آموزشکده فنی و حرفه ای سما یزد

گروه کامپیوتر

پایان نامه جهت اخذ درجه کاردانی پیوسته

رشته کامپیوتر گرایش نرم افزار

عنوان :

شبکه های نظیر به نظیر

استاد مربوطه :

.....

تقدیر و تشکر:

سپاس و ستایش بی حد خدایی را سزاست که انسانی را به زیور هستی بیاراست، آن هـم در عالی ترین و نیکوترین نمود هستی. شنوا و بینایش کرد و به او آموخت آنچه را که بی خبر بود. به نعمت هدایت مفتخرش فرمود و به انسان کرامتی خاص بخشید.

با سپاس فراوان ازاستاد محترم :

جناب آقای فیروزی که مشوق و راهنمای من در انجام این پروژه بودند.

تقدیم به پدر و مادرم:

آنان که وجودم برایشان همه رنج بود و وجودشان برایم مهر.

مویشان سپیدی گرفت تا رویم سپید بماند.

آنان که فروغ نگاهشان، گرمی کلامشان و روشنی رویشان سرمایه های جاودان زندگیم هستند.

در برابر وجود گرامیشان زانوی ادب بر زمین می‌نهم و با دلی مملو از عشق و محبت بر دستانشان بوسه می زنم.

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 کجا شروع کرد؟

-چه پارامترهایی را باید در نظر گرفت ؟

-هدف از برپاسازی شبکه چیست ؟

- انتظار کاربران از شبکه چیست ؟

- آیا شبکه موجود ارتقاء می باید ویا یک شبکه از ابتدا طراحی می شود؟

فهرست مطالب

عنوان

صفحه

فهرست اشکال

مقدمه

انتخاب یک روش p2p معمولا به دلیل یک یا چند مورد از اهداف زیر صورت می گیرد:

تقسیم و کاهش هزینه: راه اندازی یک سیستم متمرکز که بتواند از سرویس گیرنده های زیادی پشتیبانی کند، هزینه زیادی را به سرور تحمیل خواهد کرد. معماری p2p می تواند کمک کند تا این هزیته بین تمام peer ها تقسیم شود. به عنوان مثال در سیستم اشتراک فایل، فضای مورد نیاز توسط تمام peer ها تامین خواهد شد.

- افزایش مقیاس پذیری و قابلیت اعتماد: بدلیل عدم وجود یک منبع قدرتمند مرکزی، بهبود مقیاس پذیری و قابلیت اعتماد سیستم یکی از اهداف مهم به شمار می آید و بنابراین باعث نوآوریهای الگوریتمی در این زمینه می شود.

- افزایش خودمختاری: در بسیاری از موارد کاربران یک شبکه توزیع شده مایل نیستند که متکی به یک سرور متمرکز باشند، چون متکی بودن به یک سرور متمرکز باعث محدود شدن آنها می شود. مثلا در مورد کاربرد اشتراک فایل، کاربران می توانند بطور مستقل فایلهای یکدیگر را دریافت کنند بدون آنکه متکی به یک سرور متمرکز باشند که ممکن است مجوز دریافت فایل را به آنها ندهد.

- گمنامی : این واژه وابسته به همان خودمختاری می شود. کاربران ممکن است مایل نباشند که هیچ کاربر دیگری یا سروری اطلاعاتی در مورد سیستم آنها داشته باشد. با استفاده یک سرور مرکزی، نمی توان از گمنامی مطمئن بود، چون حداقل سرور باید بگونه بتواند سرویس گیرنده را شناسایی کند مثلا با استفاده از آدرس اینترنتی آن. با استفاده از معماری p2p چون پردازش ها به صورت محلی انجام می شود، کاربران می توانند از دادن اطلاعاتی در مورد خودشان به دیگران اجتناب کنند.

- پویایی : فرض اولیه سیستم های p2p این است که در یک محیط کاملا پویا قرار داریم. منابع و نودهای محاسباتی می توانند آزادانه به سیستم وارد و از آن خارج شوند.

فصل اول

شبکه کامپیوتری چیست ؟

۱-۱- شبکه کامپیوتری چیست ؟

اساسا یک شبکه کامپیوتری شامل دو یا بیش از دو کامپیوتر وابزارهای جانبی مثل چاپگرها، اسکنرها ومانند اینها هستند که بطور مستقیم 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 ابزارها وداده ها با 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 استفاده از منابع مشترک گویند.

۲ - کاهش هزینه :

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

۳ - قابلیت اطمینان :

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

۴ - کاهش زمان :

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

۵ - قابلیت توسعه :

یک شبکه محلی می تواند بدون تغییر در ساختار سیستم توسعه یابد 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 " 1[" 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.

۲-۱- مدل های شبکه[۲]

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 .

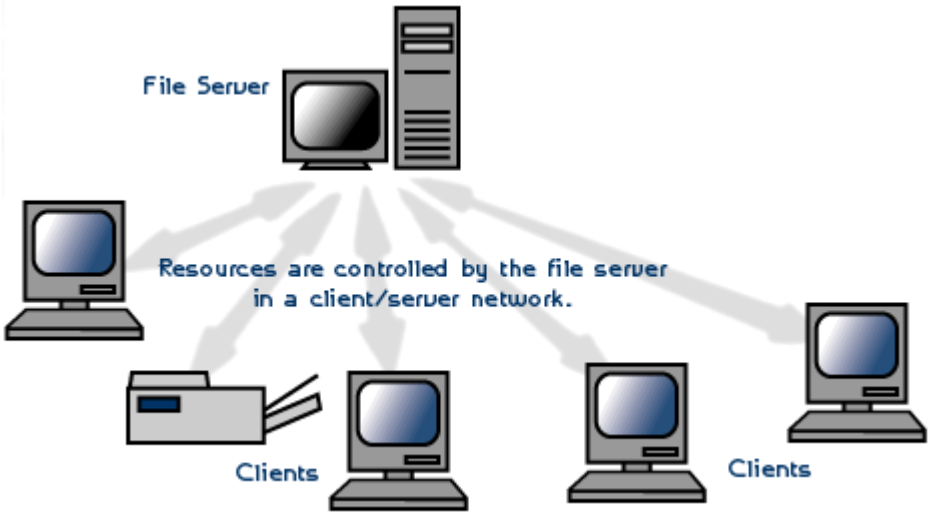
شکل ۱-۱. شبکه نظیر به نظیر

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 اجرای وظیفه محوله ، نتایج حاصل را به ایستگاه در خواست کننده عودت می دهد. در این مدل حجم اطلاعات مبادله شده شبکه ، در مقایسه با مدل مبتنی بر سرویس دهنده کمتر است واین مدل دارای کارایی بالاتری می باشد.



شکل ۲-۱. سرویس دهنده / سرویس گیرنده

هر شبکه اساسا از سه بخش ذیل تشکیل می شود[۳]:

ابزارهایی که به پیکربندی اصلی شبکه متصل می شوند بعنوان مثال : کامپیوتر ها ، چاپگرها، هاب ها " Hubs "

سیم ها ، کابل ها وسایر رسانه هایی که برای اتصال ابزارهای شبکه استفاده می شوند.

سازگار کننده ها" 4["Adaptor] :

که بعنوان اتصال کابل ها به کامپیوتر هستند . اهمیت آنها در این است که بدون وجود آنها شبکه تنها شامل چند کامپیوتر بدون ارتباط 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.

۳-۱- اجزا ءشبکه

اجزا اصلی یک شبکه کامپیوتری عبارتند از :

۱ - کارت شبکه : " 5[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 کامپیوتر های شبکه " اعم از سرویس

دهنده وگیرنده " بصورت سخت افزاری وبرای کنترل ارسال ودریافت داده نصب می گردد.

۲ - رسانه انتقال " 6[" 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 تابیده " Twisted- Pair" ، کابل کواکسیال " Coaxial" وکابل فیبر نوری "Fiber- Optic" .

سیستم عامل شبکه " 7[" NOS- Network Operating System] :

سیستم عامل شبکه برروی سرویس دهنده اجرا می شود و سرویس های مختلفی مانند: اجازه ورود به سیستم "Login" ، رمز عبور "Password" ، چاپ فایل ها " Printfiles"، مدیریت شبکه " Net work management " را در اختیار کاربران می گذارد.

۴-۱- انواع شبکه از لحاظ جغرافیایی

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

شبکه محلی " 8[" LAN= Local Area Network] :

ارتباط واتصال بیش از دو یا چند رایانه در فضای محدود یک سازمان از طریق کابل شبکه وپروتکل بین رایانه ها وبا مدیریت نرم افزاری 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 " 9["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.

۵-۱- ریخت شناسی شبکه " Net work Topology" [۱۰]

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 :

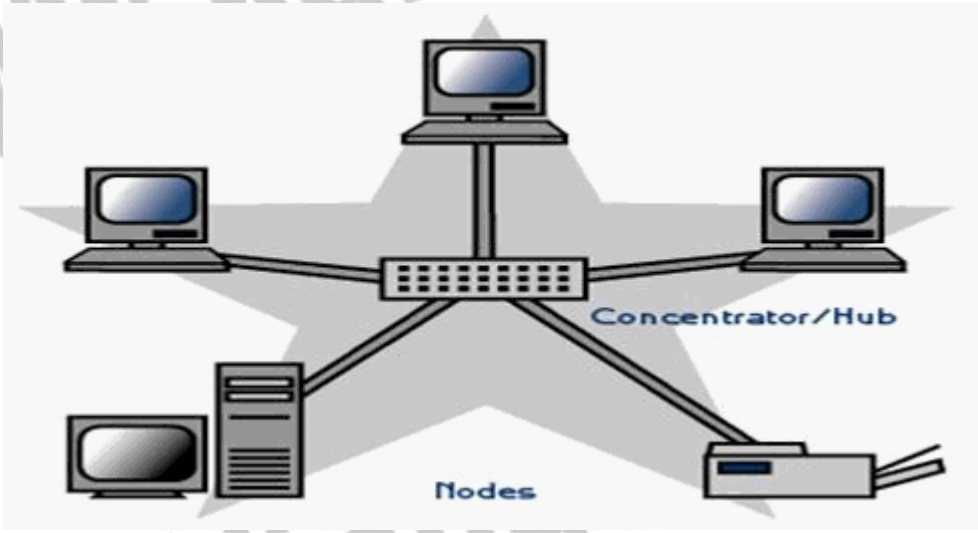
۱ - توپولوژی ستاره ای " 11["Star]:

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 کـامپیوتر شماره سه خواهد فرستاد.

نقاط ضعف این توپولوژی آن است که عملیات کل شبکه به هاب وابسته است. این بـدان معناست که اگر هاب از کار بیفتد، کل شبکه از کار خواهد افتاد . نقـاط قـوت توپولـوژی 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 شـبکه خـارج مـی شود.



شکل ۳-۱. توپولوژی ستاره ای

توپولوژی حلقوی " Ring [12 ":

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

در این توپولوژی کلیه کامپیوتر ها به گونه ای به یکدیگر متصل هستند که مجموعه آنهـا یک حلقه را می سازد. کامپیوتر مبدا اطلاعات را به کـامپیوتری بعـدی در حلقـه ارسـال نموده وآن کامپیوتر آدرس اطلاعات رابرای خـود کپـی مـی کنـد، آنگـاه اطلاعـات را بـه کامپیوتر بعدی در حلقه منتقل خواهد کرد وبهمین ترتیب این روند ادامه پیدا مـی کنـد

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 ".

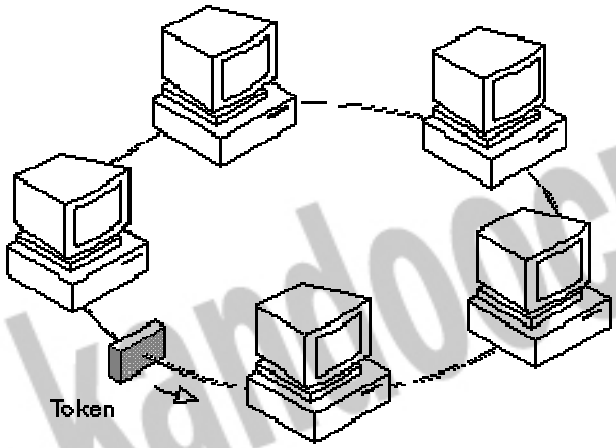
* برای اضافه کردن یک ایستگاه به شبکه باید کل شبکه را متوقف کرد.

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.

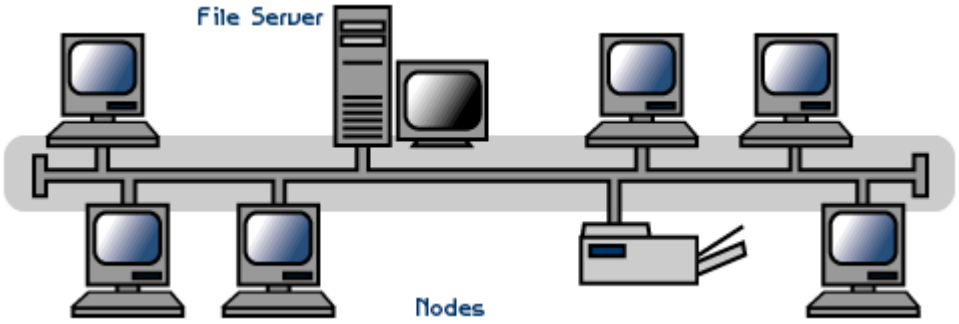


شکل ۴-۱. توپولوژی حلقوی

توپولوژی اتوبوسی " 13["BUS]:

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 متداولترین 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.

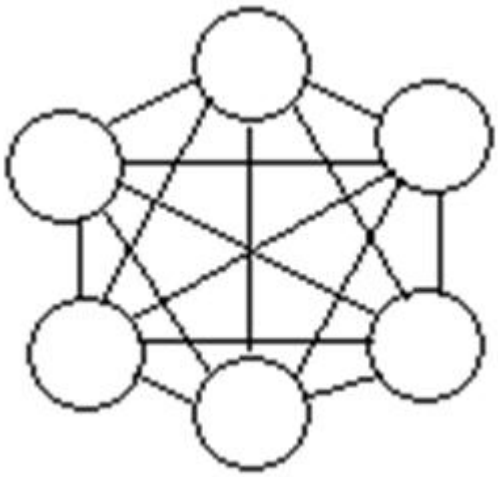


شکل ۵-۱. توپولوژی اتوبوسی

توپولوژی توری " 14["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.

