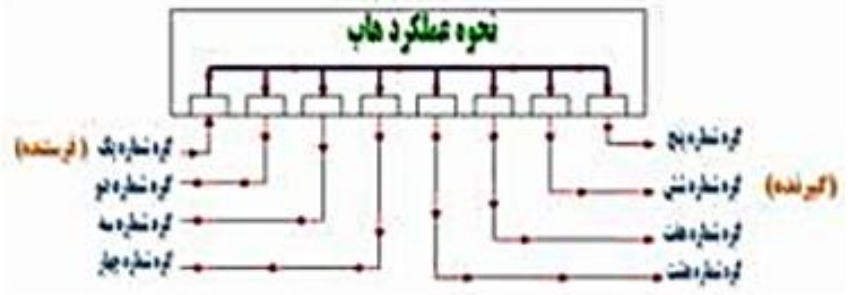
ج – آمیخته (Mixed):

که قادر به ترکیب انواع رسانه ها " کابل کواکسیال نازک، ضخیم و... " و باعث تعامل درون خطی میان سایر هاب ها می شود.

آشنایی با نحوه عملکرد هاب

HUB(8-Port)

نحوه کار هاب بسیار ساده است. زمانی که یکی از کامپیوتر های متصل شده به هاب اقدام به ارسال داده ای می نماید، سایر پورت های هاب نیز آن را دریافت خ واهند کرد (داده ارسالی تکرار و برای سایر پورت های هاب نیز فرستاده می شود). شکل زیر نحوه عملکرد هاب را نشان می دهد.



همانگونه که در شکل فوق مشاهده می نمائید، گره ۱ داده ای را برای گره ۶ ارسال می نماید، ولی تمامی گره های دیگر نیز داده را دریافت خواهند کرد. در ادامه، بررسی لازم در خصوص داده ارسالی توسط هر یک از گره ها انجام و در صورتی که تشخیص داده شود که داده ارسالی متعلق به آنان نیست، آن را نادیده خواهند گرفت. عملیات فوق از طریق کارت شبکه موجود بر روی کامپیوتر که آدرس MAC مقصد فریم ارسالی را بررسی می نماید، انجام می شود. کارت شبکه بررسی لازم را انجام و در صورت عدم مطابقت آدرس MAC موجود در فریم، با آدرس MAC کارت شبکه، فریم ارسالی دور انداخته می گردد.

اکثر هاب ها دارای یک پورت خاص می باشند که می تواند به صورت یک پورت معمولی و یا یک پورت Uplink رفتار نماید. با استفاده از یک پورت Uplink می توان یک هاب دیگر را به هاب موجود و به کمک کابل Straight، متصل نمود. بدین ترتیب تعداد پورت ها افزایش یافته و امکان اتصال تعداد بیشتری کامپیوتر به شبکه فراهم می گردد. روش فوق گزینه ای ارزان قیمت به منظور افزایش تعداد گره ها در یک شبکه است ولی با انجام این کار شبکه شلوغ تر شده و همواره بر روی آن حجم بالائی داده غیر ضروری در حال جابجائی است.

دراکثر هاب ها از یک LED به منظور نشان دادن فعال بودن ارتباط برقرار شده بین هاب و گره و از LED دیگر به منظور نشان دادن بروز یک Collision (تصادم – تصادف)، استفاده می گردد.(دو LED مجزا). در برخی از هاب ها دو LED مربوط به فعال بودن لینک ارتباطی بین هاب و گره و فعالیت پورت با یکدیگر ترکیب و زمانی که پورت در حال فعالیت است، LED مربوطه چشمک زن شده و زمانی که فعالیتی انجام نمی شود، LED فوق به صورت پیوسته روشن خواهد بود.

LED مربوط به Collision موجود بر روی هاب ها زمانی روشن می گردد که یک Collision به وجود آید. Collision زمانی به وجود می آید که دو کامپیوتر و یا گره سعی نمایند در یک لحظه بر روی شبکه صحبت نمایند. پس از بروز یک Collision، فریم های مربوط به هر یک از گره ها با یکدیگر برخورد نموده و خراب می گردند. هاب به منظور تشخیص این نوع تصادم ها به اندازه کافی هوشمند بوده و برای مدت زمان کوتاهی چراغ مربوط به Collision روشن می گردد. (یک دهم ثانیه به ازای هر تصادم).

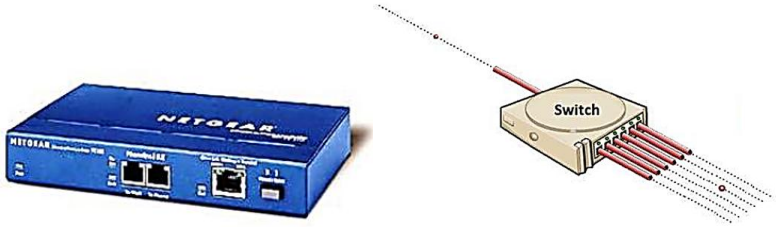
تعداد اندکی از هاب ها دارای یک اتصال خاص از نوع BNC بوده که می توان از آن به منظور اتصال یک کابل کواکسیال، استفاده نمود. پس از اتصال فوق، LED مربوط به اتصال BNC روی هاب روشن می گردد. لازم به ذکر است که این وسیله (HUB) امروزه دیگر تولید نمی شود و به جای آن در شبکه های امروزی از Switch استفاده می گردد.

به یاد داشته باشید که هاب نیز در لایه فیزیکی شبکه کار می کند و ضمن توزیع کردن سیگنال ورودی بین سایر پورت ها، سیگنال ورودی را تقویت نیز می کند. به این ترتیب در شبکه های Star در فواصل دور، برای اتصال کامپیوتر ها به یکدیگر نیز می توان از آن استفاده کرد.

سوئیچ (Switch)

سوئیچ یکی از عناصر اصلی و مهم در شبکه های کامپیوتری است. با استفاده از سوئیچ، چندین کاربر قادر به ارسال اطلاعات از طریق شبکه در یک لحظه خواهند بود. سرعت ارسال اطلاعات هر یک از کاربران بر سرعت دستیابی سایر کاربران شبکه تاثیر نخواهد گذاشت.

سوئیچ همانند روتر که امکان ارتباط بین چندین شبکه را فراهم مینماید، امکان ارتباط گره های متفاوت (معمولا کامپیوتر) یک شبکه را مستقیما با یکدیگر فراهم می نماید. شبکه ها و سوئیچ ها دارای انواع متفاوتی می باشند.



سوئیچ ها، هوشمند تر از هاب ها می باشند و به هر کاربر یا هر گروه از کاربران پهنای باند مشخصی را اختصاص می دهند. سوئیچ، براساس اطلاعات موجود در Header هر بسته، بسته داده ها را تنها به پورت گیرنده مورد نظر و متصل به شبکه LAN ارسال می کند. سوئیچ در هر انتقال ویژه باعث ایجاد تماس های فردی وموقت بین منابع و مقاصد شده و پس از اتمام مکالمه، به این تماس خاتمه می دهد.

به عبارت دیگر، سوئیچ وسیله ای است که بسته ها را مستقیما به پورت های مرتبط با نشانی های خاص شبکه هدایت می کند. سوئیچ ها فهم بیشتری به مدیریت انتقال داده اضافه میکنند.

سوئیچها معمولا در لایه ۲ مدل OSI هستند(سوئیچ لایه ۳ را بعدا توضیح می دهیم) و با تعداد پورت ۵، ۸، ۱۶، ۲۴ و گاهی ۳۶ و۴۸ پورت نیز تولید می شوند. سرعت آنها معمولا ۱۰/۱۰۰ و یا ۱۰۰۰ مگابیت بر ثقانیه است. سوئیچ ها دارای پورت های RJ-45 و یا فیبر نوری و یا ترکیبی از ر دو هستند. در دو نوع رومیزی و رکمونت (نصب در رک های ۱۹ اینچ استاندارد) وجود دارند.

سوئیچ هایی که برای هر یک از اتصالات موجود در یک شبکه داخلی استفاده می کردند، سوئیچ های LAN نامیده می شوند. این نوع سوئیچ ها مجموعه ای از ارتباطات شبکه را صرفا بین دو دستگاه که قصد ارتباط با یکدیگر را دارند، در زمان مورد نظر ایجاد می نماید.

برخی از اصطلاحات شبکه

۱- **گره.** گره، شامل هر چیزی که به شبکه متصل می گردد، خواهد بود.(کامپیوتر، چاپگر و...)

۲-**سگمنت.** سگمنت یک بخش خاص از شبکه بوده که توسط یک سوئیچ، روتر و یا Bridge از سایر بخش ها جدا شده است.

۳-**ستون فقرات.** کابل اصلی که تمام سگمنت ها به آن متصل می گردند. معمولا ستون فقرات یک شبکه دارای سرعت بمراتب بیشتری نسبت به هریک از سگمنت های شبکه است. مثلا ممکن است نرخ انتقال اطلاعات ستون فقرات شبکه ۱۰۰ مگابیت در ثانیه بوده در صورتیکه نرخ انتقال اطلاعات هر سگمنت ۱۰ مگابیت در ثانیه باشد.

۴-**توپولوژی.** روشی که هر یک از گره ها به یکدیگر متصل می گردند را گویند.

