دانشگاه آزاداسلامی
واحدایذه

کارگاه شبکه های محلی کامپیوتر
(آموزش شبکه)

قابل استفاده دانشجویان و هنرآموزان
رشته کامپیوتر

تهیه وتنظیم :
سید اصلان حسینی
مهر ۱۳۸۶

درخت تو گر بار دانش بگیرد
به زیر آوری چرخ نیلوفری را

چکیده

استفاده از شبکه های کامپیوتری در چندین سال اخیر رشد فراوانی کرده وسازمانها وموسسات اقدام به برپایی شبکه نموده اند . هر شبکه کامپیوتری باید با توجه به شرایط وسیاست های هر سازمان ، طراحی وپیاده سازی گردد. در واقع شبکه های کامپیوتری زیر ساخت های لازم را برای به اشتراک گذاشتن منابع در سازمان فراهم می آورند؛در صورتیکه این زیر ساختها به درستی طراحی نشوند، در زمان استفاده از شبکه مشکلات متفاوتی پیش آمده و باید هزینه های زیادی به منظور نگهداری شبکه وتطبیق آن با خواسته های مورد نظر صرف شود. در زمان طراحی یک شبکه سوالات متعددی مطرح می شود:برای طراحی یک شبکه باید از کجاشروع کرد؟چه پارامترهایی را باید در نظر گرفت ؟هدف از برپاسازی شبکه چیست ؟ انتظارکاربران از شبکه چیست ؟ آیا شبکه موجود ارتقاء می باید ویا یک شبکه از ابتدا طراحی میشود؟چه سرویس ها و خدماتی برروی شبکه ارائه خواهد شد؟

بطور کلی قبل از طراحی فیزیکی یک شبکه کامپیوتری ، ابتدا باید خواسته ها شناسایی وتحلیل شوند، مثلا در یک کتابخانه چرا قصد ایجاد یک شبکه را داریم واین شبکه باید چه سرویس ها وخدماتی را ارائه نماید؛ برای تامین سرویس ها وخدمات مورد نظر اکثریت کاربران ، چه اقداماتی باید انجام داد ؛ مسائلی چون پروتکل مورد نظر برای استفاده از شبکه ، سرعت شبکه واز همه مهمتر مسائل امنیتی شبکه ، هریک از اینها باید به دقت مورد بررسی قرار گیرد. سعی شده است پس از ارائه تعاریف اولیه ، مطالبی پیرامون کاربردهای عملی آن نیز ارائه شود تا در تصمیم گیری بهتر یاری کند.

سخت افزار شبکه

و همبندی شبکه های کامپیوتری

شبکه کامپیوتری چیست ؟

اساسا یک شبکه کامپیوتری شامل دو یا بیش از دو کامپیوتر وابزارهای جانبی مثل چاپگرها، اسکنرها ومانند اینها هستند کـه بطـور مـستقیم بمنظور استفاده مشترک از سخت افزار ونرم افزار، منابع اطلاعاتی ابزارهای متصل ایجاده شده است توجه داشته باشید که به تمامی تجهیزات سخت افزاری ونرم افزاری موجود در شبکه منبع۱(Source) گویند.

در این تشریک مساعی با توجه به نوع پیکربندی کامپیوتر ، هر کامپیوتر کاربر می تواند در آن واحد منابع خود را اعم از ابزارهـا وداده هـا بـا کامپیوترهای دیگر همزمان بهره ببرد.

" دلایل استفاده از شبکه را می توان موارد ذیل عنوان کرد۲" :

۱ - استفاده مشترک از منابع :

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

۲ - کاهش هزینه :متمرکز نمودن منابع واستفاده مشترک از آنها وپرهیز از پخش آنها در واحدهای مختلف واستفاده اختصاصی هر کـاربر در یک سازمان کاهش هزینه را در پی خواهدداشت .

۳ - قابلیت اطمینان :

این ویژگی در شبکه ها بوجود سرویس دهنده های پشتیبان در شبکه اشاره می کند ، یعنی به ایـن معنـا کـه مـی تـوان از منـابع گونـاگون اطلاعاتی وسیستم ها در شبکه نسخه های دوم وپشتیبان تهیه کرد ودر صورت عدم دسترسی به یک از منابع اطلاعاتی در شـبکه " بعلـت از کارافتادن سیستم " از نسخه های پشتیبان استفاده کرد. پشتیبان از سرویس دهنده ها در شبکه کارآیی،، فعالیت وآمادگی دایمی سیـستم 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 ؛ یعنـی بـدون محـدودیت جغرافیـایی تبـادل 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 وتبدیل به یک شبکه بزرگتر شود. در اینجا هزینه توسعه سیستم هزینه امکانات وتجهیزات مورد نیاز برای گسترش شبکه مد نظر است.

۶ - ارتباطات:

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

در طراحی شبکه مواردی که قبل از راه اندازی شبکه باید مد نظر قرار دهید شامل موارد ذیل هستند:

۱ - اندازه سازمان ۲ - سطح امنیت ۳ - نوع فعالیت ۴ - سطح مدیریت ۵ - مقدار ترافیک ۶ – بودجه

مفهوم گره " Node" وایستگاههای کاری [Work Stations] :

" هرگاه شما کامپیوتری را به شبکه اضافه می کنید ، این کامپیوتر به یک ایستگاه کاری یا گره تبدیل می شود.

یک ایستگاه کاری ؛ کامپیوتری است که به شبکه الصاق شده است و در واقع اصطلاح ایستگاه کاری روش دیگری است برای اینکه بگوییم یک کامپیوتر متصل به شبکه است. یک گره چگونگی وارتباط شبکه یا ایستگاه کاری ویا هر نوع ابزار دیگری است که به شبکه متصل است وبطور ساده تر هر چه را که به شبکه متصل والحاق شده است یک گره گویند".

برای شبکه جایگاه وآدرس یک ایستگاه کاری مترادف با هویت گره اش است.

پروتکل

پروتکل در شبکه های کامپیوتری به مجموعه قوانینی اطلاق می گردد که نحوه ارتباطات را قانونمند می نماید. نقش پروتکل در کامپیوتر نظیر نقش زبان برای انسان است . برای مطالعه یک کتاب نوشته شده به فارسی می بایست خواننده شناخت مناسبی از زبان فارسی را داشته باشد. بمنظور ارتباط موفقیت آمیز دو دستگاه در شبکه می بایست هر دو دستگاه از یک پروتکل مشابه استفاده نمایند.

اصطلاحات اترنت

شبکه های اترنت از مجموعه قوانین محدودی بمنظور قانونمند کردن عملیات اساسی خود استفاده می نمایند. بمنظور شناخت مناسب قوانین موجود لازم است که با برخی از اصطلاحات مربوطه در این زمینه بیشتر آشنا شویم :

- Medium (محیط انتقال) . دستگاههای اترنت از طریق یک محیط انتقال به یکدیگر متصل می گردند.
- Segment (سگمنت) . به یک محیط انتقال به اشتراک گذاشته شده منفرد، " سگمنت " می گویند.
- Node (گره) . دستگاههای متصل شده به یک Segment را گره و یا " ایستگاه " می گویند.
- Frame (فریم) . به یک بلاک اطلاعات که گره ها از طریق ارسال آنها با یکدیگر مرتبط می گردند، اطلاق می گردد

فریم ها مشابه جملات در زبانهای طبیعی (فارسی، انگلیسی ...) می باشند. در هر زبان طبیعی برای ایجاد جملات، مجموعه قوانینی وجود دارد مثلا" یک جمله می بایست دارای موضوع و مفهوم باشد. پروتکل های اترنت مجموعه قوانین لازم برای ایجاد فریم ها را مشخص خواهند کرد .اندازه یک فریم محدود بوده (دارای یک حداقل و یک حداکثر) و مجموعه ای از اطلاعات ضروری و مورد نیار می بایست در فریم وجود داشته باشد. مثلا" یک فریم می بایست دارای آدرس های مبداء و مقصد باشد. آدرس های فوق هویت فرستنده و دریافت کننده پیام را مشخص خواهد کرد. آدرس بصورت کاملا" اختصاصی یک گره را مشخص می نماید.(نظیر نام یک شخص که بیانگر یک شخص خاص است) . دو دستگاه متفاوت اترنت نمی توانند دارای آدرس های یکسانی باشند.

یک سیگنال اترنت بر روی محیط انتقال به هر یک از گره های متصل شده در محیط انتقال خواهد رسید. بنابراین مشخص شدن آدرس مقصد، بمنظوردریافت پیام نقشی حیاتی دارد. مثلا" در صورتیکه کامپیوتر B (شکل بالا) اطلاعاتی را برای چاپگر C ارسال می دارد کامپیوترهای A و D نیز فریم را دریافت و آن را بررسی خواهند کرد. هر ایستگاه زمانیکه فریم را دریافت می دارد، آدرس آن را بررسی تا مطمئن گردد که پیام برای وی ارسال شده است یا خیر؟ در صورتیکه پیام برای ایستگاه مورد نظر ارسال نشده باشد، ایستگاه فریم را بدون بررسی محتویات آن کنار خواهد گذاشت (عدم استفاده).

یکی از نکات قابل توجه در رابطه با آدرس دهی اترنت، پیاده سازی یک آدرس Broadcast است . زمانیکه آدرس مقصد یک فریم از نوع Broadcast باشد، تمام گره های موجود در شبکه آن را دریافت و پردازش خواهند کرد.

CSMA/CD

تکنولوژی CSMA/CD (detection carrier-sense multiple access with collision) مسئولیت تشریح و تنظیم نحوه ارتباط گره ها با یکدیگررا برعهده دارد. با اینکه واژه فوق پیچیده بنظر می آید ولی با تقسیم نمودن واژه فوق به بخش های کوچکتر، می توان با نقش هر یک از آنها سریعتر آشنا گردید.بمنظور شناخت تکنولوژی فوق مثال زیر را در نظر بگیرید :

فرض کنید سگمنت اترنت، مشابه یک میز ناهارخوری باشد. چندین نفر (نظیر گره) دور تا دور میز نشسته و به گفتگو مشغول می باشند. واژه access multiple (دستیابی چندگانه) بدین مفهوم است که : زمانیکه یک ایستگاه اترنت اطلاعاتی را ارسال می دارد تمام ایستگاههای دیگر موجود (متصل) در محیط انتقال ، نیز از انتقال اطلاعات آگاه خواهند شد.(.نظیر صحبت کردن یک نفر در میز ناهار خوری و گوش دادن سایرین). فرض کنید که شما نیز بر روی یکی از صندلی های میز ناهار خوری نشسته و قصد حرف زدن را داشته باشید، در همان زمان فرد دیگری در حال سخن گفتن است در این حالت می بایست شما در انتظار اتمام سخنان گوینده باشید. در پروتکل اترنت وضعیت فوق carrier sense نامیده می شود.قبل از اینکه ایستگاهی قادر به ارسال اطلاعات باشد می بایست گوش خود را بر روی محیط انتقال گذاشته و بررسی نماید که آیا محیط انتقال آزاد است ؟ در صورتیکه صدائی از محیط انتقال به گوش ایستگاه متقاضی ارسال اطلاعات نرسد، ایستگاه مورد نظر قادر به استفاده از محیط انتقال و ارسال اطلاعات خواهد بود.

Carrier-sense multiple access شروع یک گفتگو را قانونمند و تنظیم می نماید ولی در این رابطه یک نکته دیگر وجود دارد که می بایست برای آن نیز راهکاری اتخاذ شود.فرض کنید در مثال میز ناهار خوری در یک لحظه سکوتی حاکم شود و دو نفر نیز قصد حرف زدن را داشته باشند.در چنین حالتی در یک لحظه سکوت موجود توسط دو نفر تشخیص و بلافاصله هر دو تقریبا" در یک زمان یکسان شروع به حرف زدن می نمایند.چه اتفاقی خواهد افتاد ؟ در اترنت پدیده فوق را تصادم (Collision) می گویند و زمانی اتفاق خواهد افتاد که دو ایستگاه قصد استفاده از محیط انتقال و ارسال اطلاعات را بصورت همزمان داشته باشند. در گفتگوی انسان ها ، مشکل فوق را می توان بصورت کاملا" دوستانه حل نمود. ما سکوت خواهیم کرد تا این شانس به سایرین برای حرف زدن داده شود.همانگونه که در زمان حرف زدن من، دیگران این فرصت را برای من ایجاد کرده بودند! ایستگاههای اترنت زمانیکه قصد ارسال اطلاعات را داشته باشند، به محیط انتقال گوش فرا داده تا به این اطمینان برسند که تنها ایستگاه موجود برای ارسال اطلاعات می باشند. در صورتیکه ایستگاههای ارسال کننده اطلاعات متوجه نقص در ارسال اطلاعات خود گردند ،از بروز یک تصادم در محیط انتقال آگاه خواهند گردید. در زمان بروز تصادم ، هر یک از ایستگاههای مربوطه به مدت زمانی کاملا" تصادفی در حالت انتظار قرار گرفته و پس از اتمام زمان انتظار می بایست برای ارسال اطلاعات شرط آزاد بودن محیط انتقال را بررسی نمایند! توقف تصادفی و تلاش مجدد یکی از مهمترین بخش های پروتکل است .

پروتکل CSMA/CD امکان ارسال اطلاعات برای صرفا" یک دستگاه را در هر لحظه فراهم می نماید، بنابراین محدودیت هائی از لحاظ تعداد دستگاههائی که می توانند بر روی یک شبکه مجزا وجود داشته باشند، نیز بوجود خواهد آمد. با اتصال دستگاه های متعدد (فراوان) بر روی یک سگمنت مشترک، شانس استفاده از محیط انتقال برای هر یک از دستگاه های موجود بر روی سگمنت کاهش پیدا خواهد کرد. در این حالت هر دستگاه بمنظور ارسال اطلاعات می بایست مدت زمان زیادی را در انتظار سپری نماید .

تکرارکننده (Repeater)

اولین محیط انتقال استفاده شده در شبکه های اترنت کابل های مسی کواکسیال بود که Thicknet (ضخیم) نامیده می شوند. حداکثر طول یک کابل ضخیم ۵۰۰ متر است . در یک ساختمان بزرگ ، کابل ۵۰۰ متری جوابگوی تمامی دستگاه های شبکه نخواهد بود. تکرار کننده ها با هدف حل مشکل فوق، ارائه شده اند. . تکرارکننده ها ، سگمنت های متفاوت یک شبکه اترنت را به یکدیگر متصل می کنند. در این حالت تکرارکننده سیگنال ورودی خود را از یک سگمنت اخذ و با تقویت سیگنال آن را برای سگمنت بعدی ارسال خواهد کرد. بدین تزتیب با استفاده از چندین تکرار کننده و اتصال کابل های مربوطه توسط آنان ، می توان قطر یک شبکه را افزایش داد. (قطر شبکه به حداکثر مسافت موجود بین دو دستگاه متمایز در شبکه اطلاق می گردد)

Bridges و سگمنت

شبکه های اترنت همزمان با رشد (بزرگ شدن) دچار مشکل تراکم می گردند. در صورتیکه تعداد زیادی ایستگاه به یک سگمنت متصل گردند، هر یک دارای ترافیک خاص خود خواهند بود . در شرایط فوق ، ایستگاههای متعددی قصد ارسال اطلاعات را دارند ولی با توجه به ماهیت این نوع از شبکه ها در هر لحظه یک ایستگاه شانس و فرصت استفاده از محیط انتقال را پیدا خواهد کرد. در چنین وضعیتی تعداد تصادم در شبکه افزایش یافته و عملا" کارآئی شبکه افت خواهد کرد. یکی از راه حل های موجود بمنظور برطرف نمودن مشکل تراکم در شبکه تقسیم یک سگمنت به چندین سگمنت است . با این کار برای تصادم هائی که در شبکه بروز خواهد کرد، دامنه وسیعتری ایجاد می گردد.راه حل فوق باعث بروز یک مشکل دیگر می گردد: سگمنت ها قادر به اشتراک اطلاعات با یکدیگر نخواهند بود.

بمنظور حل مشکل فوق، Bridges در شبکه اترنت پیاده سازی شده است . Bridge دو و یا چندین سگمنت را به یکدیگر متصل خواهد کرد. بدین ترتیب دستگاه فوق باعث افزایش قطر شبکه خواهد شد. عملکرد Bridge از بعد افزایش قطر شبکه نظیر تکرارکننده است ، با این نفاوت که Bridge قادر به ایجاد نظم در ترافیک شبکه نیز خواهد بود . Bridge نظیر سایر دستگاههای موجود در شبکه قادر به ارسال و دریافت اطلاعات بوده ولی عملکرد آنها دقیقا" مشابه یک ایستگاه نمی باشد. Bridge قادر به ایجاد ترافیکی که خود سرچشمه آن خواهد بود، نیست (نظیر تکرارکننده) .Bridge صرفا" چیزی را که از سایر ایستگاهها می شنود ، منعکس می نماید. (Bridge قادر به ایجا د یک نوع فریم خاص اترنت بمنظور ایجاد ارنباط با سایر Bridge ها می باشند)

همانگونه که قبلا" اشاره گردید هر ایستگاه موجود در شبکه تمام فریم های ارسال شده بر روی محیط انتقال را دریافت می نماید.(صرفنظر ازاینکه مقصد فریم همان ایستگاه باشد و یا نباشد.) Bridge با تاکید بر ویژگی فوق سعی بر تنظیم ترافیک بین سگمنت ها دارد.

همانگونه که می دانید Bridge دو سگمنت را به یکدیگر متصل نموده است . در صورتیکه ایستگاه A و یا B قصد ارسال اطلاعات را داشته باشند Bridge نیز فریم های اطلاعاتی را دریافت خواهد کرد. نحوه برخورد Bridge با فریم های اطلاعاتی دریافت شده به چه صورت است؟ آیا قادر به ارسال اتوماتیک فریم ها برای سگمنت دوم می باشد؟ یکی ازاهداف استفاده از Bridge کاهش ترافیک های غیرضروری در هر سگمنت است . در این راستا، آدرس مقصد فریم ، قبل از هر گونه عملیات بر روی آن، بررسی خواهد شد. در صورتیکه آدرس مقصد، ایستگاههای A و یا B باشد نیازی به ارسال فریم برای سگمنت شماره دو وجود نخواهد داشت . در این حالت Bridge

عملیات خاصی را انجام نخواهد داد. نحوه برخورد Bridge با فریم فوق مشابه فیلتر نمودن است . درصورتیکه آدرس مقصد فریم یکی از ایستگاههای C و یا D باشد و یا فریم مورد نظر دارای یک آدرس از نوع Broadcast باشد ، Bridge فریم فوق را برای سگمنت شماره دو ارسال خواهد کرد. با ارسال و هدایت فریم اطلاعاتی توسط Bridge امکان ارتباط چهار دستگاه موجود در شبکه فراهم می گردد. با توجه به مکانیزم فیلتر نمودن فریم ها توسط Bridge ، این امکان بوجود خواهد آمد که ایستگاه A اطلاعاتی را برای ایستگاه B ارسال و در همان لحظه نیز ایستگاه C اطلاعاتی را برای ایستگاه D ارسال نماید.بدین ترتیب امکان برقراری دو ارتباط بصورت همزمان بوجود آمده است .

روترها : سگمنت های منطقی

با استفاده از Bridge امکان ارتباط همزمان بین ایستگاههای موجود در چندین سگمنت فراهم می گردد. Bridge در رابطه با ترافیک موجود در یک سگمنت عملیات خاصی را انجام نمی دهد. یکی از ویژگی های مهم Bridge ارسالی فریم های اطلاعاتی از نوع Broadcast برای تمام سگمنت های متصل شده به یکدیگر است. همزمان با رشد شبکه و گسترش سگمنت ها، ویژگی فوق می تواند سبب بروز مسائلی در شبکه گردد. زمانیکه تعداد زیادی از ایستگاه های موجود در شبکه های مبتنی بر Bridge ، فریم های Broadcast را ارسال می نمایند، تراکم اطلاعاتی بوجود آمده بمراتب بیشتر از زمانی خواهد بود که تمامی دستگاهها در یک سگمنت قرار گرفته باشند.

روتر یکی از دستگاههای پیشرفته در شبکه بوده که قادر به تقسیم یک شبکه به چندین شبکه منطقی مجزا است . روتر ها یک محدوده منطقی برای هر شبکه ایجاد می نمایند. روترها بر اساس پروتکل هائی که مستقل از تکنولوژی خاص در یک شبکه است، فعالیت می نمایند. ویژگی فوق این امکان را برای روتر فراهم خواهد کرد که چندین شبکه با تکنولوژی های متفاوت را به یکدیگر مرتبط نماید. استفاده از روتر در شبکه های محلی و گسترده امکان پذیراست .

همزمان با مطرح شدن سوئیچ های اترنت مسئله Full-duplex نیز مطرح گردید. Full-dulex یک اصطلاح ارتباطی است که نشاندهنده قابلیت ارسال و دریافت اطلاعات بصورت همزمان است . در شبکه های اترنت اولیه وضعیت ارسال و دریافت اطلاعات بصورت یکطرفه (half-duplex) بود.در شبکه های مبتنی بر سوئیچ، ایستگاهها صرفا" با سوئیچ ارتباط برقرار کرده و قادر به ارتباط مستقیم با یکدیگر نمی باشند. در این نوع شبکه ها از کابل های بهم تابیده و فیبر نوری استفاده و سوئیچ مربوطه دارای کانکنورهای لازم در این خصوص می باشند.. شبکه های مبتنی بر سوئیچ عاری از تصادم بوده و همزمان با ارسال اطلاعات توسط یک ایستگاه به سوئیچ ، امکان ارسال اطلاعات توسط سوئیچ برای ایستگاه دیگر نیز فراهم خواهد شد.

تکنولوژی های متفاوت شبکه

متداولترین مدل موجود در شبکه های کامپیوتری(رویکرد دیگری از اترنت) توسط شرکت IBM و با نام Token ring عرضه گردید. در شبکه های اترنت بمنظور دستیابی از محیط انتقال از فواصل خالی (Gap) تصادفی در زمان انتقال فریم ها استفاده می گردد. شبکه های Token ring از یک روش پیوسته در این راستا استفاده می نمایند. در شبکه های فوق ، ایستگاه ها از طریق یک حلقه منطقی به یکدیگر متصل می گردند. فریم ها صرفا" در یک جهت حرکت و پس از طی طول حلقه ، فریم کنار گذاشته خواهد شد. روش دستیابی به محیط انتقال برای ارسال اطلاعات تابع CSMA/CD نخواهد بود و از روش passing Token استفاده می گردد. در روش فوق در ابتدا یک Token (نوع خاصی از یک فریم اطلاعاتی) ایجاد می گردد . Token فوق در طول حلقه می چرخد . زمانیکه یک ایستگاه قصد ارسال اطلاعات را داشته باشد، می بایست Token را در اختیار گرفته و فریم اطلاعاتی خود را بر روی محیط انتقال ارسال دارد. زمانیکه فریم ارسال شده مجددا" به ایستگاه ارسال کننده برگشت داده شد (طی نمودن مسیر حلقه)، ایستگاه فریم خود را حذف و یک

Token جدید را ایجاد وآن را بر روی حلقه قرار خواهد داد. در اختیار گرفتن Token شرط لازم برا ی ارسال اطلاعات است . سرعت ارسال اطلاعات در این نوع شبکه ها چهار تا شانزده مگابیت در ثانیه است .

شبکه

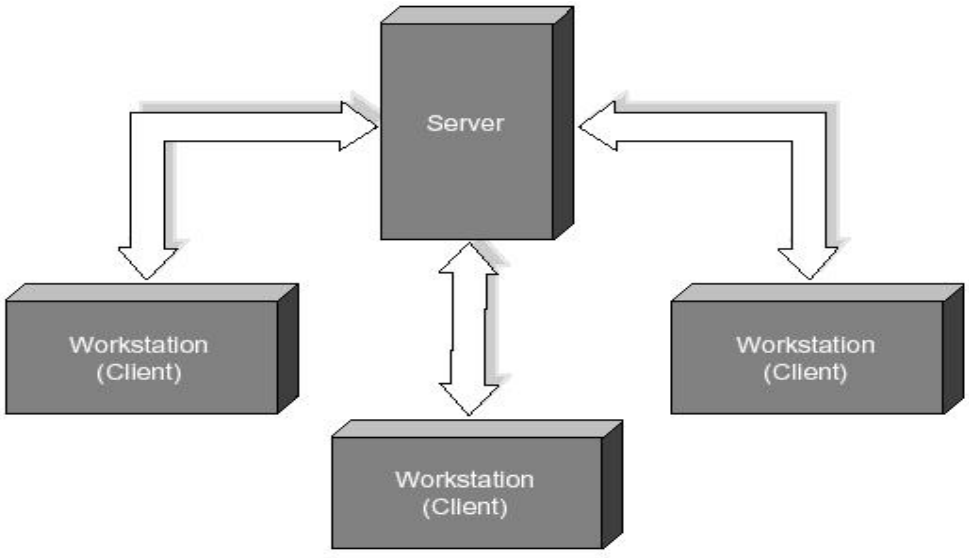
یک شبکه شامل مجموعه ای از دستگاهها (کامپیوتر ، چاپگر و ...) بوده که با استفاده از یک روش ارتباطی (کابل ، امواج رادیوئی ، ماهواره) و بمنظور اشتراک منابع فیزیکی (چاپگر) و اشتراک منابع منطقی (فایل) به یکدیگر متصل می گردند. شبکه ها می توانند با یکدیگر نیز مرتبط شده و شامل زیر شبکه هائی باشند.

تفسیم بندی شبکه ها

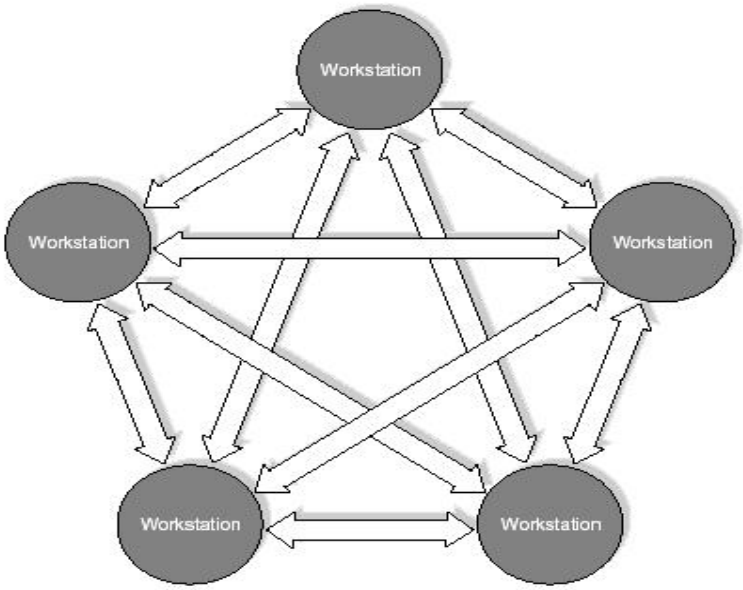
.شبکه های کامپیوتری را بر اساس مولفه های متفاوتی تقسیم بندی می نمایند. در ادامه به برخی از متداولترین تقسیم بندی های موجود اشاره می گردد .

- تقسیم بندی بر اساس نوع وظایف . کامپیوترهای موجود در شبکه را با توجه به نوع وظایف مربوطه به دو گروه عمده : سرویس دهندگان (Servers) و یا سرویس گیرندگان (Clients) تقسیم می نمایند. کامپیوترهائی در شبکه که برای سایر کامپیوترها سرویس ها و خدماتی را ارائه می نمایند ، سرویس دهنده نامیده می گردند. کامپیوترهائی که از خدمات و سرویس های ارائه شده توسط سرویس دهندگان استفاده می کنند ، سرویس گیرنده نامیده می شوند .

در شبکه های Client-Server ، یک کامپیوتر در شبکه نمی تواند هم بعنوان سرویس دهنده و هم بعنوان سرویس گیرنده ، ایفای وظیفه نماید.



در شبکه های Peer-To-Peer ، یک کامپیوتر می تواند هم بصورت سرویس دهنده و هم بصورت سرویس گیرنده ایفای وظیفه نماید.



یک شبکه LAN در ساده ترین حالت از اجزای زیر تشکیل شده است :

- دو کامپیوتر شخصی . یک شبکه می تواند شامل چند صد کامپیوتر باشد. حداقل یکی از کامپیوترها می بایست بعنوان سرویس دهنده مشخص گردد. (در صورتیکه شبکه از نوع Client-Server باشد). سرویس دهنده، کامپیوتری است که هسته اساسی سیستم عامل بر روی آن نصب خواهد شد.

- یک عدد کارت شبکه (NIC) برای هر دستگاه. کارت شبکه نظیر کارت هائی است که برای مودم و صدا در کامپیوتر استفاده می گردد. کارت شبکه مسئول دریافت ، انتقال ، سازماندهی و ذخیره سازی موقت اطلاعات در طول شبکه است . بمنظور انجام وظایف فوق کارت های شبکه دارای پردازنده ، حافظه و گذرگاه اختصاصی خود هستند.