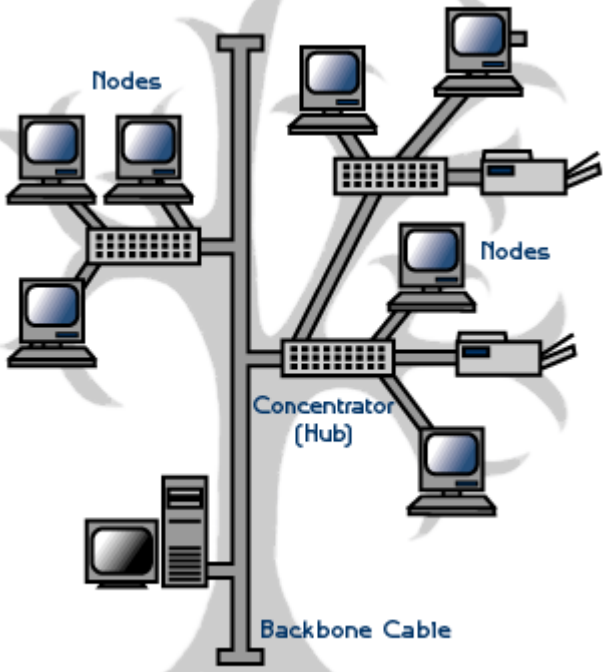
از نقاط ضعف اساسی این توپولوژی آن است که از تعداد زیادی خطوط ارتباطی استفاده می کند، مخصوصا زمانیکه تعداد ایستگاه ها افزایش یابند. به همین جهت این توپولوژی از نظر اقتصادی مقرون به صرفه نیست. برای مثال ، در یک شبکه با صد ایستگاه کاری ، ایستگاه شماره یک نیازمند به نود ونه می باشد. تعداد کابل های مورد نیاز در این توپولوژی با رابطه N(N-1)/2 محاسبه می شود که در آن N تعداد ایستگاه های شبکه می باشد.



شکل ۶-۱. توپولوژی توری

توپولوژی درختی " 15["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.



شکل ۷-۱. توپولوژی درختی

توپولوژی ترکیبی " Hybrid"

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

پروتکل[۱۶] :

برای برقراری ارتباط بین رایانه ها ی سرویس گیرنده و سرویس دهنده قوانین کامپیوتری برای انتقال ودریافت داده مشخص شده اند که به 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. پروتکل تعیین کننده مشخصه های شبکه ، روش دسترسی وانواع فیزیکی توپولوژی ها ، سرعت انتقال داده ها وانواع کابل کشی است .

۶-۱- 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 " 17["Net work]:

" 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 های کوچکتر 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 یعنی این قابلیت که به بررسی وبازبینی بسته ها ومحاسبه بسته های دریافت شده دارد. در ضمن این پروتکل فقط برای استفاده در شبکه اینترنت نمی باشد. بسیاری از سازمان وشرکت ها برای ساخت وزیر بنای شبکه خصوصی خود که از اینترنت جدا می باشد نیز در این پروتکل استفاده می کنند. [۱۸]

- پروتکل سیستم ورودی وخروجی پایه شبکه " Net work basic input/ output[۱۹] System= Net Bios" واسطه یا رابطی است که توسط IBM بعنوان استانداردی برای دسترسی به شبکه توسعه یافت . این پروتکل 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. این سیستم عامل ویژه را Net BIOS می نامند که در حافظه ROM کارت شبکه ذخیره شده است.

BIOS Net همچنین روشی را برای دسترسی به شبکه ها با پروتکل های مختلف مهیا می کند. این پروتکل از سخت افزار شبکه مستقل است . این پروتکل مجموعه ای از فرامین لازم برای در خواست خدمات شبکه ای سطح پایین را برای برنامه های کاربردی فراهم می کند تا 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 که این امتیاز درواقع ایجاد گزینه انتقال استاندارد است و Net BEUI در شبکه های محلی بسیار رایج است. همچنین قابلیت انتقال سریع داده ها را نیز دارد . اما چون یک پروتکل غیر قابل هدایت است به شبکه های محلی محدود شده است.

۷-۱- مدل "OSI Open System Interconnection"[۲۰]

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 :

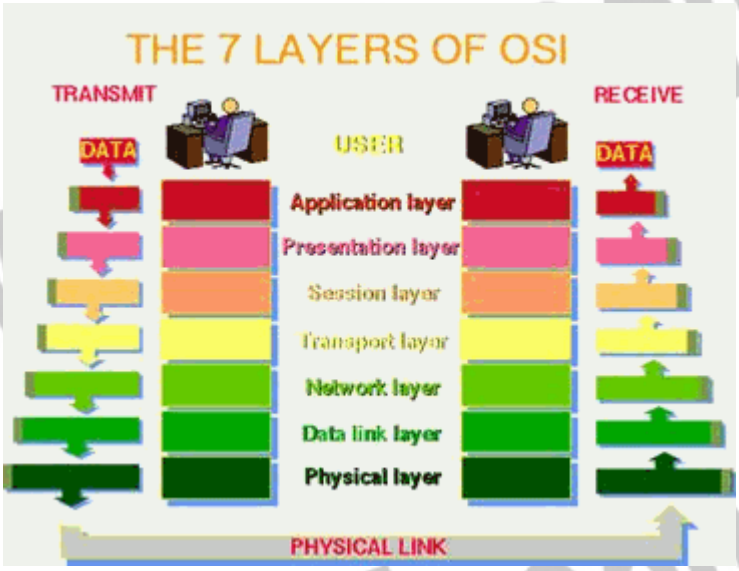
وظیفه برقراری یک ارتباط منطقی بین نرم افـزار هـای دو کـامپیوتر ی کـه بـه یکـدیگر متصل هستند به عهده این لایه است. وقتی که یک ایسـتگاه بخواهـد بـه یـک سـرویس دهنده متصل شود ، سرویس دهنده فرایند برقراری ارتباط را بررسی می کنـد، سـپس از ایستگاه ، درخواست نام کاربر، ورمز عبور را خواهـد کـرد. ایـن فراینـد نمونـه ای از یـک اجلاس می باشد.

۶ - لایه نمایش :

این لایه اطلاعات را از لایه کاربرد دریافـت نمـوده ، آنهـا را بـه شـکل قابـل فهـم بـرای کامپیوتر مقصد تبدیل می کند . این لایه برای انجام این فرایند اطلاعـات را بـه کـدهای ASCII ویا Unicode تبدیل می کند.

۷ - لایه کاربرد :

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



شکل ۸-۱. لایه کاربرد

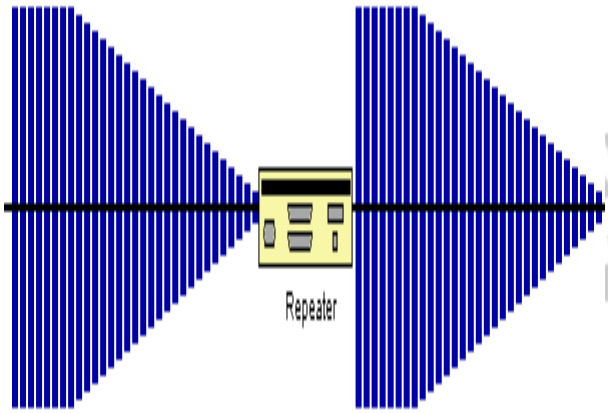
۸-۱- ابزارهای اتصال دهنده : "Connectivity Devices "

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" 21[" 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.



شکل ۹-۱. ابزارهای اتصال دهنده

۲ - هاب ها " 22["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:

شکل ۱۰-۱. هاب

الف - هاب فعال :

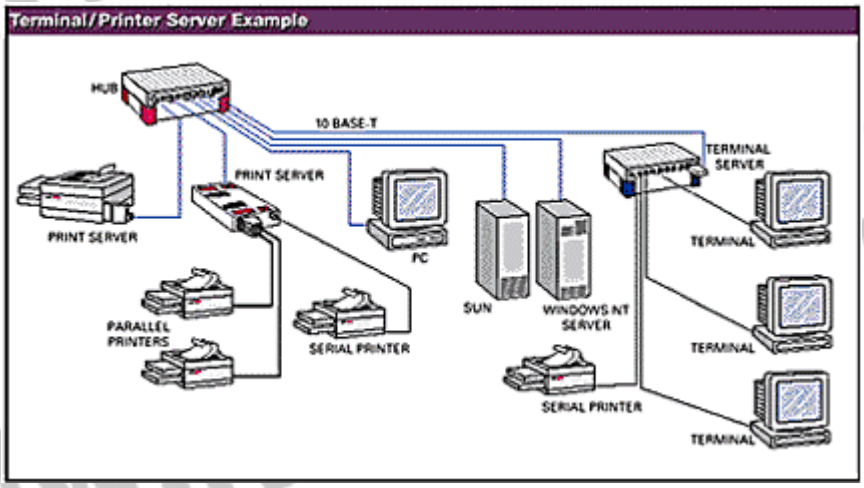
که مانند آمپلی فایر عمل می کند و باعث تقویت مسیر عبور سینگال ها می شود واز تصادم وبرخورد سیگنال ها در مسیر جلوگیری بعمل می آورد . این هاب نسبتا قیمت بالایی دارد.

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.



شکل ۱۱-۱. شبکه ترکیبی

۳ - مسیر یاب ها " 23[" 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 "]۲۴[:

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 "]۲۵[":

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 ریـزی کـرد که فریم های ارسال شده از طرف منابع خاصی را حذف کنند.

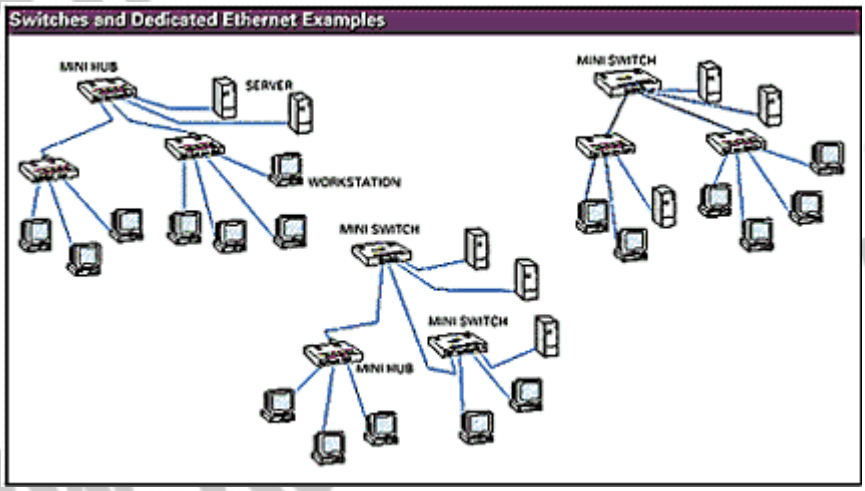
با تقسیم یک شبکه بزرگ به چندین سگمنت واستفاده از یک پل بـرای اتصـال آنهـا بـه یکدیگر ، توان عملیاتی شبکه افزایش خواهد یافت . اگر یک سگمنت شبکه از کار بیفتد ، سایر سگمنت ها ی متصل به پل می توانند شبکه را فعال نگـه دارنـد ، پـل هـا موجـب افزایش وسعت شبکه محلی می شوند.

سوئیچ ها" 26[" Switches].:

سوئیچ نوع دیگری از ابزارهایی است که برای اتصال چند شبکه محلی بـه یکـدیگر مـورد استفاده قرار می گیرد که باعث افزایش توان عملیاتی شبکه می شود. سـوئیچ وسـیله ای است که دارای درگاه های متعدد است که بسته ها را از یـک درگـاه مـی پـذیرد، آدرس مقصد را بررسی می کند وسپس بسته ها را به درگاه مورد نظر " که متعلق بـه ایسـتگاه میزبان با همان آدرس مقصد می باشد" ارسال می کند. اغلب سوئیچ های شـبکه محلـی در لایه پیوند داده های مدل ا اس آی عمل می کند.

سوئیچ ها بر اساس کاربردشان بـه متقـارن "Symmetric" ونامتقـارن " 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 نـوع نامتقـارن این عملکرد بین سگمنت هایی با پهنای باند متفاوت انجام می شود.



شکل ۱۲-۱. سوئیچ ها

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.

فصل دوم

مفاهیم مربوط به ارسال سیگنال

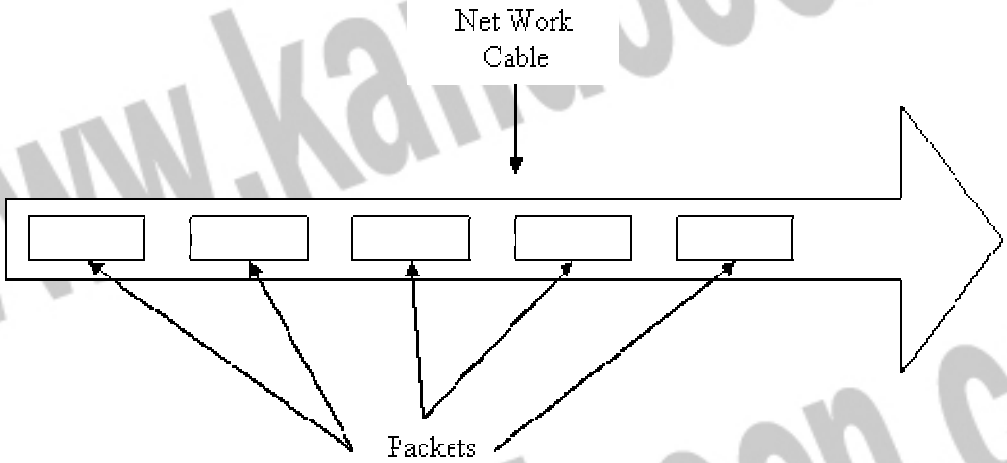
و پهنای باند

۱-۲- 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).[27]

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.



شکل ۱-۲. ارسال سیگنال و پهنای باند

عملکرد 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 کنند full-duplex گفته می‌شود. مثالی از این نوع ارتباط شبکه تلفن می‌باشد. شبکه‌های LAN با داشتن تجهیزاتی خاص بصورت full-duplex عمل کنند.