۵- **آدرس MAC.** آدرس فیزیکی هر دستگاه (کارت شبکه) در شبکه است. آدرس فوق یک عدد شش بایتی بوده که سه بایت اول آن مشخص کننده سازنده کارت شبکه و سه بایت دوم، شماره سریال کارت شبکه است.

۶- **Unicast.** ارسال اطلاعات توسط یک گره با آدرس خاص و دریافت اطلاعات توسط گره دیگر است.

۷- **Multicast.** یک گره، اطلاعاتی را برای یک گروه خاص (با آدرس مشخص یا الگوی خاص) ارسال می دارد. فقط دستگاههای موجود در گروه، اطلاعات ارسالی را دریافت خواهند کرد.

۸-**Broadcast.** یک گره اطلاعاتی را برای تمام گره های موجود در شبکه ارسال می نماید.

تکنولوژی سوئیچ ها

سوئیچ ها دارای پتانسیل های لازم به منظور تغییر روش ارتباط هر یک از گره ها با یکدیگر می باشند. تفاوت سوئیچ با رئتر چیست؟ سوئیچ ها معمولا در لایه دوم (Data layer) مدلOSI فعالیت می نمایند. در لایه فوق امکان استفاده از آدرس های MAC (آدرس های فیزیکی) وجود دارد. روتر در لایه سوم (Network) مدل OSI فعالیت می نمایند. در لایه فوق از آدرس های IP وIPX و یا Appler Talk استفاده می شود. (آدرس های منطقی). الگوریتم استفاده شده توسط سوئیچ به منظور اتخاذ تصمیم در رابطه با مقصد یک بسته اطلاعاتی با الگوریتم استفاده شده توسط روتر، متفاوت است.

یکی از موارد اختلاف الگوریتم های سوئیچ و هاب، نحوه برخورد آنان با Broadcast است. مفهوم بسته های اطلاعاتی از نوع Broadcast در تمام شبکه ها مشابه می باشد. در چنین مواردی، دستگاهی نیاز به ارسال اطلاعات داشته ولی نمی داند که اطلاعات را برای چه کسی می بایست ارسال نماید.

به دلیل عدم آگاهی و دانش نسبت به هویت دریافت کننده اطلاعات، دستگاه مورد نظر اقدام به ارسال اطلاعات به صورت Broadcast می نماید. مثلا هر زمان که کامپیوتر جدید و یا یک دستگاه به شبکه وارد می شود، یکبسته اطلاعاتی از نوع Broadcast برای معرفی و حضور خود در شبکه ارسال می دارد. سایر گره ها قادر به افزودن کامپیوتر مورد نظر در لیست خود و برقراری ارتباط با آن خواهند بود. بنابراین بسته های اطلاعاتی از نوع Broadcast در موردی که یک دستگاه نیاز به معرفی خود به سایر بخش های شبکه را داشته و یا نسبت به هویت دریافت کننده اطلاعات شناخت لازم وجود نداشته باشند، استفاده می کردند.

هاب و یا سوئیچ ها قادر به ارسال بسته ای اطلاعاتی از نوع Broadcast برای سایر سگمنت های موجود در حوزه Broadcast می باشند. روتر عملیات فوق را انجام نمی دهد. در صورتیکه آدرس یک دستگاه مشخص نگردد، روتر قادر به مسیریابی بسته اطلاعاتی مورد نظر نخواهد بد. ویژگی فوق در مواردی که قصد جداسازی شبکه ها از یکدیگر مد نظر باشد، بسیار ایده آل خواهد بود. ولی زمانیکه هدف مبادله اطلاعاتی بین بخش های متفاوت یک شبکه باشد، مطلوب به نظر نمی آید. سوئیچ ها با هدف برخورد با مشکل فوق عرضه شده اند.

سوئیچ های LAN براساس تکنولوژی Packet-Switching فعالیت می نمایند. سوئیچ یک ارتباط بین دو سگمنت ایجاد می نماید. بسته های اطلاعاتی اولیه در یک محل موقت (بافر) ذخیره می گردند، آدرس فیزیکی (MAC) موجود در هدر خوانده شده و در ادامه با لیستی از آدرس های موجود در جدول Lookup (جستجو) مقایسه می گردد. در شبکه های LAN مبتنی بر اترنت، هر فریم اترنت شامل یک بسته اطلاعاتی خاص است. بسته اطلاعاتی فوق شامل یک عنوان (هدر) خاص و شامل اطلاعات مربوط به آدرس فرستنده و گیرنده بسته اطلاعاتی است.

انواع سوئیچ های Lan از نظر طراحی فیزیکی

۱- Shared Memory: این نوع از سوئیچ ها تمام بسته های اطلاعاتی اولیه در بافر مربوط به خود را ذخیره می نمایند. بافر فوق به صورت مشترک توسط تمام پورت های سوئیچ (اتصالات ورودی و خروجی) استفاده می گردد. در ادامه اطلاعات مورد نظر به کمک پورت مربوطه برای گره مقصد ارسال خواهند شد.

۲-Matrix: این نوع از سوئیچ ها دارای یک شبکه (تور) داخلی ماتریس مانند بوده که پورت های ورودی و خروجی همدیگر را قطع می نمایند. زمانیکه یک بسته اطلاعاتی بر روی پورت ورودی تشخیص داده شد، آدرس MAC آن با جدول Lookup مقایسه تا پورت مورد نظر خروجی آن مشخص گردد. در ادامه سوئیچ یک ارتباط را از طریق شبکه ودر محلی که پورت ها همدیگر را قطع می کنند، برقرار می گردد.

۳-Bus Architecture: در این نوع از سوئیچ ها به جای استفاده از یک شبکه (تور)، از یک مسیر انتقال داخلی (Bus) استفاده و مسیر فوق با استفاده از TDMA توسط تمام پورت ها به اشتراک گذاشته می شود. سوئیچ های فوق برای هر یک از پورت ها دارای یک حافظه اختصاصی می باشند.

۴-Transparent Bridging: اکثر سوئیچ های LAN مبتنی بر اترنت از سیستمی با نام Transparent Bridging برای ایجاد جداول آدرس Lookup استفاده می نمایند. تکنولوژی فوق امکان یادگیری هر چیزی در رابطه با محل گره های موجود در شبکه، بدون حمایت مدیریت شبکه را فراهم می نماید. تکنولوژی فوق دارای پنج بخش متفاوت است:

۱. Learning
۲. Flooding
۳. Filtering
۴. Forwarding
۵. Aging

سوئیچ های مدیریتی

برای کنترل و نگهداری شبکه های بزرگ و یا شبکه هایی که نیاز به پهنای یاند زیاد و کنترل شده دارند نیاز به استفاده از سوئیچ های مدیریتی است. با اینگونه سوئیچ ها می توان تنظیمات متنوعی از قبیل پهنای باند، شبکه های مجازی، کنترل و گزارشات ترافیکی شبکه و ... را انجام داد. از مشخصاتی که تقریبا در تمام آنها مشترک است می توان به رکمونت بودن، تعداد ۲۴ پورت به بالا، امکان افزودن چندین نوع ماژول برای کاربردهای مختلف، وجود پورت سریال برای مدیریت مستقیم، امکان مدیریت از طریق وب، دارا بودن نرم افزار مدیریتی، پاور های اضافی وقیمت بسیار بالانسبت به سوئیچ های رایج اشاره کرد. سرعت سوئیچ کردن داخلی و همچنین حجم داده انتقالی در زمان واحد از جمله مشخات مهم سوئیچ ها و تعیین کننده قیمت آنها می باشد. برخی از این سوئیچ ها امکان مدیریت در لایه ۲ شبکه و بالاتر را نیز دارند.

ماژول سوئیچ

ماژول ها قطعاتی سخت افزاری هستند که به سخت افزار اصلی متصل شده و امکاناتی را بسته به نیاز شبکه به آن اضافی می نمایند. به سوئیچ هایی که دارای ورودی برای نصب ماژول هستند سوئیچ های ماژولار گفته می شود. جدید ترین ماژول ها، ماژول های SFP یا Mini GIBIC هستند که انواع پورت های گیگابیت بر روی فیبر نوری و کابل مسی ارائه می کنند. سوئیچ ماژولار این امکان را به طراح شبکه میدهد تا بتواند چندین نوع مدیا را در کنار هم داشته باشند.

پل (Bridge)

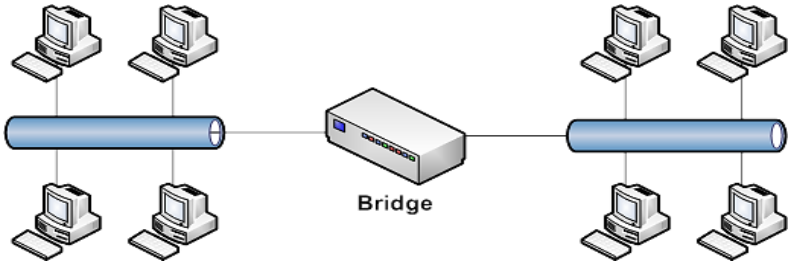
پل وسیله ای است که دو شبکه محلی را بدون توجه به اینکه از پروتکل یا ساختار یکسان استفاده می کنند یا خیر به یکدیگر متصل می کند و امکان جریان یافتن اطلاعات در بین آنها را فراهم می آورد.