● **تقسیم بندی بر اساس توپولوژی .** الگوی هندسی استفاده شده جهت اتصال کامپیوترها ، توپولوژی نامیده می شود. توپولوژی انتخاب شده برای پیاده سازی شبکه ها، عاملی مهم در جهت کشف و برطرف نمودن خطاء در شبکه خواهد بود. انتخاب یک توپولوژی خاص نمی تواند بدون ارتباط با محیط انتقال و روش های استفاده از خط مطرح گردد. نوع توپولوژی انتخابی جهت اتصال کامپیوترها به یکدیگر ، مستقیما" بر نوع محیط انتقال و روش های استفاده از خط تاثیر می گذارد. با توجه به تاثیر مستقیم توپولوژی انتخابی در نوع کابل کشی و هزینه های مربوط به آن ، می بایست با دقت و تامل به انتخاب توپولوژی یک شبکه همت گماشت . عوامل مختلفی جهت انتخاب یک توپولوژی بهینه مطرح می شود. مهمترین این عوامل بشرح ذیل است :

- هزینه . هر نوع محیط انتقال که برای شبکه LAN انتخاب گردد، در نهایت می بایست عملیات نصب شبکه در یک ساختمان پیاده سازی گردد. عملیات فوق فرآیندی طولانی جهت نصب کانال های مربوطه به کابل ها و محل عبور کابل ها در ساختمان است . در حالت ایده آل کابل کشی و ایجاد کانال های مربوطه می بایست قبل از تصرف و بکارگیری ساختمان انجام گرفته باشد. بهرحال می بایست هزینه نصب شبکه بهینه گردد.

- انعطاف پذیری . یکی از مزایای شبکه های LAN ، توانائی پردازش داده ها و گستردگی و توزیع گره ها در یک محیط است . بدین ترتیب توان محاسباتی سیستم و منابع موجود در اختیار تمام استفاده کنندگان قرار خواهد گرفت . در ادارات همه چیز تغییر خواهد کرد.(لوازم اداری، اتاقها و ...) . توپولوژی انتخابی می بایست بسادگی امکان تغییر پیکربندی در شبکه را فراهم نماید. مثلا" ایستگاهی را از نقطه ای به نقطه دیگر انتقال و یا قادر به ایجاد یک ایستگاه جدید در شبکه باشیم .

مدل های شبکه:

در یک شبکه ، یک کامپیوتر می تواند هم سرویس دهنده وهم سرویس گیرنده باشد. یک سرویس دهنده (Server) کامپیوتری است که فایل های اشتراکی وهمچنین سیستم عامل شبکه که مدیریت عملیات شبکه را بعهده دارد - را نگهداری می کند.

برای آنکه سرویس گیرنده " Client" بتواند به سرویس دهنده دسترسی پیدا کند ، ابتدا سرویس گیرنده باید اطلاعات مورد نیازش را از سرویس دهنده تقاضا کند. سپس سرویس دهنده اطلاعات در خواست شده را به سرویس گیرنده ارسال خواهد کرد.

سه مدل از شبکه هایی که مورد استفاده قرار می گیرند ، عبارتند از :

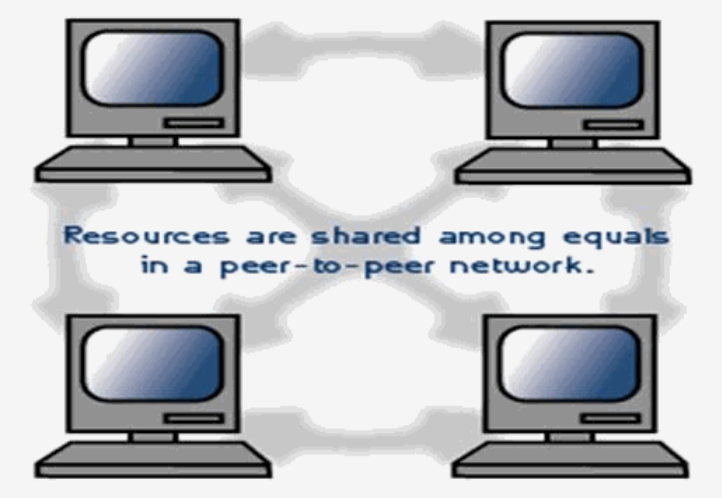
۱ - شبکه نظیر به نظیر " Peer- to- Peer "

۲ - شبکه مبتنی بر سرویس دهنده " Server- Based "

۳ - شبکه سرویس دهنده / سرویس گیرنده " Client Server"

مدل شبکه نظیر به نظیر:

در این شبکه ایستگاه ویژه ای جهت نگهداری فایل های اشتراکی وسیستم عامل شبکه وجود ندارد. هر ایستگاه می تواند به منابع سایر ایستگاه ها در شبکه دسترسی پیدا کند. هر ایستگاه خاص می تواند هم بعنوان Server وهم بعنوان Client عمل کند. در این مدل هر کاربر خود مسئولیت مدیریت وارتقاء دادن نرم افزارهای ایستگاه خود را بعهده دارد. از آنجایی که یک ایستگاه مرکزی برای مدیریت عملیات شبکه وجود ندارد ، این مدل برای شبکه ای با کمتر از ۱۰ ایستگاه بکار می رود .

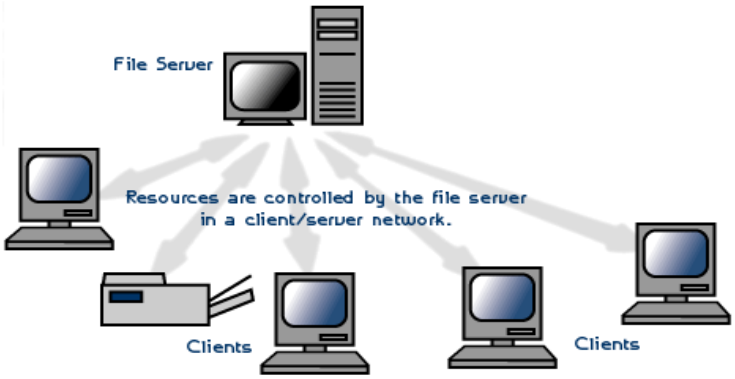


مدل شبکه مبتنی بر سرویس دهنده :

در این مدل شبکه ، یک کامپیوتر بعنوان سرویس دهنده کلیه فایل ها ونرم افزارهای اشتراکی نظیر واژه پرداز ها، کامپایلرها ، بانک های اطلاعاتی وسیستم عامل شبکه را در خود نگهداری می کند. یک کاربر می تواند به سرویس دهنده دسترسی پیدا کرده وفایل های اشتراکی را از روی آن به ایستگاه خود منتقل کند

مدل سرویس دهنده / سرویس گیرنده :

در این مدل یک ایستگاه در خواست انجام کارش را به سرویس دهنده ارائه می دهد وسرویس دهنده پس از اجـرای وظیفـه محولـه ، نتـایج حاصل را به ایستگاه در خواست کننده عودت می دهد. در این مدل حجم اطلاعات مبادله شده شبکه ، در مقایسه با مدل مبتنی بر سـرویس دهنده کمتر است واین مدل دارای کارایی بالاتری می باشد.



هر شبکه اساسا از سه بخش ذیل تشکیل می شود:

ابزارهایی که به پیکربندی اصلی شبکه متصل می شوند بعنوان مثال : کامپیوتر ها ، چاپگرها، هاب ها " Hubs " سیم ها ، کابـل هـا وسـایر رسانه هایی که برای اتصال ابزارهای شبکه استفاده می شوند.

سازگار کننده ها [Adaptor] :

که بعنوان اتصال کابل ها به کامپیوتر هستند . اهمیت آنها در این است که بدون وجود آنها شبکه تنها شـامل چنـد کـامپیوتر بـدون ارتبـاط موازی است که قادر به سهیم شدن منابع یکدیگر نیستند . عملکرد سازگارکننده در این است که به دریافت وترجمه سیگنال ها ی درون داد از شبکه از جانب یک ایستگاه کاری وترجمه وارسال برون داد به کل شبکه می پردازد.

اجزا ءشبکه :

اجزا اصلی یک شبکه کامپیوتری عبارتند از :

۱ - کارت شبکه : [NIC- Network Interface Card] :

برای استفاده از شبکه وبرقراری ارتباط بین کامپیوتر ها از کارت شبکه ای استفاده می شود که در داخل یکی از شیارهای برد اصلی کـامپیوتر های شبکه " اعم از سرویس دهنده وگیرنده " بصورت سخت افزاری وبرای کنترل ارسال ودریافت داده نصب می گردد.

۲ - رسانه انتقال [Transmission Medium]:

رسانه انتقال کامپیوتر ها را به یکدیگر متصل کرده وموجب برقراری ارتباط بین کامپیوتر های یک شبکه می شود . برخی از متداولترین رسانه های انتقال عبارتند از : کابل زوج سیم بهم تابیـده " Twisted- Pair "، کابـل کواکـسیال " Coaxial" وکابـل فیبـر نـوری " Fiber-Optic" .

سیستم عامل شبکه [NOS- Operating System Network] :

سیستم عامل شبکه برروی سرویس دهنده اجرا می شود و سرویس های مختلفی مانند: اجـازه ورود بـه سیـستم "Login" ، رمـز عبـور "Password" ، چاپ فایل ها " Printfiles" ، مدیریت شبکه " Net work management " را در اختیـار کـاربران مـی گـذارد.

انواع شبکه از لحاظ جغرافیایی:

نوع شبکه توسط فاصله بین کامپیوتر های تشکیل دهنده آن شبکه مشخص می شود:

- تقسیم بندی بر اساس حوزه جغرافی تحت پوشش . شبکه های کامپیوتری با توجه به حوزه جغرافیائی تحت پوشش به سه گروه تقسیم می گردند :

- شبکه های محلی (کوچک) LAN
- شبکه های متوسط MAN
- شبکه های گسترده WAN

شبکه های LAN . حوزه جغرافیائی که توسط این نوع از شبکه ها پوشش داده می شود ، یک محیط کوچک نظیر یـک سـاختمان اداری است . این نوع از شبکه ها دارای ویژگی های زیر می باشند :

- توانائی ارسال اطلاعات با سرعت بالا
- محدودیت فاصله
- قابلیت استفاده از محیط مخابراتی ارزان نظیر خطوط تلفن بمنظور ارسال اطلاعات
- نرخ پایین خطاء در ارسال اطلاعات با توجه به محدود بودن فاصله

شبکه های MAN . حوزه جغرافیائی که توسط این نوع شبکه ها پوشش داده می شود ، در حد و اندازه یک شهر و یـا شهرسـتان اسـت . ویژگی های این نوع از شبکه ها بشرح زیر است :

- پیچیدگی بیشتر نسبت به شبکه های محلی
- قابلیت ارسال تصاویر و صدا
- قابلیت ایجاد ارتباط بین چندین شبکه

شبکه های WAN . حوزه جغرافیائی که توسط این نوع شبکه ها پوشش داده می شود ، در حد و اندازه کشور و قاره است . ویژگـی ایـن نوع شبکه ها بشرح زیر است :

- قابلیت ارسال اطلاعات بین کشورها و قاره ها
- قابلیت ایجاد ارتباط بین شبکه های LAN
- سرعت پایین ارسال اطلاعات نسبت به شبکه های LAN
- نرخ خطای بالا با توجه به گستردگی محدوده تحت پوشش

شبکه محلی [LAN= Local Area Network] :

ارتباط واتصال بیش از دو یا چند رایانه در فضای محدود یک سازمان از طریق کابل شبکه وپروتکل بین رایانـه هـا وبـا مـدیریت نـرم افـزاری موسوم به سیستم عامل شبکه را شبکه محلی گویند. کامپیوتر سرویس گیرنده باید از طریق کامپیوتر سرویس دهنده به اطلاعات وامکانات به

اشتراک گذاشته دسترسی یابند. همچنین ارسال ودریافت پیام به یکدیگر از طریق رایانه سرویس دهنده انجام می گیرد. از خصوصیات شبکه های محلی می توان به موارد ذیل اشاره کرد:

۱ - اساسا در محیط های کوچک کاری قابل اجرا وپیاده سازی می باشند.

۲ - از سرعت نسبتا بالایی برخوردارند.

۳ - دارای یک ارتباط دایمی بین رایانه ها از طریق کابل شبکه می باشند.

اجزای یک شبکه محلی عبارتند از :

الف - سرویس دهنده ب - سرویس گیرنده ج - پروتکل د- کارت واسطه شبکه ط - سیستم ارتباط دهنده

شبکه گسترده [WAN = Wide Area Network]:

اتصال شبکه های محلی از طریق خطوط تلفنی ، کابل های ارتباطی ماهواره ویا دیگر سیستم هایی مخابراتی چون خطوط استیجاری در یک منطقه بزرگتر را شبکه گسترده گویند. در این شبکه کاربران یا رایانه ها از مسافت های دور واز طریق خطوط مخابراتی به یکدیگر متصل می شوند. کاربران هر یک از این شبکه ها می توانند به اطلاعات ومنابع به اشتراک گذاشته شده توسط شبکه های دیگر دسترسی یابند. از این فناوری با نام شبکه های راه دور " Long Haul Network" نیز نام برده می شود. در شبکه گسترده سرعت انتقال داده نسبت به شبکه های محلی خیلی کمتر است. بزرگترین ومهم ترین شبکه گسترده ، شبکه جهانی اینترنت می باشد.

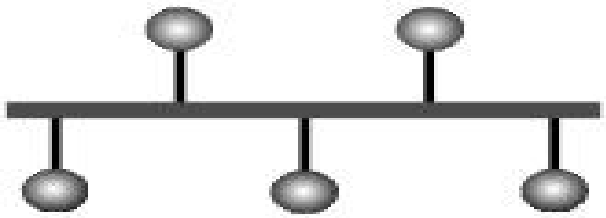
ریخت شناسی شبکه " Net work Topology":

توپولوژی شبکه تشریح کننده نحوه اتصال کامپیوتر ها در یک شبکه به یکدیگر است. پارامترهای اصلی در طراحی یک شبکه ، قابل اعتماد بودن ومقرون به صرفه بودن است. انواع متداول توپولوژی ها در شبکه کامپیوتری عبارتند از :

سه نوع توپولوژی رایج در شبکه های LAN استفاده می گردد :

- BUS
- STAR
- RING

توپولوژی BUS . یکی از رایجترین توپولوژی ها برای پیاده سازی شبکه های LAN است . در مدل فوق از یک کابل بعنوان ستون فقرات اصلی در شبکه استفاده شده و تمام کامپیوترهای موجود در شبکه (سرویس دهنده ، سرویس گیرنده) به آن متصل می گردند.



Bus

مزایای توپولوژی BUS

- کم بودن طول کابل . بدلیل استفاده از یک خط انتقال جهت اتصال تمام کامپیوترها ، در توپولوژی فوق از کابل کمی استفاده 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 ساده است . در 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 هائی به نام Repeater استفاده کرد.

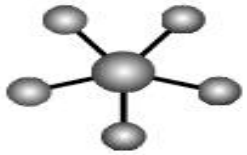
معایب توپولوژی BUS

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

- ایزوله کردن خطاء مشکل است . در صورتیکه 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 حالتیکه اشکال در محیط انتقال باشد ، تمام یک سگمنت می بایست از شبکه خارج گردد.

- ماهیت تکرارکننده ها . در مواردیکه برای توسعه شبکه از تکرارکننده ها استفاده می گردد، ممکن است در ساختار شبکه تغییراتی نیز داده شود. موضوع فوق مستلزم بکارگیری کابل بیشتر و اضافه نمودن اتصالات مخصوص شبکه است .

توپولوژی STAR . در این نوع توپولوژی همانگونه که از نام آن مشخص است ، از مدلی شبیه "ستاره" استفاده می گردد. در این مدل تمام کامپیوترهای موجود در شبکه معمولا" به یک دستگاه خاص با نام " هاب " متصل خواهند شد.



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 را آسان می نماید.

- در هر اتصال یکدستگاه . 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 زدائی خط مزبور است . عملیات فوق تاثیری در عملکرد سایر کامپیوترهای 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 بسادگی 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 و دریافت اطلاعات دارای الگوریتمی ساده خواهد بود.

معایب توپولوژی STAR

- زیاد بودن طول کابل . بدلیل اتصال مستقیم هر گره به نقطه مرکزی ، مقدار زیادی کابل مصرف می شود. با توجه به اینکه هزینه کابل نسبت به تمام شبکه ، کم است ، تراکم در کانال کشی جهت کابل ها و مسائل مربوط به نصب و پشتیبنی آنها بطور قابل توجهی هزینه ها را افزایش خواهد داد.

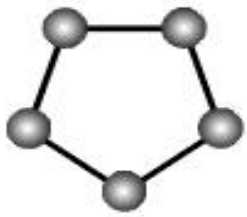
- مشکل بودن توسعه . اضافه نمودن یک گره جدید به شبکه مستلزم یک اتصال از نقطه مرکزی به گره جدید است . با اینکه در زمان کابل کشی پیش بینی های لازم جهت توسعه در نظر گرفته می شود ، ولی در برخی حالات نظیر زمانیکه طول زیادی از کابل مورد نیاز بوده و یا اتصال مجموعه ای از گره های غیر قابل پیش بینی اولیه ، توسعه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

- وابستگی به نقطه مرکزی . در صورتیکه نقطه مرکزی (هاب) در شبکه با مشکل مواجه شود ، تمام شبکه غیرقابل استفاده خواهد بود.

توپولوژی RING . در این نوع توپولوژی تمام کامپیوترها بصورت یک حلقه به یکدیگر مرتبط می گردند. تمام کامپیوترهای موجود در شبکه (سرویس دهنده ، سرویس گیرنده) به یک کابل که بصورت یک دایره بسته است ، متصل می گردند. در مدل فوق هر گره به دو و فقط دو همسایه مجاور خود متصل است . اطلاعات از گره مجاور دریافت و به گره بعدی ارسال می شوند. بنابراین داده ها فقط در یک جهت حرکت کرده و از ایستگاهی به ایستگاه دیگر انتقال پیدا می کنند.

مزایای توپولوژی RING

- کم بودن طول کابل . طول کابلی که در این مدل بکار گرفته می شود ، قابل مقایسه به 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.



Ring

- نیاز به فضائی خاص جهت انشعابات در کابل کشی نخواهد بود.بدلیل استفاده از یک کابل جهت اتصال هر گره به گره همسایه اش ، اختصاص محل هائی خاص بمنظور کابل کشی ضرورتی نخواهد داشت .

- مناسب جهت فیبر نوری . 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 فیبر نوری بمنظور محیط انتقال استفاده کرد.در صورت تمایل می توان در هر بخش ازشبکه از یک نوع کابل بعنوان محیط انتقال استفاده کرد . مثلا" در محیط های ادرای از مدل های مسی و در محیط کارخانه از فیبر نوری 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 زدائی مشکل است . بروز اشکال در یک گره می تواند روی تمام گرههای دیگر تاثیر گذار باشد. بمنظور 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 ، بدلیل ماهیت حلقوی شبکه مسائلی بوجود خواهد آمد .

- 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 .

توپولوژی ستاره ای [Star]:

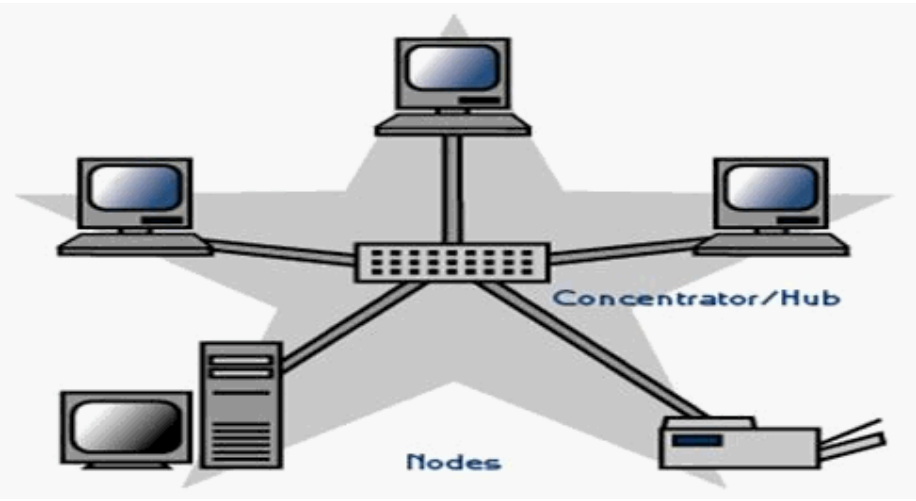
در این توپولوژی ، کلیه کامپیوتر ها به یک کنترل کننده مرکزی با هاب متصل هستند. هرگاه کامپیوتری بخواهد با کامپیوتر ی دیگری تبادل اطلاعات نماید، کامپیوتر منبع ابتدا باید اطلاعات را به هاب ارسال نماید. سپس از طریق هاب آن اطلاعات به کامپیوتر مقصد منتقل شود. اگر کامپیوتر شماره یک بخواهد اطلاعاتی را به کامپیوتر شماره ۳ بفرستد ، باید اطلاعات را ابتدا به هاب ارسال کند، آنگاه هاب آن اطلاعات را به کامپیوتر شماره سه خواهد فرستاد.

نقاط ضعف این توپولوژی آن است که عملیات کل شبکه به هاب وابسته است. این بدان معناست که اگر هاب از کار بیفتد، کل شبکه از کار خواهد افتاد . نقاط قوت توپولوژی ستاره عبارتند از:

* نصب شبکه با این توپولوژی ساده است.

* توسعه شبکه با این توپولوژی به راحتی انجام می شود.

* اگر یکی از خطوط متصل به هاب قطع شود ، فقط یک کامپیوتر از شبکه خارج می شود.



توپولوژی حلقوی [Ring]:

این توپولوژی توسط شرکت IBM اختراع شد وبهمین دلیل است که این توپولوژی بنام IBM Tokenring " مشهور است.

در این توپولوژی کلیه کامپیوتر ها به گونه ای به یکدیگر متصل هستند که مجموعه آنها یک حلقه را می سازد. کامپیوتر مبدا اطلاعات را به کامپیوتری بعدی در حلقه ارسال نموده وآن کامپیوتر آدرس اطلاعات رابرای خود کپی می کند، آنگاه اطلاعات را به کامپیوتر بعدی در حلقه منتقل خواهد کرد وبهمین ترتیب این روند ادامه پیدا می کند تا اطلاعات به کامپیوتر مبدا برسد. سپس کامپیوتر مبدا این اطلاعات را از روی حلقه حذف می کند.

نقاط ضعف توپولوژی فوق عبارتند از:

*اگر یک کامپیوتر از کار بیفتد ، کل شبکه متوقف می شود.

* به سخت افزار پیچیده نیاز دارد " کارت شبکه آن گران قیمت است ".

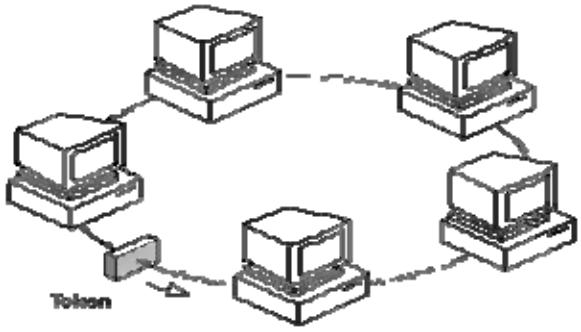
* برای اضافه کردن یک ایستگاه به شبکه باید کل شبکه را متوقف کرد.

نقاط قوت توپولوژی فوق عبارتند از :

* نصب شبکه با این توپولوژی ساده است.

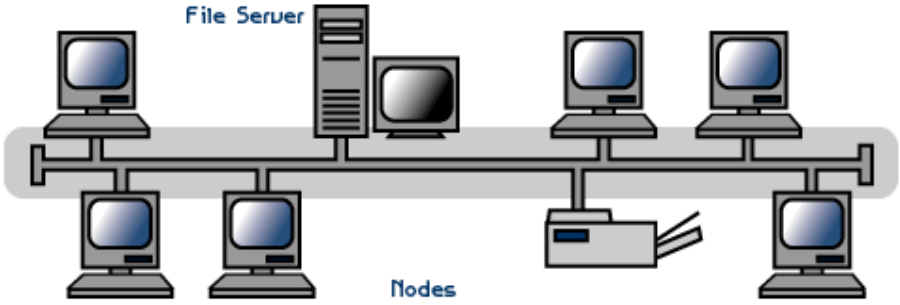
* توسعه شبکه با این توپولوژی به راحتی انجام می شود.

* در این توپولوژی از کابل فیبر نوری میتوان استفاده کرد.



توپولوژی اتوبوسی [BUS]: (خطی)

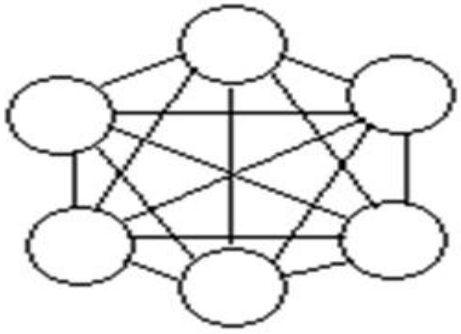
در یک شبکه خطی چندین کامپیوتر به یک کابل بنام اتوبوسی متصل می شوند. در این توپولوژی ، رسانه انتقال بین کلیه کامپیوتر ها مشترک است. یکی از مشهورترین قوانین نظارت بر خطوط ارتباطی در شبکه های محلی اترنت است. توپولوژی اتوبوس از متداوالترین توپولوژی هایی است که در شبکه محلی مورد استفاده قرار می گیرد. سادگی ، کم هزینه بودن وتوسعه آسان این شبکه ، از نقاط قوت توپولوژی اتوبوسی می باشد. نقطه ضعف عمده این شبکه آن است که اگر کابل اصلی که بعنوان پل ارتباطی بین کامپیوتر های شبکه می باشد قطع شود، کل شبکه از کار خواهد افتاد.



توپولوژی توری [Mesh] :

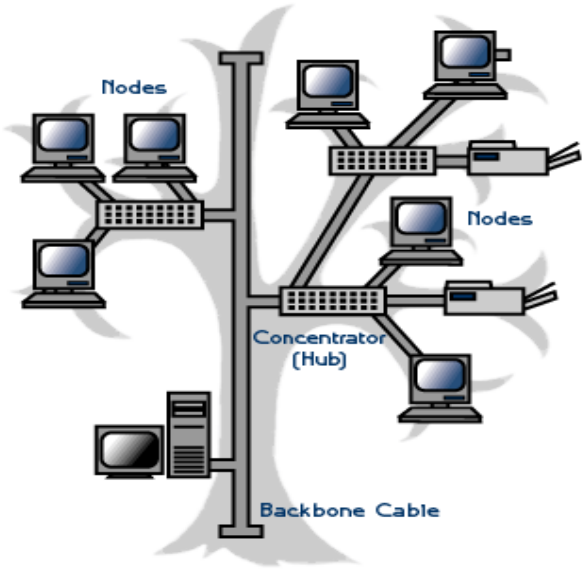
در این توپولوژی هر کامپیوتری مستقیما به کلیه کامپیوترهای شبکه متصل می شود. مزیت این توپولوژی آن است که هر کامپیوتر با سایر کامپیوتر ها ارتباطی مجزا دارد. بنابراین ، این توپولوژی دارای بالاترین درجه امنیت واطمینان می باشد. اگر یک کابل ارتباطی در این توپولوژی قطع شود ، شبکه همچنان فعال باقی می ماند.

از نقاط ضعف اساسی این توپولوژی آن است که از تعداد زیادی خطوط ارتباطی استفاده می کند، مخصوصا زمانیکه تعداد ایستگاه ها افزایش یابند. به همین جهت این توپولوژی از نظر اقتصادی مقرون به صرفه نیست. برای مثال ، در یک شبکه با صد ایستگاه کاری ، ایستگاه شماره یک نیازمند به نود ونه می باشد. تعداد کابل های مورد نیاز در این توپولوژی با رابطه $N(N-۱)/۲$ محاسبه می شود که در آن N تعداد ایستگاه های شبکه می باشد.



توپولوژی درختی [Tree] :

این توپولوژی از یک یا چند هاب فعال یا تکرار کننده برای اتصال ایستگاه ها به یکدیگر استفاده می کند. هاب مهمترین عنصر شبکه مبتنی بر توپولوژی در ختی است : زیرا کلیه ایستگاه ها را به یکدیگر متصل می کند. وظیفه هاب دریافت اطلاعات از یک ایستگاه و تکرار وتقویت آن اطلاعات وسپس ارسال آنها به ایستگاه دیگر می باشد.



توپولوژی ترکیبی " Hybrid"

این توپولوژی ترکیبی است از چند شبکه با توپولوژی متفاوت که توسط یک کابل اصلی بنام استخوان بنـدی " bone Back" بـه یکـدیگر مرتبط شده اند . هر شبکه توسط یک پل ارتباطی " Bridg" به کابل استخوان بندی متصل می شود.

پروتکل :

برای برقراری ارتباط بین رایانه ها ی سرویس گیرنده و سرویس دهنده قوانین کامپیوتری برای انتقال ودریافت داده مشخص شده اند کـه بـه قرارداد یا پروتکل موسومند. این قرارداد ها وقوانین بصورت نرم افزاری در سیستم برای ایجاد ارتباط ایفای نقش می کنند. پروتکل با قرارداد ، در واقع زبان مشترک کامپیوتری است که برای درک وفهم رایانه بهنگام در خواست وجواب متقابل استفاده می شود. پروتکـل تعیـین کننـده مشخصه های شبکه ، روش دسترسی وانواع فیزیکی توپولوژی ها ، سرعت انتقال داده ها وانواع کابل کشی است .