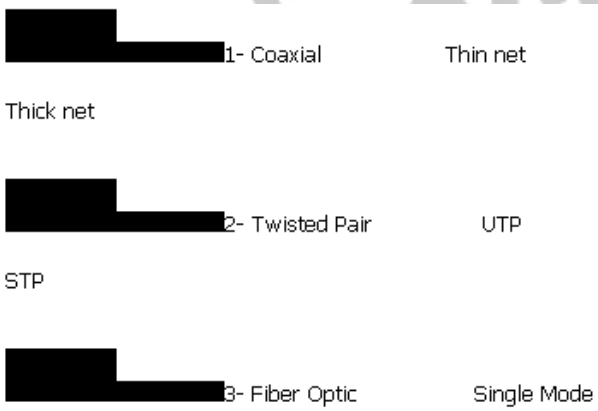
۲-۲- کابل شبکه

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 بطور 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 مختلفی از کابلها بطور معمول در شبکه های LAN

استفاده می شوند. در برخی موارد شبکه تنها از یک نوع کابل استفاده می کند، اما گاه انواعی از کابلها 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.[۲۸]

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



شکل ۲-۲. کابل شبکه

کابلهای Coaxial زمانی بیشترین مصرف را در میان کابلهای موجود در شبکه داشت. چند دلیل اصلی برای استفاده زیاد از این نوع کابل وجود دارد:[۲۹]

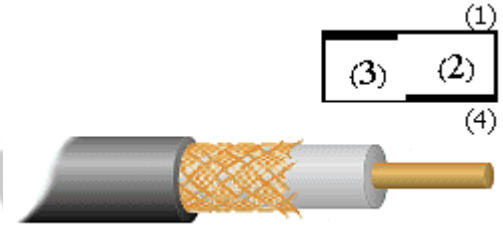
۱- قیمت ارزان آن.

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:[۳۰]



شکل ۳-۲. کابل Coaxial

(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.

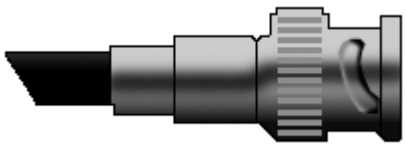
کابل Coaxial به دو دسته تقسیم می‌شود:[۳۱]

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.

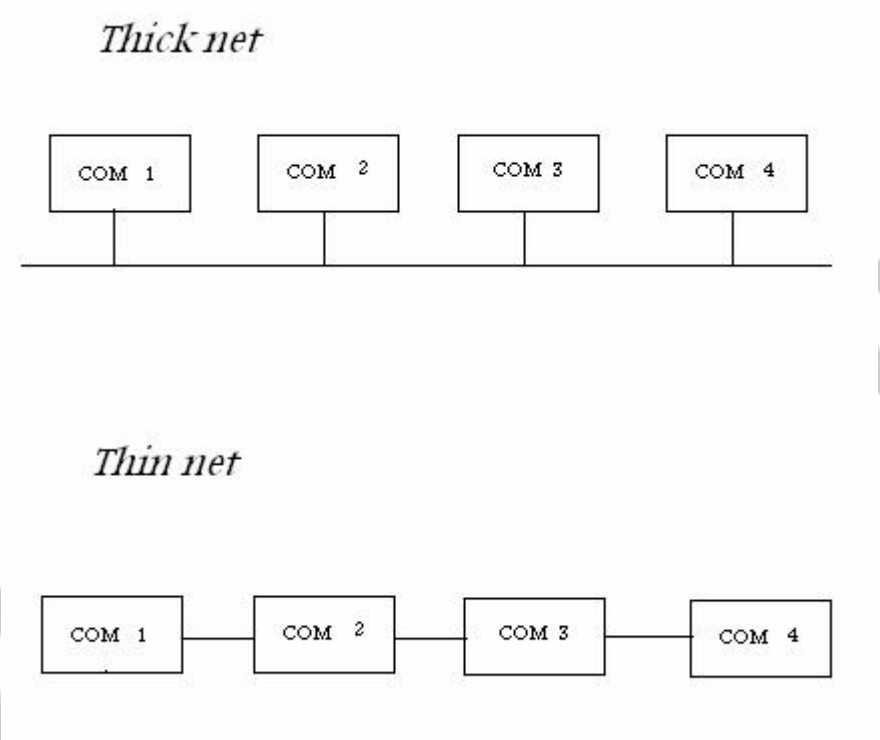
رایج‌ترین نوع اتصال دهنده (connector) مورد استفاده در کابل coaxial، Bayonet-Neill-Concelman (BNC) می‌باشد. انواع مختلفی از سازگار کننده‌ها برای BNCها وجود دارند شامل: Barrel connector ,Tconnector و Terminator.

تصویر زیر یک BNC connector را نشان می دهد:[۳۲]



شکل ۴-۲. BNC connector

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



شکل ۵-۲. Thin net

استفاده از کابل coaxial در شبکه اتوبوسی

باید دانست که از عبارتهایی مانند "Base510 " 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 "Base210" 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:[۳۴]

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 RJ11 استفاده می‌شود، اما در کابل شبکه اتصال دهنده‌ای با شماره RJ45 بکار می‌رود که دارای هشت مکان برای هشت رشته سیم است. در شکل زیر یک connector RJ45 دیده می‌شود.(برگرفته از پانویس قبلی)

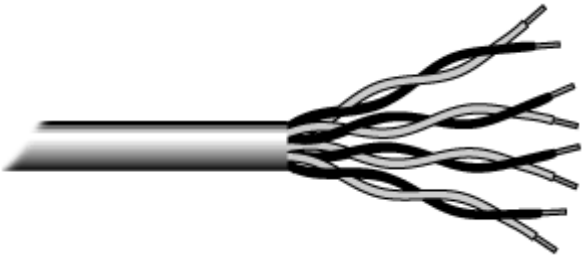
شکل ۶-۲. connector RJ45

connector RJ45

کابل UTP دارای پنج طبقه مختلف است (که البته امروزه CAT6 و CAT7 هم اضافه شده است):

- CAT1 یا نوع اول کابل UTP برای انتقال صدا بکار می‌رود، اما CAT2تا CAT5 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 CAT3 توصیه می‌شود.[۳۵]



شکل ۷-۲. کابل CAT3

کابل UTP

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 سریع۱ (Fast Ethernet) دو نوع کابل به چشم می‌خورد:

- Base TX۱۰۰: یعنی شبکه‌ای که در آن از کابل UTP نوع Cat5 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 T4۱۰۰: 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:[۳۶]

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.[۳۷]

شکل ۸-۲. فیبر نوری

فیبر نوری

بطور کلی توصیه‌هایی در مورد نصب کابل شبکه وجود دارد:[۳۸]

- 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.

۳-۲- 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.[۳۹]

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.

۴-۲- 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 لایهٔ 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[۴۱] یا همان PC Card.

کارت PC در یک شیار[۴۲] 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 یا خارج نمود و پس از نصب آنها نیازی به restart کردن کامپیوتر نیست.

۵-۲- نصب کارت شبکه

برای نصب کارت شبکه، توصیه می‌شود که از دستورالعمل‌های همراه کارت شبکه خود پیروی کنید. سعی کنید کارت شبکه‌ای را خریداری 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 یا دوستتان آن را به شما داده است، ابتدا در دو روی آن کارت شبکه نام سازنده و شماره محصول را بررسی کنید. حداقل یافتن نام سازنده - 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 شبکه وجود دارد. بر روی کارت شبکه یک کد شش رقمی است که از حروف و عدد تشکیل یافته است (مثل [OOAOC9).]43

شماره مذکور به Identifier OUI (Organizationally Unique) معروف است. در صورت وجود OUI شما قادر هستید سازنده کارت و نیز درایور مناسب را بیابید. شماره OUI توسط Engineers IEEE (Institute for Electrical and Electronical) تخصیص داده می‌شود و از طریق پایگاه داده‌های آن می‌توان به جستجوی نام سازندگان پرداخت. (www.ieee.org) شما می‌بایست به منظور کارکرد صحیح کارت شبکه در کامپیوترتان، یک درایور[۴۴] برای آن داشته باشید. اگر کارت شبکه‌ای را از یک تولید کننده معروف در دست دارید، این شانس وجود دارد که ویندوز درایور آن را در فایلهای خود داشته باشد. اما در غیر اینصورت یا باید به دریافت درایور 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 به مراحل بعدی کامل کنید. بهترین راه

برای پاسخگویی به سؤالاتی که در حین مراحل نصب ممکن است برایتان پیش بیاید، مراجعه به وب سایت سازنده است.[۴۵]

فرایند نصب کارت شبکه شامل مراحل زیر است:[۴۶]

- 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 می‌کند مشخص 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 یک مکان دلخواه برای کامپیوتر به سمت مکان دیگر حرکت کنید و بدین شکل یک طرح کلی را از کف خانه خود بدست آورید؛ همینطور که 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 نگهدارنده‌های پلاستیکی به دیوار محکم کنید. در هنگام نصب کابل در اطراف مجراهای گرمایی یا تهویه، سیستم‌های خلاء مرکزی و یا سیستم‌های برق، دقت لازم را به 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 آمده را برای بدست آوردن کل طول کابل مورد نیاز، با هم جمع کنید. اندازه‌ای حدود ده فوت را به کل اندازه کابل مورد نیاز بیفزایید، این طول اضافی بابت موانعی است که به آسانی قابل اندازه‌گیری نیستند مثل زوایا و گوشه‌ها و یا پله‌ها.[۴۷]

برای ادامه کار شما به کابل Cat5 به همراه اتصال دهنده‌های RJ-45 نیاز دارید. به منظور جایدهی فیزیکی کارت شبکه در کامپیوتر، ابتدا کامپیوتر را خاموش کنید. سپس کیس کامپیوتر را باز نمائید و به دنبال یک شیار (slot) آزاد بگردید. در بازار هر دو نوع کارت شبکه ISA و PCI وجود دارند و شما قبل از انتخاب کارت باید بررسی کنید که کامپیوترتان چه نوع شیاری را دارا می‌باشد. کارت‌های ISA برای استفاده‌های معمولی شبکه کافی هستند اما امروزه این نوع باس‌ها با PCI جایگزین شده‌اند. در صورتیکه بخواهید کامپیوتر خود را به شبکه‌های پر سرعت (۱۰۰-Mbps) وصل کنید، باس PCI را ترجیح دهید. پس از خارج 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 سخت‌افزاری عبارتند از:[۴۸]

- Interrupt requests (IRQS): یعنی خطوط سخت‌افزاری که وسایل جانبی از آنها برای فرستادن سیگنال‌ها به پردازشگر 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 با دیگر بخشهای کامپیوتر، تخصیص داده می‌شوند.
- Memory addresses: این مکانها از حافظه توسط وسایل خاص و به منظور نصب BIOS با هدف خاصی استفاده می‌شوند.
- Direct memory access (DMA) channels: یعنی مسیرهای سیستمی که وسایل از آنها برای تبادل اطلاعات با حافظه سیستم استفاده می‌کنند.

کارت‌های شبکه معمولاً از آدرسهای حافظه یا DMA استفاده نمی‌کنند، اما هر کارت شبکه به یک IRQ و نیز آدرس I/O پورت برای 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 می‌کند، همچنین منابع آزاد را مکان‌یابی کرده و به 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.

۶-۲- تنظیمات مربوط به ویندوز برای ایجاد شبکه[۴۹]

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.

۲-۷- 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[۵۰]. 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.

شکل ۹-۲. شبکه های بی سیم WirelessNetworking

تصویر یک 51[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.[۵۲]

امروزه استاندارد غالب در شبکه‌های WLAN، IEEE802.11 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 IEEE802.11a شناخته می‌شود. استاندارد IEEE802.11b که جدیدتر است، سرعت انتقال را تا ۵/۵ و ۱۱مگابیت در ثانیه می‌افزاید.[۵۳]

WLANها از دو توپولوژی حمایت می‌کنند:

- ad hoc topology
- infrastructure topology

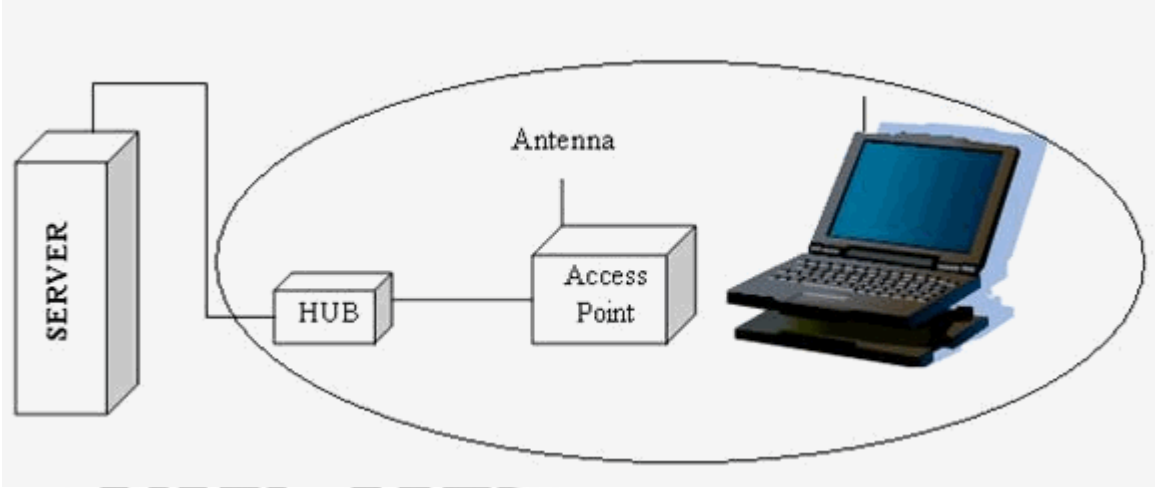
در توپولوژی ad hoc کامپیوترها به شبکه بی‌سیم مجهز هستند و مستقیماً با یکدیگر به شکل Peer- to- peer ارتباط برقرار می‌نمایند.

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 بوسیله Multi-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."[۵۴]

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.



شکل ۱۰-۲. شبکهWLANبا یکAP((AccessPoint

شبکهWLANبا یکAP((AccessPoint

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

802.11 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.[۵۶]

استاندارد IEEE 802.11 از سه نوع سیگنال در لایه فیزیکی پشتیبانی می‌کند:[۵۷]
- (Spectrum DSSS) Direct Sequence Spread: 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 802.11b به سرعت ۱۱ مگابیت در ثانیه انتقال دست یابند. در جائیکه شرایط به نحوی است که امکان تداخل، نویزپذیری 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 802.11a می‌توان از FHSS استفاده کرد اما سیستم IEEE 802.11b 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.