به عبارت دیگرBridge، سخت افزاری است که پل ارتباطی دو LAN مختلف می باشد. تفاوت بین یک پل یا Bridge و Router در تکنیک برقراری ارتباط بین دو LAN در این است که Router در هر شبکه ای عمل مسیر یابی را انجام می دهد و براساس IP مبدا و مقصد اطلاعات را در شبکه انتقال می دهد. اما یک Bridge که معمولا در شبکه های مخابراتی و بی سیم بکار می رود، سخت افزار یا نرم

افزاری است که اطلاعات از جنس لایه دوم یک شبکه (Frame) را در شبکه دیگر کپی می کند؛ به عنوان مثال دو LAN می توانند به وسیله خط تلفن به یک دیگر متصل شوند. استفاده از Bridge کارایی شبکه را تا حد زیادی کاهش می دهدو باعث کندی شبکه می شود.

پل ها اصولا در شبکه هایی استفاده می شوند که از پروتکل های غیرقابل مسیردهی استفاده می کنند. یعنی آدرس مبدا و مقصد ندارند. این پروتکل ها به راحتی از Bridge عبور می کنند. نمونه ای از این پروتکل ها NetBIOS و NetBeui می باشند. توجه داشته باشید که با تقسیم یک شبکه ی بزرگ به چندین سگمنت و استفاده از یک پل برای اتصال آنها به یکدیگر، توان عملیاتی شبکه افزایش خواهد یافت. اگر یک سگمنت شبکه از کار بیفتد، سایر سگمنت های متصل به پل می توانند شبکه را فعال نگه دارند. پل ها موجب افزایش وسعت شبکه محلی می شوند.

همانطور که می دانید، Repeater و هاب چنان طراحی شده اند که همه بار شبکه را که دریافت کرده اند به همه پورت های متصل به آنها، توزیع می نمایند. به عبارت دیگر ترافیک ایجاد شده در قسمتی از شبکه را به بخشهای دیگر شبکه عمومیت می دهند. به منظور رفع این مشکل از پل (Bridge) استفاده می کنند.



فرض کنید ۸ کامپیوتر را توسط ۲ تا هاب ۵ پورت به یکدیگر متصل کرده ایم. در این مثال، اگر اتصال هاب ها را به طور مستقیم به یکدیگر وصل کنیم، این امر باعث می شود که ترافیک هر بخش از شبکه، از هاب مربوطه رد شده و به هاب دیگر رسیده و از طریق آن، بخش دیگر شبکه را نیز تحت تاثیر خود قرار دهد. به این ترتیب ترافیک شبکه سیر صعودی خواهد داشت. برای رفع این مشکل از Bridge (پل) در نقطه میانی دو هاب استفاده می شود تا ترافیک در هر بخش، محلی باقی بماند و به بخش دیگر منتقل نشود و به این ترتیب ترافیک شبکه کاهش می یابد.

پل، این عملیات را توسط فیلتر کردن داده ها انجام می دهد. نحوه کار به این ترتیب است که پل آدرس فیزیکی تمام کامپیوتر های موجود در یک بخش را می داند و موقعیت آنها را در جدول داخل خود ذخیره می کند. وقتی که یک فریم از یک بخش وارد آن می شود، در جدول داخلی خود به دنبال آدرس فیزیکی آن می گردد تا آدرس مقصد فریم را مشخص کند.

اگر آدرس مقصد فریم در همان سگمنت آدرس مبدا باشد، پل از عبور فریم به بخش های دیگر ممانعت به عمل آورده و فریم مربوطه در همان بخش به دنبال مقصد خود می گردد. ولیکن اگر فریم به سگمنت دیگری تعلق داشته باشد، پل فریم مربوطه را به آن بخش پاس می دهد.

به عبارت دیگر پل،فریم هایی را که آدرس مبدا و مقصدشان در یک بخش از شبکه است، در همان بخش نگه می داردو با این کار باعث می شود ترافیک یک قسمت از شبکه به قسمت دیگر منتقل نشود.

به یاد داشته باشید که Bridge در لایه ۲ کار می کند و مفهوم MAC Address را از روی بسته ها می تواند بخواند و طبق جدول MAC Address ها، عمل فیلتر فریم ها را انجام می دهد.

همچنین Bridge می تواند شبکه های با رسانه های مختلف را به هم متصل کند. به عنوان مثال یک Bridge می تواند یک شبکه مبتنی بر فیبر نوری (100BaseFX) را به یک شبکه مبتنی بر کابل (10BaseTX) متصل کند و کامپیوترهای موجود در بخشهای با رسانه ها و توپولوژی های متفاوت با یکدیگر به نقل و انتقالات داده بپردازند.

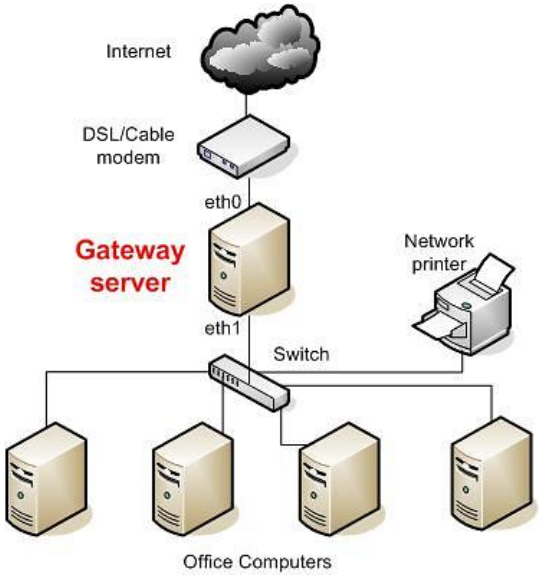
دروازه (Getway)

مهمترین و اساسی ترین وسیله ای که در یک مرکز سرویس دهی اینترنت مورد استفاده واقع می شود Gateway و یا Router می باشد . فرق اصلی ما بین این دو دستگاه این است که Router دارای جداول مسیریابی است ولی Gateway صرفاً بعنوان دروازه عمل می کند.

Gateway همان طور که از اسمش پیداست کارش اتصال بین دو شبکه است و اغلب از آن بعنوان یک درگاه یاد می شود در داخل Gatewayها باید حتماً کارت شبکه ای موجود باشد تا از طریق آن بتوان آن را به سرور اصلی متصل کرد .

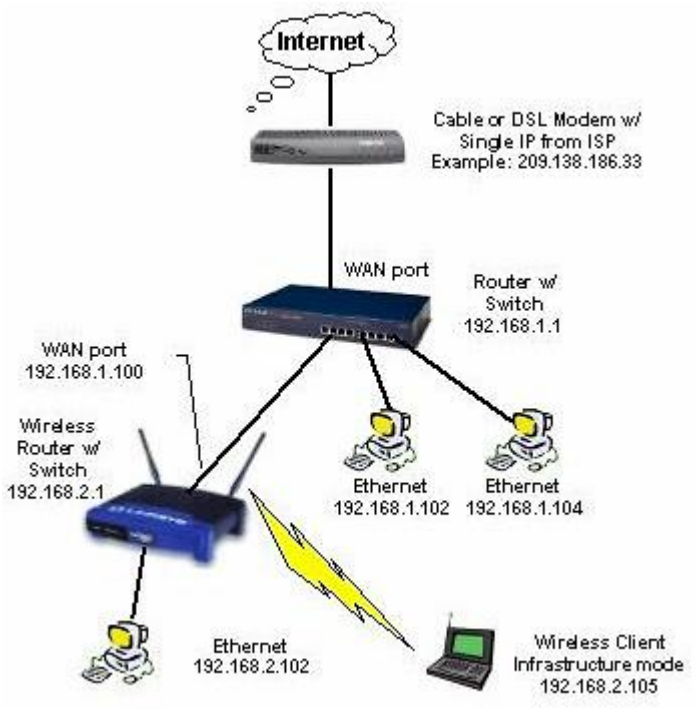
همچنین این دستگاه باید حتماً دارای محلی جهت ارسال و دریافت اطلاعات فرستاده شده به ماهواره و یا دریافت شده از ماهواره باشد. بدین منظور بر روی آن کارتهای مختلف سخت افزاری سوار است . کارت شبکه ای که در داخل یک Gateway به کار می رود با بقیه متفاوت است . سیم های متصل شده به Gateway نیز با بقیه سیم های شبکه که معمولاً STP,UTP یا Coaxial هستند متفاوت است . سیمی که جهت دریافت اطلاعات مورد استفاده قرار می گیرد مثل سیم های Reciver های معمولی می باشد ولی سیمی که جهت ارسال اطلاعات مورد استفاده قرار می گیرد کمی متفاوت است.

این سیم ضخیم تر از سیم های معمولی است و بسته به دستگاههای مختلف دارای پهنا و شکل متفاوتی است معمولاً دارای پنج پین جداگانه می باشد که باید به کانکتور مخصوص خود وصل شود.



بعضی از Gatewayها در کنار خود وسیله ای بعنوان Black Box و یا Small Box دارند که در حقیقت همان کار آداپتور را انجام می دهد. *کار Gateway ترجمه پروتکل بین دو شبکه غیر همجنس می باشد به عنوان مثال در شبکه هایی که TCP/IP Base نیستند با استفاده از یک Gateway می توان پروتکل شبکه رابه پروتکل TCP/IP و برعکس تبدیل نمود. یک کاربرد دیگر Gateway این است که می توان تنظیم نمود که تمامی Packet های خروجی یک کامپیوتر به سمت کامپیوتری خاص برود. مثلاً کامپیوتر سرویس دهنده اینترنت*

مسیریاب (Router)



مسیریاب و یا همان روتر، یک وسیله میانجی در شبکه های ارتباطی است که مسئولیت تحویل پیام ها را بر عهده دارد. در شبکه ای که کامپیوتر های زیادی را از طریق حلقه ای از اتصالات با یکدیگر مرتبط می کند، مسیریاب پیام های مورد نظر را هدایت می کند.