پروتکل های شبکه :

ما در این دستنامه تنها دو تا از مهمترین پروتکل های شبکه را معرفی می کنیم:

" پروتکل کنترل انتقال / پروتکل اینترنت

"Protoc l/ Inernet Protocol Tcp / ip= Transmission Control"

پروتکل فوق شامل چهار سطح است که عبارتند از :

الف - سطح لایه کاربرد " Application "

ب - سطح انتقال " Transporter"

ج - سطح اینترنت " Internet"

د - سطح شبکه [Net work]:

TCP / IP

TCP/IP پروتکل استاندارد در اکثر شبکه های بزرگ است . با اینکه پروتکل فوق کند و مستلزم استفاده از منابع زیادی است ، ولی بدلیل مزایای بالای آن نظیر : قابلیت روتینگ ، حمایت در اغلب پلات فورم ها و سیستم های عامل همچنان در زمینه استفاده از پروتکل ها حرف اول را می زند. با استفاده از پروتکل فوق کاربران با در اختیار داشتن ویندوز و پس از اتصال به شبکه اینترنت، براحتی قادر به ارتباط با کاربران دیگر خواهند بود که از مکینتاش استفاده می کند

امروزه کمتر محیطی را می توان یافت که نیازبه دانش کافی در رابطه با TCP/IP نباشد. حتی سیستم عامل شبکه ای ناول که سالیان متمادی از پروتکل IPX/SPX برای ارتباطات استفاده می کرد، در نسخه شماره پنج خود به ضرورت استفاده از پروتکل فوق واقف و نسخه اختصاصی خود را در این زمینه ارائه نمود.

پروتکل TCP/IP در ابتدا برای استفاده در شبکه ARPAnet (نسخه قبلی اینترنت) طراحی گردید. وزارت دفاع امریکا با همکاری برخی از دانشگاهها اقدام به طراحی یک سیستم جهانی نمود که دارای قابلیت ها و ظرفیت های متعدد حتی در صورت بروز جنگ هسته ای باشد. پروتکل ارتباطی برای شبکه فوق ، TCP/IP در نظر گرفته شد.

اجزای پروتکل TCP / IP

پروتکل TCP/IP از مجموعه پروتکل های دیگر تشکیل شده که هر یک در لایه مربوطه، وظایف خود را انجام می دهند. پروتکل های موجود در لایه های Transport و Network دارای اهمیت بسزائی بوده و در ادامه به بررسی آنها خواهیم پرداخت .

پروتکل های موجود در لایه Network پروتکل TCP / IP

- پروتکل TCP(Protocol Transmission Control) ، مهمترین وظیفه پروتکل فوق اطمینان از صحت ارسال اطلاعات است . پروتکل فوق اصطلاحا" Connection-oriented نامیده می شود. علت این امر ایجاد یک ارتباط مجازی بین کامپیوترهای فرستنده و گیرنده بعد از ارسال اطلاعات است . پروتکل هائی از این نوع ، امکانات بیشتری را بمنظور کنترل خطاهای احتمالی در ارسال اطلاعات فراهم نموده ولی بدلیل افزایش بار عملیاتی سیستم کارائی آنان کاهش خواهد یافت . از پروتکل TCP بعنوان یک پروتکل قابل اطمینان نیز یاد می شود. علت این امر ارسال اطلاعات و کسب آگاهی لازم از گیرنده اطلاعات بمنظور اطمینان از صحت ارسال توسط فرستنده است . در صورتیکه بسته های اطلاعاتی بدرستی دراختیار فرستنده قرار نگیرند، فرستنده مجددا" اقدام به ارسال اطلاعات می نماید.

- پروتکل UDP(User Datagram Protocol) . پروتکل فوق نظیر پروتکل TCP در لایه " حمل " فعالیت می نماید. UDP بر خلاف پروتکل TCP بصورت " بدون اتصال " است . بدیهی است که سرعت پروتکل فوق نسبت به TCP سریعتر بوده ولی از بعد کنترل خطاء تظمینات لازم را ارائه نخواهد داد. بهترین جایگاه استفاده از پروتکل فوق در مواردی است که برای ارسال و دریافت اطلاعات به یک سطح بالا از اطمینان ، نیاز نداشته باشیم .

- پروتکل IP(Internet Protocol) . پروتکل فوق در لایه شبکه ایفای وظیفه کرده و مهمترین مسئولیت آن دریافت و ارسال بسته های اطلاعاتی به مقاصد درست است . پروتکل فوق با استفاده از آدرس های نسبت داده شده منطقی، عملیات روتینگ را انجام خواهد داد.

پروتکل های موجود در لایه Application پروتکل TCP / IP

پروتکل TCP/IP صرفا" به سه پروتکل TCP، UDP و IP محدود نشده و در سطح لایه Application دارای مجموعه گسترده ای از سایر پروتکل ها است . پروتکل های فوق بعنوان مجموعه ابزارهائی برای مشاهده ، اشکال زدائی و اخذ اطلاعات و سایر عملیات مورد استفاده قرار می گیرند.در این بخش به معرفی برخی از این پروتکل ها خواهیم پرداخت .

- پروتکل FTP(File Transfer Protocol) . از پروتکل فوق برای تکثیر فایل های موجود بر روی یک کامپیوتر و کامپیوتر دیگر استفاده می گردد. ویندوز دارای یک برنامه خط دستوری بوده که بعنوان سرویس گیرنده ایفای وظیفه کرده و امکان ارسال و یا دریافت فایل ها را از یک سرویس دهنده FTP فراهم می کند.

- پروتکل SNMP(Simple Network Management Protocol) . از پروتکل فوق بمنظور اخذ اطلاعات آماری استفاده می گردد. یک سیستم مدیریتی، درخواست خود را از یک آژانس SNMP مطرح و ماحصل عملیات کار در یک MIB(Management Information Base) ذخیره می گردد. MIB یک بانک اطلاعاتی بوده که اطلاعات مربوط به کامپیوترهای موجود در شبکه را در خود نگهداری می نماید .(مثلا" چه میزان فضا ی هارد دیسک وجود دارد)

- پروتکل TelNet . با استفاده از پروتکل فوق کاربران قادر به log on ، اجرای برنامه ها و مشاهده فایل های موجود بر روی یک کامپیوتر از راه دور می باشند. ویندوز دارای برنامه های سرویس دهنده و گیرنده جهت فعال نمودن و استفاده از پتانسیل فوق است .

- پروتکل SMTP(simple Mail Transfer Protocol) . از پروتکل فوق برای ارسال پیام الکترونیکی استفاده می گردد.

- پروتکل HTTP(HyperText Transfer Protocol) . پروتکل فوق مشهورترین پروتکل در این گروه بوده و از آن برای رایج ترین سرویس اینترنت یعنی وب استفاده می گردد. با استفاده از پروتکل فوق کامپیوترها قادر به مبادله فایل ها با فرمت های متفاوت (متن، تصاویر ،گرافیکی ، صدا، ویدئو و...) خواهند بود. برای مبادله اطلاعات با استناد به پروتکل فوق می بایست ، سرویس فوق از طریق نصب سرویس دهنده وب فعال و در ادامه کاربران و استفاده کنندگان با استفاده از یک مرورگر وب قادر به استفاده از سرویس فوق خواهند بود.

پروتکل NNTP(Network News Transfer Protocol) . از پروتکل فوق برای مدیریت پیام های ارسالی برای گروه های خبری خصوصی و عمومی استفاده می گردد. برای عملیاتی نمودن سرویس فوق می بایست سرویس دهنده NNTP بمنظور مدیریت محل ذخیره سازی پیام های ارسالی نصب و در ادامه کاربران و سرویس گیرندگان با استفاده از برنامه ای موسوم به NewsReader از اطلاعات ذخیره شده استفاده خواهند کرد

مدل آدرس دهی IP

علاوه بر جایگاه پروتکل ها، یکی دیگر از عناصر مهم در زیرساخت شبکه های مبتنی بر TCP/IP مدل آدرس دهی IP است . مدل انتخابی می بایست این اطمینان را بوجود آورد که اطلاعات ارسالی بدرستی به مقصد خواهند رسید. نسخه شماره چهار IP (نسخه فعلی) از ۳۲ بیت برای آدرس دهی استفاده کرده که بمنظور تسهیل در امر نمایش بصورت چهار عدد صحیح (مبنای ده) که بین آنها نقطه استفاده شده است نمایش داده می شوند.

نحوه اختصاص IP

نحوه اختصاص IP به عناصر مورد نیاز در شبکه های مبتنی بر TCP/IP یکی از موارد بسیار مهم است . اختصاص IP ممکن است بصورت دستی و توسط مدیریت شبکه انجام شده و یا انجام رسالت فوق بر عهده عناصر سرویس دهنده نرم افزاری نظیر DHCP و یا NAT گذاشته گردد

Subnetting

یکی از مهمترین عملیات در رابطه با اختصاص IP مسئله Subnetting است . مسئله فوق بعنوان هنر و علمی است که ماحصل آن تقسیم یک شبکه به مجموعه ای از شبکه های کوچکتر (Subnet) از طریق بخدمت گرفتن ۳۲ بیت با نام Subnet mask بوده که بنوعی مشخصه (ID) شبکه را مشخص خواهد کرد.

کالبد شکافی آدرس های IP

هر دستگاه در شبکه های مبتنی بر TCP/IP دارای یک آدرس منحصر بفرد است . آدرس فوق IP نامیده می شود. یک آدرس IP مطابق زیر است :

- ۲۱۶,۲۷,۶۱,۱۳۷

بمنظور بخاطر سپردن آسان آدرس های IP ، نحوه نما یش آنها بصورت دسیمال (مبنای دهدهی) بوده که توسط چهار عدد که توسط نقطه از یکدیگر جدا می گردند ، است . هر یک از اعداد فوق را octet می گویند. کامپیوترها برای ارتباط با یکدیگر از مبنای دو (باینری) استفاده می نمایند. فرمت باینری آدرس IP اشاره شده بصورت زیر است :

- ۱۱۰۱۱۰۰۰,۰۰۰۱۱۰۱۱,۰۰۱۱۱۱۰۱,۱۰۰۰۱۰۰۱

همانگونه که مشاهده می گردد ، هر IP از ۳۲ بیت تشکیل می گردد. بدین ترتیب می توان حداکثر ۴,۲۹۴,۹۶۷,۲۹۶ آدرس منحصر بفرد را استفاده کرد(۲۳۲) . مثلا" آدرس ۲۵۵,۲۵۵,۲۵۵,۲۵۵ برای Broadcast (انتشار عام) استفاده می گردد . نمایش یک IP بصورت چهار عدد (Octet) صرفا" برای راحتی کار نبوده و از آنان برای ایجاد " کلاس های IP " نیز استفاده می گردد. هر Octet به دو بخش مجزا تقسیم می گردد: شبکه (Net) و میزبان (Host) . اولین octet نشاندهنده شبکه بوده و از آن برای مشخص نمودن شبکه ای که کامپیوتر به آن تعلق دارد ، استفاده می گردد. سه بخش دیگر octet ، نشاندهنده آدرس کامپیوتر موجود در شبکه است

پنج کلاس متفاوت IP بهمراه برخی آدرس های خاص ، تعریف شده است :

- Default Network . آدرس IP ۰,۰,۰,۰ ، برای شبکه پیش فرض در نظر گرفته شده است .آدرس فوق برای مواردیکه کامپیوتر میزبان از آدرس خود آگاهی ندارد استفاده شده تا به پروتکل هائی نظیر DHCP اعلام نماید برای وی آدرسی را تخصیص دهد.

- کلاس A . کلاس فوق برای شبکه های بسیار بزرگ نظیر یک شرکت بین المللی در نظر گرفته می شود. آدرس هائی که اولین octet آنها ۱ تا ۱۲۶ باشد ، کلاس A می باشند. از سه octet دیگر بمنظور مشخص نمودن هر یک از کامپیوترهای میزبان استفاده می گردد. بدین ترتیب مجموع شبکه های کلاس A ، معادل ۱۲۶ و هر یک از شبکه های فوق می توانند ۱۶,۷۷۷,۲۱۴ کامپیوتر میزبان داشته باشند. (عدد فوق از طریق حاصل ۲ - ۲۲۴ بدست آمده است) .بنابراین تعداد تمام کامپیوترهای میزبان در شبکه های کلاس A معادل ۲,۱۴۷,۴۸۳,۶۴۸ (۲۳۱) است . در شبکه های کلاس A ، بیت با ارزس بالا در اولین octet همواره مقدار صفر را دارد.

NET	Host (Node)
۱۱۵.	۲۴,۵۳,۱۰۷

- LoopBack . آدرس IP ۱۲۷,۰,۰,۱ برای LoopBack در نظر گرفته شده است . کامپیوتر میزبان از آدرس فوق برای ارسال یک پیام برای خود استفاده می کند.(فرستنده و گیرنده پیام یک کامپیوتر می باشد) آدرس فوق اغلب برای تست و اشکال زدائی استفاده می گردد.

- کلاس B . کلاس فوق برای شبکه های متوسط در نظر گرفته می شود.(مثلا" یک دانشگاه بزرگ) آدرس هائی که اولین octet آنها ۱۲۸ تا ۱۹۱ باشد ، کلاس B می باشند. در کلاس فوق از دومین octet هم برای مشخص کردن شبکه استفاده می گردد. از دو octet دیگر برای مشخص نمودن هر یک از کامپیوترهای میزبان در شبکه استفاده می گردد بدین ترتیب ۱۶,۳۸۴ (۲۱۴) شبکه از نوع کلاس B وجود دارد. تعداد کامپیوترهای میزبان در این نوع شبکه ها(هر شبکه) معادل ۶۵,۵۳۴ (۲ - ۱۶ ۲) است . بنابراین تعداد تمام

کامپیوترهای میزبان در شبکه های کلاس B معادل ۱,۰۷۳,۷۴۱,۸۲۴ (۲۳۰) است در شبکه های کلاس B ، اولین و دومین بیت در اولین octet به ترتیب مقدار یک و صفر را دارا می باشند.

NET	Host (Node)
۱۴۵,۲۴.	۵۳,۱۰۷

- **کلاس C** . کلاس فوق برای شبکه های کوچک تا متوسط در نظر گرفته می شود.آدرس هائی که اولین octet آنها ۱۹۲ تا ۲۲۳ باشد ، کلاس C می باشند. در کلاس فوق از دومین و سومین octet هم برای مشخص کردن شبکه استفاده می گردد. از آخرین octet برای مشخص نمودن هر یک از کامپیوترهای میزبان در شبکه استفاده می گردد . بدین ترتیب ۲,۰۹۷,۱۵۲ (۲ ۲۱) شبکه کلاس C وجود دارد.تعداد کامپیوترهای میزبان در این نوع شبکه ها(هر شبکه) معادل ۲۵۴ (۲ - ۸ ۲) است . بنابراین تعداد تمام کامپیوترهای میزبان در شبکه های کلاس C معادل ۵۳۶,۸۷۰,۹۱۲ (۲۲۹) است . در شبکه های کلاس C ، اولین ، دومین و سومین بیت در اولین octet به ترتیب مقدار یک ، یک و صفر را دارا می باشند.

NET	Host(Node)
۱۹۵,۲۴,۵۳.	۱۰۷

- **کلاس D** . از کلاس فوق برای multicasts استفاده می شود. در چنین حالتی یک گره (میزبان) بسته اطلاعاتی خود را برای یک گروه خاص ارسال می دارد. تمام دستگاه های موجود در گروه ، بسته اطلاعاتی ارسال شده را دریافت خواهند کرد. (مثلا" یک روتر سیسکو آخرین وضعیت بهنگام شده خود را برای سایر روترهای سیسکو ارسال می دارد) کلاس فوق نسبت به سه کلاس قبلی دارای ساختاری کاملا" متفاوت است. اولین ، دومین ، سومین و چهارمین بیت به ترتیب دارای مقادیر یک ، یک ، یک و صفر می باشند.۲۸ بیت باقیمانده بمنظور مشخص نمودن گروههائی از کامپیوتر بوده که پیام Multicast برای آنان در نظر گرفته می شود. کلاس فوق قادر به آدرسی دهی ۲۶۸,۴۳۵,۴۵۶ (۲۲۶) کامپیوتر است

NET	Host(Node)
۲۲۴.	۲۴,۵۳,۱۰۷

- **کلاس E** . از کلاس فوق برای موارد تجربی استفاده می شود. کلاس فوق نسبت به سه کلاس اولیه دارای ساختاری متفاوت است . اولین ، دومین ، سومین و چهارمین بیت به ترتیب دارای مقادیر یک ، یک ، یک و یک می باشند.۲۸ بیت باقیمانده بمنظور مشخص نمودن گروههائی از کامپیوتر بوده که پیام Multicast برای آنان در نظر گرفته می شود. کلاس فوق قادر به آدرسی دهی ۲۶۸,۴۳۵,۴۵۶ (۲۲۶) کامپیوتر است

NET	Host(Node)
۲۴۰.	۲۴,۵۳,۱۰۷

- **BroadCast** . پیام هائی با آدرسی از این نوع ، برای تمامی کامپیوترهای در شبکه ارسال خواهد شد. این نوع پیام ها همواره دارای آدرس زیر خواهند بود :

- ۲۵۵,۲۵۵,۲۵۵,۲۵۵.

- آدرس های رزو شده . آدرس های IP زیر بمنظور استفاده در شبکه های خصوصی (اینترانت) رزو شده اند :

- ۱۰.x.x.x
- ۱۷۲,۱۶.x.x - ۱۷۲,۳۱.x.x
- ۱۹۲,۱٦۸.x.x

- IP نسخه شش . نسخه فوق برخلاف نسخه فعلی که از ۳۲ بیت بمنظور آدرس دهی استفاده می نماید ، از ۱۲۸ بیت برای آدرس دهی استفاده می کند. هر شانزده بیت بصورت مبنای شانزده نمایش داده می شود. :

۲b۶۳:۱۴۷۸:۱ac۵:۳۷ef:۴e۸c:۷۵df:۱۴cd:۹۳f۲

پروتکل های پشته ای

یک پروتکل پشته ای ، شامل مجموعه ای از پروتکل ها است که با یکدیگر فعالیت نموده تا امکان انجام یک عملیات خاص را برای سخت افزار و یا نرم افزار فراهم نمایند. پروتکل TCP/IP نمونه ای از پروتکل های پشته ای است . پروتکل فوق از چهار لایه استفاده می نماید

- لایه یک (Network Interface) . لایه فوق ، لایه های Physical و Data را ترکیب و داده های مربوط به دستگاه های موجود در یک شبکه را روت خواهد کرد.

- لایه دو (Internet) . لایه فوق متناظر لایه Network در مدل OSI است . پروتکل اینترنت (IP) ، با استفاده از آدرس IP (شامل یک مشخصه شبکه و یک مشخصه میزبان) ، آدرس دستگاه مورد نظر برای ارتباط را مشخص می نماید.

- لایه سه (Transport) . لایه فوق متناظر با لایه Transport در مدل OSI است . پروتکل TCP(Trnsport control protocol(در لایه فوق ایفای وظیفه می نماید

- لایه چهار (Application) . لایه فوق متناظر با لایه های Session,Presentation و Application در مدل OSI است. پروتکل هائی نظیر FTP و SMTP در لایه فوق ایفای وظیفه می نمایند.

" از مهمترین ومشهورترین پروتکل های مورد استفاده در شبکه اینترنت است این بسته نرم افزاری به اشکال مختلف برای کامپیوتر ها وبرنامه ها ی مختلف ارائه می گردد. Tcp/ip از مهمترین پروتکل های ارتباطی شبکه در جهان تلقی می شود ونه تنها برروی اینترنت وشبکه های گسترده گوناگون کاربرد دارد، بلکه در شبکه های محلی مختلف نیز مورد استفاده قرار می گیردو در واقع این پروتکل زبان مشترک بین کامپیوتر ها به هنگام ارسال و دریافت اطلاعات یا داده می باشد. این پروتکل به دلیل سادگی مفاهیمی که در خود دارد اصطلاحا به سیستم باز مشهور است ، برروی هر کامپیوتر وابر رایانه قابل طراحی وپیاده سازی است. از فاکتورهای مهم که این پروتکل بعنوان یک پروتکل ارتباطی جهانی مطرح می گردد، به موارد زیر می توان اشاره کرد:

۱ - این پروتکل در چار چوب UNIX Operating System ساخته شده وتوسط اینترنت

بکار گرفته می شود.

۲ - برروی هر کامپیوتر قابل پیاده سازی می باشد.

۳ - بصورت حرفه ای در شبکه های محلی وگسترده مورد استفاده قرار می گیرد.

۴ - پشتیبانی از مجموعه برنامه ها وپروتکل های استاندارد دیگر چون پروتکل انتقال فایل " FTP

" وپروتکل دو سویه " Point to point Protcol = PPP " .

بنیاد واساس پروتکل Tcp/ip آن است که برای دریافت و ارسال داده ها یا پیام پروتکل مذکور ؛ پیام ها وداده ها را به بسته هـای کـوچکتر وقابل حمل تر تبدیل می کند ، سپس این بسته ها به مقصد انتقال داده می شود ودر نهایت پیوند این بسته ها به یکدیگر که شکل اولیه پیام ها وداده ها را بخود می گیرد ، صورت می گیرد.

یکی دیگر از ویژگی های مهم این پروتکل قابلیت اطمینان آن در انتقال پیام هاست یعنـی ایـن قابلیـت کـه بـه بررسـی وبـازبینی بـسته هـا ومحاسبه بسته های دریافت شده دارد. در ضمن این پروتکل فقط برای استفاده در شبکه اینترنت نمی باشد. بسیاری از سازمان وشـرکت هـا برای ساخت وزیر بنای شبکه خصوصی خود که از اینترنت جدا می باشد نیز در این پروتکل استفاده می کنند.

- پروتکل سیستم ورودی وخروجی پایه شبکه Net work basic input/ output

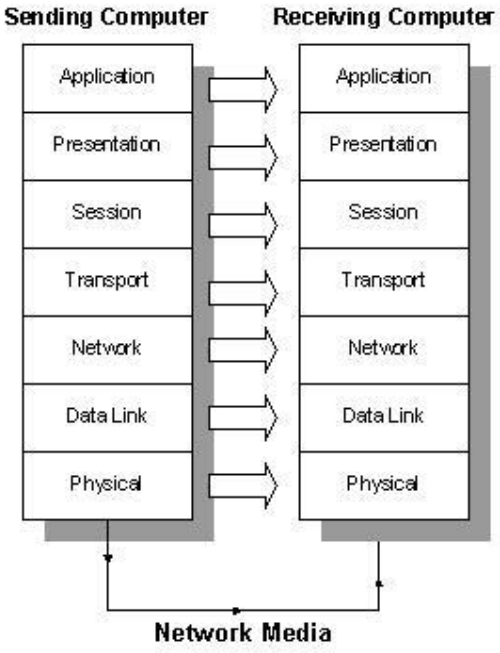
System= Net Bios" واسطه یا رابطی است که توسط IBM بعنوان استانداردی برای دسترسی به شبکه توسـعه یافـت . ایـن پروتکـل داده ها را از لایه بالاترین دریافت کرده وآنها را به شبکه منتقل می کند. سیستم عاملی که با این پروتکل ارتباط برقرار می کند سیستم عامل شبکه "NOS" نامیده می شود کامپیوتر ها از طریق کارت شبکه خود به شبکه متصل می شوند. کارت شبکه به سیستم عامل ویژه ای برای ارسال اطلاعات نیاز دارد. ایـن سیـستم عامـل ویـژه را Net BIOS مـی نامنـد کـه در حافظـه ROM کـارت شـبکه ذخیـره شـده اسـت. BIOS Net همچنین روشی را برای دسترسی به شبکه ها با پروتکل های مختلف مهیا می کند . این پروتکل از سخت افزار شـبکه مـستقل است . این پروتکل مجموعه ای از فرامین لازم برای در خواست خدمات شبکه ای سطح پایین را برای برنامه های کاربردی فراهم می کنـد تـا جلسات لازم برای انتقال اطلاعات در بین گره ها ی یک شبکه را هدایت کنند.

در حال حاضر وجود " Net BIOS Net BEUI= Net BIOS Enhansed User Interface" امتیازی جدید می دهد کـه ایـن امتیاز درواقع ایجاد گزینه انتقال استاندارد است و Net BEUI در شبکه های محلی بسیار رایج است. همچنین قابلیت انتقال سریع داده هـا را نیز دارد . اما چون یک پروتکل غیر قابل هدایت است به شبکه های محلی محدود شده است.

مدل OSI- Open System Interconnection:

بمنظور شناخت مناسب نحوه عملکرد پروتکل در شبکه می بایست با برخی از مدل های رایج شبکه که معماری شبکه را تشریح می نماینـد، آشنا گردید. مدل Open(Systems Interconnection OSI) یک مرجع مناسب در این زمینه است . ایـن مـدل در سـال ۱۹۸۴ توسط ISO (یک سازمان بین المللی استاندارد سازی با بیش از ۱۳۰ عضو) ارائه گردید. در مدل فوق از هفت لایه برای تـشریح فرآینـدهای مربوط به ارتباطات استفاده می گردد. هریک از لایه ها مسیولیت انجام عملیات خاصی را برعهـده دارنـد.. مـدل OSI بعنـوان یـک مرجـع و راهنما برای شناخت عملیات مربوط به ارتباطات استفاده می گردد. بمنظور آشنا ئی با نحوه عملکرد یک شبکه ، مطالعه مـدل فـوق، مفیـد خواهد بود. شکل زیر هفت لایه مدل OSI را نشان می دهد.

ارسال و دریافت اطلاعات از طریق لایه های مربوطه در کامپیوترهای فرستنده و گیرنده انجام خواهد شد. داده ها توسط یک برنامه و توسط کاربر تولید خواهند شد (نظیر یک پیام الکترونیکی) .شروع ارسال داده ها از لایه Application است . در ادامه و با حرکت به سمت پایین، در هر لایه عملیات مربوطه انجام و داده هائی به بسته های اطلاعاتی اضافه خواهد شد. در آخرین لایه (لایه فیزیکی) با توجه به محیط انتقال استفاده شده ، داده ها به سیگنالهای الکتریکی، پالس هائی از نور و یا سیگنالهای رادیوئی تبدیل و از طریق کابل و یا هوا برای کامپیوتر مقصد ارسال خواهند شد. پس از دریافت داده در کامپیوتر مقصد ، عملیات مورد نظر (معکوس عملیات ارسال) توسط هر یک از لایه ها انجام و در نهایت با رسیدن داده به لایه Application و بکمک یک برنامه، امکان استفاده از اطلاعات ارسالی فراهم خواهد شد. شکل زیر نحوه انجام فرآیند فوق را نشان می دهد.



لایه های OSI

همانگونه که اشاره گردید مدل OSI از هفت لایه متفاوت تشکیل شده است . در ادامه عملکرد هر لایه تشریح می گردد:

- لایه هفت (Application) . این لایه با سیستم عامل و یا برنامه های کاربردی ارتباط دارد. کاربران با استفاده از نرم افزارهای کاربردی متفاوت قادر به انجام عملیات مرتبط با شبکه خواهند بود. مثلا" کاربران می توانند اقدام به ارسال فایل خواندن پیام ارسال پیام و ... نمایند.

- لایه شش (Presentation) . لایه فوق داده های مورد نظر خود را از لایه Application اخذ و آنها را بگونه ای تبدیل خواهد کرد که توسط سایر لایه ها قابل استفاده باشد.

- لایه پنج (Session) . لایه فوق مسئول ایجاد ، پشتیبانی و ارتباطات مربوطه با دستگاه دریافت کننده اطلاعات است .

- لایه چهار (Transport) . لایه فوق مسئول پشتیبانی کنترل جریان داده ها و و بررسی خطاء و بازیابی اطلاعات بین دستگاه های متفاوت است . کنترل جریان داده ها ، بدین معنی است که لایه فوق در صورتیکه اطلاعاتی از چندین برنامه ارسال شده باشد ، داده های مربوطه به هر برنامه را به یک stream آماده تبدیل تا در اختیار شبکه فیزیکی قرار داده شوند.

- لایه سه (Network) . در لایه فوق روش ارسال داده ها برای دستگاه گیرنده تعیین خواهد شد. پروتکل های منطقی ، روتینگ و آدرس دهی در این لایه انجام خواهد شد.

- لایه دو (Data). در لایه فوق ، پروتکل های فیزیکی به داده اضافه خواهند شد. در این لایه نوع شبکه و وضعیت بسته های اطلاعاتی (Packet) نیز تعیین می گردند.

لایه یک (Physical) . لایه فوق در ارتباط مستقیم با سخت افزار بوده و خصایص فیزیکی شبکه نظیر : اتصالات ، ولتاژ و زمان را مشخص می نماید.

مدل OSI بصورت یک مرجع بوده و پروتکل های پشته ای یک و یا چندین لایه از مدل فوق را ترکیب و در یک لایه پیاده سازی می نمایند.

این مدل مبتنی بر قراردادی است که سازمان استانداردهای جهانی ایزو بعنوان مرحله ای از استاندارد سازی قراردادهای لایه های مختلف توسعه دارد . نام این مدل مرجع به این دلیل ا اس آی است چونکه با اتصال سیستم های باز سروکار دارد وسیستم های باز سیستم هایی هستند که برای ارتباط باسیستم های دیگر باز هستند . این مدل هفت لایه دارد که اصولی که منجر به ایجاد این لایه ها شده اند عبارتند از :

۱ - وقتی نیاز به سطوح مختلف از انتزاع است ، لایه ای باید ایجاد شود.