۸-۲- 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 می‌توانند 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.

فصل سوم

آشنائی با کارت شبکه

۱-۳- کارت شبکه

کارت شبکه ، یکی از مهمترین عناصر سخت افزاری در زمان پیاده سازی یک شبکه کامپیوتری است . هر کامپیوتر موجود در شبکه (سرویس گیرندگان و سرویس دهندگان) ، نیازمند استفاده از یک کارت شبکه است . کارت شبکه ، ارتباط بین کامپیوتر و محیط انتقال (نظیر کابل ها ی مسی و یا فیبر نوری) را فراهم می نماید .

اکثر مادربردهای جدیدی که از آنان در کامپیوترهای شخصی استفاده می گردد ، دارای یک اینترفیس شبکه ای onboard می باشند . کامپیوترهای قدیمی و یا کامپیوترهای جدیدی که دارای اینترفیس شبکه ای onboard نمی باشند ، در زمان اتصال به شبکه ، می بایست بر روی آنان یک کارت شبکه نصب گردد.

شکل زیر یک نمونه کارت شبکه را که دارای یک پورت RJ-۴۵ است را نشان می دهد .

شکل ۱-۳. کارت شبکه

۲-۳- وظایف کارت شبکه

- برقراری ارتباط لازم بین کامپیوتر و محیط انتقال
- تبدیل داده : داده ها بر روی گذرگاه (bus) کامپیوتر به صورت موازی حرکت می نمایند . نحوه حرکت داده ها بر روی محیط انتقال شبکه به صورت سریال است . ترانسیور کارت شبکه (یک ارسال کننده و یا دریافت کننده) ، داده ها را از حالت موازی به سریال و بالعکس تبدیل می نماید .
- ارائه یک آدرس منحصربفرد سخت افزاری : آدرس سخت افزاری (MAC) درون تراشه ROM موجود بر روی کارت شبکه نوشته می گردد . آدرس MAC در واقع یک

زیر لایه از لایه Link Data مدل مرجع OSI می باشد . آدرس سخت افزاری موجود بر روی کارت شبکه ، یک آدرس منحصربفرد را برای هر یک از کامپیوترهای موجود در شبکه ، مشخص می نماید . پروتکل هائی نظیر IP/TCP از یک سیستم آدرس دهی منطقی (آدرس IP) ، استفاده می نمایند . در چنین مواردی قبل از دریافت داده توسط کامپیوتر ، می بایست آدرس منطقی به آدرس سخت افزاری ترجمه گردد .

انتخاب کارت شبکه

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

- سازگاری با معماری استفاده شده در شبکه : کارت های شبکه دارای مدل های متفاوتی با توجه به معماری استفاده شده در شبکه (اترنت ، ring Token)می باشند . اترنت ، متداولترین معماری شبکه در حال حاضر است که در شبکه هائی با ابعاد بزرگ و کوچک ، استفاده می گردد .
- سازگاری با throughput شبکه : در صورتی که یک شبکه اترنت سریع(سرعت ۱۰۰Mbps) پیاده سازی شده است ، انتخاب یک کارت اترنت با سرعت ۱۰Mbps تصمیم مناسبی در این رابطه نخواهد بود . اکثر کارت های شبکه جدید قادر به سوئیچینگ اتوماتیک بین سرعت های ۱۰ و ۱۰۰Mbps می باشند (اترنت معمولی و اترنت سریع)
- سازگاری با نوع اسلات های خالی مادربرد : کارت های شبکه دارای مدل های متفاوتی با توجه به نوع اسلات مادربرد می باشند. کارت های شبکه PCI درون یک اسلات خالی PCI و کارت هائی از نوع ISA در اسلات های ISA نصب می گردند . کارت شبکه می بایست متناسب با یکی از اسلات های خالی موجود بر روی مادربرد، انتخاب گردد. اسلات آزاد به نوع مادربرد بستگی داشته و در این رابطه گزینه های متعددی نظیر PCI,ISA و EISA می تواند وجود داشته باشد . شکل زیر یک نمونه مادربرد را که دارای اسلات های ISA و PCI است ، نشان می دهد :

شکل ۲-۳. مادربرد

گذرگاه ISA که از کلمات Architecture Standard Industry اقتباس شده است، استاندارد استفاده شده در کامپیوترهای XT IBM است . استاندارد فوق در ابتدا به صورت هشت بیتی مطرح و در سال ۱۹۸۴ نوع شانزده بیتی آن نیز عرضه گردید. تعداد زیادی از تجهیزات سخت افزاری نظیر مودم ، کارت صدا و کارت های شبکه بر اساس استاندارد فوق تولید و عرضه شده اند . برخی از مادربردهای جدید دارای اسلات های PCI بوده و از کارت های ISA حمایت نمی نمایند . (کارت های PCI دارای سرعت بیشتری نسبت به ISA می باشند) .

PCI در سال ۱۹۹۳ معرفی و یک گذرگاه سی و دو بیتی است . PCI ۲.۱ شصت و چهار بیت را حمایت می نماید .کارت های شبکه PCI با توجه به پتاسیل های موجود دارای استعداد لازم به منظور ارائه سرعت و کارآئی بیشتری نسبت به کارت های ISA می باشند :

- بافرینگ : حافظه تراشه ها (RAM) بر روی کارت شبکه قرار داشته و از آن به عنوان بافر استفاده می گردد .از حافظه فوق به منظور نگهداری اطلاعاتی که در انتظار پردازش می باشند و یا اطلاعاتی که می بایست بر روی شبکه منتشر شوند ، استفاده می گردد .
- DMA و یا Access Memory Direct ، کامپیوترهائی که از DMA حمایت می نمایند، امکان ارسال و یا دریافت داده از حافظه را مستقیما" و بدون درگیرکردن پردازنده فراهم می نمایند .
- Mastering Bus . کارت های شبکه می توانند بگونه ای طراحی شوند که مستقیما" بدون استفاده از پردازنده کامپیوتر و یا واسطه ای دیگر به حافظه RAM

کامپیوتر دستیابی داشته باشند . ویژگی فوق به کارت های شبکه اجازه می دهد که bus را کنترل نموده و داده ئی را به حافظه RAM کامپیوتر ارسال و یا دریافت نمایند .

۳-۳- نصب کارت شبکه

برای نصب کارت شبکه می توان مراحل زیر را دنبال نمود :

- باز نمودن کیس کامپیوتر و نصب کارت شبکه در یکی از اسلات های آزاد
- بستن کیس و متصل نمودن کابل به پورت کارت شبکه
- راه اندازی کامپیوتر . در صورتی که یک کارت Plug&Play تهیه شده است و از سیستم عاملی استفاده می شود که تکنولوژی Play & Plug را حمایت می نماید ، تنها کاری که احتمالا" می بایست انجام داد ، قرار دادن دیسکت و یا CD درایور کارت شبکه در درایو مربوطه است .در صورتی که از سیستم عاملی استفاده می گردد که قادر به تشخیص سخت افزارهای جدید نمی باشد ، می بایست عملیات نصب کارت شبکه به صورت دستی انجام شود .

با توجه به این که کامپیوترهای جدید و سیستم های عاملی که بر روی آنان نصب می گردد، عموما" از فن آوری Plug&Play حمایت می نمایند ، نصب یک کارت شبکه کار چندان مشکلی نخواهد بود . کافی است کارت شبکه را درون یکی از اسلات های خالی مادربرد قرار داده و کامپیوتر را راه اندازی نمود . کارت های شبکه Plug&Play توسط سیستم عامل تشخیص داده شده و درایور آنان نصب می گردد .

در حال حاضر سیستم های عامل اندکی وجود دارد که از تکنولوژی Play& Plug حمایت نمی نمایند ، در زمان نصب کارت شبکه بر روی این نوع سیستم ها ، می بایست دارای اطلاعات لازم در رابطه با IRQ نیز باشیم (IRQ از کلمات Interrupt Request اقتباس شده است) . به هر دستگاه موجود در کامپیوتر نظیر موس ، صفحه کلید و کارت شبکه ، یک خط IRQ نسبت داده می شود. دستگاه های فوق با استفاده از IRQ نسبت داده شده ، درخواست خود را با پردازنده مطرح می نمایند (پردازش داده

ها) . هر دستگاه می بایست دارای یک IRQ منحصربفرد باشد در غیر اینصورت با یـک Conflict IRQ مواجه خواهیم شد.

جدول زیر تنظیمات IRQ در کامپیوترهای شخصی را نشان می دهد .

IRQ	کاربرد
۰	System timer
۱	Keyboard
۲	Cascade to secondary IRQ controller
۳	COM port 2 and 4 (serial port)
۴	COM port 1 and 3 (serial port)
۵	LPT2 (printer port)
۶	Floppy disk controller
۷	LPT1 (printer port)
۸	Real-time clock
۹	Free
۱۰	Primary SCSI adapter (or free)
۱۱	Secondary SCSI adapter (or free)
۱۲	PS/2 mouse
۱۳	Floating-point math coprocessor
۱۴	Primary hard disk controller
۱۵	Secondary hard disk controller (or free)

فصل چهارم

مراحل نصب ویندوز ۲۰۰۳

۱-۴- نصب ویندوز ۲۰۰۳

۱ ـ "CD" ویندوز را در "CD-ROM" می گذاریم.

۲ ـ با توجه به اینکه "CD" بوت ایبل است به محض روشن کردن رایانه با فشردن دکمه "Del" وارد برنامه "Setup" سیستم می شویم. در قسمت تعیین دستگاه های بوت کننده ، نخستین گزینه را بر روی "CD ROM" قرار می دهیم، با فشردن کلید"F10" سپس "Y" و در آخر "Enter" تغییرات اعمال شده در برنامه "Setup" ذخیره و رایانه دوباره "Boot" می شود.

۳ ـ هنگامی که پیام "Press any key to boot from CD-Rom" دیده شد ، دکمه ای را می فشاریم تا رایانه از روی "CD" بوت شده و پنجره ابتدایی نصب ویندوز ظاهرگردد. در این حال رایانه در حال بارگذاری راه اندازهای ویژه برای نصب ویندوز می باشد.
۴ ـ در پنجره بعدی در صورت تمایل به ادامه نصب کلید "Enter" و در غیر اینصورت "F3" را می فشاریم.

۵ ـ در پنجره بعدی برای نصب ویندوز دکمه "Enter" ، برای بازسازی نصب قبلی ویندوز که نیمه کاره رها شده است به کمک کنسول بازیابی (Recovery Console) دکمه "R" و برای خروج از دکمه "F3" استفاده می شود.

شکل ۱-۴. Recovery Console

۶ ـ سپس پنجره ای که حاوی توافق نامه و مجوز استفاده از این نسخه ویندوز است ظاهر می گردد. بدیهی است برای ادامه نصب باید موافقت خود را با زدن "F8" اعلام نمود. کلیدهای "Page Up" و "Page Down" کل متن را نشان خواهند داد. کلید "Esc" عدم توافق و خروج را نشان می دهد.

۷ ـ در پنجره بعدی اطلاعات مربوط به پارتیشن بندی (Partitions) دیسک سخت رایانه نشان داده می شود. اگر موافق با نصب ویندوز بر روی پارتیشن ایجاد شده از قبل که اطلاعات مربوط برای نشان داده شده هستید کلید "Enter" را بزنید. اگر مایل به ایجاد یک پارتیشن جدید بر روی ناحیه پارتیشن نشده می باشید کلید "C" و اگر به حذف پارتیشن فعلی تمایل دارید کلید "D" را بزنید با کلیدهای "Page Up" و " Page Down" می توانید بر روی پارتیشن های مختلف بروید.

شکل ۲-۴. پنجره Partitions

۸ ـ همانطور که در شکل ۲ مشاهده می کنید ، پس از انتخاب درایو و با فشردن کلید "Enter" ، برنامه "Setup" ویندوز بر روی پارتیشن برگزیده شده شروع به نصب فایل های مورد نیاز برای "Boot" شدن دوباره سیستم از روی دیسک سخت می کند.

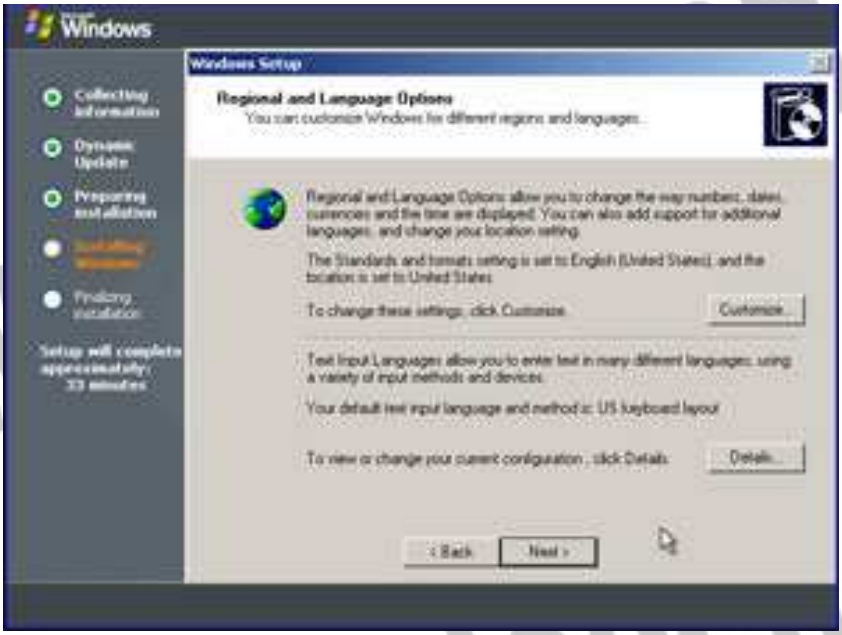
۹ ـ در مرحله بعدی برنامه "Setup" اطلاعات متنوعی را برای نصب خود تولید کرده و رایانه را مورد ارزیابی قرار می دهد.

۱۰ ـ در این مرحله برنامه آماده راه اندازی دوباره - Restart / Reboot - سیستم می شود. بهتر است ۱۵ ثانیه درنگ کنیم تا این کار بصورت خودکار صورت پذیرد. این مرحله پایان کار صفحه های با زمینه آبی (Blue background) است.