مسیریاب ها در مقایسه با هاب ها و سوئیچ ها، از هوشمندی بیشتری برخوردارند. مسیریاب ها از بسته، اطلاعات کاملتری جهت تشخیص این مسئله که کدام مسیریاب یا ایستگاه کاری، می بایست بسته بعدی را دریافت کند، دارا می باشد. مسیریاب ها از طریق نقشه مسیر شبکه، تحت عنوان " جدول مسیریابی" ، ارسال بسته ها از طریق بهترین مسیر به مقصد را تضمین می کنند. در صورت قطع ارتباط بین دو مسیریاب، مسیریاب ارسال کننده، مسیر دیگری را جهت ادامه سیر و حرکت در نظر می گیرد. در ضمن مسیریاب می تواند بین شبکه هایی که به زبانهای مختلفی صحبت میکنند، یعنی دارای "پروتکل های" مختلفی می باشند، ارتباط برقرار کند. برخی از این پروتکلها عبارتند از: پروتکل اینترنت(IP)، تبادل بسته های اینترنتی(IPX) و Apple Talk .

مسیریاب ها به سبب برخورداری از هوش بیشتر، قادرند با اجتناب از ایجاد ترافیک در برخی بخشهای دستیابی شبکه، باعث تامین امنیتی بیشتر بشوند.

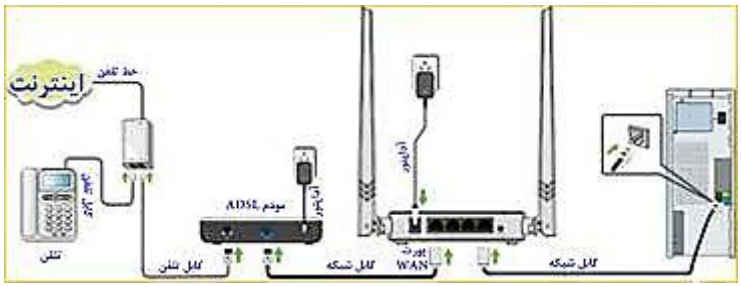
مسیریاب ها می توانند شبکه ها را به یک مکان منفرد یا مجموعه ای از ساختارها متصل کرده و سبب تامین رابط هایی برای اتصال LAN ها به WAN بشوند، درست مثل ارتباط شعبه های اداری به یکدیگر یا به اینترنت.

مسیریاب ها در لایه ۳ مدل مرجع OSI کار می کنند؛ یعنی هر مسیریاب بسته را شناخته و می تواند از روی Header بسته ها، مبدا و مقصد را تشخیص دهد. وقتی کامپیوتری در یک شبکه بسته ای را ارسال می کند که مقصد آن در شبکه محلی متصل به آن کامپیوتر موجود نیست، کامپیوتر آن بسته را تحویل Gateway می دهد تا از شبکه خارج شود. Gateway ها در شبکه معمولا تجهیزاتی هستند که عمل مسیریابی را انجام می دهند. پسRouter شبکه یا همان Gateway آدرس مقصد بسته ها را با مسیرهای خود مقایسه می کند تا کوتاه ترین و بهترین مسیر را بین مبدا و مقصد انتخاب کنند و در صورت وجود مسیر، بسته به خروجی مورد نظر ارسال می شود و در صورت عدم وجود مسیر، برای مسیریابی Router یا با مسیریاب های مجاور مشورت می نماید و یا بسته را تحویل مسیریاب بعدی که در واقع Gateway مربوط به این مسیریاب می باشد هدایت می کند.

هر Router دارای یک Routing Table می باشد که این جدول به صورت پویا نسبت به مسیریاب های همسایه به روز رسانده می شود. (پروتکل هایی مانند RIP وOSPF). به عبارت بهتر مسیریاب ها همیشه در مورد مسیریاب های موجود برروی اینترنت با یکدیگر تبادل نظر می نمایند. مسیریاب ها همواره به دنبال بهترین مسیر با کمترین هزینه بروی اینترنت می گردند.

آشنایی با روتر:

استفاده از روترها در شبکه به امری متداول تبدیل شده است. یکی از دلایل مهم گسترش استفاده از روتر، ضرورت اتصال یک شبکه به چندین شبکه دیگر (اینترنت و یا سایر سایت های از راه دور) در عصر حاضر است. نام در نظر گرفته شده برای روتر ها، متناسب با کاری است که آنان انجام می دهند: *"ارسال و مسیر دهی داده از یک شبکه به شبکه ای دیگر"* .مثلا در صورتی که یک شرکت دارای شعبه ای در اصفهان و یک دفتر دیگر در شیراز باشد، به منظور اتصال آنان به یکدیگر می توان از یک خط Leased (اختصاصی) که به هر یک از روتر های موجود در دفاتر متصل می گردد، استفاده نموده بدین ترتیب، هر گونه ترافیکی که لازم است از یک سایت به سایت دیگر انجام شود از طریق روتر محقق شده و تمامی ترافیک های غیر ضروری دیگر فیلتر و در پهنای باند و هزینه های مربوطه، صرفه جویی می گردد.



انواع Router

روترها را می توان به دو گروه عمده سخت افزاری و نرم افزار تقسیم نمود:

روتر های سخت افزاری: روترهای فوق، سخت افزارهایی می باشند که نرم افزارهای خاص تولید شده توسط تولید کنندگان را اجراء می نماید(درحال حاظر صرفا به صورت Black Box (جعبه سیاه) به آنان نگاه می کنیم). نرم افزار فوق، قابلیت مسیر دهی را برای روتر ها فراهم نموده تا آنان مهمترین و شاید ساده ترین وظیفه خود را ارسال داده از یک شبکه به شبکه دیگراست را به خوبی انجام دهند. اکثر شرکت ها ترجیع می دهند که از روتر های سخت افزاری استفاده نمایند، چرا که آنان در مقایسه با روتر های نرم افزاری، دارای سرعت و اعتماد پذیری بیشتری می باشند.

روتر های نرم افزاری: روتر های نرم افزاری دارای عملکردی مشابه با روتر های سخت افزاری بوده و مسئولیت اصلی آنان نیز ارسال داده از یک شبکه به شبکه دیگر است. یک روتر نرم افزاری می تواند یک سرویس دهنده NT، یک سرویس دهنده ویندوز سرور، یک سرویس دهنده Novell Netware و یا یک سرویس دهنده لینوکس باشد. تمامی سیستم های عامل شبکه ای مطرح، دارای قابلیت های مسیردهی از این قبیل تعبیه شده می باشند.

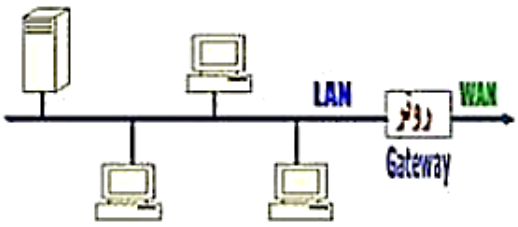
در اکثر موارد از روتر ها به عنوان فایروال یا Gateway اینترنت، استفاده می گردد. در این رابطه لازم است به یکی از مهمترین تفاوت های موجود بین روترهای نرم افزاری و سخت افزاری، اشاره گردد: در اکثر موارد نمی توان یک روتر نرم افزاری را جایگزین یک روتر سخت افزاری نمود، چرا که روتر های سخت افزاری دارای سخت افزار لازم و از قبل تعبیه شده ای می باشندکه به ،آنان امکان اتصال به یک لینک خاص WAN (از نوع Frame Relay، ISDN و یا ATM)را خواهد داد. یک روتر نرم افزاری (نظیر سرویس دهنده ویندوز) دارای تعدادی کارت شبکه است که هر یک از آنان به یک شبکه LAN متصل شده و سایر اتصالات به شبکه های WAN از طریق روتر های سخت افزاری، انجام خواهد شد.

مثال۱: استفاده از روتر به منظور اتصال دو شبکه به یکدیگر و ارتباط به اینترنت

فرض کنید از یک روتر مطابق شکل زیر به منظور اتصال دو شبکه LAN به یکدیگر و اینترنت، استفاده شده است. زمانی که روتر داده ای را از طریق یک شبکه LAN و یا اینترنت دریافت می نماید، پس از بررسی آدرس مبداء و مقصد، داده دریافتی را برای هر یک از شبکه ها و یا اینترنت ارسال می نماید. روتر استفاده شده در شکل زیر، شبکه را به دو بخش متفاوت تقسیم نموده است(دو شبکه مجزا). هر شبکه دارای یک هاب است که تمامی کامپیوترهای موجود در شبکه به آن متصل شده اند. علاوه بر موارد فوق، روتر استفاده شده دارای اینترفیس های لازم به منظور اتصال هر شبکه به آن بوده و از یک اینترفیس دیگر به منظور اتصال به اینترنت، استفاده می نماید. بدین ترتیب، روتر قادر است داده مورد نظر را به مقد درست، ارسال نماید.