۲ - هر لایه باید وظیفه مشخصی داشته باشد.

۳ - وظیفه هر لایه باید با در نظر گرفتن قراردادهای استاندارد جهانی انتخاب گردد.

۴ - مرزهای لایه باید برای کمینه کردن جریان اطلاعات از طریق رابط ها انتخاب شوند.

اکنون هفت لایه را به نوبت از لایه پایین مورد بحث قرار می دهیم:

۱ - لایه فیزیکی :

به انتقال بیتهای خام برروی کانال ارتباطی مربوط می شود. در اینجا مدل طراحی با رابط های مکانیکی ، الکتریکی ، ورسانه انتقال فیزیکی که زیر لایه فیزیکی قراردارند سروکار دارد.

۲ - لایه پیوند ها:

مبین نوع فرمت هاست مثلا شروع فریم ، پایان فریم، اندازه فریم وروش انتقال فریم . وظایف این لایه شامل موارد زیر است :

مدیریت فریم ها ، خطایابی وارسال مجدد فریم ها، ایجاد تمایز بین فریم ها داده وکنترل وایجاد هماهنگی بین کامپیوتر ارسال کننده ودریافت کننده داده ها. پروتکل های معروف برای این لایه عبارتند از :

الف - پروتکل SDLC که برای مبادله اطلاعات بین کامپیوتر ها بکار می رود و اطلاعات را به شکل فریم سازماندهی می کند.

ب - پروتکل HDLC که کنترل ارتباط داده ای سطح بالا زیر نظر آن است وهدف از طراحی آن این است که با هر نو ع ایستگاهی کارکند از جمله ایستگاههای اولیه ، ثانویه وترکیبی.

۳ - لایه شبکه :

وظیفه این لایه ، مسیر یابی می باشد ، این مسیر یابی عبارتست از : تعیین مسیر متناسب برای انتقال اطلاعات . لایه شبکه آدرس منطقی هر فریم را بررسی می کند . و آن فریم را بر اساس جدول مسیر یابی به مسیر یاب بعدی می فرستد . لایه شبکه مسئولیت ترجمه هر آدرس منطقی به یک آدرس فیزیکی را بر عهده دارد. پس می توان گفت برقراری ارتباط یا قطع آن ، مولتی پلکس کردن از مهمترین وظایف این لایه است. از نمونه بارز خدمات این لایه ، پست الکترونیکی است.

۴ - لایه انتقال :

وظیفه ارسال مطمئن یک فریم به مقصد را برعهده دارد. لایه انتقال پس از ارسال یک فریم به مقصد ، منتظر می ماند تا سیگنالی از مقصد مبنی بر دریافت آن فریم دریافت کند. در صورتیکه لایه محل در منبع سیگنال مذکور را از مقصد دریافت نکند. مجددا اقدام به ارسال همان فریم به مقصد خواهد کرد.

۵ - لایه اجلاس :

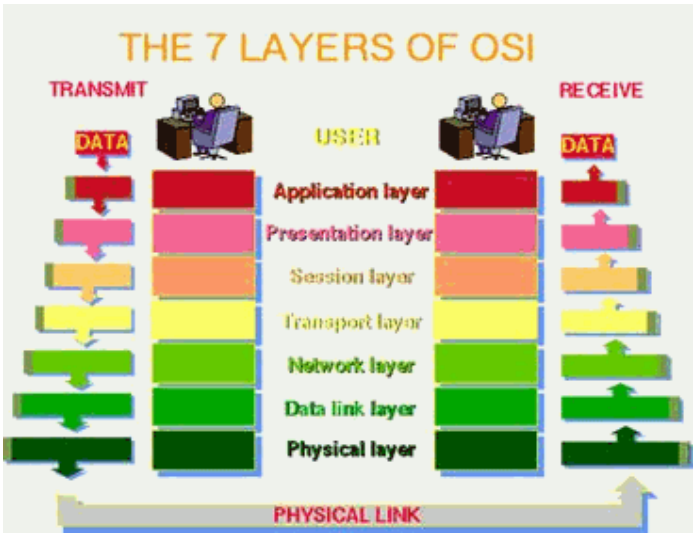
وظیفه برقراری یک ارتباط منطقی بین نرم افزار های دو کامپیوتر ی که به یکدیگر متصل هستند به عهده این لایه است. وقتی که یک ایستگاه بخواهد به یک سرویس دهنده متصل شود ، سرویس دهنده فرایند برقراری ارتباط را بررسی می کند، سپس از ایستگاه ، درخواست نام کاربر، ورمز عبور را خواهد کرد. این فرایند نمونه ای از یک اجلاس می باشد.

۶ - لایه نمایش :

این لایه اطلاعات را از لایه کاربرد دریافت نموده ، آنها را به شکل قابل فهم برای کامپیوتر مقصد تبدیل می کند . این لایه برای انجام این فرایند اطلاعات را به کدهای ASCII ویا Unicode تبدیل می کند.

۷ - لایه کاربرد :

این لایه امکان دسترسی کاربران به شبکه را با استفاده از نرم افزارهایی چون E-mail- FTP و.... فراهم می سازد.



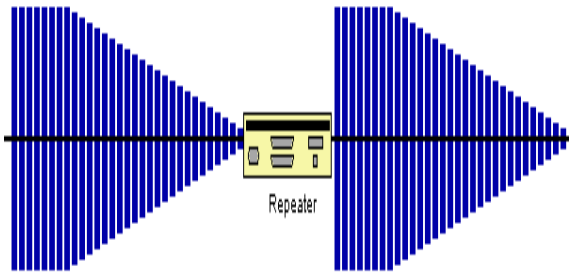
ابزارهای اتصال دهنده : "Connectivity Devices" :

ابزارهای اتصال به یک شبکه اضافه می گردند تا عملکرد وگستره شبکه وتوانایی های سخت افزاری شبکه را ارتقاء دهند . گستره وسیعی از ابزارهای اتصال در شبکه وجود دارند اما شما احتمالا برای کار خود به ابزارهای ذیل نیازمند خواهید بود:

۱ - کنترل کننده ها [Reapeaters]:

تکرار کننده وسیله ای است که برای اتصال چندین سگمنت یک شبکه محلی بمنظور افزایش وسعت مجاز آن شبکه مورد استفاده قرار می گیرد . هر تکرار کننده از درگاه ورودی " Port " خود داده ها را پذیرفته وبا تقویت آنها ، داده ها را به درگاهی خروجی خود ارسال می کند. یک تکرار کننده در لایه فیزیکی مدل OSI عمل می کند.

هر کابل یا سیم بکار رفته در شبکه که بعنوان محلی برای عبور ومرور سیگنال هاست آستانه ای دارد که در آن آستانه سرعت انتقال سیگنال کاهش می یابد ودر اینجا تکرار کننده بعنوان ابزاری است که این سرعت عبور را در طول رسانه انتقال تقویت می کند.



۲ - هاب ها [Hubs] :

ابزاری هستند در شبکه که برای اتصال یک یا بیش از دو ایستگاه کاری به شبکه مورد استفاده قرار می گیرد ویک ابزار معمول برای اتصال ابزارهای شبکه است . هابها معمولا برای اتصال سگمنت های شبکه محلی استفاده می شوند. یک هاب دارای در گاهی های چند گانه است. وقتی یک بسته در یک درگاهی وارد می شود به سایر در گاهی ها کپی می شود تا اینکه تمامی سگمنت های شبکه محلی بسته ها را ببینند.

سه نوع هاب رایج وجود دارد:

الف - هاب فعال :

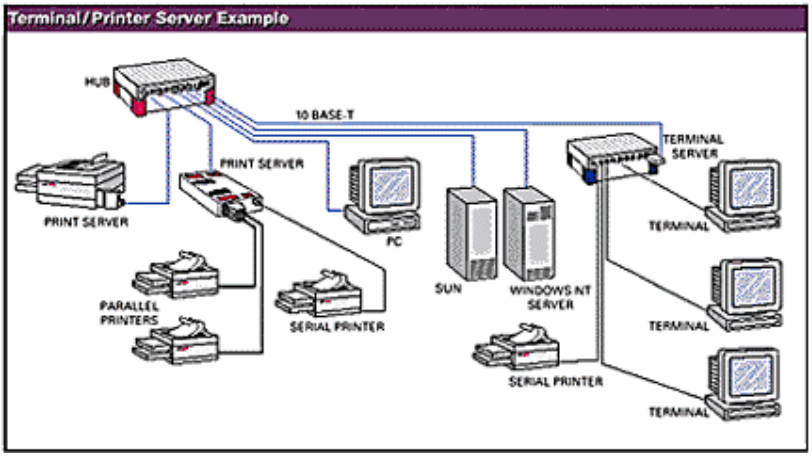
که مانند آمپلی فایر عمل می کند و باعث تقویت مسیر عبور سینگال ها می شود واز تصادم وبرخورد سیگنال ها در مسیر جلوگیری بعمل می آورد . این هاب نسبتا قیمت بالایی دارد.

ب - غیر فعال :

که بر خلاف نوع اول که در مورد تقویت انتقال سیگنال ها فعال است این هاب منفعل است.

ج - آمیخته :

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



۳ - مسیر یاب ها [Routers]:

در شبکه سازی فرایند انتقال بسته های اطلاعاتی از یک منبع به مقصد عمل مسیر یابی است که تحت عنوان ابزاری تحت عنوان مسیر یاب انجام می شود. مسیر یابی یک شاخصه کلیدی در اینترنت است زیرا که باعث می شود پیام ها از یک کامپیوتر به کامپیوتر دیگر منتقل شوند.

این عملکرد شامل تجزیه وتحلیل مسیر برای یافتن بهترین مسیر است. مسیر یاب ابزاری است که شبکه های محلی را بهم متصل می کند یا به بیان بهتر بیش از دو شبکه را بهم متصل می کند. مسیر یاب بر حسب عملکردش به دونوع زیر تقسیم می شود:

الف – مسیریاب ایستا : که در این نوع ، جدول مسیر یابی توسط مدیر شبکه که تعیین کننده مسیر می باشد بطور دستی مقدار دهی می شود.

ب – مسیر یاب پویا : که در این نوع ، جدول مسیر یابی خودش را، خود تنظیم می کند وبطور اتوماتیک جدول مسیریابی را روز آمد می کند.

۴ - دروازه ها "Gateways ":

دروازه ها در لایه کاربرد مدل ا اس ای عمل می کنند. کاربرد آن تبدیل یک پروتکل به پروتکل دیگر است. هر هنگام که در ساخت شبکه هدف استفاده از خدمات اینترنت است دروازه ها مقوله های مطرح در شبکه سازی خواهند بود.

پل ها Bridge:

یک پل برای اتصال سگمنت های یک شبکه " همگن " به یکدیگر مورد استفاده قرار می گیرد. یک پل در لایه پیوند داده ها " Data link" عمل می کند.

پل ها فریم ها را بر اساس آدرس مقصدشان ارسال می کنند. آنها همچنین می توانند جریان داده ها را کنترل نموده وخطاهایی را که در حین ارسال داده ها رخ می دهد.

عملکرد این پل عبارتست از تجزیه وتحلیل آدرس مقصد یک فریم ورودی واتخاذ تصمیم مناسب برای ارسال آن به ایستگاه مربوطه . پل ها قادر به فیلتر کردن فریم ها می باشند. فیلتر کردن فریم برای حذف فریم های عمومی یا همگانی که غیر ضروری هستند مفید می باشد، پل ها قابل برنامه ریزی هستند ومی توان آنها را به گونه ای برنامه ریزی کرد که فریم های ارسال شده از طرف منابع خاصی را حذف کنند.

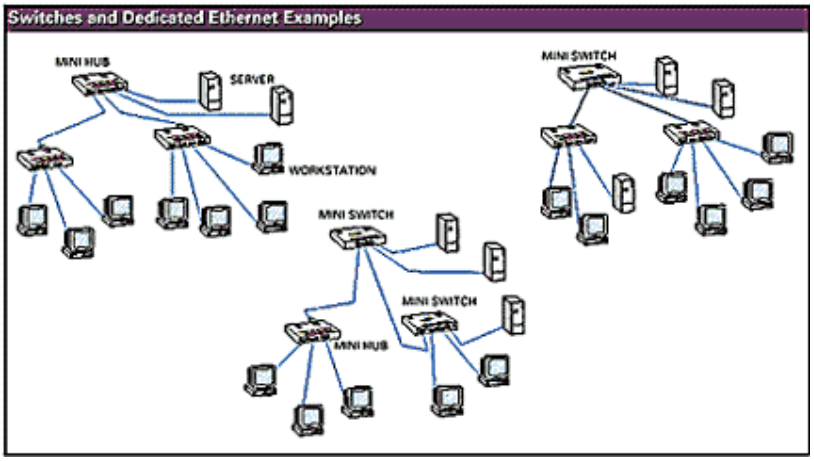
با تقسیم یک شبکه بزرگ به چندین سگمنت واستفاده از یک پل برای اتصال آنها به یکدیگر ، توان عملیاتی شبکه افزایش خواهد یافت . اگر یک سگمنت شبکه از کار بیفتد ، سایر سگمنت ها ی متصل به پل می توانند شبکه را فعال نگه دارند ، پل ها موجب افزایش وسعت شبکه محلی می شوند.

سوئیچ ها[Switches]:

سوئیچ نوع دیگری از ابزارهایی است که برای اتصال چند شبکه محلی به یکدیگر مورد استفاده قرار می گیرد که باعث افزایش توان عملیاتی شبکه می شود. سوئیچ وسیله ای است که دارای درگاه های متعدد است که بسته ها را از یک درگاه می پذیرد، آدرس مقصد را بررسی می کند وسپس بسته ها را به درگاه مورد نظر " که متعلق به ایستگاه میزبان با همان آدرس مقصد می باشد" ارسال می کند. اغلب سوئیچ های شبکه محلی در لایه پیوند داده های مدل ا اس آی عمل می کند.

سوئیچ ها بر اساس کاربردشان به متقارن "Symmetric" ونامتقارن " Asymmetric" تقسیم می شوند.

در نوع متقارن ، عمل سوئیچینگ بین سگمنت هایی که دارای پهنای باند یکسان هستند انجام می دهد یعنی ۱۰mbps به ۱۰mbps و.... سوئیچ خواهد شد. اما در نوع نامتقارن این عملکرد بین سگمنت هایی با پهنای باند متفاوت انجام می شود.



دو نوع سوئیچ وجود دارد که عبارتند از :

۱ - سوئیچ **Cut - through** : این نوع سه یا چهار بایت اول یک بسته را می خواند تا آدرس مقصد آنرا بدست آورد ، آنگاه آن بسته را به سگمنت دارای آدرس مقصد مذکور ارسال می کند این در حالی است که قسمت باقی مانده بسته را از نظر خطایابی مورد بررسی قرار نمی دهد.

۲ - سوئیچ **Store- and - forward** : این نوع ابتدا کل بسته را ذخیره کرده سپس آن را خطایابی می کند ، اگر بسته ای دارای خطا بود آن بسته را حذف می کند ، در غیر اینصورت آن بسته را به مقصد مربوطه ارسال خواهد کرد. این نوع برای شبکه محلی بسیار مناسبتر از نوع اول است زیرا بسته های اطلاعاتی خراب شده را پاکسازی می کند و بهمین دلیل این سوئیچ باعث کاهش بروز عمل تصادف خواهد شد.

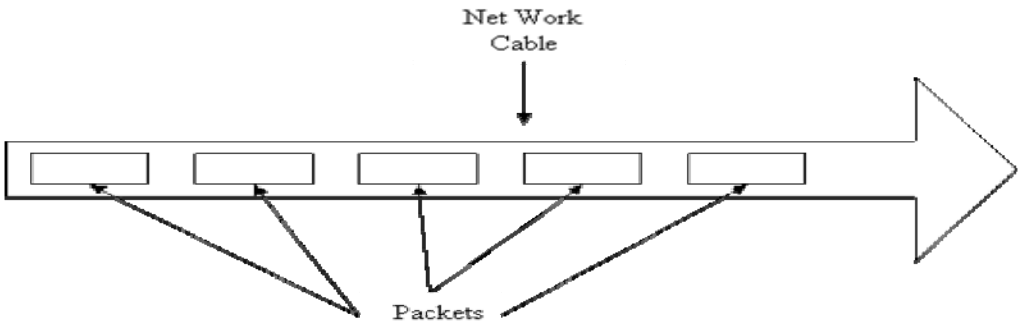
طریقه ارسال سیگنال ها

مفاهیم مربوط به ارسال سیگنال و پهنای باند

پهنای باند (Bandwidth) به تفاوت بین بالاترین و پایین‌ترین فرکانسهایی که یک سیستم ارتباطی می‌تواند ارسال کند گفته می‌شود. به عبارت دیگر منظور از پهنای باند مقدار اطلاعاتی است که می‌تواند در یک مدت زمان معین ارسال شود. برای وسایل دیجیتال، پهنای باند برحسب بیت در ثانیه و یا بایت در ثانیه بیان می‌شود. برای وسایل آنالوگ، پهنای باند، برحسب سیکل در ثانیه بیان می‌شود.

دو روش برای ارسال اطلاعات از طریق رسانه‌های انتقالی وجود دارد که عبارتند از: روش ارسال باند پایه (Baseband) و روش ارسال باند پهن[Broadband] در یک شبکه LAN، کابلی که کامپیوترها را به هم وصل می‌کند، فقط می‌تواند در یک زمان یک سیگنال را از خود عبور دهد، به این شبکه یک شبکه Baseband می‌گوئیم. به منظور عملی ساختن این روش و امکان استفاده از آن برای همه کامپیوترها، داده‌ای که توسط هر سیستم انتقال می‌یابد، به واحدهای جداگانه‌ای به نام Packet شکسته می‌شود. در واقع در کابل یک شبکه LAN،

توالی Packetهای تولید شده توسط سیستم‌های مختلف را شاهد هستیم که به سوی مقاصد گوناگونی در حرکت‌اند.شکلی که در ادامه خواهد آمد، این مفهوم را بهتر نشان می‌دهد.



۲-۱عملکرد یک شبکه packet-switching

برای مثال وقتی کامپیوتر شما یک پیام پست الکترونیکی را انتقال می‌دهد، این پیام به Packetهای متعددی شکسته می‌شود و کامپیوتر هر Packet را جداگانه انتقال می‌دهد. کامپیوتر دیگری در شبکه که بخواهد به انتقال داده بپردازد نیز در یک زمان یک Packet را ارسال می‌کند. وقتی تمام Packetهایی که بر روی هم یک انتقال خاص را تشکیل می‌دهند، به مقصد خود می‌رسند، کامپیوتر دریافت کننده آنها را به شکل پیام الکترونیکی اولیه بر روی هم می‌چینند. این روش پایه و اساس شبکه‌های Packet-Switching می‌باشد. در مقابل روش Baseband، روش Broadband قرار دارد. در روش اخیر، در یک زمان و در یک کابل، چندین سیگنال حمل می‌شوند. از مثالهای شبکه Broadband که ما هر روز از آن استفاده می‌کنیم، شبکه تلویزیون است. در این حالت فقط یک کابل به منزل کاربران کشیده می‌شود، اما همان یک کابل، سیگنالهای مربوط به کانالهای متعدد تلویزیون را بطور همزمان حمل می‌نماید. از روش Broadband به طور روز افزونی در شبکه‌های WAN استفاده می‌شود.

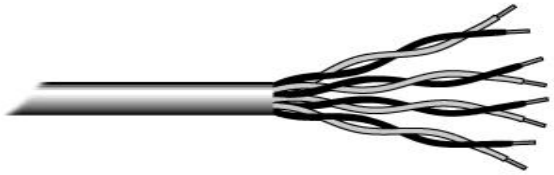
از آنجائیکه در شبکه‌های LAN در یک زمان از یک سیگنال پشتیبانی می‌شود، در یک لحظه داده‌ها تنها در یک جهت حرکت می‌کنند. به این ارتباط half-duplex گفته می‌شود. در مقابل به سیستم‌هایی که می‌توانند بطور همزمان در دو جهت با هم ارتباط برقرار کننده full-duplex گفته می‌شود. مثالی از این نوع ارتباط شبکه تلفن می‌باشد. شبکه‌های LAN با داشتن تجهیزاتی خاص بصورت full-duplex عمل کنند.

- **کابل در شبکه**

در شبکه های محلی از کابل بعنوان محیط انتقال و بمنظور ارسال اطلاعات استفاده می گردد.ازچندین نوع کابل در شبکه های محلی استفاده می گردد. در برخی موارد ممکن است در یک شبکه صرفا" از یک نوع کابل استفاده و یا با توجه به شرایط موجود از چندین نوع کابل استفاده گردد. نوع کابل انتخاب شده برای یک شبکه به عوامل متفاوتی نظیر : توپولوژی شبکه، پروتکل و اندازه شبکه بستگی خواهد داشت . آگاهی از خصایص و ویژگی های متفاوت هر یک از کابل ها و تاثیر هر یک از آنها بر سایر ویژگی های شبکه، بمنظور طراحی و پیاده سازی یک شبکه موفق بسیار لازم است .

- کابل Unshielded Twisted pair)UTP(

متداولترین نوع کابلی که در انتقال اطلاعات استفاده می گردد ، کابل های بهم تابیده می باشند. این نوع کابل ها دارای دو رشته سیم به هم پیچیده بوده که هر دو نسبت 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 : Shielded (روکش دار) و Unshielded (بدون روکش) می باشند. کابل UTP نسبت به کابل STP بمراتب متداول تر بوده و در اکثر شبکه های محلی استفاده می گردد.کیفیت کابل های UTP متغیر بوده و از کابل های معمولی استفاده شده برای تلفن تا کابل های با سرعت بالا را شامل می گردد. کابل دارای چهار زوج سیم بوده و درون یک روکش قرار می گیرند. هر زوج با تعداد مشخصی پیچ تابانده شده (در واحد اینچ) تا تاثیر پذیری آن از سایر زوج ها و یاسایر دستگاههای الکتریکی کاهش یابد.



کابل های UTP دارای استانداردهای متعددی بوده که در گروههای (Categories) متفاوت زیر تقسیم شده اند:

Type	کاربرد
Cat ۱	فقط صوت (کابل های تلفن)
Cat ۲	داده با سرعت ۴ مگابیت در ثانیه
Cat ۳	داده با سرعت ۱۰ مگابیت در ثانیه
Cat ۴	داده با سرعت ۲۰ مگابیت در ثانیه
Cat ۵	داده با سرعت ۱۰۰ مگابیت در ثانیه

مزایای کابل های بهم تابیده :

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

معایب کابل های بهم تابیده :

- تضعیف فرکانس
- بدون استفاده از تکرارکننده ها ، قادر به حمل سیگنال در مسافت های طولانی نمی باشند.
- پایین بودن پهنای باند
- بدلیل پذیرش پارازیت در محیط های الکتریکی سنگین بخدمت گرفته نمی شوند.

کانکتور استاندارد برای کابل های UTP ، از نوع RJ-۴۵ می باشد. کانکتور فوق شباهت زیادی به کانکتورهای تلفن (RJ-۱۱) دارد. هر یک از پین های کانکتور فوق می بایست بدرستی پیکربندی گردند. (RJ:Jack Registered)

- کابل کواکسیال

یکی از مهمترین محیط های انتقال در مخابرات کابل کواکسیال و یا هم محور می باشد . این نوع کابل ها از سال ۱۹۳۶ برای انتقال اخبار و اطلاعات در دنیار به کار گرفته شده اند. در این نوع کابل ها، دو سیم تشکیل دهنده یک زوج ، از حالت متقارن خارج شـده و هـر زوج از یک سیم در مغز و یک لایه مسی بافته شده در اطراف آن تشکیل می گردد. در نوع دیگر کابل های کواکسیال ، به حای لایه مـسی بافتـه شده ، از تیوپ مسی استوانه ای استفاده می شود. ماده ای پلاستیکی این دو هادی را از یکدیگر جدا می کند. ماده پلاستیکی ممکن است بصورت دیسکهای پلاستیکی یا شیشه ای در فواصل مختلف استفاده و مانع از تماس دو هادی با یکدیگر شود و یا ممکن است دو هادی در تمام طول کابل بوسیله مواد پلاستیکی از یکدیگر جدا گردند.

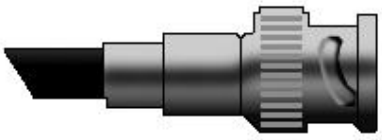
مزایای کابل های کواکسیال :

- قابلیت اعتماد بالا
- ظرفیت بالای انتقال ، حداکثر پهنای باند ۳۰۰ مگاهرتز
- دوام و پایداری خوب
- پایطن بودن مخارج نگهداری
- قابل استفاده در سیستم های آنالوگ و دیجیتال
- هزینه پائین در زمان توسعه
- پهنای باند نسبتا" وسیع که مورد استفاده اکثر سرویس های مخابراتی از جمله تله کنفرانس صوتی و تصویری 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 Neill - Concelman- Bayone) بهمراه کابل های کواکسیال استفاده می گـردد. اغلـب کـارت هـای شـبکه دارای کانکتورهای لازم در این خصوص می باشند.



- فیبر نوری

یکی از جدیدترین محیط های انتقال در شبکه های کامپیوتری ، فیبر نوری است . 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 غلاف نامیده می شود ، استقرار می یابد. ضریب شکست هسته را با M۱ و ضریب شکست غلاف را با M۲ نشان داده و همواره M۲<M۱ است . در این نوع فیبرها ، نور در اثر انعکاسات کلی در فصل مشترک هسته و غلاف ، انتشار پیدا خواهد کرد. منابع نوری در این نوع کابل ها ، دیود لیزری و یا دیودهای ساطع کننده نور می باشند.منابع فوق ، سیگنال های الکتریکی را به نور تبدیل می نمایند.

مزایای فیبر نوری :

- حجم و وزن کم
- پهنای باند بالا
- تلفات سیگنال کم و در نتیجه فاصله تقویت کننده ها زیاد می گردد.
- فراوانی مواد تشکیل دهنده آنها
- مصون بودن از اثرات القاهای الکترو معناطیسی مدارات دیگر
- آتش زا نبودن آنها بدلیل عدم وجود پالس الکتریکی در آنها
- مصون 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 فیبر نوری :

- براحتی 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 دشواری است . در چنین حالتی می توان از فیبرهای ضخیم تر استفاده کرد اما این مسئله باعث تلفات زیاد و کم شدن پهنای باند می گردد.
- از اتصالات T شکل در فیبر نوری نمی توان جهت گرفتن انشهاب استفاده نمود. در چنین حالتی فیبر می بایست بریده شده و یک Detector اضافه گردد. دستگاه فوفق می بایست قادر به دریافت و تکرار سیگنال را داشته باشد.
- تقویت سیگنال نوری یکی از مشکلات اساسی در زمینه فیبر نوری است . برای تقویت سیگنال می بایست سیگنال های توری به سیگنال های الکتریکی تبدیل ، تقویت و مجددا" به علائم نوری تبدیل شوند.

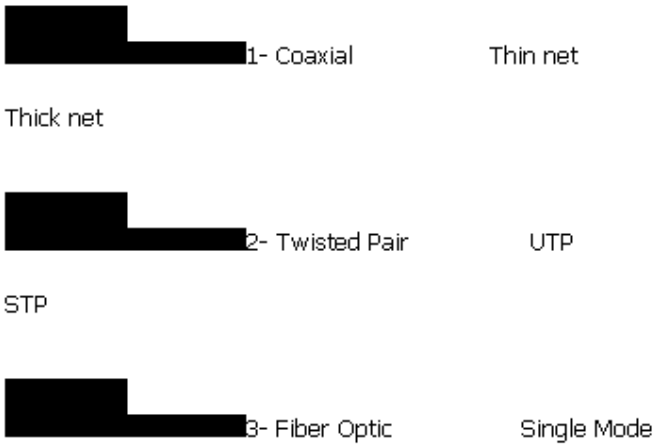
کابل های استفاده شده در شبکه های اترنت

Specification	Cable Type	Maximum length
۱۰BaseT	Unshielded Twisted Pair	۱۰۰ meters
۱۰Base۲	Thin Coaxial	۱۸۵ meters
۱۰Base۵	Thick Coaxial	۵۰۰ meters
۱۰BaseF	Fiber Optic	۲۰۰۰ meters
۱۰۰BaseT	Unshielded Twisted Pair	۱۰۰ meters
۱۰۰BaseTX	Unshielded Twisted Pair	۲۲۰ meters

پیش از اینکه در مورد انواع کابل‌ها و پهنای باند مربوط به آنها، به بحث بپردازیم، ذکر این نکته ضروری است که نوع کابل انتخابی شما بطـور مستقیم به توپولوژی شبکه تان وابسته است. در این قسمت سعی گردیده توپولوژی مناسب با هر نوع کابل ذکر شود.

کابل شبکه، رسانه ای است که از طریق آن، اطلاعات از یک دستگاه موجود در شبکه به دستگاه دیگر انتقال می یابد.انواع مختلفـی از کابلهـا بطور معمول در شبکه های LAN استفاده می شوند. در برخی موارد شبکه تنها از یک نوع کابل استفاده می کند، اما گاه انـواعی از کابلهـا در شبکه به کار گرفته می شود. غیر از عامل توپولوژی، پروتکل و اندازه شبکه نیز در انتخاب کابل شبکه مؤثرند. آگاهی از ویژگیهای انواع مختلف کابلها و ارتباط آنها با دیگر جنبه های شبکه برای توسعه یک شبکه موفق ضروری است.