۱۱ ـ پس از آغاز دوباره کار رایانه ، صفحه بوت شدن ویندوز را خواهید دید.

۱۲ ـ اگر تاکنون ویندوز "XP" نصب کرده باشید صفحه بعدی به چشمتان آشنا خواهد آمد ، تنها تفاوت تغییر رنگ آبی ویندوز "XP" به طوسی می باشد.

۱۳ ـ در صفحه بعد هنگام تغییر گزینه های زبان و منطقه (Regional and Language Options) فرا می رسد. با کلیک بر روی دکمه "Customize" و در " Languages Tab" کنار جمله "Install files for Complex Script and right to left languages (including Thai)" علامت بزنید. سپس دکمه "Details" را فشرده، سپس "Add" را زده و زبان فارسی را انتخاب نمایید. سایر تنظیمات را می توانید در همین پنجره ها انجام دهید. دکمه "ok" را بزنید.

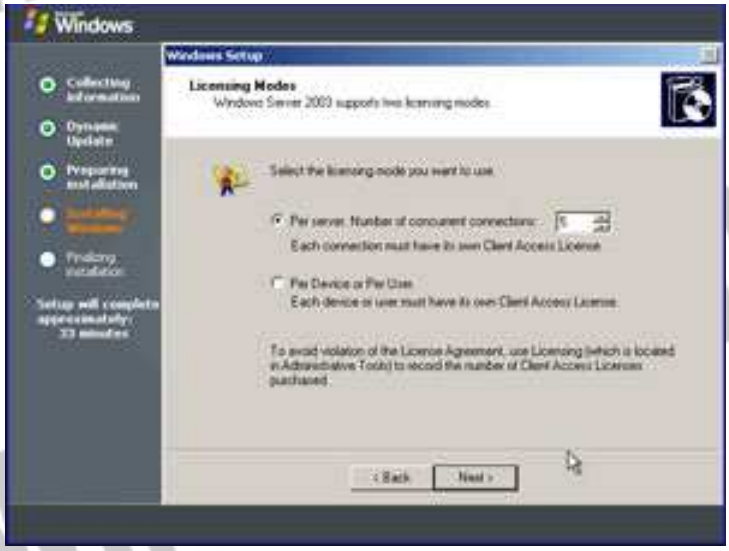


شکل ۳-۴. Regional and Language Options

۱۴ - در پنجره بعدی نام خود و سازمان مورد نظرتان را وارد کنید و دکمه Next را بزنید.

۱۵ ـ در صفحه بعدی شماره کلید ۲۵ حرفی محصول (Product key) را که احتمالا روی جلد CD یا داخل CD ویندوز۲۰۰۳ می باشد وارد کنید.

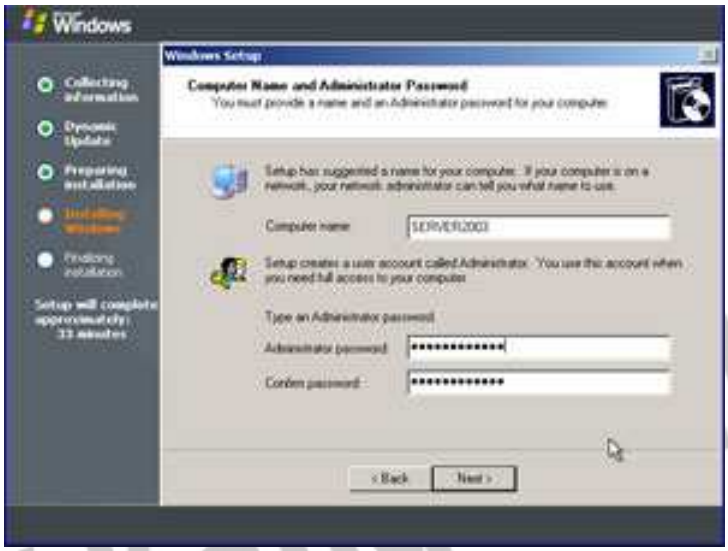
۱۶ ـ در این مرحله باید نوع مجوز استفاده از این ویندوز را معین کنید که البته در کشور ما با توجه به رونق قفل شکنی نرم افزارها ، کاری با آن نخواهیم داشت!! معمولاً در شبکه هایی که دارای یک رایانه سرویس دهنده می باشند گزینش "Per Server" درست تر می باشد. انتخاب "Per Device or Per User" معمولاً نشاندهنده آن است که تعداد اتصالات به سرویس دهنده بیش از تعداد کاربران موجود و در حال کار است.



شکل ۴-۴. انتخاب مجوز

۱۷ ـ در اینجا نام دلخواه رایانه سرویس دهنده خود را وارد کنید. رایانه سرویس دهنده از این پس بدین نام در شبکه شناسایی خواهد شد. همچنین در این پنجره باید رمز مورد نظر برای مدیر شبکه را وارد و آن را دوباره تایید

(Confirm) کنید. نام رمز نباید از خاطرتان برود وگرنه وامصیبتا!!



شکل ۵-۴. انتخاب پسورد

۱۸ـ اگر نام رمز خود را به خوبی انتخاب نکرده باشید ، پنجره ای نمایان می شود کـه در آن ضوابط و معیارهای گزینش درست ذکر شده است. توصیه می شود رمز مورد نظر از ۲ قاعده اول ذیل پیروی کرده و از بین بقیه حداقل از ۳ قاعده تبعیت کند:

الف: حداقل ۶ حرف داشته باشد.

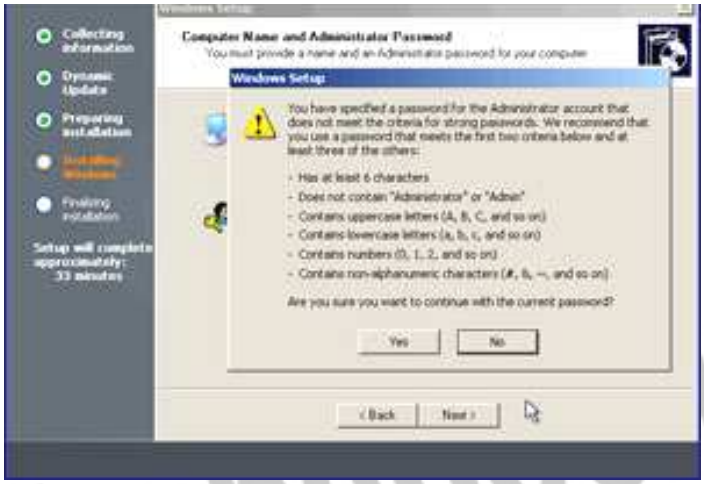
ب: در برگیرنده واژه های "Admin" یا "Administrator" نباشد.

ج : حاوی حروف بزرگ (Uppercase) مانند "A", "B" و غیره باشد.

د : حاوی حروف کوچک (Lowercase) مانند "a", "b" و غیره هم باشد.

ه : حاوی اعداد نیز باشد.

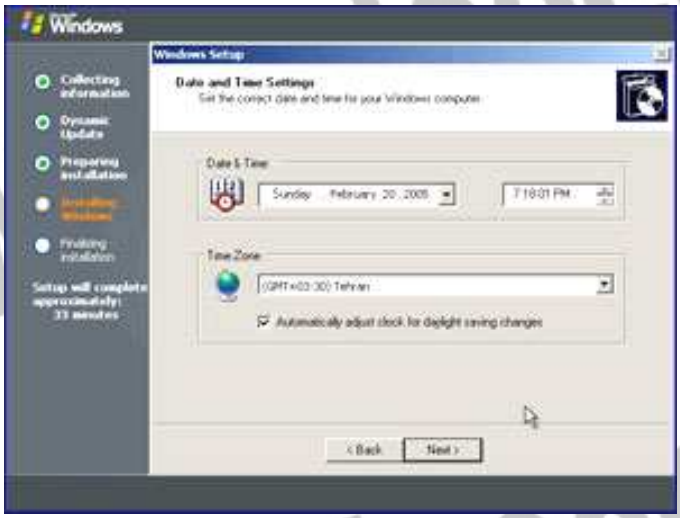
و : حاوی کاراکترهای غیر حرفـی و عـددی (non-alphanumeric characters) ماننـد "&", "~", "$", "#" و غیره هم باشد.



شکل ۶-۴. پنجره ضوابط و معیارهای گزینش

رمز مورد نظر باید دارای امنیت بوده و از یادتان نرود.

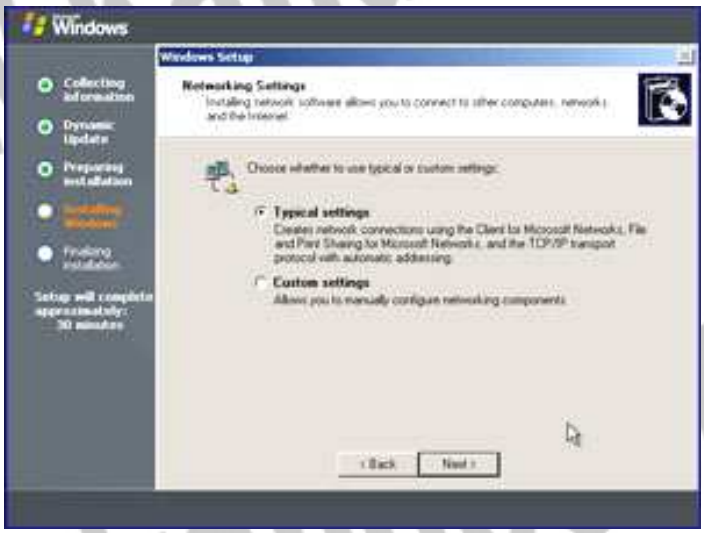
۱۹ ـ در پنجره بعدی تنظیمات زمان و تاریخ (Date and Time Settings) انجـام مـی شود که براحتی قابل تنظیم بوده و ضمناً منطقه زمانی (Time Zone) شهر مورد نظرتان نیز در اینجا انتخاب می گردد.



شکل ۷-۴.Date and Time Settings

۲۰ ـ برنامه "Setup" ادامه یافته و شما می توانید قدری از این تلاش طاقت فرسا!! بـرای نصب ویندوز دست شسته و بیاسایید!! نصب مولفه های شبکه در ایـن بخـش انجـام مـی گردد.

۲۱ ـ درنگ کنید ، بر خیزید!!در پنجره بعدی بایـد بـرای تنظیمـات شـبکه ، یکـی از دو روش عادی و از پیش تعیـین شـده (Typical) و یـا سفارشـی (Custom) را انتخـاب نمایید. از آنجایی که قصد ما نصب این ویندوز در ساده ترین شکل ممکن و کمترین توان مصرفی !! است گزینه از پیش تعیین شده "Typical" را انتخاب و "Next" را می زنیم.



شکل ۸-۴. پنجره تنظیمات شبکه

۲۲ ـ در این پنجره هنگام آن است کـه از بـین دو روش "Workgroup" و یـا "Client-Server" که رایانه سرویس دهنده را تبدیل بـه یـک کنتـرل کننـده دامنـه (Domain Controller) می کند و شرح آنها قبلاً داده شده یکی را انتخاب کنیم کـه گزینـه اول را برمی گزینیم . نام این گروه کاری می تواند بصورت دلخواه داده شود.

شکل ۹-۴. Domain Controller & Workgroup

۲۳ ـ در پنجره بعدی زمانی صرف ادامه نصب ویندوز خواهد شد که مانند همیشه شامل خودستایی های شناخته شده شرکت ها درباره محصولات شان و ذکر اینکه به قول معروف عامه ((این یکی دیگه آخرشه !!)) خواهد شد. اگر تاب تحمل گزافه گویی های مایکروسافت را ندارید ، زمان مناسبی است که قدری بیارامید ، اما گمان می کنم توجه به پیام های متوالی روی صفحه و خواندن آنها می تواند بسیار سودمند باشد.

۲۴ ـ لحظه ای که چشم به راهش بودیم فرا رسید. ویندوز ۲۰۰۳ برای اولین بار بر روی رایانه تان آغاز به کار می کند.

۲۵ـ درود سه انگشتی خود را به ویندوز بفرستید ، دکمه های "Ctrl", "Alt" را فشرده و کلید " Delete" را بزنید. بدین وسیله با مسئولیت "Administrator account" وارد ویندوز می شوید.

۲۶ ـ نام کاربری (Username) مدیر شبکه "Administrator" را خواهید دید. نام رمز که از یادتان نرفته است؟!

۲۷ ـ پنجره خوشامدگویی (Welcoming screen) به همراه اطلاعات و ابزار سودمندی برای مدیریت سرویس دهنده شما نمایان می گردد.

شکل ۱۰-۴. Welcoming screen

۲۸ـ با علامت گذاری (check mark) در کنار جمله "Don’t display this page at logon" در راه اندازی بعدی ویندوز پنجره خوشامدگویی را ندیـده و صـفحه "desktop" ویندوز نمایان خواهد شد.

فصل پنجم

مبانی امنیت اطلاعات

۱-۵- مبانی امنیت اطلاعات

امروزه شاهد گسترش حضور کامپیوتر در تمامی ابعاد زندگی خود می باشیم . کافی است به اطراف خود نگاهی داشته باشیم تا به صحت گفته فوق بیشتر واقف شویم . همزمان با گسترش استفاده از کامپیوترهای شخصی و مطرح شدن شبکه های کامپیوتری و به دنبال آن اینترنت (بزرگترین شبکه جهانی) ، حیات کامپیوترها و کاربران آنان دستخوش تغییرات اساسی شده است . استفاده کنندگان کامپیوتر به منظور استفاده از دستاوردها و مزایای فن آوری اطلاعات و ارتباطات ، ملزم به رعایت اصولی خاص و اهتمام جدی به تمامی مولفه های تاثیر گذار در تداوم ارائه خدمات در یک سیستم کامپیوتری می باشند . امنیت اطلاعات و ایمن سازی شبکه های کامپیوتری از جمله این مولفه ها بوده که نمی توان آن را مختص یک فرد و یا سازمان در نظر گرفت . پرداختن به مقوله امنیت اطلاعات و ایمن سازی شبکه های کامپیوتری در هر کشور ، مستلزم توجه تمامی کاربران صرفنظر از موقعیت شغلی و سنی به جایگاه امنیت اطلاعات و ایمن سازی شبکه های کامپیوتری بوده و می بایست به این مقوله در سطح کلان و از بعد منافع ملی نگاه کرد. وجود ضعف امنیتی در شبکه های کامپیوتری و اطلاعاتی ، عدم آموزش و توجیه صحیح تمامی کاربران صرفنظر از مسئولیت شغلی آنان نسبت به جایگاه و اهمیت امنیت اطلاعات ، عدم وجود دستورالعمل های لازم برای پیشگیری از نقایص امنیتی ، عدم وجود سیاست های مشخص و مدون به منظور برخورد مناسب و بموقع با اشکالات امنیتی ، مسائلی را به دنبال خواهد داشت که ضرر آن متوجه تمامی کاربران کامپیوتر در یک کشور شده و عملا" زیرساخت اطلاعاتی یک کشور را در معرض آسیب و تهدید جدی قرار می دهد .