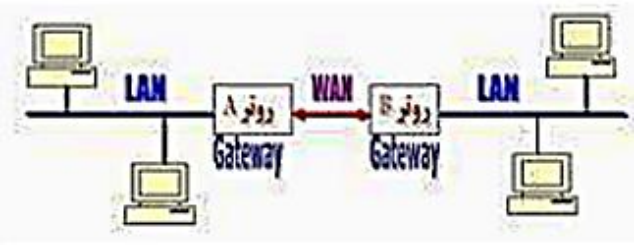
مثال۲:استفاده از روتر در یک شبکه LAN

فرض کنید از یک روتر مطابق شکل زیر در یک شبکه LAN، استفاده شده است. در مدل فوق، هر یک از دستگاههای موجود در شبکه با روتر موجود نظیر یک Gateway برخورد می نمایند. بدین ترتیب، هر یک از ماشین های موجود بر روی شبکه LAN که قصد ارسال یک بسته اطلاعاتی (اینترنت و یا هر محل خارج از شبکه LAN) را داشته باشند، بسته اطلاعاتی مورد نظر را برای Gateway ارسال می نمایند. روتر (Gateway) نسبت به محل ارسال داده دارای آگاهی لازم می باشد (در زمان تنظیم خصلت های پروتکل TCP/IP برای هر یک از ماشین های موجود در شبکه یک آدرس IP برای Gateway در نظر گرفته می شود). شکل زیر نحوه استفاده از یک روتر به منظور دستیابی کاربران به اینترنت در شبکه LAN را نشان می دهد:



مثال۳: استفاده از روتر به منظور اتصال دو دفتر کار

فرض کنید، بخواهیم از روتر به منظور اتصال دو دفتر کار یک سازمان به یکدیگر، استفاده نماییم. بدین منظور هر یک از روترهای موجود در شبکه با استفاده از یک پروتکل WAN نظیر ISDN به یکدیگر متصل می گردند. عملا، با استفاده از یک کابل که توسط ISP مربوطه ارائه می گردد، امکان اتصال به اینترفیس WAN روتر فراهم شده و از آنجا سیگنال مستقیما به شبکه ISP مربوطه رفته و سر دیگر آن به اینترفیس WAN روتر دیگر متصل می گردد. روتر ها، قادر به حمایت از پروتکل های WAN متعددی نظیر Frame Relay , ATM , HDLC و یا PPP، می باشند.



مهمترین ویژگیهای یک Router

روتر ها دستگاههای لایه سوم (مدل مرجعOSI) می باشند.

روتر ها مادامی که برنامه ریزی نکردند، امکان توزیع داده را نخواهند داشت.

اکثر روترها مهم دارای سیستم عامل اختصاصی خاص خود می باشند.

روتر ها از پروتکل های خاصی برای مبادله اطلاعات ضروری خود (منظور داده نیست)، استفاده می کنند.
نحوه عملکرد یک روتر در اینترنت: مسیر ایجاد شده برای انجام مبادله اطلاعاتی بین سرویس گیرنده و سرویس دهنده در تمامی مدت زمان انجام تراکنش ثابت و یکسان نبوده و متناسب با وضعیت ترافیک موجود و در دسترس بودن مسیر، تغییر می نماید.

آشنایی با مسیریاب های سیسکو CISCO

تاریخچه مسیریاب های سخت افزاری

نام کلی که برای مسیریاب ها در نظر گرفته شده به خاطر اولین و اصلی ترین وظیفه هر روتر یعنی عمل مسیریابی است و انتخاب این نام هم به سال ۱۹۸۴ بر می گردد. یعنی زمانی که رفته رفته با ظهور کامپیوتر های شخصی مشکل تعدد استانداردها تبدیل به یک مشکل حاد برای شبکه های موجود شد. گویا در این هنگام دو دانشمند به نام های Leonard Bosack و Sandy Lerner از دانشگاه استنفورد برای اتصال شبکه ها و مسیریابی داده ها بین این شبکه ها و حل مشکل عدم سازگاری پروتکل های مختلف در سطح مسیریاب ها، ایده مسیر یابی (Routing) را مطرح نمودند و موفق شدند اولین مسیریاب را با هزینه شخصی تولید کرده و آن را در دانشگاه استنفورد نصب نمایند. با توجه به استقبالی که از این محصول جدید شد این دو نفر تصمیم گرفتند که محصول خود را تجاری کنند.
در این سال بود که غول تجهیزات شبکه های کامپیوتری یعنی شرکت سیسکو در زمینه طراحی و تولید مسیریاب های سخت افزاری حرف اول را زد و در این زمینه به جز چند شرکت از جمله Foundry Networks و Norterl Networks رقیب جدی دیگری نداشت و طی سال ها با ارائه راه حل های جدیدی نظیر ایجاد تنوع در کلیه محصولات و ارائه گواهینامه های مهندسی تجهیزات سیکو نظیر CCNA، CCDA، CCNP وCCIE و... موقعیت خود را بیش از پیش تثبیت نموده است. به همین دلیل از مجموعه شرکت های تولید کننده روتر های سخت افزاری تنها برروی مسیریاب های شرکت سیسکو تمرکز می کنیم و به دلیل تنوع زیاد مسیریاب های این شرکت و همچنین تعدد ماژول های مورد استفاده که به منظور افزایش انعطاف پذیری مسیریاب ها استفاده می شوند، تنها به تشریح مدل های معروف تر خواهیم پرداخت. یک مسیریاب صرف نظر از نوع، سری و قیمت آن، همانند یک کامپیوتر دارای اجزای سخت افزاری نظیرجعبه (Case) برد اصلی (Mother Board)، پردازنده، حافظه موقت (RAM)، حافظه دائمی (Flash) و رابط ها و ماژول های مختلف است که بسته به کاربرد هر مسیریاب توان و ظرفیت متفاوتی دارند و همچنین هر مسیریاب دارای یک سیستم عامل است که ISA نامیده می شود
و سرنام کلمات Internetworking Operating System می باشد. ولی از آنجائی که مسیریاب ها فاقد صفحه کلید و مانیتور هستند، معمولا به سه طریق می توان فرامین سیستم عامل را برای پیکربندی مسیریاب وارد نمود، این سه روش عبارتند از :

۱-کنسول (Consol)


کابل کنسول روتر

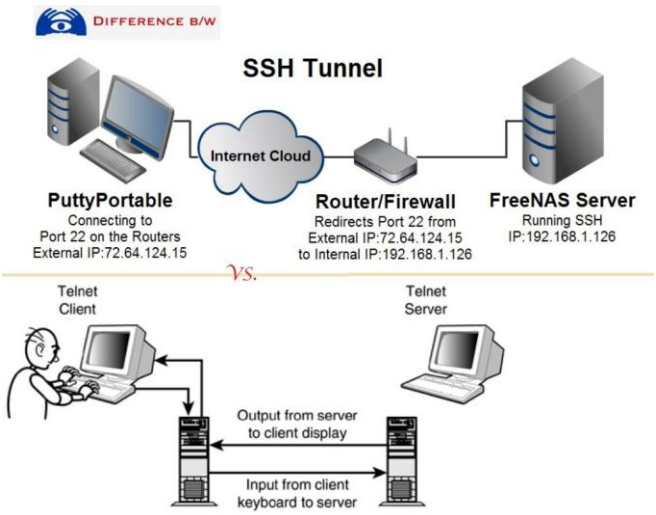
به همراه هر مسیریاب یک کابل ۸ رشته مخصوص به نام کابل Rollover ارائه می شود که با استفاده از آن و یک کامپیوتر شخصی و از طریق برنامه هایی نظیر Term90 یا HyperTerminal ویندوز که قابلیت تبادل داده با پورت های سریال کامپیوتر را دارند، می توان پیکربندی روتر را در بالاترین سطح دسترسی انجام داد.

نکته:

با امکان دسترسی فقط در این سطح، می توان تحت شرایطی حتی رمزهای عبور دستگاه را نیز تعویض نمود. به همین دلیل است که حفاظت فیزیکی دستگاه روتر بسیار حائز اهمیت است.

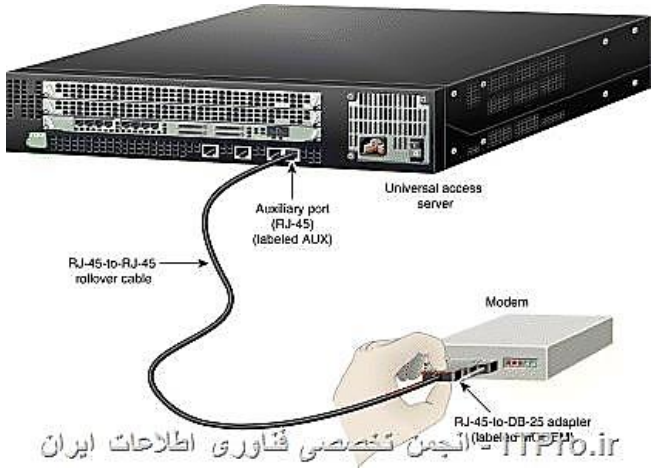
اولین باری که بخواهید پیکربندی یک روتر را انجام دهید، حتما می بایست از این طریق اقدام کنید.