امروزه سه گروه از کابل‌ها، در ایجاد شبکه مطرح هستند:



کابلهای Coaxial زمانی بیشترین مصرف را در میان کابلهای موجود در شبکه داشت. **چند دلیل اصلی برای استفاده زیاد از این نـوع کابـل وجود دارد:**

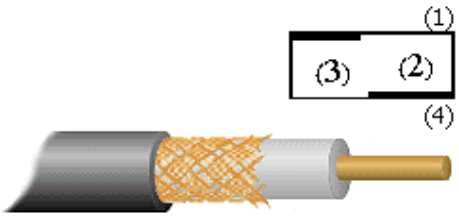
۱- قیمت ارزان آن.

۲- سبکی و انعطاف‌پذیری.

۳- این نوع کابل به نسبت زیادی در برابر سیگنالهای مداخله‌گر مقاومت می نماید.

۴- مسافت بیشتری را بین دستگاههای موجود در شبکه، نسبت به کابل UTP پشتیبانی می‌نماید.

در شکل زیر ساختار کابل Coaxial مشاهده می‌شود:



(۱) Conducting Core یا هسته مرکزی که معمولاً از یک رشته سیم جامد مسی تشکیل می‌گردد.

(۲) Insulation یا عایق که معمولاً از جنس PVC یا تفلون است.

(۳) Copper Wire Mesh که از سیم‌های بافته شده تشکیل می‌شود و کار آن جمع‌آوری امواج الکترومغناطیسی است.

(۴) Jacket که جنس آن اغلب از پلاستیک بوده و نگهدارنده خارجی سیم در برابر خطرات

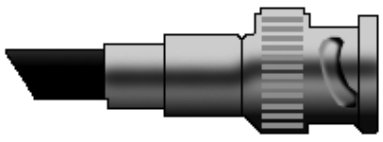
فیزیکی است.

کابل Coaxial به دو دسته تقسیم می‌شود:

۱- Thin net: کابلی است بسیار سبک، انعطاف‌پذیر و ارزان قیمت، قطر سیم در آن ۶ میلیمتر معادل ۰/۲۵ اینچ است. مقدار مسیری که توسط آن پشتیبانی می‌شود ۱۸۵ متر است.

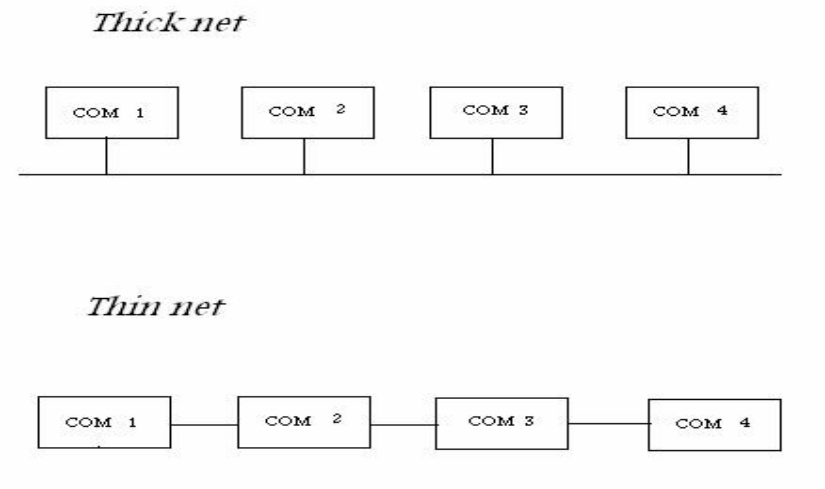
۲- Thick net: این کابل قطری تقریباً ۲ برابر Thin net دارد. کابل مذکور، پوشش محافظی را(علاوه بر محافظ خود) داراست که از جنس پلاستیک بوده و بخار را از هسته مرکزی دور می‌سازد.

رایج‌ترین نوع اتصال دهنده (connector) مورد استفاده در کابل coaxial، (BNC Bayonet-Neill-Concelman) می‌باشد. انواع مختلفی از سازگار کننده‌ها برایBNCها وجود دارند شامل:Barrel connector , Tconnector وTerminator.تصویر زیر یک BNC connector را نشان می دهد:



۳-۲یکBNC connector

در شبکه هایی با توپولوژی اتوبوسی از کابلcoaxial استفاده می‌شود. شکل زیر نمونه استفاده از این نوع کابل در شبکه اتوبوسی است:[۳۳]



۲-۴ استفاده از کابل coaxial در شبکه اتوبوسی

باید دانست که از عبارتهایی مانند "Base۵۱۰ " برای توضیح اینکه چه کابلی در ساخت شبکه بکار رفته استفاده می‌گردد. عبارت مذکور بدان معناست که از کابل coaxial و از نوع Thicknet استفاده شده، علاوه بر آن روش انتقال در این شبکه، روش Baseband است و نیز سرعت انتقال ۱۰ مگابیت در ثانیه ((mbps می‌باشد. همچنین "Base۲۱۰" یعنی اینکه از کابل Thinnet استفاده شده، روش انتقال Baseband و سرعت انتقال ۱۰ مگابیت در ثانیه است.

در طراحی جدید شبکه معمولاً از کابلهای Twisted Pair استفاده می‌گردد. قیمت آن ارزان بوده و از نمونه‌های آن می‌توان به کابل تلفن اشاره کرد. این نوع کابل که از چهار جفت سیم بهم تابیده تشکیل می‌گردد، خود به دو دسته تقسیم می‌شود:

۱-Unshielded Twisted Pair-UTP: کابل ارزان قیمتی است که نصب آسانی دارد و برای شبکه‌های LAN سیم بسیار مناسبی است، همچنین نسبت به نوع دوم کم‌وزن‌تر و انعطاف‌پذیرتر است. مقدار سرعت دیتای عبوری از آن ۴ مگابیت در ثانیه تا ۱۰۰ مگابیت در ثانیه می‌باشد. این کابل می‌تواند تا مسافت حدوداً ۱۰۰ متر یا ۳۲۸ فوت را بدون افت سیگنال انتقال دهد. کابل مذکور نسبت به تداخل امواج الکترومغناطیس (Electrical Magnatic Interference) حساسیت بسیار بالایی دارد و در نتیجه در مکانهای دارای امواج الکترومغناطیس، امکان استفاده از آن وجود ندارد.

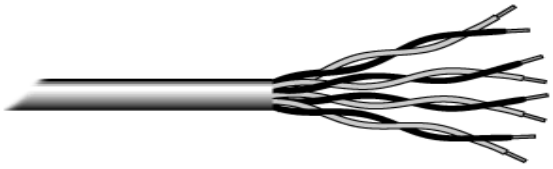
در سیم تلفن که خود نوعی از این کابل است از اتصال دهنده RJ۱۱ استفاده می‌شود، اما در کابل شبکه اتصال دهنده‌ای با شماره RJ۴۵ بکار می‌رود که دارای هشت مکان برای هشت رشته سیم است. در شکل زیر یک connector RJ۴۵ دیده می‌شود.(برگرفته از پانویس قبلی)

connector RJ۴۵ .۵-۲

کابل UTP دارای پنج طبقه مختلف است (که البته امروزه CAT۶ و CAT۷ هم اضافه شده است):

- CAT۱ یا نوع اول کابل UTP برای انتقال صدا بکار می‌رود، اما CAT۲تا CAT۵ برای انتقال دیتا در شبکه‌های کامپیوتری مورد استفاده قرار می‌گیرند و سرعت انتقال دیتا در آنها به ترتیب عبارتست از: ۴ مگابیت در ثانیه، ۱۰مگابیت در ثانیه، ۱۶مگابیت در ثانیه و ۱۰۰مگابیت در ثانیه.

برای شبکه‌های کوچک و خانگی استفاده از کابل CAT۳توصیه می‌شود.



۶-۲UTP کابل

۲- **Shielded Twisted Pair-STP** : در این کابل سیم‌های انتقال دیتا مانند UTP هشت سیم و یا چهار جفت دوتایی هستند. باید دانست که تفاوت آن با UTP در این است که پوسته‌ای به دور آن پیچیده شده که از اثرگذاری امواج بر روی دیتا جلوگیری می‌کند. از لحاظ قیمت، این کابل از UTP گرانتر و از فیبر نوری ارزان‌تر است. مقدار مسافتی که کابل مذکور بدون افت سیگنال طی می کند برابر با ۵۰۰ متر معادل ۱۶۴۰ فوت است.

در شبکه‌هایی با توپولوژی اتوبوسی و حلقه‌ای از دو نوع اخیر استفاده می‌شود. گفته شد که در این نوع کابل، ۴ جفت سیم بهم تابیده بکار می‌رود که از دو جفت آن یکی برای فرستادن اطلاعات و دیگری برای دریافت اطلاعات عمل می‌کنند.

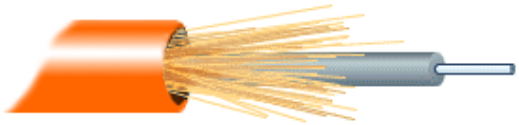
در شبکه‌هایی با نام اترنت سریع (Fast Ethernet) دو نوع کابل به چشم می‌خورد:

- Base TX۱۰۰: یعنی شبکه‌ای که در آن از کابل UTP نوع Cat۵ استفاده شده و عملاً دو جفت سیم در انتقال دیتا دخالت دارند (دو جفت دیگر بیکار می‌مانند)، سرعت در آن ۱۰۰ مگابیت در ثانیه و روش انتقال Baseband است.
- Base T۴۱۰۰: تنها تفاوت آن با نوع بالا این است که هر چهار جفت سیم در آن بکار گرفته می‌شوند.

- کابل فیبر نوری کاملاً متفاوت از نوع Coaxial و Twisted Pair عمل می‌کند. به جای اینکه سیگنال الکتریکی در داخل سیم انتقال یابد، پالسهایی از نور در میان پلاستیک یا شیشه انتقال می‌یابد. این کابل در برابر امواج الکترومغناطیس کاملاً مقاومت می‌کند و نیز تأثیر افت سیگنال بر اثر انتقال در مسافت زیاد را بسیار کم در آن می‌توان دید. برخی از انواع کابل فیبر نوری می‌توانند تا ۱۲۰ کیلومتر انتقال داده انجام دهند. همچنین امکان به تله انداختن اطلاعات در کابل فیبر نوری بسیار کم است. کابل مذکور دو نوع را در بر می‌گیرد:

- ۱- Single Mode: که دراین کابل دیتا با کمک لیزر انتقال می‌یابد و بصورت ۱۲۵/۸,۳ نشان داده می‌شود که در آن ۸,۳ میکرون قطر فیبر نوری و ۱۲۵ میکرون مجموع قطر فیبر نوری و محافظ آن می‌باشد. این نوع که خاصیت انعطاف‌پذیری کم و قیمت بالایی دارد برای شبکه‌های تلویزیونی و تلفنی استفاده می‌گردد.

- ۲- Mode Multi: که در آن دیتا بصورت پالس نوری انتقال می‌یابد و بصورت ۱۲۵/۶۲,۵ نشان داده می‌شود که در آن ۶۲,۵ میکرون قطر فیبر نوری و ۱۲۵ میکرون مجموع قطر فیبر نوری و محافظ آن می‌باشد. این نوع مسافت کوتاهتری را نسبت به Single Mode طی می‌کند و قابلیت انعطاف‌پذیری بیشتری دارد. قیمت آن نیز ارزان‌تر است و در شبکه‌های کامپیوتری استفاده می‌شود. بطورکلی کابل فیبر نوری نسبت به دو نوع Coaxial و Twisted pair قیمت بالایی دارد و نیز نصب آن نیاز به افراد ماهری دارد. شبکه‌های Base FX۱۰۰، شبکه‌هایی هستند که در آنها از فیبر نوری استفاده می‌شود، سرعت انتقال در آنها ۱۰۰ مگابیت در ثانیه بوده و روش انتقال Baseband می‌باشد. امروز، با پیشرفت تکنولوژی در شبکه‌های فیبر نوری می‌توان به سرعت ۱۰۰۰ مگابیت در ثانیه دست یافت. در شکل صفحه بعد یک کابل فیبر نوری مشاهده می‌شود.



۲-۷. فیبر نوری

بطور کلی توصیه‌هایی در مورد نصب کابل شبکه وجود دارد:

- همیشه بیشتر از مقدار مورد نیاز کابل تهیه کنید.

- هر بخشی از شبکه را که نصب می‌کنید، آزمایش نمایید. ممکن است بخشهایی در شبکه وجود

داشته باشند که خارج ساختن آنها پس از مدتی دشوار باشد.

- اگر لازم است بر روی زمین کابل‌کشی نمایید، کابلها را بوسیله حفاظت‌کننده‌هایی بپوشانید.

- دو سر کابل را نشانه‌گذاری کنید.

کارت شبکه (Adapter Network Interface)

کارت شبکه یا NIC ، وقتی که در شیار گسترش کامپیوتر(slot expansion: سوکتی در یک کامپیوتر که برای نگهداری بوردهای گسترش و اتصال آنها به باس سیستم (مسیر انتقال داده‌ها) طراحی می‌شود. شیارهای گسترش روشی برای افزایش یا بهبود ویژگیها و قابلیت‌های کامپیوتر هستند) قرار می‌گیرد، وسیله‌ای است که بین کامپیوتر و شبکه‌ای که کامپیوتر جزئی از آن است، اتصال برقرار می‌نماید.

هر کامپیوتر در شبکه می‌بایست یک کارت شبکه داشته باشد که به باس گسترش سیستم(Expansion Bus System's) اتصال می‌یابد و برای رسانه شبکه (کابل شبکه) به عنوان یک واسطه عمل می‌کند. در برخی کامپیوترها، کارت شبکه با مادربورد یکی شده است، اما در بیشتر مواقع شکل یک کارت گسترش (Expansion Card) را به خود می‌گیرد که یا به ISA سیستم (Industry Standard Architecture: مجموعه مشخصاتی برای طراحی باس‌ها که امکان می‌دهد قطعات بصورت کارت به شیارهای گسترش استاندارد کامپیوترهای شخصی آی‌بی‌ام و سازگار با آنها افزوده شوند)، و یا به PCI (Peripheral Component Interconnect: مجموعه مشخصاتی که توسط شرکت اینتل ارائه شده و سیستم باس محلی را تعریف می‌کند که امکان نصب حداکثر ۱۰ کارت گسترش سازگار با PCI را فراهم می‌کند) متصل می‌گردد.

کارت شبکه به همراه نرم‌افزار راه اندازی (device driver) آن، مسئول اکثر کارکردهای لایه data-link و لایه فیزیکی می‌باشد. کارت‌های شبکه، بسته به نوع کابلی که پشتیبانی می‌کنند، اتصال دهنده‌های (Connectors) خاصی را می‌طلبند. (کابل شبکه از طریق یک اتصال دهنده به کارت شبکه وصل می‌شود) برخی کارت‌های شبکه بیش از یک نوع اتصال دهنده دارند که این شما را قادر می‌سازد که آنها را به انواع مختلفی از کابلهای شبکه اتصال دهید.

عملکردهای اساسی کارت شبکه

کارت شبکه عملکردهای گوناگونی را که برای دریافت و ارسال داده‌ها در شبکه حیاتی هستند، انجام می‌دهد که برخی از آنها عبارتند از:[۴۰]

۱- Data encapsulation: کارت شبکه و درایور (راه‌انداز) آن، مسئول ایجاد فریم در اطراف داده تولید شده توسط لایة شبکه و آماده‌سازی آن برای انتقال هستند.

۲- Signal encoding and decoding: در واقع کارت شبکه طرح کدگذاری لایه فیزیکی را پیاده می‌کند و داده‌های دودویی (binary) تولید شده توسط لایه شبکه را به سیگنال‌های الکتریکی قابل انتقال بر روی کابل شبکه تبدیل می‌نماید. همچنین سیگنال‌های دریافتی از روی کابل را برای استفاده لایه‌های بالاتر به داده‌های دودویی تبدیل می‌سازد.

۳- Data transmission and reception: کارکرد اساسی کارت شبکه، تولید و انتقال سیگنال‌های متناسب در شبکه و دریافت سیگنال‌های ورودی است. طبیعت سیگنال‌ها به کابل شبکه و پروتکل لایه datalink بستگی دارد. در یک LAN فرضی، هر کامپیوتر هم بسته‌های عبوری در شبکه را دریافت می‌کند و کارت شبکه آدرس مقصد لایه datalink را بررسی می‌کند تا ببیند آیا بسته برای کامپیوتر مذکور فرستاده شده یا خیر. در صورت مثبت بودن پاسخ، کارت شبکه بسته را برای انجام پردازش توسط لایه بعدی از کامپیوتر عبور می‌دهد، در غیر اینصورت بسته را به دور می‌افکند.

کارت شبکه قابل نقل و انتقال (Adapters Portable Computer Network)بسیار احتمال دارد که در شبکه شما یک کامپیوتر کیفی و قابل حمل وجود داشته باشد. گستره وسیعی از کارت شبکه‌های مناسب این کامپیوترها قابل دستیابی است. نوعی از کارت شبکه که در کامپیوترهای کیفی استفاده می‌شود عبارتست از: کارت PCMCIA یا همان PC Card.کارت PC در یک شیار و یا در یک جفت شیار موجود در کناره کامپیوتر کیفی جای می‌گیرد. کابل شبکه با استفاده از ابزاری به نام "dongle" به کارت PC متصل می‌شود. کارتهای PC

جز ابزارهای "Plug-and-Play" هستند، و نیز می‌توان در حالیکه کامپیوتر روشن و در حال فعالیت است، آنها را نصب یـا خـارج نمـود و پس از نصب آنها نیازی به restart کردن کامپیوتر نیست.

نصب کارت شبکه

برای نصب کارت شبکه، توصیه می‌شود که از دستورالعمل‌های همراه کارت شبکه خود پیروی کنید. سعی کنید کارت شـبکه‌ای را خریـداری نمائید که این دستورالعمل‌ها را با خود داشته باشد. اگر قصد دارید از کارتی استفاده کنید که آن را از کامپیوتر دیگری بیرون کشیده‌اید و یـا دوستتان آن را به شما داده است، ابتدا در دو روی آن کارت شبکه نام سازنده و شماره محصول را بررسی کنید. حداقل یـافتن نـام سـازنده - درصورت وجود - آسان است. در درجه دوم، به سایت سازنده در وب مراجعه نموده و اطلاعات فنی دربارهٔ آن کارت شبکه جستجو کنید. سعی کنید شماره محصول، مدل و شماره سریال‌ها را تطبیق دهید. راهی دیگر نیز برای شناختن سازندهٔ کارت شـبکه وجـود دارد. بـر روی کـارت شبکه یک کد شش رقمی است که از حروف و عدد تشکیل یافته است مثل OOAOC۹

شماره مذکور به Identifier Organizationally Unique - OUI معروف است. در صورت وجود OUI شما قادر هستید سـازنده کارت و نیز درایور مناسب را بیابید. شـماره OUI توسـط Institute for Electrical and Electronical Engineers - IEEE تخصیص داده می‌شود و از طریق پایگاه داده‌های آن می‌توان به جستجوی نام سازندگان پرداخت. (www.ieee.org) شما می‌بایـست بـه منظور کارکرد صحیح کارت شبکه در کامپیوترتان، یک درایور برای آن داشته باشید. اگر کارت شـبکه‌ای را از یـک تولیـد کننـده معـروف در دست دارید، این شانس وجود دارد که ویندوز درایور آن را در فایلهای خود داشته باشد. اما در غیر اینـصورت یـا بایـد بـه دریافـت درایـور از اینترنت اقدام کنید و یا دیسکت و یا CD-ROM مربوط به کارت شبکه را در اختیار داشته باشید.

برخی کارت‌های شبکه در دیسکت یا CD-ROM خود، یک نصب نرم‌افزاری را پیش‌بینی می‌کنند. سعی کنید این نصب را پیش از رفتن بـه مراحل بعدی کامل کنید. بهترین راه برای پاسخگویی به سؤالاتی که در حین مراحل نصب ممکن است برایتان پـیش بیایـد، مراجعـه بـه وب سایت سازنده است.

فرایند نصب کارت شبکه شامل مراحل زیر است:

- جایدهی فیزیکی کارت در کامپیوتر.
- پیکربندی (Configuring) کارت برای استفاده از منابع سخت‌افزاری مناسب.
- نصب نرم‌افزاری راه‌اندازی (device driver) کارت.

در مراحل نصب و راه‌اندازی شبکه ابتدا می‌بایست مسیر کابل‌کشی که بطور فیزیکی کامپیوترهای شما را به یکدیگر متصل می‌کنـد مـشخص شود. یک روش آسان ولی مؤثر در طراحی مسیر جایگیری کابل‌ها، این است که با در دست داشتن یک دفترچه یادداشت و یک مداد، از یـک مکان دلخواه برای کامپیوتر به سمت مکان دیگر حرکت کنید و بدین شکل یک طرح کلی را از کف خانه خود بدسـت آوریـد؛ همینطـور کـه پیش می‌روید هرگونه مانعی را که می‌بایست فکری برایش کرد یادداشت کنید مثل دیوارها، لوله‌ها، لوازم خانه،درخت‌ها و غیره. اگر قصد دارید کابل‌کشی را بر روی زمین و به موازات لبه‌های دیوار انجام دهید، خوب است کابل‌ها را با استفاده از یک سری نگهدارنده‌هـای پلاسـتیکی بـه

دیوار محکم کنید. در هنگام نصب کابل در اطراف مجراهای گرمایی یا تهویه، سیستم‌های خلاء مرکزی و یا سیستم‌های برق، دقت لازم را بـه عمل آورید.

پس از طراحی مسیر کابل‌ها، به اندازه‌گیری مسیر واقعی آنها بر روی زمین بپردازید. فراموش نکنید که اگر قرار است یک کامپیوتر بر روی میز قرار گیرد لازم است که فاصله پشت کیس کامپیوتر را تا زمین اندازه بگیرید. همچنین اندازه گوشه‌ها و زوایای دیوارها را بیفزایید. پس از پایان این مرحله مجدداً به اندازه‌گیری مسیر کابل‌ها بپردازید و اندازه‌های قبلی خود را بررسی و اصلاح نمائید. آنگاه همهٔ اندازه‌های بدست آمـده را برای بدست آوردن کل طول کابل مورد نیاز، با هم جمع کنید. اندازه‌ای حدود ده فوت را به کل اندازه کابل مـورد نیـاز بیفزاییـد، ایـن طـول اضافی بابت موانعی است که به آسانی قابل اندازه‌گیری نیستند مثل زوایا و گوشه‌ها و یا پله‌ها.

برای ادامه کار شما به کابل Cat۵ به همراه اتصال دهنده‌های RJ-۴۵ نیاز دارید.

به منظور جایدهی فیزیکی کارت شبکه در کامپیوتر، ابتدا کامپیوتر را خاموش کنید. سپس کیس کامپیوتر را باز نمائید و به دنبال یـک شـیار (slot) آزاد بگردید. در بازار هر دو نوع کارت شبکه ISA و PCI وجود دارند و شما قبل از انتخاب کارت باید بررسی کنید کـه کامپیوترتـان چه نوع شیاری را دارا می‌باشد. کارت‌های ISA برای استفاده‌های معمولی شبکه کافی هستند اما امروزه این نوع بـاس‌هـا بـا PCI جـایگزین شده‌اند. در صورتیکه بخواهید کامپیوتر خود را به شبکه‌های پر سرعت (۱۰۰-Mbps) وصل کنید، باس PCI را ترجیح دهید. پـس از خـارج ساختن پوشش شیار، کارت را درون شیار جای دهید و آن را محکم کنید.

در مرحله دوم، پیکربندی کارت شبکه به منظور استفاده آن از منابع سخت‌افزاری خاص صورت می‌گیرد. مثالهایی از این منابع سـخت‌افـزاری عبارتند از:

IRQS –Interrupt requests : یعنی خطوط سخت‌افزاری که وسـایل جـانبی از آنهـا بـرای فرسـتادن سـیگنال‌هـا بـه پردازشـگر و درخواست توجه آن، استفاده می‌کنند.

- Input/Output (I/O) port addresses: این مکان‌ها در حافظه برای استفاده وسایل خاص و به منظور تبادل اطلاعات بـا دیگـر بخشهای کامپیوتر، تخصیص داده می‌شوند.

- Memory addresses: این مکانها از حافظه توسط وسایل خاص و به منظور نصبBIOS با هدف خاصی استفاده می‌شوند.

- access (DMA) channels Direct memory: یعنی مسیرهای سیستمی که وسـایل از آنهـا بـرای تبـادل اطلاعـات بـا حافظـه سیستم استفاده می‌کنند.

کارت‌های شبکه معمولاً از آدرسهای حافظه یا DMA استفاده نمی‌کنند، اما هر کارت شـبکه بـه یـک IRQ و نیـز آدرس I/O پـورت بـرای برقراری ارتباط با کامپیوتر نیاز دارد. وقتی شما کامپیوتر و کارت شبکه‌ای را داشته باشید که هر دو از استاندارد "Plug and Play" (یعنی توانایی یک سیستم کامپیوتری برای پیکربندی خودکار وسیله‌ای که به آن افزوده می‌شود) پشتیبانی کنند، فرایند پیکربندی (مرحله دوم) به طور خودکار انجام می‌گیرد. کامپیوتر کارت شبکه را تشخیص داده،آن را شناسایی مـی‌کنـد، همچنـین منـابع آزاد را مکـان‌یـابی کـرده و بـه پیکربندی کارت شبکه برای استفاده از آنها اقدام می‌کند. عدم وجود مکان "Plug and Play" به معنی آنست که شما باید کارت شبکه را

برای استفاده از IRQ خاص و پورت I/O پیکربندی نمائید و سپس این تنظیمات را با تنظیمات درایور کارت شبکه تطبیق دهید. البته این حالت بیشتر در کارت شبکه‌های قدیمی اتفاق می‌افتد. تقریباً از ویندوز ۹۵ به بعد، ابزارهایی به منظور تشخیص برخوردهای سخت‌افزاری در اختیار کاربران قرار گرفته است. "Device Manager" تنظیمات سخت‌افزاری همه اجزاء را در کامپیوتر فهرست می‌کند، و هنگامیکه در مورد کارت شبکه‌ای که به تازگی نصب شده، یک برخورد سخت‌افزاری پیش می‌آید، این ابزار شما را آگاه می‌سازد. شما می‌توانید از "Device Manager" برای تشخیص اینکه کارت شبکه با چه وسیله‌ای برخورد دارد و چه منبعی احتیاج به تنظیم دارد، استفاده نمائید. مرحله سوم شامل نصب درایوهای کارت شبکه است. نرم‌افزار راه‌اندازی (device driver) بخشی از کارت شبکه است که کامپیوتر را قادر می‌سازد با کارت شبکه ارتباط برقرار کرده و کارکردهای مورد نیاز را اجرا کند. در حقیقت تمامی کارت‌های شبکه برای پشتیبانی از سیستم‌های عامل مطرح، با یک نرم‌افزار راه‌اندازی عرضه می‌شوند، اما در بسیاری از موارد، شما حتی به این نرم‌افزار احتیاج پیدا نخواهید کرد زیرا سیستم‌های عاملی مثل ویندوز، مجموعه‌ای از درایوها را برای مدلهای کارت شبکه پراستفاده و رایج شامل می‌گردند. با وجود امکان "Plug and Play"، علاوه بر تنظیم پیکربندی منابع سخت‌افزاری کارت شبکه، درایور مناسب نیز نصب می‌شود. شما می‌توانید جدیدترین درایورهای مربوط به کارت شبکه را از سایت سازندهٔ آن بدست آورید. البته نصب درایور جدید تنها در صورت بروز مشکل ضرورت پیدا می‌کند.

تنظیمات مربوط به ویندوز برای ایجاد شبکه

حال وقت آن است که در سیستم عامل خود تنظیماتی را انجام دهید تا کامپیوتر شما بتواند جستجو برای کامپیوترهای دیگر و گفتگو با آنها را آغاز کند.

نحوه پیکربندی تنظیمات مربوط به ویندوز در کامپیوتر شما، توسط این مسأله تعیین می‌شود که آیا در شبکه شما Internet sharing وجود دارد یا خیر. در ادامه بر حسب این مسأله دستورالعمل‌های لازم آورده می‌شود:

Settings Non-Internet Sharing Windows

در مورد هر کامپیوتر مراحل زیر را طی کنید:

۱. بر روی آیکن Neighborhood Network بر روی desktop راست کلیک کنید.

۲. Properties را انتخاب کنید.

۳. بر روی Access Control tab کلیک کرده و Share level access را انتخاب کنید.

۴. Identification tab را انتخاب کنید. در اینجا می‌توانید نامی را برای کامپیوتر خود انتخاب کنید.

۵. Configuration tab را انتخاب کنید. از Primary Network Logon، Client for Microsoft Networks را انتخاب کنید.

۶. سپس یک آدرس IP را به کامپیوتر اختصاص دهید، مثلاً O.X. X.۱۹۲,۱۶۸ در هر کامپیوتر منحصر به فرد است و عددی بین ۱ تا ۲۵۴ می‌باشد. در این قسمت عدد Subnet mask را، ۲۵۵,۲۵۵,۲۵۵,۰ بنویسید.

Internet Sharing Windows Setting در مورد هر کامپیوتر مراحل زیر را اجرا کنید:

- در Control Panel، بر روی آیکن Program Add/Remove دو بار کلیک کنید. بر روی Windows setup tab کلیک کنید.