در این مقاله قصد داریم به بررسی مبانی و اصول اولیه امنیت اطلاعات و ایمن سازی شبکه های کامپیوتری پرداخته و از این رهگذر با مراحل مورد نیاز به منظور حفاظت کامپیوترها در مقابل حملات ، بیشتر آشنا شویم .

۲-۵- اهمیت امنیت اطلاعات و ایمن سازی کامپیوترها

تمامی کامپیوترها از کامپیوترهای موجود در منازل تا کامپیوترهـای موجـود در سـازمان ها و موسسات بزرگ ، در معرض آسیب و تهدیدات امنیتی می باشند .بـا انجـام تـدابیر لازم و استفاده از برخی روش های ساده می توان پیشگیری لازم و اولیه ای را خصوص ایمن سازی محیط کامپیوتری خود انجام داد.علیرغم تمامی مزایا و دستاوردهای اینترنت ، این شبکه عظیم به همراه فن آوری های مربوطه ، دریچه ای را در مقابل تعـداد زیـادی از تهدیدات امنیتی برای تمامی استفاده کننـدگان (افـراد ، خـانواده هـا ، سـازمان هـا ، موسسات و ...) ، گشوده است . با توجه به ماهیت حملات ، می بایست در انتظـار نتـایج نامطلوب متفاوتی بود(از مشکلات و مزاحمت های اندک تا از کار انداختن سرویس هـا و خدمات) .در معرض آسیب قرار گرفتن داده ها و اطلاعـات حسـاس ، تجـاوز بـه حـریم خصوصی کاربران ، استفاده از کامپیوتر کاربران برای تهاجم بر علیه سایر کامپیوترهـا ، از جمله اهداف مهاجمانی است که با بهره گیری از آخرین فن آوری های موجود ، حمـلات خود را سازماندهی و بالفعل می نمایند . بنابراین ، می بایست به موضوع امنیت اطلاعات، ایمن سازی کامپیوترها و شبکه هـای کـامپیوتری، توجـه جـدی شـده و از فرآینـدهای متفاوتی در جهت مقاوم سازی آنان ، استفاده گردد .

۳-۵- داده ها و اطلاعات حساس در معرض تهدید

تقریبا" هر نوع تهاجم ، تهدیدی است در مقابل حـریم خصوصـی ، پیوسـتگی ، اعتبـار و صحت داده ها .یک سارق اتومبیل می تواند در هر لحظه صرفا" یـک اتومبیـل را سـرقت نماید ، در صورتی که یک مهاجم با بکارگیری صرفا" یک دستگاه کـامپیوتر ، مـی توانـد آسیب های فراوانی را متوجه تعداد زیادی از شبکه های کامپیوتری نمـوده و باعـث بـروز اشکالاتی متعدد در زیرساخت اطلاعاتی یک کشورگردد. آگاهی لازم در رابطه با تهدیدات امنیـتی و نحوه حفاظـت خـود در مقابـل آنـان ، امکـان حفاظـت اطلاعـات و داده هـای حساس را در یک شبکه کامپیوتری فراهم می نماید .

۴-۵- ویروس ها

ویروس های کامپیوتری ، متداولترین نوع تهدیدات امنیتی در سالیان اخیر بوده که تاکنون مشکلات گسترده ای را ایجاد و همواره از خبرسازترین موضوعات در زمینه کامپیوتر و شبکه های کامپیوتری ، بوده اند. ویروس ها ، برنامه هائی کامپیوتری می باشند که توسط برنامه نویسان گمراه و در عین حال ماهر نوشته شده و بگونه ای طراحی می گردند که قادر به تکثیر خود و آلودگی کامپیوترها بر اثر وقوع یک رویداد خاص ، باشند . مثلا" ویروس ها ئی که از آنان با نام "ماکرو ویروس " یاد می شود ، خود را به فایل هائی شامل دستورالعمل های ماکرو ملحق نموده و در ادامه ، همزمان با فعال شدن ماکرو ، شرایط لازم به منظور اجرای آنان نیز فراهم می گردد.برخی از ویروس ها بی آزار بوده و صرفا" باعث بروز اختلالات موقت در روند انجام عملیات در کامپیوتر می شوند (نظیر نمایش یک پیام مضحک بر روی صفحه نمایشگر همزمان با فشردن یک کلید خاص توسط کاربر) . برخی دیگر از ویروس ها دارای عملکردی مخرب تر بوده و می توانند مسائل و مشکلات بیشتری نظیر حذف فایل ها و یا کاهش سرعت سیستم را به دنبال داشته باشند. یک کامپیوتر صرفا" زمانی آلوده به یک ویروس می گردد که شرایط و امکان ورود ویروس از یک منبع خارجی (اغلب از طریق فایل ضمیمه یک نامه الکترونیکی و یا دریافت و نصب یک فایل و یا برنامه آلوده از اینترنت) ، برای آن فراهم گردد . زمانی که یک کامپیوتر در شبکه ای آلوده گردید ، سایر کامپیوترها ی موجود در شبکه و یا سایر کامپیوترهای موجود در اینترنت، دارای استعدادی مناسب به منظور مشارکت و همکاری با ویروس،خواهند بود.

۵-۵- برنامه های اسب تروا (دشمنانی در لباس دوست)

برنامه های اسب تروا و یا Trojans ، به منزله ابزارهائی برای توزیع کد های مخرب می باشند . تروجان ها ، می توانند بی آزار بوده و یا حتی نرم افزاری مفیدی نظیر بازی های کامپیوتری باشند که با تغییر قیافه و با لباسی مبدل و ظاهری مفید خود را عرضه

می نمایند. تروجان ها ، قادر به انجام عملیات متفاوتی نظیر حذف فایل ها ، ارسال یک نسخه از خود به لیست آدرس های پست الکترونیکی ، می باشند. این نوع از برنامه ها صرفا" می توانند از طریق تکثیر برنامه های اسب تروا به یک کامپیوتر،دریافت فایل از طریق اینترنت و یا باز نمودن یک فایل ضمیمه همراه یک نامه الکترونیکی ، اقدام به آلودگی یک سیستم نمایند.

ویرانگران در وب سایت های متعددی از نرم افزارهائی نظیر اکتیوایکس ها و یا اپلت های جاوا استفاده می گردد . این نوع برنامه ها به منطور ایجاد انیمیشن و سایر افکت های خاص مورد استفاده قرار گرفته و جذابیت و میزان تعامل با کاربر را افزایش می دهند . با توجه به دریافت و نصب آسان این نوع از برنامه ها توسط کاربران ، برنامه های فوق به ابزاری مطئمن و آسان به منظور آسیب رسانی به سایر سیستم ها تبدیل شده اند . این نوع برنامه ها که به "ویرانگران" شهرت یافته اند ، به شکل یک برنامه نرم افزاری و یا اپلت ارائه و در دسترس استفاده کنندگان قرار می گیرند . برنامه های فوق ، قادر به ایجاد مشکلات متعددی برای کاربران می باشند(از بروز اشکال دریک فایل تا ایجاد اشکال در بخش اصلی یک سیستم کامپیوتری) .

حملات تاکنون حملات متعددی متوجه شبکه های کامپیوتری بوده که می توان تمامی آنان را به سه گروه عمده تقسیم نمود :

• حملات شناسائی : در این نوع حملات ، مهاجمان اقدام به جمع آوری و شناسائی اطلاعات با هدف تخریب و آسیب رساندن به آنان می نمایند . مهاجمان در این رابطه از نرم افزارهای خاصی نظیر Sniffer و یا Scanner به منظور شناسائی نقاط ضعف و آسیب پذیر کامپیوترها ، سرویس دهندگان وب و برنامه ها ، استفاده می نمایند . در این رابطه برخی تولیدکنندگان ، نرم افزارهائی را با اهداف خیرخواهانه طراحی و پیاده سازی نموده اند که متاسفانه از آنان در جهت اهداف مخرب نیز استفاده می شود.مثلا" به منظور تشخیص و شناسائی رمز های عبور، نرم افزارهای متعددی تاکنون طراحی و پیاده سازی شده است .نرم افرارهای فوق با هدف کمک به مدیران شبکه ، افراد و کاربرانی که رمز عبور خود را فراموش کرده و یا آگاهی از رمز عبور افرادی که سازمان خود را بدون

اعلام رمز عبور به مدیر شبکه ، ترک نموده اند،استفاده می گردند. به هر حال وجود این نوع نرم افزارها واقعیتی انکارناپذیر بوده که می تواند به منزله یک سلاح مخرب در اختیار مهاجمان قرار گیرد .

- حملات دستیابی : دراین نوع حملات، هدف اصلی مهاجمان ، نفوذ در شبکه و دستیابی به آدرس های پست الکترونیکی ، اطلاعات ذخیره شده در بانک های اطلاعاتی و سایر اطلاعات حساس، می باشد.
- حملات از کار انداختن سرویس ها : در این نوع حملات ، مهاجمان سعی در ایجاد مزاحمت به منظور دستیابی به تمام و یا بخشی از امکانات موجود در شبکه برای کاربران مجازمی نمایند . حملات فوق به اشکال متفاوت و با بهره گیری از فن آوری های متعددی صورت می پذیرد . ارسال حجم بالائی از داده ها ی غیرواقعی برای یک ماشین متصل به اینترنت و ایجاد ترافیک کاذب در شبکه ، نمونه هائی از این نوع حملات می باشند.

۶-۵- ره گیری داده (استراق سمع)

بر روی هر شبکه کامپیوتری روزانه اطلاعات متفاوتی جابجا می گردد و همین امر می تواند موضوعی مورد علاقه برای مهاجمان باشد . در این نوع حملات ، مهاجمان اقدام به استراق سمع و یا حتی تغییر بسته های اطلاعاتی در شبکه می نمایند . مهاجمان به منظور نیل به اهداف مخرب خود از روش های متعددی به منظور شنود اطلاعات ، استفاده می نمایند .

۷-۵- کلاهبرداری (ابتدا جلب اعتماد و سپس تهاجم)

کلاهبرداران از روش های متعددی به منظور اعمال شیادی خود استفاده می نمایند. با گشترش اینترنت این نوع افراد فضای مناسبی برای اعمال مخرب خود یافته اند (چراکه می توان به هزاران نفر در زمانی کوتاه و از طریق اینترنت دستیابی داشت) . در برخی موارد شیادان با ارسال نامه های الکترونیکی وسوسه انگیز از خوانندگان می خواهند که اطلاعاتی خاص را برای آنان ارسال نموده و یا از یک سایت به عنوان طعمه در این رابطه

استفاده می نمایند. به منظور پیشگیری از اینگونه اعمال ، می بایست کاربران دقت لازم در خصوص درج نام ، رمز عبور و سایر اطلاعات شخصی در سایت هائی که نسبت به هویت آنان شک و تردید وجود دارد را داشته باشند. با توجه به سهولت جعل آدرس های پست الکترونیکی ؛ می بایست به این نکته توجه گردد که قبل از ارسال اطلاعات شخصی برای هر فرد ، هویت وی شناسائی گردد.هرگز بر روی لینک ها و یا ضمائمی که از طریق یک نامه الکترونیکی برای شما ارسال شده است ، کلیک نکرده و همواره می بایست به شرکت ها و موسساتی که به طور شفاف آدرس فیزیکی و شماره تلفن های خود را ذکر نمی نمایند ، شک و تردید داشت .

نامه های الکترونیکی ناخواسته

از واژه Spam در ارتباط با نامه های الکترونیکی ناخواسته و یا پیام های تبلیغاتی ناخواسته ، استفاده می گردد. این نوع از نامه های الکترونیکی ، عموما" بی ضرر بوده و صرفا" ممکن است مزاحمت و یا دردسر ما را بیشتر نمایند . دامنه این نوع مزاحمت ها می تواند از به هدر رفتن زمان کاربر تا هرز رفتن فضای ذخیره سازی بر روی کامپیوترهای کاربران را شامل می شود .

ابزارهای امنیتی

پس از آشنائی با تهدیدات، می توان تمهیدات امنیتی لازم در خصوص پیشگیری و مقابله با آنان را انجام داد. بدین منظور می توان از فن آوری های متعددی نظیر آنتی ویروس ها و یا فایروال ها ، استفاده بعمل آورد .

۸-۵- نرم افزارهای آنتی ویروس

نرم افزارهای آنتی ویروس ، قادر به شناسائی و برخورد مناسب با اکثر تهدیدات مربوط به ویروس ها می باشند.(مشروط به اینکه این نوع نرم افزارها به صورت منظم بهنگام شده و بدرستی پشتیبانی گردند). نرم افزارهای آنتی ویروس درتعامل اطلاعاتی با شبکه ای گسترده از کاربران بوده و در صورت ضرورت پیام ها و هشدارهای لازم در خصوص

ویروس های جدید را اعلام می نمایند. بدین ترتیب ، پس از شناسائی یک ویروس جدید، ابزار مقابله با آن سریعا" پیاده سازی و در اختیار عموم کاربران قرار می گیرد. با توجه به طراحی و پیاده سازی ویروس های متعدد در سراسر جهان و گسترش سریع آنان از طریق اینترنت ، می بایست بانک اطلاعاتی ویروس ها بر اساس فرآیندی مشخص و مستمر ، بهنگام گردد .