Telnet –۲



از آنجایی که اصولا مسیریاب ها در لایه شبکه مدل TCP/IP کار می کنند، می توانیم به آنها آدرس IP اختصاص دهیم و طبعا با استفاده از پروتکل Telnet و پورت اترنت روتر می توانیم از راه دور به آن متصل شده و روتر را پیکربندی کنیم. البته باید بدانید که اجازه این نوع دسترسی قبلا می بایست از طریق کنسول صادر شده باشد وهمچنین این که کاربری که به این صورت به مسیریاب متصل شده، نسبت به روش اول از سطح دسترسی کمتری برخوردار است.

Aux–۳



این امکان برای مدیرانی است که می خواهند از طریق شماره گیری به مودم مسیریاب متصل شوند و آن را متناسب شرایط مد نظرشان پیکربندی کنند. برای این کار نیز لازم است از طریق کنسول دستگاه امکان استفاده ازAux را فعال نماییم.

سیستم عامل شبکه

هسته یک شبکه، سیستم عامل (Network Operrating Systerm) است. همانگونه که یک کامپیوتر بدون استفاده از یک سیستم عامل، قادر به انجام عملیات خود نخواهد بود، یک شبکه (چه شبکه Workgroup و چه شبکه Server Based) نیز بدون وجود یک سیستم عامل شبکه ای، قادر به انجام عملیات و ارائه سرویس های مربوطه نخواهد بود.

به عبارت دیگر، سیستم عامل شبکه، سیستم عاملی است که ویژه پشتیبانی از شبکه طراحی می شود. همین طور می توان گفت سیستم عامل شبکه، نرم افزاری است که یک شبکه و *ترافیک و صف پیام های روی آن* را کنترل می کند. همچنین *کنترل دسترسی چندین کاربر به یک منبع* بر روی شبکه نظیر یک فایل را بر عهده دارد و عملیات مدیریتی مهمی نظیر *کنترل امنیت* را میسر می سازد. سیستم عامل های مبتنی بر سرویس دهنده (Server) علاوه بر کارهای *نظارتی، امنیتی و مدیریتی*، پشتیبانی از کار در شبکه را نیز هم زمان برای چندین کاربر فراهم می کنند. سیستم عاملی که از وجود شبکه آگاه باشد (Network-Aware) می تواند امکان دستیابی به منابع شبکه را برای کاربران فراهم سازد.

برخلاف سیستم عامل های تک کاربره، این سیستم عامل ها باید درخواست های دریافتی از ایستگاه های کاری مختلف را پاسخ گویند و جزئیاتی چون دستیابی و ارتباطات شبکه، تخصیصو به اشتراک گذاشتن منابع، محافظت داده ها و کنترل خطاها را نیز مدیریت کنند. سر نام سیستم عامل های شبکه، NOS است که Network OS نیز نامیده می شود.

سیستم های عامل شبکه ای، سرویس ها و خدمات خاصی را در اختیار کامپیوترهای موجود در شبکه قرار خواهند داد:

۱-هماهنگی لازم در خصوص عملکرد دستگاه های متفاوت در شبکه به منظور حصول اطمینان از برقراری ارتباط در مواقع ضروری

۲- امکان دستیابی سرویس گیرندگان به منابع شبکه نظیر فایل ها و دستگاه های جانبی نظیر چاپگرها و دستگاه های فاکس

۳- اطمینان از ایمن بودن داده ها و دستگاه های موجود در شبکه از طریق تمرکز ابزارهای مدیریتی

ویژگی های یک سیستم عامل شبکه ای

یک سیستم عامل شبکه ای می بایست خدمات و سرویس های زیر را ارائه دهد:

ارائه مکانیزم های لازم به منظور برقراری ارتباط بین چندین دستگاه کامپیوتر برای انجام یک فعالیت خاص

حمایت از چندین پردازنده

حمایت از مجموعه ای (کلاستر) دیسک درایو- پردازنده – حافظه

ارائه امکانات و سرویس های امنیتی در رابطه با حفاظت از داده ها و سایر منابع موجود در شبکه

قابلیت اطمینان بالا

تشخیص و بر طرف نمودن خطا با سرعت مناسب

بر اساس نوع سیستم عامل، یک نرم افزار شبکه ای می تواند به سیستم عامل، اضافه و یا به صورت یکپارچه با سیستم عامل همراه باشد. نرم افزار سیستم عامل شبکه ای با مجموعه ای از سیستم های عامل رایج نظیر: ویندوز سرور (۲۰۰۰، ۲۰۰۳، ۲۰۰۸)، ویندوز NT، ویندوز۹۸، ویندوز ۹۵، و اپل مکینتاش، به صورت یکپارچه همراه می گردد.

البته نکته ای دیگر وجود دارد و آن اینکه برای راه اندازی یک شبکه، همیشه نیاز به داشتن سیستم عامل شبکه وجود ندارد. بلکه می توان از سیستم عامل شبکه های همه منظوره (مثل Windows XP) استفاده کرد. به خصوص در شبکه های Workgroup این موضوع بسیار مطرح می شود. اما اگر بخواهیم شبکه ای به مفهوم واقعی راه اندازی کنیم (Server Based)، عقل سلیم می گوید که برای Server از یک سیستم عامل شبکه استفاده کنیم.

برخی از سیستم عامل های معروف شبکه

- Windows NT
- IBM AIX
- Sun Solaris
- Plan 9 From Bell Labs
- Inferno
- Windows 2000, 2003, 2008 Server
- Novell NetWare
- Linux (Red Hat, Ubuntu, SUSE, …)
- Unix …,

معرفی انواع سرور

File Server

یک سروری می باشد که از طریق آن می توان امکانی جهت مدیریت فایل ها و دسترسی کاربران مختلف شبکه در درایورهای مختلف به صورت متمرکز بر روی یک سرور در شبکه خود برقرار کنیم؛ که جهت راه اندازی این نوع سرور در Windows Server از طریق Manage Your Server option در منوی Administrative Tools اقدام می کنیم.

Print Server

اگر بر روی کامپیوتری ویندوز سرور نصب شود و این کامپیوتر مجهز به یک دستگاه چاپگر باشد و این چاپگر جهت دسترسی کاربران مختلف شبکه به اشتراک گذاشته شود(Share)، این کامپیوتر می تواند به عنوان Print Server مورد استفاده قرار گیرد.

Application Server

سروری می باشد که بر روی آن برنامه های تحت وب قرار می گیرد و از طریق سرویس IIS (Internet Information Services) این برنامه در اختیار کامپیوترهای دیگر شبکه قرار می گیرد.

تعریف دیگری نیز وجود دارد و آن اینکه رایانه ای است که نرم افزارهای کاربردی را به درخواست کاربران برای آن ها اجرا کرده و نتایج حاصل از اجرا را روی رایانه خودشان نمایش می دهد. هسته ی مرکزی روی سرویس دهنده است و نه سرویس گیرنده. در اینجا سرویس گیرنده تنها یک درخواست کننده برای اجرای عمل است.

دلایل استفاده از Application Server:

- امکانات سخت افزاری سرویس گیرنده ممکن است برای اجرای مستقیم برنامه کافی نباشد، مانند دستگاه های ATM
- نیاز به مدیریت بیشتر و کنترل نرم افزارها

Terminal Serve

توسط این سرویس می توان به صورت Remote یا از راه دور به سرور متصل شده و به مدیریت مربوطه را انجام دهیم و یا برنامه ای تحت شبکه را بدین طریق و با استفاده از این سرویس اجرا نمود.

VPN/Remote Server

توسط این سرورها می توانیم به کاربران مختلف جهت متصل شدن به صورت راه دور (Remote) به شبکه داخلی مجوز هایی را بدهیم و یا با استفاده از VPN (Virtual Private Nertwork) ارتباطی امن بین دو نقطه ایجاد کنیم. (با کمک پروتکل های PPP، SSTP،L2TP و ...)

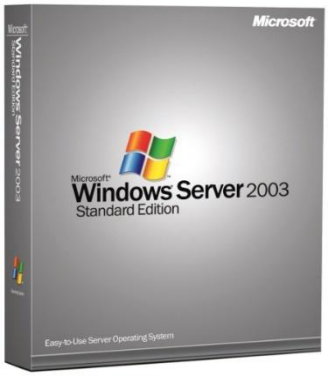
DNS Server

سروری می باشد که کار Name Resolution را برای ما انجام می دهد و وظیفه آن تبدیل IP به اسم و بالعکس می باشد.

DHCP Server

DHCP مخفف Dynamic Host Configuration Protocol می باشد. این سرور از طریق محدوده IP که بر روی آن تعریف می شود به صورت اتوماتیک به کلاینت ها IP می دهد و بسیاری کارهای دیگر که به جای خود به آن اشاره خواهیم کرد. در ضمن این سرویس حتما باید بر روی کامپیوتری که نسخه سرور دارد نصب شود.

ویندوز سرور ۲۰۰۳



سیستم عامل ویندوز سرور ۲۰۰۳، امکانات گسترده و پیشرفته ای را در اختیار کاربران قرار می دهد:

- **Multitasking:** با استفاده از ویژگی فوق، کاربران قادر به اجرای چندین برنامه به صورت همزمان بر روی یک سیستم می شوند. تعداد برنامه هایی که یک کاربر قادر به اجرای همزمان آنان خواهند بود به میزان حافظه موجود بر روی سیستم بستگی خواهد داشت.