- پس از گذشت چند لحظه از لیست اجزاء، Internet tools را انتخاب کنید.

- سپس Connection Sharing Internet را انتخاب کنید.

- در اینجا CD مربوط به ویندوز مورد نیاز است. آنگاه Internet Connection Sharing Wizard اجرا می‌گردد که پس از پایان آن، کامپیوتر را Restart نمایید.

- می‌توانید از فلاپی دیسکی که در طی مراحل Wizard ایجاد می‌کنید، در مورد کامپیوترهای دیگر شبکه استفاده کنید (در منوی Run در هر یک از آنها و پس از گذاشتن فلاپی در کامپیوتر اینگونه تایپ کنید: a:\icsclset.exe و سپس Enter را فشار دهید)

لازم به ذکر است در صورتیکه بخواهید شبکه خود را از طریق یک Proxy Server به اینترنت متصل کنید می‌بایست آن را خریداری کرده و تنظیمات مربوطه را انجام دهید. فراهم کننده خدمات اینترنت (ISP) شما باید در مورد استفاده از dynamic IP و یا static IP شما را آگاه سازد. در صورت استفاده از static IP، ISP باید در اختصاص IP به شما کمک کند.

مقدمه

امروزه اکثر شبکه هاي کامپيوتري بزرگ و اغلب سيستم هاي عامل موجود از پروتکل TCP/IP ، استفاده و حمايت مي نمايند . TCP/IP ، امکانات لازم بمنظور ارتباط سيستم هاي غير مشابه را فراهم مي آورد. از ويژگي هاي مهم پروتکل فوق ، مي توان به مواردي همچون : قابليت اجراء بر روي محيط هاي متفاوت ، ضريب اطمينان بالا ،قابليت گسترش و توسعه آن ، اشاره کرد . از پروتکل فوق، بمنظور دستيابي به اينترنت و استفاده از سرويس هاي متنوع آن نظير وب و يا پست الکترونيکي استفاده مي گردد. تنوع پروتکل هاي موجو د در پشته TCP/IP و ارتباط منطقي و سيستماتيک آنها با يکديگر، امکان تحقق ارتباط در شبکه هاي کامپيوتري را با اهداف متفاوت ، فراهم مي نمايد. فرآيند برقراري يک ارتباط ، شامل فعاليت هاي متعددي نظير تبديل نام کامپيوتر به آدرس IP معادل ، مشخص نمودن موقعيت کامپيوتر مقصد ، بسته بندي اطلاعات ، آدرس دهي و روتينگ داده ها بمنظور ارسال موفقيت آميز به مقصد مورد نظر ، بوده که توسط مجموعه پروتکل هاي موجود در پشته TCP/IP انجام مي گيرد.

Transmission control protocol / Internet protocol

Microsoft در سیستم عامل هاِی قدِیم از پروتکل NetBUI استفاده مِی کرد ولِی در حال حاضر از Tcp/ip استفاده مِی شود. ip آدرس به صورت دستِی قابل تنظِیم و تغِییر است و از 32 بیت تشکِیل شده. درحال حاضر از tcp/Ip v4 استفاده مِیشود.

هر کدام معادل 1 بایت W.x.y.z

کلاسهاِي آدرس ip :

کلاس A :

اگر سمت چپ ترين بيت سمت چپ ترين بايت 0 باشد اين آدرس IP در کلاس A قرار خواهد داشت.

(01111111).x.y.z
1-127
112.16.8.9

کلاس B :

اگردوبيت سمت چپ سمت چپ ترين بايت 10 باشد اين آدرس IP در کلاس B قرار خواهد داشت.

(01111111).x.y.z
128-191
172.16.8.9

کلاس C:

اگر سه بیت سمت چپ سمت چپ ترین بایت 110 باشد این ادرس IP در کلاس C قرار دارد

(11011111).x.y.z
192-223
EXAMPEL:192.198.0.1

آدرس IP از دو بخش تشکیل شده است

1- NETWORK ID
2- HOST ID

SUBNET MASK : برای ایجاد زیر شبکه از SUB NETMASK استفاده می شود .

SUBNET MASK پیش فرض کلاس A	255.0.0.1
SUBNET MASK پیش فرض کلاس B	255.255.0.0
SUBNET MASK پیش فرض کلاس C	255.255.255.0

توجه: در تخصیص آدرس به کامپیوترها سمت راست ترین بایت 0و 255 نمی تواند باشد.

ایجاد زیر شبکه :

فرض کنید NET ID زیر موجود است

192.168.3

میخواهیم 4 زیر شبکه ایجاد کنیم به طوریکه که در هر کدام از آنها 64 آدرس موجود باشد :

256 / 64 = 4 256 - 64 = 192
SUBNET MASK = 255.255.255.192

حال زیر شبکه های ایجاد شده عبارتند از:

192.168.3.0 _ 192.168.3.63
192.168.3.64 _ 192.168.3.127
192.168.3.128 _ 192.168.3.191
192.168.3.192 _ 192.168.3.255

مثال بعد:
می خواهیم برای آدرس 4.0.37.214 یک SUBNET MASK بنویسیم که در این محدوده HOST 508 وجود داشته باشد :

508/254=2 SUBNAT MASK=255.255.254.0
First address in this range= 4.0.36.1
Last address in this range=4.0.37.254
Broad cast address=4.0.37.255

Register & unregister ip address

برای تخصیص آدرس به کامپیوترها یک سری قوانین وجود دارد:

تمام محدوده آدرسهای زیر unregister هستند:

127.0.0.1 _ 127.255.255.254
10.0.0.1 _ 10.255.255.254
172.16.0.1 _ 172.0.31.254
192.168.0.1 _ 192.168.255.254

می دهد و طبیعتا آدرس ها یی که می دهند غیر از IP شبکه ها آدرس سه موسسه در دنیا وجود دارد که به موارد ذکر شده است.

در واقع ip address هایی که به صورت رجیستر شده هستند توسط سه موسسه به شرکتهایی که در سطح دنیا می خواهند به اینترنت وصل شوند تخصیص داده می شود . نام این موسسه ها در زیر آمده است

1- ARIN 2- APNIC 3-RIPE

به شرکتی که IP address ها را می گیرد LIR گفته میشود:

Ip address هایی که به صورت رجیستر هستند در اینترنت مسیر یابی می شوند. اما ip address هایی که به صورت un register هستند دراینترنت مسیریابی نمی شوند یعنی کسی از خارج با آنها نمی تواند ارتباط داشته باشد اما خودشان به صورت داخلی با یکدیگر ارتباط دارند.

دستورping:

این دستور به این منظور به کارمی رودکه ببینیم یک کامپیوتر راه دوربه شبکه دسترسی دارد یا نه.

Ipconfig:

برای پیداکردن ip آدرس کامپیوترمان کافی است در command تایپ کنیم ipconfig .

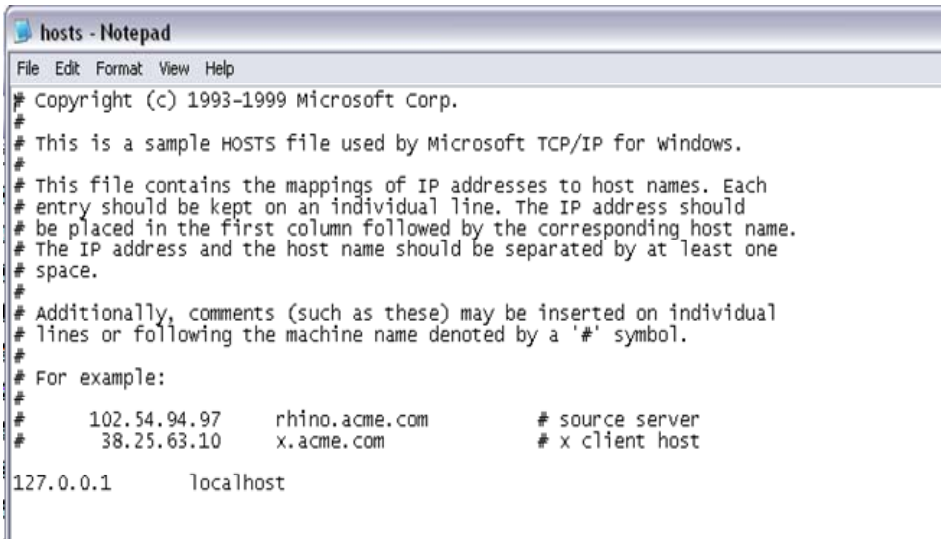
فایل Hosts :

امروزه از این فایل استفاده کمی می شود اما دربعضی مواردبخصوص برای خرابکاری از این فایل استفاده می شود . برای دسترسی به این فایل درگزینه RUN تایپ کنید :

```
Notepad %systemroot%\system32\drivers\etc\hosts
```

هکرها ازاین فایل در زمینه نابودکردن سایت و یا دربکارانداختن ویروس یاب ها استفاده می کنند.

وقتی شما در برنامه کاوشگر اینترنت نام یک سایت را به منظور دسترسی به آن تایپ می کنید در ابتدا این فایل مورد جستجو قرار می گیرد زیرا اگر آدرس آن سایت در این فایل موجود باشد کامپیوتر شما دیگر برای به دست آوردن آدرس آن نیاز ندارد به سراغ DNS SERVER برود و در نتیجه سریع تر به آن سایت دسترسی پیدا خواهد کرد .



:Workgroup

شبکه یا تحت **workgroup** ایجاد می شود یا تحت **Microsoft .domain** پیشنهاد می کند اگر در شبکه تعداد حداکثر **10** کامپیوتر وجود داشته باشد بهتر است این کامپیوتر ها تحت **workgroup** شبکه شوند .در این حالت بانک اطلاعاتی **username** و **password** ها در خود کامپیوتر قرار دارد.بطور مثال اگر تعداد **5**کاربر و **10**کامپیوتر داشته باشیم کلا **50**user**و**password باید تعریف کنیم. **user**ها و **password**ها برروی هرکامپیوتر دریک بانک اطلاعاتی قراردارد که به آن **SAM Database** می گویند.

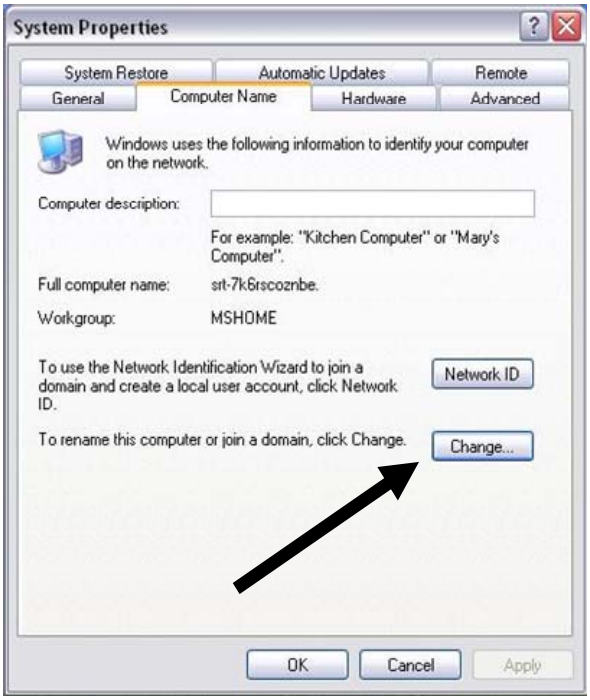
SAM:Security Account Manager

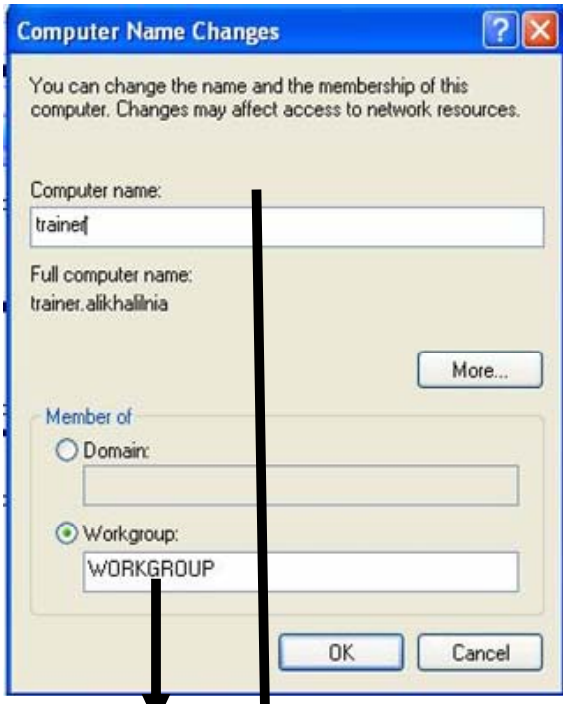
مایکروسافت پیشنهاد می دهد برای تعدادبیشتر از **10** کامپیوتر از **domain** استفاده شود.دراین حالت بانک اطلاعاتی **user**ها و **password**ها در سرور قرار دارد دراینجا هر کس بخواهد با یک کامپیوتر موجود درشبکه **login** شود باید در سرور **account** داشته باشد تا سرور به آن کاربر اجازه **login** دهد.

ایجاد یک workgroup:

برا ی این کار وارد مسیر زیر شده و یک نام برای **workgroup** انتخاب می کنیم :

Control panel ⟶ system ⟶ computer name ⟶ change



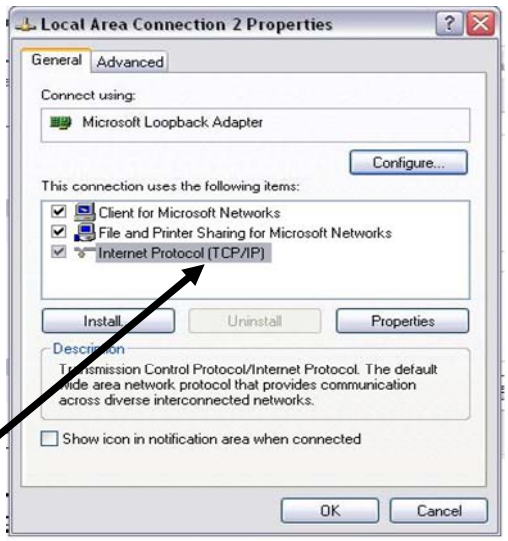


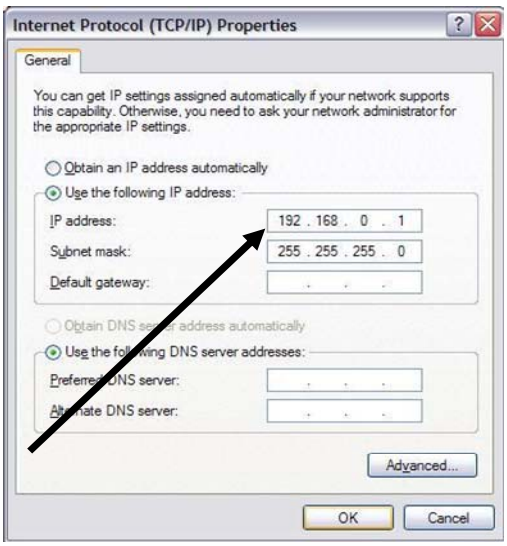
دراین قسمت می توانید نام کامپیوتر و نام workgroup را تغییر دهید

2

حال باید از مسیر زیر کارت شبکه خود را تنظیم نمایید :

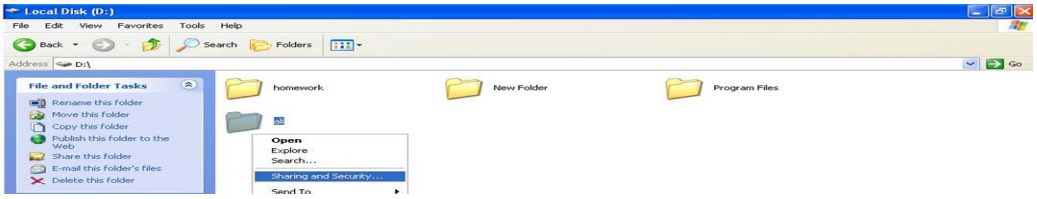
Control panel ⟶ network connection ⟶ local area network

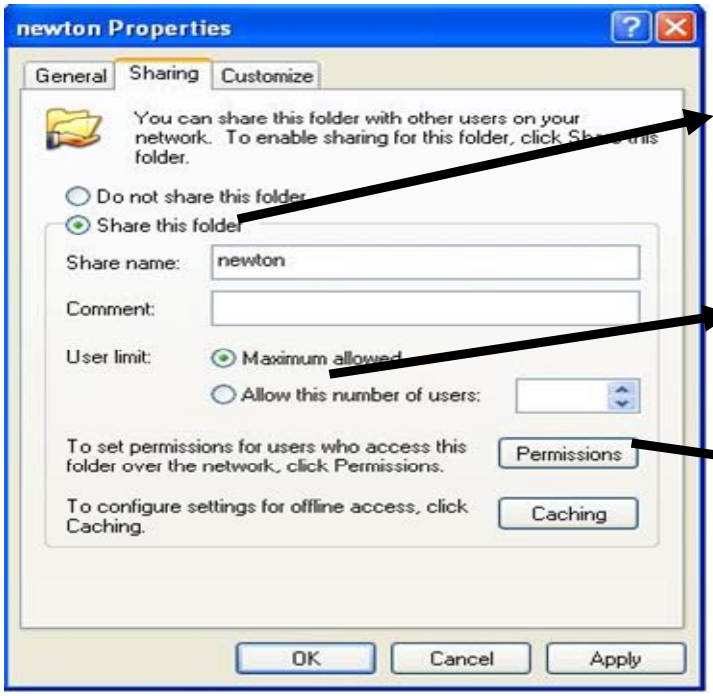




۰ اشتراک گذشتن یک پوشه

برای به اشتراک گذاشتن یک پوشه کافی است بر روی پوشه کلیک راست کرده و گزینه **Sharing and security** را انتخا ب می کنیم .

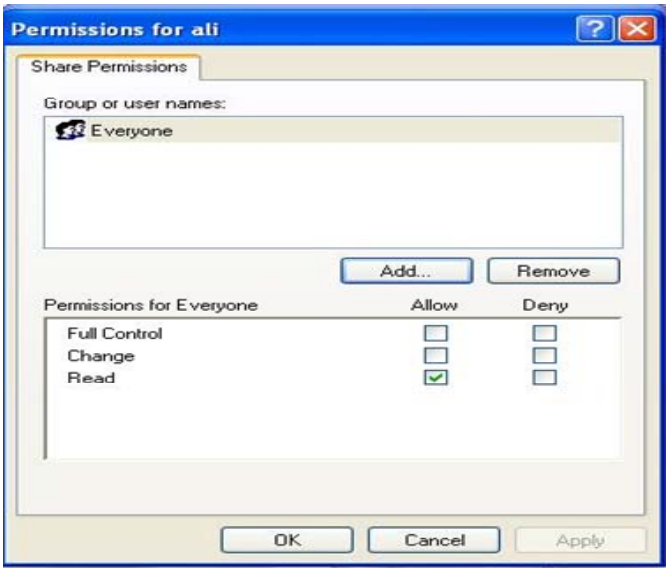




برای به اشتراک گذاشتن پوشه این گزینه باید انتخاب شود.

حداکثر تعداد کاربری که به طور همزمان می توانند از این پوشه به طور مشترک استفاده کنند.

اجازه های دستیابی



Read

Display Folder Names,File Names,FileData,Run Application

change

Create Folders,Add Files To Folders,Change Data In Files, Change File & Folder

Full control

Change + Take Ownership

به چند طریق می توانیم به یک پوشه که در حالت اشتراک است دسترسی پیدا کرد :

1- unc path

در این روش در گزینه Run تایپ کنید:

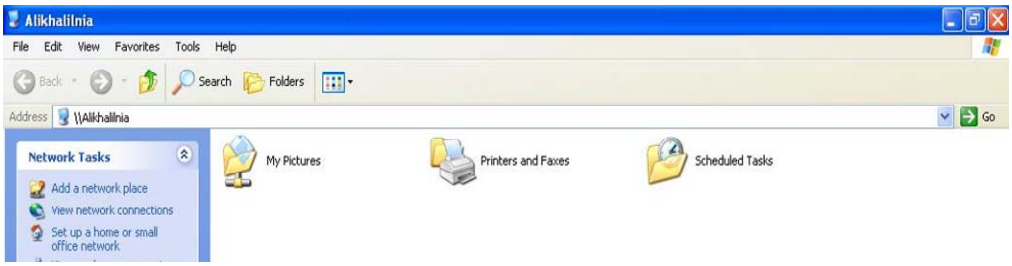
\\computer name or ip address\share folder name

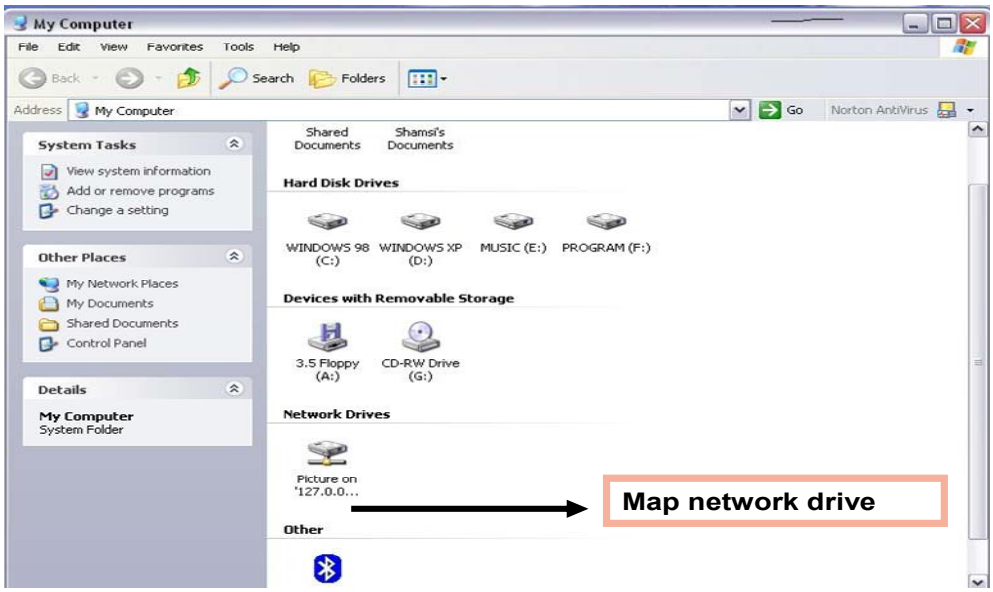
2- map network drive

برای ایجاد آن ابتدا یک پوشه را به حا لت اشترک گذاشته و با روش 1 به پوشه های مشترک کامپیوتر دسترسی پیدا می کنیم . حال بر روی پوشه ای که قصد داریم به حالت Map network drive در آوریم کلیک راست کرده و گزینه Map network drive را انتخاب می کنیم . حال این پوشه به عنوان یک درایو در My computer ظاهر می شو د و شما می توانید اطلاعاتی را که می خواهید در دسترس دیگران باشد در این قسمت قرار دهید .

روش سوم: در قسمت آدرس نرم افزار internet exploer تایپ کنید:

File://computer name or ip address



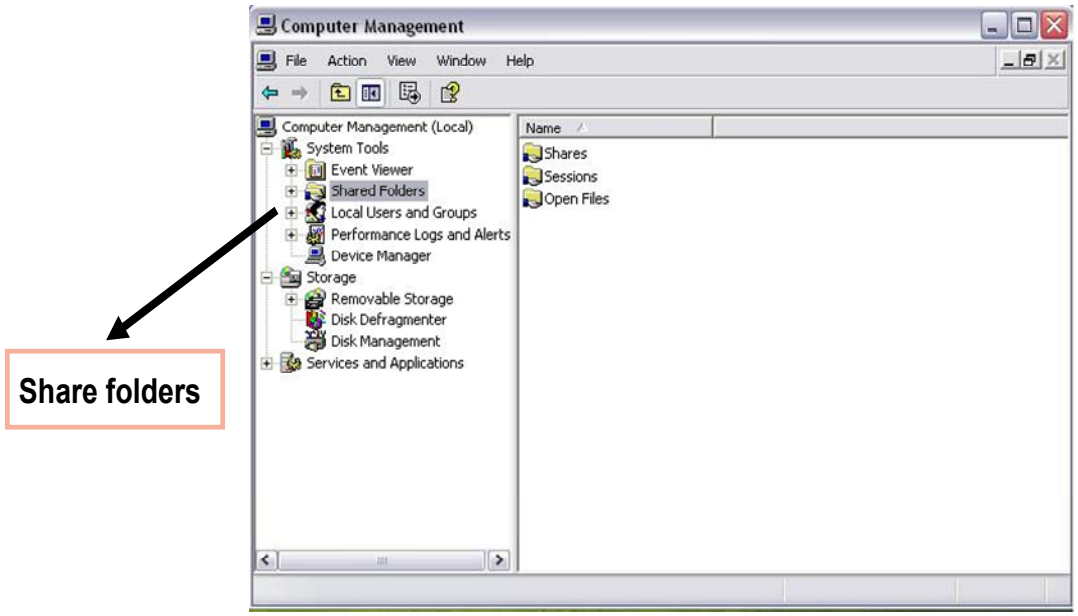


Administrative share

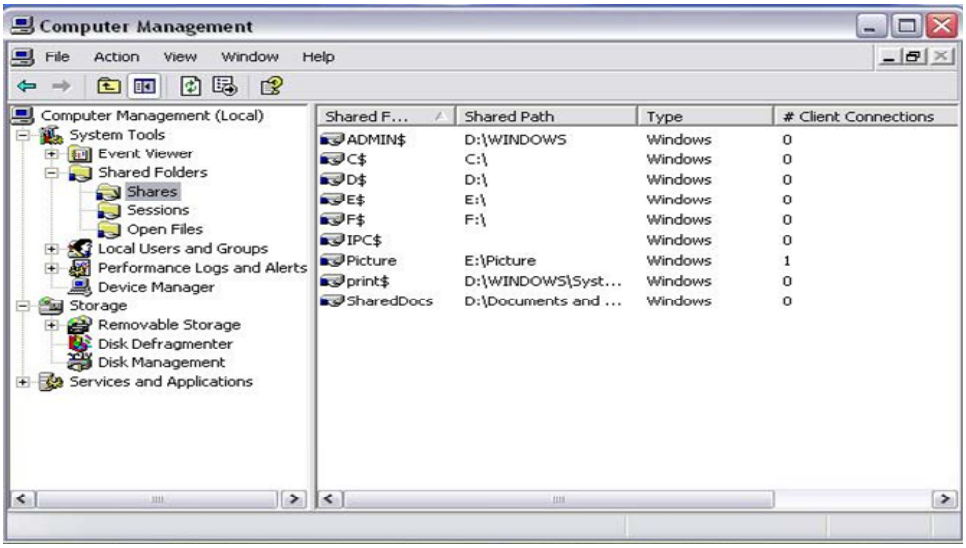
د رون هر کامپیوتر یک سری پوشه های به اشتراک گذاشته شده وجود دارد که ما در اجاد آن نقشی نداریم .به این منابع Administrative share می گویند .برای دسترسی به این منابع مشترک مسیر زیر را دنبال کنید

مشترک

Control panel ⟶ administrative tools ⟶ computer management

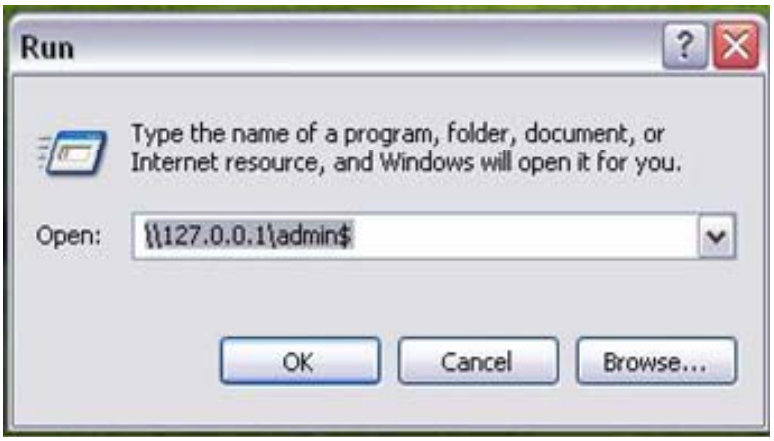


-



حال در سمت راست میتوانید Administrative share را مشاهده کنید

Admin$ اشاره دارد به پوشه ویندوز و C$,D$,E$ و الی آخربه ترتیب به درایوهای C,D,E اشاره دارد . برای دسترسی به موارد فوق مانند زیر عمل کنید :



اگر در آخر نام پوشه به اشتراک گذاشته شده $ قرار دهید کسانیکه از راه دور به کامپیوتر شما متصل می شوند فقط در صورتی می توانند به این پوشه دسترسی داشته باشند که نام پوشه را بدانند.

NTFS = NEW TECHNOLOGY FILE SYSTEM

در یک شبکه هر زمان بخواهیم از امنیت بالایی برخوردار باشیم NTFS استفاده می کنیم

نکته مهم : ویندوز 98 سیستم فایل NTFS را نمی شناسد

در حالتی که سیستم فایل شما FAT است برای تبدیل به NTFS می توانید درایوهای کامپیوتر خود را با سیستم فایل NTFS فرمت کنید که در این صورت تمامی اطلاعات آن درایو از بین خواهد رفت اما با دستور زیر به راحتی و بدون فرمت کردن می توانید درایوهای کامپیوتر را (حتی درایو ویندوز) به سیستم فایل NTFS تبدیل نمود .