سیاست های امنیتی

سازمان های بزرگ و کوچک نیازمند ایجاد سیاست های امنیتی لازم در خصوص استفاده از کامپیوتر و ایمن سازی اطلاعات و شبکه های کامپیوتری می باشند. سیاست های امنیتی ، مجموعه قوانین لازم به منظور استفاده از کامپیوتر و شبکه های کامپیوتری بوده که در آن وظایف تمامی کاربران دقیقا" مشخص و در صورت ضرورت ، هشدارهای لازم به کاربران در خصوص استفاده از منابع موجود در شبکه داده می شود . دانش تمامی کاربرانی که به تمام و یا بخشی از شبکه دستیابی دارند ، می بایست به صورت منظم و با توجه به سیاست های تدوین یافته ، بهنگام گردد (آموزش مستمر و هدفمند با توجه به سیاست های تدوین شده) .

رمزهای عبور

هر سیستم کامپیوتری می بایست دارای ایمنی مناسبی در خصوص رمز های عبور باشد . استحکام رمزهای عبور ، ساده ترین و در عین حال متداولترین روش به منظور اطمینان از این موضوع است که صرفا" افراد تائید شده و مجاز قادر به استفاده از کامپیوتر و یا بخش های خاصی از شبکه می باشند . فراموش نکنیم که زیرساخت های امنیتی ایجاد شده ، در صورتی که کاربران دقت لازم در خصوص مراقبت از رمزهای عبور خود را نداشته باشند ، موثر نخواهد بود (خط بطلانی بر تمامی تلاش های انجام شده) . اکثر کاربران در زمان انتخاب رمز عبور، از اعداد و یا کلماتی استفاده نمایند که بخاطر آوردن آنان ساده باشد(نظیر تاریخ تولد ، شماره تلفن).برخی دیگر از کاربران علاقه ای به تغییر

منظم رمزهای عبور خود در مقاطع زمانی خاصی نداشته و همین امر می تواند زمنیه تشخیص رمزهای عبور توسط مهاجمان را فراهم نماید.

در زمان تعریف رمز عبور می بایست تمهیدات لازم در خصوص استحکام و نگهداری مطلوب آنان اندیشیده گردد:

- حتی المقدور سعی گردد از رمز های عبور فاقد معنی خاصی استفاده گردد .
- به صورت منظم و در مقاطع زمانی مشخص شده ، اقدام به تغییر رمزهای عبور گردد .
- عدم افشای رمزهای عبور برای سایرین

۹-۵- فایروال ها

فایروال ، راه حلی سخت افزاری و یا نرم افزاری به منظور تاکید (اصرار) بر سیاست های امنیتی می باشد .یک فایروال نظیر قفل موجود بر روی یک درب منزل و یا بر روی درب یک اطاق درون منزل می باشد . بدین ترتیب صرفا" کاربران تائید شده (آنانی که دارای کلید دستیابی می باشند) ، امکان ورود به سیستم را خواهند داشت . فایروال ها دارای فیلترهای از قبل تعبیه شده ای بوده که امکان دستیابی افراد غیر مجاز به منابع سیستم را سلب می نمایند.

۱۰-۵- رمزنگاری

فن آوری رمزنگاری ، امکان مشاهده ، مطالعه و تفسیر پیام های ارسالی توسط افراد غیر مجاز را سلب می نماید . از رمزنگاری به منظور حفاظت داده ها در شبکه های عمومی نظیر اینترنت استفاده می گردد . در این رابطه از الگوریتم های پیشرفته ریاضی به منظور رمزنمودن پیام ها و ضمائم مربوطه ، استفاده می شود.

چند نکته اولیه در خصوص ایمن سازی اطلاعات و شبکه های کامپیوتری

- پذیرش مسئولیت به عنوان یک شهروند سایبر

در صورتی که از اینترنت استفاده می نمائید ، شما به عنوان عضوی از جامعه جهانی و یا شهروند سایبر، محسوب شده و همانند یک شهروند معمولی ، دارای مسئولیت های خاصی بوده که می بایست پذیرای آنان باشیم .

• استفاده از نرم افزارهای آنتی ویروس

یک ویروس کامپیوتری ، برنامه ای است که می تواند به کامپیوتر شما نفوذ کرده و صدمات فراوانی را باعث گردد . نرم افزارهای آنتی ویروس به منظور حفاظت اطلاعات و کامپیوترها در مقابل ویروس های شناخته شده ، طراحی شده اند . با توجه به این که روزانه شاهد عرضه ویروس های جدید می باشیم ، می بایست برنامه های آنتی ویروس به صورت منظم و مرتب بهنگام گردند .

• عدم فعال نمودن نامه های الکترونیکی ارسال شده توسط منابع نامشخص و گمنام نامه های الکترونیکی ارسالی توسط منابع ناشناس را می بایست همواره حذف نمود. به فایل هائی که به عنوان ضمیمه همراه یک نامه الکترونیکی ارسال می گردند، توجه گردد. حتی در صورتی که این نوع از نامه های الکترونیکی را از طریق دوستان و آشنایان خود دریافت می نمائید (خصوصا" اگر دارای انشعاب exe . باشند.) . برخی فایل ها مسئولیت توزیع ویروس ها را برعهده داشته و می توانند باعث بروز اشکالات فراوانی نظیر حذف دائم فایل ها و یا بروز اشکال در یک وب سایت گردند. هرگز نمی بایست اقدام به فوروارد نمودن نامه های الکترونیکی برای سایر کاربران قبل از حصول اطمینان از ایمن بودن آنان نمود .

• از رمزهای عبوری که تشخیص آنان مشکل می باشد ، استفاده نموده و آنان را محرمانه نزد خود نگه دارید

هرگز رمزهای عبور خود را بر روی کاغذ ننوشته و آنان را به کامپیوتر نچسبانید! . تعداد زیادی از کاربران کامپیوتر دقت لازم در خصوص نگهداری رمز عبور خود را نمی نمایند و همین امر می تواند مشکلات متعددی را متوجه آنان ، نماید . رمزهای عبوری که تشخیص و یا حدس آنان آسان است ، گزینه های مناسبی در این رابطه نمی باشند .

مثلا" در صورتی که نام شما Ali می باشد ، هرگز رمز عبور خود را با همین نام در نظر نگیرید . در فواصل زمانی مشخص و به صورت مستمر ، اقدام به تغییر رمز عبور خود نمائید . هرگز رمز عبور خود را در اختیار اشخاص دیگری قرار ندهید.برای انتخاب یک رمز عبور از ترکیب اعداد ، حروف و علائم استفاده گردد تا حدس و ردیابی آنان توسط افراد غیرمجاز ، مشکل شود .

- استفاده از فایروال ها به منظور حفاظت کامپیوترها

نصب و پیکربندی یک فایروال کار مشکلی نخواهد بود. یک فایروال ، امکان دستیابی و کنترل سیستم توسط مهاجمان را سلب نموده و پیشگیری لازم در خصوص سرقت اطلاعات موجود بر روی کامپیوتر را انجام می دهد .

- Back-up گرفتن منظم از اطلاعات ارزشمند موجود بر روی کامپیوتر

در فواصل زمانی مشخص و بر اساس یک برنامه خاص از اطلاعات ارزشمند موجود بر روی کامپیوتر backup گرفته شده و آنان را بر روی رسانه های ذخیره سازی نظیر لوح های فشرده ذخیره نمود .

- دریافت و نصب منظم Patch های بهنگام شده مربوط به نقایص امنیتی

نقایص امنیتی به صورت مرتب در سیستم های عامل و برنامه های کاربردی کشف می گردند . شرکت های تولید کننده نرم افزار ، به سرعت اقدام به ارائه نسخه های بهنگام شده ای با نام Patch نموده که کاربران می بایست آنان را دریافت و بر روی سیستم خود نصب نمایند.در این رابطه لازم است به صورت منظم از سایت های مربوط به تولید کنندگان نرم افزار بازدید بعمل آمده تا در صورت ارائه Patch ، آن را دریافت و بر روی سیستم نصب نمود .

- بررسی و ارزیابی امنیتی کامپیوتر

وضعیت امنیتی کامپیوتر خود را در مقاطع زمانی مشخصی ، بررسی نموده و در صورتی که خود نمی توانید این کار را انجام دهید از کارشناسان ذیربط استفاده نمائید .

- غیر فعال نمودن ارتباط با اینترنت در زمان عدم استفاده

اینترنت نظیر یک جاده دو طرفه است . شما اطلاعاتی را دریافت و یا ارسال می نمائید. غیرفعال نمودن ارتباط با اینترنت در مواردی که به آن نیاز نمی باشد، امکان دستیابی سایرین به کامپیوتر شما را سلب می نماید.

- عدم اشتراک منابع موجود بر روی کامپیوتر با کاربرانی که هویت آنان نامشخص است سیستم عامل نصب شده بر روی یک کامپیوتر، ممکن است امکان به اشتراک گذاشتن برخی منابع موجود نظیر فایل ها را با سایر کاربران شبکه، فراهم نماید. ویژگی فوق، می تواند زمینه بروز تهدیدات امنیتی خاصی را فراهم نماید . بنابراین می بایست نسبت به غیرفعال نمودن ویژگی فوق ، اقدام لازم صورت پذیرد

فصل ششم

مراحل اولیه ایجاد امنیت در شبکه

۱-۶- مراحل اولیه ایجاد امنیت در شبکه

شبکه های کامپیوتری زیر ساخت لازم برای عرضه اطلاعات در یک سازمان را فراهم می نمایند . بموازات رشد و گسترش تکنولوژی اطلاعات، مقوله امنیت در شبکه های کامپیوتری ، بطور چشمگیری مورد توجه قرار گرفته و همه روزه بر تعداد افرادی که علاقه مند به آشنائی با اصول سیستم های امنیتی در این زمینه می باشند ، افزوده می گردد . در این مقاله ، پیشنهاداتی در رابطه با ایجاد یک محیط ایمن در شبکه ، ارائه می گردد .

سیاست امنیتی

یک سیاست امنیتی، اعلامیه ای رسمی مشتمل بر مجموعه ای از قوانین است که می بایست توسط افرادیکه به یک تکنولوژی سازمان و یا سرمایه های اطلاعاتی دستیابی دارند، رعایت و به آن پایبند باشند . بمنظور تحقق اهداف امنیتی ، می بایست سیاست های تدوین شده در رابطه با تمام کاربران ، مدیران شبکه و مدیران عملیاتی سازمان، اعمال گردد . اهداف مورد نظر عموما" با تاکید بر گزینه های اساسی زیر مشخص می گردند .

" سرویس های عرضه شده در مقابل امنیت ارائه شده ، استفاده ساده در مقابل امنیت و هزینه ایمن سازی در مقابل ریسک از دست دادن اطلاعات "

مهمترین هدف یک سیاست امنیتی ، دادن آگاهی لازم به کاربران، مدیران شبکه و مدیران عملیاتی یک سازمان در رابطه با امکانات و تجهیزات لازم ، بمنظور حفظ و صیانت از تکنولوژی و سرمایه های اطلاعاتی است . سیاست امنیتی ، می بایست مکانیزم و راهکارهای مربوطه را با تاکید بر امکانات موجود تبین نماید . از دیگر اهداف یک سیاست امنیتی ، ارائه یک خط اصولی برای پیکربندی و ممیزی سیستم های کامپیوتری و شبکه ها ، بمنظور تبعیت از سیاست ها است . یک سیاست امنیتی مناسب و موثر ، می بایست رضایت و حمایت تمام پرسنل موجود در یک سازمان را بدنبال داشته باشد .

یک سیاست امنیتی خوب دارای ویژگی های زیر است :

- امکان پیاده سازی عملی آن بکمک روش های متعددی نظیر رویه های مدیریتی، وجود داشته باشد .
- امکان تقویت آن توسط ابزارهای امنیتی ویا دستورات مدیریتی در مواردیکه پیشگیری واقعی از لحاظ فنی امکان پذیر نیست ، وجود داشته باشد .
- محدوده مسئولیت کاربران ، مدیران شبکه و مدیران عملیاتی بصورت شفاف مشخص گردد .
- پس از استقرار، قابلیت برقرای ارتباط با منابع متفاوت انسانی را دارا باشد . (یک بار گفتن و همواره در گوش داشتن)
- دارای انعطاف لازم بمنظور برخورد با تغییرات درشبکه باشد .(سیاست های تدوین شده ، نمونه ای بارز از مستندات زنده تلقی می گردنند .)

سیستم های عامل و برنامه های کاربردی : نسخه ها و بهنگام سازی در صورت امکان، می بایست از آخرین نسخه سیستم های عامل و برنامه های کاربردی بر روی تمامی کامپیوترهای موجود در شبکه (سرویس گیرنده ، سرویس دهنده ، سوئیچ، روتر، فایروال و سیستم های تشخیص مزاحمین) استفاده شود . سیستم های عامل و برنامه های کاربردی می بایست بهنگام بوده و همواره از آخرین امکانات موجود بهنگام سازی (hotfixes , patches , service pack) استفاده گردد . در این راستا می بایست حساسیت بیشتری نسبت به برنامه های آسیب پذیر که زمینه لازم برای متجاوزان اطلاعاتی را فراهم می نمایند ، وجود داشته باشد .

برنامه های : BIND , Internet Explorer , OutLook ,IIS و sendmail بدلیل وجود نقاط آسیب پذیر می بایست مورد توجه جدی قرار گیرند . متجاوزان اطلاعاتی ، بدفعات از نقاط آسیب پذیر برنامه های فوق برای خواسته های خود استفاده کرده اند .

۲-۶- شناخت شبکه موجود

بمنظور پیاده سازی و پشتیبانی سیستم امنیتی ، لازم است لیستی از تمام دستگاههای سخت افزاری و برنامه های نصب شده ، تهیه گردد . آگاهی از برنامه هائی که بصورت پیش فرض نصب شده اند، نیز دارای اهمیت خاص خود است (مثلا" برنامه IIS بصورت پیش فرض توسط SMS و یا سرویس دهنده SQL در شبکه های مبتنی بر ویندوز نصب می گردد) . فهرست برداری از سرویس هائی که بر روی شبکه در حال اجراء می باشند، زمینه را برای پیمایش و تشخیص مسائل مربوطه ، هموار خواهد کرد .