- **Mermory Support:** به منظور انجام عملیات مربوط به برنامه هایی که در محیط ویندوز ۲۰۰۳ اجراء می گردند، به میزان مطلوبی از حافظه، نیاز خواهد بود. برای اجرای چندین برنامه به صورت همزمان وبا اجرای برنامه هایی که میزان بالائی از حافظه را نیاز دارند، ویندوز ۲۰۰۳ امکان حمایت تا ۶۴ و ۱۲۸ گیگابایت را فراهم می نماید.
- **Symmetric Multiprocessing:** سیستم های عامل از ویژگی فوق، به منظور استفاده همزمان از چندین پردازنده استفاده می نمایند. بدین ترتیب کارآیی سیستم بهبود و یک برنامه در محدوده زمانی کمتر اجراء خواهد شد. ویندوز۲۰۰۳، امکان حمایت(با توجه به نوع نسخه) از حداکثر ۳۲ پردازنده را فراهم می نماید.
- **Plug & Play:** با استفاده از ویندوز ۲۰۰۳، دستگاه هایی از نوع PNP به سادگی نصب می گردند. دستگاه های PNP، دستگاه هایی هستند که پس از اتصال به سیستم بدون نیاز به انجام فرآیندهای پیچیده، نصب خواهند شد. پس از اتصال چنین دستگاه هایی، ویندوز ۲۰۰۳ به صورت اتوماتیک آنان را تشخیص و عناصر مورد نیاز را نصب و پیکربندی مربوطه را انجام خواهد داد.
- **Clustering:** ویندوز ۲۰۰۳، امکان گروه بندی مستقل کامپیوترها را با یکدیگر و به منظور اجرای یک مجموعه از برنامه ها فراهم می نماید. این گروه به عنوان یک سیستم برای سرویس گیرندگان و برنامه ها در نظر گرفته خواهد شد. چنین گروه بندی، Clustering نامیده شده و گروه هایی از کامپیوتر را کلاستر می گویند. این نوع سازماندهی کامپیوترها، باعث برخورد مناسب در صورت بروز اشکال در یک نقطه می گردد. در صورتیکه یک کامپیوتر دچار مشکل گردد، کامپیوتر دیگر در کلاستر، سرویس مربوطه را ارائه خواهد داد.
- **File System:** ویندوز ۲۰۰، از۳ نوع مختلف سیستم فایل (قدیمی و جدید) حمایت می کند:FAT (File Allocation Table)، FAT32 و NTFS (New Technology File Systerm). در صورتی که نیازی به استفاده از قابلیت های بوت دو گانه (راه اندازی سیستم از طریق دو نوع متفاوت سیستم عامل با توجه به خواسته کاربر) وجود نداشته باشد، ضرورتی به استفاده از سیستم فایل FAT و یا FAT32 وجود نخواهد داشت. NTFS، سیستم فایل پیشنهادی برای ویندوز۲۰۰۳ بوده و امکانات امنیتی مناسبی را ارائه می نماید. ویندوز۲۰۰۳، با استفاده از سیستم NTFS امکانات متعددی نظیر: بازیافت سیستم فایل، اندازه پارتیش های بالا امنیت، فشرده سازی و Disk Quotas (سهمیه بندی دیسک) را ارائه می نماید.
- **Terminal Service:** با استفاده از ویژگی فوق، امکان دستیابی از راه دور به یک سرویس دهنده از طریق یک ترمینال شبیه سازی شده، فراهم می گردد. یک ترمینال شبیه سازی شده، برنامه ای است که امکان دستیابی به یک کامپیوتر از راه دور را به گونه ای فراهم می نماید که تصور می شود شما در کنار سیستم به صورت فیزیکی قرار گرفته اید (نوعی پیشرفته از Romote Desktop). با استفاده از سرویس ترمینال، می توان برنامه ای سرویس گیرنده را بر روی سرویس دهنده اجراء و بدین ترتیب کامپیوتر سرویس گیرنده به عنوان یک ترمینال ایفای وظیفه خواهد کرد (نه به عنوان یک سیستم مستقل). بدین ترتیب هزینه مربوط به عملیات و نگهداری شبکه کاهش و می توان مدیریت سرویس دهنده را از هر مکانی بر روی شبکه انجام داد.
- **Remote Installation Services (RIS):** سرویس فوق، امکان بکارگیری سیستم عامل در یک سازمان توسط مدیران سیستم را تسریع و بهبود خواهد بخشید. بدین ترتیب نیاز به ملاقات فیزیکی هر یک از کامپیوترهای سرویس گیرنده وجود نداشته و می توان از راه دور، اقدام به نصب نمود. سرویس فوق، یک عنصر انتخابی بوده و به عنوان بخشی از نسخه Windows 2003 Server است.

انواع نسخه های ویندوز سرور ۲۰۰۳

Server 2003 Web Edition

این نسخه از ویندوز سرور ۲۰۰۳ تا 2 GB حافظه RAM و در صورتی که سخت افزار شما پشتیبانی کند تا ۲ عدد CPU را به صورت متقارن (Symmetric) پشتیبانی می کند. این نسخه بیشتر در شبکه برای Web Server یا Application Server استفاده می شود و نمی توان به عنوان Domain Controller یا DHCP و یا FAX Server در نظر گرفته شود.

نکته: در اینجا مفهوم Symmetric وAsymmetric را می گوییم تا در ادامه کار اگر جایی استفاده کردیم دچار ابهام نشویم. در صورتی که در کامپیوتر خود ۲ یا تعداد بیشتری CPU داشته باشیم چه به صورت Dual Core و یا به طور کل دو CPU مجزا از هم، زمانی که دو CPU همزمان با یکدیگر کار می کنند و هر نوع دستورالعمل یا برنامه ای توسط هر یک اجرا می شود و محدودیتی در نوع دستورالعمل ها نمی باشد به این نوع CPUها متقارن یا Symmetric می گویند و در صورتی که برای هر کدام از CPUها یک سری دستورالعمل خاص تعریف شده باشد، به طور مثال یک CPU فقط دستورالعمل های سیستمی و CPU دیگر درخواستها و برنامه های کاربر را اجرا کند به این نوع پردازنده ها، نا متقارن یا Asymmetric می گویند.

Server 2003 Standard Edition

این نسخه از ویندوز سرور ۲۰۰۳ تا 4 GB حافظه RAM و تا ۴ عدد CPU را به صورت متقارن پشتیبانی می کند. این نسخه معمولا در شبکه های محلی استفاده می شود و می تواند به عنوان Web Serverو یا Application Server و یا Mail Server مورد استفاده قرار گیرد. البته این مسئله را در نظر بگیرید که مطمئنا نسخه Web Edition برای راه انداختن Web Server دارای کارایی و Performance بهتری می باشد چرا که بسیاری از سرویس هایی که در Web Edition استفاده نمی شود Stop شده اند و این مسئله سرعت سیستم را تا حد قابل توجهی بالا برده است.

Server 2003 Enterprise Edition

نسخه ۳۲ بیتی Enterprise تا 32 GB حافظه RAM و تا ۸ عدد CPU و نسخه ۶۴ بیتی آن تا 64GB حافظه RAM و تا ۸ عدد CPU را پشتیبانی می کنند. قدرت پردازش این Platform در حالت کلی بیشتر از نسخه Standard می باشد.

Server 2003 Datacenter Edition

این نسخه از ویندوز سرور ۲۰۰۳ نیز در دو نسخه ۳۲ و ۶۴ بیتی عرضه می شود. نسخه ۳۲ بیتی در حالت کلی تا 64 GB حافظه RAM و تا ۳۲ عدد CPU را به صورت متقارن پشتیبانی می کند. اما نسخه ۶۴ بتی این ویندوز تا 512 GB حافظه RAM و تا ۱۲۸ عدد CPU را به صورت متقارن پشتیبانی می کند. در جاهایی که مخواهیم حجم بسیار سنگینی را جا به جا کنیم از این نسخه استفاده می کنیم. (که باید بگویم که نسخه ۶۴بیتی این ویندوز بر روی CPUهای Itanuim اجرا می شود.

ویندوز سرور ۲۰۰۸ HPC

به همراه ویندوز سرور ۲۰۰۸، ویرایش جدیدی به نام HPC که مخفف High Performance Computing بوده و به معنای "انجام محاسبات با کارآیی بالا" می باشد، معرفی شد. در واقع HPC، نسخه بهبود یافته Windows Computer Cluster Server 2003 می باشد. این نسخه بیشتر در محافل علمی کاربرد دارد؛ به خصوص در سرور هایی که می خواهیم محاسبات علمی سنگینی را انجام دهد. یکیاز ویژگی های این ویرایش، پشتیبانیو استفاده بهینه از سخت افزارهای موازی به منظور انجام سریع تر محاسبات می باشد. در این ویرایش، Clustering به خوبی انجام می گیرد. HPC قابلیت پشتیبانی از هزاران هسته پردازشی و همچنین برخی نرم افزارهای پردازش موازی مانند LPI و MPICH2 را دارد.