CONVERT drive letter: / fs : NTFS

وقتی سیستم فایل کامپیوتر شما NTFS باشد شما به 4 خصوصیت مهم دست پیدا کرده اید :

1. FILE & FOLDER LEVEL SECURITY
2. FILE COMPRESSION

3. DISK QOUTAS

4. FILE & FOLDER ENCRYPTION

1. به این معنی که کاربران نمی توانند به پوشه ها و فایلهای یکدیگر دستزسی داشته باشند مگر در سطحی که به انها اجازه داشته باشد .

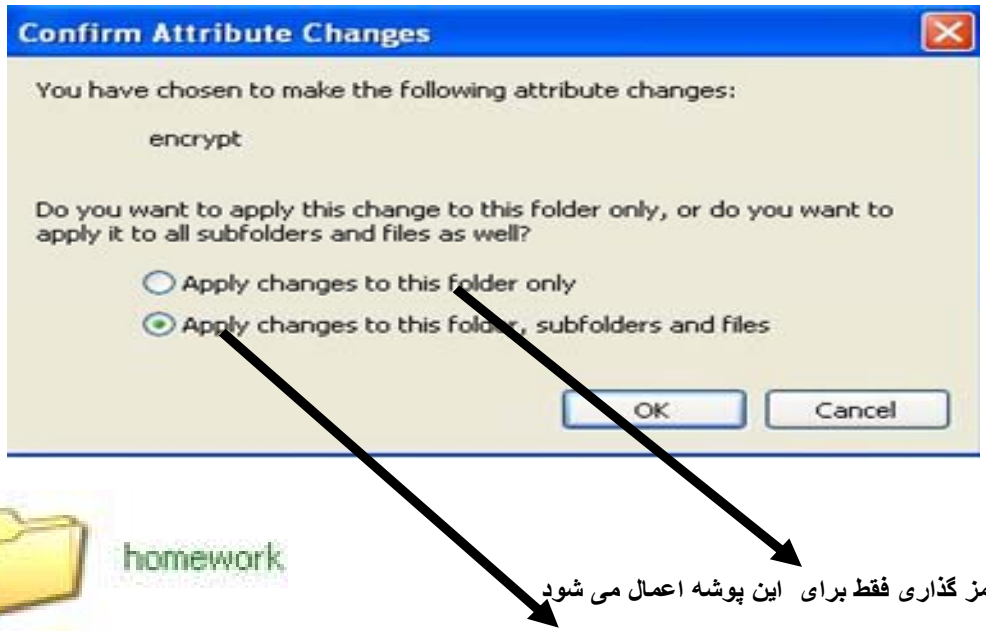
2- می توانیم فایلها را فشرده سازیم .

3. با این خصوصیت می توانیم کاربران را در استفاده از فضای هارد جهت جابجایی فایل ها و پوشه ها محدود کنیم .

4. رمز گذاری فایل ها و پوشه ها به این معنی نیست که بر روی انهاپسورد بگذاریم بلکه به این معنی است که کاربران به فایلها و پوشه هایی که مجاز نیستنند دسترسی نداشته باشند .

FILE & FOLDER ENCRYPTION

از برای رمز گزاری روی فایل کلید سمت راست را زده سپس از آن properties گرفته حال بر روی گزینه Advance کلید کنیددر این صورت شکل زیر را مشاهده خواهید کرد



رمز گذاری فقط برای این پوشه اعمال می شود

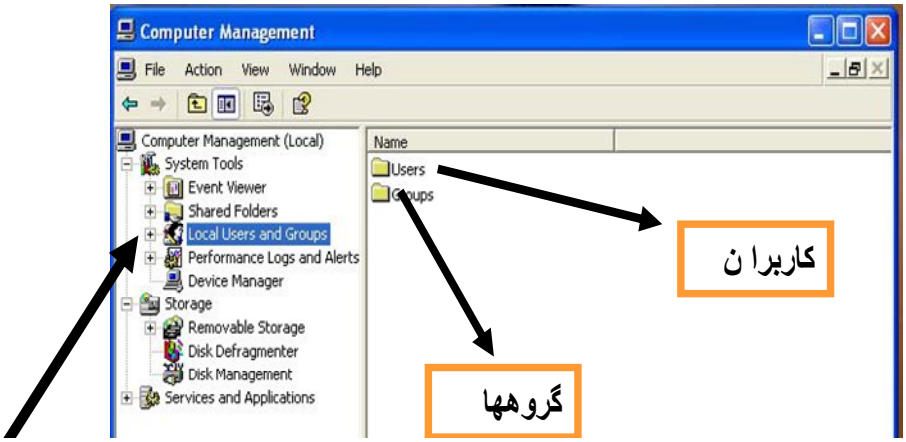
رمزگذاری هم برای این پوشه و هم برای تمام زیر پوشه ها و فایل های درون آنها اعمال می شود

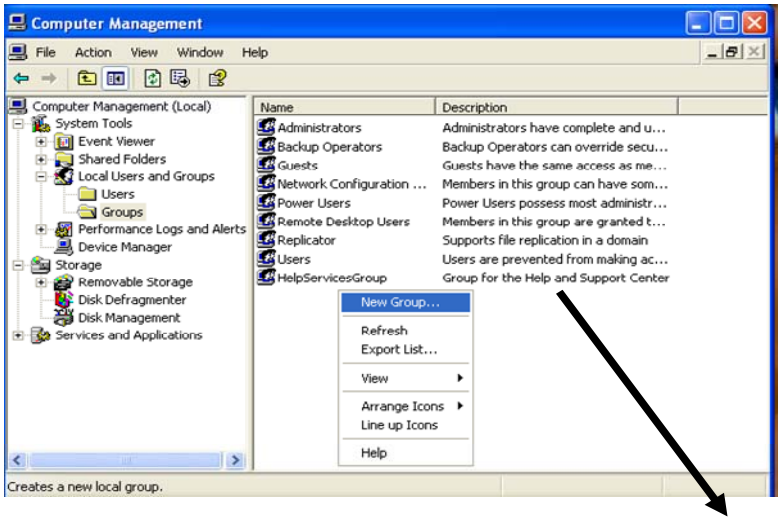
پس از اعمال رمز گذاری بر روی فایل یا پوشه تنها تغییری که ازلحاظ ظاهری ایجاد می شود این است که رنگ اسم پوشه یا فایل سبز خواهد شد.

از اینکه در مورد ایجاد سطوح امنیتی صحبت کنیم ابتدا بایددرمورد گروهها و ایجاد کاربران اطلاعاتی داشته یم .

ی دیدن تمام گروهها و کاربرانی که در کامپیوترمان وجود دارد باید مسیرزیر را دنبال کنیم .

Control panel ⟶ administrative tools ⟶ computer management



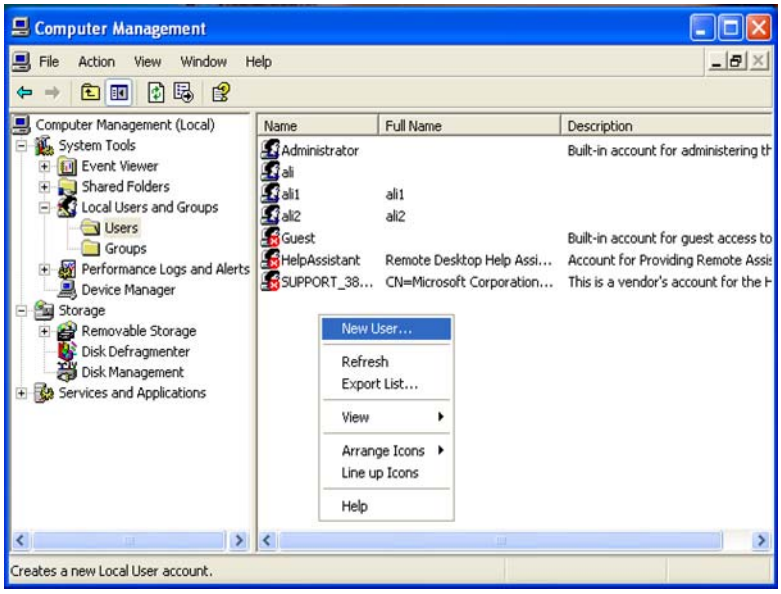


اسامی تمام گروههایی که در حال حاظر در کامپیوتر وجود دارد

برای ایجاد یک گروه بر روی این صفحه کلیک راست کرده و گزینه New Group را انتخاب می کنیم

نکته قابل توجه این است که هر کاربرمی تواند عضو هر کدام از این گروهها باشند .

گروه Administrators دارای بالاترین سطح دسترسی است

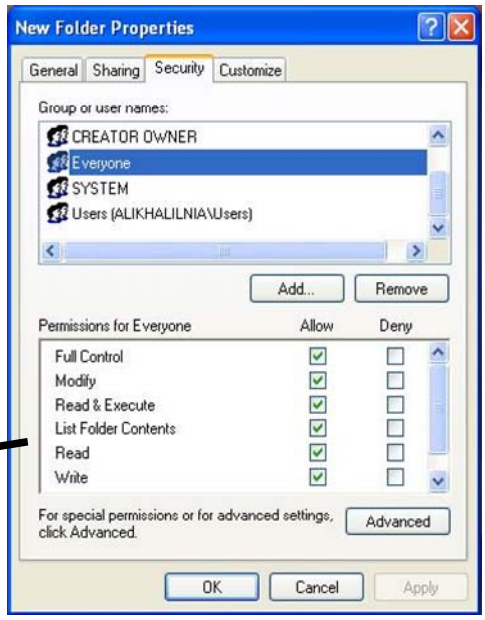


برای ایجاد یک کاربر جدید بر روی این صفحه کلیک راست کرده و گزینه New User را انتخاب می کنیم

وجود گروهها از این جهت ضروری است که ما بتوانیم محدودیتها را به‌ازاء همه کاربران موجود در یک گروه اعمال کنیم.

File & Folder level security

برای این کار بر روی یک فایل یا پوشه کلیک راست کرده و گزینـه **Properties** را انتخاب می کنیم سپس وارد تب **Securiy** می شویم . حال شکل زیر را می توانید مشاهده کنید :



به لیستی که در قسمت بالا مشاهده می شود **Acl** گفته می شود که در آن تمام گروهها و کاربرانی که به نوعی به این پوشه یا فایل سطح دسترسی دارند قرار دارد.

به هر کدام از **Item** های درون این لیست **ACE** گفته می شود.

هر کدام از این گروهها یا کاربران ممکن است سطح دسترسی های‌متفاوتی به پوشه ها یا فایل ها داشته باشند .

Permissions : در ویندوز به اجازه دستیابی بر روی فایل ها و پوشه ها **Permission** می گویند.

سطوح دسترسی که برای یک پوشه وجود دارد به قرار زیر است :

1- read

view files & subfolders in the folder

view attribute ,ownership & permissions

2- write

Create new flle & subfolders within the folder change folder attribute and view folder ownership & permissions

Folder permissions:

3 – list folder contents

view the names of files & subfolder within the folder.

4 – read and excute

travels folders + action permited by read & list folder content.

5 – modify

Delete folder + actions permited by write + read & excute.

6 – full control

Change permission + take ownership.

سطوح دسترسی که برای یک فایل وجود دارد:

File permissions:

1 – read

Read the file , view file attribute,ownership & permission

2- write

Owerwrite the file, change attributes view file owner ship & permission

3- read and excute

Run application +action permited by read permission

4 –modify

Modify and delete the file +action permited by write + read & excute

5 – full control

Modify + chang permission + take ownership

Permission های Ntfs جمع پذیر هستند.

تمام کپی شدن ها اجازه های دستیابی رااز مقصد به ارث می برند.

زمانی که شما بر روی یک پوشه هم Ntfs permission دارید و هم Share folder permission

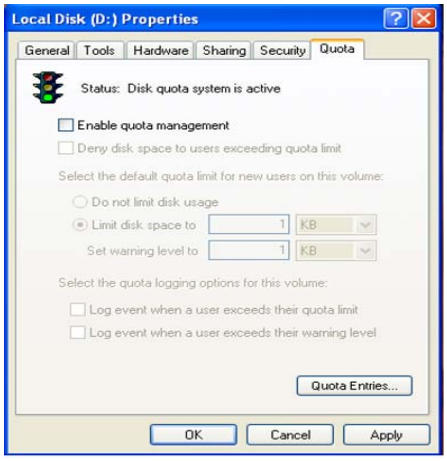
همیشه محدودترین سطح دسترسی اعمال می شود (Most restrictive)

Disk qoutas

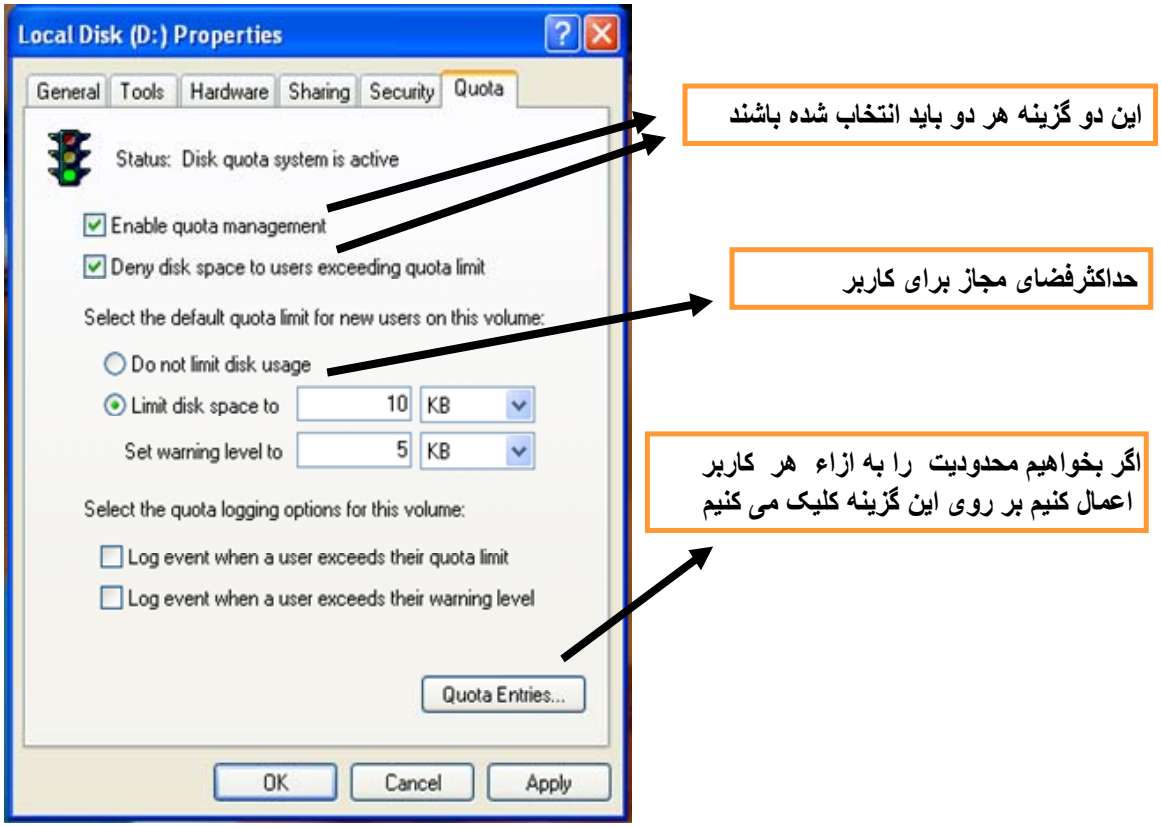
اگر بخواهیم حجم مورد استفاده برای هر کاربر را محدود کنیم از این خصوصیت استفاده میکنیم

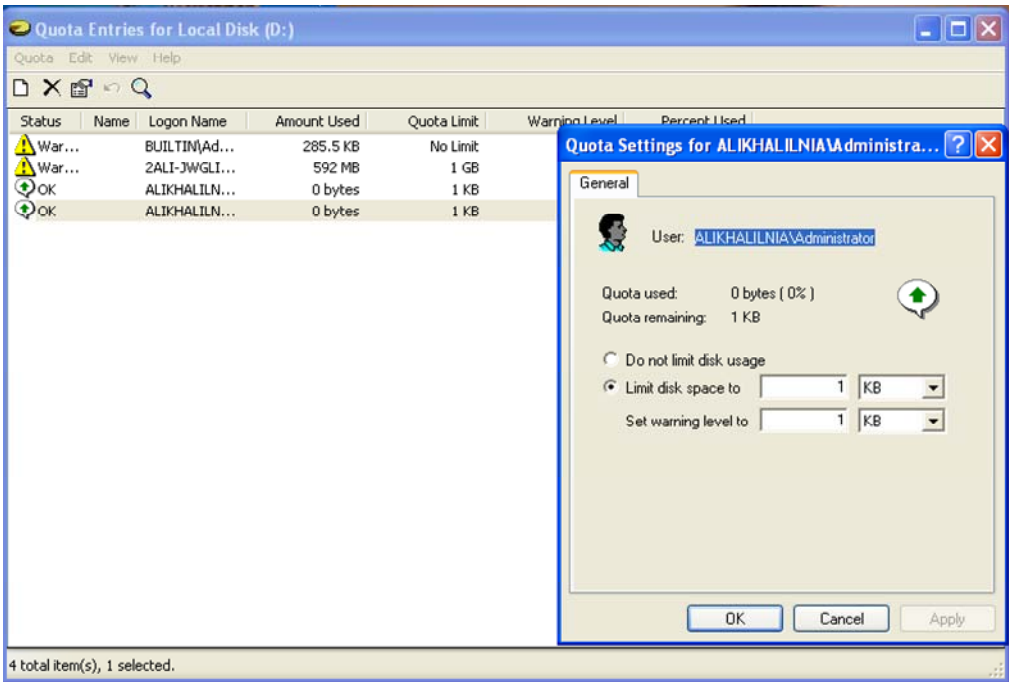
این خصوصیت به ازاء یک یا چند درایو کامپیوتر اعمال می شود.

برای استفاده از این خاصیت بر روی یک درایو کلیک راست کرده و گزینه **Properties** را انتخاب کنید .حال وارد تب **qouta** شوید.



1





حال در این قسمت می توانید بر روی هر کاربر کلیک راست کرده و به ازاء هر کاربر محدودیت ایجاد کنید.

محدودیت فضا برای تمام کاربران به جز Administrator اعمال می شود.

Primary domian contoroler & backup domian contoroler

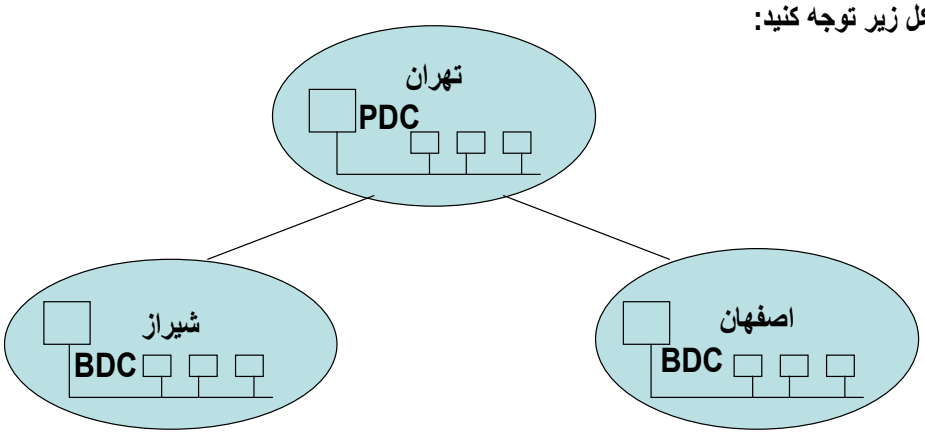
به کامپیوتر سروری که درحالت domian باشد و نرم افزار active directory روی آن نصب شده باشد Domian contoroler گفته می شود.

دونوع domian contoroler وجود دارد : PDC وBDC

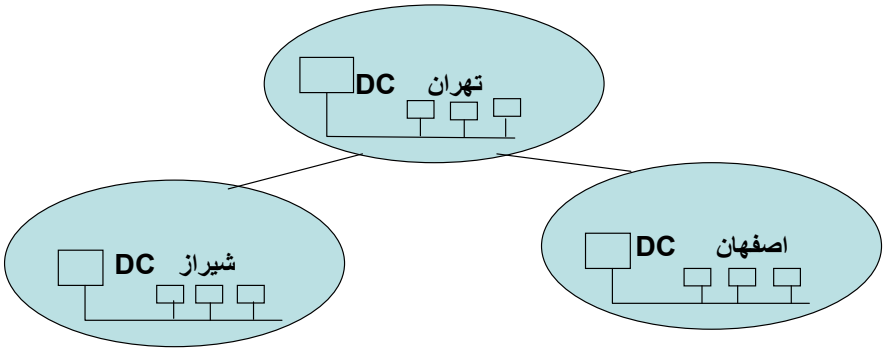
تمام کارها در PDC انجام می گیرد وBDCها ازPDC، backup می گیرند.

همیشه حداکثر یکPDC وجود دارد و تعدادی BDC

به شکل زیر توجه کنید:



درحالتی که از Win nt استفاده شود اگر به هردلیل PDC ازبین برود BDC نمی توانستند کاری انجام دهند برای رفع این مشکل یکی از BDCها خود را بطور اتوماتیک بهPDC تبدیل می کرد.مشکل دیگر دراستفاده ازWIN NT این است که هرکامپیوتری برای دسترسی به منابع شبکه باید توسط PDC مجاز شناخته شود یعنی user و passwordها باید به تهران رفته و در آنجا تایید شود این مسئله باعث ترافیک زیادی در تمامی
شبکه می شود.
در win2000 چیزی به اسم PDC و BDC وجود ندارد تمام کامپیوترها DC هستند.



حال دراینجا تمام کامپیوترها از نزدیکترین DC استفاده می کنند و از خطوط اتصال WAN فقط برای اتصال بین خودDCها استفاده می شود تا DCها بتوانند اطلاعات را بین یکدیگر مبادله کنند.
درشکل قبل مثلا اگر DC موجود درتهران خراب شود کامپیوترهای متصل به آن از نزدیکترین DC مثلا DC موجود دراصفهان استفاده می کنند.

Work Station

تعریف

کامپیوتری که توسط کاربران برای ارسال درخواست به سمت سرور و یا به تنهایی استفاده می گردد را Work station/client می گویند. با توجه به روشی که سیستم نرم افزاری استفاده می کند نوع Work station/client متفاوت می باشد.

در صورتیکه از روشclient-server استفاده شود دراین حال چون بخشی از پردازش بر روی خود client انجام می پذیرد در این حال بایستی client از نظر سخت افزاری و قدرت پردازش می تواند بخوبی ازعهده اجرای برنامه نصب شده بر روی Client برآید. اما در صورتیکه برنامه بصورت Web-Based باشد چون اجرای برنامه بر عهده سرور می باشد در این حال Client از نظر سخت افزاری نیاز به توانائی خاصی ندارد بلکه بیشتر قدرت پردازش درسمت سرور بایستی دیده شود.

این امر منجر به ایجاد رده جدیدی از Clientها تحت نام Thin-Clientها گردیده است.

درصورتیکه Client به تنهائی مورد استفاده قرار بگیرد بایستی مشخصات آن با توجه به نرم افزار مورد استفاده و با دقت انتخاب شود نظیر(Memory,Hard-Cpu).

یک دستگاهWork Station دارای قسمت های اصلی ذیل می باشند :

1- هارد دیسک 2- حافظه 3- برد گرافیکی

4- مادر بورد 5- کارتهای ارتباطی 6- مانیتور

با توجه به وجود مارکهای متنوع با کیفیت های متفاوت، مشخصات استاندارد مربوط به Work Station به شرح زیرپیشنهاد می گردد:

CPU	Pentium4 3.0 GHz L2 Cach 2×1MB FSB 800 MHZ Socket LGA 775 Chipset Intel 955X Express
RAM	512 MB DDR King Stone
HDD	80G Maxtor 7200 RPM IDE/SATA
VGA	RADEON 9000 128M
Motherboard	MSI Or Giga Or Asus
Monitor	LCD Flatron 17" With Speaker
Sound Card	On board
Ethernet Card	On board

کامپیوترها جهت اتصال به هم و استفاده از برنامه های هم و اشتراک برنامه ها از نظر سخت افزاری احتیاج به یک کارت شبکه یا LAN Card دارند. که بطور معمول در بازاردو نوع کارت معمول می باشد. یک قسم آنها کارتهای ۱۰ در ۱۰ بوده و قسم دیگر کارتهای ۱۰ در ۱۰۰ میباشند.

کنترل اتصال کارت شبکه به کامپیوتر

جهت کنترل اتصال درست کارت شبکه به کامپیوتر می‌توانید روی آیکون My Computer کلیک راست نموده و ازقسمت Properties پوشه Device manager را انتخاب نمایید. در بین ابزارهای نصب شده طبق شکل باید در قسمت Network adapters . نام ومشخصات کارت شبکه شما وجود داشته باشد.
اگر در این بخش علامت سوال یا تعجب به شکل زرد رنگ وجود داشته باشد نشان می‌دهد که راه انداز (Driver) کارت شبکه شما ناقص بوده و درست نصب نشده است و بایستی طبق روشهای Hardware settings آنرا برداشته (Remove) و با Refresh . یا از قسمت Add new hardware در بخش کنترل پنل (Control panel) درایور یا راه انداز مناسب و صحیح آنرا نصب نمایید. (برای مشاهده جزئیات نصب یک سخت افزار در صورت لزوم به جزوه آموزش نصب و راه اندازی ویندوز و تعلیمات کامپیوتر از همین سری جزوات مراجعه نمایید)
توجه نمایید که بعد از نصب کارت شبکه، آیکون Network Neighborhood در روی میز کار (Desktop) مشاهده خواهد شد که بعداً به توضیح تنظیم آن خواهیم پرداخت.

همانطور که مشاهده می نمایید در قسمت خارجی این نوع کارتها دو نوع ورودی مشاهده می شود.

از آنجاییکه ما معمولا" دو نوع شبکه BNC و UTP(HUB) را مورد استفاده قرار می دهیم بر روی اکثر کارتها جهت اتصال هر دو نوع رابط وجود دارد.

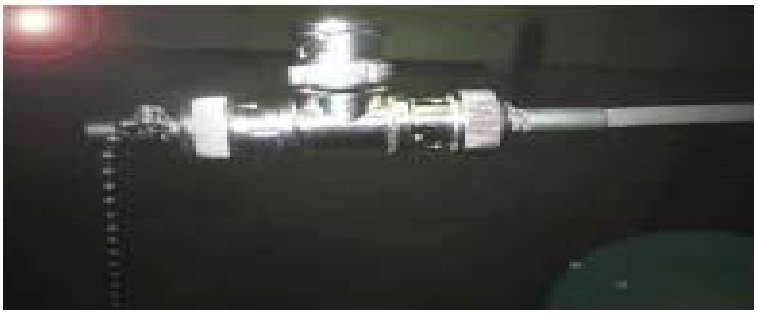
١. شبکه BNC
٢. شبکه Hub

شبکه BNC

در شبکه BNC کامپیوترها بطور سری به هم متصل می شوند و در صورتی که شبکه و سیمهای ارتباطی یک کامپیوتر خراب شود باعث از کار افتادن بقیه شبکه نیز خواهد گردید. رابط BNC که به شکل یک استوانه میباشد دارای دو برآمدگی می باشد(مانند شکل)

در ابتدا و انتهای سیمهای رابط این نوع شبکه یک عدد رابط به نام BNC پرچ شده است که جهت اتصال به سیمها و کامپیوترهای دیگر در سر هر کدام از آنها یک عدد T-Connector قرار می دهند همانطور که در شکل مشاهده می نمایید در سر تی ها برآمدگی و ی شکافها و فرورفتگیهای جهت برقرار اتصال با هم وجود دارد و شما بایست بطور دقیق هنگام اتصال دو قسمت به هم ، شکافها یا فرورفتگی ها را با برآمدگیهای قطعه مقابل جفت نمود و با یک بار چرخش آنرا قفل نمایید تا سفت شود.

در اینگونه شبکه در ابتدا و انتهای کلیه کامپیوتر (کامپیوتر اول و آخر) با دو عدد Terminator بایستی بسته شوند.



تذکر:
اینگونه سیم کشی تا حدود نسبتا" زیادی از نظر هزینه به صرفه بوده و ارزان می باشد ولی کنترل ، نگهداری آن بسیار مشکل بوده ، سرعت کمی را پشتیبانی می کندو بایستی همواره احتیاط را پیشه خود نمود. بسیار دیده شده که این سیمها و رابطها از کناره ها شکسته و قطع می گردند لذا می توانید قسمتهای انتهایی را باچسب محکم و یا سیم محک نمایید تا شکسته و قطع نشود.

Troubleshooting یا رفع اشکالات جزئی:

گاهی در شبکه مشکلاتی پیش می‌آید که شاید با کمی تامل و دقت قابل رفع باشد. اگر شبکه با کامپیوتری از شبکه قطع باشد و بعد از کنترل موارد لازم، در شبکه مطمئن شدید که از لحاظ برنامه و نرم افزار مشکلی ندارید می توانید کنترلهای زیر انجام دهید:

ترمیناتورهای دو سر شبکه را چک و کنترل نمایید و مطمئن شوید که مشکلی نداشته و محکم متصل باشند.