سرویس دهندگان TCP/UDP و سرویس های موجود در شبکه

تمامی سرویس دهندگان TCP/UDP در شبکه بهمراه سرویس های موجود بر روی هر کامپیوتر در شبکه ، می بایست شناسائی و مستند گردند . در صورت امکان، سرویس دهندگان و سرویس های غیر ضروری، غیر فعال گردند . برای سرویس دهندگانی که وجود آنان ضروری تشخیص داده می شود، دستیابی به آنان محدود به کامپیوترهائی گردد که به خدمات آنان نیازمند می باشند . امکانات عملیاتی را که بندرت از آنان استفاده و دارای آسیب پذیری بیشتری می باشند ، غیر فعال تا زمینه بهره برداری آنان توسط متجاوزان اطلاعاتی سلب گردد. توصیه می گردد ، برنامه های نمونه (Sample) تحت هیچ شرایطی بر روی سیستم های تولیدی (سیستم هائی که محیط لازم برای تولید نرم افزار بر روی آنها ایجاد و با استفاده از آنان محصولات نرم افزاری تولید می گردند) نصب نگردند .

رمزعبور

انتخاب رمزعبور ضعیف ، همواره یکی از مسائل اصلی در رابطه با هر نوع سیستم امنیتی است . کاربران، می بایست متعهد و مجبور به تغییر رمز عبور خود بصورت ادواری گردند . تنظیم مشخصه های رمز عبور در سیستم های مبتنی بر ویندوز، بکمک Account Policy صورت می پذیرد . مدیران شبکه، می بایست برنامه های

مربوط به تشخیص رمز عبور را تهیه و آنها را اجراء تا آسیب پـذیری سیسـتم در بوتـه نقد و آزمایش قرار گیرد .

برنامه های Ripper john the ، LOphtcrack و Crack ، نمونه هائی در این زمینه می باشند . به کاربرانی که رمز عبور آنان ضعیف تعریف شده اسـت ، مراتـب اعـلام و در صورت تکرار اخطار داده شود (عملیات فوق، می بایست بصورت متناوب انجام گیـرد) . با توجه به اینکـه برنامـه هـای تشـخیص رمزعبور،زمـان زیـادی از پردازنـده را بخـود اختصاص خواهند داد، توصیه می گردد، رمز عبورهـای کـد شـده (لیسـت SAM بانـک اطلاعـاتی در ویـنـدوز) را بـر روی سیسـتمی دیگـر کـه در شـبکه نمـی باشـد، منتقل تا زمینه بررسی رمزهای عبور ضعیف ، فراهم گردد . با انجام عملیـات فـوق برروی یک کامپیوتر غیر شبکه ای ، نتایج بدست آمده بـرای هـیچکس قابـل اسـتفاده نخواهد بود(مگراینکه افراد بصورت فیزیکی به سیستم دستیابی پیدا نمایند) .

برای تعریف رمز عبور، موارد زیر پیشنهاد می گردد :

- حداقل طول رمز عبور، دوازده و یا بیشتر باشد .
- دررمز عبور از حروف کوچک، اعداد، کاراکترهای خاص و Underline استفاده شود .
- از کلمات موجود در دیکشنری استفاده نگردد .
- رمز های عبور، در فواصل زمانی مشخصی (سی و یا نود روز) بصـورت ادواری تغییـر داده شوند .
- کاربرانی که رمزهای عبور سـاده و قابـل حدسـی را بـرای خـود تعریـف نمـوده انـد، تشخیص و به آنها تذکر داده شود .(عملیات فوق بصورت متنـاوب و در فواصـل زمـانی یک ماه انجام گردد).

عدم اجرای برنامه ها ئی که منابع آنها تایید نشده است .

در اغلب حالات ، برنامه های کامپیوتری در یک چـارچوب امنیتـی خـاص مربـوط بـه کاربری که آنهـا را فعـال مـی نمایـد ، اجـراء مـی گردنـد.دراین زمینـه ممکـن اسـت، هیچگونه توجه ای به ماهیت منبع ارائه دهنده برنامه توسط کاربران انجام نگـردد

. وجود یک زیر ساخت Public key infrastructure (PKI) ، در این زمینه می تواند مفید باشد . در صورت عدم وجود زیرساخت امنیتی فوق ،می بایست مراقبت های لازم در رابطه با طرفندهای استفاده شده توسط برخی از متجاوران اطلاعاتی را انجام داد. مثلا" ممکن است برخی آسیب ها در ظاهری کاملا" موجه از طریق یک پیام الکترونیکی جلوه نمایند . هرگز یک ضمیمه پیام الکترونیکی و یا برنامه ای را که از منبع ارسال کننده آن مطمئن نشده اید ، فعال و یا اجراء ننمائید . همواره از برنامه ای نظیر Outlook بمنظور دریافت پیام های الکترونیکی استفاده گردد . برنامه فوق در یک ناحیه محدوده شده اجراء و می بایست امکان اجرای تمام اسکریپت ها و محتویات فعال برای ناحیه فوق ، غیر فعال گردد .

۳-۶- ایجاد محدودیت در برخی از ضمائم پست الکترونیکی

ضرورت توزیع و عرضه تعداد زیادی از انواع فایل های ضمیمه ، بصورت روزمره در یک سازمان وجود ندارد .بمنظور پیشگیری از اجرای کدهای مخرب ، پیشنهاد می گردد این نوع فایل ها ،غیر فعال گردند . سازمان هائی که از Outlook استفاده می نمایند، می توانند با استفاده از نسخه ۲۰۰۲ اقدام به بلاک نمودن آنها نمایند . (برای سایر نسخه های Outlook می توان از Patch امنیتی مربوطه استفاده کرد) .

فایل های زیر را می توان بلاک کرد :

نوع فایل هائی که می توان آنها را بلاک نمود .
.bas .hta .msp .url .bat .inf .mst .vb .chm .ins .pif .vbe .cmd .isp .pl .vbs .com .js .reg .ws .cpl .jse .scr .wsc .crt .lnk .sct .wsf .exe .msi .shs .wsh

در صورت ضرورت می توان ، به لیست فوق برخی از فایل ها را اضافه و یا حذف کرد. مثلا" با توجه به وجود عناصر اجرائی در برنامه های آفیس ، میتوان امکان اجرای برنامه ها را در آنان بلاک نمود . مهمترین نکته در این راستا به برنامه Access بر می گردد

که برخلاف سایر اعضاء خانواده آفیس ، دارای امکانات حفاظتی ذاتی در مقابل ماکروهای آسیب رسان نمی باشد .

۴-۶- پایبندی به مفهوم کمترین امتیاز

اختصاص حداقل امتیاز به کاربران، محور اساسی درپیاده سازی یک سیتم امنیتی است. رویکرد فوق بر این اصل مهم استوار است که کاربران می بایست صرفا" دارای حقوق و امتیازات لازم بمنظور انجام کارهای مربوطه باشند (بذل و بخشش امتیازات در این زمینه شایسته نمی باشد!) . رخنه در سیستم امنیتی از طریق کدهای مخربی که توسط کاربران اجراء می گردند، تحقق می یابد . در صورتیکه کاربر، دارای حقوق و امتیازات بیشتری باشد ، آسیب پذیری اطلاعات در اثر اجرای کدها ی مخرب ، بیشتر خواهد شد . موارد زیر برای اختصاص حقوق کاربران ، پیشنهاد می گردد :

- تعداد account مربوط به مدیران شبکه، می بایست حداقل باشد .
- مدیران شبکه ، می بایست بمنظور انجام فعالیت های روزمره نظیر خواندن پیام های پست الکترونیکی ، از یک account روزمره در مقابل ورود به شبکه بعنوان administrator ،استفاده نمایند .
- مجوزهای لازم برای منابع بدرستی تنظیم و پیکربندی گردد . در این راستا می بایست حساسیت بیشتری نسبت به برخی از برنامه ها که همواره مورد استفاده متجاوزان اطلاعاتی است ، وجود داشته باشد . این نوع برنامه ها ، شرایط مناسبی برای متجاوزان اطلاعاتی را فراهم می نمایند. جدول زیر برخی از این نوع برنامه ها را نشان می دهد .

برنامه های مورد توجه متجاوزان اطلاعاتی
explorer.exe, regedit.exe, poledit.exe, taskman.exe, at.exe, cacls.exe,cmd.exe, finger.exe, ftp.exe, nbstat.exe, net.exe, net1.exe,netsh.exe, rcp.exe, regedt32.exe, regini.exe, regsvr32.exe,rexec.exe, rsh.exe, runas.exe, runonce.exe, svrmgr.exe,sysedit.exe, telnet.exe, tftp.exe, tracert.exe, usrmgr.exe,wscript.exe,xcopy.exe

• رویکرد حداقل امتیاز ، می تواند به برنامه های سرویس دهنده نیز تعمیم یابد . در این راستا می بایست حتی المقدور، سرویس ها و برنامه ها توسط یک account که حداقل امتیاز را دارد ،اجراء گردند .

ممیزی برنامه ها

اغلب برنامه های سرویس دهنده ، دارای قابلیت های ممیزی گسترده ای می باشند . ممیزی می تواند شامل دنبال نمودن حرکات مشکوک و یا برخورد با آسیب های واقعی باشد . با فعال نمودن ممیزی برای برنامه های سرویس دهنده و کنترل دستیابی به برنامه های کلیدی نظیر برنامه هائی که لیست آنها در جدول قبل ارائه گردید، شرایط مناسبی بمنظور حفاظت از اطلاعات فراهم می گردد .

چاپگر شبکه

امروزه اغلب چاپگرهای شبکه دارای قابلیت های از قبل ساخته شده برای سرویس های FTP,WEB و Telnet بعنوان بخشی از سیستم عامل مربوطه ، می باشند . منابع فوق پس از فعال شدن ، مورد استفاده قرار خواهند گرفت . امکان استفاده از چاپگرهای شبکه بصورت FTP Bound servers ، Telnet و یا سرویس های مدیریتی وب ، وجود خواهد داشت . رمز عبور پیش فرض را به یک رمز عبور پیچیده تغییر و با صراحت پورت های چاپگر را در محدوده روتر / فایروال بلاک نموده و در صورت عدم نیاز به سرویس های فوق ، آنها را غیر فعال نمائید .

۵-۶- پروتکل SNMP (Protocol Simple Network Management)

پروتکل SNMP ، در مقیاس گسترده ای توسط مدیران شبکه بمنظور مشاهده و مدیریت تمام کامپیوترهای موجود در شبکه (سرویس گیرنده ، سرویس دهنده، سوئیچ، روتر، فایروال) استفاده می گردد .SNMP ، بمنظور تایید اعتبار کاربران ، از روشی غیر رمز شده استفاده می نماید . متجاوزان اطلاعاتی ، می توانند از نقطه ضعف فوق در جهت اهداف سوء خود استفاده نمایند . در چنین حالتی، آنان قادر به اخذ اطلاعات

متنوعی در رابطه با عناصر موجود در شبکه بوده و حتی امکان غیر فعال نمودن یک سیستم از راه دور و یا تغییر پیکربندی سیستم ها وجود خواهد داشت . در صورتیکه یک متجاوز اطلاعاتی قادر به جمع آوری ترافیک SNMP دریک شبکه گردد، از اطلاعات مربوط به ساختار شبکه موجود بهمراه سیستم ها و دستگاههای متصل شده به آن ، نیز آگاهی خواهد یافت . سرویس دهندگان SNMP موجود بر روی هر کامپیوتری را که ضرورتی به وجود آنان نمی باشد ، غیر فعال نمائید . در صورتیکه بهر دلیلی استفاده از SNMP ضروری باشد ، می بایست امکان دستیابی بصورت فقط خواندنی در نظر گرفته شود . در صورت امکان، صرفا" به تعداد اندکی از کامپیوترها امتیاز استفاده از سرویس دهنده SNMP اعطاء گردد .

۶-۶- تست امنیت شبکه

مدیران شبکه های کامپیوترهای می بایست، بصورت ادواری اقدام به تست امنیتی تمام کامپیوترهای موجود در شبکه (سرویس گیرندگان، سرویس دهندگان، سوئیچ ها، روترها، فایروال ها و سیستم های تشخیص مزاحمین) نمایند. تست امنیت شبکه، پس از اعمال هر گونه تغییر اساسی در پیکربندی شبکه ، نیز می بایست انجام شود .

نتیجه گیری

امروزه اکثر فعالیتهای کتابداران در کتابخانه‌ها، به نوعی با کامپیوتر ارتباط پیدا می‌کند. از آنجا که شبکه‌ای کردن کامپیوترها امکان استفاده بهینه از منابع محدود را در اختیار کاربران قرار می‌دهد، استفاده از شبکه در کتابخانه‌ها بویژه درفرایند ذخیره و بازیابی اطلاعات، بسیار رایج است. طبیعتاً کتابداران در حین انجام فعالیتهای روزمره خود، با مشکلاتی در زمینه شبکه برخورد خواهند کرد، علاوه بر آن کتابداران با داشتن شناختی از نیازهای کتابخانه خود در ارتباط با شبکه و آگاهی از مفاهیم پایه‌ای پیرامون ساختار شبکه و ملزومات آن، می‌توانند در کنار متخصصان کامپیوتر، نیازهای اطلاع‌رسانی محیط کار خود را مرتفع سازند.

در تهیه این راهنما سعی بر این بود تا زمینه کسب آگاهیهای اساسی پیرامون شبکه‌های کامپیوتری برای کتابداران فراهم گردد. بدون شک، آگاهی از یک سری اصول اساسی نیاز به روزآمدسازی اطلاعات و ارتقاء دانسته‌ها را منتفی نمی‌سازد. بنابراین شایسته است کتابداران خود را به منظور سازگاری با محیط جدید کتابخانه‌ها آماده ساخته و پیوسته بر دانسته‌های خود در این حوزه بیفزایند.

منابع و ماخذ

[1] D. Zeinalipour, V.Kalogeraki, D.Gunopulos ,Information Retrieval in Peer-to-Peer Networks , University of California ,2003
[2] D. Zeinalipour, V.Kalogeraki, D.Gunopulos ,A Local Search Mechanism for PeertoPeer Networks , University of California ,2002
[3] K.Aberer, F.Klemm, M.Rajman, J.Wu , An Architecture for Peer-to-Peer Information Retrieval , EPFL , 2004
[4] http://www.Freesof.org/CIE/Topics/57.htm
[5] http://www.Dei.isep.ipp.pt/docs/arpa.html
[6] http://www.webopedia.com
[7] http://www.compucom.com
[8] http://www.3com.com/0files/products/guides
[9] http://www.3com.com/0files/guides/100116.html
[10] http://www.alaska.net/research/net/wiring.htm
[11] http://www.pcwebopedia.com/term/0/operating-system.htm
[11] http://www.en.wikipedia.org/wiki/local_area_network