ویژگیهای جدید ویندوز سرور ۲۰۰۸

قابلیت ایجاد محیط مجازی

قابلیت Hyper-v ویندوز سرور (نسل جدید تکنولوژی محیط مجازی Hypervisor-Based سرور) به شما امکان می دهد تا چند سرور با وظایف متفاوت در شبکه را توسط راه اندازی ماشین های مجازی مجزا روی یک ماشین فیزیکی واحد ادغام کرده و از این طریق از دارایی های سخت افزاری سرور خود بهترین استفاده را ببرند. همچنین شما می توانید سیستم عامل های مختلف مانند ویندوز، لینوکس و... را به صورت همزمان روی یک سرور واحد اجرا نمایید. برنامه های کاربردی هم می توانند با استفاده از تکنولوژی های دسترسی متمرکز شده به برنامه های کاربردی در ویندوز سرور ۲۰۰۸ به صورت موثری از مجازی سازی استفاده نمایند. با اجرای Terminal Services Gateway و Terminal Services RermoteAPPروی Terminal Server، شما به راحتی اجازه خواهید یافت بدون نیاز به اتصال VPN، از هر کجا به برنامه های استاندارد بر مبنای ویندوز دسترسی داشته باشید.

ساخته شده برای وب

ویندوز سرور ۲۰۰۸ به همراه IIS 7.0 به بازار عرضه می گردد که وب سروری با پلتفرمی ساده و امن برای توسعه و میزبانی مطمئن سرویس ها و برنامه های کاربردی وب می باشد. تغییر مهمی که در پلتفرم وب ویندوز (IIS 7.0) داده شده آن است که **به منظور کنترل و انعطاف بیشتر، از معماری طبقه بندی شده استفاده می کند**. همچنین IIS 7.0 از امکان مدیریت آسان و مکانیزم تشخیص و رفع عیب بسیار قدرتمندی بهره می برد که موجب کاهش اتلاف زمان و افزایش توسعه پذیری همه جانبه می گردد. IIS 7.0 به همراه NET Framework 3.0 پلتفرم جامعی برای ساخت برنامه های کاربردی که ارتباط بین کاربران و داده ها را برقرار می کنند، فراهم می آورد و آن ها را قادر می سازد اطلاعات مورد نیاز را ببینند، به اشتراک بگذارند و بر روی آن ها عملیات انجام دهند. به علاوه IIS 7.0 در یکپارچه سازی دیگر پلتفرم های وب شرکت مایکروسافت نظیر ASP.NET, Windows Communication Foundation Web Services, windows SharePoint یک نقش اساسی را ایفا می کند.

امنیت بالا

ویندوز سرور ۲۰۰۸ امن ترین ویندوز ارائه شده تاکنون می باشد. این سیستم عامل به منظور محافظت در **برابر خرابی ها** بسیار مقاوم شده است و از تکنولوژی های جدید متفاوتی برای **ممانعت از برقراری ارتباطات غیر مجاز** به شبکه، سرورها، داده ها و حسابرسی کاربران شما استفاده کرده است. سرویس Accerss Protection Network به شما کمک می کند مطمئن شوید کامپیوترهایی که جهت اتصال به شبکه شما تلاش می کنند با سیاست های امنیتی سازمان متبوع شما مطابقت دارند. ادغام تکنولوژی های مختلف و چندین مورد بهبود درActive Directory، آن را به ابزاری یکپارچه و قدرتمند برای راهکارهای شناسایی هویت و کنترل مبدل کرده است. در پایان سرویس های Read-Only Domain Controller و BitLock Drive Encryption به شما اجازه می دهند تا Active Directory را به صورت کاملا امن در محل شعبات خود راه اندازی نمایید.

انجام محاسبات با کارایی بالا (HPC)

مزایا و امکان کاهش هزینه ها در ویندوز سرور ۲۰۰۸ با توسعه آن توسط Windows HPC Server 2008 که برای محیط های با نیاز محاسباتی بالا طراحی شده است نمود بیشتری می یابد. ویندوز HPC سرور ۲۰۰۸ روی ویندوزهای سرور ۲۰۰۸ با تکنولوژی X64-bit ساخته شده است و می تواند بطور موثری با استفاده از عملکرد Out-Of-The-Box به هزاران هسته پردازشی گسترش یافته ودر نتیجه کارایی محیط HPC شما را افزایش داده وپیچیدگی آن را کاهش دهد. ویندوز HPC سرور ۲۰۰۸ با تجمیع توانایی کاربران یکپارچه وتوانا و تبدیل کامپیوترهای رومیزی به کلاسترهای بزرگ، شما را قادر به گسترش

همه جانبه می نماید و مجموعه جامعی از ابزارهای گسترش، مدیریت و نظارت را شامل می شود که گسترش، مدیریت و تجمیع با زیرساخت های موجود شما را ساده تر می کند.

سیستم عامل لینوکس LINOCS

سیستم عامل لینوکس برعکس سیستم عامل ویندوز سرور، به صورت پیش فرض خدمات و نرم افزار های شبکه ای را با خود به همراه ندارد (البته ویندوز سرور نیز به صورت پیش فرض تمام امکانات شبکه ای را نصب نمی کند ولی در خود دارا می باشد)، و لذا در لینوکس، شما بایستی خودتان نرم افزارها و سرویس های مورد نیاز را نصب نمایید. سیستم عامل های شکل گرفته بر پایه لینوکس، به دلیل پایداری و انعطاف، گزینه های خوبی برای نصب بر روی سیستم های سرور هستند.

نرم افزار های Serverتحت لینوکس

نمونه نرم افزار های مشهوری که معمولا تحت لینوکس به عنوان نرم افزار Server استفاده می شوند:

- سرور پروکسی –کش(Proxy-Cache)
- بایند(BIND)
- سرور سامانه نام دامنه (DNS)
- آپاچی (APACHER)
- سرور وب
- پست فیکس (Postfix)
- سرور پست الکترنیکی
- مای اس کیوال (MySQL)
- سرور پایگاه داده
- اسکوئید (SQUID)

ویژگی های اصلی لینوکس

- چند کاربره بودن (Multi user)
- چند وظیفه ای بودن (Multi- Tasking)
- واسط کاربر گرافیکی (X windows system)
- سرویس دهندههای شبکه (Network Server)
- پشتیبانی برنامه های کاربردی (Application Support)
- پشتیبانی (Support)
- اتصالات شبکه ای (Nertwork Connectivity)

چند کاربره بودن

سیستم عامل لینوکس می تواند به چندین کاربر، اجازه کار کردن با سیستم را بدهد و لذا برای هرکاربر حساب کاربری جداگان های را تعریف می کند. ضمنا چندین کاربرد می توانند به صورت همزمان به سیستم وارد شوند و در آن مشغول به کار شوند.

چند وظیفه ای بودن

در لینوکس این امکان وجود دارد که چندین برنامه در یک لحظه اجرا شوند؛ یعنی یک کاربر می تواند از چندین برنامه به صورت همزمان استفاده نماید.

واسط کاربر گرافیکی

کاربران مبتدی، ترجیح می دهند از طریق رابط گرافیکی از لینوکس استفاده نمایند. دو رابط گرافیکی GNOMERو KDEمتداول ترین رابط های گرافیکی بر روی این سیستم عامل می باشند.

سرویس دهندههای شبکه

سیستم عامل لینوکس برای کاربردهای شبکه توسعه یافته به طوری که می تواند به عنوان سیستم عامل سرور برای مدیریت منابع مختلف موجود روی شبکه پیکربندی شود.

پشتیبانی برنامه های کاربردی

به خاطر سازگاری لینوکس با استانداردهای صنعتی سیستم عامل، محدوده وسیعی از نرم افزارها برای لینوکس در دسترس می باشند. معمولا در سی دی نسخه های مختلف لینوکس، برنامه های کاربردی فراوانی وجود دارند که بسیاری از نیازهای عمومی کاربران را برآورده می سازند.

پشتیبانی

جامعه Open Sourceو برخی از شرکت های تولید کننده نسخه های لینوکس، از این سیستم عامل پشتیبانی دارند و اگر در کار با لینوکس دچار مشکل شدید، عملیات پشتیبانی را انجام خواهند داد.

اتصالات شبکه :

پشتیبانی از انواع مختلف واسط شبکه (سیمی و بی سیم)

مزایای لینوکس

- رایگان بودن
- قابلیت اعتماد
- منابع اطلاعاتی لینوکس در اینترنت

اجزای سیستم عامل لینوکس

سیستم عامل لینوکس دارای سه قسمت اصلی: هسته، محیط و ساختار فایل است.

هسته

هسته بخش اصلی لینوکس است و ارتباط میان سیستم عامل لینوکس ونرم افزارهای نصب شده بر روی آن با سخت افزار را برقرار می کند. به عبارت دیگر، اجرای برنامه ها و مدیریت سخت افزارها را برعهده دارد.

ساختار فایل

ساختار فایل، نحوه ذخیره شدن فایل ها بر روی دیسک سخت را تعیین می کند. در لینوکس نیز همانند ویندوز، فایل ها در داخل دایرکتوری ها قرار می گیرند و کاربران می توانند دایرکتوری ها و فایلهای مورد نظر خود را ایجاد کنند و سپس برای هر یک از آن ها مجوزهای دسترسی تعیین نمایند.

نسخه های مختلف سیستم عامل لینکوس

1. BlueCat
2. Caldera OpenLinux

3. Debian
4. Ubuntu
5. Dragon Linux
6. Mandrak
7. Red Hat
8. Slackware
9. SUSER
10.Fedora Core

منابع:

- نصب و راه اندازی شبکه، دکتر رضا رمضانی
- شبکه های محلی کامپیوتر، امین فرح بخش
- تاریخچه پیدایش شبکه، سهراب نیازی
- شبکه های محلی کامپیوتر، اکبر مومنی
- Cisco Sytems CCNA ، ترجمه و تألیف مهدیه توکلی