تی کانکترها متصل بوده و شیلد سیمی قطع نباشد.

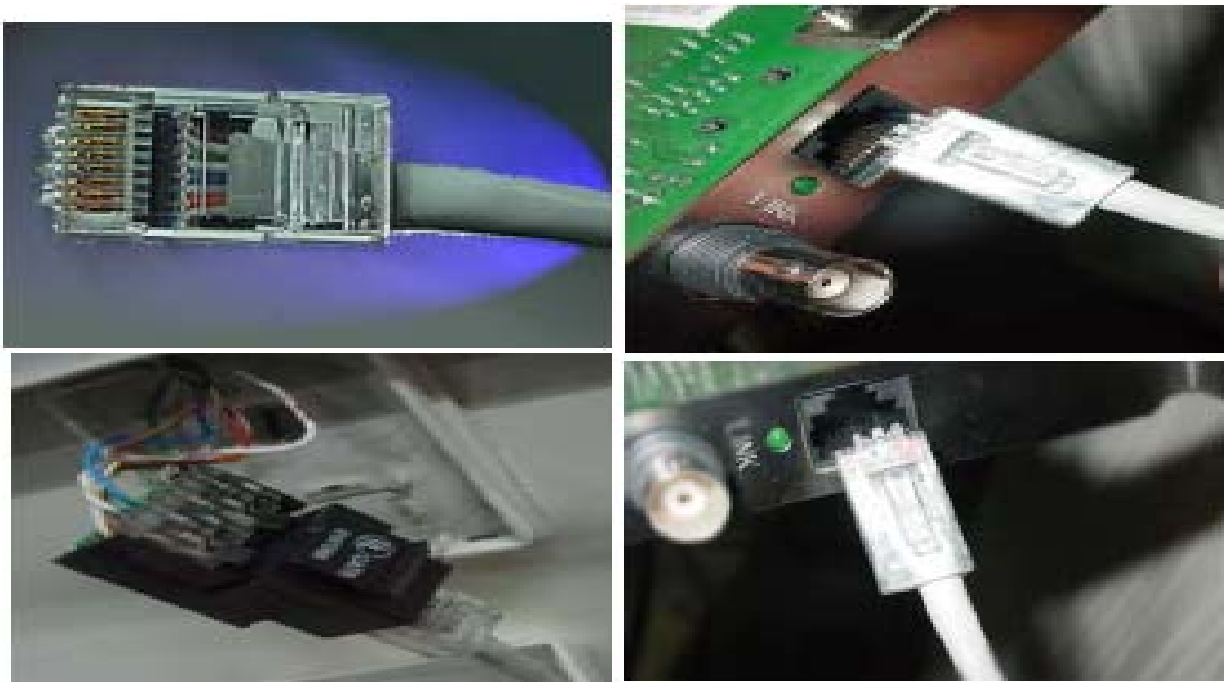
معمولا" بر اثر کشیدگی سیمها پیچ سر سیمها جدا می‌شود در صورت مشاهده و شک ، یک سیم سالم را با آن تعویض کنید.

ترمیناتور انتهایی دستگاه آخری را باز نموده و به دستگاه دومی وصل کرده و با رفع اشکال و اتصال دو دستگاه اولی ، سپس دستگاه سومی و الی آخر مشکل را(که می تواند حاصل از سیم، تی‌کانکتر و یا ترمیناتور باشد) یافته و رفع نموده و در صورت لزوم قطعه مربوطه را تعویض نمایید.

جهت تست سالم بودن سیمها در صورت لزوم می‌توانید علاوه بر تست آنها مابین دو دستگاه سالم از اهم متر نیز استفاده نمایید.

شبکه Hub

اساً یکی از مطمئن ترین و بهترین سیستم شبکه بندی ، شبکه Hub می باشد. در اینگونه شبکه از طریق سیمهای رابط به یک Hub متصل می شوند. در این سیستم بر عکس شبکه BNC اگر کامپیوتری قطع شود فقط آن قطع بوده و بقیه سیستم مختل نشده و شبکه برقرار است. رابط اینگونه شبکه ها سیمهایی است که به سر آنها یک عدد Anj 45 پیچ گردیده است که با رنگهای خاصی جهت گرفتن و فرستادن اطلاعات مشخص شده است.



این رابطها به کارت شبکه کامپیوتر وصل بوده و طرف دیگر آنها به سوکتهای دیواری (Facepalte) و یا مستقیما" به هاب متصل می شوند.

کابلها این سیمها به یک دستگاه به نام Hub متصل میشوند

بر روی این دستگاه فعالیت دستگاهها با چراغهای چشمک زن مشخص می شود و در صورت عدم فعالیت می توان از عدم اتصال آن آگاهی پیدا نمود و در جهت رفع عیب آن بر آمد.

Email address: Asl_Hoseini@yahoo.com

شبکه های بی سیم WirelessNetworking

مفاهیم و تعاریف

وقتی از شبکه اطلاع‌رسانی سخن به میان می‌آید، اغلب کابل شبکه به عنوان وسیله انتقال داده در نظر گرفته می‌شود. در حالیکه چندین سال است که استفاده از شبکه سازی بی‌سیم در دنیا آغازگردیده است. تا همین اواخر یک LAN بی‌سیم با سرعت انتقال پایین و خدمات غیرقابل اعتماد و مترادف بود، اما هم اکنون تکنولوژی‌های LAN بی‌سیم خدمات قابل قبولی را با سرعتی که حداقل برای کاربران معمولی شبکه کابلی پذیرفته شده می‌باشد، فراهم می‌کنند.

WLANها (یا LANهای بی‌سیم) از امواج الکترومغناطیسی (رادیویی یا مادون قرمز) برای انتقال اطلاعات از یک نقطه به نقطه دیگر استفاده می‌کنند. امواج رادیویی اغلب به عنوان یک حامل رادیویی تلقی می‌گردند، چرا که این امواج وظیفه انتقال انرژی الکترومغناطیسی از فرستنده را به گیرنده دورتر از خود بعهده دارند. داده هنگام ارسال برروی موج حامل رادیویی سوار می‌شود و در گیرنده نیز به راحتی از موج حامل تفکیک می‌گردد. به این عمل مدولاسیون اطلاعات به موج حامل گفته می‌شود. هنگامیکه داده با موج رادیویی حامل مدوله می‌شود، سیگنال رادیویی دارای فرکانس‌های مختلفی علاوه بر فرکانس اصلی موج حامل می‌گردد. به عبارت دیگر فرکانس اطلاعات داده به فرکانس موج حامل اضافه می‌شود. در گیرنده رادیویی برای استخراج اطلاعات، گیرنده روی فرکانس خاصی تنظیم می‌گردد و سایر فرکانس‌های اضافی فیلتر می‌شوند.

۸-۲ تصویر یک [WLAN]

در یک ساختار WLAN، یک دستگاه فرستنده و گیرنده مرکزی، Access Point(AP) خوانده می‌شود. AP با استفاده از کابل شبکه استاندارد به شبکه محلی سیمی متصل می‌گردد. در حالت ساده، گیرنده AP وظیفه دریافت، ذخیره و ارسال داده را بین شبکه محلی سیمی و WLAN بعهده دارد. AP با آنتنی که به آن متصل است، می‌تواند در محل مرتفع و یا هر مکانی که امکان ارتباط بهتر را فراهم می‌کند، نصب شود.

هر کاربر می‌تواند از طریق یک کارت شبکه بی‌سیم (Wireless Adapter) به سیستم WLAN متصل شود. این کارت‌ها به صورت استاندارد برای رایانه‌های شخصی و کیفی ساخته می‌شوند. کارت WLAN به عنوان واسطی بین سیستم عامل شبکه کاربر و امواج دریافتی از آنتن عمل می‌کند. سیستم عامل شبکه عملاً درگیر چگونگی ارتباط ایجاد شده نخواهد بود.

امروزه استاندارد غالب در شبکه‌های WLAN، IEEE۸۰۲,۱۱ می‌باشد. گروهی که بر روی این استاندارد کار می‌کند در سال ۱۹۹۰ با هدف توسعه استاندارد جهانی شبکه سازی بی‌سیم با سرعت انتقال ۱ تا ۲ مگابیت در ثانیه شکل گرفت. استاندارد مذکور با نام IEEE۸۰۲,۱۱a شناخته می‌شود. استاندارد IEEE۸۰۲,۱۱b که جدیدتر است، سرعت انتقال را تا ۵/۵ و ۱۱مگابیت در ثانیه می‌افزاید.

WLANها از دو توپولوژی حمایت می‌کنند:

- ad hoc topology
- infrastructure topology

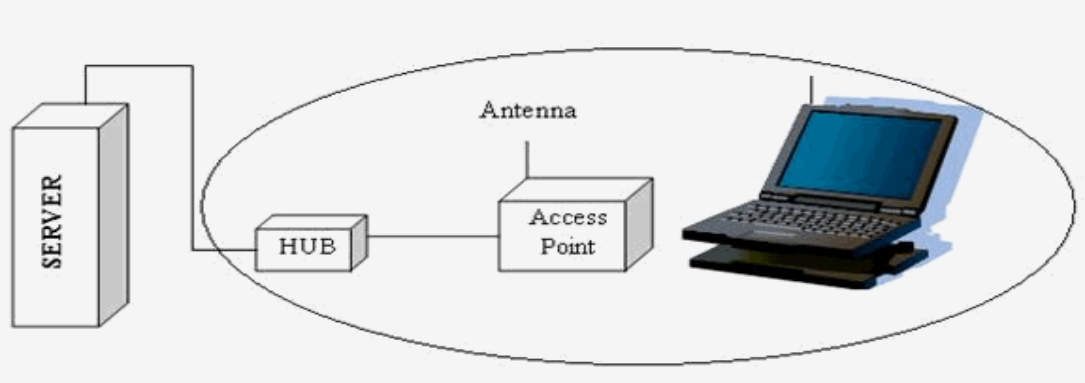
در توپولوژی ad hoc کامپیوترها به شبکه بی‌سیم مجهز هستند و مستقیماً با یکدیگر به شکل Peer- to- peer ارتباط برقرار می‌نمایند.

کامپیوترها برای ارتباط باید در محدوده یکدیگر قرار داشته باشند. این نوع شبکه برای پشتیبانی از تعداد محدودی از کامپیوترها، مثلاً در محیط خانه یا دفاتر کوچک طراحی می‌شود.

"امروزه نوعی از توپولوژی ad hoc به نام "peer-to-peer networking ad hoc" مطرح است. این نوع شبکه که به شبکه "Mesh" نیز معروف است، شبکه‌ای پویا از دستگاههای بی‌سیم است که به هیچ نوع زیرساخت موجود یا کنترل مرکزی وابسته نیست. در این شرایط، دستگاههای شبکه همچنین به مانند گرههایی عمل می‌کنند که کاربران از طریق آنها می‌توانند داده‌ها را انتقال دهند، به این معنی که دستگاه هر کاربر بعنوان مسیریاب و تکرارکننده(Repeater) عمل می‌کند. این شبکه نوع تکامل‌یافته شبکه Point-to-multipoint است که در آن همه کاربران می‌بایست برای استفاده از شبکه دسترسی مستقیم به نقطه دستیابی مرکزی داشته باشند. در معماری Mesh کاربران می‌توانند بوسیلهMulti-Hopping، از طریق گرههای دیگر به نقطه مرکزی وصل شوند، بدون اینکه به ایجاد هیچگونه پیوند مستقیم RF نیاز باشد.بعلاوه در شبکه Mesh در صورتیکه کاربران بتوانند یک پیوند فرکانس رادیویی برقرار کنند، نیازی به نقطه دسترسی(Access Point) نیست و کاربران می‌توانند بدون وجود یک نقطه کنترل مرکزی با یکدیگر، فایلها، نامه‌های الکترونیکی و صوت و تصویر را به اشتراک بگذارند. این ارتباط دو نفره، به آسانی برای دربرگرفتن کاربران بیشتر قابل گسترش است."

توپولوژی infrastructure اصولاً برای گسترش و افزایش انعطاف‌پذیری شبکه‌های کابلی معمولی بکار می‌رود. بدین شکل که اتصال کامپیوترهای مجهز به تکنولوژی بی‌سیم را با استفاده از Access Point به آن امکان می‌سازد. در برخی موارد، یک AP کامپیوتری است که کارت شبکه بی‌سیم را کنار کارت شبکه معمولی - که آن را به یک LAN کابلی متصل می‌کند - دارا می‌باشد. کامپیوترهای بی‌سیم با استفاده از AP به عنوان واسطه با شبکه کابلی ارتباط برقرار می‌کنند. AP اساساً بعنوان یک Translation Bridge عمل می‌کند، زیرا سیگنال‌های شبکه بی‌سیم را به سیگنال‌های شبکه کابلی تبدیل می‌کند. مانند تمام تکنولوژی‌های ارتباطی بی‌سیم، شرایط مسافتی و محیطی می‌توانند بر روی عملکرد ایستگاههای سیار بسیار تأثیر گذار باشند. یک AP می‌تواند ۱۰ تا ۲۰ کامپیوتر را پشتیبانی کند، بسته به

اینکه میزان استفاده آنها از LAN چقدر است. این پشتیبانی تا زمانی ادامه دارد که آن کامپیوترها در شعاع تقریبی ۱۰۰ تا ۲۰۰ فوت نسبت به AP قرار داشته باشند. موانع فیزیکی مداخله کننده این عملکرد را به طرز چشمگیری کاهش می‌دهند.



Cell

۲-۹.شبکهWLANبا یکAccessPoint - AP

در شکل فوق یک Access Point از طریق یک کابل به شبکه LAN متصل شده است. در اینجا وظیفه یک AP دریافت اطلاعات از سرویس گیرنده‌ها (Clients) از طریق هوا و ارسال آن اطلاعات از طریق یک پورت به hub می باشد. AP به عنوان یک پل ارتباطی بین شبکه WLAN و شبکه LAN عمل می‌کند.

ناحیه‌ای که توسط یک AP تحت پوشش قرار می‌گیرد سلول (Cell) نامیده می‌شود. هر ایستگاه در داخل Cell می‌تواند به AP دسترسی پیدا کند. وظیفه یک AP ایجاد هماهنگی بین سرویس گیرندگان (Clients) شبکه WLAN و یک شبکه LAN می‌باشد.[۵۵]

به منظور گسترش بخش بی‌سیم و تحت پوشش قرار دادن سرویس گیرندگان بیشتر، می‌توان از APهای متعدد در مناطق مختلف استفاده کرد، و یا اینکه یک Extension point را بکار گرفت. Extension point، یک تقویت کننده سیگنال‌های بی‌سیم است که به عنوان ایستگاهی بین سرویس گیرندگان بی‌سیم و AP عمل می‌کند. استاندارد IEEE ۸۰۲,۱۱ دو سلول را به عنوان یک BSS (Basic Service Set) در نظر می‌گیرد. اگر شبکه از چند Access Point استفاده کند، APها با یک ستون فقرات بنام DS (Distribution System) به هم اتصال می‌یابند. DS معمولاً یک شبکه کابلی است، اما می‌توان آن را بی‌سیم هم در نظر گرفت.

استاندارد IEEE ۸۰۲,۱۱ از سه نوع سیگنال در لایه فیزیکی پشتیبانی می‌کند:[۵۷]

- (Direct Sequence Spread Spectrum DSSS): یک روش انتقال رادیویی است که در آن سیگنال‌های خروجی با استفاده از یک کد دیجیتال مدوله می‌شوند. در نتیجه هر بیت از دیتا به چند بیت تبدیل می‌شود و سیگنال می‌تواند در فرکانس وسیع‌تر پراکنده شود. استفاده از DSSS به همراه روش CCK (Complimentary Code Keying) باعث می‌شود سیستم‌های IEEE ۸۰۲,۱۱b به سرعت۱۱ مگابیت در ثانیه انتقال دست یابند. در جائیکه شرایط به نحوی است که امکان تداخل، نویزنپذیری یا وجود دستگاههای کاری هم‌فرکانس در منطقه موجود نباشد یا بسیار کم باشد از شیوه DSSS استفاده می‌شود. در این شیوه می‌توان از تمامی عرض باند موجود در طیف گسترده شده (مثلاً MHZ۱۰ یا بیشتر) بهره جست و لذا به شبکه‌ای با سرعت ۱۰ مگابیت در ثانیه یا بالاتر دست یافت. اما در

محیط‌های شلوغ به لحاظ ترافیک امواج مثلاً محیط‌های شهری بزرگ، بکار بردن این تکنولوژی علیرغم وجود کدینگ‌های پیشرفته و تقسیم‌بندی‌های فرکانسی، خالی از بروز تداخل‌ها و یا اشکالات احتمالی نخواهد بود.

FHSS- Frequency Hopping Spread Spectrum : یک روش انتقال رادیویی که در آن انتقال دهنده به طور مداوم تغییرات سریعی را در فرکانس - بر طبق یک الگوریتم موجود - انجام می‌دهد. دریافت کننده برای خواندن سیگنال‌های دریافتی، دقیقاً همان تغییرات را انجام می‌دهد. در IEEE ۸۰۲,۱۱a می‌توان از FHSS استفاده کرد اما سیستم IEEE ۸۰۲,۱۱b از این روش حمایت نمی‌کند.

- Infrared: در ارتباطاتinfrared (مادون قرمز) از فرکانسهای بالا - دقیقا زیر طیف نور مرئی- استفاده می‌شود. در این روش سیگنالها نمی‌توانند از اشیاء و دیوارها عبور کنند. این امر بکارگیری تکنولوژی مادون قرمز را محدود می‌سازد. در فناوری مادون قرمز ارسال کننده و دریافت کننده باید یکدیگر را ببینند(در خط دید یکدیگر باشند) همانند یک کنترل کننده راه دور دستگاه تلویزیون. بطور کلی در ارتباطات داخل ساختمان که فاصله ایستگاهها کم باشد از این روش استفاده می‌شود. در اینجا بجای سیم یا فیبر نوری که رسانه‌های انتقال هستند، از امواج رادیویی یا نور مادون قرمز بعنوان رسانه انتقال استفاده می‌شود. امواج رادیویی بخاطر برد، پهنای باند و پوشش مکانی بیشتر، از نور مادون قرمز کاربرد بیشتری دارند.

در این قسمت به برخی مزایای یک WLAN نسبت به یک شبکه کابلی می‌پردازیم. از WLANها می‌توان در مکانهایی که امکان کابل‌کشی وجود ندارد استفاده کرد و بدون نیاز به کابل‌کشی آنها را گسترش داد. استفاده کننده WLAN می‌تواند کامپیوتر خود را بدون قطع کابل، به هر نقطه از سازمان منتقل کند. با وجود اینکه سخت‌افزار مورد نیاز برای WLAN گرانتر از تجهیزات شبکه سیمی است، ولی بهره‌وری و انعطاف‌پذیری آن باعث می‌شود که در طول زمان قیمت تمام شده کمتر شود، بخصوص در محیطهایی که شبکه مورد نظر پیوسته در حال انتقال و تغییر مداوم است.

سیستمهای WLAN می‌توانند با فناوریهای مختلف شبکه ترکیب شوند و شبکه‌هایی با کاربردها و امکانات خاص را به نحو مطلوبی ایجاد کنند. پیکربندی این شبکه‌ها براحتی قابل تغییر است و این شبکه‌ها می‌توانند از حالت نقطه به نقطه تا شبکه‌هایی با زیرساختار پیچیده با صدها کاربر متحرک گسترش یابند.

در شبکه‌های بی‌سیم مدیران شبکه می‌توانند جابجایی، گسترش و اصلاح شبکه را آسانتر انجام دهند و با استفاده از این سیستم به نصب کامپیوترهای شبکه در ساختمانهای قدیمی و یا مکانهایی که امکان کابل‌کشی در آنها وجود ندارد و نیز مکانهایی که فاصله آنها از یکدیگر زیاد است بپردازند و بدین شکل امکان دسترسی سریع به اطلاعات را فراهم کنند.

پارامترهای مؤثر در انتخاب و پیاده‌سازی یک سیستم WLAN

۱- برد محدوده پوشش: اثر متقابل اشیاء موجود در ساختمان(نظیر دیوارها، فلزات و افراد) می‌تواند بر روی انرژی انتشار اثر بگذارد و در نتیجه برد و محدوده پوشش سیستم را تحت تأثیر قرار دهد. برای سیگنالهای مادون قرمز، اشیای موجود در ساختمان مانعی دیگر بشمار می‌رود و در نتیجه محدودیتهای خاصی را در شبکه بوجود می‌آورد. بیشتر سیستمهای WLAN از امواج رادیویی RF استفاده می‌کنند، زیرا می‌تواند از دیوارها و موانع عبور کند. برد(شعاع پوشش) برای سیستمهای WLAN بین ۱۰ تا ۳۰ متر متغیر است.

۲- سرعت انتقال داده: همانند شبکه‌های کابلی، سرعت انتقال داده واقعی در شبکه‌های بی‌سیم، به نوع محصولات و توپولوژی شبکه بستگی دارد. تعداد کاربران، فاکتورهای انتشار مانند برد، مسیرهای ارتباطی، نوع سیستم WLAN استفاده شده، نقاط کور و گلوگاههای شبکه، از پارامترهای مهم و تأثیرگذار در سرعت انتقال داده بحساب می‌آیند. بعنوان یک مقایسه با مودمهای امروزی(با سرعت ۵۶ کیلو بیت در ثانیه) سرعت عملکرد WLANها در حدود ۳۰ برابر سریعتر از این مودمهاست.

۳- سازگاری با شبکه‌های موجود: بیشتر سیستمهای WLAN با استانداردهای صنعتی متداول شبکه‌های کابلی نظیر Ethernet و Token Ring سازگار است. با نصب درایورهای مناسب در ایستگاههای WLAN، سیستمهای عامل آن ایستگاهها دقیقا مانند سایر ایستگاههای موجود در شبکه LAN کابلی بکار گرفته می‌شود.

سازگاری با دیگر محصولات WLAN: به سه دلیل مشتریان هنگام خرید محصولات WLAN باید مراقب باشند که سیستم موردنظر بتواند با سایر محصولات WLAN تولیدکنندگان دیگر سازگاری داشته باشد:

- ممکن است هر محصول از تکنولوژی خاصی استفاده کرده باشد، برای مثال سیستمی که از فناوری FHSS استفاده کند نمی‌تواند با سیستمی با فناوری DSSS کار کند.

- اگر فرکانس کار دو سیستم با یکدیگر یکسان نباشد،حتی در صورت استفاده از فناوری مشابه، امکان کارکردن با یکدیگر فراهم نخواهد شد.

- حتی تولیدکنندگان مختلف اگر از یک فناوری و یک فرکانس استفاده کنند، بدلیل روشهای مختلف طراحی ممکن است با سایر محصولات دیگر سازگاری نداشته باشد.

۵- تداخل و اثرات متقابل: طبیعت امواج رادیویی در سیستمهای WLAN ایجاب می‌کند تا سیستمهای مختلف که دارای طیفهای فرکانسی یکسانی هستند، بر روی یکدیگر اثر تداخل داشته باشند. با این وجود اغلب تولیدکنندگان در تولید محصولات خود تمهیداتی را برای مقابله با آن بکار می‌گیرند، به نحوی که وجود چند سیستم WLAN نزدیک به یکدیگر، تداخلی در دیگر سیستمها بوجود نمی‌آورد.

۶- ملاحظات مجوز فرکانسی: در اغلب کشورها ارگانهای ناظر بر تخصیص فرکانس رادیویی، محدوده فرکانس شبکه‌های WLAN را مشخص کرده‌اند. این محدوده ممکن است در همه کشورها یکسان نباشد. معمولا سازندگان تجهیزات WLAN فرکانس سیستم را در محدوده مجاز قرار می‌دهند. در نتیجه کاربر نیاز به اخذ مجوز فرکانسی ندارد. این محدوده فرکانس به ISM معروف است. محدوده بین‌المللی این فرکانسها ۹۲۸-۹۰۲ مگاهرتز،۲/۴۸۳-۲/۴ گیگاهرتز، ۵۳۵-۵/۱۵ گیگاهرتز و ۵/۸۷۵-۵/۷۲۵ گیگاهرتز است. بنابراین تولیدکنندگان تجهیزات WLAN باید این محدوده مجوز فرکانسی را در سیستمهای خود رعایت کنند.

۷- سادگی و سهولت استفاده: اغلب کاربران در مورد مزیتهای WLANها اطلاعات کمی دارند. می‌دانیم که سیستم عامل اصولاً به نحوه اتصال سیمی و یا بی‌سیم شبکه وابستگی ندارند. بنابراین برنامه‌های کاربردی بر روی شبکه بطور یکسان عمل می‌نمایند. تولیدکنندگان WLAN ابزار مفیدی را برای سنجش وضعیت سیستم و تنظیمات مورد در اختیار کاربران قرار می‌دهند. مدیران شبکه به سادگی می‌توانند نصب و راه‌اندازی سیستم را با توجه به توپولوژی شبکه موردنظر انجام دهند. در WLAN کلیه کاربران بدون نیاز به کابل‌کشی می‌توانند با یکدیگر ارتباط برقرار کنند. عدم نیاز به کابل‌کشی موجب می‌شود که تغییرات، جابجایی و اضافه کردن در شبکه به آسانی انجام شود. در

نهایت به موجب قابلیت جابجایی آسان تجهیزات WLANمدیر شبکه می‌تواند قبل از اینکه تجهیزات شبکه را در مکان اصلی خود نصب کند، ابتدا آنها را راه‌اندازی کند و تمامی مشکلات احتمالی شبکه را برطرف سازد و پس از تایید نهایی در محل اصلی جایگذاری نماید و پس از پیکربندی، هرگونه جابجایی از یک نقطه به نقطه دیگر را بدون کمترین تغییرات اصلاح نماید.

۸- امنیت: از آنجایی که سرمنشأ فناوری بی‌سیم در کاربردهای نظامی بوده است، امنیت از جمله مقولات مهم در طراحی سیستمهای بی‌سیم بشمار می‌رود. بحث امنیت هم در ساختار تجهیزات WLAN به نحو مطلوبی پیش‌بینی شده است و این امر شبکه‌های بی‌سیم را بسیار امن‌تر از شبکه‌های سیمی کرده است. برای گیرنده‌هایی که دستیابی مجاز به سیگنالهای دریافتی ندارند، دسترسی به اطلاعات موجود در WLAN بسیار مشکل است. به دلیل تکنیکهای پیشرفته رمزنگاری برای اغلب گیرنده‌های غیرمجاز دسترسی به ترافیک شبکه غیرممکن است. عموما گیرنده‌های مجاز باید قبل از ورود به شبکه و دسترسی به اطلاعات آن، از نظر امنیتی مجوز لازم را دارا باشند.

۹- هزینه: برای پیاده‌سازی یک WLAN هزینه اصلی شامل دو بخش است: هزینه‌های زیرساختار شبکه مانند APهای شبکه و نیز هزینه کارتهای شبکه جهت دسترسی کاربران به WLAN.

هزینه‌های زیرساختار شبکه به تعداد APهای موردنیاز شبکه بستگی دارد. قیمت یک AP بین ۱۰۰۰ تا۲۰۰۰ دلار می‌باشد. تعداد APهای شبکه به شعاع عملکرد شبکه، تعداد کاربران و نوع سرویسهای موجود در شبکه بستگی دارد و هزینه کارتهای شبکه با توجه به یک شبکه رایانه‌ای استاندارد حدود ۳۰۰ تا ۵۰۰ دلار برای هر کاربر می‌باشد. هزینه نصب و راه‌اندازی یک شبکه بی‌سیم به دو دلیل کمتر از نصب و راه‌اندازی یک شبکه سیمی می‌باشد:

- هزینه کابل‌کشی و پیدا کردن مسیر مناسب بین کاربران و سایر هزینه‌های مربوط به نصب تجهیزات در ساختمان، بخصوص در فواصل طولانی که استفاده از فیبر نوری یا سایر خطوط گرانقیمت ضروری است، بسیار زیاد است.

- به دلیل قابلیت جابجایی، اضافه کردن و تغییرات ساده در WLAN، هزینه‌های سربار، برای این تغییرات و تعمیر و نگهداری آن بسیار کمتر از شبکه سیمی است.

۱۰- قابلیت گسترش سیستم: با یک شبکه بی‌سیم می‌توان شبکه‌ای با توپولوژی بسیار ساده تا بسیار پیچیده را طراحی کرد. در شبکه‌های بی‌سیم با افزایش تعداد APها یا WBها می‌توان محدوده فیزیکی تحت پوشش و تعداد کاربران موجود در شبکه را تا حد بسیار زیادی گسترش داد. شعاع عملکرد این شبکه تا حدود ۲۰ کیلومتر می‌باشد.

۱۱- اثرات جانبی: توان خروجی یک سیستم بی‌سیم بسیار پایین است. از آنجایی که امواج رادیویی با افزایش فاصله به سرعت مستهلک می‌گردند و در عین حال، افرادی را که در محدوده تشعشع انرژی RF هستند، تحت تاثیر قرار می‌دهند، باید ملاحظات حفظ سلامت با توجه به مقررات دولتی رعایت گردد. با این وجود اثرات مخرب این سیستمها زیاد نمی‌باشد.

Email address: Asl_Hoseini@yahoo.com